Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.34421

Criminal Regulation of Online 'Doxing' Conduct: Practical Dilemmas and Paths for Improvement

Chengkai Li[1*], Ziqi Zhuang[2]

[1]*School of Economics and Management, Tianjin University of Science and Technology, Tianjin, China*
[2]*School of Criminal Law, East China University of Political Science and Law, Shanghai, China*
**Corresponding Author. Email: chengkaili943@gmail.com*

Abstract. With the rapid development of the internet and social media, online 'doxing' has evolved into a composite cybercrime that integrates human-flesh search, unlawful data scraping, trafficking in private data, and sustained cyber violence, displaying technical, organized, and industrialized features. It seriously infringes on citizens' rights to personal information and privacy, undermines online public order, and may even trigger extreme incidents. At present, criminal-law regulation of online doxing faces practical difficulties such as challenges in determining overlapping offenses, blurred boundaries of platform responsibility, and weak administrative–criminal enforcement coordination. This article clarifies the legal attributes of online doxing and the types of offenses involved, analyzes core difficulties in criminal regulation, and proposes targeted paths for improvement, from the dimensions of criminal-law application, platform liability, and the administrative–criminal interface. It aims to provide a theoretical reference for accurately punishing doxing-related crime, improving whole-chain governance, and fostering a clean, orderly cyberspace governance system.

Keywords: Online doxing, composite cybercrime, criminal regulation, judicial determination, cyberspace governance.

1. Introduction

With the in-depth penetration of the internet and social media, cyberspace has become a key area of social life and public governance. Meanwhile, new types of cyber illegality and crimes represented by 'online doxing' have continued to spread. Doxing has evolved from early individual human-flesh search into a chained, organized, industrialized illicit gray–black industry that amalgamates unlawful acquisition, data scraping, trafficking in privacy, and cyber violence, featuring technological enablement, clear division of labor, and cross-platform diffusion [1]. Doxing centers on unlawfully disclosing sensitive information such as citizens' names, addresses, contact details, and movement trajectories, often accompanied by secondary harms such as insult, defamation, harassment, and extortion, severely infringing personal information and privacy rights and readily causing moral injuries, threats to personal safety, and even extreme incidents, posing a hazardous challenge to online public order and social stability.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.34421

At present, China's criminal legislation and judicial practice have continuously strengthened cybercrime governance and have successively issued normative documents on personal information protection and punishment of cyber violence. However, criminal regulation of the composite conduct of online doxing still shows obvious shortcomings. In judicial practice, problems stand out—such as inconsistent identification when offenses overlap, overly broad definitions of sensitive information, and non-unified sentencing standards; platform responsibility boundaries are fuzzy, with the phenomenon of invoking 'technological neutrality' to evade supervision widespreading, and ex ante prevention and ex post response mechanisms are absent; administrative–criminal coordination is poor, with delayed transfer of clues, inconsistent evidentiary standards, and jurisdictional conflicts, causing some cases to be 'punished only administratively instead of criminally' or resulting in unbalanced sanctions, making it difficult to build full-chain enforcement synergy. Existing research has mostly focused on a single offense or institution, lacking systematic sorting of the composite attributes, chain structure, and regulatory logic of online doxing, and thus struggles to meet the practical needs of precise justice and effective governance.

Accordingly, this article, building on criminal norms and judicial practice, defines the legal attributes of online doxing and the types of offenses involved, analyzes core difficulties in applying offenses, platform liability, and the administrative–criminal interface, and proposes improvement paths from such aspects as unifying judicial standards, tightening platform duties, and improving collaborative mechanisms, in the hope of furnishing theoretical references and institutional suggestions for judicial organs to accurately punish doxing-related crime and build a clean and orderly cyberspace.

