Proceeding of ICGPSH 2025 Symposium: The Globalization of Connection: Language, Supply Chain, Tariff, and Trade Wars
DOI: 10.54254/2753-7048/2025.LD24844

# *On the Supervisory Responsibility of Online Platforms in the Governance of "Doxing"*

**Yinuo Zhang**

*School of Artificial Intelligence and Law, Southwest University of Political Science and Law, Chongqing, China*
*enochzyn@126.com*

***Abstract.*** In the 21st century, while the Internet has become an important platform for information exchange, it has also facilitated new forms of cyber violence. One such form is "doxing," which refers to the illegal acquisition and disclosure of an individual's private information online, often leading to cyberbullying or harassment. This behavior poses a great threat to personal privacy and safety, causes serious psychological pressure, and results in social difficulties for victims. Furthermore, it undermines social harmony and creates widespread negative impacts. In response, the Office of the Central Cyberspace Affairs Commission has launched a campaign titled "Clear-Network Hostility Remediation" to curb such misconduct. However, the governance of "doxing" is a long-term endeavor that requires collaboration across society. As central hubs for information dissemination, online platforms bear a critical responsibility in creating a clear network environment. They should proactively implement supervisory measures, prevent and address doxing-related cyber violence, and ensure the protection of users' lawful rights and interests, thereby upholding order and stability in cyberspace.

***Keywords:*** Governance of online violence, Doxing, Human flesh search, Online platform supervisory responsibility

## 1. Introduction

With the growing integration of the Internet into daily life, the risk of personal privacy breaches has significantly increased. Criminals exploit online platforms to violate individuals' privacy and personal safety, as seen in the 2023 cyber incident involving large-scale doxing against Bilibili content creators [1]. This behavior goes beyond traditional doxing and refers to the illegal collection and exposure of personal information online, followed by targeted attacks and stigmatization by netizens [2]. Such acts not only infringe upon privacy and personal information rights but also often escalate into online group violence and even offline intimidation, posing serious threats to social order. Since the widely publicized Jiang Yan case in 2008, the legal regulation of cyberviolence has received great attention. However, the existing legal framework struggles to keep pace with rapid technological changes and evolving online behaviors. In particular, there are notable challenges in defining individual responsibility, clarifying the responsibility of network platforms, and determining applicable legal norms [3].

© 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: 10.54254/2753-7048/2025.LD24844

This study takes the doxing phenomenon as an entry point to examine privacy violations under cyberviolence. It explores the legal responsibilities involved, including civil, criminal, and administrative aspects. In addition to analyzing the accountability of the direct perpetrators, the paper also addresses the legal implications for those who forward or amplify harmful content and the supervisory obligations of network platforms acting as digital "gatekeepers" [4].

## 2. Legal framework and responsibility challenges in the regulation of cyber violence

### 2.1. Current legal framework governing cyber violence

The complexity and rapid dissemination of doxing behavior make it difficult for traditional legal tools to provide timely and effective regulation. In response, China has initially constructed a relatively comprehensive legal system for cyber violence, encompassing the Personal Information Protection Law of the People's Republic of China, Criminal Law of the People's Republic of China, Civil Code of the People's Republic of China, Cybersecurity Law of the People's Republic of China, Administrative Measures for Internet Information Services, Law of the People's Republic of China on Penalties for Administration of Public Security, and Provisions on the Governance of Online Violence Information. Each of these laws plays a distinct role. The Civil Code—particularly its tort liability provisions—establishes compensation standards for infringements and outlines the obligations of both individual users and network service providers. The Criminal Law defines criminal liability for acts such as illegal collection and disclosure of personal information [5]. Meanwhile, the Cybersecurity Law and Provisions on the Governance of Online Violence Information emphasize the responsibility of network governance and the management of violent cyber information.

