Proceedings of ICILLP 2025 Symposium: Digital Governance: Inter-Firm Coopetition and Legal Frameworks for Sustainability
DOI: 10.54254/2753-7048/2025.BR28073

# *Research on Evidence Collection Models for Cyberbullying from the Perspective of Platform Responsibility*

**Zhimei Nan**

*Institute of Civil and Commercial Economics, China University of Political Science and Law, Beijing, China*
*3460629440@qq.com*

***Abstract.*** Cyberbullying has become increasingly prevalent in the digital age, with its anonymity, cross-regional nature, and instantaneous spread posing significant challenges to traditional evidence-gathering methods, thereby increasing obstacles for victims seeking redress and for judicial accountability. Current online violence evidence collection models face challenges such as the easy loss of evidence, insufficient ability of complainants to provide evidence, and the ineffective operation of police assistance in evidence collection. As the 'gatekeepers' of online violence and key participants in collaborative governance, online platforms should have a duty to actively assist in preventing and addressing online violence. At the institutional level, platforms should be legally obligated to conduct pre-incident evidence preservation, respond during incidents, and assist post-incident. Specific operational standards should be clarified. At the technical level, efficient evidence collection mechanisms should be implemented, and a tiered response and evidence coordination governance system should be established to enhance the effectiveness of platform regulation and achieve effective governance of cyberbullying.

***Keywords:*** Cyberbullying, Platform Responsibility, Evidence Collection, Dual-Track System Model

## 1. Introduction

Cyberbullying refers to the use of digital media in cyberspace to insult, defame, slander, mock, or invade the privacy of others through words, images, videos, or other means. Such behaviour often causes psychological trauma, damage to reputation, and even disruption to the victim's life. Cyberbullying is not only an extension of real-world violence into cyberspace but also a manifestation of the disorder in new social relationships formed by the internet. With the development of digital technology, cases of cyberbullying have become increasingly frequent, with various forms of defamation, discrimination, abuse, and doxxing spreading rampantly in virtual spaces. In a 2023 survey on this topic, over 60% of respondents reported having experienced cyberbullying to varying degrees, while only 38.2% explicitly stated they had never been subjected to it. Additionally, 76.7% of respondents believed that addressing cyberbullying was either 'very urgent' or 'fairly urgent.' A series of heinous incidents, such as a woman in Hangzhou being falsely accused of infidelity while picking up a package, a pink-haired girl named Zheng Linghua being

© 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.BR28073

falsely accused of suicide, the influencer 'Guan Guan' being subjected to sustained cyberbullying leading to suicide, and Dr. Shao being cyberbullied to the point of jumping from a building, not only inflict irreparable mental trauma and substantial rights violations on individual victims but also severely undermine the overall ecosystem of online platforms. Therefore, combating cyberbullying and creating a clean virtual space are essential for safeguarding citizens' legitimate rights and maintaining social order.

Compared to offline infringements, cyberbullying has distinct characteristics such as anonymity, cross-regional nature, instantaneous dissemination, and massive information volume. This makes it extremely difficult to preserve or retrieve key evidence, posing significant challenges for victims and judicial authorities in identifying, securing, and extracting valid evidence. In response, the Cyberspace Administration of China issued the 'Provisions on the Governance of the Ecological Environment of Online Information Content' in 2020 and the 'Provisions on the Governance of Online Violence Information' in 2024, both of which explicitly emphasise the primary responsibility of online information service providers in preventing and combating online violence. This formally establishes the important role of online platforms in the governance of online violence. However, in practice, issues related to the obligations, standards for fulfilment, and legal liabilities concerning key aspects such as the preservation and retention of evidence of online violence remain vague in the relevant legal provisions, with unclear specific enforcement mechanisms. This has led to insufficient motivation and ineffective results in platform compliance. From the perspective of platform responsibility, how to systematically address the challenges of evidence collection in cases of online violence and explore practical and effective pathways for platform governance optimisation has become a pressing issue for both the academic and practical communities.