2. Legal character of online doxing, types of involved offenses, and judicial status quo

2.1. Composite legal character of online doxing

Online doxing exhibits composite, chained, and industrialized features, and judicial practice commonly generates overlapping offenses with criminal-law application often involving concurrent offenses which mainly includes: unlawfully obtaining and publishing others' sensitive information may constitute the crime of infringing citizens' personal information; subsequent conducts that degrade personality or spread false information, where circumstances are serious and may violate the crimes of insult or defamation; sustained insult and harassment causing serious disruption of public order may be deemed the crime of picking quarrels and provoking trouble; relying on unlawful platforms to disseminate information may implicate the crime of unlawful use of information networks; downstream use of information to threaten, extort, or swindle property may respectively constitute extortion or fraud [2].

From the perspective of constitutive elements, subjects include individuals, groups, and corporate-style operators; objects include citizens' rights to personal information and privacy, while online public order is also disturbed; subjective intent is direct in all cases, with motives commonly including profit-seeking, revenge, venting, and traffic-chasing; objectively, conduct covers the full chain of information acquisition, processing, publication, dissemination, and subsequent cyber violence, featuring composite and continuing infringement and posing multiple threats to citizens' rights and social order.

DOI: 10.54254/2753-7048/2026.34421

2.2. Principal criminal offenses involved in online doxing

The composite nature of doxing dictates that offense application must synthesize the stage of conduct, legal interests infringed, and degree of harm. The crime of infringing on citizens' personal information is central, governing the core phase of unlawfully obtaining and spreading citizens' sensitive information [3]. Where, after disclosure, individuals insult others or fabricate facts harming reputation and the circumstances are serious, the conduct respectively constitutes the crimes of insult or defamation (private prosecution offenses, except where serious harm is done to social order or national interests). Where doxing is used to launch online sieges and disrupt online order, the crime of picking up quarrels and provoking trouble may apply.

Providing information publication or technical support for doxing, where circumstances are serious, constitutes the crime of unlawful use of information networks. Using leaked information to extort property constitutes extortion; using fabricated facts to swindle property constitutes fraud. Where network platforms refuse to fulfill security management duties and this causes large-scale leakage of information, they may be liable for the crime of refusing to fulfill obligations of network information security management.

2.3. Constitutive features of online doxing offenses

The constitutive elements of doxing offenses display composite, chained, and continuing infringement, going beyond the scope of a single cybercrime. The subject is the general subject (persons aged 16 and above); units may also be held criminally liable, and there is a trend toward organization and industrialization.

Subjective elements are uniformly direct intent: actors know their conduct will infringe citizens' rights and disrupt order yet actively proceed, with motives including profit, revenge, venting, and traffic-chasing; negligent leakage of information does not constitute such offenses.

Objective elements manifest as chained, continuous conducts along the full chain: early-stage unlawful acquisition and processing of information, mid-stage publication and dissemination, and late-stage insult, defamation, and extortion. Conducts are highly diffusive and persistent; once information is published, it spreads rapidly and remains accessible for a long time, superimposing and magnifying harmful consequences, causing multiple harm to victims and continuously undermining online and social order. The infringed legal interests are layered, and social harmfulness is markedly higher than in ordinary cybercrime.

2.4. Overall trends in criminal cases related to online doxing

As 'doxing' conduct has increased, related criminal cases have trended upward; some cases are handled as civil disputes or administrative violations, and the aggregate volume remains generally controllable. At present, 'online doxing' has formed a clearly divided illicit gray–black industry chain, and judicial crackdown intensity continues to increase [4]. In 2025, procuratorial organs nationwide prosecuted more than 6,000 people for online doxing and related cybercrime [5]. Courts typically select the principal offense based on information type, dissemination scope, and severity of consequences, treating other offenses as sentencing circumstances; for multi-stage, multi-subject situations, they mostly apply the rule of the heavier penalty among concurrent offenses, with relatively few cases of cumulative punishment for multiple crimes.

The basis for applying the heavier penalty among concurrent offenses lies in the strong linkage among stages of online doxing, which belongs to an integrated criminal process and fits the profile

DOI: 10.54254/2753-7048/2026.34421

of connected offenses; only where multiple acts are mutually independent, infringe different legal interests, and each meets the threshold for criminal liability should multiple crimes be punished concurrently in accordance with law.

