Proceedings of the International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/32/20230783

Standardization of the Application Rules for Presumption in Aiding Cybercrime

- From the Perspective of 1345 Judgments

Yin Yiming[1,a,*]

[1]*School of Humanities and Arts, China University of Mining and Technology, Tongshan District, Xuzhou, China*
a. yym1791542570@163.com
**corresponding author*

Abstract: The crime of aiding cybercriminal activities has shown an explosive growth trend in recent years, evolving to the risk of becoming a "pocket crime". To address the existing challenges and issues with this crime, it is crucial to clarify the connotation and denotation of "knowingly" within the context of this crime and establish a set of relatively standardized and rational inference rules. Through a criminal law analysis of the term "knowingly", judicial pathway reviews, and academic theory reflections, the term should be understood as "know" or "clearly know". This interpretation aims to limit judicial scope and alleviate the pressure on the judicial system. The construction of a standardized set of inference rules for "knowingly" in the context of aiding cybercrime is both necessary and rational. Scholars, both domestic and international, have presented relevant theories, with the current trend favoring an objective-oriented approach complemented by subjective evaluation. After analyzing over a thousand case studies and combining related thoughts, the author proposes a "Weighted Scoring Rule" and offers several recommendations concerning the current judicial system's institutional design.

Keywords: aiding cybercriminal activities, knowingly, inference rules

1. Introduction of the Issue

In the context of the rapid development of the Internet, the industry chain of cybercrime has gradually taken shape, [1] with acts aiding cybercrime playing a role throughout this criminal process. To effectively and comprehensively combat cybercrime, judicial authorities have continuously expanded the application scope of Article 287-2 of the Criminal Law related to the crime of aiding cybercrime activities. Data released by the Supreme People's Procuratorate in July 2022 showed that in the first half of 2022, 64,000 individuals were prosecuted for allegedly aiding cybercrime activities (hereinafter referred to as "aiding cybercrime"), ranking third among all types of criminal offenses. This figure was nearly 130,000 in 2021, which is 9.5 times that of 2020. [2] The application of aiding cybercrime is showing a significant expanding trend. In terms of its definition and application, the legal stance seems to be leaning towards a more lenient recognition. If we cannot promptly clarify the connotation and scope of "knowingly" within aiding cybercrime, and timely establish a relatively

DOI: 10.54254/2753-7048/32/20230783

balanced set of inference rules, there is a risk of blurring its judicial recognition and application, leading to the offense falling into the category of a "pocket crime". [3]

Considering the constitutive elements of aiding cybercrime, offering internet access or other aiding acts require the subjective element where the individual reaches the standard of "knowingly". However, there are divergences regarding the meaning and scope of "knowingly", and a standardized application path has not yet been established, inevitably leading to obstacles in its judicial practice. In light of this, this paper will examine the meaning of "knowingly" and the rules for its inference, proposing solutions for the standardization of these inference rules, aiming to achieve a restriction in its judicial application.

2. Interpretation of the Current Status of the Presumption Application for "Knowingly" in Aiding Cybercrime

2.1. Criminal Law Norm Interpretation of "Knowingly

According to statistics, in the "Criminal Law Amendment (XI)" passed by the 24th session of the Standing Committee of the 13th National People's Congress on December 26, 2020, a total of 41 articles in 46 instances pertain to the stipulation of "knowingly". Article 14 of the General Provisions of the Criminal Law stipulates: "If one is aware that their actions will lead to adverse societal outcomes and either desires or allows such results to occur, thus committing a crime, it is an intentional crime. For intentional crimes, criminal liability should be borne." Furthermore, based on the data results retrieved by the author, there are 39 articles in the Specific Provisions of the Criminal Law relating to intentional crimes that involve the term "knowingly". The only controversial provision is Article 138 of the Criminal Law: "Those who are aware of dangers in school buildings or educational teaching facilities, but fail to take measures or report timely, resulting in serious casualties, shall be sentenced to fixed-term imprisonment of no more than three years or criminal detention; if the consequences are especially serious, they shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years." In the Chinese criminal law academia, the general consensus views the subjective elements of this crime as negligence. Although Professor Zhang Mingkai has academically interpreted the term "knowingly" used in this article, believing it is not equivalent to the "knowingly" in intentional crimes and merely indicates that the perpetrator had foreseen the danger of the harmful result occurring. [4] Nevertheless, including views from both Professor Zhang Mingkai and Professor Wang Xin, the prevailing academic opinion believes that, at a basic stance, the use of "knowingly" in this article is within the category of negligent crimes. [5] It's evident that, with the sole exception of this one provision, nearly all instances of "knowingly" in the current Chinese criminal law system are categorized under intentional crimes. Therefore, the "knowingly" in aiding cybercrime should be classified under intentional crimes. If the meaning of "knowingly" is expanded to not only encompass "know", "clearly know", or "definitely know", but also "might know" or "should know", this approach undeniably increases the risk of criminal negligence inclusion. This not only contradicts the prevailing academic opinion but also deviates from the value orientation of judicial restriction, leading to the risk of the crime becoming a "pocket crime", which isn't conducive to clear judicial practice in the future and accurate application of the principle of legality in criminal law.

On May 8, 1998, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, and the State Administration for Industry and Commerce jointly issued the "Regulations on the Lawful Investigation and Handling of Motor Vehicle Theft and Robbery Cases." Article 17 of these regulations states: "The term 'knowingly' as used in these provisions refers to either 'being aware' or 'should be aware'." [6] Based on this, it can be inferred that the judicial interpretation in China construes "knowingly" to encompass both "being aware" and "should be

DOI: 10.54254/2753-7048/32/20230783

aware", with the latter also falling under the ambit of "knowingly." Professor Chen Xingliang believes that the "knowingly" stipulated in the judicial interpretation belongs to the general provisions' definition of "knowingly", serving as an indicative provision in the concept of criminal intent in the general provisions of the Criminal Law, which is different from the "knowingly" in the specific provisions. [7] The author's view is that Articles 14 and 15 of the Criminal Law stipulate two types of the perpetrator's awareness of harmful consequences: the "inevitable occurrence" and the "possible occurrence." That is, the general provisions of the Criminal Law include both inevitability and possibility in the subjective understanding of harmful consequences by the actor. [8] However, the crux of the matter is that "knowingly" and inevitability as provided in the general provisions are both attributes of intentional crimes, while "ought to foresee" and possibility belong to negligent crimes. Theoretically, "ought to foresee" implies that the actor essentially did not foresee, that is, they were actually unaware; while "should be aware" means the actor was actually aware, having already foreseen, marking a significant difference between the two. [9] Yet, if the situation is such that the actor should have been aware (having already foreseen) but naively believed they could avoid it, leading to harmful societal consequences, they would still fall under the scope of negligent crimes. Hence, "should be aware" cannot escape the risk of being categorized as a negligent crime. In summary, while the judicial interpretation reads "knowingly" to include "ought to know," it's clear that "ought to know" can't evade the risk of negligent crime. Now, by incorporating "ought to know" into the scope of "knowingly" — given that "knowingly" clearly belongs to the category of intentional crimes in the general provisions of the Criminal Law — this leads to a conflation of possibility and inevitability, a collision between negligent and intentional crimes, and a contradictory and awkward situation between the judicial interpretation and the stipulations of the general provisions of the Criminal Law.

