

Research on the Dilemmas and Paths of Criminal Law Regulation of Cyber Violence

Qiaoling Zhang^{1,a,*}

¹School of Law and Public Administration, Yibin University, Yibin, Sichuan, China

^a978247937@qq.com

*Corresponding author

Abstract: The 57th Statistical Report on Internet Development in China released by the China Internet Network Information Center provides data showing that as of December 2025, the number of netizens in China reached 1.125 billion, and the internet penetration rate exceeded 80%, with the benefits of digital age development reaching more social groups. In recent years, the state has continuously improved relevant laws and regulations and increased governance efforts, but there are still many practical problems in criminal regulation. In practice, the characterization of cyber violence is unclear; there are disagreements on the selection and application of charges, and the determination of causality, evidence fixation, and evidence collection are difficult. There is no unified quantitative standard for "serious circumstances." These problems together have resulted in poor effectiveness of criminal governance of cyber violence. In response, criminal legislation should be further improved, the standards for conviction and the rules for the application of charges should be refined, the boundaries of the application of each charge should be clarified, the mechanism for the connection between public prosecution and private prosecution should be improved, and a governance system involving judicial organs, network platforms, and social forces should be built to effectively curb cyber violence and effectively safeguard the legitimate rights and interests of citizens and a clean and orderly cyberspace.

Keywords: Cyberbullying; Criminal Law Regulation; Insult; Defamation

1. Overview of cyberbullying

1.1. The concept of cyber violence

According to the "Guiding Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Punishing Cyber Violence Crimes According to Law" and Article 32 of Chapter VII Supplementary Provisions of the "Regulations on the Governance of Cyber Violence Information," cyber violence information refers to illegal and harmful information that is collectively released to individuals through the internet in the form of text, images, audio, and video, containing content such as insults, slander, defamation, incitement of hatred, coercion, invasion of privacy, and accusations, ridicule, denigration, and discrimination that affect physical and mental health. ^{[1][2]} Such illegal information can cause psychological pressure on victims, damage to their reputation, psychological trauma, infringement of personal and property rights, and seriously endanger the order of cyberspace and the legitimate rights and interests of citizens. The academic community does not agree on the definition of "cyber violence." The main focus is that some scholars advocate defining it from a broad perspective, believing that cyber violence not only includes verbal violence but also technical violence such as cyber theft, cyber extortion, cyber robbery, and cyber blackmail. ^[3] According to academic theoretical research and official documents, cyber violence is defined as the act of a network user, through network media, in cyberspace, to insult, defame, incite hatred, coerce, violate privacy, or belittle and discriminate against a specific natural or legal person by means of text, pictures, videos, audio, etc.

1.2. Types of Cyberbullying

1.2.1. Online insults and defamation

The act of publishing insulting content or fabricating false information in the form of text, images, or videos directly infringes upon the personal dignity of others. Taking the case of Jiang Ge's mother

suing netizens for insult and defamation as an example, after Jiang Ge's unfortunate death, her mother's efforts to protect her daughter's rights and seek the truth should have been understood by the public. However, online public opinion gradually evolved into a malicious trial against her. On February 25, 2018, Tan Bin published a cartoon created by another person on his Sina Weibo account "Posh-Bin," openly defaming Jiang Qiulian's image and insulting her personality. The cartoon series was notarized and viewed over 24,600 times. Many netizens published harsh and aggressive comments on the platform, launching personal attacks against the parties involved—a typical example of online insult. Others fabricated and widely disseminated false information, such as the parties involved using the incident to make money or distorting the facts, intentionally damaging the parties' personal reputation—this constitutes online defamation. Some scholars have stated that these cases highlight the collective nature of online violence. Initially, public attention stemmed from simple emotions, but as online sentiment spread, it gradually morphed into collective insults and the spreading of rumors against the individuals involved. This online bullying ceased to be a normal judgment of the event and instead constituted an infringement on their personal dignity, causing severe psychological trauma to the individuals involved.^[4]

