International Journal of Law and Politics Studies
ISSN: 2709-0914
DOI: 10.32996/ijlps
Journal Homepage: www.al-kindipublisher.com/index.php/ijlps

IJLPS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Identification and Countermeasures of Network Defamation Crime: Present Situation, Supervision Status, and Criminal Applications

Renze Qu
Wuxi Foreign Language School, Wuxi 214031, China
Corresponding Author: Renze Qu, **E-mail**: 3305725811@qq.com

| ABSTRACT
The network defamation crime presents a serious legal quandary in the digital age. This paper delves into the identification, supervision, criminal applications, and countermeasures of the network defamation crime. First, we clarify the constitutive requirements of the crime and propose a meticulous standard to balance freedom of speech with safeguarding individuals' rights and interests. Second, we establish an effective onus of proof, thereby alleviating the plaintiff's load and expediting the judicial process. Simultaneously, we emphasize combating false information to uphold the integrity of cyberspace and further explore the intricate impact of network environments' anonymity and virtuality on evidence collection, as well as the balance between freedom of speech and individual rights. Finally, this paper puts forward the establishment of transnational cooperation mechanisms and the oversight of social media platforms as a comprehensive strategy to effectively tackle the global challenges in the network defamation crime and contributes valuable insights and suggestions for the wholesome development of cyberspace through detailed discussion.

| KEYWORDS

Network defamation crime; Supervision; Criminal applications

| ARTICLE INFORMATION

ACCEPTED: 04 September 2023 **PUBLISHED:** 23 September 2023 **DOI:** 10.32996/ijlps.2023.5.5.6

1. Introduction

With the rapid development of Internet technology, the network defamation crime has garnered intense scrutiny within the realm of law. This paper aims to systematically explore the identification standards and countermeasures of the network defamation crime, thereby providing theoretical support and practical reference for legal practice and social governance. In the information society, the network defamation crime significantly impacts personal dignity and social harmony, making its identification standards the core of law application. This paper starts with identifying the characteristics of the network defamation crime, delves into its similarities and differences with traditional defamation, and explores its constitutive requirements and judicial interpretation to lay a solid foundation for legal identification. Meanwhile, this paper acknowledges the divergent approaches to identifying such crimes across different jurisdictions and analyzes the culture, values, and legal traditions behind these disparities, facilitating the establishment of a rationalized international standard. The prevention and treatment of crime necessitates both legal mechanisms and diversified social cooperation. This paper not only discusses the role of social media platforms in supervising online speech but also deeply studies their self-discipline mechanism, information review, and swift responsiveness to provide practical suggestions for fortifying the cyberspace order. Additionally, this paper examines the legal difficulties posed by the application of the network defamation crime, particularly concerning the balance between freedom of speech and individual rights, to ensure the harmonization of public interests and individual rights. Through in-depth discussion on the identification and countermeasures of network defamation crime, this paper aspires to furnish intellectual support for building a robust legal system and a holistic social governance system. Its positive and far-reaching significances encompass the advancement of a wholesome cyber domain,

Copyright: © 2022 the Author(s). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) 4.0 license (https://creativecommons.org/licenses/by/4.0/). Published by Al-Kindi Centre for Research and Development, London, United Kingdom.

the preservation of the social order and ethical standards, and the reinforcement of human rights safeguarding and judicial integrity (Men, 2017).

2. Identification of the Network Defamation Crime

2.1 Definition and Characteristics of the Network Defamation Crime

The network defamation crime refers to the illegal act of fabricating, derogating, and attacking others through malicious and insulting words, images, sounds, or other media in the digital sphere (Fan, 2016). Its first striking characteristic is the rapidly spreading information. Through the Internet platform, speech can traverse the globe instantaneously, which aggravates the repercussions of insults and defamations. Secondly, network defamations often exploit the veil of anonymity, rendering tracking and prosecution arduous and consequently cloaking the crimes in secrecy (Sun, 2021). Furthermore, the victims subjected to the crime range widely from individuals to enterprises, whose social reputation may be damaged, underscoring the escalating social detriment of the crime. The identification of the network defamation crime necessitates a precise delineation of its constitutive elements and clarifies the balance with freedom of speech to ensure the protection of legitimate speech rights while combatting crimes. A profound comprehension of the definition and characteristics of the network defamation crime is pivotal in constructing a robust legal and social mechanism and upholding the integrity and justice of cyberspace (Xu, 2016).

