Decriminalization Path of Net Neutrality Assisting Actions: A Perspective from Aiding and Abetting Cybercrimes

Boya Zhang *

Department of Law, Shandong University, Qingdao, China

* Corresponding Author Email: byzhang8003@mail.sdu.edu.cn

Abstract. Network neutrality assistance actions pertain to the provision of technical or service aid in an online environment to third parties, which may result in harm to others or facilitate unlawful conduct. However, when attempting to regulate such online assistance activities, traditional complicity theories encounter numerous challenges. This is primarily due to the inherent differences between online actions and conventional criminal behaviors, rendering the traditional notions of complicity difficult to apply directly. Analyzing from the perspective of aiding and abetting crimes, the decriminalization path determination of network neutrality assistance actions also confronts issues, such as defining responsibility boundaries and discerning behavioral intent. To address this, this paper adopts the "Restricted Punishment Theory" for the decriminalization path, rationally weighing the benefits and risks of network neutrality assistance actions. Utilizing empirical research, case study analysis, and comparative research methodologies, and based on the overlap analysis of the constitutive elements of aiding and abetting crimes and the refusal to fulfill cyber security management obligations, it's suggested to categorize network service providers. This provides a clearer and more rational basis for their decriminalization.

Keywords: Network Neutrality Assistance Actions, Aiding and Abetting Crimes, Refusal to FulfillCyber Security Management Obligations, Restricted Punishment Theory.

1. Introduction

Assigning responsibility to neutral assistance behaviors, and determining how to attribute it, remains a salient issue in criminal law theory. This concern is intrinsically linked with complicity theory and the essence of criminality, further complicating its assessment. With the evolution of the information society, information network technology increasingly permeates various facets of our daily lives. As cybercrimes become more rampant, the cybersecurity challenges become even more prominent. With the growing intricacies of industrialization and specialization, the propelling role of neutral assistance behaviors under the purview of cybercrime has gained significant traction. Malicious actors frequently exploit technological and platform conveniences to abet a myriad of unspecified cybercrimes, reaping benefits in the process. This has thrust the challenge of determining neutral online behaviors into the spotlight.

Given the current academic consensus and status of judicial practice, even after the promulgation of the "Ninth Amendment to the Criminal Law," which introduced the crime of aiding cybercrime activities (hereinafter referred to as "Aiding and Abetting Crimes"), the regulation of online assistance behaviors remains problematic. In a landscape where there's no unified definition for neutral online assistance behaviors and where clear standards for its punishability are absent, debates linger over whether such behaviors should fall under punitive measures. If they should, under what circumstances should regulations apply? Judicial practice typically identifies these behaviors either as complicity or narrows it down to traditional aiding crimes, leading to an unjust expansion of the punishment scope. This demotivates the involved parties and hampers economic development and societal progress in a data-driven era.

During the research on this topic, this paper primarily employed case study analysis, empirical research, and comparative research methodologies. Innovatively, this paper began with the QVOD case to identify the inherent independence of neutral online assistance behaviors. Depending on the type of online service provider, and by considering the overlapping constitutive elements between

Aiding and Abetting Crimes and the crime of not fulfilling cybersecurity obligations, this paper discerned the path of decriminalization for neutral online assistance behaviors.

2. Determination of Net Neutrality Assistance Behavior

To comprehend the notion of neutral assistance behavior from a cybercrime perspective, it's crucial to first clarify the definition of neutral assistance behavior. Neutral assistance is often discussed in terms of its role within joint crimes, emphasizing how neutrality impacts the adjudication and sentencing process. According to the verdict in the QVOD case, neutral assistance behavior refers to actions that, on the surface, align with daily or business practices and do not pursue illicit objectives but objectively facilitate or abet criminal activities by others [1]. Put differently, such actions generally lack inherent criminality and punishability. They do not seek illicit goals but, in effect, aid in the realization of a criminal outcome.