To cite a classic example, in 2009, the Supreme People's Court issued the "Interpretation on Several Issues Concerning the Application of Law in the Trial of Money Laundering and Other Criminal Cases" (hereinafter referred to as the "Interpretation on Money Laundering Crimes"). This interpretation emphasized that in order to avoid potential misunderstandings in judicial practice where negligent situations might be incorporated into "knowingly", and to adhere to China's legislative intent that money laundering crimes only encompass intentional crimes, the draft of the "Interpretation on Money Laundering Crimes" ultimately removed the expression "should be aware". It is evident from this that the "Interpretation on Money Laundering Crimes" holds a clear negative stance on the understanding that "should be aware" falls under "knowingly". [10] Thus, the prevalent view in judicial interpretations that "knowingly" is defined as both "being aware" and "should be aware" is evidently untenable. This view presents contradictions, whether it is evaluated from the stipulations of the general provisions of the Criminal Law or from the internal interpretative framework of the interpretations themselves. Therefore, the interpretation of "knowingly" should be confined to the semantics of "being aware", "clearly aware", or "definitely aware". Such an interpretation not only aligns with the stance of the general provisions of the Criminal Law but also reduces the burden in judicial practice of determining whether there is a possibility of an actor's awareness. This allows judicial officers to adjudicate more clearly, thereby enhancing judicial efficiency.

2.2. Judicial Interpretation of the Application of the Meaning of "Knowingly

Through a thorough examination of a substantial number of judgments sourced from the Judgement Documentation Network, I have delineated the research dimensions as follows:

- Case Type: Criminal Cases
- Case Cause: Assisting in Cybercrime Activities
- Case Procedure: First Instance Cases

DOI: 10.54254/2753-7048/32/20230783

- Document Date Range: September 2, 2020, to September 2, 2023
- Document Nature: Judgement
- Document Type: Judicial Document

Upon scanning based on the above criteria, a total of 1,345 sample cases were compiled, and this data set was subsequently analyzed.

To begin with, the current judicial interpretation in our country regarding the understanding of "knowingly" in aiding cybercrime suggests that "knowingly" should encompass both "explicitly aware" and "should be aware", that is, "knowingly" includes both "being aware" and "ought to be aware". There's a significant academic perspective asserting that "knowingly", apart from "explicitly aware", should also encompass "possibly aware", allowing for two cognitive states in the individual: certainty and possibility. Personally, I believe we should adhere to the most fundamental semantics of "knowingly" and confine its interpretation and application strictly within the purview of "explicitly aware".

Upon analyzing the 1,345 judgments as sample data, the results reveal that, in 1,214 cases where inference was required to argue whether an individual acted with subjective knowledge, the cases where "being aware" was equated to the meaning of "knowingly" and was subsequently argued, were most prevalent (762 cases)(see Figure 1), accounting for 59.39% (as shown in Figure 2)of the three perspectives, 62.77% of the inferred cases, and 56.65% of the total sample. Next, the cases where "possibly aware" was used to define the meaning of "knowingly" were fewer compared to "explicitly aware" (441 cases)(see Figure 1), making up 34.37% (as shown in Figure 2)of the three perspectives, 36.33% of the inferred cases, and 32.79% of the total sample. Lastly, cases where the court specifically and clearly argued in sections like "as determined by this court" or "as believed by this court" that the individual "should be aware" were relatively rare compared to the first two scenarios, with only 80 cases(see Figure 1). These accounted for 6.24%(as shown in Figure 2)of the three perspectives, 6.59% of the inferred cases, and a mere 5.95% of the total sample.

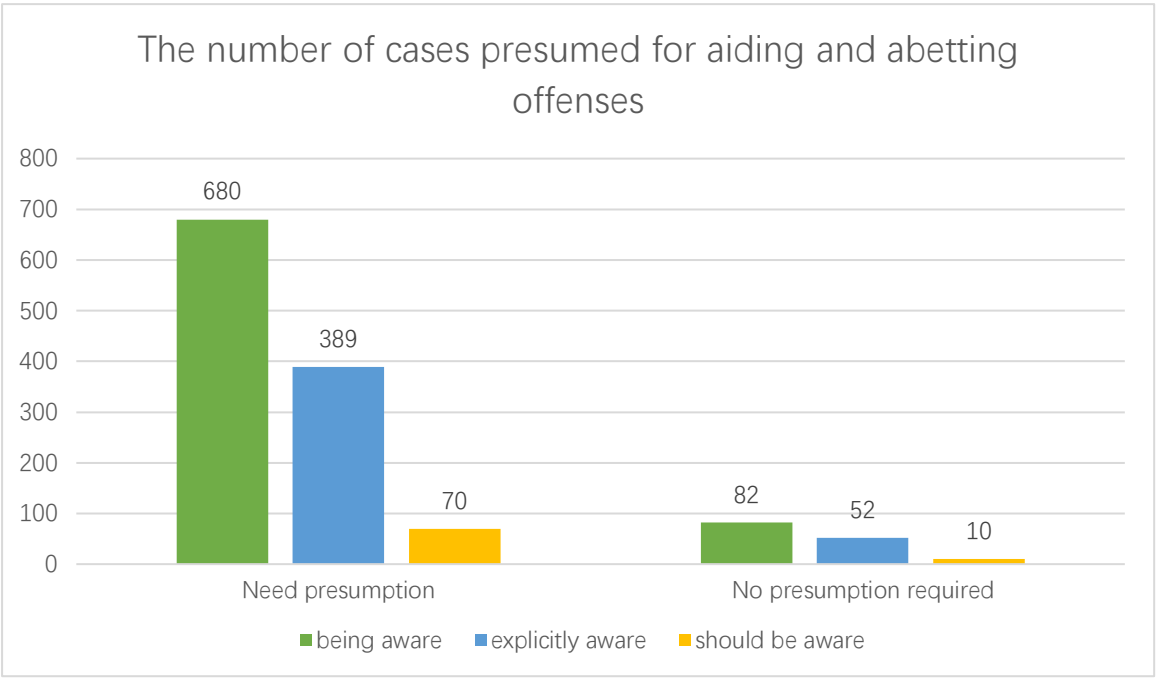

Figure 1: The number of cases presumed for aiding and abetting offenses.

