Advances in Social Science and Culture
ISSN 2640-9682 (Print) ISSN 2640-9674 (Online)
Vol. 8, No. 2, 2026
www.scholink.org/ojs/index.php/assc

*Original Paper*

# Principalization in Criminal Imputation of Online Facilitating Acts

Zheng Mao[1]

[1] Law School of Beijing Normal University, Beijing, China

Received: February 26, 2026 Accepted: April 10, 2026 Online Published: April 20, 2026

doi:10.22158/assc.v8n2p170 URL: http://dx.doi.org/10.22158/assc.v8n2p170

***Abstract***

*Online facilitating acts refer to conduct in which internet service providers, in the course of their routine operations, provide technical support for crimes committed by others. Such acts are characterized by both technicality and neutrality, and the actors generally lack the volitional element of actively pursuing the completion of a crime. Within the structure of cybercrimes, facilitating acts exhibit a trend of alienation—manifested in heightened independence and expanded harmfulness. The "one-to-many" model of facilitation may render its social harm greater than that of the principal offense, while the virtual nature of cyberspace weakens the communication of intent between facilitators and principals, making subjective culpability difficult to establish. Consequently, the traditional accomplice liability framework—centered on the principles of subordination and common intent—proves inadequate. Therefore, treating online facilitating acts as principal offenses (principalization) has become a necessary approach to address practical needs. In its specific application, the subjective element should adopt "actual knowledge" and "constructive knowledge" as the standards for determining knowing. Objectively, the scope of criminalization should be limited by substantive criteria such as whether the conduct complies with industry norms and the timing of knowledge, considered in light of legitimate business practices and the unlawful nature of the assisted conduct. At the same time, the principalized offense should serve as a "residual" ground for liability, giving priority to applying accomplice liability or other offenses with heavier penalties to prevent excessive expansion of the criminal sphere.*

***Keywords***

*online facilitating acts, principalization, imputation, judicial application*

## 1. Introduction

The study of principalization as the method of imputation for online facilitating acts originates from

changes in criminal legislation and the demands of judicial practice. In the internet era, network technology has been widely applied across various fields of economic and social life, becoming the primary means of data and information exchange as well as an important platform for socioeconomic activity. Alongside the rapid development of information networks, crimes committed by offenders using such networks have become increasingly severe. Offenses that rely on or are facilitated by networks have continued to grow, emerging as a new feature of criminal activity. While network technology facilitates daily life, it also facilitates the commission of crimes. When traditional crime models are combined with network technical assistance, they give rise to technology-assisted cybercrimes with heightened social harm, of which telecom network fraud, online gambling, online dissemination of obscene materials, and live-streaming pornography are common manifestations.

As a tool for committing crimes, network technical services have restructured the relationship between independent criminal conduct and participation in criminal conduct. In traditional crimes, the existence and punishment of facilitating acts are subordinate to the principal act, with the principal offense occupying a central position in the overall crime. Facilitating acts and principal acts are carried out under the guidance of common intent, sharing commonality in both subjective and objective dimensions. In crimes involving online facilitating acts, however, the centrality of the principal offense diminishes within the overall criminal structure. Facilitating acts may also dominate or control the crime, acquiring equivalent value in terms of infringement upon legally protected interests—or even, to some extent, surpassing the harmfulness of the principal act. The common intent between the two parties tends to dissolve in the dual virtuality of identity and space. The objective commonality of conduct weakens, as facilitating acts gain relative independence, with reduced temporal and spatial connection to the principal act, yet they rival the principal act in advancing the completion of the crime. In essence, after traditional facilitating acts evolve into online facilitating acts, the pattern of technology-assisted participation in crimes shifts from a holistic perspective: cyber joint crimes exhibit pronounced decentralization and independence of conduct, subordination in both subjective and objective dimensions declines while harmfulness increases, and the criminal chain extends significantly. Simultaneously, a “one-to-many” model of online facilitation gradually takes shape, resulting in the cumulative and diffused harmfulness of multiple principal acts supported by the same online facilitation, collectively transforming into new forms of cybercrime with greater social harm. These developments also create difficulties in characterizing and imputing online facilitating acts.

