

# ***Current Measures for Handling Cyber Bullying and Its Path to the Rule of Law: Based on a Comparative Study***

Yiming Cheng<sup>1</sup>, Yulin Ye<sup>2,a,\*</sup>, Yijia Yu<sup>3</sup>

<sup>1</sup>*School of Law, Hainan University, Haikou, China*

<sup>2</sup>*School of Law, Ocean University of China, Qingdao, China*

<sup>3</sup>*School of Economics and Management, Shanghai University of Political Science and Law, Shanghai, China*

*a. 20130002171@stu.ouc.edu.cn*

*\*corresponding author*

**Abstract:** The third technological revolution and the vigorous development of the Internet industry have made it easy for people to obtain information and publish news on the Internet. While Internet penetration continues to reach new highs, so do incidents of cyber bullying. From "a woman was subjected to rumors and cyberbullying just for picking up a courier" to "Xuezhou Liu, a boy looking for relatives, committed suicide", there are countless tragedies caused by cyber bullying. Since 2008, all sectors of society have been continuously studying the issue of cyber bullying, and until 2024, there are countless studies on cyber bullying, mainly in journalism, sociology, political science, law, education and psychology, etc., with a wide range of research topics. In this context, this study will compare and contrast the similarities and differences between Chinese and foreign measures for dealing with cyber bullying and the path of rule of law, and fill in the lack of boundaries between cyber violence and ordinary violence in criminal law theory.

**Keywords:** Cyber Violence, Internet, Criminal Law, Comparative Study

## **1. Introduction**

According to the latest Statistical Report on the Development of China's Internet Network released by the China Internet Network Information Center, as of June 2023, the number of Internet users in China has reached 1.079 billion, an increase of 11.09 million from December 2022, and the Internet penetration rate has reached 76.4%. According to the 2019 "Social Blue Book" released by the Chinese Academy of Social Sciences, nearly three-tenths of young people in China have suffered cyber bullying, and the most important scenario is social software, which is 68.48%; followed by online communities, with a proportion of 55.30%. In addition, 25.36% of teenagers encountered violent and abusive messages on Weibo.

The cyberspace constructed by the Internet has profoundly affected the real society, which has led to frequent cyber chaos. China has formulated relevant laws and regulations in an effort to build a complete regulatory system. Since 1994, China has formulated and promulgated more than 140 pieces of legislation in the field of cyber power, providing a solid institutional guarantee for the construction of a cyber power. It has successively formulated and promulgated laws such as the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, and promulgated many

administrative regulations and departmental rules to promote the construction of a harmonious network society. In 2014, the state established the Central Leading Group for Cyber Security and Informatization, which aims to coordinate major issues of cyber security and informatization in multiple fields.

However, as a social problem with increasing frequency, cyber violence has a lower priority in legislation and discussion than on topics such as data security.

## **2. The Concept and Characteristics of Cyber Bullying**

### **2.1. The Concept of Cyber Violence**

As a term often quoted by self-media, there are still some disputes and uncertainties in the academic and judicial circles about the definition of cyberviolence, and no relevant laws against cyberviolence have yet been issued. As of November 2023, the procuratorate has prosecuted a total of 280,000 people for various cybercrimes, an increase of 35.5% year-on-year, accounting for 18.8% of all criminal offenses [1]. In such criminal cases, the charges used are still based on the original offences of insult and defamation. From the perspective of the current judicial organs, cyber bullying is an insult and defamation in traditional crimes, using the Internet as its communication medium and tool, which makes the dissemination of harmful information wider, increases the social harm, and makes it difficult to eliminate the impact. On social platforms, group cyber bullying is becoming increasingly prominent, and its manifestations include but are not limited to malicious attacks, insults, defamation, doxing, etc., causing serious psychological and emotional harm to victims, and even affecting their real lives. Specifically, group cyber bullying on social platforms falls within the scope of crimes such as "picking quarrels and provoking trouble", "insulting, and defaming" in the Criminal Law. These acts not only infringe upon the legitimate rights and interests of the victims and undermine the harmony and stability of cyberspace, but also have serious social harm [2].

