

A Study on Criminal Liability of Network Platforms in the Crime of Aiding Information-Network Criminal Activities

Sihua Wang

Faculty of Law, Macau University of Science and Technology, Macao, China

Abstract: The Amendment (IX) to the Criminal Law established the Crime of Aiding Information-Network Criminal Activities to address industrialized cyber-crimes that traditional complicity theory struggles to regulate. Network platforms, core digital-society carriers, are frequently misused by cyber grey-and-black industries. Current judicial practice faces problems including the crime's pocket-crime expansion, generalized presumption of platforms' "knowledge", and flawed unit-liability mechanisms, leading to inconsistent rulings. This paper reviews mainstream theories of the crime and analyzes practical dilemmas in platform criminal-liability imputation. It distinguishes this offence from the Crime of Refusing to Perform Obligations for Information-Network Security Management. To balance cyber-crime crackdown and healthy digital-industry growth, it suggests refining the judicial test for "knowledge", clarifying offence boundaries, setting rules for neutral assisting conduct, improving unit-crime rules, and optimizing administrative-criminal linkage.

Keywords: Crime of Aiding Information-Network Criminal Activities; Network Platform; Knowledge; Neutral Assisting Conduct; Unit Criminal Liability

1. Introduction

With the iterative upgrading of digital technologies reshaping the patterns of traditional crimes, telecom and online fraud, online gambling, illegal information dissemination and other crimes keep evolving via network platforms. Criminal division of labor has become increasingly refined, forming cross-regional grey-and-black industrial chains with unspecified victims. The traditional joint-crime theory takes mutual intentional communication as the core constituent element

of joint crimes and requires that principal offenders can be identified and brought to justice. Nevertheless, under the decentralized nature of cyber-crimes, a large number of upstream criminals hide overseas. Participants in each link often have no direct communication or contact, so many network platforms merely providing technical support can hardly be held criminally liable under traditional complicity rules.[1] Against this realistic background, Article 287-2 of China's Criminal Law, namely the Crime of Aiding Information-Network Criminal Activities, was added by the Amendment (IX) to the Criminal Law. It imposes independent criminal punishment on severe assisting conducts: knowing that others commit crimes by means of information networks and providing them with technical support including internet access, server hosting, network storage, communication transmission, advertisement promotion, payment and settlement, thus realizing the pre-positioning of criminal regulation.

Network platforms cover various subjects such as cloud-service providers, social-interaction platforms, payment-and-settlement service providers, API interface technical service providers, and short-video traffic platforms. Platforms of different types differ objectively in technical control capabilities, business models and levels of security-management obligations, which determines that a unified standard cannot be adopted to evaluate criminal liability for all network platforms. A review of existing judicial documents reveals that most cases of this crime involve grassroots participants such as natural persons who sell or lend "two types of cards". There are relatively few judicial precedents that impose criminal convictions on internet platform enterprises. Judicial practice presents a polarized attitude toward criminal liability of platform entities. On the one hand, some judicial decisions excessively expand the scope of criminal evaluation. General management oversights arising from platform operations are

directly elevated to criminal offences. The neutral nature of platform businesses is ignored, and internet enterprises are burdened with control obligations beyond their technical capacity, generating unnecessary suppression over normal operations of the digital industry. On the other hand, some network platforms are fully aware that their services are exploited for illegal and criminal activities yet allow grey-and-black industries to continuously commit harmful acts by using platform services. Such platforms only bear limited administrative penalties, and the deterrent function of criminal law cannot be fully exerted.

Meanwhile, the Crime of Refusing to Perform Obligations for Information-Network Security Management is a specific charge regulating omissive dereliction by network-service providers. It sets a statutory precondition: “refusing to take corrective measures after being ordered to do so by regulatory authorities”. Restricted by this requirement, this charge yields very few judgments in practice and has nearly become a “zombie clause” under symbolic legislation. In practice, many platform omission cases that should be evaluated under the Crime of Refusing to Perform Obligations for Information-Network Security Management are directly convicted under the Crime of Aiding Information-Network Criminal Activities, so as to bypass the administrative precondition of regulatory correction orders. This gives rise to misalignment of legislative functions of the two charges and disrupts the logical system of crimes as designed by legislators.[2] Faced with such practical contradictions, how to accurately demarcate the boundary of network platforms’ criminal liability, distinguish normal commercial conducts, administrative violations and criminal offences of platforms, and fully activate the institutional value of the existing criminal-law system has become a vital topic for both criminal-law theory and judicial practice. Based on current criminal-law provisions, judicial interpretations and existing academic achievements, this paper conducts a systematic analysis on the application of the Crime of Aiding Information-Network Criminal Activities to network platforms and attempts to provide theoretical references for judicial handling of similar cases.

