# The Dilemma and Outlet of the Criminal Responsibility of the Network Rumor Platform

**Yuming Tian**

School of Law, Beijing Normal University, Beijing 100875, China

**Abstract:** The definition of criminal responsibility of network rumor platform is the core proposition of cyberspace governance in the digital era. At present, China's network platform plays the dual role of information intermediary and content regulator in rumor governance, but the identification of criminal responsibility is faced with two major difficulties: first, the legal obligation is not clear, the conflict between law enforcement and privacy protection; second, the subjective "knowing" proof is difficult, and the lack of unified provisions on the connotation and proof standard of "knowing", leading to the imbalance risk of responsibility expansion or restriction in judicial practice. By comparing external experience, propose the localization improvement path: firstly, clarify the platform obligation boundary, balance law enforcement cooperation and privacy protection through quantitative technical standards and stratified data transfer rules; secondly, optimize the identification mechanism of "knowing", introduce the distinction standard between "actual knowing" and "should know", and construct the "preliminary proof-proof transfer" rules, combine the expert jury system and block chain storage technology to strengthen the objectivity and scientificity of judicial recognition.

**Keywords:** Internet rumors; Criminal responsibility; Platform obligations; Knowing

The rapid development of information technology has reshaped the mode of information dissemination, and also makes the network rumors show the characteristics of widespread spread, concealment and uncontrollable harm. Although China has stipulated the criminal responsibility of [1] network platforms in legislation, there are some deficiencies in the classification and definition of responsibility, which leads to significant difficulties in investigating the criminal responsibility of network platforms in practice. On the one hand, the boundaries of the legal obligations of the network platforms are unclear. When determining the criminal responsibility of the network platform, the court needs to judge whether the platform has fulfilled its due responsibilities according to the clear obligations in the relevant laws and regulations. The determination of the legal obligations of the network platform is the basis and premise for the determination of its criminal responsibility. On the other hand, it is difficult for the platform to "know" subjectively. When dealing with illegal information such as Internet rumors, it is a difficult point to determine the criminal responsibility to prove whether the platform knows the illegal nature of the information and intentionally fails. In this context, how to clarify the boundary of platform responsibility and optimize the proof mechanism has become the key proposition to balance network freedom and order maintenance. Based on the local practice, combined with the legislative experience of the United States, Germany and other countries, this paper systematically analyzes the institutional shortcomings of the platform responsibility identification, and puts forward targeted suggestions for improvement, in order to provide theoretical support for the construction of a scientific and reasonable system of network rumor punishment.

## 1 The Harm of the Network Rumor Spread and the Role of the Platform in it

### 1.1 The harm of online rumor spread

The Constitution gives citizens the right to freedom of speech, allowing them to freely express their personal views on hot - button issues in society through diverse channels and means. However, this freedom, while facilitating personal expression, also has [2] potential drawbacks. With the advent of the Internet era[3], Internet rumors have developed into a network phenomenon that cannot be ignored. Internet rumors refer to the

dissemination of information without factual basis through the Internet platform. Network rumors differ from traditional ones due to the Internet, a powerful information - dissemination medium.

First, the spread of the universality. In recent years, the number of Internet users in China is rising, on August 29,2024, China Internet Network Information Center (CNNIC) released the 54th "China Internet development statistical report", the report shows that as of June 2024, the scale of China's Internet [4] users nearly 1.1 billion people (1.09967 billion), an increase [5] of 7.42 million people compared with December 2023, the Internet penetration rate of 78.0%. Second, the concealment of transmission. "The human boundaries of the cyber society will be broken." With the development of social life, any unspecified public can become the maker, disseminator, receiver and even the secondary disseminator of network rumors. Third, the degree of social harm is difficult to control. Internet rumors can break through the boundaries of time and space with the help of the Internet platform, and the social harm is difficult to control. Specifically speaking, it is mainly reflected in the following three aspects: first, the infringement [6] of personal legal interests. In order to attract people's attention, the makers of network rumors often make up, exaggerate and distort the facts to weave misleading false information, which brings serious negative impact to the victims and causes irreversible damage to the personality right of the rumor mongers. Second, it of social legal interests. Due to the universality and speed of network rumors, they can easily cause social panic, destroy social stability and interfere with the normal social order. Cyberspace is not only the "second space" of human activities, but also the "second society" of human life. Once the false information is spread on a large scale on the network, it is easy to make the social order out of control, causing huge social harm. Third, it infringes on the national legal interests. The concealment of network rumor spread makes the process of judicial organs to investigate and collect evidence relatively difficult, and increases the cost of social management.

