Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 15, No. 2, 2026

A Study on Countermeasures for Tackling Cyberbullying in the Digital Age

Wanxin Tang

Chengdu University of Arts and Sciences, Chengdu, Sichuan, China

Abstract: In the digital age, the phenomenon of cyberbullying poses a serious challenge to citizens' personal dignity and social order; its governance has thus become an urgent issue for the development of the rule of law and social governance. Based on an analysis of current legal provisions and judicial practice, this paper discusses the nature of the conflict between the two and the primary challenges in combating cyberbullying. To address these challenges, the paper proposes effective measures to curb cyberbullying through legislative and judicial channels. A multi-stakeholder governance system should be established, comprising government regulation, platform accountability, judicial safeguards and public participation, to maximise the protection of citizens' legitimate freedom of expression in cyberspace. In summary, the path to addressing online violence is not a static set of provisions, but rather a practical wisdom that seeks a dynamic balance in individual cases. Only by achieving multi-stakeholder collaborative governance within the framework of the rule of law can we curb the harm caused by online violence to individuals and society, whilst safeguarding an open and inclusive environment for expression.

Keywords: Cyberbullying; Freedom of Speech; Legal Provisions; Legal Framework.

1. Current Status of Cyberbullying Governance

According to the 57th Statistical Report on the Development of China's Internet, published on 5 February 2026, as of December 2025, China's internet user base had reached 1.125 billion, with an internet penetration rate of 80.1%, and the benefits of digital development have reached a wider audience.[1] The internet has permeated every aspect of social life; cyberspace has effectively become an extension of the real world, with its applications rapidly penetrating both the productive and domestic spheres. As the central arena for information exchange and public discourse in contemporary society, the internet not only serves as a vital platform for citizens to exercise their constitutionally guaranteed freedom of speech, but also, due to its anonymity, instantaneous dissemination and collective nature, has given rise to cyberbullying—a new form of social scourge. Consequently, the governance of cyberbullying has become an urgent priority for the development of the rule of law and social governance.

China's legal framework regarding cyberbullying is constantly being refined, with a systematic set of legal norms being established across multiple jurisdictions.From the 2023 'Guiding Opinions on Punishing Online Violence-Related Criminal Offences in Accordance with the Law' issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security—which defined the offence from the dual perspectives of conduct and consequences—to the 'Regulations on the Governance of Online Violence Information' implemented in 2024, which further defines online violence information as "illegal and harmful information disseminated via the internet in the form of text, images, audio or video, targeting an individual in a concentrated manner, and containing insults, abuse, rumours, defamation,incitement to hatred, intimidation and coercion, invasion of privacy, as well as accusations, ridicule, denigration and discrimination that affect physical and mental health".[2] The evolution of the definition of cyberbullying is not merely a simple iteration, but rather constitutes a progressive regulatory framework spanning from information content management to criminal sanctions. It presents a more precise categorisation of cyberbullying from a content perspective, providing more specific operational guidelines for platform identification and law enforcement determinations.At the same time, the governance principles explicitly state the need to "uphold prevention at source, combine prevention with control, address both symptoms and root causes, and promote collaborative governance", reflecting a shift in philosophy from outcome-oriented governance to holistic, process-oriented governance.

Although China has established a multi-tiered legal framework for the governance of online violence—spanning civil compensation, administrative penalties and criminal sanctions—there remains a significant gap between legal provisions and practical outcomes. From the 2022 case of Liu Xuezhou, who took his own life after being subjected to online abuse whilst searching for his family, to the 2023 death of Zheng Linghua, who passed away from depression following online harassment over her pink hair, and now Olympic champion Quan Hongchan's tearful plea for netizens to stop insulting her.In 2024 alone, public security authorities nationwide handled over 8,600 cases of cyberbullying, whilst new forms of online abuse, such as 'unboxing' videos, continue to emerge. All these incidents serve as repeated reminders that, in the digital realm, we must pay close attention to the boundary between criticism and harm when expressing views, and consider how the law should protect citizens' fundamental right to personal dignity whilst avoiding the stifling of public discourse.