Sentencing focuses on: the quantity, type, and sensitivity of personal information unlawfully obtained and disclosed; the scope of dissemination, clicks, and shares; consequences such as psychological harm to victims and threats to personal safety; whether the actor sought profit or repeatedly offended; and mitigating circumstances such as voluntary surrender, meritorious service, and negotiated guilty pleas. After the 2023 joint Guiding Opinion on Punishing Cyber Violence in accordance with law took effect, characterization of conduct linking online doxing with cyber violence became clearer, and standards for applying offenses were further normalized [6, 7].

3. Practical dilemmas in criminal regulation of online doxing

3.1. Difficulty determining overlapping offenses and unifying adjudication standards

Online doxing spans personal and public legal interests; conduct is continuous and connected, making it hard for traditional single-offense evaluation to cover the full chain. Whether combined conduct of information disclosure and cyber violence constitutes connected offenses or multiple crimes differs among courts. Whether cyber violence should be punished under the crime of picking quarrels and provoking trouble is unsettled because 'serious disruption of public order' is vague, and some courts distinguish cyberspace from real-world order, leading to a low application rate for that offense, insufficient evaluation of harm to online order, and inadequate criminal regulation.

Judicial practice shows a tendency toward over-broad identification of sensitive personal information in the crime of infringing citizens' personal information [8]. Some courts directly treat general information such as lodging records or delivery addresses as highly sensitive movement-trajectory information and even bring lawfully public information within the scope of criminal protection [9]. Unduly expanding the scope of punishment contravenes the original intent of typified protection and also complicates identification of overlapping offenses, affecting judicial fairness and the deterrent force of sanctions.

3.2. Vague platform responsibility boundaries make supervision and accountability difficult to implement

Network platforms are key carriers of information dissemination and an important link in curbing doxing, yet current laws and regulations leave platform duties and liability boundaries ambiguous, causing regulatory gaps and enforcement difficulties. Specific obligations and time limits for ex ante review, in-process handling, and ex post tracing are unclear; response deadlines and operational standards are missing, delaying identification and handling of doxing-related information. Some platforms invoke technological neutrality and 'safe harbor' defenses and fail to delete, block, or disconnect links in time, allowing harm to expand.

Against the background of the digital economy, criminal regulation of platforms tends toward heavy-handed and over-criminalizing approaches [10]. Simple punishment has failed to curb crime and instead traps platforms in passive rectification without incentives for active prevention. Establishing platforms' subjective knowledge is difficult; the threshold of 'serious circumstances' in the crime of refusing to fulfill network security management obligations is unspecific, and most cases end in administrative sanctions, making criminal liability hard to pursue. At the same time, platform compliance mechanisms are formalistic, ill-equipped to address the ubiquity, concealment,

DOI: 10.54254/2753-7048/2026.34421

and technicality of information risks, and unable to prevent leakage and dissemination of doxing-related information effectively.

3.3. Weaker administrative–criminal interface and insufficient law-enforcement and judicial coordination

Regulating online doxing involves cyberspace administration, public security, procuratorial, and judicial organs; effective administrative–criminal linkage is key to crackdowns, yet the current mechanism shows obvious loopholes and even dilemmas of 'reverse' administrative–criminal interface [11]. Delayed transfer of clues and information barriers are prominent: regulatory clues from cyberspace departments are not transferred completely and promptly to public security, which struggles to obtain full supervisory data and platform information, and some cases cannot be filed due to lost clues. There is no unified clue intake platform across departments, procuratorial recommendations lack rigidity, and inertia in administrative enforcement is hard to correct effectively.

The line between administrative illegality and criminal offenses is unclear and standards are indeterminate; a large number of cases that should incur criminal liability are handled only with fines or administrative detention, and 'administration instead of criminal punishment' is common; some decriminalized cases show reversed severity between administrative and criminal sanctions—for example, administrative fines for aiding conduct far exceed criminal penalties—contravening the principle of proportionality between crime, liability, and punishment. Cross-regional doxing conduct causes administrative–criminal jurisdictional conflicts; inconsistent delineation of the place of crime and the place of illegal conduct easily creates jurisdictional gaps and impairs enforcement and judicial efficiency.