1.2.2. "Doxxing" and Privacy Violations

The illegal acquisition and public release of others' detailed personal information poses numerous real-life security risks. For example, in the case of Wu Mouhui and Chen Mouqiang's infringement of citizens' personal information, the two illegally obtained others' identity, address, contact information, and other private information through improper means, and then mass-produced this information on online platforms, causing widespread online attention and dissemination.^[5] Some netizens, influenced by this, resorted to offline harassment, severely impacting the normal lives of the individuals involved and their families. Even if there were prior disputes, the act of doxxing by bypassing judicial procedures and privately disclosing others' information constitutes a secondary infringement on the individuals. Relevant judicial interpretations stipulate that disclosing the personal information of individuals involved in disputes or suspected of illegal activities without following legal procedures, if the circumstances are serious, also constitutes the crime of infringing on citizens' personal information.

1.2.3. "Unboxing" and the Violence of Public Opinion

The act of fabricating evidence from another person's private information and publicly disclosing it to induce netizens to commit secondary harm constitutes a typical case of trial by public opinion. "Opening boxes" online is a prevalent form of online infringement, the core of which involves illegally obtaining and disclosing highly private information such as the victim's call records, whereabouts, home address, and family information, and then spreading it indiscriminately on online platforms, causing online scrutiny and targeted harm. Taking the case of Xie Guangjun, vice president of Baidu, and his daughter's "opening boxes" as an example, illegal netizens obtained and widely disseminated the victim's privacy through illegal means, resulting in online insults, text message and phone harassment, and offline disturbances—a typical example of "opening boxes." Such behavior spreads rapidly, has a wide reach, and a significant social impact. The victim not only suffers continuous online violence but also real-world harassment, with serious threats to their personal safety and normal life. From a criminal law perspective, this behavior constitutes the crime of infringing on citizens' personal information. If accompanied by insults, defamation, or other acts, it may also constitute crimes such as insult and disturbing public order. Traditional doxxing mostly relies on netizens spontaneously searching and integrating scattered information from public channels, which is a relatively loose method of information gathering; while "opening boxes" relies on technical means to illegally steal information, and on the black and gray industry chain of the Internet, the information is obtained more accurately and efficiently, and the information disclosed is the core privacy of personal life and personal safety, which is more serious and has a more obvious subjective malice.

2. Major Crimes Regulated by Current Criminal Law

In response to the different manifestations of cyberbullying, as shown in the diagram below, the current criminal law mainly applies the following crimes for conviction and sentencing:

2.1. Crime of infringing on citizens' personal information

The term "doxxing" applies when an individual illegally obtains, sells, or provides another person's personal information (such as ID number, address, and whereabouts records). In the "Wu Mouhui

case," the defendant illegally obtained the personal information of the victim and her family, and used it to smear and harass them. The court determined that her actions constituted the crime of infringing on citizens' personal information.^[6]

2.2. Defamation

The term "online defamation" applies to situations where false facts are fabricated to damage another person's reputation. For example, in the case of Lang and He, the defendant fabricated chat logs and videos alleging the victim's infidelity, causing damage to the victim's reputation. The court, based on Article 246 of the Criminal Law, determined that their actions constituted the crime of defamation.^[7]

2.3. Crime of provoking trouble

The term "creating disturbances in public places" applies to situations where disturbances are caused in public places through online means, thereby disrupting social order. In the online context, "public places" can refer to online platforms with widespread influence. When cyberbullying leads to victims being forced to resign, experiencing extreme psychological stress (such as "social death"), and has widespread dissemination, it may be considered "picking quarrels and provoking trouble."

