

On the Improvement of Legal Regulation of Online Violence Infringement

Xinwei Mei

Law School, Southwest Petroleum University, Chengdu 610000, China

Abstract: In the information age, the rapid development of the internet has led to an increasing frequency of "cyber violence" cases that have a negative impact on public order. The concept of "cyber violence" lacks a specific legal definition. Initially, it was defined from a non-legal perspective, referring to the behavior of forming an offensive group by unspecified netizens on the internet to target controversial events, engaging in cyber violence and doxing against the parties involved, seriously infringing upon their civil rights and violating social public order. However, this definition is more aligned with moral and ethical characteristics rather than legal ones. This paper points out the imperfections in domestic legal regulation of cyber violence and the susceptibility of judicial practice to influence, and puts forward some suggestions. Firstly, it is recommended to improve the network real-name identification system to materialize virtual networks. Secondly, corresponding legal norms for groups should be formulated. Additionally, strengthen legal education and publicity to enhance netizens' legal awareness and consciousness. In view of the weak links in the anti-cyber violence legal system, it is suggested to improve the relevant legal system. Finally, it is proposed to establish a network credit system to urge network users to strictly adhere to network norms. China has a large number of netizens, which poses significant challenges to the governance of the domestic network environment. However, if the legal system can better combat cyber violence, the network environment will become more stable, which will contribute to social stability and economic development.

Keywords: Cyber Violence, Human Flesh Search, Virtual Space, Online Infringement.

1. Introduction

Citizens enjoy the right to freedom of speech, but they should not abuse this right. Cyberbullying refers to the behavior of some internet users who, with the intention of disrupting public order, attack the parties involved through articles, videos, and other means. Freedom of speech is one of the most basic and important human rights for participating in public life. Without freedom of speech, there can be no human rights and freedom. Despite the importance and widespread use of freedom of speech, most people do not use it correctly. Cyberbullying is usually a large-scale behavior in which netizens express moral emotions offline through language, text, videos, and other means. How to further regulate and restrict netizens, improve the legal system of cyberbullying, and curb the abuse of the right to freedom of speech by many netizens is crucial for reducing cyberbullying.

2. Overview of Cyberbullying

Cyber violence is a concept with extremely rich and uncertain connotations. Some scholars argue that cyber violence refers to "the malicious actions launched by unspecified majority of Internet users against specific targets in cyberspace, primarily through verbal attacks, doxxing, threats, harassment, insults, and rumors, which are collective, provocative, offensive, and persistent, seriously infringing upon the legitimate rights and interests of other citizens or organizations" [1]. Others believe that cyber violence should be limited to unspecified subjects' actions of insulting, defaming, invading privacy, and cyberbullying that infringe upon others' rights and interests in cyberspace [2]. The "Seminar on Promoting Anti-Cyber Violence Legislation" [3] unanimously decided that cyber violence refers to the act of disseminating illegal and harmful information in the form of

text, images, audio, and video, targeting individuals and containing insults, rumors, defamation, invasion of privacy, incitement to trouble-making, etc., which seriously infringes upon others' personal rights and disrupts normal network order [4]. Although scholars differ in their wording when defining cyber violence, there is still consistency. The author believes that the definition provided by the "Seminar on Promoting Anti-Cyber Violence Legislation" covers a broader scope.

Due to the anonymity of cyberbullying, perpetrators can hide their identities and avoid bearing the consequences of their remarks, thus attacking others without any scruples [5]. Cyberbullying is often caused by the contagion of group emotions. According to statistics from June 2023, the number of internet users in China has reached 1.079 billion [6]. With such a large number of internet users and the rapid speed of online communication, it is easy to form groups around certain issues, which can have serious destructive impacts on society. At the same time, the herd mentality also makes individuals more likely to blindly follow group behavior, further exacerbating the occurrence of cyberbullying.

Cyberbullying can be realized through personal attacks and doxxing. Personal attacks refer to behaviors that harm others' physical or psychological well-being through violence or other illegal means. The most common form of this is cyber language violence, including acts such as abuse, discrimination, defamation, contempt, ridicule, harassment, assault, insult, bullying, pornography, and sexual discrimination [7]. These behaviors not only cause psychological and physical harm to the victims but also have adverse effects on society. Doxxing involves using the Internet as a medium to manually identify the authenticity of information provided by search engines, and sometimes involves anonymous insiders providing data to intervene in investigations [8]. Disseminating others' information such as

name, address, phone number, and work unit on the Internet without the consent of the parties involved [9] involves infringing upon the privacy and reputation rights of others and other legitimate rights and interests.