German scholars define "neutral assistance behavior" as "external neutral actions", "daily activities", "profession-typical behaviors", and "routine business practices" [2]. Japanese scholars term it as "daily activities" [2]. Academics in Taiwan often characterize it as "neutral actions in daily life" [3]. In Mainland China, various scholars have provided their interpretations, such as "seemingly harmless 'neutral' actions", synonymous with "daily life behaviors" [4].

Regarding neutral assistance behavior in the realm of cybercrime, in the digital era, providing technological support, like internet access, has become a commonplace technical service. This service is inherently neutral and is a quintessential example of neutral assistance behavior [5]. For instance, activities like supplying network connections, facilitating information transfer, sharing resources, and enabling platform transactions for others involved in cybercrimes can be construed as such [6]. Thus, it can be summarized as the practical application of the neutral assistance theory within the domain of cybercrime.

3. Decriminalization Analysis of Net Neutrality Assistance Behavior under the Perspective of Assisting in Cybercrimes

3.1. The Inapplicability of Traditional Accomplice Theory in the Context of the Digital Age

Traditional complicity in crimes requires that all involved parties have a shared criminal intent on a subjective level (satisfying both the cognitive and volitional requirements) and that they collectively carry out the intended criminal act objectively. However, in the context of the digital age, the criminal intent connection among co-offenders is diminishing. Situations arise where assistants might vaguely or not at all be aware of another's criminal intent, lack any clear intent connection with others, and, while not displaying criminal intent themselves, still objectively aid the principal offender.

When digital technology services are offered to an unspecified majority, they should, in principle, be recognized as inherently harmless and a normal business activity. However, if these services are exploited by criminals to carry out cybercrimes, and the service providers, despite lacking intent communication with these criminals, adopt a laissez-faire attitude for their own interests, how should such neutral assistance be addressed? Judicial practice has not provided a clear answer.

Objectively, the neutral online assistance aids the primary offender's criminal act, establishing an objective causal relationship with the harmful results of the cybercrime committed by the primary offender. Given the virtuality, widespread dissemination, and other characteristics of the internet, the societal harm of such assistance might even surpass the societal harm of the primary offense, necessitating regulation.

The tension and balance between the freedom of action and the protection of legal interests is a perpetual challenge in criminal law. This clash and equilibrium have prompted the emergence of the neutral assistance theory [7]. Objectively, while neutral online assistance indeed facilitates the occurrence of a criminal outcome, impacting legal interests, the individuals behind such actions always have the freedom rooted in everyday needs or business operations. However, this freedom

should be exercised within reasonable boundaries. A comprehensive crackdown on such actions, based purely on the criminal outcome, places an undue burden on the actors, potentially creating an excessively strained adversarial relationship between internet service providers and users [8]. Judicial practices that treat neutral online assistance actors as accomplices, or even as traditional aiders, result in an unwarranted expansion of the scope of punishment, dampening the enthusiasm of online service providers, which is not conducive to economic growth and societal progress in the era of big data.

Based on the above analysis, it is imperative to clarify the punishable scope of neutral online assistance behaviors, establishing a clear boundary between penalization and non-penalization.

3.2. The Dilemma in Analyzing the Decriminalization of Neutral Online Assistance Under the Perspective of Abetting Information Crimes

Given the significant societal risks associated with online assistance behaviors, some scholars have proposed elevating assistance behaviors to the level of principal offenses for adjudication. This proposal has been acknowledged in legislation. The "Criminal Law Amendment (IX)" stipulates the "Assisting Communication Crime" from an act perspective and has issued related judicial interpretations. This reflects that, at the criminal legislative level, the punishable status of neutral assistance behavior is formally recognized [9]. It also indirectly demonstrates the central authority's affirmation of the criminal punishability of neutral assistance behavior in specific situations online, thereby partially addressing the legal foundation for punishing online service providers' assistance behaviors.

However, the establishment of this crime has been contentious in academic circles.

Some scholars argue that the addition of the Assisting Communication Crime is not only fully justified and necessary but also has a solid legal rationale [10]. Those facilitating actions in cyberspace might be assessed and sanctioned as accomplices in joint crimes, or as individual perpetrators. They might also face sanctions due to their role as online service providers, based on the "platform responsibility" and potential negligence in fulfilling cybersecurity management obligations [11].