2.4. Insult

The definition of "cyber insult" applies to the use of insulting language that severely degrades the victim's personal dignity. Even if cyberbullying only manifests as insulting verbal attacks without fabricating facts or leaking information, it may still be considered a crime of insult. (See Figure 1)

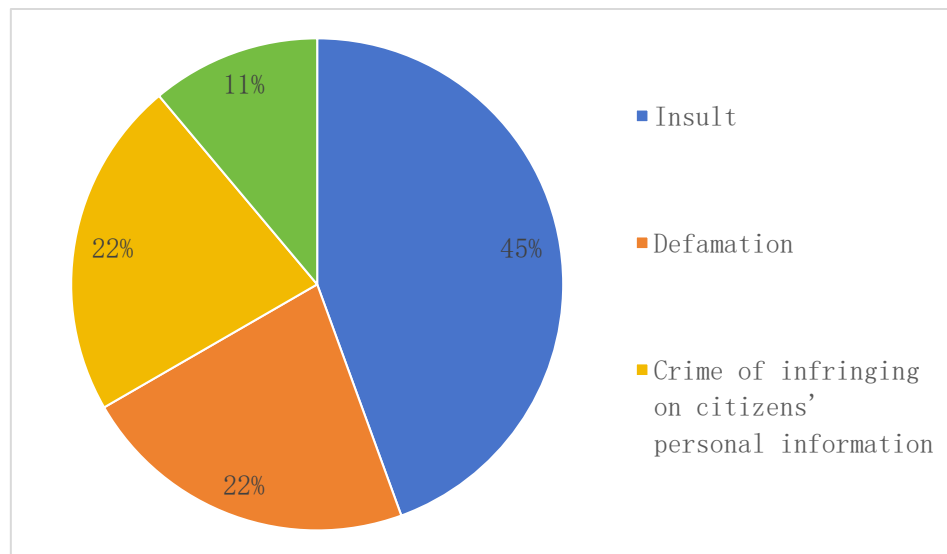


Figure 1: Major Criminal Offenses Applicable to Popular Cyberbullying Incidents from 2006 to 2026

3. The Dilemma of Current Criminal Law Regulation of Cyber Violence

3.1. The system for prosecuting cyberbullying is not well-coordinated

The fundamental reason why victims of cyberbullying face difficulties in seeking redress lies in the current system's emphasis on the parties' initiative to file lawsuits, with very few cases involving public prosecution by the procuratorate. Lawyer investigations show that in criminal cases stemming from cyberbullying, very few result in guilty verdicts through private prosecution, while a significant number are prosecuted through public prosecution. Taking the private prosecution route requires victims to personally collect and preserve various materials such as chat logs and screenshots, and complete notarization procedures. The entire process is time-consuming and laborious, posing a high legal barrier for ordinary people. Many victims are unwilling to reveal their identities, fearing continued harassment from their abusers, and thus give up seeking help. Besides individual criminal

liability, online platforms themselves also bear undeniable responsibility. In September 2023, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security jointly issued the "Guiding Opinions on Punishing Cyberbullying Crimes According to Law," providing a targeted response to the difficulties in seeking redress. The opinions stipulate that public security organs should file cases according to law for online insults and defamation that seriously disrupt social order, and that procuratorates can initiate public interest litigation for acts that harm the public interest, strengthening the judicial concept of "public prosecution as the primary method and private prosecution as a supplementary method." When victims face difficulties in obtaining evidence through self-prosecution, courts can request public security organs to assist in collecting evidence of the spread and impact of defamatory information, thereby lowering the threshold for rights protection. In June 2024, multiple departments issued the "Regulations on the Governance of Cyberbullying Information," standardizing the management of the online environment. According to the new regulations, cyberbullying refers to acts such as spreading false or true information to insult, defame, or infringe on privacy, damaging the personality and reputation of others, and causing serious consequences such as social death, mental disorder, or even suicide. These institutional arrangements provide a new path to overcome the difficulties in protecting rights against cyberbullying, but further implementation is needed in practice to ensure that these regulations truly benefit victims.

