Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/17/20231219

Judicial Determination of the Provision of VPN Behavior

Qing Cao[1,a,*]

[1]*School of Transnational Law, China University of Political Science and Law, Beijing, 102299, China*
a. 200301349@cupl.edu.cn
**corresponding author*

Abstract: The issue of a judicial determination of the act of providing Virtual Private Network software is currently a hot topic of discussion in the judicial practice as well as theoretical urgent, and research has found that many VPN providers have engaged in many illegal acts by taking advantage of loopholes in legislation and justice. The offshore network activities have been categorized as one major national security concern by many countries and VPN providers are surely among those potential criminals. Since the use of offshore networks may involve infringement of national security as well as national ideology, China has implemented restrictions on access to specific foreign networks. However, the reason behind its formation is that there is not yet a uniform interpretation and determination standard for the application of the relevant issues. Therefore, this article will propose a set of unified standards as well as legislative improvement suggestions through the analysis of the crimes involved.

Keywords: judicial determination, VPN provider, knowledge

1. Introduction

As the Internet continues to grow and become more and more popular in our daily lives, the number of Internet users using Virtual Private Network is increasing dramatically. Since the use of offshore networks may involve infringement of national security as well as national ideology, China has implemented restrictions on access to specific foreign networks. For various purposes, Internet users often need to use some restricted offshore networks, which leads to an increasing number of people using VPNs to access external networks.

However, the issue of the criminality of the provision of the relevant software providers is highly controversial in judicial sessions. Many scholars have put forward different opinions on the crime involved in the relevant issue and also provided their own opinions on the determination of some core issues in determining the crime. Whereas, the theoretical discussion has mainly focused on the analysis of individual crimes, without combining the related crimes and discussing the caveats and priorities of application in the determination. Therefore, this paper will start with the analysis of the crime and study a set of criteria for the determination of the crime that can be universally applied.

2. Research Background

Currently, to protect the security of network information and to comply with national ideological requirements, Chinese authorities have imposed restrictions on access to some foreign networks and set up the Great Fire Wall of China (GFW), which prevents domestic users from directly accessing

DOI: 10.54254/2753-7048/17/20231219

the relevant Internet platforms. However, due to various demands and reasons, users in China often utilize some technical means to break through the relevant restrictions and access foreign networks. This kind of technical means to break through the national restrictions on specific foreign networks is what people call wall climbing. The wall in this context is not the objective wall in our daily lives but is the corresponding IP blocking, content filtering, domain name hijacking, traffic restriction, and other blocking methods [1]. And the way to break through these technical blocking means is a virtual private network(VPN).

Since such restrictions prevent users in China from directly accessing Google, Facebook, and other offshore services, Western public opinion has exploited this as a basis for criticizing the boundaries of the People's Democratic Government. The firewall does not separate China's Internet from the Internet outside China but rather blocks individual websites and specific pages from outside China. The websites blocked by China are mainly platforms involving politically sensitive words, pornographic information, and personal privacy, while the rest of the platforms not involving that related information are not restricted. In other words, the firewall is China's attempt to protect national security and the security of citizens' information, and not to restrict the "Internet freedom" of its citizens. At the same time, the restriction of network firewalls does not restrict nationals' interaction outside of China. Information exchange within and outside of China is generally smooth, and there are no substantial obstacles to normal online contact and communication among people, not to mention the need for online help with logistics.

In contrast, in Western countries where firewalls do not exist, it is difficult to protect the security of personal information of nationals and information involving state secrets. For example, Google Maps is a globally influential application platform that provides users with extremely accurate location information. But Chinese government restricts the use of this platform. The reason for this restriction is that the software's location information is so accurate that it can be used to locate a country's confidential places such as national military sites. Meanwhile, owning to the extreme accuracy of the positioning system, criminals can use the software to steal citizens' privacy, exposing a threat to personal information security. In short, the Western way of letting the network develop freely is not the optimal solution, but rather the Chinese side of the network development of reasonable restrictions, resulting in China's Internet today's booming development. Perhaps without the relevant restrictions, the Chinese own search engine "Baidu" will not have such an overwhelming development and will be replaced by Google, and Yahoo.