## 2. Overview of the evidence collection model for cyberbullying

According to Article 246, Paragraphs 1 and 2 of the Criminal Law of the People's Republic of China, "Whoever, by means of violence or other methods, publicly insults another person or fabricates facts to defame another person, under circumstances of serious nature, shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, control, or deprivation of political rights. The offence specified in the preceding paragraph shall be prosecuted only upon complaint, except where it seriously endangers social order or national interests." Since most cyberbullying cases fall under the category of private prosecution cases, Article 51 of the Criminal Procedure Law of the People's Republic of China stipulates that the burden of proof lies with the complainant in private prosecution cases. Therefore, victims of cyberbullying, as complainants in criminal proceedings, bear the burden of proof and must actively collect and provide sufficient evidence to support their allegations against the perpetrators of cyberbullying. Article 246, Paragraph 3 of the Criminal Law further stipulates that 'if the victim files a complaint with the people's court for acts committed through information networks as specified in the first paragraph, but faces difficulties in providing evidence, the people's court may request the public security authorities to assist in evidence collection.' This indicates that in addition to the complainant's own evidence collection methods, the public security authorities may assist in evidence collection when the complainant faces difficulties in providing evidence. This model of police assistance in evidence collection was further specified in the newly added second paragraph of Article 325 of the 2021 Interpretation of the Criminal Procedure Law and in the 2023 Guidelines on the Lawful Punishment of Cyberbullying Criminal Offences (hereinafter referred to as the 'Guidelines'). The Guidelines explicitly state that the legal provisions regarding public security organs' assistance in evidence collection must be implemented. Public security organs have the duty to assist in promptly

DOI: 10.54254/2753-7048/2025.BR28073

identifying the perpetrators, collecting evidence materials regarding the dissemination and impact of cyber violence information, and if they are unable to collect relevant evidence materials, they shall submit a written explanation to the people's court.

It is evident that China's evidence collection model for cyber violence crimes is a dual-track system, comprising both self-collection of evidence by the complainant and assistance from public security authorities. Among these, self-collection of evidence by the complainant serves as the foundation, while assistance from public security authorities acts as a supplement and support when the complainant faces difficulties in providing evidence. In judicial practice, due to the immaturity of the public security authorities' assistance in evidence collection and its limited practical application, most self-prosecution cases involving cyberbullying are handled through the plaintiff's independent evidence collection, with few instances of public security authorities assisting in evidence collection.

## 3. Analysis of the limitations of the current evidence collection model for cyberbullying

### 3.1. The difficulty of self-evidence collection for victims of cyberbullying

The relatively limited ability of private prosecutors to present evidence is a common issue in private prosecution cases. First, private prosecution cases differ from public prosecution cases in their purpose, which is not to pursue the overall social order but rather to protect the legitimate rights and interests of the victim. Therefore, the initiative to present evidence is primarily held by the private prosecutor. China follows the principle of substantive review in private prosecution cases. Article 316 of the Interpretation of the Criminal Procedure Law stipulates that the conditions for a people's court to accept a private prosecution case include a clear defendant, specific litigation requests, and evidence proving the defendant's criminal acts. While this establishes the criteria for filing a private prosecution case, it does not specify the specific requirements for evidence proving the defendant's criminal acts, which may make it difficult for private prosecutors to collect evidence effectively and for people's courts to accurately assess the probative value of the evidence. Secondly, unlike the evidence-gathering model in public prosecution cases where the investigative authorities bear the primary responsibility for evidence collection, although the Interpretation of the Criminal Procedure Law stipulates that plaintiffs have the right to apply to the court for assistance in obtaining evidence when the court deems it necessary, i.e., the right to investigate and collect evidence, the criteria for determining 'necessity' are unclear, and the court's discretion is significant, making it difficult for plaintiffs to fully exercise their right to investigate and collect evidence. Thirdly, in order for the evidence collected by the private prosecutor to have probative value in proving the defendant's criminal conduct in a private prosecution case, it often needs to be notarised at a notary office. However, in many regions, the fees for notarising evidence such as electronic data and witness statements may exceed 1,000 yuan per item, which can directly increase the economic burden on the private prosecutor and thereby limit their proactive efforts in evidence collection [1].