2. Normative Attributes of the Crime of Aiding Information-Network Criminal

Activities and the Basis for Imputing Liability to Network Platforms

Since its enactment, no complete consensus has been reached in criminal-law academia regarding the normative attributes of the Crime of Aiding Information-Network Criminal Activities. Different theoretical stances directly affect the logic for imputing criminal liability to network platforms and determine the boundary of punishment scope for this crime. Only by clarifying its normative positioning can we further interpret the jurisprudential foundation on which network platforms bear criminal liability for this crime.

Some scholars represented by Professor Zhang Mingkai adhere to the sentencing-rule theory. Upholding the traditional principle of complicity subordination, this theory holds that the Crime of Aiding Information-Network Criminal Activities does not create brand-new perpetrating acts.[3] It merely establishes an independent sentencing rule for accessories in cyber-crimes, and the charge still belongs to the complicity system of upstream crimes. According to this theory, assisting acts under this crime are essentially accessories. However, specific provisions of the Criminal Law prescribe separate statutory penalties for such online assisting conducts, so general provisions on punishment for accessories in the Criminal Law shall no longer be invoked directly. It means that the establishment of this crime must abide by complicity subordination: upstream assisted conducts must constitute criminal unlawful acts that satisfy constitutive requirements. Assisting conducts cannot be punished independently decoupled from the unlawfulness of upstream principal offenders. When applied to network-platform cases, if the sentencing-rule theory is adopted, to convict a network platform of this crime, it must be confirmed that upstream unlawful criminal acts satisfy both material and quantitative elements. Platforms cannot be held criminally liable merely because platform services are exploited by others to cause harmful consequences. This theory helps constrain the punishment scope of this crime via complicity subordination and prevents it from becoming a pocket crime. Yet it encounters practical obstacles in cyber-crime governance: when upstream offenders hide overseas and cannot be verified, technical support provided by network platforms can hardly be subject to criminal accountability,

which fails to adapt to the “one-to-many” pattern of cyber-crimes.

In contrast, the accessory-to-perpetrator transformation theory represents the mainstream academic stance. It argues that legislators have elevated online assisting conducts originally categorized as accessories into independent perpetrating acts with separate charges and statutory penalties, thus breaking free from the traditional complicity system. Even if all upstream principal offenders cannot be identified, actors can be held independently criminally liable as long as all constitutive elements of this crime are satisfied. In network-platform scenarios, this theory justifies separate convictions against platform entities without waiting for all upstream offenders to be brought to justice, matching practical demands for combating grey-and-black cyber-industrial chains.[4] Nevertheless, this theory carries risks: unlimited recognition of accessory-to-perpetrator transformation may bring a large number of neutral technical services merely exploited by crimes within the scope of criminal punishment, creating hidden dangers of objective imputation.

Professor Jing Lijia puts forward the substantive preparatory-offense theory, offering a new perspective for understanding this crime. This theory regards the Crime of Aiding Information-Network Criminal Activities as a substantive preparatory offence. Assisting acts are preparatory acts committed by others to create conditions for numerous potential cyber-crimes. Their unlawfulness originates from abstract legal-interest risks created by assisting conducts themselves, rather than depending on any specific upstream principal offender. Accordingly, the crime is divided into organized substantive preparatory offences and non-organized substantive preparatory offences. For network platforms, platforms organizing or participating in the provision of systematic technical services for grey-and-black industries constitute organized substantive preparatory offences; assisting conducts without organized features and clear clues fall under non-organized substantive preparatory offences.[5] Focusing on evaluating legal-interest risks created by assisting conducts, the substantive preparatory-offense theory better fits the reality where network platforms provide large-scale technical services, with a single assisting act supporting countless potential crimes. Still,

over-expansion of abstract risks must be guarded against. Criminal conviction cannot be reached merely based on superficial risks; subjective knowledge and behavioural attributes shall be comprehensively assessed.