2. The Dilemma of Governing Online Violence

The challenges in tackling cyberbullying reflect a conflict between the constitutionally guaranteed right to freedom of expression and the dignity of the individual. Essentially, this stems from the lag in legislation, which makes it difficult for

traditional legal norms to address new forms of verbal violence in the digital age. At the same time, as both providers and beneficiaries of online activities, platforms' profit-driven nature causes them to remain invisible in the process of tackling cyberbullying. When online discourse shifts from public debate to personal abuse, insults, rumour-mongering, defamation and doxxing, it has already crossed the reasonable boundaries of freedom of speech and descended into the abyss of cyberbullying.

(1) Unclear Legal Definitions

Among the many challenges in tackling cyberbullying, the ambiguity in characterising such behaviour is the most fundamental yet also the most intractable. This ambiguity concerns the very question of what constitutes cyberbullying, a fundamental issue that precedes any legal judgement.The emergence of this governance dilemma stems from two deep-seated contradictions: firstly, the vagueness of legal definitions, which leads to a tendency towards conceptual generalisation in academic discourse; and secondly, the existence of a boundary—one that is easily blurred yet must be clearly defined—between cyberbullying and the public oversight guaranteed by the Constitution.

The 'Regulations on the Governance of Online Violence Information' mentioned above provided the first legislative definition of online violence information in 2024. At the same time, the regulations stipulate that 'this provision shall not apply to cases where individuals report or expose others' illegal or criminal activities via the internet in accordance with the law, or where they exercise public opinion supervision in accordance with the law.' The Regulations describe the scope of online violent information in detail from two dimensions: positive enumeration and negative exclusion. However, in today's rapidly evolving online environment, a closed-ended, positive definition of online violent behaviour struggles to resolve the ever-evolving contradictions .[3] As the law struggles to keep pace with the demands of the times, some scholars have now taken the initiative to engage in discussions on cyberbullying, substituting moral criticism for legal judgement. Scholars' characterisation of behaviour in cyberbullying cases exhibits a tendency towards over-expansion, vagueness and one-sidedness; not only does this fail to provide the necessary theoretical support for the rule of law in cyberbullying governance, but it may also misguide policy direction and judicial practice in this area.

Well-intentioned acts such as public scrutiny are legally recognised as legitimate. Defining the boundary between public scrutiny and cyberbullying is key to effectively addressing cyberbullying and safeguarding citizens' personal dignity. Therefore, distinguishing between cyberbullying and public scrutiny primarily involves the following three aspects: the nature of the incident, the subjective motive, and the consequences of the behaviour.[4] In terms of the nature of the incident, the consequences of public oversight fall within the bounds of what is socially recognised or accepted; for example, an illegal act may be rectified as a result of public oversight. Cyberbullying, on the other hand, often causes harm to the individuals involved, such as the disclosure of private information or damage to personal dignity;In terms of subjective motive, public scrutiny aims to seek the truth, uphold justice and promote social improvement, and is characterised by rationality and public interest, whereas cyberbullying is often driven by motives such as venting anger, collective emotional release or malicious retaliation, and is distinctly aggressive and destructive;In terms of behavioural consequences, public scrutiny typically addresses matters of public interest or pressing social issues, centring on fact-based analysis and constructive discussion, whereas cyberbullying frequently deviates from public affairs to target the private lives or non-public spheres of specific individuals, launching unwarranted attacks or even fabricating false information to defame them.