On the other hand, there are different opinions on the definition of cyber violence. Some scholars believe that cyber bullying has five characteristics: slander, incitement, defamation, infringement of others' reputation, and damage to legitimate rights and interests, and is manifested in the form of publishing untrue and insulting texts, pictures, videos, etc., on online platforms, verbally attacking others such as insulting, slandering, and slandering through comments and forwarding, or disclosing or disseminating personal information without the consent of the parties, inciting the formation of a group effect, so as to achieve the purpose of mentally suppressing others [3]. Some scholars have pointed out that online linguistic violence is an unspecified number of netizens who take advantage of the concealment of the Internet to maliciously expose their privacy, or slander, insult, or attack specific parties, deprive others of their right to speak in a hegemonic manner, infringe on the legitimate rights and interests of the parties, and cause serious physical and mental harm to the parties [4]. Some scholars have defined online public opinion violence on social media platforms, arguing that online public opinion violence refers to the public release of texts, pictures, audio, video, etc. on self-media platforms, thereby causing many netizens to verbally abuse, personal attacks and other stigmatizing behaviors against others, causing mental harm to victims [5].

Based on the views of the above scholars, cyber violence can be used as a derivation of traditional insults and slanders in the new era and new technologies. It can also be regarded as a new malicious act with elements of insult and defamation because of its difference from the characteristics of traditional insult and slander; It can even be further subdivided into traditional insults and slanders, malicious leakage of information, infringement and deprivation of the right to speak, inciting emotions, causing large-scale public opinion turmoil, and other behaviors that are difficult to cause such bad effects in the era when the information medium is paper. Although the current judicial practice is still able to cope with the increasing frequency of cyber bullying incidents, it has the

limitations of the times, and it is urgent to introduce new judicial interpretations to expand its scope of application. Further, with the further development of the Internet and the acceleration of the pace of information circulation, cyber bullying is likely to develop into a new form of subjective malice and large-scale social destructiveness, and at the same time, to a certain extent, it also circumvents the scope of application of the original statutory provisions that are subject to the interpretation procedure.

## 2.2. Characteristics of Cyber Bullying

There are many opinions about the characteristics of cyber bullying, but there is a significant overlap in some of them. The first is its collective nature, and an illogical reality is: why is it that what started as a one-on-one abusive attack on the Internet is likely to turn into a large-scale scolding war? Before the age of the Internet, such behavior was rare. The reason may be that large-scale cyber bullying incidents often begin with a long article by one party, the content of which is mainly to criticize the other party's behavior and morality [6]. This kind of behavior is rare in real life, because offline scolding not only consumes energy, but later onlookers often do not know why they do not know because they have not heard the previous long moral criticism, and they just watch in silence for fun. Conversely, the cost of searching for a person's previous statements and events on the Internet is greatly reduced, and later bystanders quickly understand the cause and effect of the event, which makes it less effortless for them to enter the venue [7]. Such moral criticism can quickly form a wave in the Internet community, exploiting the public's sense of justice to engage them in cyber bullying. However, at this time, the cyber bullying has not yet fermented to the point of seriousness, until the group has formed a certain scale. James Stoner proposed the concept of "group polarization", arguing that groups are more likely to make extreme choices than individuals because the responsibility of each individual is apportioned and dissolved. It was only at this point that a devastating cyber violence began. Therefore, the collective nature of cyber bullying not only refers to the large scale of the perpetrators, but also means that they have a very low threshold for participation in each third party, and constantly attract them to become a member of the perpetrators with low-responsibility, low-cost emotional catharsis channels and group identity. Due to the collective nature, when the judiciary pursues responsibility, only the initiator is investigated, and those who follow the trend are often not pursued.

The second is suddenness, where information goes viral through the Internet, as does the one-sided moral critique issued by the abuser. Because of preconceived notions, it is difficult for individuals to change their perceptions, so cyber bullying often quickly leads to irreversible damage [8].

