Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD30581

From "Knowing Destruction" to "Magnificent Crime": Re-evaluating the Standards for Knowingly in the Crime of Assisting Information Network Criminal Activities

Yi Hin Tuen Muk

ITS Education Asia, Hong Kong, China
briantuenmuk@gmail.com

Abstract. The standard for establishing "knowingly" in China's crime of assisting information network criminal activities has long posed challenges in the Chinese judicial practice. The unidirectional and indirect nature of this offence often created barriers for judicial authorities from effectively deducing the defendant's subjective intention through direct evidence. This paper studies the evolution from "knowing destruction" to "magnificent crime" in the standards for establishing "knowingly" in the crime of assisting information network criminal activities. The result shows that recently, Chinese judicial system faces an imbalance between effectively combating crime and safeguarding individual human rights. Since 2019, judicial interpretation issued by the Supreme People's Court and Supreme People's Procuratorate in China has lower the standard for establishing "knowingly" in China's crime of assisting information network related Criminal activities from "certain knowing" to "general knowing". However, "general knowing" heavily relies on objective facts such as abnormal transaction records to presume the defendant's intention. At the same time, this shift has decreased the standard and boundaries of "knowingly", it has essentially by passed a genuine inquiry into the defendant's subjective awareness, resulting in an overly vague identification standard. Therefore, the doctrine of "wilful blindness" from Anglo and American criminal law offers a new approach to reconstructing the standard for establishing "knowingly" in the crime of assisting information network criminal activities. "wilful blindness" can help by first identifying "red flags" by examining whether the defendant has aware of any suspicious signs and determine did the defendant deliberately avoided confirming those signs.

Keywords: crime of assisting information network criminal activities, knowingly, wilful blindness, certain knowing, general knowing

1. Introduction

With the rapid technological development in China, network has become an indispensable part of people's modern life. Networks and technology provide services such as communication, data transfer and digital payment which enhance human's standard of living. However, the advancement

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.LD30581

in technology has also led to increasingly diverse tools and methods for cybercrime, such as internet fraud.

Moreover, there are now significant differences between the methods and means of cybercrime and traditional crime in China. The current cybercrime ecosystem shows clear features of decentralization and external empowerment. Current criminal activities in China are no longer rely on a complete industry chain, but involved in a flexible “service based” model. Criminals in China can obtain technical from third party to make their crimes more flexible which also make the cost of cybercrime in China extremely low. For example, criminals can purchase sim cards from the third party to commit internet fraud without any personal information provided.

As a result, the crime of assisting information network criminal act was introduced by the Criminal law amendment (IX) in China in 2015. However, there is a problem in this law when the courts are trying to prove the subjective intention (mens rea) of the defendant about “whether do the defendant acknowledge that their client will use the technical support provided by the defendant to commit cybercrime” which also refers to “knowingly” in the crime of assisting information network criminal activities. Due to problem of unidirectional and Indirectness of this offence [1]. Judicial authorities in China face it difficult to prove the mens rea of the defendant of “whether the defendant acknowledges their client will commit cybercrime” through the court evidence. Meanwhile, it creates an over dependence for the Chinese courts by using objective evidence to prove the defendant’s subjective intention such as are there any abnormal transaction records made by the defendant. In order to solve the problem, The Supreme people court and Supreme people Procuratorate in China has introduced a judicial interpretation in 2019 which has lowered the standard for “knowingly” in the crime of assisting information network criminal activities.

Although, decreasing the standard of “knowingly” from “certain knowing” to “general knowing” increases the efficiency of combating cybercrime in China but it also increases the risk of objectively attributing guilty and an imbalance between effectively combating crime and protecting human’s right [2].

Furthermore, the determination of "knowingly " in most cases of assisting information network criminal activities has leads to social unrest with more than a thousand of people claiming that the result of most cases are full of uncertainty and unfairness. Therefore, how to construct a more subjective and fair standard for determining "knowingly" has become a difficult problem that Chinese judicial authorities urgently need to solve [3].

2. A review of the unidirectional and indirect nature of "knowingly" in the crime of assisting information network criminal activities

2.1. The problem of unidirectional in the crime of assisting information network criminal activities when establishing the mens rea “knowingly”

The term unidirectional in the crime of assisting information network criminal activities refers to the unilateral knowledge of the defendant(person who provide technical support to the criminal) in the absence collusion with the person being assisted . Most of the time, the defendants do not have actual knowledge about whether their clients are going to commit cybercrime or not because in most of the cases, there is a lack of connections between the defendant and the criminals. Is it difficult for judicial authorities to prove that the defendants have deliberately provided technical support to the criminals in order to have a capital gain. Because there may be a possibility where the defendant did not notice the risk of their actions.