In response to these issues, China’s criminal legislation, judicial interpretations, and criminal judicial practice have all provided responses. In 2015, the Criminal Law Amendment (IX) added the crime of assisting information network criminal activities and the crime of illegally using information networks to Article 287 of the Criminal Law, aiming to precisely combat facilitating acts in cybercrime, protect citizens’ personal and property rights as well as public social interests, and ensure the healthy development of information networks. The Supreme People’s Court and the Supreme People’s Procuratorate have also issued relevant judicial interpretations, resolving certain issues regarding

conviction and sentencing for online facilitating acts. However, existing judicial interpretations still have shortcomings in addressing issues such as the characterization of the assisted party's conduct, the determination of quantitative thresholds and circumstances, and the identification of accomplice liability. Several difficulties remain in fully combating online facilitating acts. For example, how should the evidentiary standards for "knowing" be determined when establishing the mental state of online facilitators? If the assisted party's conduct does not fully satisfy all elements of the relevant offense in terms of "quantitative thresholds" or "circumstances," does the online facilitator nonetheless warrant independent conviction and punishment? When practitioners in the internet service industry provide technical tools on a one-time basis to criminal organizations—such as telecom fraud groups in the preparatory stage or online pornography platforms—and subsequently have only a vague understanding of the specific implementation of the ensuing crimes, does their conduct lose its neutral business nature? These issues require refined research and verification.

At the level of judicial practice, how to balance the inherent tensions between current legal norms and theoretical frameworks, and thereby provide directional guidance for the judicial application of principalization in online facilitating acts, carries significant theoretical and practical value. This article will conduct a theoretical interpretation and criminal law applicability analysis of the principalization of online facilitating acts, aiming to provide a reference for the accurate application of relevant offenses in judicial practice and to offer theoretical support for legislators and judicial interpretation drafters in examining the rationality of relevant norms.

## 2. Overview of Online Facilitating Acts in Chinese Criminal Law

### *2.1 Definition of Online Facilitating Acts*

Although Chinese criminal law currently does not provide a clear definition of online facilitating acts, such acts do not constitute an independent new legal term. The theory of facilitating acts has long existed in traditional criminal law theory, and online facilitating acts are related to the concept of facilitating acts committed by accessories. Providing online technical support for crimes committed by others broadly refers to conduct that does not directly perpetrate the crime but merely provides conditions or prepares tools for it. For example, in the *Kuaibo* case, the company provided video uploading and playback channels for disseminators of obscene content. In this sense, online facilitating acts may be understood by reference to the facilitating acts of an accessory. At present, under Chinese criminal law, perpetrators of online facilitating acts are deemed to form a joint crime with the assisted party only in limited circumstances, such as where the act constitutes the crime of assisting information network criminal activities under Article 287 of the Criminal Law.

### *2.2 Subjects of Online Facilitating Acts*

The subjects of online facilitating acts are providers of online technical services. Technologies such as internet access, data storage, and information promotion hold instrumental significance for cyber offenders. Online technical services constitute the foundational conduct for practitioners in

internet-related industries. The providers of such services include both entities—such as telecommunications companies and internet technology firms—and the natural persons employed therein. Internet access service providers or online platform service providers primarily refer to those who offer technical support including internet access, server hosting, and communication transmission. (Zhou, 2015)

In my view, individuals' use of internet technology begins with network access and subsequently relies primarily on mobile devices or other network terminals connected to the internet, meeting their living and working needs through various online platforms and different types of software clients. Therefore, telecommunications service providers that facilitate network access, as well as those involved in the development, operation, and servicing of online platforms and various software applications, all fall within the category of internet service providers.

In Chinese criminal legislation, both the crime of assisting information network criminal activities and the crime of failing to fulfill obligations regarding information network security management impose specific supervisory duties on internet service providers concerning the proper use of their technical services. These duties require that, when providers become aware that their services are being used to commit crimes, they must cease providing technical assistance and delete relevant illegal or criminal information.

*2.3 Characteristics of Online Facilitating Acts*

2.3.1 Technicality

Technicality is an inherent characteristic of online facilitating acts. The widespread application of information technology has accelerated the dissemination of information and expanded the scope of criminal harm. On the one hand, traditional crimes such as fraud and defamation have been transformed into new types of cybercrimes through technological means. On the other hand, technologies such as network communications, social platforms, and data encryption result in a lack of clear communication of intent between facilitators and principals—they may not even know each other—making imputation difficult. For example, in the 2020 South Korean *Nth Room* case, the perpetrators used Telegram to create secret chat rooms where they shared illegally filmed sexual videos and photos. "As many as 74 women were sexually victimized, including 16 minors, and up to 260,000 users joined the rooms to share child sexual exploitation material." (Tong, 2020) In this case, the technical characteristics of Telegram made it difficult to obtain criminal evidence, and the scale of harm far exceeded that of traditional crimes. The technicality of online facilitating acts renders their harmful effects more severe than those of the principal acts themselves, making them a primary driver of the expansion of crime, while simultaneously creating challenges in evidence collection and difficulties in establishing culpability.