2.2 Identification Standards of the Network Defamation Crime in Different Jurisdictions

There are significant disparities in the identification standards of the network defamation crime in different jurisdictions, which stems from the influence of multiple factors such as legal systems, cultural backgrounds, and social values in various countries.

First, variations exist in the constitutive requirements of the network defamation crime across diverse jurisdictions. Some countries focus on the malicious intent or fictional nature of the language used, while others prioritize whether the words actually harm an individual's reputation. This divergence can mirror distinct national inclinations toward striking a balance between safeguarding personal dignity and upholding the principles of freedom of speech (Liu & Zhang, 2018). Second, the degree of criminal responsibility for the network defamation crime has also changed within various countries. Some jurisdictions classify it as a criminal offense resulting in a criminal penalty, while other countries lean towards civil litigation, underscoring the compensation rights of victims. These disparities illuminate the differences in the application of laws in various jurisdictions. In addition, the treatment of anonymity also emerges as a significant quandary. Certain countries have instituted stringent identification mechanisms to trace individuals disseminating insulting and defamatory remarks. However, other countries may pay more attention to safeguarding freedom of speech, fostering a more lenient stance towards anonymity (Huang & Hu, 2013). Finally, there are differences in the supervision of social media platforms in various jurisdictions. In some countries, platforms are obligated to rigorously scrutinize user-generated comments to curb insults and defamation, while other countries may permit platforms greater operational freedom and assign them a varying degree of responsibility.

3. Supervision Status of the Network Defamation Crime

Under the background of Internet popularization, the supervision status of the network defamation crime has become notably urgent and vital in China. Firstly, China has codified the network defamation crime in its criminal law. According to Article 246 of China's Criminal Law, anyone disseminating fabricated falsehoods or engaging in insults or defamations online, under circumstances of gravity, shall be investigated for criminal responsibility. This provision furnishes a lucid legal foundation for the crackdown on network defamations (Ying, 2012). Secondly, China has strengthened its efforts in supervising the network defamation crime. Law enforcement departments, including public security organs, have intensified their endeavors to combat network defamations and enhanced collaboration between the online and offline domains. Social media platforms have also actively cooperated to reinforce user identity verification and the real-name system to better track content publishers. Moreover, China has also established a network reporting platform, affording the public a seamless channel to report online insults and defamations. This avenue facilitates prompt detection, investigation, and mitigation of such occurrences. Simultaneously, the relevant departments regularly publicize their investigations and sanctions against network defamations, thereby amplifying public awareness of these issues (Sun, 2010).

However, the supervision of the network defamation crime in China encounters certain challenges. On the one hand, the anonymity of cyberspace often enables content publishers to elude responsibility, rendering their tracking a formidable task. On the other hand, the legal standards delineating network defamations still need increased precision and specificity to prevent excessive restrictions on legitimate speech.

4. Issues and Challenges in Criminal Applications of the Network Defamation Crime

The network defamation crime presents a myriad of complicated legal and evidentiary challenges during its application, which involves various facets such as the precise delineation of the crime's standard, assurance of evidence credibility, and balance between freedom of speech and individual rights.

4.1 Establishing Clear and Specific Standards for the Network Defamation Crime

Defining the standard for the network defamation crime proves to be an intricate challenge, particularly in transnational cases. The differences in legal systems and cultural backgrounds among various countries and regions contribute to diverse interpretations of fictional facts, malicious defamation, and other constituent elements, which become obvious in specific cases. For example, the law of country A defines the elements of the network defamation crime relatively broadly, emphasizing the actual harm of words to an individual's reputation. Conversely, in country B, the focus centers more on the malicious nature of the speech. In scenarios where a citizen of Country A posts a comment on a social media platform, it might be perceived as an insult by a citizen of Country B, yet it would not qualify as insult libel in Country A. Such transnational legal difference engenders confusion about identification standards, thereby posing challenges in the crackdown on insults and defamations. Additionally, the variance in cultural backgrounds also affects the comprehension of the network defamation crime. In some countries, specific expressions might be considered ordinary facets of social interaction, whereas, in other countries, the same expressions could be interpreted as insults. This phenomenon is particularly prevalent on international social media platforms due to the rapid dissemination of information across different countries, sparking clashes of cultural values (Zhang, 2016).