DOI: 10.54254/2753-7048/32/20230783

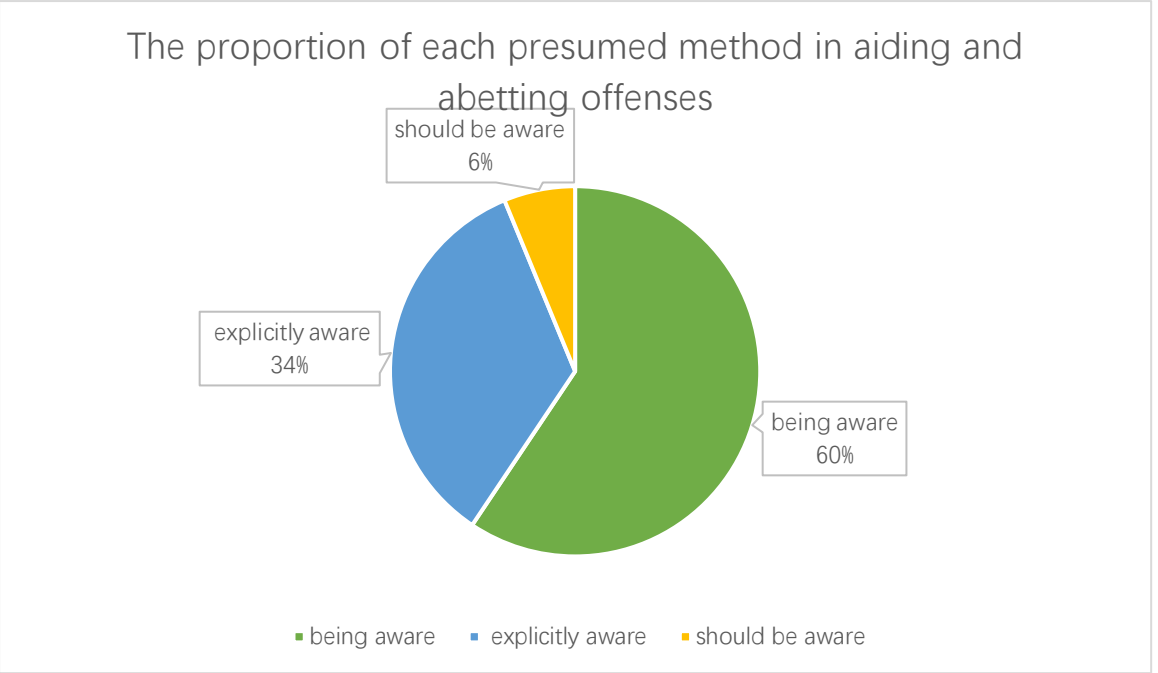

Figure 2: The proportion of each presumed method in aiding and abetting offenses.

Through comprehensive research and empirical analysis of the above data, the following conclusions can be generally drawn: Excluding a small number of cases that don't require inference, out of the 1,214 judgments, those based solely on "being aware" or "explicitly aware" for inference and argumentation were the most numerous (762 cases)(see Figure 1). They were followed by cases based on "possibly aware" (441 cases)(see Figure 1), while the number of cases where "should be aware" was clearly and explicitly argued was quite limited (80 cases)(see Figure 1). Among the three perspectives, judgments that used "being aware" alone as the meaning for "knowingly" to make inferences were in the majority, significantly outnumbering those that used "possibly aware" or "should be aware" for such purposes. This indeed corroborates that the judicial choices made in practice align well with my personal viewpoints. The reason for this is that if there is a possibility of "being aware," it necessarily implies the existence of "possibly not aware." This logically creates certain flaws and gaps, as "possibly not aware" clearly cannot be incorporated into the category of "knowingly" and therefore does not meet the constitutive elements of aiding cybercrime. Thus, it cannot be considered within the system of aiding cybercrime. From another perspective, proving and inferring either "possibly aware" or "should be aware" are both evidently more complex than simply proving "being aware," undeniably increasing judicial pressure and raising the cost of justice. Additionally, the previous discussion provisionally concluded that "knowingly" should fall under the scope of criminal intent. Given that "explicitly aware" is currently the most common interpretation in judicial practice and clearly belongs to the category of criminal intent, this demonstrates a degree of alignment between the theoretical "ought" and the practical "is," thereby reflecting the rationality of judicial practice in guiding academic theory.

2.3. Synthesis and Reflection on Theoretical Disparities in the Semantics of "Knowing Full Well

In the context of criminal law theory and judicial practice, there are academic disputes and disagreements regarding the semantic interpretation of "knowing full well". Mainstream views on this topic can be broadly divided based on a narrow to broad definition of its scope into three

DOI: 10.54254/2753-7048/32/20230783

perspectives:

1. Literal Interpretation: When "knowing full well" is deconstructed from its literal meaning, it should mean "being aware." This can be inferred as "explicitly aware" or "precisely aware." A mere vague awareness or reasonable suspicion cannot be included within the ambit of "knowing full well." In this context, "knowing full well" should possess specificity, directness, and reality, as opposed to being abstract, vague, or potential. [11]

2. Dual Awareness Interpretation: "Knowing full well" should encompass both "being aware" and "possibly being aware." The former refers to an individual having a definitive understanding or awareness of another person's criminal act, where they are sufficiently convinced internally. The latter denotes a possible recognition of another person's criminal act based on the facts of a case, a state of mind where they recognize a possibility but are not completely sure, having a certain degree of probability.

3. Comprehensive Interpretation: "Knowing full well" includes both "being aware" (definite knowledge) and "should be aware" (ought to know). This perspective has been adopted by the judicial interpretations in China, and it holds a certain authority. It's also accepted and agreed upon by most scholars in the field of Chinese criminal law, making it a mainstream viewpoint.

