On the Criminal Laws and Regulations of Cyber Violence in the Environment of the New Era and Suggestions for Improvement

Hanfei Qu *

Southwest University of Political Science and Law, Baosheng Road, Chongqing, China

*Corresponding author's Email: quhanfei@ldy.edu.rs

Abstract. Today, with the rapid development of the Internet, the network provides convenience to the general public, but also creates new problems. Because of the virtual nature of the Internet, it is often difficult to hold individuals accountable for what they say on the Internet, thus generating cyber-violence that is group-based and covert, inflammatory and blindly obedient, and with lower costs for cyber-violence offences. Cyber violence is quite different from traditional violent crimes, and the criminal forms of cyber violence often are often manifested as cyber language violence, cyber moral judgement and cyber human flesh search and so on. However, the existing traditional legal provisions are not able to regulate cyber violence crimes in the environment of the new era well, and therefore it is necessary to improve the legal provisions for the new forms of crimes. Through research methods such as literature analysis and comparative analysis, this paper proposes three levels of recommendations based on the existing dilemma of regulating online violence, including strengthening active guidance and supervision of the online public, improving legislation and justice, and deepening regulatory responsibility. The purpose of this paper is to analyse the current situation and predicament of cyber violence and put forward suggestions for improvement, with a view to building a better spiritual home on the Internet.

Keywords: Cyber violence; criminal regulation; refinement of the proposal

1 Introduction

With the advent of the age of self-media, the dissemination of information is no longer limited to the traditional paper-based media, and the public can learn about the world's affairs without leaving their homes, but this over-expansion of freedom of expression has also led to the increasingly serious problem of cyber-violence. Insults, defamation, invasion of privacy and other remarks made against others on the Internet gradually evolve into cyber-violence with the accumulation of time, creating a storm of public opinion, and may even lead to serious consequences such as mental disorders or suicides of the victims. At the same time, a large amount of negative information converges in cyberspace, which invariably aggravates social hostility and is not conducive to maintaining a positive social state.

L. Zhu et al. (eds.), *Proceedings of the 2024 4th International Conference on Public Relations and Social Sciences (ICPRSS 2024)*, Advances in Social Science, Education and Humanities Research 874,
https://doi.org/10.2991/978-2-38476-305-4_12

Liability for acts of cyberviolence in China is mostly regulated through civil and administrative law, and the criminal law covers the offences of insult and defamation; however, the criteria for applying these offences in the cyberenvironment are unclear, and in practice, few cases brought as a result have resulted in a conviction. Academic research on cyberviolence covers a variety of fields, including law, journalism and communication, psychology and sociology. From a legal point of view, the current law does not make specific provisions on the concept, nature and identification criteria of cyber-violence, and it is difficult for traditional legal regulation to produce effective deterrence and remedial effect on cyberviolence.

This paper proposes theoretical support for this emerging field by discussing the concept of cyber-violence at the theoretical level, and analysing the current legal provisions and application dilemmas of cyber-violence in China. At the practical level, this paper puts forward regulatory proposals from the perspective of citizens, law enforcers, legislators and superviors, with a view to contributing to the development of the criminal law system for the governance of cyber violence.

2 Definition of Concepts Related to Cyberviolence

2.1 The Concept of Cyberviolence

At the level of jurisprudence, different countries do not have the same definition of cyber-violence, and British scholar Peter K. Smith considers cyber-violence to be a purposeful and aggressive behaviour carried out by an individual or a group of individuals, which attacks the victim multiple times, repeatedly and injures the victim by means of electronic communication technology [1]. The National Crime Prevention Council of the United States of American in Washington, D.C., considers cyberviolence to be the use of the Internet, mobile phones or other electronic communication devices to post or send words or images intended to harm another person [2]. However, the concept of cyber-violence is not clearly defined in existing Chinese law, and there are different views on the definition of cyber-violence in Chinese academia. With the rapid development of the Internet and the increasing popularity of the information network, cyber violence has become increasingly visible, mainly consisting of human flesh searches of citizens' personal information and group cyber language violence, which infringes on the personality rights, honour rights and privacy rights of a particular subject by means of verbal bullying of the subject, and inflicts harm on the spirit of a particular subject [3].