4.2 Complexity of Evidence Collection in the Anonymity and Virtuality of Cyberspace

In the investigation, both the originator of the speech and their underlying malicious intent become a formidable challenge, which requires law enforcement agencies to have high technical and legal literacy. Moreover, the authenticity and reliability of digital evidence often become the focus of controversy. Ensuring the legitimacy and credibility of evidence stands as a pivotal hurdle in network defamation cases. The investigation and trial of the network defamation crime are frequently swayed by anonymous accounts, virtual identities, and other factors, rendering the confirmation of speech originators extremely challenging. Malicious actors may employ technical means to obfuscate real IP addresses or forge fictitious accounts to conceal their identities. This necessitates a remarkable technical level from law enforcement departments, calling for the utilization of network tracing and digital forensics technologies to uncover the actual publisher. Meanwhile, the authenticity and reliability of digital evidence further complicates investigations and trials. Online information can be tampered with, deleted, or forged, generating intricacies in substantiating the legality and authenticity of evidence in the court. Scrutinizing the source, collection process, and storage method of digital evidence becomes imperative to safeguard against manipulation or fabrication. This requires law enforcement departments and judicial systems to enlist professional digital forensics experts to ensure the integrity and credibility of the evidence chain.

4.3 Significance of Balancing Freedom of Speech with Individual Rights

Crackdown on the network defamation crime inevitably entails restricting freedom of speech. While ensuring the social order, it is necessary to protect the legitimate rights and interests of individuals. The challenge lies in striking a harmonious balance between legal principles and practice, thereby fostering a cyberspace that not only allows uninhibited discourse but also curtails malicious attacks. Freedom of speech stands as a foundational right within modern society, promoting democracy, knowledge dissemination, and social progress. However, abusing this freedom to insult and defame online can inflict severe harm upon personal dignity and social stability (Zhao & Ma, 2009). Therefore, how to curtail online insults and defamations while safeguarding freedom of speech necessitates a thorough and thoughtful examination.

4.4 Challenges in Criminal Applications of the Network Defamation Crime Due to its Internationality

Due to the global reach of the Internet, crimes can traverse national borders, and legal differences and law enforcement cooperation between various jurisdictions may also be constraints. Therefore, international cooperation and coordination will play a pivotal role in criminal applications. The internationality of the network defamation crime introduces the potential for multiple jurisdictions to be entwined within a single case, entailing distinct legal frameworks, cultural disparities, and collaboration among various law enforcement departments. Investigations and accountability are complicated, for example, when a fabricated defamatory statement originating in Country A adversely impacts the public reputation of Country B. Disparities in the identification standard and criminal liability degree of the network defamation crime can engender legal conflicts and complicate case management across diverse countries. Furthermore, different countries uphold varying regulations concerning the collection, examination, and utilization of digital evidence, impacting both its accessibility and legality. Law enforcement departments must adeptly harmonize the legal prerequisites of different countries to ensure the reliability and validity of digital evidence for utilization in international cooperation.

Overall, the network defamation crime encounters a series of legal and evidence challenges, which require the joint support and efforts of legal systems, technical means, and social consensus. Safeguarding individual rights while simultaneously upholding the public order and wholesome growth of cyberspace demands a united effort from all parties to seek innovative solutions, thereby addressing this intricate and significant challenge.

5. Countermeasures and Suggestions

To address the challenges of network defamation crime, a series of legislative improvements are imperative to ensure accurate identification of the crime and appropriate punishment.

5.1 Clarity of Constitutive Requirements of the Crime

Legislation should make clear and specific provisions on the constitutive requirements of the network defamation crime, such as words of necessary characteristics of actual fiction, insults, and aggression, to avoid excessive restrictions on legal speech. First, we should define defamation behaviors specifically. Legislation can clearly stipulate that words with characteristics of actual fiction, insults, and aggression should qualify as a network defamation crime. Such explicit provisions can forestall excessive restrictions on general speech, thus safeguarding the freedom of legitimate speech. Second, a comprehensive elaboration of the crime is vital. Legislation could intricately detail the types of language constituting the network defamation crime, including malicious misrepresentations, offensive language, and discourse that directly damages an individual's reputation. Such detailed explanations serve as a guide for law enforcement departments and the judiciary in determining the precise constitutes of criminality. Third, we can consider interpreting the crime constitutes in the form of case law. Legislation can learn from actual cases, enumerate specific words within diverse contexts, and explain the specific constitution of the network defamation crime. This method bolsters the law's specificity and aids in the accurate adjudication of cases in practice. Finally, we should establish a judicial interpretation mechanism. Legislation can empower the judicial department to formulate judicial interpretations and clearly define the constitutive requirements and applicable standards of the network defamation crime. These methods maintain the law's adaptability, permitting the timely refinement of the crime constitution with societal evolution and technological advancements.