4. Paths for improving criminal regulation of online doxing

4.1. Clarifying standards for criminal-law application and unifying rules of adjudication

To address overlapping offenses and non-unified adjudication, application rules should be standardized, with unified judicial scales. And a criminal evaluation system suited to composite features should be constructed to achieve accurate conviction and sentencing. Legislative and judicial organs should issue specialized judicial interpretations and guiding cases, refine boundaries for applying offenses, strictly delimit standards for sensitive personal information, and reject over-generalized evaluation. They should clarify quantified elements for 'serious disruption of public order' in picking quarrels online and 'serious circumstances' in insult and defamation, furnishing clear guidance for adjudication.

Establish the crime of infringing citizens' personal information as the core. For subsequent conduct, distinguish connected offenses from concurrent multiple crimes: where a connected relationship with the core phase exists, apply the heavier penalty among concurrent offenses; where new legal interests are independently infringed and thresholds for criminal liability are met, applying cumulative punishment in accordance with law, reducing identification disputes. Unify sentencing standards by building a quantitative system that incorporates information volume, sensitivity, dissemination scope, harm to victims, subjective malignancy, and statutory circumstances, avoiding disparate outcomes in similar cases. Strictly implement the Guiding Opinion on punishing cyber violence, clarify rules linking doxing with cyber violence, bring online sieges and sustained harassment within the regulatory framework, and realize full-chain evaluation.

DOI: 10.54254/2753-7048/2026.34421

4.2. Refining platform legal liability and building compliance incentives

As one of the governance subjects in cyberspace, network service platforms must bear primary responsibility for curbing online doxing. Legislation and regulations should refine platforms' legal obligations and liability boundaries while abandoning over-criminalizing thinking and constructing compliance incentives. Through legislative amendment or departmental rules, specify concrete obligations and response time limits for discovering, blocking, and deleting doxing-related information. Platforms should build mechanisms for routine patrols, keyword detection, one-click reporting, and rapid takedown, use data technologies proactively to detect and identify channels for illicit trading of personal information, treat content that publishes others' personal information as presumptively infringing and withhold display, and, upon discovering violations, timely fulfill reporting duties and preserve evidence.

Clarify dual compliance duties: ex ante risk assessment, in-process security safeguards, and ex post emergency response as front-end obligations; employee management and leakage prevention as criminal compliance duties, with designated responsible persons and regular training. Incorporate compliance performance into assessment, establish specialized compliance-based non-culpability models, and for platforms that improve personal information protection systems and perform duties effectively, find absence of criminal unlawfulness, promoting a shift from 'passive rectification' to 'active prevention' [12, 13]. Strengthen application of the crime of refusing to fulfill network security management obligations, clarify 'serious circumstances', and pursue liability in law against platforms that still fail to act after orders to rectify.

4.3. Improving the administrative–criminal interface and resolving reverse-interface dilemmas

To overcome poor administrative–criminal linkage, build normalized, institutionalized collaboration among cyberspace, public security, procuratorial, and judicial organs, and target jurisdiction, evidence, and supervision difficulties in reverse administrative–criminal interface, achieving a seamless connection between administrative regulation and criminal sanction.

First, cyberspace departments should build a unified clue acceptance platform for administrative–criminal linkage, integrating supervisory data from cyberspace organs, user data from platforms, investigative data from public security, and prosecution data from procuratorial organs, enabling real-time clue circulation and information interconnection, overcoming information barriers and difficulties in serving procuratorial recommendations, and ensuring that illegal clues discovered by cyberspace departments are promptly transferred to administrative enforcement or judicial organs with corresponding jurisdiction.

