JOURNAL OF LEGAL STUDIES
"Vasile Goldiș" Western University of Arad
J. L. S.
2026 – 37(51)
DOI: 10.2478/jles-2026-0007

OVERCRIMINALIZATION IN CYBERCRIME GOVERNANCE: JUDICIAL RESTRAINT IN REGULATING ASSISTANCE TO ONLINE CRIMES IN CHINA

Rui Li*
School of Law, Dalian Ocean University, Dalian, Liaoning 116023, China
E-mail: a2028ksuasciiz@gmail.com

(**Received: March 2026; Accepted: April 2026; Published: May 2026**)

Abstract: Overcriminalization has become a central concern in contemporary cybercrime governance. In China, the Crime of Assisting Information Network Criminal Activities (CAINCA), introduced in 2015, criminalizes assistance that creates abstract risks within cybercrime networks. In judicial practice, however, the offense has gradually expanded through permissive presumptions of knowledge and mechanical reliance on quantitative thresholds, particularly after the 2020 "Duanka" campaign. Drawing on doctrinal analysis and three representative cases from the People's Court Case Database, this article demonstrates how courts have blurred the boundary between neutral technical services and culpable facilitation. To address these risks, it proposes a framework of judicial restraint: restricting mens rea to actual knowledge, applying objective imputation to neutral assistance, prioritizing accomplice liability where upstream crimes can be identified, and strengthening individualized sentencing. These reforms aim to reconcile effective cybercrime governance with the principles of culpability and proportionality in criminal law.

Keywords: Overcriminalization; cybercrime; neutral assistance; judicial restraint; accomplice liability.

1. Introduction

Overcriminalization remains one of the most persistent pathologies of contemporary criminal law. When the scope of criminal liability expands beyond morally blameworthy conduct, causes concrete harm, or serves a substantial state interest, the criminal sanction loses its legitimacy and becomes an instrument of regulatory convenience rather than justice (Husak, 2017). Husak identifies two interlocking sets

* Corresponding author: Rui Li. *E-mail: a2028ksuasciiz@gmail.com*

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

of limiting principles: moral-philosophical constraints that require prohibited conduct to be wrongful and deserving of punishment, and political-theoretical constraints that demand the criminalization advance a legitimate state interest without being broader than necessary (Husak, 2017, p. 25). When these constraints are disregarded, criminal law inflates, diluting the moral stigma of conviction, overwhelming enforcement resources, and punishing conduct that could be addressed through less intrusive means (Luna, 2004).

The governance of cybercrime has dramatically intensified this global tension. The transnational, anonymous, and infrastructure-dependent nature of digital offenses blurs traditional distinctions between principals and accomplices, prompting legislatures to enact broad, risk-based assistance offenses that target facilitators independently of completed crimes (Wall, 2008). Wall describes this legislative response as part of a wider "culture of fear" surrounding cyber threats, in which exaggerated perceptions of risk drive expansive criminalization strategies that prioritize prevention over precise culpability assessment (Wall, 2008, p. 862). Gordon and Ford's influential typology further illuminates the problem: Type I cybercrime is primarily technological, while Type II is human-element driven and relies heavily on legitimate commercial infrastructure such as payment gateways, advertising platforms, and technical support services (Gordon & Ford, 2006). In such environments, ordinary business conduct can be exploited as facilitation without the provider's direct intent, tempting courts and prosecutors to relax evidentiary standards and expand liability downward to low-level or neutral actors.

In China, the Crime of Assisting Information Network Criminal Activities (CAINCA), introduced by the Ninth Amendment to the Criminal Law in 2015 (Art. 287(2)), exemplifies this dynamic. The provision independently criminalizes the knowing provision of internet access, server hosting, network storage, communications transmission, advertising promotion, payment settlement, or other technical support when another person uses an information network to commit a crime, and the circumstances are serious. Legislators designed CAINCA to sever assistance chains in borderless cyberspace, where principal fraudsters are often unreachable while facilitators remain readily apprehendable (Li, 2017; Yu, Z. G., 2017). The nationwide "Duanka" (Break the Card) campaign launched in October 2020 dramatically accelerated enforcement. Judicial big data show a 34-fold increase in CAINCA prosecutions in 2020 and a further 17-fold rise in 2021, with annual indictments exceeding 140,000 by 2023 (Liu, 2023; Wu, 2025). While the campaign successfully disrupted fraud syndicates, it also generated systemic pressure toward mechanical application of incrimination thresholds and permissive presumptions of

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

subjective knowledge, transforming CAINCA into a de facto catch-all instrument (Du et al., 2025).

This judicial expansion manifests in three primary dimensions: first, mechanical reliance on quantitative thresholds (card numbers, transaction volumes) without requiring proof of actual upstream crime; second, unrestricted inference of "knowledge" from objective anomalies such as cash remuneration, cross-province travel, or irregular business registration; and third, erosion of boundaries between neutral technical services and culpable facilitation (Liu, 2023; Chen, 2008, 2022). These practices have progressively recast CAINCA as a risk-management tool rather than a culpability-based offense, raising serious concerns about proportionality and the principle that criminal law should be used only as a last resort (Husak, 2017; Garland, 2001). In response, the Supreme People's Court, Supreme People's Procuratorate, and Ministry of Public Security issued the 2025 Joint Opinion, accompanied by typical cases that signal a corrective orientation toward judicial restraint, subsidiarity, and stricter proof of mens rea (Du et al., 2025).

Against this backdrop, the present article adopts a criminal-law dogmatic approach to examine the rational boundaries of CAINCA adjudication. It argues that subjective knowledge must be strictly construed as actual and specific awareness, that objective imputation theory should delimit neutral technical assistance, that an accomplice-priority principle should replace the prevailing CAINCA-first approach in cases of concurrence, and that sentencing proportionality must be enforced through individualized assessment of the defendant's role and vulnerability. By integrating global theoretical insights (Husak, 2017; Luna, 2004; Wall, 2008) with detailed analysis of three representative cases from the People's Court Case Database, including the acquittal-oriented "Zhang" case, the advertising-facilitation "Wang Mousheng" case, and the cross-province account-opening "Yang Moulei" case, this study demonstrates both the global parallels and the distinctive challenges of regulating digital assistance in China's high-volume digital economy.