5.2 Establishment of an Effective Onus of Proof

In cases of network defamation crime, establishing an effective onus of proof is pivotal to ensure a fair trial and alleviate the plaintiff's load. This measure can require defendants to prove their words being legal or not constituting defamation under specific contexts, thus promoting the efficiency and impartiality of judicial trials. First, the establishment of such an onus of proof helps to ensure defendants have a degree of accountability for the lawfulness of their expressions. Given the rapid dissemination of online discourse, the impact of malicious attacks can often inflict irrevocable harm upon individuals' reputations (Yao, 2014). Thus, defendants should undertake a certain obligation of proof when facing the accusation of insults and defamations to safeguard the legitimacy of their speech and protect the legitimate rights and interests of the plaintiff. Second, an effective onus of proof can alleviate the plaintiff's evidentiary obligation. In network defamation cases, plaintiffs grapple with the onus of demonstrating that the defendant's words constitute defamation, which often demands a substantial amount of evidence and incurs significant costs. If the defendant has a certain onus of proof for the legality of their words or their absence of defamations, the overall evidentiary burden on the plaintiff can be lightened, thus facilitating the streamlined progression of the trial. In addition, the establishment of an effective onus of proof can improve the efficiency of the judicial trial. In heightened controversial cases, defendants must defend and substantiate their speech, prompting them to furnish more comprehensive evidence and rationales. This compels the court to judge the facts and evidence of the case, expedites the trial process, and ensures a fair trial. However, it is imperative to underscore that in establishing the onus of proof, the rights of defendants must be protected, and the undue onus should be averted. A delicate balance must be struck between the rights and interests of both plaintiffs and defendants, thus ensuring that while safeguarding freedom of speech, cases of network defamation crime can be tried fairly.

5.3 Enhancement of the Crackdown on False Information

To deal with online false information more comprehensively, we can consider encompassing the dissemination of false information within the scope of the network defamation crime, which promotes the clarity and order of cyberspace. By introducing the notion of false information into the crime definition, the scope would cover not only explicit malevolent attacks and insulting language but also the dissemination of fabricated information undermining any individual's reputation. The spread of false information may lead to false accusations and injuries to victims, thus affecting their social reputation and interpersonal relationships. Incorporating false information into the scope of the network defamation crime will aid in the crackdown on the dissemination of malicious speech and false information more pertinently. Simultaneously, it would serve as a conduit for underscoring the significance of nurturing an authentic and honest cyberspace, prompting individuals to express viewpoints and information with honesty and accountability. However, the imperative of balance must be upheld, ensuring that the crackdown on false information does not inadvertently curtail freedom of speech (Li, 2014). When determining the standard of false information, we can consider the clarity of the facts' authenticity, the malicious intent of information publishers, and other factors to avoid improper restrictions on legitimate speech.

5.4 Promotion of Transnational Cooperation Mechanisms

Due to the transnational nature of cybercrime, countries should strengthen their cooperation and coordination and establish transnational cooperation mechanisms. Firstly, countries can establish cooperation mechanisms by signing international agreements that can stipulate the principles, scope, and methods of transnational cooperation and clarify the obligations and

responsibilities of countries in combating network defamation crime. The formulation of such international agreements helps to forge a shared legal framework and provides clear guidance for cooperation among countries. Secondly, bolstering information sharing is the key to transnational cooperation. Law enforcement departments across various countries can establish information exchange channels, facilitating the prompt dissemination of intelligence and evidence of network defamation cases. This accelerates the tracking of transnational routes taken by criminal activity, ultimately fortifying case investigations and crackdowns. Moreover, we can explore the establishment of collaborative investigation teams with the participation of law enforcement departments of various countries. These teams can conduct joint investigations across national borders, assemble the law enforcement expertise and resources of various countries, and more effectively combat transnational network defamations. Throughout the advancements of transnational cooperation mechanisms, countries should fully respect sovereignty and differences in legal systems and strike a balance of cooperation. Concurrently, they should strengthen the support of international organizations and cooperation institutions, promote cooperation and exchanges among countries through multilateral channels, and jointly safeguard the order and security of global cyberspace.