Against the backdrop of inherent difficulties in evidence collection for plaintiffs in private prosecution cases, the unique characteristics of cyberspace, such as its anonymity and openness, further exacerbate the challenges faced by plaintiffs in obtaining evidence. The evidence typically obtained by plaintiffs is often limited in type and insufficient in quantity. When perpetrators of cyberbullying use online platforms to verbally attack victims through insults, defamation, or the dissemination of false information, or to harm victims through the use of images, videos, or audio files, they can exploit the characteristics of cyberspace to quickly delete, alter, or conceal previously posted information, making it difficult for victims lacking professional evidence-gathering

DOI: 10.54254/2753-7048/2025.BR28073

techniques and capabilities to preserve comprehensive and effective evidence in a timely manner, let alone collect electronic data that meets court standards and can serve as evidence for case adjudication. Furthermore, in most cases, the perpetrators are not solitary actors. In addition to the primary perpetrators who directly attack and abuse the victim, there are numerous individuals hiding within the internet—such as those who repost, comment, or echo the attacks—who actively participate in cyberbullying. Collective cyberbullying is not uncommon [2]. According to the crowd psychology mechanisms described by Le Bon in The Crowd, individuals are easily driven by 'collective unconsciousness' when they integrate into a group, exhibiting characteristics such as impulsiveness, suggestibility, and emotionality. This psychology leads them to be more inclined to follow collective actions while ignoring personal rationality and sense of responsibility. For victims, the likelihood of obtaining the true identities and criminal information of all perpetrators of online violence is minimal. Without timely assistance from platforms or public security authorities, they often fail to meet the conditions for filing a case, such as having a clear defendant and evidence proving the defendant's criminal acts. Even if victims obtain some evidence related to certain perpetrators of online violence, they still find it difficult to hold the unspecified group responsible for the online violence.

### 3.2. The application of the public security assistance in evidence collection model is relatively limited

Article 11 of the 'Guiding Opinions on the Lawful Punishment of Cyber Violence Crimes' stipulates that 'public security organs shall, in accordance with the requirements of the people's courts and the specific circumstances of the case, promptly identify the perpetrators, collect evidence materials such as the dissemination and spread of relevant insulting and defamatory information, and the impact caused.' Network service providers shall provide necessary technical support and assistance to public security authorities in evidence collection in accordance with the law. If, through the assistance of public security authorities in evidence collection, the case meets the conditions for acceptance as a private prosecution case, the People's Court shall decide to file the case; if relevant evidence materials cannot be collected, the public security authorities shall submit a written explanation to the People's Court." This provision reflects that when the plaintiff faces significant difficulties in providing evidence, the public security authorities bear the direct responsibility for promptly collecting evidence related to cyberbullying. The public security assistance in evidence collection model is a institutional arrangement where state power intervenes in the private sphere to provide redress. On one hand, the prerequisite of 'significant difficulties in providing evidence' maximises respect for citizens' rights, to some extent preserving the victim's right to choose the criminal litigation procedure; on the other hand, the moderate intervention of state power helps address the obstacle of victims' weak prosecutorial capacity, facilitating the smooth progress of private prosecution cases, thereby embodying the principle of inquisitorialism in criminal proceedings.

Although the public security assistance in evidence collection model has corresponding laws and regulations as its framework, its practical application is limited and imperfect, with instances where private prosecutors apply to the court for public security assistance in evidence collection but are refused occurring from time to time. The reasons for this can be attributed in part to the unclear application criteria of this model. First, the criteria for determining whether 'providing evidence is indeed difficult' are uncertain, and practices vary across regions. Courts have significant discretion and uncertainty when deciding whether to require police assistance in evidence collection. In the current context of rapidly increasing cyberbullying cases, courts may be more inclined to reject self-