Conversely, others believe that the behaviors constituting the Assisting Communication Crime typify neutral assistance behaviors [12]. They see it as the criminalization of neutral assistance behavior and neutral business assistance behavior [13,14]. The addition of this crime expands criminal law interventions in neutral behaviors, thereby limiting the ways to exempt neutral online assistance behaviors from criminality [15,16].

The question arises: can we simply equate the Assisting Communication Crime with the criminalization of neutral assistance behavior [16]? Or, does the active expansion of the criminal punishability of neutral online assistance behaviors by our criminal legislation and judiciary mean we are moving towards a path of comprehensive punishability [16]? When online service providers, without any criminal intent, offer technically neutral services that, while being exploited by criminals, also cater to the broader public engaged in lawful online activities, should they be sanctioned under the Assisting Communication Crime? Applying penalties to neutral online assistance behaviors might reduce cybercrimes to some extent. However, it might also hinder the general public's lawful use of online services, increase the operational costs of internet technologies, dampen the enthusiasm of online service providers, and stymie the growth of internet technology. Given these concerns, exploring paths to decriminalize neutral online assistance behaviors within the scope of the Assisting Communication Crime becomes particularly crucial.

4. A Detailed Analysis of the Decriminalization Pathway for Neutral Online Assistance in Practice under the Perspective of Abetting Information Crimes

4.1. Analysis Based on Interest Balancing under the Theory of Limited Punishment

Research into the punishability of neutral assistance behavior in Germany and Japan primarily diverges into two theoretical schools: the Comprehensive Punishment Approach and the Restricted Punishment Approach. The Comprehensive Punishment Approach, due to its oversight of the "neutral" nature of the neutral assistance behavior, is deemed as unduly constraining citizens' freedoms. Thus, it garners minimal support in both countries. In Germany and Japan, apart from a few scholars advocating for the Comprehensive Punishment Approach, the overwhelming majority lean towards the Restricted Punishment Approach [17]. Most scholars in our country also favor the Restricted Punishment Approach, arguing that mechanically treating various everyday actions as abstract aiding offenses could result in an unacceptably broad overextension of the punitive scope [13].

From a jurisprudential perspective, the punishability of online neutral assistance behavior is not purely a doctrinal matter. It should be approached from a standpoint of balancing societal interests, taking into account the anticipated societal outcomes. Guided by the principle of restraint in criminal law, a balance between ensuring freedom and protecting legal rights should be achieved. The principle of prioritizing administrative and civil liabilities should be followed, resorting to criminal penalties only in cases of grave severity. The crux lies in determining whether the online assistance behavior has at a particular juncture, lost its "neutrality". This loss of neutrality is primarily manifested subjectively in the knowledge of the action's nature and objectively in providing indispensable assistance at a crucial moment.

4.2. Feasibility Analysis of Decriminalization Pathways Based on the Overlapping Elements of "Aiding and Abetting Crimes" and "Failure to Fulfill Information Network Security Management Obligations"

Some scholars posit that when network service providers, despite being ordered by regulatory authorities to make corrections, remain non-compliant, they can be determined to have "knowingly" provided technical support for others to commit crimes using the information network, thus constituting the offense of aiding in cybercrime. Additionally, they can also be judged as failing to fulfill their statutory management obligations, hence establishing the crime of refusing to perform information network security management duties. As a result, there's an overlap in the constituent elements of these two offenses. This paper endorses this view and based on this, proceeds to analyze the decriminalization pathways of neutral online assistance behaviors:

According to Article 287(2) of the Criminal Law of the People's Republic of China (Amended 2020), the crime of aiding in cyber offenses is established when one knowingly assists others in using the information network to commit crimes by providing internet access, server hosting, network storage, communication transmission, or offering services like advertising promotion, payment clearing, etc., with severe circumstances. A major judicial challenge lies in the ambiguous standards for determining "subjective knowledge" and the severity of the situation, which hinders decriminalization of neutral online assistance behaviors. In response to this judicial predicament, it's suggested that based on the overlapping elements of the two aforementioned crimes, decriminalization pathways should be determined by the type of network service provider. The detailed analysis is as follows:

Providers should be categorized based on their roles. Different network service providers should fulfill regulatory obligations in accordance with the specificity of their services. The scope of these obligations should be determined not only by laws, regulations, and industry standards but also by referencing the relative demands the online industry places on its professionals, tailored to specific cases [18].