This article makes three principal contributions. First, it integrates global overcriminalization theory with granular doctrinal analysis of Chinese law to offer the first systematic four-pillar judicial-restraint framework grounded in the People's Court Case Database. Second, it diagnoses the specific mechanisms through which judicial practice has over-expanded CAINCA liability, drawing on three representative cases decided between 2021 and 2024. Third, it situates China's enforcement trajectory within the broader comparative context of European cybercrime regulation, identifying structural differences with implications for

legislative design and judicial interpretation. The scope of the research encompasses CAINCA adjudication from 2015 to 2025, with particular emphasis on the post-Duanka enforcement surge and its doctrinal consequences.

The article is organized as follows. Section 2 develops the theoretical framework of overcriminalization and judicial restraint. Section 3 analyzes the legislative design and judicial expansion of CAINCA, including three representative cases. Section 4 proposes a normative reconstruction grounded in the four pillars of restraint. Section 5 situates China's experience in a comparative and global perspective, with particular attention to European cybercrime regulatory frameworks. Section 6 concludes with reflections on the research's strengths, limitations, and implications for the legal community.

2. Theoretical Framework: Overcriminalization and Judicial Restraint

Overcriminalization represents one of the central pathologies of contemporary criminal law systems. It occurs when the scope of criminal liability expands beyond what is justified by moral blameworthiness, concrete harm, or legitimate state interests, resulting in excessive punishment and erosion of the criminal law's normative legitimacy (Husak, 2017). The phenomenon is not merely a quantitative increase in the number of criminal offenses but a qualitative failure to adhere to principled constraints. Husak identifies two main sets of limiting principles: moral-philosophical constraints requiring that prohibited conduct be wrongful, cause or risk harm, and be deserving of punishment; and political theoretical constraints demanding that criminalization serve a substantial state interest, actually advance that interest, and be no broader than necessary. When these constraints are disregarded, criminal law degenerates into an instrument of regulatory convenience rather than justice, producing what scholars describe as "criminal law inflation," the routine deployment of penal sanctions for conduct that could be adequately addressed through civil, administrative, or social mechanisms (Luna, 2004).

This inflation carries profound systemic consequences. Overcriminalization dilutes the moral stigma of criminal conviction, making punishment less meaningful and more routine. It overwhelms prosecutorial and judicial resources, forcing selective enforcement that introduces arbitrariness and inequality. Most critically, it violates the principle of culpability by punishing individuals whose conduct lacks sufficient blameworthiness, thereby undermining the moral foundations of the criminal sanction (Husak, 2017). In regulatory states, criminal law increasingly functions as a risk-management tool rather than a response to concrete wrongdoing, a tendency that becomes particularly acute in rapidly evolving technological domains where

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

legislatures and courts face strong pressure to act decisively in response to emerging threats (Luna, 2004).

The De Facto Dimension of Overcriminalization in Digital Enforcement

The problem of overcriminalization is not only de jure (embedded in statutory language) but equally de facto, arising from the law in action. As Husak observes, whether overcriminalization is a de jure or de facto phenomenon depends on how enforcement practices transform broad legislative provisions into tools of selective and arbitrary punishment (Husak, 2023, p. 266). In the cybercrime context, this de facto expansion manifests through prosecutorial incentives, performance metrics tied to case clearance rates, and simplified evidentiary shortcuts that lower the practical threshold for conviction. Luna explains that such selective enforcement introduces systemic arbitrariness: prosecutors and courts, under pressure to demonstrate results in high-volume digital crime campaigns, routinely rely on quantitative indicators rather than individualized culpability assessments, producing unequal treatment of similarly situated defendants and punishing peripheral or low culpability actors who could be addressed through administrative or civil measures (Luna, 2004). This enforcement-driven inflation is especially pronounced in digital assistance cases, where the sheer volume of potential facilitators creates institutional temptation to presume knowledge and contribution without rigorous proof.

The governance of cybercrime amplifies these dynamics in distinctive ways. Because digital offenses rely heavily on infrastructure provided by commercial actors, the distinction between Type II facilitators and neutral service providers becomes acutely contested. As Gordon and Ford (2006, p. 14) observe, ordinary commercial services can be exploited as components of criminal enterprise without the provider's direct intent, generating "human-element driven assistance chains" that challenge conventional accomplice liability rules. In such environments, prosecutors face a persistent temptation to expand liability downward, sweeping standard infrastructure providers into criminal nets designed for deliberate facilitators. The result is a proliferation of conduct-based offenses that sweep in neutral or low-culpability behavior, often justified by the difficulty of prosecuting upstream principals. In such environments, criminal law risks becoming a blunt regulatory instrument rather than a mechanism of justice, reproducing the very overcriminalization pathologies that Husak and Luna identify in more conventional regulatory contexts (Husak, 2017; Luna, 2004).

Judicial restraint emerges as the essential corrective principle. Restraint requires courts to enforce the limiting constraints that legislatures too often disregard. At a

minimum, it demands adherence to the principles of proportionality, subsidiarity, and minimal criminalization. Proportionality insists that the severity of punishment correspond to the gravity of the wrong and the degree of culpability involved. Subsidiarity requires that criminal law be used only when less intrusive means, such as civil liability, administrative sanctions, or technological regulation, are inadequate. Minimal criminalization demands that penal liability attach only to conduct that is both wrongful and deserving of censure (Husak, 2017, 2023). Garland traces the historical shift toward a "culture of control" in late-modern societies, where punitive responses replace welfare-oriented strategies and criminal law becomes a default governance tool; as Garland (2001, p. 156) puts it, "policy has become the problem rather than the solution." Restraint counters this trend by insisting that courts apply a strict construction of mens rea, rigorous objective imputation, and preference for specific offenses over catch-all provisions. In the context of cybercrime, judicial restraint is particularly urgent. The anonymity and transnational character of digital offenses create strong temptations to relax evidentiary standards and expand liability to facilitators. Yet it is precisely in such high-pressure environments that doctrinal discipline is most needed to prevent the normalization of overcriminalization (Wall, 2008). Courts must therefore serve as a backstop against legislative and prosecutorial overreach, ensuring that criminal sanctions remain tethered to blameworthy conduct rather than perceived risk alone.
This theoretical framework, overcriminalization as principled failure, cybercrime governance as risk-driven expansion, and judicial restraint as a necessary counterbalance, provides the analytical lens for examining China's CAINCA regime. The following sections apply these concepts to the legislative design, judicial expansion, and normative reconstruction of CAINCA, demonstrating both the global parallels and the specific challenges of regulating digital assistance in an emerging digital economy.