3. The Question Raised: How to Identify the Act of Providing VPN Software

From the case below, people can analyze the problems in judicial recognition of the act of providing VPN. Xi was engaged in information technology, with a certain foundation of Internet knowledge. From December 2017 to September 2020, Xi built a VPN platform without authorization using leasing an offshore server and purchased a domain name for the promotion and sale of VPN software to provide access to offshore Internet services for domestic IP addresses. By the time of the verdict of the case, Xi had made a profit of more than RMB 2.5 million from the sale of VPN software. After the case entered the trial stage, there was a huge controversy in the court regarding the characterization of Xi's behavior [2]. Among them, three main views were included:

The first view is that Xi's behavior violated the Interim Provisions of the People's Republic of China on the Management of Computer Information Network International Networking, which is only an administrative violation and does not constitute a crime.

The second view is that Xi, in the absence of a business license, provided value-added telecommunications services such as VPN software to consumers for a fee, which violated the provisions of the Telecommunications Regulations of the People's Republic of China and

DOI: 10.54254/2753-7048/17/20231219

undermined the business order of the telecommunications market, constituting a crime of illegal operation.

The third view is that Xi, by providing a VPN, provided domestic users with the technical means to bypass the national firewall to access the Internet outside the country, constituting the crime of providing programs and tools to intrude into and illegally control computer information systems [2].

In the case of Zhu, who has the same criminal fact as Xi (creating a network platform, using technology to create VPN software and accounts on his own, and selling them to unspecified users), the main controversy of the judicial determination made by the judge is focused on the crime of providing intrusion and illegal control of computer information system programs and tools, the crime of helping the letter and the crime of illegal operation [3].

As seen from the above judicial precedents, there is still a great controversy concerning the legal characterization of the provision of VPN software. What exactly is the issue in dispute? How should such a dispute be resolved? The following article will start with the classification of the act of providing VPN software and conclude with a unified judicial recognition standard to resolve the controversy.

4. Behavior Analysis

4.1. Used in Lawful Conduct

The reason why China restricts access to some extra-territorial websites is out of the perspective of creating a harmonious network environment and maintaining the national ideology. Since the actor's use of VPN does not bring any negative impact on the network environment or national security, the law should come to give the actor some space to freely use the network [2]. Therefore, if the perpetrator simply uses the VPN for legitimate entertainment activities or access to overseas literature, the VPN provider should not be considered a crime.

4.2. Used in Illegal Acts

Conduct 1: The provider knows that the perpetrator is engaged in illegal conduct. The determination of what constitutes "knowledge" is the main issue in distinguishing the subjective aspects of the different acts of the provider, and plays an important role in determining the crime. The content of knowledge and the standard of knowledge are currently controversial in judicial practice and theory:

The first view is that "knowledge" means "definite knowledge, certain knowledge, clear knowledge". This view is that the provider does not have general knowledge of the act of providing and the nature of the actor, but has a clear knowledge [4]. That is, if the provider's knowledge of the foregoing elements is vague and unclear then it does not constitute a crime.

The second view is that "knowledge" includes "clear knowledge and probable knowledge". "Probable knowledge" means that the perpetrator may know that his or her actions will produce harmful results [5]. This viewpoint identifies "may know" as the knowledge that cannot be discharged beyond a reasonable doubt, so "may know" should belong to "knowledge".

The third view is that "knowledge" includes "clear knowledge and should have known". However, there is a consensus that "should have known" does not fall within the scope of "knowledge", so this view has been rejected.

The fourth view is that "knowledge" includes "knowing, recognizing, or foreseeing". The scholars who hold this view believe that foresight is not conjecture, but according to the rule of thumb, the law of development of things to anticipate what will happen in the future [5]. The actor in the implementation of a certain behavior foresaw the content of the harmful results of the behavior, of course, belongs to the awareness of the content of the harmful results.