2.2 Characteristics of Cyberviolence

Cyber violence is characterised by four main subjects. Firstly, cyber violence has a group and hidden nature. Cyberviolence is distinguished from traditional forms of violence in that it is often verbal violence perpetrated by unspecified groups. In practice, the perpetrators of cyber violence are often the so-called "passers-by", unspecified subjects who infringe on the interests of others without knowing the facts or under the guidance of malicious organisers, and the roles assumed by the subjects who carry out

cyber violence are not fixed from the beginning, and the initial "passers-by" are not fixed from the beginning. Initially, "passers-by" are only participants or discussants of the topic, but after several "passers-by" spontaneously forward or comment on the follow-up posts, they gradually transform into group abusers. Cyberspace itself is a virtual space with significant virtuality, cyberspace is a non-physical space constructed by algorithmic language, cyberspace is the second living space of human beings produced under the environment of the new era, and physical space is different from the physical space, the subjects in the physical space have clear identity information, while the subjects in the virtual space are all mysterious and only digitally expressed [4]. The existing technical means can not be the subject of the network virtual space specific positioning to the individual, can only lock the subject account IP address, but for the actual use of the IP address under the person still can not be determined, the subject of network behaviour has a strong hidden. Secondly, cyberviolence is inflammatory and blind. The dissemination of online events tends to be rapid and, unlike the paper medium, the dissemination of online hotspots is instantaneous. Cyber violence resulting from hot-button events is often inflammatory. Cyber violence is different from violence in the traditional sense, cyber violence usually takes advantage of and exaggerates social hotspot events, stimulates the attention of the cyber public through remarks of unknown truth or subjective bias, blames individuals for normal contradictions, and then incites the cyber public to attack the hotspot events, which leads to individuals suffering from cyber verbal violence and affects their normal life and mental health [5]. Participants in cyber violence are not all based on malicious purposes, network information is often mixed and it is difficult to distinguish between truth and falsehood, the network public based on the herd mentality will be based on their own limited knowledge of the situation to make a subjective evaluation, but there is still a one-sided negative evaluation of the harm caused by cyber violence results occur. Thirdly, cyber violence is harmful. Cyber violence often provokes a moral judgement of the cyber public against a specific subject by means of antagonism, showing a situation of "winning by many against few", causing a specific subject to suffer from psychological oppression as well as collective negative judgement and bullying intrusion, which in turn may cause a specific subject or his close relatives to suffer from mental torture or even serious consequences such as suicide [6]. Fourthly, the cost of violating the law for cyberviolence is low. Because of the group nature of cyberviolence, participants often develop a mentality of legal impunity. Cyberpublics often believe that they are merely expressing their subjective opinions on the Internet by tapping on their keyboards, and do not believe that there is a casual link between their behaviour and the eventual serious consequences. Moreover, most participants in cyberviolence incidents take a chance, believing that even if there are serious consequences, due to the complexity of the cyberworld and the groups involved, it is ultimately difficult to trace their true identities and hold them legally accountable. In judicial practice, the current legal provisions for network violence punishment is small, and in practice for the relevant evidence is more difficult to identify, in practice, network violence often make a judgement of innocence, which contributes to the network language violence of the undesirable trend, but also aggravated the hostility of cyberspace.

2.3 Types of Cyber Violence

Cyber-language Violence.

Online language violence is a negative comment against the rights and interests and mental health of a specific subject published through an online platform. Internet language violence can generally be divided into fabricated language violence and anger-expelling language violence [7], and fabricated Internet language violence often involves insulting and slandering others by fabricating false facts. Article 246 of *the Criminal Law of the People's Republic of China* stipulates the crimes of insult and slander, which are the acts of blatantly contaminating another person or fabricating facts to slander another person by means of violence or other methods. Indignant online language violence is due to the aggravation of social hostility, the Internet public out of malignant purposes, wantonly venting and attacking others on the Internet. The rights and interests violated by cyberlanguage violence are usually the rights of honour and personality of others, causing damage to the psychological and mental health of others. Even if remedies are made afterwards by clarifying or deleting the relevant remarks, the impact on the person concerned is already irreversible [8].