3. Types of Online Violence Infringement

3.1. Infringement of General Personality Rights

According to Article 990 of the Civil Code, the law protects personal freedom and human dignity. General personality rights refer to the general personality interests enjoyed by civil subjects, which are summarized as the equality, independence, and dignity of personality. It is a general right, characterized by the universality, specificity, legality, and abstractness of the subject. When netizens are subjected to personal attacks, their general personality rights are infringed upon, their dignity is harmed, and there is a high possibility of causing serious mental harm to the parties involved [10].

3.2. Violation of the Right to Health

The right to health is the legal entitlement of citizens to be protected from illegal infringement on their physical health. This right encompasses the maintenance of bodily health, which includes the normal functioning of physiological mechanisms and a good psychological state, encompassing both physical and mental health. When netizens engage in cyber attacks against individuals, causing severe mental harm, their psychological functions are damaged. In reality, there are numerous cases of individuals suffering from depression, mental illness, or even committing suicide due to unbearable cyber violence.

3.3. Infringement of Reputation Right

The right to reputation refers to the right enjoyed by civil subjects to receive fair treatment and protection for the social evaluation manifested by their own characteristics. Reputation is a factual and value judgment made on the credit, morality, etc. of the subject. The specific content of this right includes: prohibiting others from engaging in illegal insults, defamation, disclosure of one's privacy, etc., and having the right to safeguard one's reputation from infringement. In numerous incidents of cyber violence, acts of cyber violence such as verbal abuse, online rumors, and doxing often damage the reputation rights of the parties involved [11].

3.4. Infringement of Privacy

The right to privacy refers to a specific personality right that individuals enjoy, which protects their personal information, private activities, and private domains unrelated to public interests from being illegally intruded, known, collected, utilized, and disclosed by others in accordance with the law. In contemporary society, protecting personal privacy from infringement is the obligation of every citizen and is also clearly stipulated in civil law. Infringing on others' privacy is an illegal act that can cause serious mental harm and material losses to the victims. In cyberbullying, netizens use various means to dig up various information about the parties involved and post it online at will. This behavior causes serious physical harm and psychological trauma to the parties involved, infringing and trampling on their right to privacy [12].

4. Inadequacies in Legal Regulation of Cyberbullying

4.1. Deficiencies in Legal Regulation of Cyber Violence

China's network laws and regulations started relatively late, coupled with the rapid development of the Internet, and the network is changing rapidly, making it inevitable that there are imperfections in management. Although the law has established remedies such as ceasing the infringement, restoring reputation, eliminating influence, offering apologies, and compensating for mental damage in the face of infringement, when infringement occurs, it is difficult to completely eliminate the already spread information due to the rapid dissemination of the network. These remedies appear unsatisfactory. When personal rights and interests are infringed, the duty of care of network service providers is too high. Because infringement of personal rights and interests such as reputation is difficult to judge in terms of information authenticity, it is not appropriate to require network service providers to passively notify for handling or actively review [13]. At the same time, due to the group characteristics and anonymity of violent online speech, it is difficult to initiate judicial proceedings, resulting in long litigation periods and secondary harm, which makes it difficult for victims to obtain evidence and increases the cost of safeguarding their rights [14]. The law generally imposes strict requirements on individuals, but the provisions for group behavior are not perfect. When group violence occurs, there is often no suitable law to apply, which requires the formulation of enforceable laws targeting groups. Currently, the network real-name system is not yet perfect, and after many incidents of online violence, it is still impossible to identify the infringer or hold the infringer legally responsible [15].

4.2. Imperfections in the Judicial System

In the Internet plus era, public opinion is highly influential, and judicial authorities should base their decisions on law and facts. However, it is inevitable that they will be influenced by public opinion. For example, the "Yao Jiaxin incident" attracted widespread attention, and public opinion tended to support the victim. As a result, Yao Jiaxin and his friends, parents, colleagues, etc. also suffered from cyberbullying and personal attacks. The Internet has memory, and even for cases that occurred decades ago, when they are retrieved or discussed again, the impact of cyberbullying at that time will continue to affect the parties involved. According to the principle of judicial independence, judicial authorities should exercise their powers independently, emphasizing the overall independence of the court [16], and only the law can influence the trial. It is inevitable that judicial personnel will be influenced by external factors, and the verdicts of some cases indeed have a guiding role in society. Guiding cases have a strong guiding effect. Rather than waiting for cyberbullying to continue to escalate, it is better to address it at its source. Network regulators must take systematic actions to fill judicial loopholes and conduct comprehensive supervision of the online environment. When cyberbullying occurs, all parties must work together to control the online environment.