2.3.2 Neutrality

Neutrality may also be understood as "everydayness." German law refers to neutral facilitating acts as everyday acts. This is reflected in two dimensions: first, the neutrality of the online technical services

themselves, and second, the neutrality of the service providers' conduct. Currently, network technology has become an infrastructure of social life, and its everyday nature allows criminals to exploit it freely. Internet companies typically provide technical services as business activities directed at an unspecified public. Such conduct itself lacks both intentionality (i.e., a specific intent to assist) and harmfulness in the sense of criminal law, and therefore does not constitute harmful conduct. Only when the service objectively promotes or aggravates criminal conduct does it acquire harmfulness, yet the subjective intentionality remains absent. For instance, if multiple individuals use mobile phone numbers or social media applications provided by a telecommunications company to commit fraud, the service provider does not bear criminal liability for its ordinary business conduct. Perpetrators of online facilitating acts generally lack actual knowledge that others are using their services to commit crimes, and maintain a neutral stance toward the criminal outcome, merely perceiving themselves as performing routine work. The everyday nature of the conduct makes it difficult to determine subjective culpability, and consequently, to establish culpability—the conduct itself does not directly infringe upon legally protected interests, and even if the actor has a vague awareness of possible social harm, it is difficult to criminalize such conduct.

## 3. The Necessity of Adopting Principalization as the Method of Imputation for Online Facilitating Acts Under the Criminal Law

### *3.1 The Alienation of Facilitating Acts in Cyberspace*

#### 3.1.1 Increased Independence

In traditional accomplice theory, facilitating acts are subordinate to the principal offense, and both require common intent. In cyberspace, however, facilitating acts—relying on technology—exhibit independence, primarily reflected in two aspects: first, the subjective communication of intent between the facilitator and the principal is weakened; second, facilitators often provide technical support to multiple or even unspecified principals, or serve only unlawful conduct. The unique structure of cybercrime grants facilitating acts a degree of relative independence. Facilitators and principals often lack direct contact and may be located in different countries, unlike the close cooperation seen in traditional accomplice relationships. Therefore, some scholars argue that the relationship between them is one of collaboration rather than joint crime. (Wang, 2020)

Data from criminal judicial practice show that, as of 2021, the China Judgments Online website had collected 1,124 judgments for the crime of assisting information network criminal activities, in which 69.3% of defendants had no communication of intent with the principal offender. (Zhou, Z., & Zhao, C. , 2022)

The virtual nature of the internet results in little genuine exchange of criminal intent between the parties. Taking social media platforms as an example: when users post fraudulent information on WeChat or Weibo, platform technicians, faced with massive amounts of information, have neither the obligation nor the authority to review each piece individually. Subjectively, it is difficult for them to

have actual knowledge of others' crimes, let alone share common intent. Even in the case of technicians specifically hired by a fraud ring, the ring's use of covert command structures and segmented operations often prevents them from having a clear understanding of the number, identity, or specific acts of the principals. For instance, if Zhang San provides communication technology to a ring and later leaves, and months afterward others use that technology to commit fraud, Zhang San's conduct is disconnected from the principal act in both time and space. Such conduct may only constitute assistance at the preparatory stage, rather than accomplice liability or the crime of assisting information network criminal activities.

In terms of objective conduct, online technical assistance possesses instrumental and stable characteristics. Regardless of when, where, or how many legally protected interests the principal harms, the facilitating act itself—such as server maintenance or communication transmission—remains constant, independently serving each specific principal.

In sum, the interaction between technical assistance and principals in cybercrime significantly enhances the independence of facilitating acts. Such acts are less influenced by the will of the assisted party and are not limited to specific crimes.

3.1.2 Increased Harmfulness

In cybercrime, the harmfulness of facilitating acts may surpass that of the principal act, and may even play a primary role in the completion of the crime. Even where the principal fails to achieve the criminal purpose, facilitating acts may independently create a real danger of infringement upon legally protected interests. The root cause lies in the fact that online facilitation, by virtue of virtuality, borderlessness, and technological convenience, expands the spatiotemporal conditions of crime, amplifies the impact of harm, reduces criminal risk, and enhances the survivability of criminal activity.

