The Nature and Restriction of the Crime of Helping Information Network Crime

Jindong Gu[1, *,†] Shuhui Song[2,†]

[1] Economic Law School, Southwest University of Political Science and Law, Chongqing, Chongqing, China
[2] Law Faculty, Meiji University, Tokyo, Tokyo, Japan
[*]Corresponding author. Email: 2019022015@stu.swupl.edu.cn

[†]These authors countribute equally.

ABSTRACT
Given the huge number and rapid growth rate of cases related to the crime of helping information network crime, it can be concluded that the crime is likely to be abused. In practice, the crime does not depend on its downstream crimes and the standard of 'knowing' proves rather ambiguous. In theory, there are three theoretical controversies on the fundamental nature of the crime. Each of them has exposed intrinsic drawbacks. Meanwhile, the extent to 'knowing' is unclear surrounded by different opinions. Reasons for such weakness include the contradiction between the theory of aiding acts as principal offender and the theory of accomplice belongingness, unclear judicial interpretation, and different understanding of every judge. The article has put forward two remedies as response. The first one is that the crime should be based on downstream crimes according to different types of cyber assisting actions. The other one is that the extent of 'knowing' should be relatively specific examined by four factors.

Keywords: *The crime of helping information network crime, The theory of accomplice belongingness, Japanese criminal law.*

1. INTRODUCTION

There has been a huge number of cases related to the crime of helping information network crime since the Amendment IX to the Criminal Law of the People's Republic of China came out. According to the relevant information released from the Supreme People's Procuratorate in the first three quarters in 2021, the number of this crime has increased almost 21 times, involving nearly 80,000 people prosecuted [1]. Likewise, based on the Magic Weapon of Peking University, the total number of relevant cases has exceeded 10,000 with an extremely high rate of increase. As a result of such facts, it is possible that the crime of helping information network crime could be abused, developing into 'pocket crime'. There has been much difficulty in applying the crime in both practice and theory. In practice, it has become highly common that the crime is dependent on the rule of helping behavior criminalization and the term 'knowing' is explained as probable intention, which lowers the application standard of the crime. In theory, there has been three doctrines as to the nature of the crime, which are helping behavior criminalization, outward helping behavior criminalization but substantive accomplice belongingness, and sentencing rules. These doctrines, to some extent, are all equipped with intrinsic imperfection. The article will put forward two optimization paths to restrict the crime of helping information network crime. The first path is that the crime should rely on downstream crimes on the basis of different types of cyber assisting actions. The second one is that the extent of 'knowing' should be relatively specific according to four factors. There will be three parts to be analyzed. The first part is the difficulty of the application of the crime of helping information network crime in practice and theory. The second part focuses on the reasons for such difficulty. The third part shows optimization paths with the help of Japanese criminal law.

2. THE WEAKNESS OF PRACTICAL AND THEORETICAL RESEARCH IN CHINA

Current research regarding the crime of helping information network crime has made the standard of application ambiguous both practically and theoretically. In practice, the crucial problem is that the crime is treated

in contradictory ways in different courts, embodied in the connection between aiding activities and downstream crimes and the explanation of 'knowing'. The theorical weakness relies on the practical predicament, illustrated by three incompatible theories on the nature of the crime. The term 'knowing' also raises some debates from different perspectives.

2.1. The Weakness of Practical Research

There is a trend that the crime of helping information network crime in juridical practice in China could be abused. According to the relevant information released from the Supreme People's Procuratorate in the first three quarters in 2021, the number of this crime has increased almost 21 times, involving nearly 80,000 people prosecuted. Likewise, based on the Magic Weapon of Peking University, the total number of relevant cases has exceeded 10,000 with an extremely high rate of increase. Cases ended by first-instance procedure, simple procedure and quick judging procedure have accounted for a large proportion. In addition, in second instance, the judicial decision is almost affirmed in fact. Thus, it is thought that the crime of helping information network crime is commonly dealt with by virtue of the rule of helping behavior criminalization in practice. This demonstrates that it is relatively easy to make decisions on this crime as it does not rely on downstream crimes. Also, the standard of 'knowing' is rather ambiguous, decided as general intention and without objective evidence sometimes. This proves that the explanation of the term 'knowing' is not clear, lacking specific stipulations. Consequently, it can be concluded that the standard of the crime is rather low, which could evolve into 'pocket crime' in the network era if still short of exact guidelines.

2.2. The Weakness of Theorical Research

Theoretical controversies have fiercely been aroused in China's criminal law circle, focusing on the basic nature and legislative terms as to the crime of helping information network crime. However, current theoretical achievements are not clear enough to some extent. The uncertainty would in turn make it hard to make decisions on the crime in practice.