Scholars supporting the first view believe that the second and third viewpoints cannot wholly encompass the constitutive elements of a crime. For example, the "knowing full well" in the second scenario includes "possibly being aware," which inherently implies "possibly not being aware." This creates ambiguity both theoretically and in judicial practice. Determining this is fraught with a degree of probability and poses quantification challenges, often leading to evaluative dilemmas and challenges to the principle of legality in criminal law. [12] However, the opposition to the first viewpoint suggests that such a narrow definition limits the scope of "knowing full well," confining it within an overly restrictive literal semantic space. This potentially provides legal loopholes for malefactors, allowing them room to exploit legal interpretations to evade legal sanctions. Furthermore, the third perspective is the most vocally supported and is the one currently adopted by China's legislation. For example, Article 219, Paragraph 2 of the Criminal Code on the crime of infringing on trade secrets initially articulated subjective intent as "knowing full well or should know." Yet, from March 1, 2021, the "Criminal Law Amendment (XI)" removed this articulation, unifying the representation of subjective intent as "knowing full well" in the Criminal Code. Some judicial interpretations stating that "knowing full well" includes "being aware or should be aware" can be traced back to the 1992 "Interpretation on Several Issues Concerning the Specific Application of the Law in Handling Theft Cases" by the two highest courts. Although this interpretation was abolished in 2013, the provision that "knowing full well" includes "should be aware" has been incorporated into subsequent judicial interpretations and is widely applied in judicial practice. [13]

While the third perspective has been adopted in judicial interpretation, it still encounters the following obstacles:

1. Firstly, "ought to know" falls within the scope of criminal negligence, while the general principles of criminal law categorize "fully aware" as criminal intent. Interpreting "fully aware" as "ought to know" is contradictory to the legislative intent.

2. As evidenced by the above data analysis, cases in current judicial practice where "ought to know" is applied under the presumption rule of "fully aware" are extremely rare, accounting for a very low proportion. This indicates that this viewpoint struggles to find its footing in practical judicial work, with limited applicability, and fails to meet the demands of actual practice.

3. Compared to the straightforward and efficient "knowing," inferring whether the defendant's mental state is "ought to know" is considerably more complex. It demands greater effort and squeezes the already limited judicial resources. This does not align with the current value orientation of China's judicial status, suggesting room for reflection and improvement on this mainstream view. The first

DOI: 10.54254/2753-7048/32/20230783

perspective is more appropriate. It confines the essence of "fully aware" within the semantic boundaries of "explicitly aware" or "precisely aware". Whether from a theoretical analysis or judicial practice standpoint, this perspective has an unparalleled advantage over the other two in terms of precision and practical operability. Under the guidance of the first viewpoint, judicial determinations are undoubtedly more accurate, judicial efficiency is markedly higher, and the difficulty in practical operation is manifestly the lowest. This approach can undoubtedly reduce judicial costs, alleviate the burden in judicial practice, and save judicial resources. In contrast, the second and third perspectives deviate from the original meaning of "fully aware" right from their foundational semantic interpretation. Not to mention, expanding the definition of "fully aware" to include "possibly aware" or "ought to know" contradicts the general semantic concept. Compared to the first perspective, the second and third perspectives not only lack coherence in their theoretical interpretations, presenting inherent contradictions, but also introduce significantly increased difficulty in practical application. The primary critique against the first viewpoint is that its restrictive definition indirectly provides criminals an opportunity to exploit legal loopholes. However, I believe that "fully aware" should only represent a concrete awareness. Mere reasonable doubt cannot be accurately categorized under "fully aware." The term should be understood in its specific sense. When determining if an individual's mental state meets the "fully aware" criteria, there should be no room for ambiguity. While broadening the scope of "fully aware" to include both "explicitly aware" and "possibly aware" or "ought to know" might limit criminals' evasion strategies and cover a wider range of illegal activities, it undeniably introduces confusion and complications in judicial recognition, amplifying the risk of catch-all charges. Furthermore, both the judicial interpretation and the academic consensus state that "fully aware" should encompass both "knowing" and "ought to know." This view risks including criminal negligence. Strictly speaking, "explicitly aware" clearly falls under the category of criminal intent, but "ought to know" cannot be arbitrarily defined as such. This creates a loophole in including criminal negligence, posing challenges to judicial practice. The common flaw of the second and third perspectives is the inherent risk of broadening the scope of what constitutes a crime. Adopting either of these perspectives would necessarily involve incorporating "possibly aware" or "ought to know," essentially further expanding the definition of the crime, leading to a compounded risk of over-criminalization. [14] The first perspective not only aligns most closely with the original and genuine meaning of "fully aware" both in terms of textual content and semantic interpretation, but also restricts its definition, avoiding excessive criminalization. This minimizes the risk of inadvertently categorizing actions as criminal offenses.

3. Value Equilibrium in the "Knowing" Presumption Rule for Assisting Cybercrime

Following the interpretation of criminal law norms related to the meaning of "knowingly" in aiding cybercrime, the analysis of the judicial path, and the summary and reflection on academic theories, the author tentatively concludes: In the elements constituting the crime of assisting cybercrime, the meaning of "knowingly" should be narrowly interpreted as "know," encompassing only "explicitly know" or "definitely know," and should not include "might know" or "should have known." However, clarifying the meaning is only the first step, as situations encountered in judicial practice are often much more complex than in theory. Understanding the linguistic level of "knowingly" is straightforward, but precisely determining in judicial practice whether an actor falls under the "knowingly" category cannot rely solely on the literal meaning. At this juncture, it becomes essential to introduce corresponding presumption rules as powerful tools in judicial discretion to assist judicial officials in evaluating whether the actor's actions in various practical scenarios reflect their internal state as "knowingly." Therefore, building a standardized and relatively value-balanced rule for the presumption of "knowingly" is of significant importance to judicial practice.

DOI: 10.54254/2753-7048/32/20230783

3.1. Necessity of Standardizing the "Knowing" Presumption Rule

First, the standardized construction of the presumption rule for "knowingly" in aiding cybercrime can effectively respond to the call for rule of law in the era's development and meet the urgent needs of judicial practice. Since the implementation of the "New Cybercrime Interpretation" on November 1, 2019, the number of cases involving aiding cybercrime has surged, showing an explosive growth trend. The "Card Suspension" action launched nationwide in October 2020 brought a large number of illegal and criminal cases of selling or renting "dual cards" into the criminal procedure, greatly increasing the application rate of aiding cybercrime. From January to September 2021, the number of prosecutions for this crime by national procuratorial organs reached over 79,000, an increase of 21.3 times year-on-year [Sun Fengjuan: "National Procuratorial Organs' Main Case Data from January to September," published in "Procuratorial Daily," Issue 1, 2021]. The Supreme People's Procuratorate released a set of case data in July 2022: in the first half of 2022, 64,000 people were prosecuted for alleged cybercrime assistance, ranking third among all types of criminal offenses; in 2021, nearly 130,000 people were prosecuted, which is 9.5 times that of 2020. [15] Meanwhile, scholars have counted the number of effective judgments on aiding cybercrime in recent years: from 2015 to 2019, the number of effective judgments were 1, 2, 10, 22, and 81, respectively. In 2020, there were 2,371 cases (20.44 times the sum of the previous five years), and 17,299 in 2021 (6.93 times the total of the previous six years). [16] The sudden increase in the number of criminal cases undoubtedly puts tremendous pressure on the current judicial system. As is well known, China's judicial resources have long been scarce, and there's a significant imbalance between the number of judicial staff and the number of judicial cases, especially in grassroots courts, which often face the pressure of adjudicating a massive number of cases. With the steady advancement of the rule of law strategy in recent years and the continuous strengthening of the legal consciousness of the people, judicial demand is increasing. However, judicial resources are hard-pressed to meet current needs, resulting in a severe mismatch between supply and demand. Given the current growth trend of aiding cybercrime cases, if these challenges and issues are not addressed promptly, the imbalance between judicial resource supply and demand will further exacerbate. At this time, clarifying the connotation and extension of "knowingly" in aiding cybercrime and constructing a relatively standardized applicable presumption rule becomes particularly important. By standardizing the construction of the presumption rule and using theory to guide practice, it is possible to effectively address current challenges and pain points in judicial practice, alleviate the case-handling burden of the judicial system, especially grassroots courts, and save and efficiently use judicial resources.