### 1.2 The role of the network platform in the rumor dissemination

In the digital era, the Internet, as an information dissemination medium, brings more new possibilities for the wide dissemination of discourse, but the resulting "noise" and "dandelion effect" also makes network security face great challenges. With [7] the rapid development of the Internet and AI technology, the universality, concealment and speed of information dissemination has become more and more obvious. These characteristics provide a hotbed for the breeding and diffusion of network rumors, and network rumor incidents occur frequently. For example, the flood in Qinghai caused the death of dozens and thousands of missing people, the fire loss of wind turbines in Karamay, Xinjiang, and the explosion of Southwest University. These events highlight the complexity of the network platform in the rumor dissemination: on the one hand, as the platform, the infrastructure of the information dissemination, facilitates the rapid circulation of information; on the other hand, its technical characteristics also greatly enlarge the diffusion speed and scope of rumors, and become the "accelerator" of the rumor dissemination. This dual attribute of the network platform is not only the intermediary of information dissemination, but also plays the role of content regulator, making it play a key role in the governance [8] of network rumors, the protection of users' rights and interests, and the maintenance of cyberspace order.

Social media platforms not only provide technical support, but also intervene in information dissemination through instant messaging functions, algorithm recommendation, content review and other means. Among them, recommendation algorithms play a key role in rumor dissemination. To increase user engagement and stay time, the platform algorithm tends to recommend content that triggers strong emotional reactions. However, rumors are often novel, controversial and emotional

and inflammatory, and they are easier to gain the favor of algorithms, so as to obtain more exposure and dissemination opportunities. This algorithmic mechanism inadvertently serves as a booster for rumor spreading. The changing role of the [9] Internet platform makes it assume more obligations in the governance of network rumors. As content regulators, [10] network platforms need to review and manage the information released [11] by users to ensure the legitimacy and authenticity of the information. The status of content regulators of online platforms is clarified through a series of laws and regulations. For example, the Network Security Law requires the network platform to prevent and dispose the bad information content to ensure the clear cyberspace ; The Electronic Commerce Law details the content supervision responsibility of the e-commerce network platforms, clarifying the legal responsibility of the network platform in the transaction information management ; the Personal Information Protection Law emphasizes the obligation of the network platform in the protection of user data. In addition, online platforms should also assist law enforcement departments in investigating and dealing with illegal activities to ensure the order and security of cyberspace.

## 2 The Difficult Problem of Determining the Criminal Responsibility of the Network Rumor Platform

### 2.1 The obligations of the network platforms are not clear

In the governance of network rumors, the clarity of the legal obligations of the network platform is the basis and premise of determining its criminal responsibility. At present, although China's relevant laws and regulations have stipulated the obligations of network platforms, their boundaries are still not clear enough, which brings challenges to judicial practice.