In terms of the basic nature of the crime, the theory of helping behavior criminalization argues that since the criminal law sets the crime of helping information network crime independently, the crime should not rely on downstream crimes [2]. However, this theory does not mean that the independent status should be acknowledged in justice. The range of helping behavior related to the crime is so complex that it is hard to evaluate with a sole standard. It means that neutral helping behavior, marked by normal business activities, would be incriminated. The social harmfulness of this behavior is uncertain, which should be evaluated based on comprehensive factors such as the function and outcome of the behavior [3]. As a result, behavior that does not deserve punishment would be incriminated, which would overturn the principle of suiting punishment to crime. The theory of outward helping behavior criminalization but substantive accomplice belongingness argues that the criminalization should be seen as one characteristic of the crime but still depends on downstream crimes [4]. It has realized the intrinsic tension between criminalization of helping behavior and accomplice belongness. However, this theory makes the standard of this crime more complex, for the connection between the characteristic and application is not clarified exactly. Likewise, it would be difficult to examine the indirect helping behavior for this crime. The theory of sentencing rules contends that the crime relies on downstream crimes [5]. The provision only gives effect to this crime's sentencing rule in exclusion to general sentencing rules as to joint crimes. However, this theory would bring two issues. The first one is that it would preclude the function of the setting of crime name [6]. The other is that it would result in the general provisions with no substantive effect [7].

In terms of 'knowing', there are two problems to be identified. Firstly, there is a debate that whether 'should have known' could be classified into 'knowing'. It is generally believed that 'should have known' creates a presumption that perpetrators understand potential harmfulness. Secondly, the extent to know is not clear enough. Traditionally, it is thought that perpetrators should have a detailed understanding of their behavior, involving its objects, types and etc. However, such traditional standard is supported on 'one helps one' model while cyber assisting actions involve more than one people. It would be too strict to require that perpetrators should be aware of every detail as to people who are helped [8]. In contrast, some argue that it could be concluded as 'knowing' as long as there are possibilities that helping behavior could incur potential crimes. This is similar to the way current judicial authorities deal with the term 'knowing'. It is likely that the number of relevant cases would rapidly increase, making it 'pocket crime'. This would also give too much duty of care to internet service providers, burdening their running cost and thus impeding the development of internet industry [9].

3. THE REASONS FOR THE PREDICAMENT

There are mainly three reasons for the theorical and practical predicament on the crime. Firstly, there is an intrinsic contradiction between the theory of aiding acts as principal offender and the theory of accomplice belongingness. In theory circles, it is thought that these two theories cannot coexist. In other words, a particular

type of behavior can be regulated by one theory only. As a result, the theorical controversy on the crime can be substantially seen as the debate on these two theories on which there have not been a specific and clear conclusion. Some scholars have recently put forward the theory of minimum dependence. It means that the crime of helping information network crime only needs to rely on the outward constitutive requirements of downstream behavior without a need to acknowledge the illegality of the principal offender [10]. Under the theory of minimum dependence, the crime can be explained with both the theory of aiding acts as principal offender and the theory of accomplice belongingness. The purpose of such theory is to lessen their objective tension [11]. However, it is inevitable to avoid the illegality of the principal offender in practice. It is difficult to ignore the intrinsic connection between the constitutive requirements and illegality. The standard of distinguishing constitutive requirements and illegality is so vague that it would be hard for judges to consider such difference [12]. In addition, if downstream behavior that is not illegal can act as the threshold of the crime of helping information network crime, the scope of criminal penalty may be unfairly extended. In other words, it would be unreasonable that the principal offender is not prosecuted but the accessorial criminal is punished. Secondly, the term of 'knowing' is vaguely defined. Judicial interpretation on the crime has demonstrated the objective conditions of 'knowing' according to distinct categories [13]. However, it did not point out the substantial meaning of 'knowing'. In other words, judicial authorities can merely decide the term 'knowing' according to conditions that have been listed. Their discretionary power could be limited as there is no basic standard of 'knowing' to respect. The conditions listed cannot contain all kinds of behavior because the economic and technological innovations are rapidly growing with a huge amount of uncertainty. The numerous innovations would bring many new types of cybercrime helping behavior, which means that the categories of 'knowing' have to be modified constantly to adapt to the technological development. This would increase the burden of judicial authorities since it is extremely difficult for them to understand details of a new type of behavior in a short time. Accordingly, the nature of 'knowing' should be firstly considered rather than finite types of behavior. Thirdly, cases on the crime are resolved based on various reasons in different courts as a result of the theorical uncertainty. There is no unified standard as to the elements of the crime. Consequently, it is hard for judges to learn how previous cases were addressed due to their different conclusions. This could lead to a negative domino effect that courts in different regions adopt controversy standards to consider the crime in the absence of a unified explanation.