3.2. The Dilemma of Criminal Standards for Cyber Violence

Currently, the Criminal Law regulates cyberbullying through multiple crimes, but the conditions for conviction differ and the judicial discretion varies among these crimes. For new types of privacy violations like "unboxing," there is no specific standard for identification, and existing rules for conviction are insufficient to cover all. In judicial practice, the thresholds for conviction vary significantly across different crimes. Insult and defamation require serious circumstances as a prerequisite for conviction; provoking trouble requires egregious circumstances and disruption of public order; and infringing on citizens' personal information determines serious circumstances based on factors such as the quantity, type, and illegal gains of the information. These three crimes have different logics for conviction, further increasing the confusion in judicial determination. In 2021, the case of Chang et al. in Mianzhu, Sichuan, involved a dispute over a swimming pool. Chang organized and incited cyberbullying, publishing numerous insulting statements and publicly revealing the names, workplaces, and photos of Qiao and An, launching a concentrated attack for several days. The related content garnered over a million views online. An died from overdose due to the unbearable pressure. The court determined this to be a serious offense and sentenced the main perpetrator to one year and six months imprisonment. In the 2024 Qingdao Xue case involving defamation, Xue, a livestreamer, repeatedly defamed a fellow livestreamer, Ms. Jia, online, leaking Ms. Jia's daughter's school information and fabricating false claims about her chaotic private life over a six-month period, accumulating millions of views on her livestreams. This behavior led to Ms. Jia's attempted suicide by cutting her wrists, and her daughter was diagnosed with severe anxiety and depression. The court deemed the circumstances serious and sentenced Xue to six months in prison for defamation, while also banning him from livestreaming for three years. In the 2024 second-instance case of Ke v. Ai Fen for defamation, Ai Fen posted numerous accusatory posts on Weibo, garnering over 5 million views. The prolonged insults led to widespread sharing and even doxxing by netizens. However, Ke only claimed damage to his reputation, without any mention of suicide or serious injury, and failed to provide a mental illness diagnosis. Therefore, the court ultimately ruled against the case due to insufficient evidence. In the 2023 Guangzhou case of Li Jianhua suing Chen for defamation, Chen, a prominent online figure, published over 700 defamatory messages over seven consecutive months, with the highest single message reaching 290,000 views and the video garnering 527,000 views. Chen also publicly disclosed Li Jianhua's work information and maliciously insulted him. Li Jianhua did not claim suicide, serious injury, or mental illness; he only filed a civil claim. While the court acknowledged the sufficient number of views, it determined there was no substantial harm, and the sentence was significantly lighter than in similar cases where suicide occurred.

Therefore, current criminal convictions for cyberbullying rely excessively on explicit harmful consequences such as victim suicide, self-harm, serious injury, or severe mental illness. Online traffic, duration of insults, privacy breaches, and actions like exposing addresses, phone numbers, whereabouts, and private photos are only used as references in judicial decisions and cannot be the sole basis for conviction. Many cases that do not result in physical injury or serious psychological harm cannot be classified as criminal offenses and are mostly resolved through civil litigation and administrative penalties. When determining crimes, judicial organs overemphasize substantial harmful consequences. For new forms of cyberbullying like "exposure," there is a lack of specific criteria for assessing the

circumstances; the single threshold of harmful consequences is insufficient to meet the regulatory needs of various cyberbullying crimes.

3.3. The gray areas of application and overlap of charges

Cyberbullying manifests in various forms, often leading to confusion when choosing which charge to apply. The lines between defamation and disturbing public order are blurred in judicial determination, making a clear distinction difficult. In reality, when someone publishes false information that triggers large-scale online mob violence, the victim may feel they have been defamed, but prosecutors generally consider disturbing public order and social panic more likely. This raises the issue of concurrent charges, with no clear consensus on which charge should take precedence. For example, in the 2023 defamation case of Xu in Shanghai, Xu fabricated false private information about a neighbor due to a neighborhood dispute and publicly disseminated it on multiple online platforms, directly damaging the neighbor's reputation. The court ultimately convicted and punished him for defamation. In the 2024 disturbing public order case of Lin in Hangzhou, Lin fabricated false information about an industry group to gain online attention, inciting netizens to attack and causing chaos in online public order. The court ultimately found him guilty of disturbing public order. The same act of online "doxxing" and exposing others' privacy can result in completely different judicial outcomes. Some cases were classified as crimes of infringing on citizens' personal information, others as crimes of provoking trouble, and still others as crimes of insult. Some similar acts were ultimately not found to constitute crimes, indicating a lack of unified standards for the judicial handling of similar offenses. Both insult and defamation are crimes of infringing on the right to reputation. The main difference lies in the method of insult: insult uses "public insult" as a means, does not require fabrication of facts, and the perpetrator can use real personal information, but express it in a derogatory manner; defamation, on the other hand, requires "fabricating false facts" and disseminating them. In cyberbullying, insult and defamation often occur together. The perpetrator publishes false information such as "someone is a liar," along with insulting language such as "shameless." According to judicial interpretations, if the same act constitutes both crimes, it is generally punished more severely as defamation, because defamation has a stronger social harm in spreading false information. However, in practice, it is difficult to distinguish between factual statements and opinions, or between the two, resulting in a lack of unified standards for judicial organs when choosing charges.