Second, clarify the boundary and transfer standards between administrative illegality and criminal offenses for online doxing, detail legal liability for different circumstances and harmful consequences, and standardize administrative–criminal jurisdiction. The Administrative Penalty Law should expressly provide that, in cybercrime cases, administrative enforcement organs at both the place where the criminal conduct occurs and the place where criminal results occur have jurisdiction, avoiding jurisdictional gaps. In addition, establish a model prioritizing administrative evidence collection with criminal evidentiary linkage, compel administrative organs to fix doxing-related evidence timely and efficiently, and resolve legality issues in applying criminal evidence in administrative proceedings. At the same time, strengthen necessity review in reverse administrative–criminal interface, prevent 'excessive punishment for minor wrongs', avoid reversing the severity of administrative penalties and criminal punishments, and, for actors exempted from criminal

DOI: 10.54254/2753-7048/2026.34421

punishment, reasonably determine the scope of administrative penalties according to the circumstances of conduct to ensure correspondence among crime, liability, and punishment.

Finally, strengthen procuratorial legal supervision: where administrative organs are remiss in performing duties, urge correction in accordance with law and issue circulars to enhance the binding force of procuratorial recommendations.

5. Conclusion

As a technical, organized, and industrialized composite cybercrime, online doxing, through full-chain conduct and layered infringement of legal interests, poses a severe challenge to traditional criminal rules. At present, criminal regulation of such conduct in China faces practical dilemmas—disagreement in identifying overlapping offenses, vague platform responsibility boundaries, and an ineffective administrative–criminal interface—reflecting the limits of a single-track criminal sanction model.

Therefore, systemic governance responses are necessary: at the judicial level, specialized interpretations should unify adjudication scales and establish offense-application rules centered on the crime of infringing citizens' personal information while accounting for connected relationships; at the platform governance level, statutory platform duties should be refined, specialized compliance incentives constructed, 'technological neutrality' defenses dismantled, and platforms shifted from passive rectification to active prevention; at the enforcement-coordination level, a unified administrative–criminal clue platform should be built, jurisdiction and transfer standards clarified to resolve reverse-interface dilemmas.

In sum, building the rule of law in cyberspace is a systemic project. Effective regulation of online doxing requires not only refinement of criminal norms and unified application rules, but also moving beyond a singular punitive thinking to construct a pluralistic, collaborative governance system that deeply integrates criminal sanctions, administrative regulation, platform performance of duties, and social prevention, thereby safeguarding citizens' rights and maintaining a clean, orderly cyberspace.

Authors contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

[1] China Internet Network Information Center (2023) The 52nd Statistical Report on China's Internet Development.
[2] Zhang, X. (2021) Understanding and Application of the Personal Information Protection Law. Renmin University of China Press, Beijing.
[3] Yu, Z. (2020) Criminal Law Responses to Cybercrime and Paths of Regulation. China Legal Publishing House, Beijing.
[4] Pi, Y. (2022) Criminal Law Protection of Public Order in Cyberspace. China Legal Science, (03), 146-164.
[5] Liu, Y. (2021) Criminal Law Identification and Regulation of Composite Cybercrime. Chinese Journal of Law, (05), 110-126.
[6] Wang, L. (2023) On Civil-Law Regulation of Cyber Violence. China Legal Science, (02), 5-22.
[7] Yang, N. (2025) Distortion and Correction in Applying the Crime of Infringing Citizens' Personal Information in the Field of Digital Intelligent Governance. ECUPL Journal, (06), 35-48.
[8] Gong, W. (2024) Platforms' Compliance Duties in Processing Personal Information and Paths to Non-Culpability. ECUPL Journal, (02), 51-65.
[9] Hebei Provincial People's Procuratorate (2026) Concrete Application of Reverse Administrative–Criminal Interface in Cyber Information Network Crime Cases. Procuratorial Theory Research, (02), 45-52.

DOI: 10.54254/2753-7048/2026.34421

[10] Chen, R. (2023) Specialized Compliance Plans in Corporate Compliance Rectification. Tribune of Political Science and Law, (01), 1-16.
[11] Liu, Y. (2023) Legislative Research on Compliance Incentives in Substantive Criminal Law. Law Science, (01), 78-92.
[12] Han, X. (2023) Annual Report on Data Governance Observations (2022). Digital Law Review, (01), 201-230.
[13] Lei, L. (2020) On Identifying Movement-Trajectory Information in the Crime of Infringing Citizens' Personal Information. China's Procuratorate, (01), 6-10.