DOI: 10.54254/2753-7048/2025.BR28073

prosecution applicants' requests for police assistance to conserve judicial resources, and police departments may also be reluctant to provide such assistance. Second, the target of police assistance in evidence collection is not clearly defined. Some scholars argue that the purpose of police assistance in evidence collection is to ascertain the truth, and their evidence-gathering activities serve as a supplement to the court's duty to collect evidence. Other scholars argue that since the court has no obligation to investigate and collect evidence during the case filing stage, the police's assistance in evidence collection is an exercise of their litigation functions, and thus assert that the subject of assistance is the plaintiff. However, the lack of clarity in identifying this subject may pose issues for subsequent evidence collection procedures. Additionally, although China has established a certain system of ex post facto supervision to regulate the evidence-gathering activities of public security organs, prior to the fact, the court's requests for assistance in evidence collection often lack binding force over public security organs, and the evidence-gathering activities of public security organs lack effective supervisory mechanisms [3]. Since there are no corresponding laws or regulations stipulating the legal liability of public security organs for refusing to cooperate with the court's requests for assistance in evidence collection, public security organs are more likely to passively respond to such requests when their own case-handling workload is heavy.

The ideal operational state of the two evidence-gathering models for cyberbullying crimes in China should be one where the boundaries between the two are clear, the transition between them is smooth, and their functions complement each other. However, in reality, the effectiveness of police assistance in evidence gathering is limited, making it even more difficult for the two evidence-gathering methods to form an effective collaborative mechanism. Therefore, clarifying the conditions for initiating and applying the police assistance evidence-gathering model is a prerequisite for promoting its effective application and a key step in improving the overall evidence-gathering model for cyberbullying cases.

## 4. The legal basis for platforms' responsibility in assisting with evidence collection for cyberbullying

### 4.1. The legitimacy of platforms as key entities in assisting with evidence collection

As the core hub for the dissemination of online information and the 'first scene' where cyberbullying occurs, online platforms not only provide information services but also effectively construct and manage digital public spaces. Platforms exercise significant control over their operational spaces, which manifests in technical aspects such as data storage, content distribution, and permission management, and extends to the formulation and enforcement of user behaviour rules. For this reason, platforms cannot be viewed merely as neutral 'channels' but should be recognised as 'gatekeepers' with substantive governance functions. While enjoying data dividends and operational autonomy, they must also assume corresponding social responsibilities and legal obligations. Assisting in effective evidence collection and clarifying liability for infringement are intrinsic requirements for managing internal risks and fulfilling their managerial duties. From the perspective of the overall framework of internet ecosystem governance, platforms occupy a critical node in the generation, storage, and retrieval of evidence. Their assistance in evidence collection not only concerns the redress of individual rights but also directly impacts public interests and the overall order of the internet space. In recent years, China has continuously conducted special governance campaigns against cyberbullying and issued corresponding laws and policies, strengthening and clarifying the responsibilities of platforms in cyberbullying governance, including requirements for assisting in evidence collection. The 2022 'Notice on Effectively Strengthening the Governance of

DOI: 10.54254/2753-7048/2025.BR28073

Cyber Violence' explicitly states that the primary responsibility of website platforms must be enforced, including four major areas: establishing and improving cyber violence early warning and prevention mechanisms, strengthening the protection of cyber violence victims, strictly preventing the spread and dissemination of cyber violence information, and strictly enforcing legal penalties. This sets out the preliminary obligations for platforms to proactively fix, preserve, and provide evidence to victims. Article 25 of the 2024 Regulations on the Governance of Online Violence Information stipulates that when platforms discover and handle online violence information, they should promptly preserve the content and related data, provide users with a quick evidence collection function for online violence information, and promptly provide necessary technical support and assistance to public security and cyberspace administration departments that legally request evidence. Article 28 of China's Cybersecurity Law also stipulates that platforms should provide technical support and assistance to public security organs and national security agencies. These provisions collectively form the direct legal basis for platforms' obligations to assist in evidence collection, strengthening their risk prevention and review supervision obligations, and elevating them from a passive supporting role to an active collaborator with legal obligations.

