Academic Journal of History and Culture
ISSN: 3081-0000 (Print), ISSN: 3081-0019 (Online) | Vol. 1, No. 2, 2026

The Legal Framework for Online Reputation Protection in China: Challenges and Regulatory Mechanisms

Fangnan Chen

North China University of Technology, Beijing 100144, China

Abstract: The Internet has long been the main position for people to express their opinions, but the abuse of the right to freedom of expression on the Internet makes the infringement of network reputation more and more intense. Therefore, how to balance the conflict of rights between network reputation and network freedom of speech rights, to establish a reasonable regulation of the law, and to clarify the boundaries of network speech rights has become a hot issue of current concern. First of all, this paper puts forward several types of cases that are easy to produce reputation disputes in China's network environment, and then further explores the reasons for the conflict between the two through the common focus of dispute in these cases. In order to establish a balanced rule of checks and balances for the conflicts between the two, China should improve the boundary between online reputation infringement and online freedom of expression in its legislation, so as to strengthen the protection and restriction of the two rights.

Keywords: Online reputation Protection, conflict, regulation.

1. Introduction

In the era of big data, the network and people's connections are becoming increasingly inseparable, and in recent years, there have been frequent cases of online reputation infringement on major online social platforms, and the right to online reputation inevitably conflicts with the right to freedom of expression of online users. Therefore, we need to make further research on how to coordinate the citizens' right to freedom of expression and the conflict caused by freedom of expression. This paper will combine the relevant judicial practice in China, discuss how to identify the infringement of the right to reputation in the network, the current boundaries between the right to reputation and the right to freedom of expression in China, and analyze how to balance the conflict between the right to freedom of expression and the right to reputation in the network. Online reputation refers to the social evaluation and public perception of an individual or organization in cyberspace. Unlike traditional reputation disputes, online reputation infringement is characterized by rapid dissemination, anonymity, cross-platform transmission, and long-lasting influence.[1] False statements, malicious rumors, cyberbullying, and manipulated online content can severely damage a person's social standing, mental health, and professional opportunities within a short period of time.

In recent years, China has witnessed a growing number of disputes involving online defamation, cyberbully, "human flesh searches," deepfake technology, and the malicious spread of rumors on social media platforms. As a result, online reputation protection has become an important issue in Chinese cyberspace governance and civil law protection. To address these issues, China has gradually developed a relatively comprehensive legal framework involving civil liability, administrative regulation, criminal punishment, and platform governance obligations. This paper aims to analyze the evolution of China's legal framework for online reputation protection, examine the major legal challenges in practice, and evaluate existing regulatory mechanisms.

2. Background

Before the emergence of the internet era, reputation protection in China primarily relied on traditional civil law doctrines concerning personality rights. Reputation rights were recognized as a fundamental component of personal dignity and social evaluation, deeply rooted in both legal statutes and societal values. The General Principles of Civil Law (1986) explicitly stipulated the protection of citizens' and legal persons' reputation rights, prohibiting any form of defamation, false accusation, or public insult. Subsequently, the Tort Liability Law (2010) provided more comprehensive legal remedies for acts of defamation and reputation infringement, including provisions for fault-based liability, joint torts, and measures to stop ongoing infringement. Under this traditional legal framework, victims of reputation harm could request cessation of the infringing act, restoration of reputation, a public apology, and compensation for actual damages, including both economic losses and moral damages in severe cases. Court proceedings generally followed established evidentiary rules, where the plaintiff bore the burden of proving the defamatory nature, publication, and actual harm caused by the defendant's conduct. Moreover, judicial interpretations from the Supreme People's Court further clarified the standards for determining defamation, such as the distinction between opinion and fact, and the privileged status of certain official statements or fair comments on public issues. However, these traditional legal rules were primarily designed for offline disputes, typically involving limited circulation of information (e.g., local newspapers, public speeches, posters) and relatively clear chains of attribution and harm. Consequently, they could not fully address the unique characteristics of cyberspace communication, where information flows instantaneously across jurisdictional boundaries and anonymous users can republish content without accountability. The rapid development of internet technologies since the late 1990s, particularly the rise of Web 2.0 platforms in the 2000s, significantly changed the nature of reputation infringement. Social networking platforms such as Weibo (launched in

2009), WeChat (2011), and short-video applications like Douyin (the Chinese version of TikTok, 2016) enabled information to spread instantly to millions of users, often outpacing the ability of victims or platform moderators to respond. For example, a single defamatory post on Weibo could be forwarded tens of thousands of times within hours, with each share adding layers of commentary and emotional charge, thereby amplifying the reputational harm exponentially.