Specifically, online technical assistance breaks through the traditional "one-to-one" model of facilitation, achieving a "one-to-many" empowerment through cyberspace, thereby multiplying harm. Take online fraud as an example: Zhang San provides network communication, virtual IP addresses, and other technical services to multiple unspecified fraud perpetrators. Each perpetrator may commit a single fraud amounting to only RMB 1,000 to 2,000, none of which individually meets the threshold for fraud. However, numerous fraudulent acts rely on the same technical support, cumulatively causing serious infringement upon legally protected interests. In this context, Zhang San's technical assistance becomes an indispensable component of each principal act, and its social harmfulness essentially exceeds that of each individual principal act. Criminal punishment should be imposed based on the substantive infringement of legally protected interests.

Moreover, technical assistance enhances the concealment of criminal activity, lowers the threshold and risk of committing crimes, and objectively stimulates the occurrence of cybercrime.

Taking online pornography crimes as an example, some scholars have argued that where internet service providers, knowing that others are committing crimes, provide deep links or technical support for the dissemination of obscene videos, they appear formally to occupy a secondary or auxiliary

position in the dissemination of obscene materials, but in reality play a dominant role. (Liang, 2017)

Network technology creates a borderless virtual space with high dissemination efficiency. In the context of live-streaming pornography crimes, perpetrators use live streaming, linking, and aggregation technologies as criminal tools, cloaking themselves in a virtual guise to evade supervision, significantly enhancing the survivability of the platform. Specifically, platforms increase concealment through complex linking technologies: "Deep linking is specifically manifested in framed links and embedded links, dividing the display interface of a website on PC and mobile terminals into several independent sections, presenting the content of linked websites within specific frames on the platform's own page." (Wu, Y., & Wan, X., 2016) At the same time, platforms often host servers overseas, frequently change domain names, and even use aggregation technologies to integrate content from multiple overseas pornographic live streams for users to view. Take the 2018 Chinese *Peach Blossom Island Treasure Box* app as an example: from October 2017 onward, this platform aggregated content from over one hundred pornographic live-streaming platforms, with daily viewership exceeding one million and total funds involved reaching RMB 350 million. (Beihu District People's Court of Chenzhou City, Hunan Province, Criminal Judgment, 2020) Through technological means such as nested links, the platform not only evaded regulatory tracking but also addressed the short lifecycle that had plagued traditional pornography websites.

It is evident that, with the assistance of live-streaming, linking, and aggregation technologies, pornography crimes have seen a significant expansion in the scope of victims, the amount of funds involved, and the resulting harm, compared with traditional obscenity-related crimes. The overall harmfulness has increased substantially.

*3.2 Difficulties in Applying Traditional Chinese Criminal Law Theories of Imputation*

3.2.1 Difficulty in Responding to Cybercrime as a Whole

Traditional accomplice theory struggles to impute online facilitating acts in a holistic manner. Due to characteristics such as multi-point dispersion and decentralization, cybercrime has gradually become chain-based and collaborative, exhibiting a trend toward refined horizontal division of labor and vertical segmentation. The number of participating links and levels has increased, giving rise to a large number of facilitating acts that form part of the online "black and gray" industrial chain. This development toward chain-based and organized structures has fragmented the overall criminality of facilitating acts and principal acts.

Take online fraud as an example: new types of fraud organizations feature specialized and professional division of labor. They purchase citizens' personal information through online gray-industry chains and select fraud targets accordingly. After the fraud is completed, they engage in transactions with hackers for technical services, and may even outsource "withdrawal operations" to individuals or companies with money-laundering channels. Among these, preparatory facilitating acts—such as stealing or purchasing QQ accounts or WeChat accounts—are difficult to establish as punishable due to their technical neutrality. At the same time, "customized precision fraud" relies upstream on the illegal

trading of citizens' personal information, while downstream conceals criminal proceeds through money laundering. Different links may also connect with other crimes, increasing the likelihood that facilitating acts and principal acts span the elements of different offenses.

Similarly, in live-streaming pornography crimes, platform operation, technical maintenance, customer service, domain name changes, and financial management are each handled by dedicated personnel, forming a highly refined division of labor. Although such facilitators may potentially be identified as accessories to the relevant principal offenses, convicting them under offenses such as the crime of assisting information network criminal activities or the crime of illegally using information networks may be more conducive to protecting legally protected interests and combating crime. In summary, the new behavioral patterns of cybercrime have broken through the integrity and singularity of crime that characterized traditional accomplice relationships, making holistic imputation unsuitable for participation in facilitating acts across various links.

3.2.2 Difficulty in Responding to Independent Online Facilitating Acts

Traditional Chinese accomplice theory, centered on the theory of limited subordination, struggles to accommodate online facilitating acts with increased independence. In terms of both subjective and objective elements, this theory requires that facilitating acts and principal acts achieve unity of subjective and objective elements within the same crime. However, in cybercrime, such a determination is difficult to accomplish.