3. The Chinese Context: Legislative Design and Judicial Expansion of CAINCA

The introduction of the Crime of Assisting Information Network Criminal Activities (CAINCA) through the Ninth Amendment to the Criminal Law in 2015 represented a significant legislative response to the rapidly evolving landscape of cyber-enabled crime in China. By 2015, telecom and internet fraud had become a major public security issue, with criminal groups exploiting the anonymity and borderless nature of cyberspace to operate large-scale fraud schemes. Principal offenders frequently resided overseas or used anonymized tools, making it nearly impossible for law enforcement to apprehend them or prove their specific criminal acts in many cases

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

(Yu, H. S., 2019). Traditional complicity doctrine under Articles 27–29 of the Criminal Law required proof of a completed principal offense before an accessory could be punished, creating a structural enforcement gap: facilitators who provided essential technical, financial, or logistical support could rarely be convicted because the upstream crime could not be fully established (Zhang, 2016).

The legislative purpose of CAINCA was therefore twofold. First, it aimed to sever the assistance chains that sustained cybercrime ecosystems by criminalizing the provision of support services independently of the principal offense. Second, it sought to shift the focus from completed harm to abstract risk creation, allowing early intervention against behaviors that objectively increase the likelihood of cybercrime (Li, 2017). Article 287(2) explicitly targets internet access, server hosting, network storage, communications transmission, advertising promotion, payment settlement, or "other technical support," provided the actor knows the services will be used for criminal purposes and the circumstances are serious. This design deliberately departs from the accessory nature of traditional complicity, establishing CAINCA as a semi-independent principal offense focused on disrupting the infrastructure of cybercrime networks (Yu, Z. G., 2017). The legislative choice reflected a pragmatic judgment that the unique features of digital crime transnationality, anonymity, and dependence on legitimate infrastructure necessitated a departure from conventional accomplice liability rules.

The nationwide "Duanka" (Break the Card) campaign, launched in October 2020 by the Ministry of Public Security and coordinated with judicial and procuratorial organs, dramatically accelerated the enforcement of CAINCA and exposed its expansionary potential. The campaign targeted the provision of bank cards, telephone cards, and online payment accounts used in telecom and internet fraud, treating such conduct as a core facilitator of upstream crimes. Under the campaign's high-pressure enforcement model, procuratorates and courts were incentivized to rapidly process large volumes of cases, often relying on simplified evidence standards and performance metrics tied to case clearance rates (Du et al., 2025). This led to a massive surge in CAINCA prosecutions: judicial big data reports indicate a 34-fold increase in case numbers in 2020 compared to the previous year, followed by a further 17-fold rise in 2021, with annual indictments exceeding 140,000 by 2023 (Liu, 2023; Wu, 2025). While the campaign achieved notable success in dismantling fraud syndicates and recovering illicit proceeds, it also generated systemic pressure to expand liability downward to low-level facilitators, many of whom were

economically marginalized individuals recruited through debt coercion or online promises of easy income.

The campaign's emphasis on quantitative indicators, such as the number of cards provided, transaction volume, and number of downstream victims, further entrenched the mechanical application of incrimination thresholds. Prosecutors frequently treated these metrics as near-conclusive evidence of both objective contribution and subjective knowledge, bypassing the need for detailed proof of actual awareness of the criminal purpose (Wu, 2025). This enforcement model, while effective in disrupting fraud chains, transformed CAINCA from a targeted measure against culpable assistance into a broad instrument of social control, disproportionately affecting rural migrants, young people with limited financial literacy, and debt-burdened individuals who constituted the majority of defendants (Liu, 2023). In response to these expansionary tendencies, the Supreme People's Court, Supreme People's Procuratorate, and Ministry of Public Security issued the 2025 Joint Opinion, accompanied by typical cases that explicitly signal a corrective orientation toward stricter proof of subjective knowledge, objective contribution, and subsidiarity, urging courts to avoid mechanical presumptions and overbroad application (Du et al., 2025).

These legislative and policy developments set the stage for significant judicial expansion in practice, vividly illustrated in three representative cases from the People's Court Case Database.

3.1. Zhang Mou Case

Zhang Mou and five co-defendants traveled from Chongqing to Beijing's Shunyi District in September 2021 after being recruited by a card-collecting intermediary. They were promised 3,000–5,000 yuan per credit card for opening personal and corporate accounts. Zhang opened seven cards across multiple banks. After completion, he handed the cards to the intermediary for inspection; the intermediary rejected two for insufficient credit limits and instructed Zhang to hold the remaining five until a downstream buyer was ready. Before any delivery occurred, police intercepted the group based on anti-fraud intelligence and seized the cards from the defendants' possession. The public prosecutor charged all six under CAINCA, citing "sale of five or more credit cards" under the 2021 Joint Opinion on Telecom Fraud as satisfying "serious circumstances".

The Shunyi District Court, however, refused to convict. In its detailed reasoning, the court identified two independent grounds for declining conviction. First, the transfer of cards to an end-user had not been completed at the time of interception, meaning the assistance transaction was still in a preparatory stage; the selling behavior had

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

not been completed because the cards had never been delivered to the actual downstream recipient who would use them in telecom fraud. Second, no traceable connection to an upstream criminal act had been established: the relevant credit cards had not entered the information-network crime chain and could not be linked to any specific criminal facts or harmful outcomes. This dual-requirement reasoning establishes that "serious circumstances" under CAINCA demands both completed delivery and demonstrated upstream linkage, not mere possession above a numerical threshold. Without an identifiable upstream principal offense and completed assistance, the quantitative threshold alone could not establish "serious circumstances." The prosecution subsequently withdrew the indictment on the grounds of changed evidence, and the court approved the withdrawal under Article 296 of the SPC Interpretation on the Criminal Procedure Law. All six cases became final (Zhang Mou et al. Case, 2023-04-1-257-001).