This framework achieves a degree of functional coordination, addressing the responsibilities of perpetrators, platforms, victims, and other parties. For example, the Civil Code and Criminal Law jointly deter malicious online behavior by providing both civil compensation mechanisms and strict criminal sanctions [6]. Provisions on the Governance of Online Violence Information, as a new category of cyber legislation, focuses on preventing and sanctioning illegal acts of cyberattacks and protecting the cybersecurity of individuals and organizations.

However, despite this progress, the framework still faces many challenges in the implementation of the new type of cyber violence, such as doxing and the articulation of legal responsibility.

### 2.2. Difficulties in respnsibility convergence in cyber violence governance

A key challenge in regulating cyber violence is the separation and coordination of legal responsibilities. The traditional "three-law" model—dividing civil, criminal, and administrative responsibilities—often fails to respond effectively to complex online behavior. In many cyber violence cases, the actions of perpetrators may simultaneously involve violations of privacy (criminal liability), defamation (civil liability), and dissemination of harmful content (administrative penalties). These overlapping legal domains make it difficult to determine the appropriate legal pathway and enforce accountability.

In addition, sentencing standards are uniform and regulated, and there are differences in judicial interpretations. The subjectivity of administrative authorities in administrative rulings has sometimes resulted in inconsistent enforcement standards, creating uncertainty for both plaintiffs and defendants. At the same time, the criminal law for cybercrime penalties for cybercrime and the

DOI: 10.54254/2753-7048/2025.LD24844

civil law on the network of injury compensation standards are inconsistent; the reconciliation and convergence of the two show obvious difficulties [7].

Another major issue lies in the unclear responsibility of online platforms. Existing laws provide limited and vague guidance on their legal obligations. Even in policy documents such as the Notice on the Special Action on Clearing Network Hostility, the roles and duties of platforms are not clearly defined. The psychological screening mechanism, technical monitoring capability, and emergency response mechanism of online platforms need to be further refined and clarified. Therefore, it is imperative to establish an efficient mechanism for the connection of responsibilities between civil, criminal, and administrative laws to rectify cyber violence, and at the same time, delineate the boundaries of responsibilities of cyber platforms according to their actual operational capabilities so as to provide solid legal protection for a clear environment in cyberspace.

## 3. Polarised approaches in the criminal-civil interface of cyber violence governance: positive civil law and negative criminal law

### 3.1. Positive civil law: Optimising civil liability and prosecution methods

In the increasingly complex online environment, it is particularly urgent to properly address the issue of civil liability for online violence such as doxing. Firstly, such behavior essentially infringes on an individual's right to privacy and reputation [6]. Although fact-based commentary falls under the protection of free speech, acts such as insults, defamation, and unauthorised disclosure of private information clearly cross legal boundaries and should be explicitly regulated [8]. To this end, a diversified civil liability system should be established. This includes obligations for perpetrators to delete infringing content, pay compensation, issue formal apologies, and undertake other remedial measures. Such a system ensures that victims of cyber violence can obtain necessary remedies.

In terms of enforcement, litigation procedures should be simplified and trial cycles shortened. Introducing small-claims or summary proceedings should be implemented in cases of cyberviolence so as to respond immediately to victims' claims and ensure that their legitimate rights and interests are not delayed. In addition, considering the trans-geographical nature of cyber-violence, remote court hearings using Internet technology should be explored in legal practice to overcome geographic limitations and improve the efficiency of judicial resource allocation. A specialized rapid response mechanism for online infringement should be further established, requiring online platforms to be able to block offending accounts and remove infringing content within a short period of time after receiving an infringement complaint, as well as collaborate with the judiciary to retain relevant evidence. On this basis, the establishment of a comprehensive lawyer assistance system to provide legal counselling and representation services for victims of cyberviolence reduces the cost of defending victims' rights and improves the efficiency of defending rights. At the same time, public interest legal service organisations are encouraged to participate actively in providing low-cost or even no-cost legal assistance to victims.

In short, optimizing the civil liability bearer and the prosecution method not only provides practical relief for the victims of cyber violence but also helps to build a clear and mutually supportive cyber environment and promote the process of a society based on the rule of law.