DOI: 10.54254/2753-7048/2025.LD30581

Therefore, “knowingly” in the crime of assisting information network criminal activities is different from the “knowingly” from the Chinese traditional criminal law. The specific methods for determining "knowingly" in different crimes have both general regularities and certain particularities. This precisely explains the significant difference between the "knowingly" in the crime of assisting information network criminal activities in China's criminal law and the knowledge determination standards for other criminal offenses in the special provisions of China's criminal law.

Taking the co-conspirator in the crime of telecommunications network fraud in China’s Criminal law as an example. According to article 25 of the Chinese Criminal law, a joint crime is a crime committed by two or more than two persons with the same intention and the same purpose which means that the technical support provider must possess the same “criminal purpose” and “intention” to the criminals who are being helped by the technical support provider, as also refers to “two way communication of intention” [4]. However, the requirement of “knowingly” in the crime of assisting information network criminal activities is opposite [5]. In order for the crime to be established, the defendant only requires to unilaterally realize that the principle offender will use the information network to commit crimes, without the need of “two - way communication of intention” [6].

Furthermore, the problem of unidirectional in the term of "knowingly" can easily lead to reliance on "confessions of the accused" in the trial. Once a suspect denies having "one-sided knowledge" in their subjective consciousness, the case becomes difficult to prosecute and may even reach a dead end. Since a two-sided connection between the precursor crime and the subsequent crime is not required, even with irrefutable evidence that the perpetrator committed a cybercrime, it is difficult for judicial authorities to obtain direct evidence that an accomplice had one-sided "knowledge" of the criminal conduct. Therefore, Circumstantial evidence is often necessary.

For example, according to a case reported by the Jinan Intermediate People’s Court in China. The court held that the defendant had “knowingly assisted others in committing crimes”. The only reason given is that the court found serval abnormal transactions record made by the defendant where the court suspect that the defendant has deliberately provided technical support to the criminal at the situation where the defendant knew that the technical support may help for cybercrime. This result shows that the whole conclusion was mainly based on indirect evidence such as abnormal transactions record or abnormal cash flow record made from the bank account of the defendant. The court considered these evidences are sufficient to prove the mens rea “knowing” in the crime of assisting information network criminal activities. However, this ruling has leads to a conflict between “reasonable doubt” in the Common law and create social unrest or debates in the legal circles of China. Some scholars argue that the court judgment is too vague when the court only rely on objective facts when determining “knowingly” [7].

At the same time, other pointed that due to the problem of unidirectional, shifting the standard of “knowingly” from “certain knowing” to “general knowing” is considered as reasonable.

2.2. The problem of indirect nature in the crime of assisting information network criminal activities when proving the mens rea “knowingly ” of the defendant

The term “indirect nature” means that in general, the technician support provider (the accused) often can't directly acknowledge that their actions can be used for cybercrime. Due to the anonymity separation common in cyber offences. The defendant usually don’t know who are they helping or exactly what criminal acts are being committed [8].

At the same time, the criminal chain in cybercrime is different from the chain in traditional crime. The accused of the crime of assisting information network criminal activities are often placed the

DOI: 10.54254/2753-7048/2025.LD30581

end of the criminal chain, which create a huge distance between the accused and the main offender by serval intermediaries. As a result, the accused usually do not notice the final purpose of the crime or the consequences of their actions .

Similarly, when judging whether someone “knowingly” assisted a cybercrime by proving technical supports, courts often lack direct evidence. The courts often rely on objective facts to infer the defendant’s state of mind. This relates to the idea of “one side knowledge” where the accused in the crime of assisting information network criminal activities may sense the risk of their actions by providing technical to their clients but may not know which exact illegal actions will be carried out and which specific clients will use the technical support provided by the accused to commit crime.

3. Why both “certainly knowing” and “generally knowing” should be removed

3.1. The original “knowingly” in the crime of assisting cybercrime

Back in 2015, the Chinese criminal law introduced a regulation known as the crime of assisting information network of criminal activities". the Criminal law amendment(IX) stated that “someone is defined as guilty if they knowingly knew that other party will use the technology provided by them to commit cybercrime but are still willing to provide this service”, it can be argued that the term “knowingly” is not justified clearly at the time when the statute law was established, there definition lack detailed guidance or interpretation by the judicial authorities. as a result, courts in China have applied a strict standard to determine a standard definition of the term “knowingly” which is “certainly knowing”. if this were to be presented using statistical method, in average, level of “knowingly” the defendant is aware of his/her role within a case to be claimed guilty will have to be around 80% to 100%, however, due to the existence of the unidirectional and indirect nature of the standard definition of ”knowingly” committing a crime, the level of standard made it difficult for the court to convict suspicious suspects.