The obligations of network platforms in pre - prevention and proactive review are unclear. Although Article 47 of the Network Security Law requires network operators to strengthen user - information management, in practice, such management mainly focuses on establishing and perfecting the internal security management system and operating procedures, to ensure the implementation of network security protection responsibility, and take a series of technical means to defend the computer virus and the occurrence of network attacks. Most of these established security protection measures focus on the technical level of security, and the content of the review level is inadequate. In particular, the current legal system never stipulates the obligation of online rumors and other illegal information for active monitoring, identification and timely deletion, which makes online platforms often fall into the awkward situation of passive response when facing the spread of rumors, and it is difficult to take the initiative and effectively curb the spread of rumors. The root cause is that the current laws lack quantitative provisions on the technical standards and response time limit of the platform content review, which leads to the platform often relying on the passive mode of "reporting-processing". This system design defect is highlighted in the rumor incident of "teacher persecution of 49 Middle School students in Chengdu" fermented on the microblog platform in 2021. The interval from the release of the rumor to the official rumor refuting has exceeded 12 hours, and the number of reposts has exceeded one million times, causing a major adverse social impact.

The obligations of online platforms in assisting law enforcement agencies remain imperfect. As the controller of vast user data and technical - support provider, the network platform should shoulder the corresponding obligation to assist law - enforcement in combating network crimes. However, there are conflicts and contradictions between this obligation to assist law enforcement and the legal obligation of the network platform to protect users' personal information. Take real-name social network platforms as an example, such platforms should not only strictly abide by the principle of user [12] privacy protection to ensure that the security

and privacy of users' personal information are not infringed, but also must respond to the requirements of law enforcement departments and provide specific user information to assist in case investigation. How to find a reasonable balance between maintaining user privacy and cooperating with law enforcement needs has become a major problem facing the current network platform, and also one of the urgent problems to be solved to improve the legal obligations of the network platform. For example, in the track tracking of a map software with epidemic prevention and control in 2021, it also appears that when the platform provides the activity track to the CDC department, the risk of personal information leakage is caused due to the imperfect data desensitization technology. All these cases reveal the structural contradictions in the current system design: it not only requires the platform to act as the "electronic eye" of network governance, but also lacks clear boundaries of authority and operational norms, which makes the platform often fall into the dilemma of "excessive intervention" and "insufficient performance of duties" when fulfilling legal obligations.

### 2.2 Network platform subjective "knowing" proof of difficulties

In the governance of network rumors, defining the "knowing" behavior of network platforms is the key to identify the criminal responsibility. Taking China's special criminal responsibility rules for Internet platforms, that is, the crime of refusing to perform the information network security management obligation added in a part of the Criminal Law Amendment (IX), as an example, the subjective aspect of this crime can only be intentional, and negligence does not constitute this crime. Specifically, the network service provider knows it has the laws and administrative regulations, and knowing that fails to perform these obligations may lead to illegal information dissemination, user information leakage caused serious consequences, criminal case evidence loss such as serious consequences, but still refused to perform the relevant [13] obligations. However, China's law does not clear the specific connotation and identification standard of "knowing", which leads to a variety of interpretation and application methods in judicial practice, such as "should know", "knowing the possibility", "generalize knowing" and so on. This ambiguity makes the judicial personnel enjoy greater discretion in determining whether the platform "knows", which increases the uncertainty and inconsistency of the identification. Although the presumption rule of "knowing" , the presumption rule presumes the existence of subjective knowledge by determining the underlying facts. However, there is a dilemma in the application of the presumptive rule. The presumption rule may lead to a reduction of the standard of proof, making the platform identified as "knowing" if the underlying facts do not meet the "facts are clear and the evidence is indeed sufficient" standard. At the same time, the application scope and conditions of the presumption rules are not clear enough, which can easily lead to the arbitrary discretion of judicial personnel, and further aggravates the confusion of subjective knowing identification.