DOI: 10.54254/2753-7048/17/20231219

The author believes that ‘knowingly’ should not be limited to ‘definite knowledge, certain knowledge, clear knowledge’. Knowledge should also include ‘foreseeing.’ ‘Knowingly may’ is not the same as ‘may know’. ‘may know’ is not enough to constitute knowledge. Only the actor knows that his behavior may constitute a harmful result can be identified as “knowledge”. In other words, the act does not require the provider to know specifically what kind of crime the user uses the VPN to engage in, nor does it require the provider to be sure that the user uses the VPN it provides to commit a crime, but only that the provider knows that the user may use the VPN it provides to engage in illegal activities. But this knowledge must be proved by evidence. Only mere suspicion can not constitute knowledge.

After having a good command of the precise meaning of ‘knowledge’, some detailed categories are as follows.

4.3. Providing Intrusion, Illegal Control of Computer Information Systems, Programs

To determine whether the act of implementation is in line with the ‘provider knowing that others carry out intrusion, illegal control of the computer information system of illegal criminal acts and provide the program, tools’ behavior, people need to first analyze what is so-called the provision of behavior. In the mainstream doctrine, the way of providing mainly includes selling, delivering, informing, and giving. That is to say, the provision includes both paid and unpaid provisions. Therefore, whether it is for profit or not is not an element of judgment for this crime. As long as the provider’s behavior conforms to one of the several acts mentioned above, it can be recognized as providing.

Regarding what is “computer information system” and what is “intrusion and illegal control”. Article 1 of the Interpretation of Several Issues on the Application of Law in Handling Criminal Cases of Crisis in Computer Information System Security issued by the Supreme Court has already explained this.

From the subjective aspect, the provider needs to “know” that the perpetrator is using the VPN software it provides to commit illegal acts.

Finally, it is necessary to analyze whether the act itself infringes on the security operation order of the computer information system.

If the above conditions are met, that is, ‘the provider provides programs and tools to others knowing that they are committing the criminal act of intrusion or illegal control of computer information system’ and meets the requirements of ‘aggravating circumstances’ as stipulated in the law. The provider can be found guilty of providing programs and tools for intrusion and illegal control of computer information systems.

4.4. Providing Specific Help

To determine whether the behavior belongs to the ‘provider knows that others use the information network to commit crimes, still provide Internet access, server hosting, network storage, communication transmission, and other technical support, or provide advertising, payment, and settlement help’, the most important thing is to clarify the nature of the act of assistance. Providing Internet access, server hosting, network storage, communication transmission, and other technical support, or providing advertising and promotion, payment and settlement of the Internet help behaviors is neutral help behavior. Inherently neutral help behavior law is not punishable, if it is directly recognized as a criminal activity, it will expand the scope of neutral assistance behavior punishment. We need to clarify what kind of assistance behavior should be criminalized [6]. Currently, there are three main doctrines in the academic community regarding the criteria for limiting the scope of punishment of neutral assistance behavior: subjective, objective, and compromise doctrines.

DOI: 10.54254/2753-7048/17/20231219

However, those three doctrines are all defective to some extent, and people should adopt a compromise doctrine based on objectivity to determine the scope of punishment for neutral assistance behavior [7]. That is to say, the punishable crime of neutral assistance behavior should be identified through the restrictions of the objective theory, and on this basis, the subjective cognition of the helper should be used as a further qualification [8].

If the act is in the scope of punishment of neutral assistance while meeting the requirements of "the provider knows that others use information networks to commit crimes, but still provide technical support for their crimes such as Internet access, server hosting, network storage, communication transmission, or provide advertising and promotion, payment and settlement assistance," the act can be considered as the crime of assistance. However, in the determination of the crime, it is necessary to meet the requirement of "accomplice accessory". That is, in the determination of the crime, it is necessary to exclude that although the act of helping constitutes the elements of the crime of helping the letter, the act of the person being helped does not have the objective illegality of this type of behavior [9].

5. The Existence of Complicity Between the Provider and the Perpetrator

Above all, people should classify joint crime into different types whether the provider and the perpetrator have a conspiracy or not.

If there is a conspiracy between the provider and the perpetrator at the time of the act or before which is so-called general assistance, the provider can be found guilty as a co-perpetrator of the act.