Secondly, after a thorough analysis of 1,345 verdict documents sourced from the Judgments Online database and subsequent data processing, it was ascertained that among these verdicts, 1,158 cases, or 86.10%, specifically referred to "knowingly" assisting crimes related to "telecommunications fraud". Additionally, 522 cases, or 38.81%, specifically cited "knowingly" assisting crimes linked to "online gambling". Without accounting for overlaps, crimes related to aiding and abetting primarily involved telecommunications fraud, followed by online gambling. Other types of upstream crimes were sporadically distributed across various crime categories, with a minute fraction not categorized or unclassifiable under a specific type of cybercrime. Notably, just the telecommunications fraud-related cases alone accounted for nearly 90% of the total. Through the study of these judicial documents, it became evident that a substantial number of judicial decisions not only have an arguably inappropriate presumption regarding the meaning of "knowingly", but there is also ambiguity in determining which criminal activities should fall under the category of "crimes committed using information networks". As such, a definitive and unified evaluation standard is challenging to establish in current judicial practice. To illustrate with specific cases: in the cases involving individuals named Tu and Wan, the judgment generally stated that the defendants purchased a large

DOI: 10.54254/2753-7048/32/20230783

number of bank cards in large quantities to assist others in committing cybercrimes, without detailing the exact nature of these crimes, making the description abstract. In Xue's case, it was explicitly mentioned that others used equipment and phone cards set up by Xue to commit online fraud. In Xu's case, it was noted that the defendant, Xu, while being aware of the illegal operation of a gaming private server by criminals, still provided technical support for its iOS platform listing. In the case involving Zhang and Tan for the illegal use of information networks, it was clearly stated that defendants Tan, Zhang, and Qin, despite being aware that the online advertisement for boosting online metrics was fraudulent (without repayment of capital after clicking farming), continued to aid others in posting such scam advertisements. In the case against Long and Li for copyright infringement, the defendant, Cheng, despite being aware that the operators of "Waiwai Shenwu" were unlawfully setting up and operating a private server game via the internet, still connected with the "Waiwai Shenwu" private server website through the "Pai Love Payment" platform, facilitating player recharging and payment settlements. In the case against Zhao, the defendant, Zhao, despite knowing the requirements to provide business licenses, the legal person's ID, and other documentation for payment interface application, and being aware of the potential misuse of the illegal payment interface for criminal fund transfers and money laundering, still applied for a payment account with a third party using pre-purchased corporate information and fake domain records. He then sold these accounts to others, charging between 2,000 to 3,500 yuan per account, and taking around 0.3% of the deposited amount in those accounts as profit. From the aforementioned cases and data, it's evident that crimes of aiding and abetting, especially those "knowingly" done, in judicial practice, include not just telecommunications fraud and online gambling but also illegal operation of gaming private servers, money laundering, and other crimes. It is challenging to categorize them simply under the larger umbrella of "cybercrimes". In light of this, there is an evident need to establish standardized rules for making determinations in such cases.

Moreover, there are shortcomings and deficiencies in the current judicial interpretations, which necessitate the support and supplementation of standardized inference rules. Among the numerous judicial interpretation rules in effect, the main provisions and articles related to the presumption rule of "knowingly" assisting in internet crime are found in the "Interpretation on New-Type Internet Crime," the "Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases of Telecom and Internet Fraud (II)," and the "Meeting Minutes on 'Disconnecting Cards'." Specifically, the 11th article of the "Interpretation on New-Type Internet Crime" regarding the criterion for "knowingly" aiding in cyber-crimes is not necessarily comprehensive or optimal. The 7th provision, which addresses "other circumstances that sufficiently determine the knowledge of the actor," serves both as a catch-all clause and an area for judicial interpretation that allows for revisions and improvements. Firstly, the third provision of the "Interpretation on New-Type Internet Crime" posits that transactions "with conspicuously abnormal prices or methods" can be inferred as "knowingly." However, the interpretation lacks a quantitative metric for transaction prices and a clear standard for defining "conspicuously abnormal transaction methods." The sixth provision states that providing technical support or assistance "to help others evade regulation or investigation" needs to be differentiated into at least two scenarios: If one knowingly provides technical support or assistance to someone intending to evade regulation or investigation, it clearly falls under the category of "knowingly" assisting in a crime. However, if only a part of an individual's existing technology is integrated or borrowed into the overall technology for evasion, and the technology owner is not fully aware, there is significant ambiguity in categorizing this as "knowingly" assisting in a crime. "The law cannot compel someone to perform to the best of their intellect and understanding." [17] When an individual provides technical support or assistance, they are not inherently obligated to verify the real purpose of the requester. However, some provisions in the "Interpretation on New-Type Internet Crime" require the actor to bear the adverse consequences, raising questions about the complete

DOI: 10.54254/2753-7048/32/20230783

rationality of such provisions.

Lastly, the standardization of the "knowingly" presumption rule can effectively protect the legal interests of the people and prevent the crime of aiding and abetting from evolving into a catch-all "pocket" crime. "If the handling of criminal cases and the application of criminal law are solely based on doctrinal interpretations without resonating with the concerns and sentiments of the public, they may deviate from the people's sense of fairness and justice, failing their expectations." [18] Lastly, the standardization of the "knowingly" presumption rule can effectively protect the legal interests of the people and prevent the crime of aiding and abetting from evolving into a catch-all "pocket" crime. "If the handling of criminal cases and the application of criminal law are solely based on doctrinal interpretations without resonating with the concerns and sentiments of the public, they may deviate from the people's sense of fairness and justice, failing their expectations."