The proof difficulty of the subjective knowledge will lead to the expansion or limitation of the responsibility of the Internet platform in practice. In order to effectively control online rumors, judicial practice tends to expand the responsibility of the platform through presumption rules, and bring the omission of the platform into the scope of criminal regulations. Such as "li mou some v. a technology co., LTD. Beijing network tort liability disputes" [14], the plaintiff li mou some portrait, name, WeChat ID information by others by the defendant operating the social software into video, content contains pornographic rumors, personal attacks, etc., video spread rapidly after release, more than 30000 views. The plaintiff claims that the defendant should be jointly and severally liable for not timely deleting the infringing content; the defendant argued that as a network service provider, it has fulfilled its legal obligation and the

infringing content is uploaded by the user and is not at fault. In the end, the court combined the characteristics of the surge of video views in a short time (more than 30,000 times a day), and the court assumed that the platform has the technical monitoring ability and can find infringing information through algorithm or manual review. According to Article 1197 of the Civil Code, the platform fails to take necessary measures such as deletion, which constitutes a fault of "should know" and shall be jointly and severally liable with the direct infringer. Although this determination reflects the court's strict requirements on the responsibility of online platforms, such responsibility expansion may also lead to excessive obligations of the platform and restrain its innovation and development. However, the irrationality of the allocation of the subjective aspects of Internet platforms may lead to the limitation of the responsibilities of Internet platforms. According to Article 51 of the Criminal Procedure Law, the burden of proof of the defendant in a public prosecution case shall be borne by the complainant. However, in Internet rumor cases, it is often difficult for the complainants to obtain direct evidence to prove the subjective knowledge of the platform. For example, in the process of spreading online rumors, the platform may hide its cognition of rumors through technical means, making it difficult for the complainant to prove that the platform "knows" the existence of rumors. The irrationality of the distribution of proof burden makes it more difficult to identify the subjective [15] knowledge of the platform in judicial practice, and affects the accurate identification of criminal responsibility. This requires further refinement of the platform's obligations to assist law enforcement at the legislative level, and to balance the relationship between public interest and personal privacy protection.

## 3 Comparison of the Responsibility Regulation of Network Platform

### 3.1 The current situation of the legal liability of the off-domain network rumor platform

From the perspective of international legislation and judicial practice, the treatment of the responsibility of the network platform presents a change process from the initial radical response to the moderate adjustment and regulation through legislation. Take the United States and Germany, for example:

The United States, a representative of the Anglo - American legal system and the birthplace of Internet technology, has developed a relatively complete legislative system for Internet governance[16]. The regulatory model of Internet platform responsibility in the United States has gone through a process from strict responsibility to [17] legislative correction. In the early judicial practice, the court imposed relatively strict tort liability provisions on the network platform. For example, in the 1995 Stratton Oakmont v. Prodigy Services Co. case , the New York State Supreme Court held that because the online platform has edited the user content, it should bear the same strict responsibilities as traditional publishers. However, this strict liability model has had a negative impact on the development of the Internet industry, prompting the United States to correct the platform liability through Article 230 of the Communications Code Act (CDA), which mainly targets Internet defamation. The CDA is a law passed by the US Congress in 1996. One of the highlights of the CDA is the "safe haven principle" stipulated in Article 230, which gives the platform extensive exemption rights. At the same time, three exceptions are stipulated: first, the platform actively intervenes in information dissemination: if the platform actively promotes or participates in the dissemination of illegal content, the "safe haven principle" does not apply. Second, the platform knowingly or intentionally allows the dissemination of illegal content: when the platform knows that users release illegal content and fails to take measures, it may bear legal responsibility. Third, the law or the court order requires the platform to take action, and if the platform fails to fulfill its obligations, it may lose its immunity. Although the CDA does not directly mention online rumors, it sets an obligation of information review

and supervision for online platforms.