This outcome stands as a rare but powerful exemplar of substantive de-criminalization (Liu, 2023; Li, 2017). It demonstrates that CAINCA cannot be triggered by preparatory or incomplete facilitation absent proof of actual linkage to a concrete upstream crime, thereby preventing the offense from absorbing neutral or inchoate conduct.

3.2. Wang Mousheng Case

Wang Mousheng incorporated a sole-proprietorship network technology company in early 2020 and recruited two employees. The company solicited clients seeking advertising promotion for loan websites. Using legitimate enterprise credentials, the firm "cloaked" fake loan sites to make them appear credible on search engines and social platforms, then charged advertising fees totaling 2,354,529 yuan. The court explicitly distinguished this platform-level promotion from communication-layer conduct under Article 287(1) (illegal use of information networks). The court's reasoning drew a critical distinction between standard digital advertising and the company's conduct of "cloaking," that is, using legitimate enterprise credentials to fraudulently enhance the search-engine credibility of fake loan sites. The judgment treated this conduct as "actively elevating criminal risk" rather than passive service provision, and therefore found intentional facilitation rather than merely negligent assistance. The court convicted all three of CAINCA for actively elevating criminal risk through fraudulent credential enhancement and organized facilitation. The corporate-crime defense was rejected because the company was established and operated primarily for illegal promotion (Wang Mousheng et al. Case, 2023-03-1-257-001).

This case illustrates the boundary between neutral advertising services and culpable assistance: standard marketing becomes criminal when it deliberately enhances the credibility of fraudulent sites. The judgment also highlights the risk of overbreadth: when courts equate ordinary digital marketing with intentional criminal assistance, legitimate platform economies face chilling effects (Chen, 2022).

3.3. Yang Moulei Case

Yang Moulei, burdened by gambling debts, accepted a friend's suggestion to "facilitate loans." Despite explicit warnings that the intermediaries were unreliable, Yang traveled to Yanji, Jilin Province. There, an individual using an alias reimbursed his travel and daily expenses (300-yuan cash per day) and instructed him to open a corporate bank account. Yang completed facial recognition, obtained a business license, and handed over the corporate accounts, U-shield, and passwords. The account recorded a turnover of 39.23 million yuan, with funds traced to a telecom-fraud victim. The court applied the 2021 Joint Opinion and held that Yang's conduct constituted "other circumstances sufficient to determine knowledge" Specifically, the court identified four cumulative objective circumstances: (a) cash remuneration at above-market rates (300 yuan per day); (b) irregular cross-province travel for account-opening purposes; (c) the use of an alias by the directing individual; and (d) the surrender of banking credentials, U-shield, and passwords to third parties. Taken together, these factors were treated as sufficient to establish knowledge under the 2021 Joint Opinion, relying on cumulative objective indicators rather than direct proof of subjective awareness. The court convicted Yang of CAINCA and sentenced him to one year's imprisonment (Yang Moulei Case, 2024-04-1-257-001).

This decision exemplifies the "ought-to-know" expansion criticized in doctrine: financial desperation and contextual anomalies were treated as sufficient to infer actual knowledge without direct proof that Yang understood the specific fraud scheme (Zhang, 2023; Wu, 2025). The inference effectively lowered mens rea from actual awareness to negligence, illustrating the institutional risk of excessive presumptive authorization.

3.4. The Three Typical Manifestations of Judicial Expansion

Empirical review of CAINCA adjudication reveals three recurring patterns of over-expansion. First, generalization of subjective knowledge: courts routinely equate "ought to know" or "possibly know" with the statutory requirement of "knowing," shifting the burden of proof and treating objective anomalies, such as cash payment, cross-province travel, and irregular registration, as near-conclusive evidence of mens rea (Liu, 2023). Second, expansion of assisted objects: assistance is increasingly imputed to any downstream activity that might involve information networks, even

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

without proof of a completed principal offense or direct linkage (Chen, 2022). Third, lowering of the "serious circumstances" threshold: quantitative indicators of five or more cards, transaction volume is applied mechanically without requiring actual harm or a completed upstream crime, turning CAINCA into a low-barrier catch-all provision (Wu, 2025; Du et al., 2025). These patterns, while responsive to enforcement needs, have transformed the offense into an instrument of social control rather than targeted culpability-based punishment, disproportionately impacting vulnerable groups and undermining the principle of proportionality.

Taken together, the legislative design, policy-driven enforcement surge, and case outcomes demonstrate that CAINCA has deviated from its original intent. The provision, while necessary to address enforcement gaps in cyberspace, has been stretched through permissive presumptions, quantitative shortcuts, and blurred boundaries of neutrality. This judicial expansion mirrors global overcriminalization dynamics but carries unique risks in China's high-volume digital economy. The following section proposes a normative reconstruction grounded in judicial restraint to restore doctrinal precision and proportionality.

4. Normative Reconstruction: Toward Judicial Restraint

The judicial expansion of CAINCA has exposed a fundamental tension between effective cybercrime governance and the bedrock principles of criminal law. While the provision was legitimately conceived to sever assistance chains in anonymized digital networks, its application has progressively deviated from culpability-based foundations, producing disproportionate punishment and eroding public trust in the justice system (Liu, 2023). To restore doctrinal integrity, a normative reconstruction grounded in judicial restraint is imperative. This reconstruction draws on four interlocking pillars: restricting subjective knowledge to actual and specific awareness; applying objective imputation theory to delimit neutral technical assistance; adopting an accomplice priority principle in cases of offense concurrence; and enforcing proportionality in sentencing. These proposals are principled applications of existing criminal law dogmatics, reinforced by the 2025 Joint Opinion's corrective agenda and global scholarship on overcriminalization.