### 3.2. Negative criminal law: Limiting criminal liability for public order offences

Although certain acts of cyber violence, especially doxing, can be severe, criminal law should adopt a restrained approach to regulating cyber public order offenses. A passive legislative strategy

DOI: 10.54254/2753-7048/2025.LD24844

is more appropriate: reducing the scope of criminal liability can help alleviate pressure on the judicial system without excessively curtailing users' freedom of expression.

Currently, the number of cyberviolence cases prosecuted under criminal law is on the rise. However, inconsistent legal standards and vague offense classifications often result in inefficiencies and inconsistent sentencing. To address this, legislative bodies should refine the categorization of cybercrime to facilitate more precise application of criminal law. The scope of criminal liability must be clearly defined to avoid overly broad interpretations [9]. A tiered penalty system is also recommended. For less severe offences that disrupt public order, lighter penalties such as fines or probation should be imposed, with a focus on education and correction. In contrast, serious cybercrimes that significantly harm individuals or public interest should be met with stronger punitive measures. This differentiation ensures criminal law functions both as a deterrent and as a proportionate tool in maintaining cyber order.

Lawmakers and cybertechnology experts should work collaboratively to study patterns of cyber behavior, regularly assess the effectiveness of current legislation, and revise laws accordingly. As online behaviours evolve, the criminal definition of cyber public order offences should also be dynamically updated to reflect technological advancements and cultural shifts in cyberspace.

By adopting clear legal definitions, implementing a graded system of penalties, and maintaining adaptive legal frameworks, it is possible to uphold freedom of expression while ensuring effective regulation of cyber public order offenses. This dual approach strengthens legal protections, reduces the prevalence of cyber violence, and promotes a safe and orderly digital environment.

## 4. Administrative control first, criminal sanctions later: An integrated approach to cyber violence governance

In the face of rising incidents of cyber violence, relying solely on criminal justice is no longer sufficient. The "administrative control first, criminal sanction later" model has emerged as a more effective strategy, using administrative measures to contain harm early and laying the groundwork for subsequent criminal prosecution.

When administrative authorities detect cyber violence, they can act swiftly—issuing warnings, imposing fines, or restricting content publication—to curb the immediate spread of harm. These rapid responses prevent escalation and bridge the delay often associated with criminal procedures, reflecting a strong stance against online misconduct. Administrative actions also help pave the way for criminal accountability. The evidence gathered through these early interventions supports later investigations, enhancing efficiency and integrating legal resources. Moreover, for less severe offenses that do not meet the threshold for criminal charges, administrative penalties serve an educative and preventive function, aligning with corrective and preemptive legal principles. This model also compels online platforms to strengthen internal governance, improve content moderation systems, and protect user data—reducing their own legal risks and helping maintain a healthy online environment.

In summary, this integrated approach creates a seamless link between administrative and criminal enforcement, setting clear boundaries for online behavior. Going forward, refining this model requires legal clarity, defined responsibilities for all stakeholders, and the application of digital technologies to improve regulatory precision. With continuous improvement, this dual-track strategy holds significant potential for building a safer and more orderly cyberspace.

DOI: 10.54254/2753-7048/2025.LD24844

## 5. Perpetrators, reposters and platforms: Collaborative attribution of responsibility to multiple subjects

### 5.1. Direct perpetrators: Multi-level liability under civil, criminal and administrative law

In incidents of "doxing" and cyber violence, direct perpetrators who collect, disclose, or disseminate others' personal information bear legal responsibility on civil, criminal, and administrative levels. Civilly, perpetrators infringe upon victims' privacy and reputational rights, requiring them to compensate for economic and moral damages. Especially for persistent or large-scale violations, compensation should take on a punitive aspect to deter future misconduct. Criminal liability arises when actions violate laws related to personal information infringement, insult, or defamation. Depending on the severity, perpetrators may face detention or imprisonment, sending a clear signal of zero tolerance for cyber violence.