According to the Peking University law database, very few suspects were being charged under the standard of “certainly knowing”. As between 2015 and 2019, an analysis of 69 relevant cases showed that most of the court decisions did not use the concepts of “the defendant should have known” or “might have known” as the standard for “knowingly” (generally knowing) which makes it difficult for the court to combat crimes as the standard for “knowingly” is way too high .

Then, in 2019, a new judicial interpretation issued by the Supreme People’s Court and the Supreme People’s Procuratorate listed seven specific situations where “knowingly” could be possibly presumed [9]. One of the examples were “Generally, a third party payment platform would normally charge a 1.5% fee but suddenly demand over 10 % in a specific case such as involving gambling.” The judicial interpretation stated that an abnormal high fees suggested by the third party payment platform might by a sign of crime, thus supporting a finding of “knowingly” as it’s allowed the courts to determine “knowingly” based on any abnormal objective senses . This change effectively lowered the standard for proving “knowingly”. According to statistics, official data conducted by the Chinese judicial authorities shown that the number of people prosecuted under “ the crime of assisting information network criminal activities” has increased rapidly after when the judicial interpretation was imposed in 2019. The data stated that the number of people who were prosecuted have increased from 449 in 2018 to 13673 in 2020 [10,11]. This demonstrates the impact of decreasing the standard of “knowingly” from “certainly knowing” to “generalise knowing”.

However, when the courts are using “certainly knowing” as a standard of “knowingly”. The courts face it hard to combat crimes as there aren't sufficient evidence to prove the mens rea of the

DOI: 10.54254/2753-7048/2025.LD30581

crime. Therefore, there is a massive gap between effectively combating crimes and protecting human's right.

3.2. Pros and cons of each approach “knowingly”

“Certainly knowing” means that the accused has clear understanding of what they are doing or what they are involved in [12]. For example “The defendant knowingly knew that their provision of technical support will be used for their clients (criminals) to commit internet fraud.” “Certainly knowing” can be broken down into three categories: First, the defendants knew what exactly they are providing. For example, they are selling a bank card or a phone sim card. Second, the defendants knew what specific services they are providing. Third, the defendant knew for sure that the person they are helping will use the technical support to commit cybercrime.

On the other hand, “generalise knowing” means that the defendant knew what kind of service they are providing but merely knows it is possible that their assistance (technical support) could be used for cybercrime . There isn’t a fixed standard for this. Instead, courts always infer it from suspicious behaviour. For instance, if someone deletes their chat history right after proving technical supports to the criminals, courts may see this as an “abnormal objective act” and take as an evidence of “knowingly”.

However, this method of inference is controversial. Some argue that relying on objective facts to guess a person’s subjective state of mind is inaccurate. Deleting chat history may have innocent explanations and it does not accurately prove guilty. If the courts heavily rely on those objective evidence such as abnormal behaviour. The result of the judgement may be unfair and injustice.

While connecting to the problem of indirect nature of this offence. It is hard for the prosecutor to find direct evidence to prove that the accused certainly knows what the criminal would do or will the provision of technical support be used by their clients as a tool for cybercrime [13]. Meanwhile, decreasing the standard of “knowingly” from “Certainly knowing” to “Generalise knowing” may makes it easier to combat crimes and increase the overall efficiency for police and courts. But it may punish people who are merely unaware of the situation and potentially holding them criminally liable for simple mistakes. Although “certainly knowing” may increase the difficulty when fighting crimes, but “Generlised knowing” still can't be considered as a better option for the judicial authorities in China to determine “knowingly” .

In order to show the negative effects of “Generalise knowing”, case laws will be necessary to imply.

In the first case, a man named Wu was accused of “the crime of assisting information network criminal activities” in 2021. During the trial, the court held that the defendant MR Wu “should have known” his help was being used to commit cybercrime Because he admitted he knew the bank cards he provided would be used for cross border transactions in unusual ways. Outside of that, the defendant’s abnormal money flow through his bank credit cards was seems as sufficient for the court to prove “knowingly” [14].