(2) Difficulties in holding perpetrators accountable

Due to the lack of clarity in legal regulations, establishing a causal link between cyberbullying behaviour and the resulting harm has become a significant challenge. Cyberbullying constitutes a form of indirect violence, often involving sustained, collective attacks. It generates overwhelming harm by aggregating fragmented offensive content, causing victims to suffer emotional breakdowns within a very short timeframe.Unlike traditional physical violence, the harmful consequences of cyberbullying are dispersed, cumulative and indirect. On the surface, a single act of aggression by any individual participant may appear insufficient to cause significant direct harm to the victim; however, attributing severe consequences such as suicide or self-harm to a specific perpetrator of cyberbullying presents a major challenge in judicial practice.[5] Current legislation lacks clear standards of liability for new forms of harm such as indirect violence and cumulative damage, leaving judicial authorities without operational legal grounds when determining the causal relationship between specific acts of cyberbullying and extreme consequences such as the victim's suicide or self-harm. This ambiguity not only weakens the deterrent effect of the law on potential perpetrators but also makes it difficult for victims to obtain effective judicial redress, constituting a systemic bottleneck that urgently needs to be resolved in the governance of cyberbullying.

At the same time, the aforementioned predicament has led to a situation where the law fails to hold the masses accountable. That is, when harmful acts are carried out in a large-scale, unstructured group format, although the perpetrators have clearly crossed legal boundaries and even constituted a systematic infringement of citizens' legitimate rights and interests—such as personality rights and the right to reputation—the decentralised and non-standardised nature of their actions makes it difficult, within the current legal framework, to accurately identify the responsible parties and scientifically apportion liability. This ultimately results in a governance dilemma characterised by "the blurring of responsible parties—obstruction of accountability procedures—failed punitive outcomes".[6] At the judicial level, the principle of "the law does not punish the multitude" is one of the most perplexing aspects of identifying perpetrators of cyberbullying. Combined with the inherently collective and covert nature of cyberbullying, this effectively amounts to condoning such criminal behaviour.The sheer number of participants imposes enormous costs in evidence collection and procedural burdens on judicial authorities when holding each individual to account. More problematically, even if judicial authorities succeed in holding perpetrators accountable at great expense, the vast number of minor offenders makes it difficult to define their actions under criminal or civil law, thereby rendering the actual deterrent effect of punishment extremely limited.

(3) Platforms' evasion of responsibility

Online platforms play a crucial role in the governance of cyberbullying, and the issue of their accountability is directly linked to the actual effectiveness of cyberbullying prevention

and control. However, some platforms passively evade liability by invoking the safe harbour principle; others allow algorithmic recommendation mechanisms to amplify controversial content; and still others, in balancing interests, prioritise traffic revenue over governance investment.[7] Platforms face a dual dilemma when fulfilling their governance responsibilities. On the one hand, most platforms have weak content moderation mechanisms, making it difficult to identify increasingly complex and subtle offensive content; on the other hand, some platforms tend to prioritise traffic over governance, lacking the willingness to take proactive preventive measures due to economic incentives.

When platforms use algorithmic recommendation technology to actively intervene in or amplify online abuse, they transform from passive internet service providers into active disseminators of information.The basis for the application of the safe harbour principle is thereby lost, and platforms should assume a higher duty of care, or even joint liability, in accordance with the 'red flag' principle. Consequently, the current dilemma regarding platform liability does not lie in the safe harbour principle itself, but in how to prove whether a platform had actual or constructive knowledge. The criteria for determining actual or constructive knowledge are difficult to identify in the context of online abuse, which allows platforms to evade responsibility after such incidents occur.Secondly, driven by economic interests, platforms utilise algorithmic recommendation mechanisms to actively push controversial and emotionally charged content to a wider audience. Such sensationalised topics are more likely to attract attention and generate substantial traffic, which can be directly converted into financial gain.[8] Consequently, in the context of online abuse, whilst platforms, as governing entities, must bear social responsibility, their commercial nature simultaneously makes them beneficiaries of such incidents.