As the representative of mainland law system countries, the legal provisions of Internet rumor governance are also of reference significance. The legal responsibility of German online platforms in rumor dissemination is mainly regulated through the Network Enforcement Law (NetzDG). NetzDG It mainly applies to social networking platforms with more than 2 million registered users in Germany, such as Facebook, Twitter and YouTube. According to the Network Implementation Law, social network platforms should assume the following responsibilities and obligations: First, establish a complaint handling mechanism, and platforms must set up clearly visible online reporting forms for users to report illegal content. Second, the time limit for deleting illegal content. Obviously illegal content (such as hate speech and false news) must be deleted or blocked within 24 hours after users report, and other controversial illegal content should be dealt with within 7 days. The third is to stipulate the obligation to preserve the evidence: the platform shall keep the illegal content and its copies for 10 weeks, for criminal prosecution. Fourth, the obligation of periodic reporting is stipulated. The platform shall publish a report every quarter, and shall be released within one month after the end of the quarter at the latest, explaining the number of user complaints received and the handling situation. It also stipulates that online platforms will face penalties if they fail to fulfill their obligations. If the platform fails to meet its obligations, it will face a fine of up to 50 million euros. While setting the fine, the Network Implementation Law treats different platforms of different sizes through the limitation of the number of users. The bill will only apply to social networking platforms that have more than 2 million registered users in Germany. This threshold of "2 million users" not only ensures effective legal constraints on large social platforms, but also avoids overregulation of start-ups or small platforms, thus forming a powerful [18] deterrent to large platforms while protecting innovation.

### 3.2 Localization enlightenment of external experience

The external regulations on the legal liability of online rumor platforms provide many useful inspirations for the governance of online rumors and platform responsibility regulation in China.

First of all, balance the relationship between freedom of speech and network governance, and clarify the legal responsibility of network platforms in the dissemination of rumors. Through the "safe haven principle", the CDA defines the responsibility boundary of the platform on the content published by users, and stipulates the liability of the network platform more carefully and specifically, requiring the platform to establish and implement the policy of "repeated infringer" to prevent the recurrence of infringement. In contrast, although China's Regulations on the Protection of the Right of Information Network Communication also stipulates the obligation of "notice-deletion", it does not specify the general conditions similar to the policy of "repeated infringer", which makes it difficult to effectively curb the repetition of infringement. China can learn from foreign ideas, clarify the responsibility boundaries of Internet platforms, and strengthen the protection of network platforms.

Secondly, strengthen the self-discipline ability of the platform and optimize the supervision of the platform. Germany's Internet Implementation Law passes strict platform liability regulations, requiring platforms to delete illegal content in time after discovery, or they will face high fines. The combination of this "notification-deletion" mechanism with strict legal responsibility not only strengthens the management obligation of the platform, but also provides a powerful grasp for the governance of network rumors. Similarly, the EU's Digital Services Act (DSA) requires platforms to proactively monitor and review content posted by users and impose high fines on platforms that fail to fulfill their obligations. China can learn from the experience of outside the region, further improve the active review obligation of platforms, clarify the time limit and standards for platforms to handle

rumors after discovering them, and ensure that rumors can be contained and eliminated in a timely manner.

Finally, the experience of foreign legislation reveals that China should pay attention to the combination of technical means and legal regulation in the governance of network rumor. The Communication Code Act, through the principle of technology neutrality in the United States, encourages platforms to use technology to filter and manage content, rather than relying solely on manual review. This technology-driven governance model not only improves efficiency, but also reduces the operating costs of the platform. China can learn from this experience and promote platforms to use artificial intelligence, big data and other technical means to establish a more intelligent rumor identification and disposal system.

## 4 Suggestions on Perfecting the Criminal Responsibility of the Network Rumor Platform

### 4.1 Define the boundary of the platform obligations

As the carrier of the Internet information dissemination, the network platform not only has the right to manage the information, but also undertakes the obligation to maintain the network information security. As the last line of defense to maintain social fairness and justice, criminal law has a strong deterrent means of criminal punishment, but it should follow the principle of modesty and should not be easily used unless necessary. “In cases of online rumors, online platforms do not always bear criminal liability. When a rumor - spreading incident occurs, it must first be confirmed that the rumor - spreading activities actually utilize platform resources like Weibo or TikTok. Secondly, online rumor spreading and rumor spreading must cause serious social harm, and should be supported by sufficient evidence. Finally, the identification of criminal responsibility of the platform should meet the relevant conditions of omission of crime. Therefore, clarifying the obligation boundary of the network platform is the basic premise to determine the illegality of its behavior.