### 4.2. The necessity of platforms as key entities in assisting evidence collection

Evidence collection is a critical component of cyberbullying governance. Compared to individual victims, platforms possess unparalleled technical advantages and data control capabilities in terms of data acquisition, storage, and analysis. In the aforementioned online survey, 50.5% of respondents indicated that they were more likely to report incidents of cyberbullying to the platform after experiencing such incidents, highlighting the significant importance of platform assistance and support for cyberbullying victims. Some scholars argue that since platforms are the monopolistic holders of cyberbullying-related data that users cannot directly access, and they possess cutting-edge algorithmic technologies and intelligent surveillance systems for cyberbullying governance, platforms are the only entities capable of addressing cyberbullying in terms of resources and technology [4].

In the early stages of internet industry development, platforms adhered to the 'principle of technological neutrality,' meaning they did not assume proactive pre-emptive regulatory obligations or take responsibility for users' online speech. However, platforms are now expected to actively assume pre-emptive obligations within reasonable limits, no longer able to remain detached from online disputes. However, in practice, judicial remedies primarily focus on punishing perpetrators of online violence, often neglecting platform responsibility [5].Therefore, it is necessary to clarify the platform's responsibility as an important entity in assisting with evidence collection.

### 4.3. The feasibility of platforms as key entities in assisting with evidence collection

Platforms have become key entities in the process of collecting evidence related to online violence. This role not only possesses legal legitimacy and practical necessity but also has practical feasibility. This feasibility stems from platforms' unique technical capabilities, data control capabilities, and their positioning within the current legal framework.

Firstly, all user activities on the platform, such as posting, commenting, sharing, and private messaging, are stored as electronic data on the platform's servers. Therefore, the platform is not only the most powerful channel for information dissemination but also the sole holder and controller of vast amounts of data. Its effective assistance in governance can help address the limitations of self-reporting in evidence collection. Additionally, the platform's 'backend real-name, frontend

DOI: 10.54254/2753-7048/2025.BR28073

voluntary' management principle means it can access the real identity information or valid contact details of registered users. In the face of increasingly common collective cyberbullying incidents, this can help victims identify actual infringers and address the challenge of 'no punishment for the masses.' Secondly, platform assistance can also enhance the efficiency of police assistance in evidence collection. When police agencies intervene in self-prosecution cases at the request of the court to assist in evidence collection, they often face challenges such as dispersed targets and vague leads due to the cross-regional nature of online cases. As a data source, the platform can swiftly provide precise information identifiers and account information of associated users, significantly enhancing the targeted nature of police investigations and evidence collection. Therefore, the platform serves as a connection point between victims of cyberbullying and judicial authorities, providing robust technical support and playing an indispensable role in evidence discovery, preservation, and transfer. It is imperative to establish a comprehensive cyberbullying governance model that prioritises platform responsibility.

## 5. Optimisation recommendations for the governance of online violence platforms

Based on an analysis of the legitimacy, necessity, and feasibility of platform responsibility, the key to addressing the challenges of evidence collection in cases of online violence lies in strengthening platform responsibility and collaboratively establishing a new governance ecosystem centred on platforms as key hubs, with clear delineation of rights and responsibilities and robust oversight mechanisms.

### 5.1. Clarifying the legal obligations and operational standards for platform assistance in evidence collection

Firstly, clarifying the specific obligations, operational norms, and responsibility boundaries of platform assistance is a crucial foundation for optimising cyberbullying governance. It is essential to strengthen the rigidity and operability of their responsibilities, while ensuring smooth access for victims to obtain platform assistance and establishing strict supervision and accountability mechanisms. Since online platforms differ from state agencies in that they lack clear responsibility boundaries and the backing of state coercive power, merely emphasising platform responsibilities in general terms may lead to a passive attitude when handling online violence incidents, making it difficult for them to effectively fulfil their role as 'gatekeepers.' Therefore, the primary task is to refine the legal obligations and operational standards for platform assistance in evidence collection, addressing the current situation where regulations are too generalised and result in ineffective implementation. Prior to incidents, platforms must fulfil their obligations for risk warning and preliminary identification. On one hand, platforms should automatically conduct basic evidence preservation operations on all user-posted content, rather than only initiating preservation measures after receiving complaints or reports. This preventive evidence preservation mechanism provides a foundational safeguard for potential future disputes, effectively addressing the challenge of evidence being lost or destroyed in an instant. On the other hand, once platforms identify risk information, they should immediately initiate mild intervention measures to swiftly contain the escalation of online violence. During the process, the platform's 'immediate response' obligation should be clearly defined. Upon receiving a valid complaint or report from a victim that meets legal requirements or an official subpoena from an authorised agency, the platform must locate, confirm, fix, and extract the target information within the statutory time limit and immediately take technical measures to prevent the evidence from being tampered with or lost. Post-incident, once cyberbullying incidents