3.2. Theoretical Reflection on the "Knowingly" Presumption Rule

Regarding the theoretical conception of the "knowingly" presumption rule for aiding and abetting cybercrime, scholars from both domestic and international criminal law circles have differing perspectives. Some scholars propose the "Majority Rule," arguing that it should be the most rational quantitative measure for determining the "ought to know" in the crime of aiding internet-based criminal activities. [19] The "Majority Rule" refers to the premise that if electronic evidence shows that over half of the neutral business activities assisted are used for committing crimes via the internet, it should be presumed that the internet service provider should have known or had sufficient reason to suspect that their business activities supported entities committing online crimes, yet they still decided to provide technical support and assistance. If more than half of their service recipients are involved in criminal activities, this can lead to the presumption that the neutral business actor had an "ought to know" subjective awareness. Firstly, this theoretical conception is based on the presumption of "ought to know" in the crime of aiding and abetting. Hence, the proponents inherently assume that "knowingly" in the crime of aiding and abetting should encompass "ought to know." However, as the author argued earlier, it is more rational to believe that "knowingly" in the crime of aiding and abetting should not include "ought to know." Therefore, due to this difference in foundational assumptions, not only will there be theoretical discrepancies, but the practices guided by these theories will differ as well. However, regardless of whether one supports the inclusion of "ought to know" within "knowingly" or believes that "knowingly" means only "explicitly aware," both approaches aim to determine a unique cognitive state within the actor's mind. In other words, regardless of whether the actor's mental state regarding "others using the internet to commit crimes" pertains to a certain or probable awareness, it still needs to be proven and inferred in judicial practices and rulings. Therefore, even if the "Majority Rule" was originally designed to determine "ought to know," it doesn't prevent us from drawing insights from its underlying wisdom. It undoubtedly has value worth studying and researching. The "Majority Rule" offers a quantifiable metric for determining "knowingly" in judicial practices, representing a clear and precise standard. However, due to the inherent strictness of any highly objective criteria, there are bound to be omissions and deficiencies in flexibility. Given the diverse scenarios in judicial practices, relying solely on a single criterion to handle the myriad of individual cases will inevitably result in oversights and errors, often failing to meet the diverse demands of practical situations.

It's worth noting that in the realm of online intellectual property crimes, the U.S. criminal law community has introduced a notable presumption rule known as the "Red Flag Standard." [20] This rule suggests that if facts and circumstances regarding another party's infringement actions are as blatant as a brightly colored red flag waving openly before an internet service provider, to the extent that the provider could not possibly remain unaware of the infringement, then the service provider can be deemed to have "knowingly" been aware. The rule originated in the United States and has

DOI: 10.54254/2753-7048/32/20230783

since been widely adopted by countries around the world. The core essence of this presumption rule involves a comprehensive application of general societal concepts for judgment. For instance, a history of bearing civil, administrative, or criminal responsibilities, charging fees significantly above the industry standard, manipulating, transferring, or forging relevant industry qualification certificates, destroying evidence or providing false proofs, and having special business collaborations and vested interests, among others, can all be integrated as elements for consideration within this reference system. Contrary to the "Majority Rule," the "Red Flag Standard" provides a relatively broad conceptual framework for presumption research. Its inclusivity is high, and the determination criteria are relatively more flexible. However, it also introduces challenges such as an unclear presumption rule, relatively vague and generalized determination criteria, making it difficult to find a relatively objective point of entry.

In conclusion, when considering the presumption rules surrounding the meaning of "knowingly," from both theoretical and practical perspectives, the challenge lies in finding the most applicable balance between objectivity and subjectivity, as well as between absoluteness and relativity. This holds significant research value.

3.3. Predominant Objective Value Tendency in the Presumption Rules of "Knowing"

While current judicial interpretations and existing rules remain imperfect, the objective value trend manifested in the presumption rules for "knowing" in aiding and abetting cybercrimes can still be discerned. The prior sections mainly discussed the two theories of presumption rules, namely the "Majority Rule" and the "Red Flag Standard." After analysis, it's evident that the "Majority Rule" possesses a high degree of objectivity and quantifiability but lacks a comprehensive judgmental framework, with criteria that seem quite singular. In contrast, the "Red Flag Standard," while comprehensive with a broader scope, leans heavily on subjectivity, somewhat sidelining objectivity. Given this, the author proposes that a main direction for research is to find a relative value balance between subjectivity and objectivity. By comparing the "Majority Rule" and the "Red Flag Standard," and considering their respective merits and shortcomings alongside the preferences and tendencies demonstrated in the newly issued "Interpretation on New Types of Cybercrimes," it becomes apparent that mainstream official authority gravitates towards a more objective standpoint. More specifically, the tendency leans towards a combined value approach—predominantly objective while also accommodating subjectivity—a stance the author personally agrees with and endorses. Firstly, regardless of how comprehensive or perfect a theory may seem, it must ultimately be applicable in real-world practice. Given the characteristic of theory guiding practice, all presumption rules intended for judicial application inevitably lean towards objectification, as only objective rules can truly be applied and operationalized. While subjective-oriented rules might appear more complete theoretically, they risk being excessively intricate and often prove challenging to translate into concrete practical results. Secondly, compared to subjective rules, objective rules are often clearer. This not only facilitates precise understanding and judgment but also can significantly enhance judicial efficiency, save on judicial costs, and effectively utilize and mobilize judicial resources. Thirdly, acknowledging the superiority of objectivity over subjectivity in this field doesn't negate the value of subjectivity entirely or unreservedly affirm objectivity. A commendable theoretical framework or set of rules will extract the essence, discard the superfluous, thoroughly delve into the strengths of all aspects, combine them, and also endeavor to avoid flaws and address deficiencies. Thus, the author believes that the current value stance and orientation for the presumption rules of "knowing" in aiding cybercrimes should predominantly focus on objectivity, incorporate subjectivity, and combine and apply both comprehensively to achieve a genuine value balance.

DOI: 10.54254/2753-7048/32/20230783

4. Constructing the Applicable Pathway for the Presumption of Aiding Cybercrimes

From the discussions above, it is evident that there is a necessity to structure the rules for the presumption of aiding cybercrimes, and the presumption of "knowingly" should predominantly be objective, while also incorporating subjective elements. However, after the author's analytical review, current legal theories such as the "Majority Rule" and the "Red Flag Standard" have imperfections and room for improvement. Based on this, it's essential to further deduce the "is" from the "ought" in the presumption rules for aiding cybercrimes, to construct a standardized and rational judicial application pathway.