On the one hand, the technical standard and the response time are further quantified. In the context of information technology, China can consider using artificial intelligence and other technical means to clearly stipulate the platform's active obligation to review online rumors in the Network Security Law, Data Security Law and other regulations, requiring the platform to establish a dynamic monitoring system based on semantic analysis and artificial intelligence. At the same time, the technical standards for quantitative rumor identification, such as the update cycle of keyword database, the identification accuracy threshold of AI model, etc., and specify the response time. For example, after the rumor spread reaches a certain magnitude, the platform needs to start the disposal process within 24 hours. This quantitative regulation of technical standards [19] and response time limit can not only provide clear operational guidance for the platform, but also enhance the enforceability and deterrence of the law. In addition, the relevant provisions of the German Telecommunications Media Act (TMG). Different types of service providers assume different degrees of responsibility. Based on the ability to control the facts, TMG divides different levels of responsibility, and constructs a responsibility framework for network service providers with both general principles and concrete rules. Stones from other hills may serve to polish the jade. According to the specific functions of the network platform, China can divide the platform into "technical service providers" (such as China Telecom, China Mobile, China Unicom, etc.) and "content service providers" (now Japanese tiao, Tencent News, Netease News, etc.), so as to distinguish the differences between their obligations. The former, such as Deepseek, is based on the "safe haven principle" and only needs to fulfill the post-remedial obligation; the latter needs to assume a higher responsibility for active review, such as establishing a "secondary audit" mechanism for reprinting information on aggregated platforms.

On the other hand, to coordinate the conflict between

law enforcement cooperation and privacy protection. Formulate operation norms for data retrieval, clarify the authority boundary for the platform to cooperate with law enforcement agencies [20] to obtain user data, require the retrieval procedures to comply with the "minimum necessary [21] principle" of the Personal Information Protection Law, and stipulate the technical standards for security measures such as data desensitization and encrypted transmission. For example, when assisting in the retrieval of real-name information, on the basis of the "special notification + separate consent" procedure, the zero-knowledge proof technology is used to ensure that only the necessary fields are provided. At the same time, the type of personal information can be controlled by stratification. The authority constraint that distinguishes according to the information type is the key to clarifying the authority boundary. For example, the acquisition of communication secrets stored on the platform should be subject to constitutional reservation, and strictly observe the purpose, subject and procedural requirements set by the Constitution. For general information and public information, simple legal reservation applies; for sensitive information, "aggravated legal reservation" shall be applied, that is, when the government is required to obtain sensitive information stored on the platform, not only with legal authorization, but also for specific purpose and method.

### 4.2 Clarify the subjective "knowing" judgment of the network platform and the distribution of the burden of proof

Under the background of network rumor governance, it is the key to clarify the judgment standard of "knowing" to improve the criminal responsibility identification mechanism of "knowing". In the spread of online [22] rumors, the "knowing" of the platform usually means that the information spread is false and may cause harm to society. The knowledge of rumors on network platforms usually depends on multiple factors, but they are all vague. This paper believes that "knowing" can be divided into "actual knowing" and "should know": "actual knowing" requires direct evidence. If the platform fails to timely deal with the report or deletion of the specific rumor content requested by users or regulatory authorities, it can be regarded as "knowing". For example, a user repeatedly reported that a post contained false epidemic information, and the platform did not delete it and did not report it to the Internet and information department. This behavior indicates that the platform has a clear understanding of the existence of rumors, but does not take measures, so it should be identified as "knowing". At the same time, the identity of the publisher, the historical record of the published content, the frequency of the release, and whether the platform has taken reasonable measures to review and supervise, are all important factors to judge whether [23] the platform "knows". For example, if a user has posted false information many times and is dealt with by the platform, but the platform does not review the similar content in its subsequent release, the platform can be presumed to be "knowing". In addition, the platform's internal audit records and employee testimonies can prove the platform's actual recognition of specific illegal information."Should know", the platform should fulfill its duty of care through objective behavior. For example, when the platform algorithm actively recommends, sets the top or the commercial cooperation content involves illegal information, it directly presumes that the platform has subjective knowledge and strengthens the obligation constraints on the traffic-driven platform. But we should avoid "one size fits all" to increase the burden of the platform. A list of differentiated obligations of care should be developed according to the platform scale, technical capabilities, and content types (such as social networking, e-commerce, and short video). In addition, the above mentioned "li mou some v. a technology co., LTD. Beijing network tort liability dispute" presumption platform "should know" judicial precedents, while affirming its positive significance, also should pay attention to, to balance the responsibility and protection of rights