5.5 Improvement of the Supervision and Cooperation of Social Media Platforms

Social media platforms wield a pivotal influence in the propagation of network defamation crime, so a series of measures are necessary to strengthen their supervision and cooperation. First, necessitating augmented user identity verification stands as a crucial step to ensure the genuineness of user accounts, consequently mitigating the possibility of anonymous malicious behavior. Second, the formulation of robust speech norms, accompanied by a lucid demarcation between permissible and prohibited expressions, empowers users to comprehend the contours of acceptable discourse. Third, an effective reporting mechanism should be established to facilitate the convenient flagging of malicious content, thus promptly stemming the dissemination of detrimental information. Finally, social media platforms should engage proactively with law enforcement departments and provide necessary information and cooperation to investigate network defamation cases. Through these measures, we can strengthen the role of social media platforms in combating network defamation crime and maintain the health and harmony of the network environment.

In short, the legislation for enhancing the identification of the network defamation crime necessitates comprehensive consideration of the balance between the protection of legal speech and the crackdown on defamations. By clarifying the crime constitution, establishing an effective onus of proof, strengthening the crackdown on false information, promoting transnational cooperation mechanisms, and improving the supervision and cooperation of social media platforms, we can better cope with challenges of the network defamation crime and maintain the health and harmony of cyberspace.

6. Conclusions

To sum up, as a booming social problem in the digital age, network defamation crime requires comprehensive cognition and global response. Through the in-depth study of its identification standard, supervision status, criminal applications, and countermeasures and suggestions, this paper calls on all social parties to make joint efforts to build a healthy network environment, with balancing freedom of speech and individual rights as the starting point. Based on clarifying the constitutes of the crime, we can provide practical solutions for preventing and responding to the network defamation crime by establishing a reasonable onus of proof, effectively combating false information, promoting transnational cooperation mechanisms, and strengthening the supervision and cooperation of social media platforms. Through various means, such as law, technology, and education, we aspire to create a cyberspace that not only allows freedom of speech but also maintains justice and respect, enabling it to be a platform for communication, cooperation, and inclusion.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Fan, J. (2016). *Research on judicial determination of network "communication" crime* [Master's thesis, Nanjing Normal University]. CNKI. https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD201801&filename=1017282319.nh

[2] Huang, H. S., & Hu, Y. (2013). Difficulties and countermeasures in investigation and evidence collection of victims of internet defamation crime. *Journal of Jiangxi Normal University of Science and Technology,* (5), 67-69.

[3] Li, J. H. (2014). *Research on the defamation crime in network environment* [硕士, South China University of Technology]. CNKI. https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD201501&filename=1015021065.nh

[4] Liu, W. Y., & Zhang, T. Y. (2018). Problems and countermeasures of criminal law regulation of internet defamation. *Academic Exchange,* (10), 90-97.

[5] Men, Z. Y. (2017). *The dilemma and countermeasures of information network insult and defamation in the context of the amendment* [Paper presentation]. Order and Responsibility in Cyberspace——The Second Internet Law Conference, Hangzhou.

[6] Sun, H. M. (2021). *Research on Criminal Justice Identification of Cyber Violence* [Master's thesis, South China University of Technology]. CNKI. https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD202301&filename=1021893919.nh

[7] Sun, X. B. (2010). *On the application of public prosecution system of defamation in China – Taking Han Xingchang's internet defamation case as an example* [Master's thesis, Northwest University]. CNKI. https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD2012&filename=1011037895.nh

[8] Xu, J. (2016). Examination and reconstruction of the identification of online defamation crime – Focusing on the influence of "true malice". *Research on Prevention of Juvenile Delinquency,* (2), 44-54.

[9] Yao, S. (2014). *On the judicial determination of defamation crime under the network environment* [Master's thesis, Anhui University]. CNKI. https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD201402&filename=1014229604.nh

[10] Ying, S. X. (2012). Criminal countermeasures of defamation. *Oriental Corporate Culture,* (5), 60.

[11] Zhang, K. R. (2016). *Criminal law regulation of internet defamation* [Master's thesis, Tianjin Normal University]. CNKI. https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD201701&filename=1016301396.nh

[12] Zhao, Y., & Ma, B. (2009). Dilemma causes and countermeasures of network violent crime. *Professional Time and Space, 5*(02), 118-119.