If the provider and the perpetrator have no prior conspiracy, but the helper knows that the person being helped is engaging in illegal acts and provides help to him, and the person being helped does not know it himself, which is shorted as one-sided helping behavior, the helper shall be found guilty of joint criminality by the relevant provisions of one-sided helping behavior.

Exception: Except from the two classifications, a specific judicial interpretation has clarified conduct that should be convicted as a joint crime, although this behavior also infringes other legal interests. According to Article 4 of the Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases of Telecommunications Network Fraud and Other Criminal Cases, a person who provides technical support such as communication transmission knowing that another person is committing telecommunications network fraud shall be punished as a joint criminal. Therefore, even if the provider's act of providing VPN constitutes the constituent elements of the crime of helping a letter or the crime of providing programs or tools for intrusion into or illegal control of computer information systems, the provider shall be punished as an accomplice to the crime of fraud if the perpetrator's act of implementation constitutes telecommunication fraud.

The provider does not know that the perpetrator uses the VPN software it provides to engage in illegal behavior. Network service providers refuse to fulfill the information network security management obligations.

To determine whether the implementation of the act belongs to the "network service providers do not fulfill the laws and administrative regulations of the information network security management obligations, the supervisory department ordered to take corrective measures and refused to correct" the act, the first need to analyze the network service providers, the scope of the supervisory department at the same time need to clarify what is the refusal to correct the act. To determine the attributes of the behavior, according to the "Supreme People's Court, the Supreme People's Procuratorate on the handling of illegal use of information networks, help information network criminal activities and other criminal cases on the application of the provisions of the first three articles to determine the subject of the act and the content of the act is in line with the requirements of the composition of the elements.

DOI: 10.54254/2753-7048/17/20231219

At the same time, it is not necessary for the network service provider to "know" that the perpetrator is using the VPN software provided by the provider to engage in illegal acts, but only to take corrective measures after being informed by the "supervisory authority", to constitute the crime of inaction. The crime. If the behavior meets the above constituent elements and satisfies the relevant provisions of the crime of refusing to fulfill the obligations of information network security management regarding specific circumstances, the crime can be found.

5.1. Infringement of Copyright

To determine whether the act of the provider constitutes "the act of reproducing and distributing, without the permission of the copyright owner, written, audio and video works, computer software and other works, publishing books to which others have exclusive rights of publication, reproducing and distributing audio and video products produced by the producer without the permission of the producer, producing and exhibiting artworks under the name of others" for profit, first of all, It is necessary to clarify whether the provider's behavior is classified as "the act of reproduction and distribution of its written works, music, movies, television, video works, computer software, and other works without the permission of the owner of the copyright". In other words, the VPN software provided by the provider should be copyrighted by others, and the actor should provide it to others without the permission of the copyright owner. The main act that constitutes this type of crime is the act of publishing as one's own the work of software developed and designed by others, including partial and total copying. Partial copying is not the copying of all programs, but rather the modification or deletion of parts of the program code by covert means. China's Computer Software Protection Regulation defines computer software, computer programs, and documentation, and specifies that computer software referred to in the Regulation refers to computer programs and their related documentation [10]. Partial plagiarism is also known as copying, which is the most common form of software plagiarism today and involves the use of technical disguises in the process of illegal copying [11].

Furthermore, the provider's provision must be for "profit". The purpose of the provider's conduct is different from that of other conduct. Although it is stated above that the act of providing includes providing free of charge, the act of infringing a copyright must exclude the act of providing VPN software without the purpose of "profit". However, the purpose is not required to be realized, that is to say, it is only necessary for the provider to act "for profit", and it is not necessary to determine whether the provider receives benefits.

Finally, the determination of the act does not need to be premised on the provider being engaged in illegal acts. Whether the act constitutes an infringement of copyright only requires judging whether the VPN software provided is problematic, and constitutes an infringement of copyright as long as others own the copyright of the relevant computer software [12].