Drawing from German and EU legal provisions, network service providers can be broadly categorized into four main types: internet access providers, online content providers, online information exchange platform providers, and online content reception providers [18]. The influence of online content reception providers in cybercriminal activities is relatively minimal. As for online content providers, it's generally believed that providing information online holds no distinct criminal implications compared to expressing opinions in physical spaces. Analyzed under the tri-level theory of criminal law, online content providers' liability for illicit content they supply, provided it meets the criteria of crime constitution, illegality, and culpability, is uncontested. In essence, determining criminal responsibility for such behavior in the online environment isn't particularly challenging. Therefore, this discussion primarily focuses on the recognition issues concerning the punishability of neutral assistance behaviors in the context of the remaining two types of entities.

4.2.1 Internet Connectivity Service Provider

Regarding online connectivity service providers, these primarily include entities that provide internet access, server hosting, network storage, and communication transmission services to facilitate the dissemination of online information.

In general, this paper believes it is inappropriate to hastily deem such entities guilty of aiding and abetting cybercrimes for the following reasons:

Firstly, the internet houses a vast amount of information. Connectivity service providers typically adopt a neutral stance, merely facilitating information transfer. As merely platforms or carriers, they do not have the right to inspect user permissions or access user data, and they cannot decide the content users transfer. It is unreasonable to expect them to proactively review or constantly monitor illicit content or websites, as they are not in a position of guarantorship, and lack substantive review obligations and capabilities regarding user-generated content [18].

Secondly, given the rapid evolution of the internet and its expansive reach combined with high transmission speeds, it's challenging for most service providers to sift through the massive amount of user data to identify potentially criminal online information. Imposing strict review obligations without differentiation could be overly burdensome on service providers.

However, a completely laissez-faire approach to these entities isn't advisable either, and exceptions necessitating punitive actions exist. As per Article 286(1) of the "Criminal Law of the People's Republic of China (Amended in 2020)" concerning the "refusal to fulfill cyber-security management obligations," providers that refuse to correct their actions even after being directed by regulatory departments, under the following circumstances, can be sentenced to less than three years of imprisonment, detention, or be placed under custody and fined:

(1) Causing widespread dissemination of illegal information;

(2) Leading to user information leaks with severe consequences;

(3) Resulting in the loss of evidence in criminal cases with serious circumstances;

(4) Having other serious implications.

For corporate offenses, the entity will be fined, and penalties will be imposed on responsible supervisors or other directly accountable individuals. If the behaviors mentioned also constitute other crimes, the more severe penalty should apply.

Additionally, Article 11 of the "Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Illegal Use of Information Networks and Assisting in Cybercrimes" offers criteria to determine knowledge in aiding and abetting crimes. Behaviors indicating a person knows someone else uses the internet to commit crimes, barring contrary evidence, include:

(1) Continuing relevant actions after notification from regulatory departments;

(2) Failing to fulfill statutory management responsibilities after a complaint;

(3) Having notably unusual transaction prices or methods;

(4) Providing specific tools or technical support for illegal or criminal actions;

(5) Frequently adopting covert online practices, encrypted communications, data destruction, or using fake identities to evade supervision or investigations;

(6) Providing technical support or aid to others to evade supervision or investigation;

(7) Other situations proving the person's knowledge.

Thus, it's clear from legislative intent that connectivity service providers are obligated to take effective measures, such as disconnecting or removing information, only after receiving valid notices from rights holders or correctional instructions from statutory regulators [19]. If they fail to act despite knowledge that their users might be spreading illegal or criminal information or using the internet for criminal purposes, they should be considered culpable, possibly under aiding and abetting cybercrimes or the refusal to fulfill cyber-security management obligations.