5. Suggestions for Regulating Cyber Violence

5.1. Standardize the Network Real-name System

Due to the virtual nature of the internet, people may lower their guard when browsing online, which is one of the reasons for the occurrence of cyberbullying. However, the internet is not a lawless place, and individuals should be held accountable for their online behaviors. Improving the internet real-name registration system is of great significance for "identifying the subject of tort liability" [17] and helping victims safeguard their rights. It also helps internet users clearly understand their obligations in the virtual online environment [18]. The government should establish a comprehensive real-name authentication system, standardize the operational procedures and standards for real-name authentication. In the process of implementing real-name authentication, internet platform providers and internet service providers should be required to fulfill their obligation of real-name authentication to ensure the authenticity and accuracy of users' real-name registration information. At the same time, when formulating regulations, everyone's "online identity card" should be fixed, which can effectively promote the development of the real-name system and thereby reduce the incidence of cyberbullying. Network supervision is also essential. The government should strengthen the supervision of internet platforms, urge them to fulfill their supervisory responsibilities, and promptly detect and deal with cyberbullying behaviors. Internet platforms that fail to fulfill their obligation of real-name authentication should be punished according to law.

5.2. Formulate Laws Applicable to Groups

Cyberbullying is often collective in nature. However, in light of current circumstances, many participants in each instance of cyberbullying often evade any responsibility. As most individuals in the group have taken part in the violent actions, they should all bear corresponding responsibilities [19]. Currently, China's laws and regulations regarding cyberbullying are not yet comprehensive, lacking specific implementation details and operational procedures. When formulating collective laws, it is imperative to clarify the responsible parties and scope of application, including governments, enterprises, and individuals. Simultaneously, the rights and obligations of each party should be clearly defined to prevent mutual shirking or regulatory gaps. Many individuals believe that the law does not punish the masses, arguing that with so many participants, how could everyone be held accountable? It is precisely because of this mindset that netizens feel more emboldened to express their opinions. We should view this group as a unified entity, attributing the consequences to all. Individuals should bear corresponding responsibilities based on their degree of behavior within the group. The legal system should establish standard criteria for responsibility allocation and delineate responsibilities according to each person's responsibility. In cyberbullying incidents, the behaviors of all participants should be evaluated, and responsibilities should be allocated based on the severity of their actions.

5.3. Establishing a Specialized Court for Cyber Violence Cases

With the frequent occurrence of cyber violence, its characteristics of infringing privacy, damaging reputation, and even endangering personal safety have become increasingly prominent. Traditional courts may face issues such as low trial efficiency, complex case types, and difficulties in legal application when adjudicating such cases. The establishment of specialized courts can refine the division of labor, enhance the professionalism of judges in handling cyber violence cases, make the work of judicial personnel more detailed and clear, and improve the efficiency of their adjudication of cyber violence cases, saving litigants' litigation costs [20] and enhancing the efficiency and fairness of case handling. From the perspective of legal support, existing laws such as the Civil Code and the Cybersecurity Law have provided legal basis for cyber violence. Courts can adjust judicial resources based on the characteristics of cases. Moreover, since the 1990s, courts across the country have begun to establish specialized judicial organizations for various types of cases [21], and the well-established intellectual property courts and financial courts can serve as references. At the same time, the establishment of specialized courts can also meet the new demands of social governance and build a clearly defined and orderly cyberspace. Therefore, the establishment of specialized courts for cyber violence cases is not only an urgent task but also an important measure to achieve modernization of network governance and protect the legitimate rights and interests of the people. As the saying goes, "Each profession has its own specialization." Cyber violence cases are complex and ever-changing, and the establishment of specialized judicial organizations can better fulfill the functions of the courts.

5.4. Building a Network Personal Credit System

Credit has achieved remarkable results in social practice. The banking credit system and Alipay's Zhima Credit have established a widespread credit system. Credit has a profound impact on users, so everyone strives to improve their credit level. The Personal Information Protection Law of the People's Republic of China has made detailed provisions on the protection of citizens' personal information. Therefore, we need to establish a network credit evaluation mechanism. By recording and evaluating users' online behavior, their credit levels can be classified, thus constraining and managing their actions. The establishment of a network credit system should be combined with the construction of a network real-name system to enhance the credit level of the online society. To evaluate the credit of netizens, we must first strengthen the application of technical means, such as artificial intelligence and big data, which can analyze and predict users' online behavior. Based on the degree of netizens' participation, abnormal situations can be detected and dealt with in a timely manner, thereby reducing the occurrence of cyber violence. [22]