In continental criminal law theory, it is generally understood that the limited subordination theory posits a relationship of shared interests between accomplice and principal, with their illegality being interconnected and consistent. (Li, 2007) According to the limited subordination theory, the establishment of accomplice liability is predicated on the principal act satisfying the elements of the offense and unlawfulness. Where the principal act is unlawful, the instigation or facilitation, as forms of secondary liability, are naturally unlawful as well. (Qian, 2022) Conversely, under the limited subordination theory, facilitating acts in the context of "accomplice without a principal" cannot satisfy the elements of the offense or unlawfulness; this theory does not support the independent culpability of accomplice conduct separate from the principal.

China generally adopts the theory of "extreme subordination" (Qian, 2012), under which accomplice liability exists only when the principal constitutes a crime. (Sun, 2020) As a result, it is difficult to impose separate punishment for unilateral technical facilitating acts, potentially leading to impunity for such conduct.

Subjectively, facilitators and principals lack clear communication of intent, making it difficult to establish accomplice liability. Objectively, if the culpability of facilitating acts is held to be subordinate to the unlawfulness of the principal act, then where the facts concerning the principal act are unclear, the identity of the principal is unknown, or the principal act does not meet the threshold for criminality, the culpability of the facilitating act cannot be established. For example, in online pornography or gambling crimes, the servers or principals are often located overseas, making it difficult to ascertain all

the facts based solely on virtual IDs, and thus technical facilitators are difficult to impute. Even if the facts are clarified, if the principal act does not meet the quantitative threshold for criminality—such as when multiple individuals each commit fraud amounting to RMB 1,000 using Zhang San's technology, none individually meeting the threshold for fraud, but the cumulative harm is serious—under traditional theory, Zhang San would still be exempt from liability because the principals committed no crime. This clearly contradicts the substantive need for legal interest protection: the facilitating act plays a key role, and its harmfulness may even exceed that of the principal act, yet it cannot be imputed due to inconsistency with the degree of unlawfulness of the principal act, hindering effective protection of legally protected interests.

## 4. Application of the Principalization Method of Imputation for Online Facilitating Acts

### *4.1 Determination of Subjective Elements of Online Facilitating Acts*

#### 4.1.1 Determination of Criminal Intent

Under existing criminal law provisions, the objects of regulation under the principalization of online facilitating acts mainly include: network access, online promotion, data storage, payment settlement, and failure to fulfill management obligations after receiving notice. The above acts may be committed with either intent or negligence, but the primary targets of imputation are those who act with a subjective intent. Based on common types of cyber joint crimes, the most frequently occurring offenses are profit-oriented crimes such as fraud, gambling, and obscene electronic information, often involving large sums of money. The subjective culpability in such cases is predominantly direct intent—that is, the actor possesses "knowledge coupled with desire" regarding the harmful consequences. In contrast, technical facilitating participation, due to the neutrality of technology and the difficulty in establishing accomplice intent, often only reaches the level of indirect "willful blindness" intent.

For example, "in obscene electronic information crimes, technical facilitators providing support often claim that they merely neglected management and argue that they did not know the information or websites were obscene in order to avoid punishment." (Zhang & Xiong, 2010) In crimes such as online fraud, the key issue lies in how to determine the content of the technical facilitator's "knowledge" regarding the nature of the conduct and its consequences. The virtual nature of cyberspace and the indeterminacy of communication targets result in the communication between facilitator and principal being one-sided and unidirectional. Traditional accomplice theory requires communication of intent to be bidirectional and effective. However, in technology-participatory crimes, the identities, communication terminals, and even spatiotemporal conditions of the parties may be virtual or misaligned. For instance, when communication occurs through non-real-time methods such as email, the expression of intent becomes more ambiguous, making it difficult to confirm whether the other party has accurately understood it, thereby weakening the characteristics of mutual criminal intent. Additionally, network technology itself is neutral; most technologies are not specifically developed for criminal purposes. Moreover, the duration of technical facilitating conduct may not align with that of

the principal act—an actor may not initially know that the software they were hired to develop would be used for criminal purposes and may withdraw after becoming aware, or may know in advance but lack comprehensive understanding of the specific subsequent criminal circumstances and the "quantum" of harm after delivering the tools.

Therefore, technical facilitators' "knowledge" of the nature of the conduct and its consequences often remains at the level of "possible use for illegal purposes," lacking clear awareness of the specific criminal circumstances, and at most adopting an attitude of willful indifference toward the harmful results. This determines that in judicial practice, technical facilitating acts are predominantly characterized by "willful blindness" intent.