Beyond the above representative theories, scholars such as Liu Ziliang, proceeding from the norm-violation theory and the obligation-offender theory, deny the complicity-subordination feature of this crime. They advocate breaking the inherent framework of complicity theory. The unlawfulness of this crime lies not in infringing upstream legal interests, but in actors’ breach of normative communication obligations in cyberspace and special obligations established by pre-positive laws such as the Anti-Telecom and Online Fraud Law that prohibit providing support and assistance for cyber-crimes, thus justifying the independent nature of this crime. [6] The obligation-offender perspective well explains the imputation logic for omissive conducts of platforms. However, the boundary between administrative obligations under pre-positive laws and criminal-law obligations must be clarified: mere violation of administrative regulatory obligations shall not be equated with criminal unlawfulness.

Each theory has its merits, and no single theory can perfectly interpret all judicial scenarios. When handling network-platform criminal-liability issues, rigid adherence to one single theory shall be avoided. Where network platforms proactively modify their functions to specially develop and provide technical tools adapted for illegal and criminal activities and actively empower cyber-crimes, the accessory-to-perpetrator transformation theory is more applicable. For ordinary platforms providing general and basic online services, constraints from complicity subordination shall be moderately absorbed to prevent unlimited expansion of criminal punishment scope.

After clarifying normative attributes, two paths exist for imputing liability to network platforms for this crime: commission and omission. Commission means platforms actively engage in positive objective conducts, such as developing crime-specific programs and customizing illegal interfaces. Knowing others commit cyber-crimes, platforms voluntarily provide various technical support including internet access, server hosting, advertisement promotion and payment-and-settlement services. Such

conducts directly contribute to upstream crimes and satisfy objective constitutive elements of this crime. Omission-based establishment of this crime is premised on network platforms' guarantor obligations: platforms clearly know users are committing crimes via platforms, possess technical capacities to block or delete illegal activities yet refuse to take disposal measures and continuously allow platform services to be exploited for crimes. It shall be emphasized that omission-based application of this crime cannot be expanded without limits. Distinction must be drawn from the Crime of Refusing to Perform Obligations for Information-Network Security Management, and not all platform management oversights shall be evaluated under the Crime of Aiding Information-Network Criminal Activities.

Guarantor obligations of network platforms stem from multiple sources. Pre-positive administrative laws including the Cybersecurity Law, Anti-Telecom and Online Fraud Law and Data Security Law impose network-security-management obligations on network platforms, constituting a major source of such obligations. Platforms' own business models also give rise to corresponding risk-control obligations. Where platforms' prior conducts intervene in fields of legal-interest infringement, guarantor obligations under criminal law will also arise. [7] Nevertheless, it must be clarified that security-management obligations under administrative law cannot be directly equated with guarantor obligations under criminal law. Platforms' failure to fully meet administrative-regulation requirements shall not directly presume their criminal liability. Guarantor obligations under criminal law require substantive filtering judgment. Obligation intensity shall match platforms' technical capacities, business scales and service types. The law cannot demand small-and-medium-sized platforms to identify and filter one hundred percent of potential illegal information within platforms.

3. Practical Dilemmas and Jurisprudential Contradictions in Applying the Crime of Aiding Information-Network Criminal Activities to Network Platforms

A review of existing judicial documents reveals massive caseloads for the Crime of Aiding Information-Network Criminal Activities, yet most cases concern natural persons selling or

renting bank cards and phone cards. There are relatively few precedents holding internet platform enterprises criminally liable. Judicial practice shows contradictory phenomena. On the one hand, some judicial authorities tend to convict platforms of this crime merely for management loopholes or failure to remove illegal content, generating risks of objective imputation. On the other hand, large-scale internet platforms face high thresholds for criminal accountability due to complex business architectures and difficulties in evidence collection. Most problems are only addressed via administrative fines and rectification orders, and the deterrent effect of criminal law is insufficient. Meanwhile, the Crime of Refusing to Perform Obligations for Information-Network Security Management is rarely applied. A large number of platform omission cases that should be judged under this charge bypass its statutory administrative precondition of regulatory correction orders and are handled under the Crime of Aiding Information-Network Criminal Activities. This results in misalignment of legislative functions of the two charges, and the crime-system originally designed by legislators fails to be fully implemented. [8]