4. Exploring Pathways to Improve Criminal Regulation of Cyber Violence

4.1. Improve the mechanism for linking prosecution with enforcement to solve the difficulties in protecting the rights of victims.

Currently, most cyberbullying cases are initiated by victims independently, with individuals bearing the entire burden of evidence collection and litigation. This is time-consuming, risky, and ineffective in preventing violence. The legal conditions for converting private prosecutions to public prosecutions should be clearly defined, allowing the procuratorate to directly prosecute cyberbullying cases involving serious personal injury, negative social impact, large-scale privacy breaches, or organized acts. Simultaneously, the power to intervene early should be granted to public security organs, enabling them to immediately secure electronic evidence, identify perpetrators, and prevent the spread of harmful information upon receiving reports, preventing evidence loss and reducing the pressure on rights protection. A unified judicial standard should be established to regulate the specific procedures for public power intervention. Cyberbullying cases involve numerous participants and diverse behaviors, and varying judicial standards across regions can easily lead to inconsistent outcomes in similar cases. A unified judicial guidance document should be formulated, detailing the standards for identifying violations, differentiating the scope of responsibility for different participants, clarifying the accountability methods for platform oversight negligence, and unifying judgment standards. This will ensure fair case handling while providing clear guidance for public power intervention. Finally, the mechanism for protecting victims' rights should be improved, and the primary responsibility of platforms should be reinforced. Evidence of cyberbullying is easily deleted and difficult to preserve, making it very challenging for victims to collect evidence themselves. The evidence-gathering process should be simplified, the legal validity of platform backend data and electronic evidence should be confirmed, and judicial authorities should assist in obtaining key evidence upon request. The obligation of platforms to preserve evidence should be clearly defined, the coverage of legal aid should be expanded, related litigation costs should be reduced or waived, privacy protection and psychological

counseling should be strengthened, and victims should be prevented from being harmed again. The responsibilities of platforms in information verification, risk warning, and other aspects should be detailed to encourage platforms to proactively prevent and control the risk of cyberbullying, reducing its occurrence at its source.

4.2. Refine the quantitative standards for the severity of circumstances to achieve fairness and uniformity in judicial decisions.