and interests platform, to "should know" presumption must strictly follow the principle of proportion, only in accordance with two or more legal objective situations (such as abnormal transmission amount, repeated records, active intervention, algorithm, etc.) can start, avoid a single index trigger excessive burden platform.

In the governance of online rumors, it is the key to the identification of criminal responsibility to clarify the "knowing" responsibility of online platforms. However, in the current judicial practice, the prosecution faces many difficulties in proving that the platform "knows". This paper believes that the following two aspects can be considered: First, optimize the distribution of the burden of proof: implement the "preliminary proof-proof transfer" mechanism. In online rumor cases, the prosecution often needs to prove that the platform has the objective possibility of finding illegal information. For example,the platform should know the existence of rumors through basic facts such as the amount of content dissemination and the frequency of reports. However, this burden of proof is heavy for the prosecution, especially in the face of complex network technology and huge amounts of information. To this end, the mechanism of "preliminary proof-proof transfer" mechanism can be introduced, and the prosecution should prove that the platform has the objective possibility of finding illegal information, such as that the platform should know the existence of rumors through basic facts such as the amount of content dissemination, frequency of reports and keyword matching. These underlying facts can be used as preliminary evidence that the platform has an obligation to further investigate and address related rumors. Once the prosecution has completed the preliminary proof, the burden of proof shifts to the platform. The platform shall provide audit records, algorithm rules, technical capabilities and other evidence to prove that it has taken reasonable measures to prevent the spread of rumors, or that it cannot know the existence of rumors. For example, the platform can provide the operation records of its AI audit system, the detailed description of the manual audit process, and the processing records of the reported information. On the premise of not breaking through Article 51 of the Criminal Procedure Law, this mechanism alleviates the proof dilemma of the prosecution through the reasonable distribution of the burden of proof. This mechanism not only improves the judicial efficiency, but also ensures that the platform takes a proactive attitude in the face of rumors. Secondly, in the network rumor cases, technical problems often become the key factor to identify the responsibility of the platform. However, these issues are more professional, and it may be difficult for ordinary judges and jurors to accurately understand and judge them. In order to solve this problem, we can explore the "expert jury" participation system. In criminal cases involving online platforms, technical experts are introduced as jurors. They can assess whether the platform's algorithm rules are reasonable, whether the data processing meets industry standards, and whether the platform has the technical ability to find rumors, etc. These assessments will assist judges to more accurately judge whether the platform has the technical cognitive conditions of "knowing". In addition, in order to ensure that the evidence is destroyed, the relevant provisions of the German Network Implementation Law can be used to clarify the obligation of the platform to preserve evidence and the obligation of regular reporting. At the same time, the "blockchain" technology can be used to force the platform to store the content audit log, user report records and other data on the chain in real time, so as to ensure that it cannot be tampered with during judicial evidence collection. This technology not only improves the credibility of the evidence, but also can effectively prevent the loss or tampering of the evidence.

## 5 Epilogue

The definition of criminal responsibility of network platform needs to balance the dual value of freedom of speech and order maintenance. By analyzing the dilemma of platform obligation ambiguity and "knowing", this

paper puts forward suggestions on quantitative standards and optimizing the distribution of burden of proof, and emphasizes the coordination between technical means and legal regulation. Future research can further explore the application of artificial intelligence in rumor identification and the construction of transnational governance mechanisms, so as to realize long-term governance in cyberspace.