4.1. Restricting Subjective Knowledge to Actual and Specific Awareness

Current judicial practice frequently conflates the statutory requirement of "knowing" with lesser cognitive states such as "ought to know" or "possibly knowing," effectively lowering the mens rea threshold from intentionality to negligence (Zhang, 2023, p. 38). This substitution is incompatible with the principle of

culpability, as actual awareness of the criminal nature of the assisted conduct is constitutively required. Courts must adopt a multi-factor comprehensive assessment framework that evaluates the totality of circumstances rather than isolated objective indicators. Relevant factors include the defendant's prior relationship with principal offenders, the specificity of communications regarding criminal purpose, the degree of service customization for crime, and the presence of concrete warning signs that would alert a reasonable person to the criminal nature of the enterprise. Only when this assessment yields confident actual awareness should the subjective element be satisfied.

This shift restores the burden of proof on the prosecution to adduce affirmative evidence of knowledge, rather than shifting it to defendants through permissive presumptions. While this may increase prosecutorial difficulty, it upholds the foundational principle that the state bears the burden in criminal proceedings (Jiang, 2020). The 2025 Joint Opinion's typical cases provide practical guidance by demonstrating granular, contextual reasoning that traces connections between particular objective facts and conclusions about subjective awareness. In the Yang Moulei case, for example, the court's reliance on cash reimbursement and irregular travel to infer knowledge could be subjected to stricter scrutiny under this framework, requiring direct evidence that Yang understood the specific fraud scheme rather than merely suspected irregularity. Such a restrictive reading of "knowing" not only aligns with Zhang Mingkai's doctrinal insistence on actual awareness but also prevents the systematic over-criminalization of economically vulnerable defendants who lack a sophisticated understanding of downstream fraud chains.

4.2. Applying Objective Imputation Theory to Delimit Neutral Technical Assistance

Routine infrastructure services, including internet access provision, server hosting, software development, and payment settlement, satisfy CAINCA's objective elements whenever a client engages in criminal activities, regardless of provider awareness. Without a principled limiting framework, the provision is capable of sweeping the entire commercial technology sector within its ambit (Chen, 2008). Objective imputation theory provides the required limiting framework: criminal attribution requires not merely causal contribution but that the provider's specific conduct created a legally disapproved risk that materialized in the harmful outcome. Routine commercial provision, absent actual knowledge or deliberate customization for criminal purposes, does not satisfy this requirement.

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

Three specific criteria should guide the application. First, whether the service was standard and commercially available or specifically adapted for crime. Second, whether the provider took affirmative prevention steps, such as content moderation, abuse reporting, due diligence, or deliberately turned a blind eye. Third, whether there is proportionality between the criminal risk created and the legitimate social value of the service. Only when the first criterion is negative or the second and third weigh heavily against the provider should attribution occur (Chen, 2008). Applying these criteria to the Wang Mousheng case confirms the distinction between active facilitation, credential cloaking, SEO optimization targeting fraudulent sites, and passive provision, while standard hosting prosecutions illustrate the need for rigorous application to avoid chilling legitimate innovation. The framework aligns with the 2025 Joint Opinion's emphasis on distinguishing malicious grey-market services from ordinary commercial conduct and directly operationalizes Chen Hongbing's neutral-assistance theory in the digital context.

4.3. Adopting an Accomplice Priority Principle in Offense Concurrence

In complex cases where conduct constitutes both CAINCA and complicity in upstream fraud, judicial practice has exhibited a systematic preference for CAINCA, often prioritizing prosecutorial convenience over doctrinal precision (Jiang, 2020). This CAINCA-first approach violates the proportionality principle by imposing lighter penalties on individuals whose culpability corresponds to that of accessories in serious fraud. When the helper possesses clear, specific knowledge of the exact crime they are actively facilitating, they transcend the abstract risk creation targeted by CAINCA. In such scenarios, the helper must be prosecuted and punished strictly as an accomplice to the primary offense (Li, 2017). CAINCA should serve merely as a supplementary catch-all, reserved for cases lacking definitive upstream knowledge proof.

Evidentiary guidelines should specify indicators of specific knowledge: direct communication about criminal schemes, instructions describing fraud details, active evasion assistance, and compensation tied to upstream success (Jiang, 2020). This realignment ensures sentences reflect actual culpability and removes perverse incentives to charge under CAINCA. By adopting Li's (2017) "sentencing-rule" interpretation, courts can preserve the original legislative intent without undermining the accessory nature of assistance when a principal offense is provable.

4.4. Enforcing Proportionality in Sentencing and Substantive Assessment

Even when CAINCA liability is established, sentencing practices must reflect the principle of proportionality. Current trends often impose uniform penalties based on

quantitative thresholds of the number of cards and transaction volume, without adequate consideration of the defendant's position in the criminal hierarchy, actual profit scale, or degree of involvement. Small facilitators, often debt-burdened individuals recruited online with minimal profit, receive sentences disproportionate to their culpability, while higher-level organizers sometimes escape severe punishment (Liu, 2023). Proportionality requires individualized assessment: minor assistants who provide one or two cards with low remuneration and no active participation in fraud planning should receive suspended sentences or community corrections; those with substantial profit or organizational roles should face custodial terms commensurate with the harm facilitated.

The 2025 Joint Opinion implicitly supports this approach by issuing typical cases that differentiate between low-level "card mules" and active facilitators. Courts should explicitly consider the defendant's economic vulnerability, lack of prior criminal record, and peripheral role in the scheme. Beyond doctrinal reconstruction, institutional reforms are essential. First, performance metrics for prosecutors and courts must be decoupled from conviction rates to eliminate incentives for mechanical application. Second, legal aid for vulnerable defendants, rural migrants, students, and debt-burdened youth should be strengthened. Third, pre-charge knowledge assessments should become mandatory, treating permissive presumptions as an exception rather than the default (Wu, 2025). Finally, seamless integration between administrative and criminal measures through judicial recommendations, occupational prohibitions, and regulatory warnings can achieve effective governance without over-reliance on penal sanctions (Du et al., 2025). These institutional safeguards, combined with the four doctrinal pillars, form a closed-loop system that restores CAINCA's original purpose while safeguarding the restrained character of criminal law in the digital era.

5. Comparative and Global Implications

China's experience with CAINCA is neither unique nor isolated; it reflects broader global patterns in the regulation of cyber-assisted crime. Jurisdictions worldwide have responded to the scale and anonymity of digital offenses by enacting or expanding conduct-based assistance offenses that target facilitators independently of completed principal crimes. Yet the Chinese trajectory from legislative innovation in 2015 to rapid enforcement-driven expansion after 2020 and tentative corrective signals in 2025 offers both cautionary and constructive lessons for comparative criminal law scholarship and policy design.