Regarding subjective constitutive elements, "knowing that others commit crimes by means of information networks" constitutes an indispensable subjective element for this crime, and it is also the most challenging difficulty in hearing network-platform cases. The judicial interpretation jointly issued by the Supreme People's Court and the Supreme People's Procuratorate in 2019 enumerates seven circumstances for presuming actors' knowledge, including continuing relevant conducts after being notified by regulatory authorities, refusing to perform management duties upon receiving reports, obviously abnormal transaction prices or patterns, specially providing programs or tools for illegal and criminal activities, frequently adopting encrypted and concealed means to evade supervision, etc. A catch-all clause "other circumstances sufficient to establish actors' knowledge" is also included. Such presumption rules work well in natural-person "two-card" cases, yet expose many practical problems when applied to network-platform cases.

First, the concept of knowledge tends to be generalized in judicial practice, blurring boundaries among actual knowledge,

constructive knowledge and mere possibility of foreseeing risks. Some investigating authorities equate objective risks of platform businesses being abused by offenders or platforms' foreseeability of potential criminal exploitation with criminal-law "knowledge", elevating platforms' management negligence to criminal intent. General-purpose network platforms inevitably risk being exploited by wrongdoers in business operations. Mere foresight of abstract risks of business abuse does not equal the criminal-law requirement of "knowing others are committing information-network crimes". Second, the boundary of generalized knowledge remains controversial. Academia generally agrees that knowledge under this crime refers to generalized knowledge: actors do not need to precisely identify whether upstream crimes are telecom fraud or online gambling, nor do they need to know specific names of upstream crimes. However, generalized knowledge cannot be unbounded. Mere awareness of general administrative violations on platforms cannot be directly equated with knowledge of criminal offences under criminal law; administrative violations and criminal crimes must be strictly distinguished. Third, presumption-of-knowledge rules lack complete counter-evidence mechanisms. The judicial interpretation stipulates objective circumstances for presuming knowledge but does not systematically define defense paths for platforms to rebut such presumption. Where network platforms establish supporting compliance systems for risk control, review, early-warning and disposal matching their business risks and effectively implement them in operations, whether knowledge presumption can be rebutted lacks consistent judicial standards. Pre-event compliance construction by enterprises can hardly exert its exculpatory defense effect.

In terms of objective constitutive elements, ambiguous boundaries for criminalization of neutral assisting conducts constitute a prominent contradiction in network-platform cases. Most businesses of network platforms are neutral in technical appearance. Technical tools are value-neutral per se: they can serve massive legitimate social subjects while risking exploitation by criminals. The core spirit of the neutral-assisting-conduct theory lies in constraining punishment scope of criminal law and preventing criminal punishment from suppressing normal market-economy activities.

Translated into judicial practice, the challenge becomes distinguishing normal neutral commercial businesses of platforms from punishable assisting conducts under this crime. Where network platforms provide general-purpose and basic online services without modifying functions for criminal demands, they shall in principle not be subject to criminal punishment even if their services are exploited by crimes. Only where platform services are highly adapted for criminal activities and platforms subjectively clearly know that crimes will exploit such services do the conducts possess criminal punishability. Nevertheless, some judicial decisions ignore the value of the neutral-assisting-conduct theory. Platforms are directly held criminally liable merely based on objective harmful consequences and exploitation of platform services by criminals, generating risks of objective imputation.

Confusion over demarcation standards between the Crime of Aiding Information-Network Criminal Activities and the Crime of Refusing to Perform Obligations for Information-Network Security Management represents a core controversy in the field of platform criminal liability. The two charges jointly regulate network-service providers yet differ significantly in behavioural patterns, subjective elements and procedural prerequisites. The Crime of Refusing to Perform Obligations for Information-Network Security Management requires the statutory precondition of "refusing to take corrective measures after being ordered by regulatory authorities", which is not required for the Crime of Aiding Information-Network Criminal Activities. The former mainly evaluates omissive management dereliction of network platforms, namely platforms' refusal to perform statutory information-network-security-management obligations. The latter prioritizes positive commission-based technical assisting conducts, though it can theoretically cover certain omissive circumstances. From the perspective of subjective culpability, the Crime of Aiding Information-Network Criminal Activities requires actors' knowledge of others' information-network crimes and intent to assist crimes. As for the Crime of Refusing to Perform Obligations for Information-Network Security Management, academia holds the mixed-culpability theory: actors intend to refuse

rectification, yet they may act either intentionally or negligently regarding resulting serious harmful consequences, so its scope of subjective culpability is broader than that of the Crime of Aiding Information-Network Criminal Activities.