Several factors have intensified online reputation risks in China, making the traditional legal framework inadequate. First, the anonymity of internet users—while not absolute due to real-name registration requirements imposed on major platforms—still allows many individuals to create pseudonymous or secondary accounts, making it difficult to identify the original source of defamatory content. Second, the low cost of information dissemination means that anyone with a smartphone can publish content to a vast audience at near-zero marginal cost, leading to a flood of unverified or malicious statements. Third, algorithmic recommendation systems, which power content distribution on platforms like Toutiao (Jinri Toutiao) and Kuaishou, often prioritize engagement metrics such as clicks, comments, and shares, thereby inadvertently promoting sensational or controversial content—including defamatory material—over neutral or corrective information. Fourth, emotional amplification on social media, driven by features such as likes, angry emojis, and threaded comments, encourages users to react quickly and often aggressively, fueling the rapid spread of hostile or defamatory narratives. Fifth, the permanent digital storage of harmful content through search engine caches, internet archives, and screenshots means that even if the original post is deleted, copies may continue to resurface, causing recurring harm to the victim's reputation years after the initial incident.In addition, emerging technologies such as artificial intelligence and deepfake technology have further complicated online reputation protection by enabling the creation of highly realistic fabricated images, videos, and audio recordings. Deepfake algorithms, which use generative adversarial networks (GANs) or diffusion models, can produce synthetic media that convincingly depicts a person saying or doing something they never actually did. For instance, a malicious actor could generate a fake video of a public figure making inappropriate remarks, or a doctored audio clip impersonating a private individual giving false testimony. Such content is often indistinguishable from authentic recordings to the naked eye or ear, making it extremely challenging for courts and platform administrators to verify truthfulness in a timely manner. Moreover, the same AI technologies can be used to automate the creation of defamatory content at scale, such as generating thousands of unique negative comments or fake news articles targeting an individual or organization. While China has enacted laws like the Personal Information Protection Law (2021) and the Deep Synthesis Provisions (effective 2023) that impose obligations on deep synthesis service providers—including labeling synthetic content and obtaining consent from subjects—enforcement remains difficult due to cross-border data flows, rapid technological evolution, and the ease with which deepfakes can be shared via encrypted messaging apps. Consequently, the protection of reputation in China's internet era requires not only an adaptation of traditional civil law doctrines but also new regulatory frameworks, platform governance mechanisms, and forensic tools for detecting and removing AI-generated defamatory content.

3. China's Legal Framework for Online Reputation Protection

The enactment of the Civil Code of the People's Republic of China marked a major development in online reputation protection. The Civil Code formally established an independent chapter on personality rights and strengthened legal protection for reputation, privacy, and personal information. Under the Civil Code of China, individuals enjoy the right to reputation, and no organization or individual may infringe upon this right through insult, defamation, or dissemination of false information. Victims of online reputation infringement may request deletion of harmful content, cessation of infringement, restoration of reputation, public apology, and compensation for economic and emotional damages. [3] The Civil Code also introduced stronger protections for personal information and privacy, which are closely connected to online reputation protection in cyberspace. In addition, the Cybersecurity Law of the People's Republic of China imposes important obligations on network operators and internet platforms. Platforms are required to monitor illegal online information, remove unlawful content, cooperate with government authorities, establish complaint and reporting mechanisms, and preserve user data when necessary. Under the "notice-and-takedown" mechanism, platforms may bear legal liability if they fail to remove infringing content after receiving notification from victims. This framework significantly strengthens platform responsibility in online reputation governance. The Personal Information Protection Law further enhances protection against misuse of personal information and online harassment. The law regulates the collection, processing, and dissemination of personal information and requires platforms to follow principles of legality, necessity, and good faith. The unauthorized disclosure of personal information often contributes to cyber violence and reputational harm. Therefore, personal information protection has become closely linked with reputation protection in cyberspace. In severe cases, online defamation may constitute criminal offenses under Chinese criminal law. Judicial interpretations issued by the Supreme People's Court of China and the Supreme People's Procuratorate clarify that online defamation involving serious consequences or widespread dissemination may result in criminal liability. This demonstrates China's increasingly strict approach toward malicious online behavior and cyber violence.