4.1.2 Determination of Subjective "Knowing"

"Knowing" (*mingzhi*) is a neutral term in ordinary Chinese context, but its use in criminal law often serves the function of affirming that certain conduct satisfies the subjective elements of an offense, thereby contributing to a finding of guilt. Therefore, it must carry a value judgment with negative connotations. Under Chinese criminal law concerning intentional offenses, "knowing" constitutes the cognitive element of criminal intent and serves as a general element of intent, while "knowing" in the specific provisions functions as a particular element of intent. (Zhang, 2011) In terms of typology in criminal legislation, "knowing" appears in various verb-object structures: first, the "knowing + illegal item" type, such as in the crime of selling toxic or harmful food; second, the "knowing + illegal conduct" type, such as in Article 311 of the Criminal Law, which provides "knowing that another person is committing espionage…"; third, the "knowing + specific subject" type, such as in the crime of harboring or shielding, which provides "providing shelter to a person known to be a criminal." (Wang, 2013) "Knowing" exists only in intentional crimes, and typological analysis helps clarify the meaning of "knowing" in offenses related to cybercrime. Among the offenses associated with the principalization of online facilitating acts, both the crime of illegally intruding into computer information systems and the crime of assisting information network criminal activities explicitly require "knowing" as an element for conviction.

First, in both offenses, the type of knowing falls under the "knowing + illegal conduct" category. In criminal legislation, this type of knowing requires that the objective element possess criminal unlawfulness, thereby clarifying that the content of knowing in these two offenses is that "the conduct of another person constitutes a crime prohibited by the Criminal Law." Second, due to the particularities of determining accomplice intent in cybercrime, judicial application must delineate the degree of "knowing." It is generally understood that knowing in intentional crimes includes "actual knowledge" and presumptive "should have known." Some scholars have proposed that the scope of knowing can be divided into three categories, from narrow to broad: the first category limits knowing to "definite knowledge"; the second category includes both knowledge and presumptive should have known; the third category includes both actual knowledge and constructive knowledge. (Sun, 2019) "Should have known" refers to a presumption that facts not actually known to the actor are nonetheless

deemed known, the rationale being that the actor failed to exercise reasonable care. However, in cybercrime, such presumptions may impose excessively heavy obligations on internet service providers, leading to over-evaluation of neutral business conduct. Technology itself is neutral. When service providers engage in activities such as network access and storage for the public, their conduct constitutes normal business operations as long as customers comply with industry norms. If they clearly know in advance that another party is committing a crime and still provide assistance, knowing may be established. If they did not know in advance but become aware during the course of service—whether through a "directive" from an administrative authority or a report from a third party—and continue to provide technical support, the subsequent conduct should also be deemed knowing. Similarly, for the conduct of providing tools for intruding into computer information systems under Article 285(3) of the Criminal Law, the subjective knowing generally should not be presumed through the "should have known" standard.

The value of applying the "constructive knowledge" standard lies in addressing the characteristics of online facilitating acts. Because the communication of intent between facilitators and principals is often one-sided, unidirectional, and ambiguous—particularly when separated in time and space—technical providers lack comprehensive awareness of the nature and consequences of the conduct. If "actual knowledge" is adopted as the sole standard, the scope of principalization imputation would be unduly restricted, making it difficult to effectively regulate "one-to-many" online facilitating acts and preventing the full realization of the legislative value of relevant provisions.

*4.2 The Limits of Principalization Imputation for Online Facilitating Acts*

4.2.1 Restricting Punishment for Neutral Online Facilitating Acts

Neutral facilitating acts are generally not punishable due to their everyday and business nature; otherwise, the normal order of society would be disrupted. This is reflected in traditional criminal contexts—for example, when a supermarket sells a kitchen knife that is later used in a homicide, the seller is not punished because no criminal intent exists. In cybercrime, internet service providers, faced with users' virtual identities and vast amounts of information, find it even more difficult to know whether their technology is being used for criminal purposes, and criminal law should not impose excessively heavy obligations of review. Moreover, network technology itself is neutral, requiring even greater caution in imposing punishment to avoid hindering technological development. From the provisions of Articles 286 and 287 of the Criminal Law, it can be seen that the objects of principalized punishment are primarily everyday technical services such as network access, storage, promotion, and payment. Whether punishment is warranted should be determined by substantively examining whether the conduct remains neutral throughout its performance and continuation: if the conduct constitutes normal business at the time it is performed and does not subsequently lose its neutrality, it should not fall within the scope of principalized punishment.