4. REMEDIES OF JUDICIAL PRACTICE RELATED TO CYBERCRIME AIDING ACTIVITIES

The article will take Japanese criminal law as reference to tackle the application of the crime of helping information network crime in China. In Japan, until the late 1990s, people's perception of crime risk and crime anxiety did not receive much public attention. The reason is that the public safety of Japan is better than that of western developed countries and that the number of crimes in Japan has been declining since the 1960s. Therefore, it is necessary for Chinese criminal law to borrow from Japan [14]. In Japan, the theory of accomplice belongingness acts as the principle to identify the accessory in Japan. Accordingly, the article will focus on the aiding intention of the offender and the essential causation between the aiding activities and its downstream crimes based on Winny copyright infringement case [15].

4.1. Reference to the theory of accomplice belongingness to Restructure the Finding of Facts

Japanese criminal law recognizes that to identify an accessory it must follow the theory of accomplice belongingness, which has four factors. First of all, the defendant must give limited help and encouragement. Also, the behavior must be controlled under the guilty mind. Subsequently, there must be downstream crimes when deciding the existence of the aiding behavior. Finally, there must be an imperative connection between the help and the downstream crime [16]. Physical promotion is one crucial factor to recognize the connection, which is different in specific cases. For example, in Japan, if a knife is given to A who uses the given knife to commit the killing, then the act of providing the knife can be found to be necessarily linked to the murder. Thus, it can be concluded that the helper is physically contributing to the downstream crime. However, in judicial practice in China the recognition of imperative causation is largely neglected, which is one of the reasons that the application of the crime of helping information network crime become so extensive.

The judicial practice of cybercrime aiding activities should be based on the classification of aiding activities in terms of social harm, given the uncertainty of cybercrime. Some scholars have categorized cybercrime aiding activities according to its function [17]. The first category refers to the aiding activities that significantly contribute to the commission of lower crimes completely. It is expected to be equipped with 80% above likelihood to promote the commission of downstream crimes. The second category is the behavior that contributes to downstream crime partially with the possibility of nearly 30% to 80%. The third category involves the preparation

and finishing touches of the lower crimes regarded as having less than 30% participation.

Whether aiding activities should rely on their downstream crimes is based on such classification. For the first and second category, there is no need of specific downstream crimes. It would be sufficient to know the existence of the crimes only, as the first and second category already have the inclination of being hazardous to society separately. For the third one, since the aiding activities cannot pose social harm independently, the investigation of downstream crimes should be conducted completely, ranging from downstream activities to downstream offenders.

The scope of 'knowing' also corresponds to the three categories of actions. For the first and second category, in view of the more prominent social harm itself, it can be presumed that the subjective state of the perpetrator at least 'should have known'. For the third category, the standard of 'knowing' should be raised due to its lesser social harm. Japanese criminal law uses 'knowing' to examine whether the victim has mens rea. To identify mens rea, there will be four factors that should be concerned. The first factor is the principle of high possibility. Such high possibility depends on whether the provider of assistance has foreknowledge that the person who is given the tools, means and methods will use them to commit a crime. The second one is that whether the tools, means and methods have a general function and whether the provider is unable to precisely know the user's use of the tools, means and methods. The third one is that whether there is an intention of the perpetrator to use the assistance activity for the commission of the offence. The time of 'knowing' should be when the assistance activity is supplied rather than when it has been operated for a while. The final one is whether the value of the assistance activity in other uses outweighs the offence.

4.2. The Degree of Identification of Downstream Crimes and Classification of 'Knowing'

In light of Japanese criminal law, there are two routes to the optimize the application of the crime of helping information network crime. Firstly, cybercrime aiding activities are established as subordinate to downstream crimes with different standards. For the first and second category of actions, they are literally subordinate to downstream crimes and only requires the existence of downstream crimes when identifying 'knowing'. For the third category, since cybercrime aiding activities are substantially subordinate to downstream crimes, the type and objective of the downstream crimes need to be specifically identified. In judicial practice, when it comes to how to correctly distinguish the type of aiding activities, the nature of the aiding activities (for example, the presentation of 'one-to-one' or 'one-to-many'), the breadth of dissemination, the rate of dissemination, profit aiding action and many other factors objectively identified should be specifically concerned.

Such two methods are beneficial to address the theoretic and practical predicament on the crime of helping information network crime. Theoretically, these methods can provide an access for the interpretation of the crime. In judicial practice, it can also provide judges with ways on how to apply the crime. The article has adopted a step-by-step approach to the operation of the offence in judicial practice in order to limit its wide application in the modern society, trying to balance the accuracy of judicial application and legislative significance of the crime. However, the typology of cybercrime aiding activities and the criteria of 'knowing' still require further discussion and depend on practical experience and new theories to explore.