Administratively, those violating rules like the Cybersecurity Law may face fines, account bans, or restrictions. This triadic liability structure ensures a comprehensive response to the perpetrators' misconduct and enhances the credibility of law enforcement in cyberspace.

### 5.2. Reposters: Clarifying fault and responsibility with precision

In the internet age, reposting is a common behavior that may unintentionally or deliberately intensify online violence. Especially in the context of "doxing," the role of forwarders is pivotal. However, current Chinese legislation lacks clarity regarding the legal responsibilities of retweeters, which often allows malicious actors to escape sanctions. To regulate this behavior, it is essential to define when reposting constitutes infringement—whether it violates privacy, damages reputation, or amplifies misinformation. Key considerations include the subjective intention of the reposter, their role in the retweet chain, and their impact on the extent of harm. The aggregation of reposts often creates a group psychology effect, intensifying public shaming and thus increasing the harm to the victim.

On a technical level, platforms should deploy monitoring tools that trace retweet chains, identify original sources, and flag high-risk content. From a judicial perspective, reviewing precedent cases can help establish clearer standards for liability, though current practice remains fragmented and inconsistent. To address this gap, it is necessary to strengthen legal interpretations and enforcement, improve platform regulation mechanisms, and enhance public legal awareness. A multi-stakeholder governance model involving platforms, netizens, and authorities can contribute to building a rational and enforceable responsibility system for retweeters, balancing freedom of expression and protection of rights.

### 5.3. Platforms: Dual responsibility for technology and compliance

As a key node and "gatekeeper" of information dissemination, network platforms have unshirkable regulatory responsibilities. The roles and responsibilities of online platforms in the act of doxing are becoming more and more complicated, and it is necessary to fine-tune the configuration of their legal responsibilities. First of all, it should be clear that network platforms must bear the basic responsibility in the security management of private data. According to the latest network security regulations, network platforms need to establish a sound user information protection system, including but not limited to storage encryption, access control, and desensitization of sensitive information. On this basis, for private information uploaded by users,

DOI: 10.54254/2753-7048/2025.LD24844

online platforms should implement a strict content review mechanism to prevent illegal disclosure of private information.

Second, online platforms should actively adopt technical means to detect and intercept unlawful acts that contain private information. When the platform monitors potential doxing behaviors, it should take timely measures such as blocking and deletion and report them to the relevant departments to prevent the proliferation and escalation of infringement behaviors. At the same time, through algorithm optimisation, the visibility and dissemination efficiency of malicious content can be reduced so as to reduce its negative impact on the public [10].

Again, communication and cooperation with law enforcement agencies should be strengthened. Online platforms not only need to develop a strict internal monitoring system but should also build an information-sharing mechanism with government regulators so as to respond in a timely manner to adjustments in laws and regulations and law enforcement needs. When illegal behaviors such as doxing occur, platforms should provide the necessary technical support and data information in accordance with the law to assist in responding to and combating online violence.

Finally, penalties for violations of users' legitimate rights and interests should be increased. Network platforms should clearly define the code of conduct for users and impose penalties such as account suspension, function restriction, and permanent bans on users who violate it. By formulating strict user agreements and terms of service, the rights and obligations between online platforms and users should be clarified to effectively deter offenders and protect the legitimate rights and interests of Internet users.

While implementing the above measures, it is also necessary to refine the implementation program for the specific circumstances of different online platforms. Taking into account the characteristics and operation modes of different platforms, the configuration of legal liabilities should be designed in a targeted manner to ensure the maximisation of the regulatory effect and the compliance of platform operations. Through the reasonable allocation of legal responsibility, the triple goals of maintaining network order, protecting the legitimate rights and interests of citizens, and promoting the healthy development of cyberspace can be achieved.