Not all cases in judicial practice where "providing technical support" is found to constitute the crime of assisting information network criminal activities involve the criminalization of neutral facilitating acts.

Examples include:

(1) Developing, producing, providing, selling, renting, or maintaining software, platforms, or websites specially designed for committing crimes such as gambling or fraud; (Ninghe County People's Court, Tianjin, Criminal Judgment, 2019)

(2) Providing services to modify the location settings of WeChat or QQ accounts; (Guangling District People's Court of Yangzhou City, Jiangsu Province, Criminal Judgment, 2020)

(3) Assisting others in registering domain names, creating illegal websites, and providing website maintenance; (Miluo City People's Court, Hunan Province, Criminal Judgment, 2018)

(4) Renting overseas servers and providing related technical support for obscene or pornographic forums; (Lijin County People's Court, Shandong Province, Criminal Judgment, 2019)

(5) Searching for and renting servers exempt from filing requirements for illegal websites.

Whether a neutral facilitating act may be criminalized should be judged based on whether it possesses the characteristics of everydayness and legitimate business nature. If an actor, knowing that another person is committing a crime, nonetheless provides technical assistance through means that do not comply with industry norms, the act loses its neutrality and should fall within the scope of punishment. For example, in the case of Tang, the defendant registered to lease a server using false information and fraudulently used Li's identity to make payments for the server he leased. Tang knew that an individual identified only as "Manager Li," whose true identity was unknown to him, intended to purchase the server for use in fraud, yet he nonetheless rented out the server, providing server hosting and routine maintenance assistance. After the fraudulent website he had set up experienced technical issues, Tang provided maintenance services upon request. The court held that Tang, knowing that another person was committing a crime, provided technical support such as server hosting, and his conduct constituted the crime of assisting information network criminal activities. (Taihe District People's Court of Jinzhou City, Liaoning Province, Criminal Judgment, 2019) This judgment is correct. Tang's conduct was punishable because he violated the industry norm requiring real-name registration, registering to lease the server using false information and subleasing it to another individual who likewise had not completed real-name registration, thereby losing the legitimate business nature of his conduct.

In another example, Leng operated an online store leasing fixed telephone numbers. Despite knowing that certain lessees were engaging in fraudulent and other illegal activities, Leng nonetheless provided communication services such as call forwarding. A fraud ring used the numbers leased by Leng to defraud Lou of RMB 3.59 million. The court found Leng guilty of the crime of assisting information network criminal activities. (Shangyu District People's Court of Shaoxing City, Zhejiang Province, Criminal Judgment, 2016) This judgment is questionable. Leng's conduct of leasing fixed telephone numbers through an online store constituted everyday conduct that complied with industry norms for e-commerce operations; he should not have been convicted as a principal offender of the crime of assisting information network criminal activities. Although Leng possessed subjective knowledge, his conduct remained a routine business activity of providing call forwarding communication services,

rather than harmful conduct in the sense of criminal law. If telecommunications companies such as China Mobile or China Unicom were to have their mobile phone numbers used by criminals to commit fraud, these companies would not bear criminal liability as a result. When only a small number of users exploit technical services to commit crimes, criminal law should not impose substantive review obligations on internet service providers; otherwise, normal business operations would be impossible. Conversely, where actors specifically provide technical services to criminal organizations, or actively provide tools or deeply participate after learning of another's criminal conduct, their conduct has departed from the realm of legitimate business and should fall within the scope of principalized punishment.

In summary, in determining whether an online facilitating act is punishable, substantive examination should be conducted as to whether it complies with industry norms: lawful and compliant business conduct, even if used for criminal purposes, remains a neutral facilitating act. If the conduct itself violates norms, or if the actor, after knowing of another's criminal conduct, actively provides technical tools or deeply participates in the crime, the conduct has departed from the realm of legitimate business and should fall within the scope of principalized punishment. In cases of "knowledge acquired during the course of conduct," the focus of examination should be on whether the subsequent technical services remain neutral.

4.2.2 Principalized Offenses for Online Facilitating Acts Should Be Used as a Residual Ground for Liability

The offenses related to the principalization of online facilitating acts possess a residual applicability, which aligns with their legislative logic. This logic can be articulated as follows: where such acts overlap with other offenses, the offense carrying the heavier penalty shall apply; where they can constitute accomplice liability for other crimes, they shall be punished as accomplice liability; only where neither of the foregoing circumstances applies shall they be independently imputed under principalized offenses. This arrangement is supported by the following rationales:

First, it achieves proportionality between crime and punishment while maintaining the stability of criminal law. Although online facilitating acts have been established as independent offenses, their nature remains that of facilitating acts. Where they play a critical and controlling role in the crime, punishment as accomplice liability should be permitted to achieve heavier penalties. Take online fraud as an example: if a technical facilitator is punished under the crime of assisting information network criminal activities, the maximum sentence does not exceed three years. If, however, the facilitator can be found to constitute accomplice liability for fraud, a higher statutory sentence may apply, better aligning with the principle of proportionality between crime and punishment.