Currently, criminal law regulates cyberbullying through multiple offenses, but the conditions for conviction differ and the standards of judicial discretion vary among these offenses. Consistency in judicial rulings is crucial for the law to exert its deterrent effect. To resolve the challenges in the judicial determination of cyberbullying, it is necessary to base decisions on the different regulatory logics of each offense, refine and quantify the standards for identification in a targeted manner, and include privacy violations such as "opening boxes" in the scope of special evaluations to achieve fair and consistent judicial rulings. For the crimes of insult and defamation, the main dimensions for determination are the flow of information, the harmful consequences, and the circumstances of the behavior. Quantitative thresholds are set for reading and forwarding, and severe mental depression, forced resignation or school transfer, etc., are classified as serious consequences. Violence against vulnerable groups and the exposure of privacy accompanied by "unboxing" are directly identified as serious circumstances. For the crime of provoking trouble, the degree of disruption to cyberspace order is used as the standard for determination, and situations such as inciting large-scale cyber violence and causing offline disturbances are identified as egregious circumstances. For the crime of infringing on citizens' personal information, a separate standard for criminalizing sensitive information such as "unboxing" is set, and the crime is determined based on the type, number, and scope of information such as whereabouts, address, and private photos, rather than simply relying on the actual harmful consequences. Based on this, a comprehensive evaluation mechanism combining objective data and subjective harm will be established. Complex cases will be evaluated in conjunction with professional opinions from multiple fields. The degree of harm caused by "opening boxes" will be given more consideration. The Supreme People's Court will release typical cases and conduct judicial training to unify the national judgment standards, improve supporting judicial interpretations, and make up for the shortcomings in the regulation of new types of cyber violence. This will fundamentally solve the problems of inconsistent judgments in similar cases and ambiguous standards of identification, and effectively improve the effectiveness of criminal governance of cyber violence.

4.3. Expand the scope of application of crimes, clarify the rules of concurrence and cooperation, and fill legal loopholes.

Currently, the criminal law's regulation of cyberbullying has significant shortcomings. On the one hand, the scope of the crimes is narrow, leaving many legal blind spots, and some malicious acts cannot be prosecuted criminally. On the other hand, the boundaries between crimes are unclear, and the handling of concurrent offenses is not standardized, resulting in an imbalance in sentencing. From the perspective of the effectiveness of the current crime regulation, there are still many deficiencies. In judicial practice, the application of the crimes of defamation and provoking trouble is unclear. For cases of defamation against specific individuals, the more targeted crime of defamation should apply, but in practice, the crime of provoking trouble is applied instead. This results in overly lenient sentences for malicious cyberbullying, violating the principle of proportionality between crime and punishment and weakening the deterrent effect of the criminal law. Therefore, it is necessary to broaden the scope of application of the crime, clarify the rules of concurrent crimes, and include online violence behaviors such as non-fabricated malicious insults, personal defamation, and group attacks under criminal law, clarifying the statutory penalty standards to complement traditional crimes of insult and defamation; refine the provisions on the crime of infringing on citizens' personal information, listing malicious doxing, "unboxing" to expose core privacy, and leaking privacy that leads to violent attacks as serious circumstances, and increasing the severity of punishment; and clarify that those who organize and instigate others to commit cyber violence and use algorithms to expand the scope of harm should be punished more severely. Strictly adhering to the boundaries of the applicable crimes, the crimes of insult and defamation should be given priority when infringing on the reputation rights of specific natural persons; the crime of infringing on citizens' personal information should be given priority when engaging in "unboxing" or illegally disseminating others' private information; and the crime of provoking trouble should only be applied to a limited extent when cyber violence seriously disrupts online public order and does not constitute the first two types of crimes. Regarding the

frequent occurrence of "box-opening" behavior in judicial practice, a rule for determining guilt based on different circumstances should be established. Specifically, if an individual uses technical means or the black market to illegally obtain core personal information such as another person's home address, contact number, whereabouts, family information, or private images, and then disseminates it publicly without authorization, with the primary act being the disclosure of privacy, the crime of infringing on citizens' personal information should be directly applied. If, after disclosing privacy through "box-opening," insulting remarks or fabricated facts to defame the individual are also published, thus infringing on the individual's right to reputation, then both the crimes of infringing on citizens' personal information, insult, and defamation are constituted. If the "box-opening" behavior causes a large-scale online uproar and insults, seriously disrupting the order of online public communication, and does not constitute the aforementioned crimes, the crime of provoking trouble can be applied cautiously, resolutely preventing the arbitrary application of charges. At the same time, the principle of "punishing for the most serious crime" should be established, meaning that for the same act of cyberbullying, if multiple crimes are committed simultaneously, the crime with the heavier sentence should be used for conviction and punishment, preventing arbitrariness in the selection of charges.