3. Measures to Tackle Online Violence

Faced with multiple challenges in the governance of cyberbullying—including unclear legal definitions of such behaviour, difficulties in holding perpetrators accountable in practice, and platforms shirking responsibility —the question of how to effectively combat cyberbullying whilst avoiding undue suppression of freedom of expression has become a core issue that the rule of law must address.Guided by the principle of proportionality, this paper will explore a legal framework for the coordinated governance of cyberbullying and freedom of speech by examining four key areas: refining definitions, strengthening practical implementation, platform accountability, and systemic governance.

(1) Refining Ambiguous Definitions

The standardisation and rule of law in the governance of cyberbullying first and foremost depend on improvements at the legislative level.In addition to the existing documents such as the 'Guiding Opinions on Punishing Online Violence-Related Criminal Offences in Accordance with the Law' and the 'Regulations on the Governance of Online Violence Information', the 2026 Central Political and Legal Affairs Work Conference placed great emphasis on the comprehensive governance of cyberspace. It explicitly called for the advancement of the 'Clean Internet' special campaign to combat and regulate online rumours, online violence, and online trolls in accordance with the law, whilst collaboratively promoting the governance of the online ecosystem and reinforcing the responsibilities of principal entities and regulators.

Although legislative practice has made some progress to date, it requires further development. Given the rapidly evolving nature of the online environment, rigid definitions struggle to address emerging issues. Future legislative efforts should therefore clarify the criteria distinguishing online violence from public oversight, moving beyond existing regulations to address the ever-changing challenges of cyber governance, and providing more practical guidance for law enforcement and the judiciary.[9] At the same time, legislative design must consistently incorporate the principle of proportionality; the severity of restrictive measures should be commensurate with the degree of harm caused by the speech in question. This approach must avoid both unduly restricting the space for public discourse and selective enforcement resulting from ambiguous standards.Consequently, a more open-ended definition of cyberbullying should be adopted to prevent the law from becoming a dead letter due to overly restrictive definitions; public oversight activities, such as online reporting and monitoring, must have a clear legal basis and factual grounds. The disclosure of information regarding the subject of a report must comply with the principle of proportionality, and the subsequent actions of the monitor must not violate prohibitive regulations.

(2) Strengthening Practical Accountability

In practice, the judicial process is central to the governance of online violence. In recent years, China's judicial authorities have actively explored solutions to the challenges of attributing liability for online violence, with notable breakthroughs including the mechanism for converting private prosecutions into public prosecutions and judicial advances in establishing causality.The mechanism for converting private prosecutions into public prosecutions has provided a vital institutional tool for resolving the dilemmas of 'the law not punishing the masses' and the difficulties victims face in providing evidence when holding perpetrators of online violence to account. For instance, in the case of a woman in Hangzhou who was falsely rumoured to have had an affair whilst collecting a parcel, the case was originally a private prosecution; however, due to the extremely wide scope of online dissemination and the severe disruption to public order, the Yuhang District People's Procuratorate in Zhejiang initiated the conversion of the private prosecution into a public prosecution.[10] By facilitating the conversion of private prosecution to public prosecution in such specific cases, proactively intervening at an early stage to guide investigations, and establishing the judicial principle through the publication of guiding cases that "for online defamation that seriously endangers social order and national interests, the procuratorial organs shall initiate public prosecution proceedings in a timely manner in accordance with the law", the Supreme People's Court's 2026 Work Report further clarified that crimes such as online violence must be punished in accordance with the law to promote comprehensive governance of cyberspace security.The People's Court Case Database has also included reference cases involving new forms of online violence, such as "online unboxing and doxxing" and "AI voice and face swapping", continuously providing judicial guidance to refine the adjudication rules system and sending a clear signal that the internet is not a lawless zone.

In the process of strengthening the role of judicial authorities in practice, the application of the principle of proportionality is particularly crucial.When determining acts

of online violence, judicial authorities should avoid simplistic assessments and instead comprehensively consider factors such as the content, context, motive and consequences of the speech in each individual case. At the same time, guiding cases are also crucial in the current governance of online violence; as a medium, cases transform abstract norms into practical experience. Accelerating the construction of a comprehensive system of guiding cases on online violence—one that is sufficient in number, complete in type and clear in hierarchical effectiveness—should be a key focus in perfecting the institutional framework for the governance of online violence.