Second, it maintains the modesty of criminal law and prevents principalized offenses from becoming "catch-all" offenses. If all technical facilitating acts were uniformly criminalized as independent offenses, the scope of criminalization would be improperly expanded. Where technical facilitating acts are minor in nature, limited in harm, or constitute an accomplice relationship with the assisted conduct,

accomplice theory should be prioritized, and the act should be punished as accessory liability. This approach both accords with the substantive judgment of legal interest infringement and avoids excessive penal evaluation.

Third, it ensures coordination with accomplice theory. If the principal act itself entails minimal social harm, the technical facilitating act should not be independently punished. For example, in a "one-to-one" technical assistance scenario, if the amount of fraud is only RMB 5,000, whether punished under the crime of assisting information network criminal activities or as an accomplice to fraud, the sentence would fall within the range of less than three years. In such cases, priority should be given to applying the general provisions on accomplice liability in the Criminal Law, punishing the actor as an accessory with a lighter or mitigated penalty.

**References**

Li, H. (2007). *Reflections on general theories of criminal law*. Beijing: China Renmin University Press.

Liang, G. (2017). The networking of traditional crimes: Imputation obstacles, criminal law responses, and doctrinal limitations. *Law Science*, (2), 4.

Qian, Y. (2012). The advocacy of the theory of accessory's dependence on the principal's act. *Law Science*, (11), 119.

Qian, Y. (2022). Re-proposing the theory of restricted dependence: Focusing on the critique of the theory of minimum dependence. *ECUPL Journal*, (5), 146.

Sun, D. (2020). *A preliminary study on cyber criminal law*. Beijing: China University of Political Science and Law Press, p. 290.

Sun, Y. (2019). The core issue on the crime of helping information cybercrime. *Tribune of Political Science and Law*, *37*(2), 88.

Tong, L. (2020). The warning of the "Nth Room" incident in South Korea for the issue of "social network child sexual exploitation" in China. *Issues on Juvenile Crimes and Delinquency*, (3), 3.

Wang, S. (2020). On the principal quality of cybercrime participation: Rethinking based on the offence of assisting cybercrime. *Journal of Comparative Law*, (1), 171.

Wang, X. (2013). The meaning and determination of "knowledge" in Chinese criminal law: Analysis based on criminal legislation and judicial interpretations. *Law and Social Development*, (1), 68.

Wu, Y., & Wan, X. (2016). Deep linking by aggregation platforms: Using "link services" to disguise "content provision". *Electronics Intellectual Property*, (8), 48.

Zhang, J., & Xiong, X. (2010). *Interpretation of criminal legal documents* (No. 56 in total). Beijing: People's Court Press, p. 47.

Zhang, M. (2011). *Principles of interpretation of the specific provisions of criminal law: Volume 1*. Beijing: China Renmin University Press, pp. 158, 390.

Zhou, G. (2015). The scope of criminal liability of Internet service providers. *China Law Review*, (2), 177.

Zhou, Z., & Zhao, C. (2022). An empirical study on the crime of aiding information network criminal activities: Based on 1,081 judgments. *Journal of Law Application*, (6), 84.

**Note(s)**

Note 1. Beihu District People's Court of Chenzhou City, Hunan Province, Criminal Judgment, (2020) 湘 1002 刑初 10 号, (2018) 湘 1002 刑初 217 号.

Note 2. Ninghe County People's Court, Tianjin, Criminal Judgment, (2019) 津 0117 刑初 84 号.

Note 3. Guangling District People's Court of Yangzhou City, Jiangsu Province, Criminal Judgment, (2020) 苏 1002 刑初 204 号.

Note 4. Miluo City People's Court, Hunan Province, Criminal Judgment, (2018) 湘 0681 刑初 358 号.

Note 5. Lijin County People's Court, Shandong Province, Criminal Judgment, (2019) 鲁 0522 刑初 108 号.

Note 6. Taihe District People's Court of Jinzhou City, Liaoning Province, Criminal Judgment, (2019) 辽 0791 刑初 45 号.

Note 7. Shangyu District People's Court of Shaoxing City, Zhejiang Province, Criminal Judgment, (2016)浙 0604 刑初 1032 号.