While some scholar's express concerns over potential overreach by regulatory authorities, ambiguous penalty standards, and the legal basis behind them, cautioning that excessive directives might hinder normal operations, these service providers, while enjoying their statutory rights, should also bear legal responsibilities for not fulfilling certain duties. Proper refinement of relevant cyber governance laws and regulations, coupled with clear rectification directives from authorized regulatory bodies, can balance non-interference in the business rights of service providers while promoting a healthy online service industry.

4.2.2 Online Information Exchange Platform Service Provider

This type of online service provider primarily refers to entities that offer users a platform space, enabling them to search, browse, upload, and share information. In the realm of cybercrime, these online platform providers play a pivotal role. Typical platforms include search engines, chat applications, and other user-friendly platforms accessible via mobile devices.

For these providers, given their intermediary nature in the digital ecosystem, they generally shouldn't be unduly criticized. As a rule of thumb in cyberspace, "the risk should be allocated to those who upload or provide the information, not the platform providers [5]". When unlawful content on the platform leads to specific legal violations, the uploader should bear the responsibility. However, under special circumstances, in accordance with the provisions on online infringement responsibility in the "Civil Code" and the "Criminal Law of the People's Republic of China (2020 Amendment)" regarding the refusal to fulfill information network security management obligations and abetment, if the platform providers fail to remove unlawful information after receiving valid notifications from the rightful parties or legal regulatory bodies, they may be held accountable for tort liabilities and even criminal responsibilities [20].

If an online platform provider also delivers specific software services, they may also bear responsibilities due to the software's inherent nature. A classic case is the 2016 first-instance judgment of the "QVOD case", where the court opined that the case neither applied the "technological neutrality" principle nor was considered "neutral assistance". QVOD, as an online video service provider, should have adhered to network security obligations. Yet, with profit motivations, they turned a blind eye to the propagation of obscene videos, clearly neglecting their security responsibilities. Their actions were interpreted as having implicit intention and evident maliciousness. QVOD's behavior lacked the "neutrality" of technological support, as they stored and propagated obscene videos using caching servers. The act was done with illicit profit intent, and thus wasn't considered neutral assistance in joint crime theories [1]. Due to the technical feature in QVOD's video player software, where video content could be shared among its users, the company was found guilty of distributing obscene materials for profit [8]. Some scholars argue that had the QVOD case occurred after the issuance of the "Ninth Amendment to the Criminal Law", QVOD could have been convicted based on the refusal to fulfill information network security management obligations [21,22].

Beyond delivering software of specific nature, attention should also be given when platform providers publish content on their platforms. In such scenarios, they should undoubtedly be responsible for the content they post. If a platform provider sides with a user and loses its neutrality, it may bear the liability of a joint offender or principal offender [23].

5. Conclusion

In the current era of digitalization, the role and status of online service providers in cybercrimes have been steadily increasing. An escalating number of neutral online assistance behaviors, which promote principal offenders' criminal actions but also exhibit daily, life-related, and professional characteristics, are emerging into public view, consistently challenging traditional criminal law theories. Academic debates persist over the punitive range criteria for neutral online assistance actions, and current judicial practices lack effective identification measures. The path to determining the scope of punishment for such behaviors remains fraught and long-winding.

This article delves into the definition of neutral online assistance behavior as an independent act and, under the perspective of the overlapping elements of aiding in crimes and failing to fulfill cyber-security management obligations, explores the identification of culpable pathways for different online service entities providing neutral assistance. The intention is to offer some guidance in handling such actions in practical cases. However, the relevant theories concerning neutral online assistance are intricate, extensive, and beyond the full scope of this paper. Here, we've only touched upon these topics at a surface level. Furthermore, foundational theories like those on complicity; comparative legal studies on the punishability of neutral assistance actions; distinctions between neutral and general assistance behaviors; clarifications of related concepts; the legitimacy of neutral assistance actions; and the criminalization of aiding actions all require further exploration. There are undoubtedly shortcomings in the preliminary insights provided on neutral online assistance behaviors in this paper, and I humbly welcome constructive criticism and corrections.