DOI: 10.54254/2753-7048/2025.BR28073

enter the judicial process, the platform's obligations should focus on assisting judicial authorities and restoring the online ecosystem, strictly implementing the requirements of the 'Guiding Opinions' to provide comprehensive technical assistance to public security authorities in their investigations and evidence collection [6].

Secondly, identifying the reasonable boundaries of platform control is a necessary requirement for balancing the interests of multiple parties and optimising the governance of cyberbullying. Although platforms have a series of obligations regarding review, control, management, and disposal, and can establish relatively effective models for identifying illegal information and rules for manual review, they are still unable to screen and identify all instances of cyberbullying, especially those expressed through more everyday and subtle means, such as insults and abuse. If platforms improperly expand their review mechanisms or overly control netizens' normal speech expression, it may result in excessive interference with the free speech space online, infringing upon the entertainment attributes of social media and the open and shared principles of the internet [7].

### 5.2. Establishing a convenient and efficient 'one-click evidence collection' platform mechanism

Empowering the platform through technological advancements is the foundation for enhancing its ability and efficiency in assisting with evidence collection. The goal is to utilise advanced technology to achieve intelligent identification, secure preservation, efficient management, and convenient retrieval of evidence related to cyberbullying. Both the 'Notice on Strengthening the Governance of Cyberbullying' and the 'Regulations on the Governance of Cyberbullying Information' explicitly emphasise that platforms should establish a 'one-click evidence collection' mechanism to facilitate users in collecting evidence. However, in reality, many platforms have not established such mechanisms in accordance with these requirements, or when users encounter cyberbullying and seek assistance from the platform, the platform is unable to provide effective assistance. Therefore, it is essential to optimise the convenient channels for victims to apply for evidence collection from the platform, reduce the technical barriers and procedural burdens for obtaining platform assistance, and fully implement the 'one-click evidence collection' mechanism as a standardised and efficient platform function. Especially for online platforms with comment and social features, they should set up intuitive and user-friendly 'evidence preservation' or 'report and apply for evidence preservation' function buttons in the user interface. When users apply to use this function and provide relatively clear evidence, the platform system should immediately automatically preserve the information suspected of cyberbullying, its complete contextual environment, and the current dissemination status of the information, and promptly feedback this to users as important evidence for their subsequent rights protection efforts. When victims submit formal evidence collection requests through the platform online, the materials required should, in principle, only include basic information verifying their true identity, direct links or clear screenshots of the infringing information, and a brief description of the situation. The platform's review standards for such requests should focus on formal review, primarily confirming the existence of the complained-about information and making an initial determination of whether it constitutes online violence. Complex or subjectively stringent review conditions that indirectly hinder users from collecting evidence should not be imposed. Through the above measures, the platform's technical advantages can be leveraged to address the evidence-gathering disadvantages faced by self-reporting parties.

DOI: 10.54254/2753-7048/2025.BR28073

### 5.3. Establishing an evidence collaboration governance system

Cyberbullying governance is a systematic endeavour that requires integrating platforms into a multi-stakeholder governance framework, transcending the existing dual-subject evidence-gathering model, and establishing an evidence collaboration mechanism among judicial authorities, self-reporting parties, and platforms.