4. Regulatory Mechanisms and Future Improvements

To improve online reputation protection, China should continue strengthening platform responsibilities and regulatory mechanisms. Internet platforms should establish more effective content moderation systems, reporting procedures, and rapid response mechanisms for removing harmful content. Artificial intelligence technologies may also assist platforms in identifying deepfakes, malicious rumors, and cyber violence more efficiently. At the judicial level, courts should further improve online evidence preservation rules and simplify litigation procedures for cyberspace disputes. [4] The continued development of specialized internet courts may also help improve judicial efficiency and professionalism in handling online reputation cases.

Moreover, effective online reputation governance requires cooperation among governments, courts, internet companies, industry associations, and users. Public legal education and digital literacy programs should be strengthened to reduce irrational online behavior and enhance public awareness of legal responsibilities in cyberspace. Given the global nature of internet communication, China should also strengthen international cooperation regarding data governance, cross-border platform regulation, and enforcement against online defamation. International collaboration is increasingly necessary to address jurisdictional conflicts and ensure effective protection of reputation rights in the digital era.

AI may also assist platforms in identifying deepfakes, malicious rumors, and cyber violence more efficiently. AI-powered tools, such as neural networks trained on large datasets of authentic and manipulated media, can detect subtle inconsistencies in lighting, facial movements, or audio waveforms that are imperceptible to human viewers. For example, deepfake detection algorithms can flag synthetic videos by analyzing unnatural blinking patterns or artifacts generated during the creation process. Similarly, natural language processing (NLP) models can scan millions of posts in real time to identify potentially defamatory statements, classify them by severity, and even predict their potential spread. Machine learning systems can also detect coordinated inauthentic behavior, such as botnets or brigades that mass-report or mass-amplify certain content to cause reputational damage. However, AI is not a panacea; false positives and negatives remain challenges, and over-reliance on automation may suppress legitimate speech or miss novel forms of manipulation. Therefore, AI should be used as an assistive tool augmented by human judgment, especially in borderline or context-sensitive cases. Platforms should also be required to disclose their use of AI in content moderation and to allow users to appeal automated decisions. Moreover, as generative AI continues to improve, platforms must invest in continuous research and development to keep detection methods ahead of adversarial techniques, including those used to produce hyper-realistic deepfakes or voice clones. At the judicial level, courts should further improve online evidence preservation rules and simplify litigation procedures for cyberspace disputes. Traditional evidence rules often require original documents or physical exhibits, but online defamation exists as digital data—screenshots, server logs, metadata, and hashed timestamps—that can be easily altered or deleted. Therefore, courts should adopt standardized protocols for collecting and authenticating electronic evidence, including the use of blockchain-based notarization services that can fix the content, time, and source of online posts. China's internet courts in Hangzhou, Beijing, and Guangzhou have already piloted such technologies, allowing plaintiffs to upload encrypted evidence directly to the court's platform. Expanding these practices nationwide would reduce evidentiary hurdles for reputation victims. Additionally, litigation procedures should be simplified: for example, by allowing small-value reputation claims to be resolved through expedited online mediation or arbitration, rather than requiring full trial processes. Courts could also develop model complaint forms and automated case assignment systems for defamation cases, reducing legal costs and time delays. The continued development of specialized internet courts may also help improve judicial efficiency and professionalism in handling online reputation cases. These courts, staffed by judges trained in both law and technology, are better equipped to understand complex issues such as algorithm-driven amplification, anonymity tracing, and cross-platform data flows. They can also issue more consistent rulings on novel questions—such as whether a deepfake constitutes defamation if it does not use the victim's real name but makes them identifiable by context. Expanding the jurisdiction of internet courts to cover all online reputation disputes, and enabling them to enforce judgments against non-compliant platforms or anonymous users (via orders to internet service providers for identity disclosure), would further strengthen the protective framework. Moreover, effective online reputation governance requires cooperation among governments, courts, internet companies, industry associations, and users. No single actor can solve the problem alone. Governments at the central and local levels should coordinate policies to avoid conflicting regulations, while courts provide judicial interpretations that clarify the boundaries of lawful speech versus defamation. Internet companies must not only comply with regulations but also proactively design their platforms to reduce reputational risks—for example, by introducing cooling-off periods for highly emotional content or requiring identity verification for users who wish to post about specific individuals. Industry associations, such as the Internet Society of China, can develop voluntary codes of conduct, share best practices, and facilitate cross-platform dialogue. Users, as both potential victims and potential infringers, play a dual role: they should be empowered to report violations easily, but also educated about the consequences of spreading unverified claims. Public legal education and digital literacy programs should be strengthened to reduce irrational online behavior and enhance public awareness of legal responsibilities in cyberspace. Schools, community centers, and media outlets can offer training on how to identify misinformation, understand defamation laws, and respect others' dignity online. Special campaigns could target high-risk groups, such as adolescents and senior citizens, who may be both vulnerable to reputational harm and prone to sharing harmful content unknowingly. Furthermore, employers and professional organizations can incorporate digital ethics modules into continuing education, helping to foster a culture of accountability that supplements formal legal sanctions.