4.1. Clarification of the "Knowingly" Subject

Reviewing from a legislative perspective, Article 12, Paragraph 2 of the "Interpretation on New Types of Cybercrimes" stipulates: If one commits the behaviors stated in the previous paragraph and cannot verify whether the aided subject reaches the extent of committing a crime due to objective conditions, but the total related amount reaches five times or more of the standards set in items 2 to 4 of the previous paragraph, or results in especially severe consequences, the individual should be held criminally responsible for aiding cybercrime activities. Firstly, according to Article 12 of the "Criminal Procedure Law": No one shall be deemed guilty without a lawful judgment by the People's Court. In essence, for one's actions to constitute a crime in the truest sense, it must satisfy both formal and substantive elements—that is, it must be judged as a crime through legal procedures and substantively conform to the crime's definition. The provision in the "Interpretation on New Types of Cybercrimes" breaks this norm, essentially creating an exception. If any of the following four situations are met, it surpasses the semantic restrictions of "committing a crime using information networks":

1. Payment settlements of over 1 million yuan.
2. Providing funds exceeding 250,000 yuan through advertising or similar methods.
3. Illicit gains over 50,000 yuan.
4. Causing especially severe consequences.

In essence, the existence of the above four situations replaces the determination of "crime," meaning that even if the act doesn't semantically constitute a "crime," its substantive determination in judicial practice has an equivalent effect to "crime."

In summary, due to the diverse nature of crimes in current judicial practice, making it challenging to discern if they pertain to cybercrimes, and in combination with the standards of the "Interpretation on New Types of Cybercrimes," the author believes that the "knowingly" subject of aiding cybercrimes, or the upstream crime, should be interpreted more broadly. If it meets the basic crime elements, then there is no need to be entangled with whether it can be classified as "cybercrime" in the strictest sense. If it does not meet the crime elements, it should be judged against the circumstances in the "Interpretation on New Types of Cybercrimes" that break the semantic limitations of "committing a crime using information networks." In both scenarios, if one is met, it can be considered the subject of "knowingly" in aiding cybercrimes. If neither is met, then it does not fall under the category of the "knowingly" subject in aiding cybercrimes.

4.2. Conceptualizing the "Weighted Scoring Rule"

Empirical research has shown that the application rate of Article 11 of the "Interpretation on New Types of Cybercrimes" in judicial practice is only 15.3%. [21] The "Interpretation on New Types of Cybercrimes" provides a judicial perspective for the presumption of "knowingly" in aiding cybercrimes. However, as explored earlier by the author, it still has vulnerabilities and imperfections. On a theoretical level, the "Majority Rule" offers an objective quantitative measure but lacks

DOI: 10.54254/2753-7048/32/20230783

flexibility; the "Red Flag Rule" introduces a diversified judgment mechanism but is more subjective. The "Weighted Scoring Rule" proposes incorporating all composite factors as references, assigning different weights based on the severity of subjective malice each factor portrays, and tallying scores. If certain conditions are met, points are added, and when the aggregate score reaches a particular threshold, it can be presumed as "knowingly." The strength of the "Weighted Scoring Rule" lies in its amalgamation of the objectivity and quantitative benefits of the "Majority Rule" and the multifaceted considerations of the "Red Flag Rule." Compared to the approach of Article 11 of the "Interpretation on New Types of Cybercrimes," it offers a more refined quantitative scale and objectivity. Moreover, it circumvents the subjectivity shortfall of the "Majority Rule" and the overgeneralization of the "Red Flag Rule." By integrating each subjective judgment factor into its evaluation system, the "Weighted Scoring Rule" compensates for the subjectivity gap and retains objectivity through a quantifiable point system. This rule effectively bridges subjective and objective judgments, identifying a relatively rational threshold, achieving an optimized balance of values.

To illustrate the operation of the "Weighted Scoring Rule": assuming a higher score indicates a stronger inclination toward the presumption of "knowingly," and if the total score is set at 100 points, then electronic evidence showing more than half of neutral business activities aiding cybercrimes, as prescribed by the "Majority Rule," would be assigned a weight of 30% (or thirty points). Once this situation occurs, 30 points are added to the total score. Similarly, for example: A history of assuming civil, administrative, or criminal responsibilities is weighted at 15%. Charging fees significantly above industry standards is weighted at 10%. Falsifying, transferring, or forging relevant industry certifications is weighted at 15%. Destroying evidence or providing false proofs is weighted at 20%. Possessing unique business cooperation and vested interests is weighted at 10%.

Accumulating scores based on the occurrence of each situation and assuming 50 points as the benchmark threshold, if an individual's neutral business activity aids cybercrimes over the majority (adding 30 points) and provides false evidence or proofs (adding 20 points), reaching a combined score of 50 points, it can be presumed as "knowingly."

However, the proposition of the "Weighted Scoring Rule" is currently a bold hypothesis and conjecture from the author, and its feasibility requires further deliberation. Nonetheless, the core idea is clear, synthesizing the advantages of various doctrines while avoiding their limitations and shortcomings. It aims to find a relatively applicable balance between subjectivity and objectivity, academic theory, and judicial practice.

4.3. Judicial Rule Application and Recommendations

Firstly, the burden of proof for the accused must strictly adhere to the current standards without any reduction. The standard of proof for "knowingly" aiding cybercrimes has not changed due to the application of the presumption rule and should still follow the criminal conviction proof standard of "evidence being true, sufficient, and excluding reasonable doubt." Since the release of the "Interpretation on New Types of Cybercrimes", the identification of aiding cybercrimes in judicial practice has become overly broad, increasingly resembling a catch-all or "pocket crime." Precisely because of this, it's imperative to adhere strictly to the criminal evidence standard, follow the "legality principle" in crime and punishment, and rely closely on the established scope set by the legislation. The stipulation in the judicial interpretation of "except where there is contrary evidence" embodies the criminal proof standard of excluding reasonable doubt.

Secondly, leverage the plea-bargaining system. From 2019 to 2021, the application rate of China's leniency system for plea and penalty rose from 49.3% in 2019 to 89.4% in 2021, an increase of 40.1 percentage points. From January to September 2022, this rate further increased to 90.5%. The presumption of "knowingly" in aiding cybercrimes is a relatively complex academic issue. Combining it with the leniency system for plea and penalty can, to some extent, alleviate the difficulty

DOI: 10.54254/2753-7048/32/20230783

of determining subjective knowledge in such crimes. In other words, the explosive growth in the number of aiding cybercrimes cases in recent years indicates that they are generally minor offenses. This suggests that a significant portion of such cases can be resolved through simplified or expedited procedures. Compared to adversarial litigation structures, the complexity of determinations under consensual litigation structures is inevitably reduced. The swift promotion of the leniency system for plea and penalty has played a role in eliminating obstacles in the identification of minor offenses like aiding cybercrimes, thereby providing significant support for a simplified mode of determining subjective knowledge. In conclusion, when there are challenges and dilemmas in assessing and presuming subjective knowledge in aiding cybercrimes, it is not necessary to persistently seek a perfect direct pathway. An alternative approach, adopting a side strategy, can be chosen by introducing the leniency system for plea and penalty to mitigate some of the identification challenges and reduce the pressure on judicial verdicts.