Nevertheless, prominent misapplication emerges in judicial practice. To bypass the rectification-order precondition of the Crime of Refusing to Perform Obligations for Information-Network Security Management, some purely omissive platform cases that should be judged under that charge are directly characterized as the Crime of Aiding Information-Network Criminal Activities. Such judicial reasoning empties the legislative value of the Crime of Refusing to Perform Obligations for Information-Network Security Management and unduly expands the application scope of the Crime of Aiding Information-Network Criminal Activities. The legislative design of the rectification-order precondition embodies the modesty principle of criminal law: for purely omissive dereliction by platforms, administrative supervision shall intervene in priority. Criminal punishment shall only be triggered after regulatory authorities issue formal rectification orders and platforms still refuse compliance. Bypassing this element and directly applying the Crime of Aiding Information-Network Criminal Activities deviates from legislative purposes.

Defects in unit-crime imputation mechanisms also restrict reasonable implementation of network-platform criminal liability. Criminal-law provisions explicitly state that units can commit the Crime of Aiding Information-Network Criminal Activities. In judicial practice against internet platform enterprises, however, only individual employees who directly commit acts are often punished, while convictions against platform units themselves are avoided. The unit-crime system is to some extent nominalized in platform-related cases. Many platform-related crimes originate from organizational dimensions: risks stem from enterprises' overall business models and defects in internal risk-control systems rather than merely individual will of several employees. Punishing only grassroots employees cannot force enterprises to improve cybersecurity compliance construction at the institutional level and fails to realize the general-prevention effect of criminal law. The

organizational-responsibility theory advocates assessing unit criminal liability from perspectives of organizational systems, decision-making processes and corporate cultures of entities, instead of fully depending on subjective intent of senior natural-person personnel within units. This theory better adapts to governance realities of large-scale internet platforms yet has not been fully adopted in judicial decisions. How to prove subjective intent of platform units and whether effective enterprise compliance systems can serve as defenses for unit crimes lack unified and clear guidance in current judicial documents.

In addition, the mechanism connecting administrative and criminal procedures does not operate smoothly. A large number of illegal circumstances of network platforms lie at the intersection of administrative violations and criminal offences. Where platforms fail to perform security-management obligations, administrative competent authorities including cyberspace-affairs departments, public-security organs and communications-administrative authorities shall first impose administrative sanctions. However, clear and operable standards are absent regarding what degree of harm and subjective status mark the crossing from administrative-law boundaries into criminal-law evaluation. Two types of deviations co-exist in practice: some cases skip administrative-law enforcement and initiate criminal procedures prematurely; others only end with administrative penalties while clues of suspected criminal offences are not transferred to judicial organs in accordance with law, resulting in unbalanced sanctions.

4. Enlightenment from Extraterritorial Institutional Experience

Faced with challenges in determining liability of network-service providers, extraterritorial digital legislation has accumulated certain institutional experience, which can provide references for handling criminal liability of network platforms under the Crime of Aiding Information-Network Criminal Activities in China. Still, extraterritorial institutions are rooted in local legal systems and cannot be mechanically transplanted without discrimination.

The European Union's Digital Services Act establishes a tiered-liability system for network-service providers. Providers are

classified into ordinary service providers, hosting service providers and very large online platforms according to business types and scales, and differentiated duty-of-care obligations are allocated to different tiers of platforms. [9] In principle, basic neutral network-service providers shall not be held liable for illegal acts committed by users. Liability assessment is triggered only when platforms actually and definitely know of illegal content yet possess technical disposal capacities and refuse to take actions. Meanwhile, compliance-defense mechanisms are established: platforms can obtain liability mitigation or exemption if they prove that they have implemented risk-prevention and-control measures required by law. The tiered-liability concept offers important enlightenment: one-size-fits-all standards shall not be adopted for platforms' security-management obligations. Obligation intensity shall match platforms' technical capacities, business scales and service types. Small-and-medium-sized platforms with weak technical capabilities shall not be burdened with identical review obligations as leading large-scale platforms.