(3) Platform Liability

Online platforms play a crucial 'gatekeeper' role in the governance of online violence, and the delineation of their responsibilities directly affects the balance between governance effectiveness and the protection of freedom of speech.The current legal framework systematically stipulates the governance responsibilities of platforms from multiple dimensions. However, the true crux lies in separating the platform's dual roles as both beneficiary and regulator, to prevent platforms from profiting unjustly by exploiting incidents of online violence. Consequently, online platforms should place greater emphasis on establishing victim protection mechanisms.[11] As key nodes in the dissemination of online information, platforms possess a unique advantage in controlling cyberbullying at its source; they have the technical capability to identify and monitor such content, the financial capacity to invest in governance resources, and the institutional capacity to formulate and enforce platform rules. This equivalence between 'capacity and responsibility' constitutes the legitimacy of platforms' obligation to undertake proactive governance.

The introduction of algorithmic recommendation technology has further complicated the determination of platform liability. The prevailing view in academic circles is that online service providers bear a higher duty of care due to algorithmic recommendation technology, and that the expansion of this duty of care for providers of algorithmic recommendation services is justified.[12] This implies that when platforms actively push controversial or emotionally charged content via algorithms to generate traffic and economic gains, they can no longer evade responsibility by invoking the safe harbour principle, nor can they continue to prioritise economic interests above all else.From the perspective of protecting freedom of expression, the transparency of platform moderation standards, the accessibility of redress mechanisms, and the unimpeded availability of user complaint channels serve as institutional safeguards against platforms unduly restricting lawful expression.

(4) Systemic Governance

The effective governance of cyberbullying ultimately depends on the establishment of a multi-stakeholder governance system comprising government regulation, platform accountability, judicial safeguards, public participation and social collaboration.[13] At the institutional level, public interest litigation by the procuratorate is emerging as a key innovative mechanism for tackling cyberbullying.The government should, through the exercise of powers by various law enforcement and judicial bodies, focus on the chaos surrounding online violence and other content, prioritising the crackdown on and governance of illegal and criminal activities such as online rumours and online violence, and promote collaborative governance to drive end-to-end governance and comprehensive protection of the cyberspace.

At the macro level, the 2026 Central Political and Legal Affairs Work Conference proposed to collaboratively advance the governance of the online ecosystem, reinforce primary and regulatory responsibilities, strengthen research into new technologies, and strictly prevent the use of encryption technologies such as blockchain to evade regulation. The Supreme People's Court has also proposed measures such as issuing judicial recommendations to promote effective coordination between law enforcement and the judiciary, thereby fostering the formation of a comprehensive online governance system comprising government regulation, platform accountability, judicial safeguards and public participation.[14] The establishment of a systemic governance framework hinges on coordination and checks and balances among various stakeholders. Government regulation must effectively combat cyberbullying whilst preventing excessive interference, requiring the establishment of a feasible boundary between combating cyberbullying and preventing overreach. Platforms must fulfil their social responsibilities whilst avoiding the suppression of free expression through excessive moderation, establishing risk assessments and monitoring mechanisms tailored to their scale and content types.Finally, the public must, whilst participating in online activities, play an active role in social oversight whilst exercising their rights within legal boundaries to avoid causing harm to others.