5. Conclusion

The theoretical foundation for the standardization of the presumption rules for aiding cybercrimes (Crime of facilitating criminal activities in the information network) lies in acknowledging that the term “knowingly” within such crimes should be interpreted as “aware of” or “clearly aware of”. This interpretation is not only consistent with the logical consistency at the theoretical level of legal norms but also aligns with the imperative to streamline and enhance judicial practices. The standardization of presumption rules is necessary across various theoretical and practical dimensions and should adopt an orientation primarily based on objectivity, supplemented by subjectivity. Based on this, the author introduces the “Weighted Scoring Rule” built upon the foundations of the “Majority Rule” and the “Red Flag Rule”. This also offers suggestions to the existing judicial rules, providing insights into the presumption rules of “knowingly” for aiding cybercrimes. Clarifying the meaning of “knowingly” in aiding cybercrimes and constructing standardized presumption rules not only advances a new theoretical perspective but also holds practical significance in curbing the surge of such cases in current judicial practice and alleviating the increasing pressure on the judicial system. As mentioned at the beginning of this article, the prevailing backdrop of our times is the continuous development of information network technology, leading to the proliferation of cybercrimes. The evolution of the era necessitates reforms and advancements in the judicial system. If contemporary judicial personnel are ignorant about the specificities of related information network technologies and have no understanding of the upstream and downstream industry chains of cybercrimes, it’s implausible to trust that the current judicial system can fairly and reasonably adjudicate the burgeoning aiding cybercrime cases. Therefore, adjustments and reforms in related domains of the judicial system are imperative. Specifically, for aiding cybercrime cases, judicial reforms can begin with the judicial personnel. Strengthening internal training ensures that professionals within the system possess a clear understanding and awareness of contemporary developments in the field of information networks, including information network technologies, cybercrimes, and the spectrum of black and grey activities online. Introducing guiding mechanisms for typical cases of aiding cybercrimes can facilitate the better dissemination of practical wisdom and experiences in judicial practice. Furthermore, academic seminars and discussions can be organized to allow scholars to critique and suggest from various perspectives, with the crucial objective being to foster internal communication among judicial personnel. This can help find the most appropriate judicial path by amalgamating diverse practical experiences.

References

[1] *Yu Chong. (2017) Interpreting the Normative Criminalization of Aiding and Abetting Cybercrime. China Criminal Law Journal, 1, 80.*

DOI: 10.54254/2753-7048/32/20230783

[2] *The Supreme People's Procuratorate of the People's Republic of China. (2022). The Details of Cases Related to "Aiding and Abetting Cybercrime": Disclosed by the Supreme People's Procuratorate of the People's Republic of China. Retrieved from https://www.spp.gov.cn/spp/zdgz/tj/202207/t20220723_567126.shtml.*
[3] *Chen Hongbing. (2022) Correction of the 'Pocketization' of Aiding and Abetting Cybercrime. Journal of Hunan University (Social Sciences), 2, 128.*
[4] *Zhang Mingkai. (2007) Criminal Law (3rd Edition). Law Press, 1.*
[5] *Wang Xin. (2013) The Meaning and Determination of 'Knowing' in China's Criminal Law: An Analysis Based on Criminal Legislation and Judicial Interpretation. Rule of Law and Social Development, 1, 67.*
[6] *The General Office of the State Council of the People's Republic of China. (May 8, 1998) Provisions on the Lawful Handling of Theft and Robbery of Motor Vehicles. Document No. [1998] 31.*
[7] *Chen Xingliang. (2013) Interpreting 'Knowing' in the Criminal Law Part: Exploring the Approach of Expressive Offense. Jurist, 3, 82.*
[8] *Zhang Wen. (2022) Clarification of the Meaning of 'Knowing' in Aiding and Abetting Cybercrime and the Application of Presumptions. Youth Crime Issues, 6, 107.*
[9] *Qin Xuena. (2013) On the Meaning and Determination of 'Should Know' in the Criminal Law Part and Judicial Interpretation. Journal of Yunnan University (Law Edition), 4, 66.*
[10] *Liu Weibo. (2009) Understanding and Application of the "Provisions on the Specific Application of Law in the Trial of Criminal Cases Involving Money Laundering". People's Justice, 23, 26.*
[11] *Sun Yunliang. (2019) Research on Core Issues of Aiding and Abetting Cybercrime. Forum on Politics and Law, 2, 83.*
[12] *Liu Ke. (2015) An Analysis of Aiding and Abetting Cybercrime: A Perspective on Criminal Acts that Assist in Intellectual Property Crimes on the Internet. Intellectual Property, 12, 48.*
[13] *Zhang Haijun. (2022) Research on Judicial Practice and Difficulties in Cases of Aiding and Abetting Cybercrime. Research on Preventing Juvenile Delinquency, 3, 43.*
[14] *Sun Yunliang. (2019) Research on the Core Issues of Aiding and Abetting Information Cyberrime. Political and Legal Forum, 2, 84.*
[15] *The Supreme People's Procuratorate of the People's Republic of China. (2022). The Details of Cases Related to "Aiding and Abetting Cybercrime": Disclosed by the Supreme People's Procuratorate of the People's Republic of China. Retrieved from https://www.spp.gov.cn/spp/zdgz/tj/202207/t20220723_567126.shtml.*
[16] *Ji Yang. (2022) Simplification of Proof for Aiding and Abetting Cybercrime and Its Limitations. Law Review, 4, 94.*
[17] *[US] Fuller, Lon L. (2005) The Morality of Law. Commercial Press, 11.*
[18] *Hu Yunteng. (2022) Criminal Legal Theory of Xi Jinping's Rule of Law and New Practices Guided by It. Rule of Law and Social Development, 5, 28.*
[19] *Liu Xianquan and Fang Huiying. (2017) Identification Challenges in Aiding and Abetting Cybercrime. People's Procuratorial Daily, 19, 12.*
[20] *Liu Ke. (2015) An Analysis of Aiding and Abetting Cybercrime: A Perspective on Criminal Acts that Assist in Intellectual Property Crimes on the Internet. Intellectual Property, 12, 49.*
[21] *Zhou Zhenjie and Zhao Chunyang. (2022) Empirical Research on Aiding and Abetting Cybercrime: A Sample Analysis of 1081 Judgments. Application of Law, 6, 88.*