5. Conclusion

As a new type of social hazard bred in the digital age, cyber violence has evolved from individual verbal conflicts into a compound harmful act that can seriously erode personal dignity, disrupt public order, and even endanger life. Although the current criminal law has initially constructed a regulatory framework covering crimes such as insult, defamation, infringement of citizens' personal information, and picking quarrels and provoking trouble, and judicial practice has continuously explored governance boundaries through guiding cases and judicial interpretations, there are still significant shortcomings in the coordination of litigation procedures, quantification of conviction standards, and coordination of charge application when facing the special object of "cyber violence", which is characterized by anonymity of participants, complexity of infringing acts, and superimposition of harmful consequences.

This study shows that the deep root of the governance dilemma lies in: the traditional criminal law's conviction logic centered on "actual harmful consequences" cannot effectively respond to the new harmful generation models of "traffic equals harm" and "exposure equals punishment" in cyber violence; the private prosecution-oriented prosecution procedure, when facing technical obstacles to evidence collection and group-based infringements, actually weakens the deterrent effect of criminal law; and the ambiguous boundaries between charges and the lack of concurrence rules lead to imbalances in judicial discretion, which may either condone crimes due to "downgraded handling" or violate the principle of proportionality between crime and punishment due to "light sentencing for serious crimes."

To solve the above dilemmas, it is urgent to achieve a deep coupling of criminal law norms and the laws of cyber governance. This not only requires, through judicial interpretation or legislative amendment, bringing new types of privacy infringements such as "deep doxxing" into an independent evaluation dimension, and refining the quantitative standards of "serious circumstances" to eliminate legal ambiguity; but also requires constructing a smoothly connected "private prosecution-public prosecution" mechanism for public power intervention, strengthening the platform's obligations for data preservation and risk warning, so as to open the "last mile" of rights relief. At the same time, the applicable boundary of the crime of picking quarrels and provoking trouble in cyberspace must be carefully defined, and the priority order of charges such as insult and defamation should be established to prevent the tendency of "pocket crimes" from eroding the foundation of the principle of legality.

Ultimately, the criminal law regulation of cyber violence is by no means a purely technical legal issue, but a systematic proposition concerning the protection of citizens' fundamental rights in the digital age, the maintenance of order in cyberspace, and the perception of social fairness and justice. In the future, on the basis of adhering to the principle of modesty of criminal law, we should promote the coordinated progress of criminal legislation, judicial practice, platform governance, and improvement of civic literacy, and build a diversified co-governance system featuring "precise legal regulation, substantive platform responsibility, convenient rights relief, and normalized preventive education." Only in this way can we build a solid legal dam for the protection of citizens' rights in the turbulent digital torrent, and achieve a deep leap from "symptomatic treatment" to "root cause treatment" for a clean and orderly cyberspace. Only thus can criminal law truly become a sharp sword to curb the evil of cyber violence, rather than a helpless shield after the fact.

References

- [1] Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security. *Guiding Opinions on Punishing Cyber Violence Crimes According to Law: Fa Fa [2023] No. 14 [Z]*. 2023-09-20.
- [2] Cyberspace Administration of China, Ministry of Public Security, Ministry of Culture and Tourism, et al. *Regulations on the Governance of Cyberbullying Information: Cyberspace Administration of China Order No. 17 [Z]*. 2024-06-12.
- [3] Liu Xianquan, Zhou Zijian. *The dilemma of criminal law regulation of cyber violence and its solution [J]*. *Legal Research*, 2023 (5):16-27.
- [4] Chu Chencheng. *The Evolution of Criminal Law's Response to Cyber Violence and Its Basic Stance [J]*. *Chinese Journal of Criminal Law*, 2023 (4):35-52.
- [5] Supreme People's Court. *Typical Cases of Punishing Cyber Violence and Crimes According to Law [EB/OL]*. (2023-09-26)
- [6] *Criminal Law of the People's Republic of China [M]*. Beijing: Law Press, 2024.
- [7] Supreme People's Procuratorate. *34th Batch of Guiding Cases: Case No. 137, Lang and He's Defamation Case [Z]*. 2022-02-22.