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

5.1. Preventive Criminalization under the Culture of Fear

The global turn toward preventive, risk-based criminalization in cyberspace is deeply intertwined with what David Wall has termed the "culture of fear" surrounding cyber threats. Wall argues that exaggerated perceptions of digital vulnerability, amplified by media narratives, political rhetoric, and high-profile incidents, generate public and institutional demands for expansive control measures that prioritize symbolic reassurance over precise culpability assessment (Wall, 2008). In many common-law systems, this manifests through broad secondary-liability doctrines or specific computer-misuse statutes that criminalize preparatory conduct with minimal proof of intent. Civil-law and hybrid jurisdictions, including several EU member states, have adopted independent assistance offenses modeled on Article 287(2) CAINCA, yet most retain stronger proportionality safeguards such as mandatory harm thresholds or narrow mens rea requirements (Wall, 2008).

China's CAINCA regime represents an extreme variant of this preventive logic. The provision's abstract-risk orientation, combined with the Duanka campaign's quantitative enforcement model, has produced one of the highest per-capita prosecution rates for digital-assistance offenses worldwide. The surge in indictments, exceeding 140,000 annually by 2023, mirrors the enforcement-driven inflation that Wall associates with fear-based penal policy. Yet the 2025 Joint Opinion and its accompanying typical cases signal an emerging recognition that unchecked preventive criminalization risks undermining legitimacy. Brenner similarly highlights how the transnational and technically complex nature of cybercrime creates persistent enforcement dilemmas that tempt legislatures toward over-inclusive liability regimes, often at the expense of doctrinal precision (Brenner, 2012). China's rapid shift from legislative creativity to judicial overreach thus highlights a universal risk: when technological complexity meets institutional pressure for visible results, criminal law tends to relax doctrinal discipline unless courts actively reassert restraint.

5.2. The European Regulatory Model: Proportionality as Structural Constraint

A comparative examination of European cybercrime governance reveals a structurally different approach to the regulation of digital assistance, one that embeds proportionality and subsidiarity as positive legal constraints rather than mere interpretive principles. The Council of Europe's Budapest Convention on Cybercrime (2001), ratified by most EU member states, criminalizes aiding and abetting computer-related offenses but expressly confines liability to intentional facilitation, thereby excluding negligent or reckless assistance from the penal net

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

(Clough, 2012). The European Union's Directive 2013/40/EU on attacks against information systems similarly requires proof of intent and causally linked harm, leaving no room for the abstract-risk presumptions that characterize CAINCA enforcement in its expansive phase. This structural proportionality is reinforced by the European Court of Human Rights' jurisprudence under Article 7 ECHR (no punishment without law), which demands legal certainty and foreseeability in criminal liability, constraining broad catch-all provisions that would permit conviction on the basis of administrative anomalies or quantitative thresholds alone. Germany's approach under the Strafgesetzbuch (StGB) is particularly instructive. German criminal law applies the theory of objective imputation (objektive Zurechnung) as a mandatory analytical step in evaluating complicity, requiring not only that the assistant's conduct causally contributed to the principal offense but also that it created a legally disapproved risk that actually materialized in harm (Jakobs, 2004). As Jakobs explains, the basic assumption of objective imputation theory holds that whether a person has the right to behave in a certain way "cannot be determined by considering an isolated individual and a norm" but must always be determined "in the light of persons, i.e., of certain rules of a society" (Jakobs, 2004, p. 503). This doctrine functionally mirrors the limiting framework proposed in Section 4 of this article: neutral services that are standard in the marketplace do not satisfy the disapproved-risk criterion even if subsequently misused by a client. France's Code pénal adopts a comparable mens rea threshold under Article 121-7, requiring that the accomplice knowingly facilitated the commission of a crime or misdemeanor, a standard substantially more demanding than the permissive "ought-to-know" inferences that have characterized post-Duanka CAINCA adjudication.

The contrast between the Asian regulatory model exemplified by China's CAINCA and the European model illuminates a fundamental structural difference. As Clough (2012) observes, the Budapest Convention functions as a framework upon which specific offenses can be based, allowing countries to modify their laws while retaining core proportionality safeguards, rather than delegating those limits entirely to judicial interpretation after the fact. While both frameworks seek to disrupt cybercrime assistance chains, the European approach integrates proportionality constraints at the legislative design stage, requiring affirmative proof of intent, specific knowledge, and causally linked harm before criminal liability can attach. The CAINCA regime, by contrast, relies on judicial interpretation to impose these limits after the fact, creating conditions for enforcement-driven expansion when institutional pressure is high. The 2025 Joint Opinion's corrective orientation suggests a convergence toward European-style proportionality norms, but the

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

absence of structural legislative constraints means that judicial restraint remains fragile and contingent on sustained institutional commitment.

The European experience holds three lessons for China's CAINCA reform agenda. First, independent assistance offenses can coexist with strong mens rea protections if courts are institutionally empowered to resist prosecutorial pressure and apply rigorous contextual analysis. Second, the proportionality principle need not be sacrificed for enforcement efficacy: European jurisdictions have successfully prosecuted organized cybercrime assistance chains while maintaining high evidentiary standards by focusing investigative resources on high-culpability actors rather than peripheral facilitators. Third, the subsidiarity norm treating criminal law as a measure of last resort is operationalized in EU law through the requirement that member states first exhaust administrative, civil, and regulatory measures before invoking penal sanctions. This graduated enforcement model offers a template for China's coordination between the criminal justice system and the administrative regulation of fintech platforms, payment gateways, and cloud-service providers.

5.3. Implications for Emerging Technologies: Web3.0 and AI-Assisted Fraud

The challenges posed by CAINCA will intensify with the proliferation of decentralized technologies and AI-driven fraud. Blockchain-based platforms, decentralized finance (DeFi) protocols, and Web3.0 infrastructures further obscure assistance chains by distributing control across peer-to-peer networks and smart contracts. AI tools already enable automated phishing, deepfake impersonation, and adaptive social-engineering scripts at unprecedented scale. In such environments, infrastructure providers' wallet services, node operators, oracle providers, and AI developers risk being swept into liability under expansive assistance theories unless courts maintain strict limiting principles (Liu, 2023).