4. Conclusion

In the digital age, the legal boundary between freedom of speech and online violence is not a fixed, immutable red line, but rather a dynamic equilibrium achieved through wisdom in specific contexts and individual cases.The effective curbing of cyberbullying ultimately depends on the deep involvement of legal mechanisms and the broad consolidation of social consensus. Only when government regulation is present, platforms fulfil their responsibilities without dereliction, and public participation is informed rather than blind, can we weave a web of the rule of law within an open and inclusive digital environment—one that protects both human dignity and freedom of expression—thereby achieving the organic unity of the rule of law and good governance in the digital age.In the future, as emerging technologies such as generative artificial intelligence continue to evolve, cyberbullying may take on new forms that are more covert and technologically sophisticated. Legal scholarship must maintain a keen insight into technological developments, continuously scrutinising and adjusting the dynamic boundaries between freedom of speech and the governance of cyberbullying, in order to meet the digital society's heightened expectations for fairness and justice.

References

[1] Tu Xinyun, Liang Zhuxiang. The Dilemmas and Policy Recommendations for Governing Online Violence Based on Its Crowd-Based Characteristics [J/OL]. Economy and Social Development, 1–12 [12 April 2026]. https://doi.org/ 10. 16523/ j.45-1319.20260401.001.

[2] Zhang Wei, Guo Ziqi, Zhang Jianwei. Generative Artificial Intelligence Empowering the Governance of Online Violence: Logic, Risks and Countermeasures [J]. Journal of Chengdu University (Social Sciences Edition), 2025, (04): 28–33.

[3] Fan Jie. An Analysis of the Criminalisation of 'Insulting' Online Violence [J]. Law, 2025, (08): 89–105.

[4] Cai Pengcheng. Constructing a Theory of the Limits of Criminal Liability for Online Rumours: With a Discussion on the Demarcation Between Online Rumours and Cyberbullying [J]. Yuejiang Journal, 2023, 15(05): 58–75+169–170. DOI: 10.13878/j.cnki.yjxk.2023.05.005.

[5] Chen Yongfeng, Li Jiaxuan. The Governance Dilemma of 'The Law Does Not Punish the Masses' in Cyberbullying and Pathways to Resolution [J]. Journal of the Railway Police College, 2025, 35(04): 28–34. DOI: 10.19536/j.cnki.411.

[6] Cheng Hua. Governance Dilemmas and Legal Countermeasures for Cyberbullying [J]. Law and Economy, 2019, (10): 132–133.

[7] Wei Qi. Platform Obligations in the Governance of Cyberbullying [J]. Jingchu Law Review, 2025, (03): 50-63.

[8] Chen Ye, Xu Hao, Cheng Qingxuan. The Spread of Online Violence in the Smart Society under the Dual Role of Algorithms: Trends, Drivers and Governance Pathways [J]. Journal of Information Resource Management, 2026, 16(01): 10-22. DOI: 10.13365/j.jirm.2026.01.010.

[9] Wang Minyuan, Wang Ge. A Study on the Legal Integration of Cyberbullying Governance [J]. Journal of the National Prosecutors College, 2025, 33(04): 132–146.

[10] Li Zeyuan. Dilemmas and Improvements in the Criminal Law Governance of Cyberbullying [J]. Journal of Shandong Youth Political College, 2024, 40(06): 59-65. DOI: 10.16320/j.cnki.sdqnzzxyxb. 2024.06.003.

[11] Pan Yinzhu. A Study on the Norms Governing the Obligations of Social Media Platforms in the Governance of Online Violence [D]. East China University of Political Science and Law, 2025. DOI: 10.27150/d.cnki.ghdzc.2025.000636.

[12] Li Huaisheng. The Dilemmas of Platform Governance of Cyberbullying and the Limits of Liability [J]. Research on Public Security, 2025, 8(01): 41–59+123–124.

[13] Fang Huiying. The Basis, Dilemmas and Boundaries of Criminal Liability for Platform Participation in the Governance of Cyberbullying in the Age of Artificial Intelligence [J]. Journal of Hunan University (Social Sciences Edition), 2026, 40(02): 130-139. DOI: 10.16339/j.cnki.hdxbskb.2026.02.015.

[14] Liu Yanhong. The Transition to the Rule of Law in the Governance of Online Violence and the Construction of a Legislative Framework [J]. Legal Studies, 2023, 45(05): 79–95.