In the second case, In the second case, defendants Zheng and Chen were the owners of an internet cafe. The court claimed that the defendant's cafe lacked security cameras and required patrons to register their identities, and the staff management was appalling. Additionally, it was discovered that one day a patron of the defendant's internet cafe had committed an online scam using a computer provided by the internet cafe of the defendants , resulting in a victim losing roughly 33,000 RMB. As a result, the Shanxi Province Shanyin County People's court charged defendants Zeng and Chen with "the crime of assisting information network criminals activities." The court found Zeng and Chen guilty in this case, stating that they "may have known" that others were using their computers

DOI: 10.54254/2753-7048/2025.LD30581

as a means of committing cybercrime because of inadequate staff management, proving their mens rea of "knowingly" committing this crime.

However, according to the informations provided, there are no direct evidence that demonstrates any personal connected between the defendant and the criminal (the defendant's client), nor was there a proof that the Zeng and Chen were specially aware that the perpetrator would utilize the technologies for internet fraud. According to the judgment, the case essentially hinged on inferring the defendant's awareness based on the possibility that the defendants "might have known someone would exploit the cafe's poor security system to commit crimes". At most, one could argue they might have been aware of the possibility that someone could misuse their services [15]. But their level of awareness might only reach 20% to 30% of the base standard of "knowingly", falling far short of being certain..

Based on cases like these, some observers agree that the current legal standards for "knowingly" are not applied consistently across different courts in China for judgment. The lack of a fixed standard leads to unclear and sometimes unpredictable verdicts, making the current legal system difficult to balance goal of effectively combating cybercrime with the important goal of protecting individuals human rights.

4. "Wilful blindness" as a tool for inferring "knowledge"

4.1. The concept of "wilful blindness"

In order to solve the problems of both "Certainly knowing" and "Generally knowing", some legal experts have looked at the concept of "wilful blindness" from the Anglo and American common law.

In the book "Turning a Blind Eye", the author Sheif Gordon defines wilful blindness as "Wilful blindness exists where A deliberately shuts his eyes to the means of knowledge because he prefers to remain in ignorance. Wilful Blindness should be restricted to the situation where the accused believes that a certain state of affairs exists, knows that he can confirm this belief by taking a simple step like asking a question ,but does not do so" [16]. In pure English, it's meant wilful blindness exist if a person subjectively knows to strongly suspect that there is a criminal activity happening around him, but deliberately avoids confirming it so they can claim they didn't know in order to escape from the responsibility. This idea is oftenly used in Western courts when trying to prove the subjective awareness of the defendants/asscued in the court.

Interestingly, courts in these countries sometimes also struggle with the same problem shown in " the crime of assisting information network criminal activities" where judicial authorities face it difficult to prove "knowingly" in the court. Therefore, it is necessary for people to think " How to deal with someone who suspected a crime but makes sure not have concrete proof?" became a problem from the whole legalisation.

In case R v Moys, a farmer discovered that in one morning, a horse that worth between 600 pounds to 700 pounds has gone missing from it's stable [17]. The very next day, the defendant was found by selling the exact same horse that the farmer was missing by selling it with the price of 400 pounds. The defendant was quickly convicted under section 22(2) of the Theft Act 1968 for the offence of "handling stolen goods"

However, the Theft Act 1968 has clearly stated that " a person if guilty of handling stolen goods if they knowingly or believing the goods to be stolen, dishonesty received them, or assist in their retention, removal, disposal or sale it to other people in order to claim benefit." This shown that in

DOI: 10.54254/2753-7048/2025.LD30581

order from the defendant to be guilty, the court must prove the mens rea of the defendant which means that the court has to prove that the defendant knew that goods are from dishonest .

Over a period of time, the defendant has appealed for justice. The Court of Appeal so far has disagreed with the initial judge's ruling and accepted the appeal.

So far, the judge from the appellate court has started that "To direct the jury that the offence is committed if the defendant , suspecting that the goods were stolen, deliberately shuts his eyes to the circumstances as an alternative to knowing or believing that goods were stolen is a misdirection" [18]. In pure English, its meant that there are situations in which the first-instance judge deceives the jury in first-instance litigation. It would be incorrect to assume that the defendant "knowingly" knew that the products he sold were stolen based only on his suspicions and his willful failure to report the theft. The second-instance judge then went on to say that the court could use the judicial concept of "willful blindness" to ascertain whether the parties were aware that the goods were obtained illegally. The judge also backed the use of "willful blindness" as a means of inferring the defendant's subjective "knowing" state of mind.