Anonymity is mentioned in the views of most scholars. However, with the implementation of the online real-name system and the improvement of the cyber police system, the Internet has become completely unlaureless. The technology to track an IP address can be traced directly through the account to the real identity of the user behind it. Traditionally, the role of anonymity is embodied in controlling multiple accounts at the same time to amplify the impact of personal speech, or using anonymity to hide identities and avoid being held accountable. However, with the development of the above-mentioned tracking technology, these two points have become increasingly unsustainable: controlling multiple accounts at the same time is no longer so secretive and can be easily traced back for inappropriate speech, and pseudonymous nicknames on the Internet cannot hide the IP addresses and account IDs behind them [9]. The use of social platforms by the initiators of cyber bullying has gradually changed from a curtain of hiding their identities to a stage for inciting the audience and elevating their own morality. Although sooner or later their true identities will be revealed, the public emotional catharsis it causes can quickly and irreversibly damage the lives and spirits of the victims.

### **3. Current Measures to Deal with Cyber Bullying over the World**

#### **3.1. China's Current Measures to Deal with Cyber Bullying**

##### **3.1.1. Laws and Regulations**

China has enacted a series of laws and regulations against cyber bullying, such as the Criminal Law, the Civil Code, the Personal Information Protection Law, and the Public Security Administration Punishment Law. They answer general and important questions about the prevention and control of cyber violence. In addition, specific regulations and standards for punishing crimes have also been made. These laws and regulations clearly stipulate cyber bullying and provide a legal basis for the governance of cyber bullying.

##### **3.1.2. Regulatory Mechanisms**

The Chinese government has strengthened its supervision of online platforms, requiring them to establish and improve user reporting mechanisms and promptly address cyber bullying. These platforms can be managed by accurately controlling user data. This helps to reduce the occurrence of cyber violence. At the same time, the government has also strengthened the management of cyberspace and cracked down on illegal activities such as online rumors and online fraud. This is conducive to preventing the platform from excessively pursuing benefits, but ignoring its social responsibility.

##### **3.1.3. Governance Means**

China has adopted a variety of measures to combat cyber bullying, including strengthening publicity and education, improving public quality, and promoting industry self-discipline. In addition, the government has actively advocated measures such as the real-name system and the development of technology to prevent cyber bullying. In addition, the Chinese government attaches great importance to social propaganda about building a good school atmosphere, and many official public accounts can often be seen on social platforms to express their attitudes and positions on some bullying incidents.

##### **3.1.4. Preventive Mechanisms**

China attaches great importance to preventing the occurrence of cyber bullying at the source. The government has strengthened education and guidance for young people to raise their awareness of and prevention of cyber bullying. At the same time, the government also encourages all sectors of society to participate in the prevention of cyber bullying. Learning the Code of Conduct has been added to the school's computer classes, and basically every student who uses the Internet knows some basic Internet literacy, such as staying rational, being kind to others, and so on.

##### **3.1.5. Personal Rights Protection**

China has always placed the protection of the legitimate rights and interests of online users in an important position, actively providing comprehensive support and assistance to victims. Firstly, China encourages victims to protect their rights through legal means. The government continuously improves relevant laws and regulations to provide legal protection for victims. Secondly, the government is increasing its crackdown on online violence. Public security organs, network supervision departments and other relevant departments should strengthen cooperation to jointly combat online violence. In addition to legal support, China also provides psychological assistance services for victims and actively carries out online literacy education.

### **3.2. Measures in Place to Deal with Cyber Bullying in Other Areas of the World**

As the first country in the world to issue a written law on the Internet, Germany has a very complete Internet management system. Germany has a higher level of penalties for cyber bullying, raising the cost of crime. At the same time, Germany also pays attention to the implementation of industry self-discipline and technical prevention measures.