## 6. Conclusion

Cyber violence, especially the phenomenon of doxing, poses a serious threat to personal privacy and mental well-being. The promulgation of the Regulations on the Control of Online Violence Information reflects the government’s active stance in combating such behavior. However, as digital technology evolves, regulatory mechanisms must also adapt. The effective governance of online violence requires a multi-level approach involving legal regulation, platform accountability, and enhanced public awareness. This study aims to analyze the existing legal regulatory framework of online violence, especially the phenomenon of doxing, and suggests how the system of "three laws" can work better and how to allocate responsibilities among online platforms, information disseminators, and various sectors of society. In terms of the interface between criminal and civil law, it was advocated that civil law should play a more active role in protecting citizens' personal information and their rights, while criminal law should maintain a prudent attitude in dealing with cybercrime. In addition, the study emphasizes the interface between administrative control and criminal sanctions, proposing the introduction of an administrative antecedent element in cyber-regulation, i.e., giving priority to administrative penalties and education before criminal intervention.

With regard to the distribution of responsibilities among perpetrators, reposters, and online platforms, the study points to the need for a coordinated approach to the issue, with the formation of

DOI: 10.54254/2753-7048/2025.LD24844

an online communication order governed by strict regulations by clarifying the legal responsibilities of retweeters and the legal obligations of online platforms in their role as "gatekeepers." This not only requires platforms to take responsibility for information censorship and user education but also requires all Internet users to work together to maintain harmony in cyberspace.

Ultimately, the study calls on the whole society to reflect on and improve the situation, strengthen legal regulation, social governance, and cultural guidance, and work together to build a clear, healthy, and well-ordered online environment. After all, the network is virtual, but the harm suffered by individuals is real. Every care and respect, every choice of reason and self-discipline, is a positive contribution to network civilization and the most basic goodwill for this era. We look forward to the strength of the law and the enhancement of the sense of responsibility of citizens, which can jointly promote the benign development of cyberspace so that the function of the network has been more fully and positively played.

## References

[1] Li, Ying. (2023). "Human flesh open box" violates online privacy, official document platforms act quickly. China Quality Miles, (12), 56-57.
[2] Penrose News . (2024-06-13). Worse than "human flesh search"! Spotlight on the new style of online violence "open box hanging people", retrieved from https://baijiahao. baidu. com/s?id=1801702488937980773
[3] Suzhiguga. (2023). Research on the legal regulation of online violence (Master's thesis, Hebei Normal University). Master's degree. https://link. cnki. net/doi/10. 27110/d. cnki. ghsfu. 2023. 000677doi:10. 27110/d. cnki. ghsfu. 2023. 000677.
[4] Yi, Qianliang. (2020). The role of online platforms as "online gatekeepers" in content governance. Young Journalist, (07), 24-26. doi:10. 15997/j. cnki. qnjz. 2020. 07. 008.
[5] QNJZ. (2020). Criminal Law of the People's Republic of China (Article 253). China Law Press.
[6] Ma Songjian. (2015). On the criminal regulation of malicious "human flesh search". Zhongzhou Journal, (07), 53-58.
[7] Li, Minamata-Ran. (2023). Research on the regulation of online violence crimes (Master's thesis, Nanjing University of Finance and Economics). Master's degree. https://link. cnki. net/doi/10. 27705/d. cnki. gnjcj. 2023. 000347doi:10. 27705/d. cnki. gnjcj. 2023. 000347.
[8] Yang, L. X. (2008). (2008). The key to solving the illegal behaviours in "human flesh search" lies in regulating network behaviours according to law. Information Network Security, (10), 7-9+25.
[9] Wang, T. L. . (2023). Research on China's cyber violence crimes and countermeasures (Master's thesis, People's Public Security University of China). Master https://link. cnki. net/doi/10. 27634/d. cnki. gzrgu. 2023. 000189doi:10. 27634/d. cnki. gzrgu. 2023. 000189.
[10] Zhang Linghan. (2021). The construction of algorithmic accountability of online platform regulation. Oriental Law, (03), 22-40. doi:10. 19404/j. cnki. dffx. 20210430. 009.