Given the global nature of internet communication, China should also strengthen international cooperation regarding data governance, cross-border platform regulation, and enforcement against online defamation. Reputation attacks often originate from servers or users located in foreign jurisdictions, making it difficult for Chinese courts to assert personal jurisdiction or to serve legal process. International collaboration is increasingly necessary to address jurisdictional conflicts and ensure effective protection of reputation rights in the digital era. Bilateral and multilateral agreements could establish mutual legal assistance procedures for obtaining user identification data from foreign platforms, as well as frameworks for recognizing and enforcing court judgments involving online defamation. China could engage with organizations such as the International Telecommunication Union (ITU), the World Trade Organization (WTO), or the G20 Digital Economy Working Group to develop harmonized standards for content moderation and cross-border takedown requests. Moreover, cooperation with regional partners—especially in East Asia and the Belt and Road Initiative countries—could lead to joint task forces against cyber harassment and reputation-based

crimes. At the same time, China should participate actively in global dialogues on balancing free expression with reputation protection, ensuring that its domestic approaches are both effective and compatible with international human rights norms. Finally, information-sharing mechanisms among national cybersecurity agencies can help track and disrupt transnational disinformation campaigns that aim to harm the reputations of individuals, organizations, or even governments. Without such international cooperation, malicious actors will continue to exploit jurisdictional gaps, safe harbors, and conflicting laws to inflict reputation damage with impunity.

5. Conclusion

The rapid development of digital technologies has greatly increased the complexity of online reputation protection in China. In response to the growing risks of cyber violence, online defamation, and algorithm-driven dissemination, China has gradually established a comprehensive legal framework combining civil law protection, administrative regulation, criminal sanctions, and platform governance obligations. [5] Although the current system has achieved significant progress, substantial challenges remain, including anonymous infringement, platform algorithm amplification, and the tension between reputation protection and freedom of expression. In the future, China should continue improving its legal framework, strengthening platform accountability, enhancing judicial remedies, and promoting international cooperation in cyberspace governance. Only through a balanced and comprehensive regulatory approach can online reputation rights be effectively protected while maintaining an open and dynamic digital environment.

References

[1] Creemers, R., & Trevaskes, S. (2017). Cyber China: Upgrading propaganda, public opinion work and social management. *Journal of Contemporary China*, *26*, 85.

[2] Chen, Y. (2022). The development of China's network and data security laws: A new phase of Chinese internet regulation. *Computer Law & Security Review*, *44*, 105654.

[3] Greenleaf, G.. (2021). China's Personal Information Protection Law: Full analysis. *Privacy Laws & Business International Report*, *177*, 1.

[4] Ge, J., & Chen, L. (2022). The Chinese Civil Code's impact on the protection of virtual reputation in China. *Asia Pacific Law Review*, *29*, 366.

[5] Chen, G. (2022). How equalitarian regulation of online hate speech turns authoritarian: A Chinese perspective. *Journal of Media Law*, *14*, 159.