In the United States, laws and regulations such as the Cyberbullying Prevention Act and the Megan Mayer Cyberbullying Prevention Act have been enacted in response to cyber violence. The U.S. government has strengthened regulation and education to curb the occurrence of cyber bullying. In addition, the United States also focuses on protecting the cybersecurity of minors [10].

French criminal law clearly states that cyberbullying is the same crime as harassment or bullying in general, and that mental bullying is punishable. The French government has set up a toll-free hotline for young people to make anonymous reports, and in addition, France has paid more attention to the implementation of measures such as industry self-regulation and technical prevention.

Japan focuses on the development and application of technology in the prevention of cyber bullying. The Japanese government commissioned a company to develop the "Cybercrime Alert" software to prevent cybercrime. At the same time, Japan has also strengthened the supervision of online platforms and required them to fulfill their information network security management obligations.

South Korea has been implementing a real-name system online for more than a decade, and although it has been controversial, it has greatly reduced the frequency of cyber bullying. The South Korean government has also strengthened its regulation of online platforms and required them to take necessary measures to prevent cyber bullying.

### **3.3. Comparative Analysis**

#### **3.3.1. Laws and Regulations**

China and other countries have made clear provisions on cyber bullying in terms of laws and regulations, and have provided a legal basis for its governance. Due to the differences in legal systems and legal cultures in different countries, there will be differences in specific legal provisions and penalties. China focuses on punishing cyber bullying in accordance with the law, emphasizing the deterrent effect of the law.

However, foreign legal systems are relatively complete, focusing on individual legislation and special handling of special cases.

#### **3.3.2. Regulatory Mechanisms**

China and other countries have strengthened their regulation of online platforms and required them to comply with their management obligations. There are certain differences in the way and intensity of regulation in different countries. China pays attention to technical prevention and public opinion discovery, emphasizing the punishment of accounts and platforms that violate laws and regulations. Foreign governments have strengthened the supervision of online platforms, focusing on technical monitoring and early warning.

#### **3.3.3. Governing Tools**

China and other countries have taken a variety of measures to combat cyber bullying, including strengthening publicity and education, improving public quality, and promoting industry self-regulation. In China, publicity and education and technical prevention are the mainstay, emphasizing



public participation and industry self-discipline. Foreign countries pay more attention to the implementation of measures such as industry self-discipline and online real-name system.

### **3.3.4. Preventive Mechanisms**

China and other countries are actively engaged in the arduous task of preventing cyberbullying, in order to create a healthier and safer online environment. In China, our focus is mainly on establishing sound protection mechanisms and measures to curb the spread of cyberbullying information. In other countries, the prevention of cyberbullying has also received high attention. They pay more attention to preventing cyberbullying from the source and have taken various measures to strengthen youth education and social participation. In addition, other countries also focus on establishing sound social support systems to provide timely psychological and legal support for victims. They have established specialized aid institutions to provide counseling, psychological counseling, and other services to victims, helping them overcome their shadows and regain confidence.

### **3.3.5. Personal Rights Protection**

Governments of various countries are well aware that the security and stability of cyberspace are crucial for social development. Therefore, they are actively committed to safeguarding the legitimate rights and interests of internet users and encouraging victims to protect their rights through legal means. In this regard, although there are certain differences in current measures among countries due to differences in national conditions, legal systems, and judicial practices, these differences have not reached a very significant level. Governments around the world have recognized the importance of protecting the rights and interests of internet users and have taken corresponding legal, administrative, and technical measures to safeguard them.

## **4. Countermeasures and Recommendations**

In view of the severe situation of group online violent crimes on social platforms, this study puts forward the following countermeasures and suggestions.