The doctrinal proposals advanced in this article, actual and specific knowledge, objective imputation for neutral services, and accomplice priority when upstream crimes are provable remain robust even under these conditions. Requiring concrete awareness of criminal purpose prevents the automatic criminalization of general-purpose tools. Objective imputation ensures that liability attaches only when a provider's specific conduct creates a disapproved risk that materializes in harm, rather than merely because the tool was later misused. Accomplice priority preserves proportionality by channeling high-culpability cases into upstream fraud offenses with commensurate penalties. These constraints are especially urgent in decentralized systems, where the absence of centralized control makes broad preventive liability particularly prone to overreach and chilling effects on legitimate

innovation (Liu, 2020). Zhang Mingkai's insistence on distinguishing "possible knowing" from actual knowledge provides a critical safeguard: mere foreseeability that a general-purpose technology might be misused cannot substitute for specific awareness of criminal application (Zhang, 2023). Jurisdictions confronting Web3.0 and AI fraud can therefore draw directly from China's experience: technological complexity does not justify doctrinal relaxation; it demands even stricter adherence to culpability and proportionality.

5.4. The Universal Value of China's Judicial-Restraint Model

China's CAINCA saga ultimately yields a transferable model for balancing security and justice in high-volume digital-crime environments. The combination of an independent assistance offense with subsequent judicial expansion followed by corrective signals from the highest judicial organs illustrates a dynamic that is increasingly common across legal systems. The proposed four-pillar framework, which includes restrictive knowledge, objective imputation, accomplice priority, and individualized proportionality, offers a concrete, doctrinally grounded pathway to reverse overcriminalization without sacrificing enforcement efficacy.

More importantly, the Chinese case reaffirms that judicial restraint is not a luxury of low-crime societies but an essential safeguard in high-pressure digital contexts. When legislatures and prosecutors face overwhelming caseloads and public demands for results, courts remain the last institutional bulwark against the normalization of overbroad liability. By insisting on actual culpability, objective risk creation, and proportionate punishment, jurisdictions can disrupt criminal networks while preserving the moral legitimacy of criminal law. The path forward, therefore, lies not in more expansive criminalization but in more principled governance, a lesson that transcends national boundaries and technological generations.

6. Conclusions

The rapid evolution of cybercrime governance in China, epitomized by CAINCA, illustrates both the necessity and the peril of preventive criminalization in the digital age. Enacted in 2015 to address genuine enforcement gaps in anonymized, transnational fraud networks, CAINCA represented a legitimate legislative innovation. Yet the subsequent Duanka campaign and judicial expansion transformed it into a high-volume, low-threshold instrument that increasingly punishes peripheral facilitators, often economically vulnerable individuals, with disproportionate severity. The three-fold pattern of over-expansion, generalization of subjective knowledge, broadening of assisted objects, and mechanical application of "serious circumstances" has eroded the offense's culpability foundation and

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

undermined the principle that criminal law should remain a last resort (Liu, 2023; Wu, 2025).

This trajectory is neither inevitable nor irreversible. The 2025 Joint Opinion, together with its typical cases, signals an emerging institutional willingness to correct course. The normative reconstruction proposed in this article, restricting mens rea to actual and specific awareness, applying objective imputation to neutral technical assistance, prioritizing accomplice liability when upstream crimes are provable, and enforcing individualized proportionality in sentencing, offers a doctrinally coherent pathway to restore balance. These four pillars are not radical departures but faithful applications of existing criminal law principles: culpability, subsidiarity, proportionality, and minimal intervention (Husak, 2017, 2023; Zhang, 2023). Their implementation requires sustained judicial discipline rather than new legislation.

Institutional reforms are equally indispensable. Prosecutorial and judicial performance metrics must be decoupled from conviction volume to eliminate incentives for mechanical application. Mandatory pre-charge knowledge assessments should become standard practice, treating permissive presumptions as exceptional rather than routine. Legal aid for economically disadvantaged defendants, rural migrants, debt-burdened youth, and students must be strengthened to counteract structural biases. Seamless coordination between criminal and administrative measures, occupational prohibitions, regulatory warnings, and civil recovery can achieve effective disruption without over-reliance on penal sanctions (Du et al., 2025).

Looking forward, the challenges will only intensify. The proliferation of decentralized technologies, blockchain, DeFi, and Web3.0 platforms, and AI-assisted fraud will further obscure assistance chains, multiply general-purpose infrastructure, and heighten pressure for broad preventive liability. Yet technological complexity does not justify doctrinal relaxation; it demands stricter adherence to culpability and proportionality (Liu, 2020, 2023). The lesson from CAINCA is clear: criminal law can disrupt criminal networks without sacrificing its moral legitimacy, but only if courts maintain principled restraint rather than succumbing to enforcement convenience.

Ultimately, the overcriminalization of digital assistance is not merely a technical or jurisdictional problem; it is a normative one. When ordinary people are swept into the penal net because they provided routine services or fell into economic desperation, criminal law risks losing its claim to justice. As global cybercrime enforcement continues to grapple with similar dilemmas of scale and anonymity,

China's experience, including its tentative steps toward restraint, underscores a universal truth: effective governance requires more principled discipline, not more expansive punishment (Brenner, 2012). Restoring restraint is therefore not only a matter of doctrinal precision but of preserving the last line of protection for individuals in an increasingly surveilled and algorithmically mediated society.

The principal strengths of this research lie in its integration of global overcriminalization theory with Chinese doctrinal analysis and empirical case study, as well as in its construction of a practical four-pillar framework of judicial restraint. Its primary limitation is the reliance on a purposive selection of three cases from the People's Court Case Database, which, while representative, does not constitute a large-N empirical analysis. Future research should complement this approach with quantitative studies of sentencing patterns across regions and defendant groups. A further limitation is the relatively limited engagement with comparative enforcement practice, as the comparative analysis remains primarily doctrinal.