## Reference


[1] See Sun Daocui, Thinking and Path of Criminal Sanctions for Online Platform Crimes, Oriental Law, no. 3,2017, p. 85.

[2] See Liu Xianquan: The Construction and Improvement of the Criminal Regulation System of Online Rumors and spreading Rumors, jurists, no. 6,2016, p. 106.

[3] See Shen Changxiang, Zuo Xiaodong, Information Security, Zhejiang University Press, 2007, p. 107.

[4] China Internet Network Information Center (CNNIC). The 54th Statistical Report on Internet Development in China (2024-8-29) [2024-8-30]. Link:https://www.cnnic.cn/n4/2024/0829/c88-11065.html

[5] See Yang Zhengming, Research on CyberCrime, Shanghai Jiao Tong University Press, 2004, p. 3.

[6] See Yu Zhigang, The Era of All Media and Sanctions on fabricating and DisseminFalse Information, Legal Review, No.2,2014, p. 93.

[7] See Fan Xiaoling, Liu Yonghou, Influential Factors, Causes and Solution Path of the Production and Communication of National Discourse, Journal of Shanghai Jiao Tong University (Philosophy and Social Sciences Edition), No.1,2025, pp. 44-45.

[8] See Zhou Hui: "Supervision of Online Platforms and Their System Improvement from the Perspective of Double Order", Legal Science (Journal of Northwest University of Political Science and Law), no. 6,2024, pp. 49-52.

[9] Article 47 of the Cyber Security Law.

[10] Article 38 and Article 29 of the E-commerce Law.

[11] Article 51 of the Personal Information Protection Law.

[13] See Chen Qingan, Concept, Path and Scheme of Criminal Governance of Online Rumors, Legal Science (Journal of Northwest University of Political Science and Law), no. 3,2024, pp. 160-161.

[14] For example, Article 11 of the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of the Law to Handling Criminal Cases such as Illegal Use of Information Network and Helping Information Network Criminal Cases (No.15,2019). Interpretation (28 of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Specific Application of Law in Handling Criminal Cases of Making, Copy, Publishing, Selling and Disobobscene Electronic Information Using the Internet, Mobile Communication Terminal and Voice Platform (2) (No.3,2010).

[15] From the case database of the people's court, the database number: 2024-14-2-369-001

[16] See Zhou Hui: "Obligations and Responsibilities of Platforms in Network Governance", Chinese Journal of Social Sciences, No.1203, September 15,2017.

[18] See Xie Yaowen, On the Responsibility Regulation Model of American Internet Platforms, Administrative Law Research, no. 3,2018, pp. 133-144.

[19] Supreme Court, Nassau County, New York, Trial IAS Part 34.May 24, 1995.

[20] See Jia Yin: Germany's "Network Implementation Law" Regulatory Storm , China Information Security, no. 2,2018, pp. 77-79.

[21] See Wang Huawei, The Transmutation and Enlightenment of German Network Platform Responsibility, Peking University Law Review, No.1,2018, p. 126.

[22] See Ma Yun: The Structure and Boundary of Data Power of Government Acquisition Platform, Journal of Shanxi University (Philosophy and Social Sciences Edition), No.2,2024, pp. 49-53.

[23] Zero-knowledge proof is a cryptographic technique that allows the demonstrator to prove the authenticity of a statement to the verifier without revealing any actual information. The core idea is that the verifier can be sure that a statement is true, but can't know why.

[24] See Feng Li, "The Scope and boundary of Government Regulation of Online Rumors in the context of COVID-19", Journal of Dongbei University of Finance and Economics, no. 6,2021, pp. 88-92.

[25] See Zhou Hui: "Obligations and Responsibilities of Platforms in Network Governance", Chinese Journal of Social Sciences, September 15,2017, No.1203.