Secondly, the degree of 'knowing' should be distinguished. The state of 'knowing' should be specific between definite mens rea and generalized mens rea, or at least having the 'knowing' of types and objectives of downstream crimes based on four factors. The first one is the principle of high possibility. The existence of this principle depends on whether the provider of assistance has foreknowledge of the possibility that the person who is given tools and methods would use them in the commission of the offence. The second one is whether such tools and methods have an unspecified use. In other words, it is necessary to identify whether the provider is unable to know precisely and unambiguously the user's use of the tools, means and methods. The third one is whether there is an intention to use the assistance activity for the commission of the offence. The time point of 'knowing' should be when the assistance activity is supplied rather than when it has been operated for a while. The final one is that whether the value of aiding activities in other uses outweighs downstream crimes themselves.

5. CONCLUSION

The article has referred to Japanese criminal law to put forward two preferable methods in the judicial practice of the crime of helping information network crime. Firstly, the existence of cybercrime aiding activities depends on downstream crimes. In terms of aiding activities that significantly (80% above) and partially (30%-80%) facilitate downstream crimes, the existence of the downstream crimes is only required. In terms of cybercrime aiding activities regarding preparation and finishing touches of downstream crimes, the existence, the type, and the objective of downstream crimes need to be strictly examined. Secondly, the definition of 'knowing' should be comparatively clearer, which can be explained by four factors. The first one is the principle of high possibility. The existence of this principle depends on whether the provider of assistance has foreknowledge of the possibility that the person who

is given tools and methods would use them in the commission of the offence. The second one is whether such tools and methods have an unspecified use. What has to be examined is whether the provider is unable to know precisely and unambiguously the user's use of the tools, means and methods. The third one is whether there is an intention to use the assistance activity for the commission of the offence. The time point of 'knowing' should be when the assistance activity is supplied rather than when it has been operated for a while. The final one is whether the value of aiding activities in other uses outweighs downstream crimes themselves.

REFERENCES

[1] The Supreme People's Procuratorate of The People's Republic of China, (2021) Data on major prosecution cases from January to September released by The Supreme People's Procuratorate of the People's Republic of China. https://www.spp.gov.cn/spp/xwfbh/wsfbt/202110/t20211018_532387.shtml#1.

[2] Y. Liu. (2016) Criticism of the criminalization of helping behaviour in cybercrime. Study in Law and Business, 3: 18-22. DOI: 10.16390/j.cnki.issn1672-0393.2016.03.004.

[3] H. Chen. (2021) Research on the punishability of network neutral help behavior. Academic Forum, 2: 51-60. DOI: 10.16524/j.45-1002.2021.02.005.

[4] Y. Xiong, Y. Huang. (2016) Judicial application of the crime of helping information network crime. People's Judicature (Application), 31: 75-79. DOI: 10.19684/j.cnki.1002-4603.2016.31.016.

[5] M. Zhang. (2016) A discussion on the crime of helping information network crime. Political Science and Law, 2: 2-16. DOI: 10.15984/j.cnki.1005-9512.2016.02.001.

[6] S. Jiang. (2020) The explanatory direction of the crime of helping information network crime. Criminal Science, 5: 76-93. DOI: 10.19430/j.cnki.3891.2020.05.005.

[7] R. Liu, X. Yang. (2017) Internet context of aiding: a concurrent discussion about reflections on the theory of criminal participation. Science of Law, 3: 123-130. DOI: 10.16290/j.cnki.1674-5205.2017.03.012.

[8] H. Wang. (2019) A critical interpretation of the criminalization of helping behavior in the network context. Law Review, 4: 129-138. DOI: 10.13415/j.cnki.fxpl.2019.04.011.

[9] Z. Wang. (2021) The re-proposal of the theory of minimum dependence and nature of assisting information network criminal activities crime. Tribune of Political Science and Law, 39: 165-179.

[10] Y. Deng. (2019) Can theory of accessory accomplice be applied in transformed principal. Peking University Law Journal, 31: 780-796.

[11] The Supreme People's Court of The People's Republic of China and The Supreme People's Procuratorate of The People's Republic of China, (2019) Explanation on several issues concerning the application of law of criminal cases of illegal use of information network and helping criminal activities of information network. https://www.spp.gov.cn/spp/xwfbh/wsfbh/201910/t20191025_436138.shtml.

[12] Y. Sakaguchi. (2008) Determinants of the Perceived Risk of Crime: The unique factors identified in Japan through an international comparison. Japanese Sociological Review, 59: 462-477. DOI: https://doi.org/10.4057/jsr.59.462.

[13] Winny copyright infringement case, Supreme Court of Japan, No. A1900, December 19, 2011.

[14] A. Yamaguchi. (2015) Criminal Law. Yuhikaku, Tokyo.

[15] J. Deng. (2019) Categorization of Cybercrime Aiding Activities. Chinese Journal of Law, 41: 138-156.