4.2. How to apply wilful blindness in court trials

In the case of US v. Oscar Frigerio Milano, the defendant, Frigerio was charged by the US government with the crime of conspiracy to commit money laundering under the US law in 1956. The court has stated that Frigerio worked for a company name "Phone Home", which appeared to operate as selling phones to other electronics devices. But in fact, it was a company that used to launder more than $26 million in drug money. He was prosecuted of wilful blindness and conspiring to commit money laundering with his company [19].

During the trial, the US government and multiple witnesses provide a direct evidence to prove that Phone Home was involved in drug money laundering. However, there is a problem similar with China's "crime of assisting information network criminal activities". Which is even though there is sufficient evidence that prove that the company "Phone Home" was involved in money laundering and it's still remains difficult to prove whether was the defendant aware that the company was engaged with his company money laundering. Although there are evidence that can prove the company has involved in money laundering, their statements could not directly establish that Frigerio actually knew about the money laundering. As the case has gotten closer to a dead end with no clear confession or testimony from either both sides. The judge turned to the concept of "red flag" to determine whether did the defendant Frigerio had actual knowledge and acted with wilful blindness.

"Red flag" refers to a clear sign of potential risk or wrongdoing that should leads to an attention of a "reasonable man". When a man has caught attention of a "red flag", they suspected that there might be a criminal activity existed around them.

The court applied a two steps test. First, whether did the defendant noticed these red flag, and second is whether did the defendant deliberately chose to ignore those red flag after when he had noticed it. Evidence shown that the defendant Frigerio had worked at the company for less than seven weeks and had no access to the computer system in the company that was used to recorded crucial transactions records. Based on the evidence that was given in the court, the court held that the defendant Frigerio had no opportunity to get access to the illegal sense in the company and therefore the defendant Frigerio had no opportune to become aware of any red flags.

The judge further emphasized that not every suspicious circumstance is equal to wilful blindness. For the defendant to be guiltily of wilful blindness, the red flags must be obvious enough that a "reasonable man" in the third party would recognise it [20].

DOI: 10.54254/2753-7048/2025.LD30581

4.3. Applying wilful blindness to the "crime of assisting information network criminal activities" of the important element of "knowingly"

In China's judicial practice, the concept of wilful blindness can help the courts to better understand the defendant's state of mind and their intention. Which makes the court easier to prove the mens rea of the offence. This approach focuses on whether the defendant has notice any red flags in his circumstances such as abnormal transactions records. Then, the court has to find out that did the defendant deliberately chose to ignore those red flags. For example, after dealing with a suspected criminal, did the defendant try to escape from their responsibility by finding any legal loophole such as deleting the chat history between the defendant and the criminals. The practical frame work can be applied in three steps. First, the court should identify whether red flags were present in the situation such as abnormal financial activity. Second, it must shown that the defendant has the ability to notice or recognize these flags. The court can take account into the defendant's educational background, career or past behaviour (like did the defendant has committed similar offences). The third which is also the most important step in the whole trial, after when the court has proved that the there is a red flag in the scenario and the defendant acquires the ability to notice the red flag (as the defendant that's actually noticed it). The court has to prove that did the defendant consciously avoided responding to these warming. For example, deleting the chat history or failing to ask necessary questions. This approach can help to identify the actus reus and mens rea of the defendant which resulting in an increase in the efficiency of the whole trail process.

Take the case of defendants Zeng and Chen, who ran an internet cafe for their business with no identity checks. From the perspective of a reasonable operator, the business model from the case of Zeng and Chen significantly lowers the barrier for criminal activity. If the defendant Zeng and Chen had prior experience in the industry, they should have recognised this risk and take it as a reg flag and make changed to avoid further criminal activities.

So far, the key question is whether the defendants deliberately ignored the risk and the red flags. If they were aware of the risk but took no steps to prevent crimes. The defendant could be guilty under "the crime of assisting information network activities"

In essence, wilful blindness and the crime of assisting information network criminal activities share the same features and characteristics. They both rely on circumstances abnormalities to infer subjective awareness. The main diffence is the standard of liability. Wilful blindness focuses on did they defendant deliberately avoid to prevent the risk, while the crime requires knowing assistance to someone using network serviced to commit cybercrimes.

However,in both cases, the core question is whether the person acted responsibly when faced with possible illegality. A reasonable person who notices suspicious signs would normally try to clarify the situation as not trying to escape away from the situation.