First, a tiered response mechanism based on the nature and urgency of the case should be established. Referring to the Cybersecurity Law and the Guidelines, cases can be categorised into 'major and urgent' and "general" based on whether the cyberbullying 'seriously endangers social order and national interests' or may pose a significant threat to the victim's life, health, or other major legal interests. For major urgent cases, a special response channel should be activated: public security authorities have the right to require the platform to synchronously and in real-time fix and retain relevant evidence, and the platform must immediately respond and promptly notify judicial authorities of evidence leads, achieving a critical shift from 'post-incident retrieval' to 'real-time synchronisation' to address the risk of evidence being lost in an instant. For general self-prosecution cases, the focus is on enhancing the platform's 'one-click evidence collection' functionality to empower victims, supplemented by police assistance in evidence collection when victims face difficulties in providing evidence. Secondly, it is necessary to refine the standardised procedures for public authorities to request evidence from platforms. To avoid platforms being overwhelmed by frequent and disorderly requests for evidence and to protect user data security, judicial interpretations or departmental regulations should be established to regulate the evidence-gathering activities of public security authorities and procuratorial organs. Additionally, mechanisms for prosecutorial agencies to intervene early in major cyberbullying cases could be explored. For cases that may harm public interests, prosecutorial agencies may legally intervene early to guide public security authorities and platforms in targeting and collecting key evidence, thereby creating a strong legal deterrent against cyberbullying perpetrators.

## 6. Conclusion

The effectiveness of cyberbullying governance largely depends on whether the core bottleneck of evidence collection can be effectively overcome. Currently, self-reporters face significant disadvantages in their ability to collect evidence, and there are systemic shortcomings in police assistance for evidence collection. Online platforms must assume the role of 'gatekeepers' in the governance of the online ecosystem and take on the responsibility of actively assisting in evidence collection. At present, platforms have evolved from mere information intermediaries into key stakeholders in the governance of online violence, holding core resources and serving as a bridge between upper and lower levels. At the institutional level, efforts should be made to clarify and enforce platform obligations, and establish a convenient channel for victims to obtain platform assistance. At the technological level, emphasis should be placed on developing intelligent identification and evidence preservation systems, building a secure and efficient unified evidence management platform, and exploring the application of blockchain and other trustworthy evidence preservation technologies to enhance the platform's ability and efficiency in identifying, preserving, managing, and providing evidence. Effectively safeguarding citizens' legitimate rights and interests in the digital age, deterring and punishing cyberbullying behaviour, and ultimately creating a clear, orderly, and safe cyberspace are not only the inevitable requirements for online platforms to fulfil their legal and social responsibilities but also an urgent strategic task in the process of advancing the modernisation of the national cyberspace governance system and governance capabilities.

DOI: 10.54254/2753-7048/2025.BR28073

## References

[1] Zhang Zhiying, Zeng dan. The Dilemma of Evidence Collection in Criminal Private Prosecution Cases and Its Solutions. (2025) Journal of Tianzhong, 3, 44-45.
[2] Zhang Qian. Study on the Public Security Assistance Evidence Collection System in Self-Prosecuted Cases of Cyberbullying. (2025) Research on Rule of Law, 2, 135-136.
[3] Zhang peizheng. The Logic Formation and Rational Reflection of the Public Security Assistance Evidence Collection System in Self-prosecuted Cases of Cyberbullying. (2024) Journal of Sichuan Police College, 1, 59-60.
[4] Wang Ran. On the Platform Technology Governance of Cyberbullying. (2024) Science of Law(Journal of Northwest University of Political Science and Law), 2, 124.
[5] Xie Shu. Towards Three-Dimensional Collaboration: Evidence Provision in Cybercrime Cases. (2025) Political Science and Law, 7, 150.
[6] Zhao Jingwu. Alienated Cyber Comments: Revisiting the Phased Governance of Cyber Violence Information. (2023) Northern Legal Science, 5, 32-34.
[7] Zhu Xiaoyan. From Content Supervision to Ecological Regulation: Reshaping Platform Obligation of Network Violence Information Governance. (2024) Journal of Nanjing University (Philosophy, Humanities and Social Sciences), 1, 79-80.