If the act of infringement meets the requirements of copyright infringement and infringes on the national copyright management system and the copyright and copyright-related rights and interests of others, and meets the requirements of "a large number of serious circumstances", the act of infringement of intellectual property rights can be considered a crime.

5.2. Legislative Recommendations

To circumvent the illegal provision of VPN and to guarantee the fairness of justice and the unity of crime, I believe that relevant judicial interpretations or legislative documents should be issued to fill the above-mentioned gaps in the law.

DOI: 10.54254/2753-7048/17/20231219

5.3. Clarify the Scope of "Knowingly"

At present, the judicial and academic circles do not make uniform provisions on what is "knowingly", which leads to great controversy in determining whether the provider constitutes a criminal act. The author believes that relevant laws should be introduced to clarify the meaning of "knowingly" and follow the principle of criminality. Through the above analysis, the author believes that judicial practice should adopt the fourth viewpoint, that is, the definition of "knowledge" should include "know, recognize, foresee" and does not include should know.

5.4. Clarify the Scope of Punishability of "Neutral Assistance"

At present, China does not adopt the objective-based compromise mentioned above, which leads to the problem of determining the punishability. Therefore, to determine the scope of punishability of "neutral assistance", people should first abandon the objective or subjective criteria and adopt the compromise approach. Secondly, the determination of the punishability of "neutral assistance" should be limited by the principle of "accessory to complicity", that is, only based on the objective culpability of the perpetrator can the "assistance" be deemed The "condensability. In addition, although the crime of aiding and abetting a separate crime is very controversial, to determine the punishability of "helping behavior" must comply with the general principles of the requirements of the accomplice is undoubted. Finally, although the legislation is difficult to specify which neutral acts of assistance are criminal in to which degree, people can refer to the jurisprudence and apply the same level of severity to prevent the situation of different sentences in the same case.

5.5. Summarize the Types of Acts That Provide VPN

The judiciary should issue judicial interpretations to combine judicial precedents and theoretical studies to determine a set of unified and universal applicable standards [12]. The relevant judicial interpretation can not only fill the legislative loopholes and meet the requirements of the principle of crime and punishment but also make up for the problem of legislative lag, which is constantly improved with the ever-rich Internet behavior.

6. A Universal Application Criteria

Combined with the above analysis of several crimes, people can summarize the unified criteria for determining the judicial characterization of the problem of providing VPN software.

Above all, people need to clarify whether the perpetrator is using the VPN software to engage in illegal acts or whether the VPN software utilized by the perpetrator is provided by the provider. If the perpetrator is only using the VPN for academic seminars, or if the perpetrator is not using the VPN provided by the provider for illegal activities, the provider's behavior should not be considered a criminal act.

Secondly, after it is clear that the perpetrator is engaged in illegal acts, people need to analyze whether the provider knew that the perpetrator was engaged in illegal activities at the time of implementing the act of provision. If the provider knows, it is necessary to first determine whether the provider's behavior of providing VPN software constitutes the crime of providing intrusion and illegal control of computer information system programs and tools. If it does not constitute the crime consider whether it constitutes the crime of helping the letter. Only in the above two crimes can not be identified and the existence of prior conspiracy or one-sided help or the provider knows that the perpetrator engaged in telecommunications fraud, the provider can be found to be the perpetrator's helper or accomplice.

DOI: 10.54254/2753-7048/17/20231219

At the same time, if the perpetrator does not know that the perpetrator will use the software to engage in illegal activities when providing VPN software, it is necessary to determine firstly whether the provider knows afterward (i.e. whether it meets the requirement of being informed by the supervisory authority or meets other circumstances). And secondly, whether it continues to provide the software after knowing if the above circumstances are met, then the provider of the network service should be found guilty of refusing to fulfill the information network security management obligations, but if the provider does not belong to the network service provider, it should be found to be a non-crime. It should be noted that if the network service provider in the provision of software has been the perpetrator engaged in illegal activities constitutes knowledge, then directly identified as the crime of helping the letter or providing intrusion, illegal control of computer information system programs, tools, regardless of their identity. The reason why the crime of providing programs and tools for intrusion into or illegal control of computer information systems needs to be given priority over the crime of helping to trust and the crime of refusing to fulfill the obligations of information network security management is that both subsequent crimes have the provision that "if the above-mentioned acts constitute other crimes at the same time, the person shall be convicted and punished by the provisions of the heavier penalty". Such a provision can be interpreted as these two crimes are the bottom clause, when there are other crimes, the other crimes will be given priority.