In addition, introducing the concept of wilful blindness into China's judicial practice may not directly solve the problem of this offence. Instead, it offers a more precise way to determine the mens rea of the defendants.

5. Conclusion

Overall, though, the criminal law of China will not be completely fair if wilful blindness is used as a means of identifying "knowingly." To a certain extent, subjective incriminating can be achieved by the judicial authorities using this line of reasoning, which can help them better identify the defendant's subjective consciousness. Additionally, there is agreement that upholding human rights and successfully combating crime go hand in hand.

DOI: 10.54254/2753-7048/2025.LD30581

References

[1] Long Zongzhi, Hu Jia. (2024) “Knowing” identification of aiding information network crime. Journal of Ethnology of Southwest University (Humanities and Social Sciences Edition), 45(1): 61-72.
[2] Liu Xiaomin. (2024) The intermediate path of knowingly determining the crime of assisting information network criminal activities. Legal Application, (6): 165-177.
[3] Zeng Lei. (2023) Judgment Logic and Scope Limitation of “Knowing” in the Crime of Assisting Information Network Criminal Activities. Journal of Chinese People’s Public Security University (Social Sciences Edition), 39(1): 59-66
[4] Wang Jutao and Zhang Shuaijie (2023) Triple Adjustment" approach ensures the approval of "knowingly and aiding" telecom network crimes. Procuratorial Daily Theoretical Edition.
[5] Wang Jia, (2024) Phase-by-Phase Handling of the Difficult Problem of Competing with Aid-in-Aid Crimes and Related Crimes, " Procuratorial Daily Theoretical Edition.
[6] Criminal Ruling of the Intermediate People's Court of Jinan City, Shandong Province (2022) Lu 06 Xingzhong No. 182.
[7] Qin Xuena. (2023) Clarifying the "Subjective Knowledge" Requirement of Aid Based on the Intent Requirement. Procuratorial Daily - Theoretical Edition.
[8] Chen Liwen. (2025) On the "knowing" in the crime of assisting information network criminal activities. Journal of South China University of Technology (Social Science Edition), 27(1): 122-131.
[9] Interpretation of Several Issues Concerning the Application of Law in Handling Criminal Cases of Illegal Use of Information Networks and Assisting Information Network Criminal Activities (2019).
[10] Guo Hongping. (2022) "Aiding in Fraud": Increased 21-fold in one year, becoming the "number one crime" in telecom network fraud. Procuratorate Daily, May 17, 2022. https: //www.spp.gov.cn/zdgz/202205/t20220517_557036.shtml
[11] Zheng Zhi. (2022) From January to September this year, over 92, 000 people were prosecuted for aiding and abetting corruption. Procuratorial Daily, October 30, 2022. https: //www.spp.gov.cn/spp/zhuanlan/202210/t20221030_591203.shtml
[12] Zhiqiang. (2019) On “Knowing” in Criminal Law. Beijing: Legal Publishing House.
[13] Liu Yanhong. (2023) Judicial expansion trend and substantive limitation of the crime of assisting information network criminal activities. China Law Review, (03): 58-72.
[14] Xuan Min. (2025) Research on the identification of "knowingly" in the crime of assisting information network criminal activities. Journal of Liaoning Public Security and Judicial Administration Cadre College, (01): 23-30.
[15] Jiang Luoyi. (2025) Judicial Determination of “Knowing” in the Crime of Assisting Information Network Criminal Activities from the Perspective of “Duality”: A Study of 1082 Related Judgments. Journal of Law, 46(05): 73-93.
[16] Hong Kong Court of Final Appeal. (n.d.-a). https: //www.hkcfa.hk/data.json?lang=C& case_court_sys=FA& case_type=CV& case_ser_no=11& case_yr=2022& i_doc_int_no=1
[17] LawTeacher. (2018, November 30). R v moys. LawTeacher.net. https: //www.lawteacher.net/cases/r-v-moys.php
[18] Hong Kong E. Legislation. (n.d.). https: //www.elegislation.gov.hk/hk/cap210!en.
[19] U.S. v. Frigerio-MIGIANO, 254 f.3d 30: 1st cir., Judgment, law, Casemine.com. https: //www.casemine.com. (n.d.)https: //www.casemine.com/judgement/us/5914b988add7b0493478ba64.
[20] 254 f.3d - volume 254 of the federal reporter, 3rd Series : : US federal case law : : Justia. (n.d.). https: //law.justia.com/cases/federal/appellate-courts/F3/254/.