The United States' safe-harbour rule originated from civil copyright-infringement fields. Its core gist is: where network platforms are unaware of infringing content and remove relevant content promptly upon receiving valid notices, they can be exempted from civil liability. Although the safe-harbour rule belongs to civil-law institutions, its jurisprudence can also be referenced for criminal justice. It rejects unduly elevating platforms' proactive monitoring obligations. The law does not require platforms to conduct indiscriminate screening of all information within platforms. Platforms bear disposal obligations only upon receiving clear and valid reports. This logic reminds us that criminal law shall not impose unlimited ex-ante monitoring obligations on network platforms; otherwise platforms may conduct excessive censorship over online information to evade criminal risks and inhibit innovation vitality of the internet industry.

It shall be soberly recognized that extraterritorial institutions grow from corresponding social contexts. China bears special practical governance demands in combating telecom-and-online fraud and other cyber-crimes. Therefore, extraterritorial rules shall not be copied directly to fully relax

platform liability. Instead, their rational core shall be absorbed. We shall adhere to the basic logic of matching liability with capacity and strike a balance between crime governance and development of the digital industry.

5. Improvement Paths for Criminal Liability of Network Platforms under the Crime of Aiding Information-Network Criminal Activities

Based on current criminal-law provisions and judicial interpretations of China, targeting various contradictions exposed in determining criminal liability of network platforms, comprehensive measures shall be taken from multiple dimensions including subjective-element identification standards, coordination of the crime system, substantive judgment framework for neutral assisting conducts, improvement of unit-imputation systems, optimization of administrative-criminal connection mechanisms and refinement of judicial interpretations, to construct a criminal-liability-determination system adapting to realities of network platforms.

First, standardize judicial determination of "knowledge" under this crime and establish adjudication rules with parallel presumption of knowledge and counter-evidence defense. (1) In judicial decisions, strictly distinguish criminal-law knowledge from foreseeable risks in business operations. Knowledge required for establishing this crime is not equivalent to management negligence in platform operations. Mere foresight of abstract risks of business abuse by wrongdoers is insufficient to satisfy subjective constitutive elements of this crime. Actors must know or highly confirm that others are committing criminal offences via platforms; mere negligence cannot establish this crime. (2) Refine the applicable boundary of generalized knowledge. To establish this crime against platforms, it suffices to know others commit information-network crimes without knowing specific names of upstream crimes. Nevertheless, existence of general administrative violations on platforms shall not be directly presumed as knowledge of criminal offences under criminal law. Judicial decisions shall comprehensively determine subjective knowledge based on multiple pieces of objective evidence including formal written notifications from regulatory authorities, massive valid crime-clue reports, transaction patterns obviously deviating from

market common sense, and platforms' special development of functions adapted for criminal activities. Mutual corroboration among multiple pieces of evidence is required; presumption of platforms' subjective knowledge shall not be made based merely on single objective facts. (3) Clarify the counter-evidence effect of platform compliance systems. [10] Where judicial organs presume knowledge based on objective facts, network platforms shall be granted opportunities to submit evidence for defense. If platforms adduce evidence proving that they have established and practically implemented compliance systems for risk control, review, early-warning and disposal matching their business-risk levels and have fulfilled reasonable network-security-management obligations, the presumption of knowledge can be rebutted and criminal establishment can be precluded. Pre-event compliance construction of platforms shall be transformed into defenses under criminal law to motivate platforms to conduct proactive pre-event risk governance rather than merely take post-event remedies after harmful consequences occur.