6. Conclusion

Based on the above analysis, it can be concluded that cyber violence refers to the damage caused to others' reputation, rights, and mental health through speech, text, images, and videos that are "defamatory, slanderous, destructive, and infringing on reputation" and are led by netizens. Addressing

the issue of cyber violence is an inevitable requirement for comprehensively governing the country according to law, as well as for improving people's happiness index and building a harmonious society. To fundamentally solve the problem, it is necessary to proceed from reality, break the virtuality of the network, establish a real-name system, and improve it based on the characteristics of cyber violence. Addressing cyber violence requires sound laws, timely action, and the joint efforts of the government and netizens who respect and abide by the law. Among them, the role of law is particularly important. Therefore, it is necessary to improve relevant laws and strengthen law popularization work, enhance the legal literacy of the entire population, use law as a weapon to protect their legitimate rights and interests, respect the rights of others, and eliminate infringement and cyber violence. The government should strengthen supervision of the network and put forward higher requirements for judicial authorities. Under the guidance of legal authorization, judicial authorities should proactively supervise law enforcement and strengthen and improve the legal system to combat cyber crimes, in order to purify the network environment, maintain network order, and thus safeguard the rights and freedoms of netizens.

References

- [1] Liu Xianquan, Zhou Zijian: "The Dilemma and Solution of Criminal Regulation of Cyber Violence Crimes", published in "Law Studies", 2023, Issue 5, p. 18.
- [2] Li Bencan. Dogmatic Construction of the Scope of Punishment for Cyber Violence Crimes [J]. Global Legal Review, 2025, 47 (01): 5-23
- [3] On December 27, 2024, the "Seminar on Promoting Anti-Cyber Violence Legislation," hosted by the School of Criminal Justice at China University of Political Science and Law, was held in Beijing. The meeting conducted in-depth discussions on key issues such as defining the concept of "cyber violence" in anti-cyber violence legislation, determining the responsibilities of various stakeholders, and establishing a reasonable regulatory mechanism.
- [4] Jiang Anjie. Experts and Scholars Advocate for Anti-Cyberbullying Legislation [N]. The Rule of Law Daily, 2025-01-22 (009)
- [5] Fan Renyi. Realistic Obstacles and Solutions in Accountability for Online Fraud [J]. Law and Society, 2018, (09):
- [6] See the 52nd Statistical Report on Internet Development in China released by the China Internet Network Information Center (CNNIC) in Beijing.
- [7] Liu Wenyu, Li Ke. A Research Framework for Online Language Violence Based on Critical Discourse Analysis [J]. Journal of Northeast Normal University (Philosophy and Social Sciences Edition), 2017, (01): 119-124
- [8] Li Jia. Research on the Civil Law Protection of Online Privacy Rights [D]. Dalian Ocean University, 2020
- [9] Fan Xiaoling. "Human-flesh Search" and Legal Regulation of Privacy Protection [D]. Shandong University, 2010
- [10] Beijing: Law Press, January 2014. Edited by Lin Jianjun; Co-edited by Chen Zhengzheng, Fang Bin, Li Hongxing, et al. - Litigation Guidelines and Practical Answers: Personal Injury Compensation Disputes
- [11] Chen Ting. Exploring Cyberbullying and Its Governance in the Age of We-Media [D]. Harbin Institute of Technology, 2020
- [12] Bi Donglei. Research on the Issue and Governance of Cyberbullying [D]. Hebei Normal University, 2016
- [13] See Wu Handong, "An Analysis of Online Tort Liability from the Perspective of the Tort Liability Law", Law and Business Research, 2010, Issue 6.
- [14] Wang Xiaoyu. The Dilemma and Suggestions of Judicial Remedies for Cyber Violence Infringement [D]. Shanghai Normal University, 2024
- [15] Han Xiaozhen. Research on Legal Regulation of Cyberbullying in the New Media Era [D]. Hebei University of Economics and Business, 2020
- [16] Ding Wei. Jurisprudential Reflections on Optimizing the Allocation of Judicial Authority [D]. Liaoning Normal University, 2017
- [17] See Zhang Fan. "On the Legal Regulation of Cyber Violence" [D], Heilongjiang University, 2021, p. 30.
- [18] Jiang Qinqi. Research on the Improvement of Tort Liability for Cyberbullying from the Perspective of the Civil Code [D]. Jiangxi Normal University, 2024
- [19] Xu Yi. The Formation and Governance of Cyber Violence [J]. Industry and Technology Forum, 2016, 15(12):
- [20] Wang Jiageng. Civil Remedies for Cyber Violence Infringement: Dilemmas and Paths [J]. Journal of Henan Polytechnic University (Social Science Edition), 2024, 25 (01): 7-13
- [21] Chen Ming. The Legal Structure and Institutional Framework of Specialized Courts [J]. Southeast Judicial Review, 2014, 7(0): 203-215
- [22] Chai Lingling. Research on the Social Psychological Motivations and Countermeasures of Cyberbullying Phenomenon among College Students [D]. Harbin Institute of Technology, 2022