Furthermore, if the perpetrator does not know that the perpetrator is engaged in illegal acts throughout the process of providing VPN software, or simply suspects it, then the provider should not be found to constitute several of the above crimes.

Finally, after considering the above-mentioned several crimes, people need to analyze separately whether the provider's act of providing VPN constitutes the crime of copyright infringement, at this time, there is no need to consider whether the perpetrator engages in illegal acts, and if it does, it needs to imagine competing with the above-mentioned several crimes and be punished severely.

7. Conclusion

This article introduces a case to raise the issue of how to make a universal approach to the determination of the act of providing VPN software. Then, through the relevant crimes and theoretical analysis, the author provides a set of unified standards. Currently, there is no unified standard for the determination of related issues in judicial practice, and the judicial precedents of related cases are not sufficient. Therefore, the current literature only provides a superficial analysis of the relevant issues and related crimes, and there may be some crimes and some acts omitted. At the same time, this paper only refers to the domestic discussion of the act, but does not study and research the foreign definitions of the relevant issues, so the conclusions drawn cannot fully cover the issue. Future research should start from a general reading of judicial precedents to learn more about the legal penalties involved in the relevant behaviors and to make a more universally applicable standard of recognition.

References

[1] *Cheng, Y. (2023) Criminal law qualitative analysis of the illegal provision of VPN wall climbing service for profit. Master's thesis, Yanbian University,2.*

[2] *Chinese Prosecutor Magazine, (2022), Retrieved from http://www.lib.shnu.edu.cn/b1/0e/c26256a700686/page.htm on May 2nd, 2023*

[3] *Chen, Y.X. (2021) Criminal characterization of illegal sales of VPN "wall" software. Master's thesis, Southwest University of Political Science and Law, 2.*

[4] *Chen, J. X., Yue, M.L. (2023) The expansion of "knowingly" in the crime of helping information network criminal activities and its limitation. Journal of Dalian Maritime University (Social Science Edition),22, 63-67.*

[5] *Ren, J., Zhang, K. (2023) The normative analysis and judicial determination of "knowingly" in criminal law. Journal of Xi'an Petroleum University (Social Science Edition), 32, 02, 86-91.*

[6] *Zhang, M. K. (2023) The "knowledge" in criminal intent. Journal of Shanghai Academy of Political Science and Law (Rule of Law Series), 2, 79.*
[7] *Xiong, Y. W., Huang, Y. (2016) Judicial application of the crime of assisting criminal activities in information network. People's Justice (Application), 31.*
[8] *Mao, B. (2022) The dilemma of knowingly determining the crime of assisting criminal activities in information networks and reflections on it. Evidence Science,30, 06, 730-742.*
[9] *Zhang, M. (2012) On the Crime of Aiding Criminal Activities in Information Network. Journal of the International Criminal Court Politics and Law, 2.*
[10] *He, M., Zhang, J. (2023) Construction of criminal proof objects of software copyright in the context of the digital economy: A case-specific proof of 100 adjudication documents. Electronic Intellectual Property, 375, 02, 87-96.*
[11] *Zhang, Y. Y. (2022) Analysis on the protection of computer software copyright. Journal of Culture, 148, 02, 165-168.*
[12] *Bo, L, Guo, Y. (2022) A qualitative study on the illegal provision of VPN "wall" software, State Prosecutor's College, Office of the Research Steering Group of the Supreme People's Procuratorate on Punishing Cybercrime and Maintaining Cyber Security, Law School of the Renmin University of China. The theory and practice of cybercrime management for better criminal prosecution - Proceedings of the 16th National Senior Prosecutors' Forum, 4. DOI:10.26914/c.cnkihy.2020.047348.*