Second, rationalize the division of application between the Crime of Aiding Information-Network Criminal Activities and the Crime of Refusing to Perform Obligations for Information-Network Security Management and clarify their boundaries. The following adjudication thinking shall be established: where platforms commit positive commission-based acts, proactively provide technical tools specially adapted for crimes and actively empower cyber-crimes, the Crime of Aiding Information-Network Criminal Activities shall apply in priority without satisfying the administrative rectification-order precondition. Where platforms merely provide general-purpose online services without positive assisting conducts and only learn of users' crimes afterwards yet refuse to delete or block illegal activities, such purely omissive management dereliction shall be judged under the Crime of Refusing to Perform Obligations for Information-Network Security Management in priority, and the statutory precondition "refusing to take corrective measures after being ordered to do so by regulatory authorities" stipulated in criminal-law provisions must be strictly observed. Judicial organs shall not arbitrarily bypass this element and convict under the Crime of Aiding Information-Network

Criminal Activities. Where one act satisfies constitutive elements of both crimes, punishment shall be imposed for the more serious crime in accordance with concurrence-of-offence rules of criminal-law provisions, and repeated negative evaluation for one single act is prohibited. Such division can not only curb the tendency of the Crime of Aiding Information-Network Criminal Activities becoming a pocket crime, but also activate the institutional value of the Crime of Refusing to Perform Obligations for Information-Network Security Management and fully realize functions of the crime system designed by legislators.

Meanwhile, establish a substantive judgment framework for neutral assisting conducts adapting to judicial practice to demarcate criminal-punishment boundaries for platforms. To distinguish neutral platform businesses from criminal assisting conducts, hierarchical and progressive substantive judgment shall be carried out. Step one: examine objective attributes of services provided by platforms and distinguish general-purpose public technical services from specially customized services oriented toward illegal and criminal activities. Basic cloud storage, ordinary communication transmission and other businesses are typical neutral general-purpose services and shall in principle not trigger criminal liability. Specially developed tool interfaces for fund-laundering, supervision evasion, fraud and so on carry inherently high criminal risks. Step two: conduct subjective review and examine whether platforms subjectively and definitely know that others will exploit such services to commit crimes. Step three: assess primary purposes and profit sources of platform businesses, and judge whether platform operations target legitimate markets or deliberately pursue illegal gains generated by criminal activities. After three-layer substantive judgment, normal neutral commercial businesses, even if exploited by criminals to generate serious harmful consequences, shall be regulated under administrative law rather than readily subject to criminal punishment, preventing excessive intervention of criminal law into normal operations of the digital market.

Further improve unit-crime criminal-liability imputation systems for network platforms and implement the organizational-responsibility theory to change the judicial reality of punishing only individuals while ignoring unit entities. (1)

Clearly distinguish unit crimes from natural-person crimes. Where crime decisions originate from platform management, acts are carried out relying on the whole platform business system and illegal gains belong to platforms as a whole, unit crimes shall be established. Fines shall be imposed on platform units, while criminal liability of persons-in-charge and directly-responsible personnel shall be pursued simultaneously. Crimes originating from organizational dimensions shall not be simplistically downgraded to individual employee crimes. (2) Take effective platform compliance systems into sentencing considerations for unit crimes and endow them with limited exculpatory reference value. Pre-established and practically-operated network-risk-prevention compliance systems of platforms can serve as mitigating circumstances for units. If so-called compliance systems exist only on paper without practical implementation, aggravating factors shall be considered in evaluation. (3) Refine liability division among internal personnel of units, distinguishing decision-makers, active executors and ordinary grassroots employees. Prevent undue expansion of punishment scope and avoid ordinary employees bearing excessive criminal liability merely due to defects in enterprise systems.

Constantly improve the institutional design connecting administrative and criminal procedures and build a step-by-step governance model featuring administrative priority and criminal law as the last resort. Most compliance defects and management oversights of network platforms shall first be subject to administrative penalties imposed by competent authorities including cyberspace-affairs departments, public-security organs and the Ministry of Industry and Information Technology to urge platforms to complete rectification. Criminal accountability procedures shall only be initiated when acts satisfy all constitutive elements including subjective knowledge and serious circumstances. Improve case-transfer mechanisms: where administrative organs discover suspected criminal offences in administrative-case handling, clues shall be transferred to judicial organs in a timely manner in accordance with law. Where judicial organs hold that conducts do not reach criminal-punishment standards after trial, cases shall be transferred to competent administrative authorities for administrative sanctions. Both

mistakes of substituting criminal punishment for administrative sanctions and substituting administrative penalties for criminal punishment shall be prohibited. Implement the criminal-policy of tempering justice with mercy and impose differentiated dispositions by comprehensively considering platforms' subjective malignancy, actual harmful consequences, platforms' rectification and cooperation performance, and effects of loss recovery.