In terms of applicability, the CAINCA framework provides useful lessons for other emerging and middle-income economies facing similar challenges, including high-volume digital fraud, limited capacity to prosecute transnational principals, and strong enforcement pressures. Countries in Southeast Asia, Latin America, and Sub-Saharan Africa that are constructing or revising cybercrime assistance offenses may draw from both the design flaws and corrective innovations of the Chinese model. The proposed four-pillar framework is adaptable across legal systems, provided that proportionality constraints are embedded within local institutional structures through constitutional review, supreme court guidance, or prosecutorial policy.

For the legal community, the practical impact of this research is threefold. Judges and prosecutors in Chinese courts may draw upon the four-pillar framework as an operational reference for distinguishing culpable facilitation from neutral technical assistance, reducing the risk of wrongful conviction and bolstering the legitimacy of CAINCA adjudication. Defense lawyers may use the objective imputation criteria and mens rea analysis to construct more principled arguments on behalf of peripheral defendants, particularly those recruited through economic coercion. At the policy level, the research supports the Supreme People's Court's corrective agenda under the 2025 Joint Opinion and provides doctrinal scaffolding for future judicial interpretations or legislative amendments aimed at consolidating restraint-based enforcement as the normative standard across China's high-volume digital crime environment.

Journal of Legal Studies Volume 37 Issue 51/2026
ISSN 2457-9017; Online ISSN 2392-7054.
Web: publicatii.uvvg.ro/index.php/jls. Pages 121 – 143

Acknowledgments
The author thanks the anonymous reviewers and the editor for their valuable contributions.

Funding
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author Contributions
R.L. conceived the study and was responsible for the design and development of the research framework, data collection from the People's Court Case Database, doctrinal analysis, literature review, and writing of the original draft, as well as review and editing of all revisions.

Disclosure Statement
The author has no competing financial, professional, or personal interests from other parties.

References
1. Beijing Shunyi District People's Court. (2023). Wang Mousheng et al. Case (Case No. 2023-03-1-257-001). People's Court Case Database.
2. Beijing Shunyi District People's Court. (2023). Zhang Mou et al. Case (Case No. 2023-04-1-257-001). People's Court Case Database.
3. Brenner, S. W. (2012). Cybercrime and the law: Challenges, issues, and outcomes. UPNE.
4. Chen, H. B. (2008). On neutral assistance behavior. Peking University Law Journal, 20(6), 931–957.
5. Chen, H. B. (2022). Correcting the "pocket crime" tendency of the crime of assisting information network criminal activities. Journal of Hunan University (Social Sciences), 36(2), 127–135. https://doi.org/10.16339/j.cnki.hdxbskb.2022.02.017
6. Clough, J. (2012). The Council of Europe Convention on Cybercrime: Defining "crime" in a digital world. Criminal Law Forum, 23(4), 363–392.
7. Du, X. Y., Hou, R. Y., & Yang, L. (2025). Understanding and application of the opinions on handling criminal cases involving assisting information network criminal activities issued by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security. People's Procuratorate, (20), 30–36.
8. Garland, D. (2001). The culture of control: Crime and social order in contemporary society. Oxford University Press.

9. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20.
10. Husak, D. (2017). Overcriminalization. In E. Luna (Ed.), Reforming criminal justice: Volume 1 – Criminalization (pp. 25–42). Arizona State University Academy for Justice. https://law.asu.edu/sites/g/files/litvpz156/files/pdf/academy_for_justice/3_Reforming-Criminal-Justice_Vol_1-Overcriminalization.
11. Husak, D. (2023). Six questions about overcriminalization. Annual Review of Criminology, 6(1), 265–284.
12. Jakobs, G. (2004). Imputation in criminal law and the conditions for norm validity. Buffalo Criminal Law Review, 7(2), 491–512.
13. Jiang, S. (2020). The interpretive directions for the crime of assisting information network criminal activities. Chinese Journal of Criminal Law, (5), 76–93. https://doi.org/10.19430/j.cnki.3891.2020.05.005
14. Li, H. (2017). On the nature and application of the crime of assisting information network criminal activities. Application of Law, (21), 33–39.
15. Liu, Y. H. (2020). Intergenerational characteristics of cybercrime in the Web3.0 era and criminal law responses. Global Law Review, 42(5), 100–116.
16. Liu, Y. H. (2023). The trend of judicial expansion and substantive restriction of the crime of assisting information network criminal activities. Chinese Journal of Law Review, (3), 58–72.
17. Luna, E. (2004). The overcriminalization phenomenon. American University Law Review, 54, 703.
18. Shanxi Province Xiaoyi City People's Court. (2024). Yang Moulei Case [(2024) Jin 1181 Xing Chu No. 73] (Case No. 2024-04-1-257-001, Apr. 19, 2024). People's Court Case Database.
19. Supreme People's Court Criminal Adjudication Third Division Research Group. (2025). Structural forms and judicial handling of the crime of assisting information network criminal activities. Digital Rule of Law, (1), 66–74.
20. Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. Information, Communication & Society, 11(6), 861–884. https://doi.org/10.1080/13691180802007788
21. Wu, H. Q. (2025). Normative review and correction of the rules for determining "knowledge" in the crime of assisting information network criminal activities. Forum on Law, 40(2), 17–27.
22. Yu, H. S. (2019). Judicial application of emerging cybercrimes. Chinese Journal of Applied Jurisprudence, (6), 150–165.
23. Yu, Z. G. (2017). Legislative exploration and theoretical clarification of the principalization of accomplice conduct: From the perspective of the legislative positioning of the crime of assisting information network criminal activities. Science of Law (Journal of Northwest University of Political Science and Law), 35(3), 83–92. https://doi.org/10.16290/j.cnki.1674-5205.2017.03.008

24. Zhang, M. K. (2016). On the crime of assisting information network criminal activities. Political Science and Law, (2), 2–16. https://doi.org/10.15984/j.cnki.1005-9512.2016.02.001
25. Zhang, M. K. (2023). "Knowledge" in criminal intent. Journal of Shanghai University of Political Science and Law (Rule of Law Forum), 38(1), 38–54. https://doi.org/10.19916/j.cnki.cn31-2011/d.20230104.008.