References

[1] Criminal judgment of the case of Shenzhen QVOD Technology Co., Ltd., Wang Xin, and others for profiting from the dissemination of obscene materials. Haidian District People's Court of Beijing, 2015 Hai Xing Chu Zi No. 512.

[2] Chen Hongbing. On Neutral Assisting Acts. Chinese and Foreign Jurisprudence, 2008, 20(06): 931-957.

[3] Lin Shantian, Xu Zetian. General Theory of Criminal Law. Yuanzhao Publishing Company, Taiwan, 2006.

[4] Zhang Mingkai. Criminal Law (Third Edition). Law Press, 2007.

[5] Zhang Mingkai. On the Crime of Assisting Cybercrime Activities. Politics and Law, 2016(02): 2-16.

[6] Ma Jun. An Exploration of Neutral Assisting Acts in Cyberspace: With a Discussion on the Understanding of Article 287, Paragraph 2, Clause 1 of the Criminal Law. Times Law Studies, 2018, 16(04):35-42.

[7] Ma Rongchun. On the Harmony of Criminal Law. Hebei Law Review, 2006(12):72-74.

[8] Che Hao. Who Should Pay for Neutral Acts in the Internet Era? China Law Review, 2015(01):47-50.

[9] Ma Rongchun. Neutral Assisting Acts and Their Excessiveness. Eastern Jurisprudence, 2017(02):2-16.

[10] Liu Xianquan. On the Criminal Responsibility for the Abuse of Information Network Technology: Understanding and Application of Relevant Provisions in the Criminal Law Amendment (IX). Political and Law Forum, 2015, 33(06):96-109.

[11] Yu Zhigang. Sanction System and Improvement Ideas for Criminal Assisting Acts in Cyberspace. Chinese Procurators, 2016(13):80.

[12] Liu Yanhong. Critique on the Formal Criminalization of Cybercrime Assisting Acts. Legal and Business Studies, 2016, 33(03):18-22.

[13] Che Hao. Jurisprudential Reflections on Criminal Legislation - Based on the Analysis of Criminal Law Amendment (IX). Jurisprudence, 2015(10):3-16.

[14] Liu Xianquan. Criminal Risks and Liability Boundaries of Internet Financial Platforms. Global Law Review, 2016, 38(05):78-91.

[15] He Ronggong. Prevention of the Expansion of Criminal Law and Its Limits. Legal Studies, 2017, 39(04):138-154.

[16] Liu Yanhong. Evolution and Critique of the Punishability of Neutral Assisting Acts in Cyberspace: Comparative Insights from German and Japanese Theories and Practices. Jurisprudence Review, 2016, 34(05):40-49.

[17] [Japanese] Yamanaka Keiichi. Punishability by Neutral Acts. Kansai University Law Review Vol. 56, No. 1 (2006).

[18] Li Yongsheng, Zhang Chu. Criminal Law Regulation of Neutral Assisting Acts in Cyberspace. Criminal Law Review, 2018, 53(01):276-315.

[19] [German] Erik Hilgendorf: "German Criminal Law: From Tradition to Modern", translated by Jiang Zhu, Huang Xiaoyan, et al., Peking University Press, 2015.

[20] Lv Kai, Li Ting. Copyright Protection Responsibility of Internet Service Providers. Tianjin Jurisprudence, 2016, 32(01):5-12.

[21] Sun Daocui. Sanction Boundaries of Partial Joint Cyber Crimes: A Discussion on the "QVOD" Case. Journal of Zhejiang Gongshang University, 2016(04):52-60.

[22] Wang Suzhi. From Reactive to Proactive: The Normative Shift in Cybercrime Criminal Law Legislation: A Review of the Legislative Provisions of Criminal Law Amendment (IX). Hebei Law Review, 2016, 34(08):155-164.

[23] Chen Hongbing. On the Punishment Boundaries of Neutral Assisting Acts. China Law Science, 2017(01):189-208.