In the long run, judicial interpretations shall further refine identification standards for "serious circumstances" targeting network-platform subjects. Quantitative indicators for "serious circumstances" in existing judicial interpretations are mostly designed for natural-person "two-card" cases, while judgment criteria adapted to large-scale technical services of network platforms are scarce. Future judicial interpretations may combine characteristics of platform businesses, comprehensively consider factors including quantity of assisted crimes, total losses of victims, illegal gains of platforms, circumstances of platforms' refusal of regulatory rectification, and whether platforms specially modify business functions for crimes, and establish conviction standards balancing quantitative indicators and comprehensive evaluation to reduce arbitrariness in judicial discretion.

6. Conclusion

As critical infrastructure of the digital society, applying the Crime of Aiding Information-Network Criminal Activities to network platforms undertakes dual value missions. On the one hand, criminal-law weapons must be utilized to crack down grey-and-black cyber-industrial chains bred by platforms, protect people's property safety and respond to public demands for cybersecurity. On the other hand, criminal law shall adhere to its modesty principle. The scope of criminal punishment shall not be expanded without limits, and excessive suppression over normal innovation and operations of the internet shall be avoided.

Criminal liability of network platforms cannot be handled in a simplistic and one-size-fits-all manner. Not all management defects and risk-control loopholes in platform operations shall be indiscriminately incorporated into

criminal evaluation. Judicial practice shall return to basic principles of criminal-law dogmatics, strictly grasp the standard for determining subjective “knowledge” under this crime, establish rules with parallel presumption and counter-evidence, conduct substantive screening of neutral assisting conducts, rationalize the division of application between the Crime of Aiding Information-Network Criminal Activities and the Crime of Refusing to Perform Obligations for Information-Network Security Management, activate the original institutional functions of the latter crime, improve unit-crime imputation rules for platforms, optimize disposal procedures connecting administrative and criminal procedures, and give full play to the defense value of enterprise compliance. A balance shall be struck between punishing cyber-crimes and safeguarding the sound development of the digital economy to realize unification of legal and social effects.

References

- [1] Wang Yanqiang. Research on Concurrence Issues of the Crime of Aiding Information-Network Criminal Activities. *Law Forum*, 2025, (02):28-41.
- [2] Yu Hongyao, Lan Luxiao. Dogmatic Interpretation on Normative Attribute of the Crime of Aiding Information-Network Criminal Activities. *Journal of Heilongjiang Administrative Cadre Institute of Politics and Law*, 2024, (05):38-42.
- [3] Zhang Mingkai. On the Crime of Aiding Information-Network Criminal Activities. *Political Science and Law*, 2016, (02):2-16.
- [4] Chen Xingliang. Turning the Accomplice into the Perpetrator: Perspective from the Crime of Providing Assistance in Cybercriminal Activities. *Comparative Law Review*, 2022, (02):44-58.
- [5] Jing Lijia. On the Normative Attribute of the Crime of Aiding Information-Network Criminal Activities. *The Jurist*, 2025, (02):116-130+194-195.
- [6] Liu Ziliang. Negation of Subordination and Justification of Independence of the Crime of Aiding Information-Network Criminal Activities — From the Standpoint of Normative Theory. *Journal of Henan University of Economics and Law*, 2024, (02):106-118.
- [7] Li Miao. Criminal Regulation Approach of Omission of Network Platforms. *Oriental Law*, 2026, (01):44-60.
- [8] Wang Zhiyuan, Wang Yubo. Crime of Aiding Information-Network Criminal Activities or Concealment-Disguise Crime: Dilemma and Solution of Attribution of Payment-Settlement-Type Assisting Behaviors. *Journal of Shandong Police College*, 2023, (06):5-12.
- [9] Ding Xiaodong. Second-Generation Internet Rules? Platform Liability in Light of the EU Digital Services Act. *Journal of East China University of Political Science and Law*, 2026, (1):22-37.
- [10] Chen Hongbing. Review on Legislation and Application of New- type Cyber- crime in China. *Journal of Guangxi University (Philosophy and Social Science Edition)*, 2022,(02):185-198.DOI:10.13624/j.cnki.jgu pss.2022.02.013.