First of all, the country needs to improve its laws and regulations. If you want to regulate criminal behavior by law, the first step is to clarify the definition of the criminal act. There is a lack of a definition of cybercrime in China's current law. Even the Guiding Opinions on Punishing Violations and Crimes of Cyber bullying in Accordance with Law, jointly issued by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security in 2023, do not provide a clear definition of the act [11]. The second step is to further clarify the specific constituent elements of cyber bullying after determining the boundaries and distinctions between cyber bullying and criminal acts. In the third step, when refining the legal provisions, we can start from the two aspects of individual responsibility and group responsibility to solve the main obstacles to the criminalization of online violent crimes, that is, the situation where individuals are not guilty and groups are guilty. Second, the state and online platforms need to strengthen supervision and law enforcement, and assume the main responsibility. On the one hand, the state should improve the network supervision departments, clarifying the functions and powers of public security departments, internet management departments, and other such bodies, so that public power can play its role. On the other hand, it can be compared to the "duty of care" that platforms need to bear in terms of intellectual property protection. At the same time, different information on internet platforms is handled differently, such as directly deleting words and sentences that are obviously of a violent nature, and formulating perfect judgment standards for words and sentences that are obscure or difficult to determine the nature of cyber bullying, and dispatching special personnel to be responsible for fulfilling the obligation of review, giving full play to the power of multi-subject supervision, and so on.

Finally, it is necessary to strengthen education and publicity, and establish prevention and response mechanisms. The state and society shall increase the public's awareness and vigilance of online violent crimes, periodically carry out lectures and publicity on the theme of preventing cyber bullying, and advocate civilized online access and rational expression. At the same time, strengthen online literacy education for young people, regularly carry out mental health screenings, formulate different judgment standards, and carry out key interventions for students with a tendency to cyber bullying. This kind of method can also be applied to the general public, where tasks are assigned to various communities, and after screening out people with cyber bullying tendencies, the community and state institutions will focus on them, intervene immediately, and cultivate the correct values and morals of the masses. At the same time, establish and improve mechanisms for responding to cyber bullying, including rapid response, public opinion monitoring, psychological counseling, etc., to provide timely and effective help and support to victims, and solve the dilemma of victims who have no way to seek help and compensation.

## 5. Conclusion

With the increasing pressure of social life and the increasing frequency of emotional incidents, everyone has the right to demand that they be free from cyber bullying. However, group online violent crimes on social platforms have become a social problem that cannot be ignored. This paper compares the various legal means and characteristics of the regulation of cyberviolence and puts forward countermeasures and suggestions, aiming to provide useful reference and reference for relevant departments to jointly maintain the harmony and stability of cyberspace. Cyber violence is not only a social problem unique to the period, but also another difficult problem that challenges the development of current legal theories.

## Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

## References

- [1] Zhang Cong. (2024) *The Procuratorate Punishes Online Violent Crimes in Accordance with Law*.
- [2] Chen Daibo. (2013) *Analysis of the Concept of Online Violence*. *Hubei Social Sciences*, 6,1003-8477.
- [3] Gao Yuan. (2021) *Legal Regulation of Online Violence in Self-media*. 39(2),8-12.
- [4] Sun Longhui. (2018). *An Analysis of the Legal Regulation of Online Language Violence*
- [5] Gao Yulu. (2023) *The Legal Regulation of Public Opinion Condemnation in the Self-media*.
- [6] Jing Lijia, Hu Xie. (2021) *A path to Improve the Legal Regulation of Online Violence*. *Journal of Chinese People's Public Security University*, 37(05),142-149.
- [7] Lian Zhiliang. (2019) *Improvement of Legal Regulation of Online Violence and Torts*. *Procuratorial research and guidance*, 2,111-114.
- [8] Wang Huawei. (2024) *Governance of Online Violence: Platform Responsibility and Gatekeeper Role*. *Jiaotong University Law*, 3,51-64.
- [9] Liu Jinrui. (2024) *Improvement of the Legal Path of Online Violence and Tort*. *Political and Legal Forum*, 42(03),66-76.
- [10] Ji Xiaowei. (2022) *An Empirical Study on Cybe Violent Crime*.
- [11] Kyung-Shick Choi, Jin Ree Lee. (2017) *Theoretical Analysis of Cyber-interpersonal Violence Victimization and Offending using Cyber-routine Activities Theory*.