Cyber Trial of Ethics.

Morality refers to the sum of codes of conduct and norms that are sustained and brought into play by social opinion, traditional customs and inner beliefs [9]. Moral judgement means that the perpetrator accuses and criticises the actions or omissions of others through a high standard of moralty, overly magnifies the faults and shortcomings of others, with the aim of controlling them, and cirticises and attacks others through moral and public opinion pressure. However, the standards of moral judgement are often not practical and often surreal and unattainable [10]. Netizens who carry out online moral judgement often stand on the moral high ground, demanding unreasonable moral standards from others, and blaming conflicts and faults on the deficiencies of other people's character without considering the actual situation. Due to the group nature of cyber violence and blind obedience, cyber moral judgement is very easy to trigger the support and followers of the cyber public, and then form a large number of cyber moral judgement, which will eventually cause great oppression and damage to the victim's psychology, and may even lead to serious consequences such as suicide. There is a certain commonality between public opinion monitoring and cyber moral judgement, both of which are targeted at words and deeds that violate morality or the law, and both of which negatively evaluate some negative social phenomena. In contrast to cyber-ethics trials, the monitoring of public opinion is an expression of the right to freedom of expression that citizens enjoy under *the Constitution*, as well as an expression of democracy and the rule of law. What's more, public opinion monitoring is not absolute but relative, and public opinion monitoring is limited to the extent that it does not infringe upon the interests of the state, the public interest and the interests of others. While *the Constitution of the People's Republic of China* grants citizens the right to monitor public opinion, it also imposes restrictions on the exercise of that right [11].

Internet Flesh Searches Violate Personal Information.

Internet human flesh search refers to the network public through the electronic network information platform, the collection of personal information of a specific object, through the virtual network to publish the personal information of a specific object, without the permission of a specific party that is exposed to its personal information, which leads to the person concerned to suffer a lot of verbal abuse and even threatened, and its impact on the person concerned by the virtual network extends to the person's real life, seriously affecting the person concerned and his or her close family members of the normal life[12]. The behaviour of online human flesh search violates the privacy and personal information of the person concerned, and *the Civil Code of the People's Republic of China* contains detailed provisions on the definition of the right to privacy and the scope of protection and so on, which provide comprehensive and detailed regulations on the right to privacy.

Cyber Provocations.

With the development of the network gradually appeared network-type provocations, cyber provocations are mainly divided into verbal abuse and intimidation type and false information type [13], in cyberspace, verbal abuse, intimidation of others or fabricated false information, so that the victim's property or personal rights and interests have been infringed upon. However, cyber provocation is not the same as provocation in the traditional sense. Firstly, due to the virtual nature of cyberspace, and the hidden nature of cyberviolence itself, cyber provocations provide a place of offence that is difficult to trace. Secondly, compared with traditional provocations, cyber-type provocations have a diversity of modes of behaviour and are no longer restricted by time, space and persons, and can be committed in words, pictures or any other form at any time against an unspecified person, and therefore have more serious consequences [14].

3 Existing Legal Provisions Relating to The Regulation of Cyber Violence and the Dilemma of their Application

3.1 Existing Legal Provisions Regulating Online Violence

China's current legal system does not provide a clear definition of cyberviolence, and there are no specific laws or regulations on cyberviolence, with only some vague and scattered provisions.

China's system law system does not have direct provisions on cyber violence, but rather through the rights and interests related to the concept of cyber violence*, the Civil Code of the People's Republic of China*, promulgated and implemented in 2021, has added a personality rights section, which stipulates that the rights to privacy, reputation, personality, personal information and other rights are protected by law, and the tort liability section also provides for the pursuit of liability for cyber infringement, Article 1194 to 1196 specifically provide for the tort liability of network users and network service providers.

China's administrative law system also does not provide criteria for the identification of cyberviolence, and in practice it is difficult for administrative law enforcement officials to identify cyberviolence, which is generally dealt with in accordance with *the Law of the People's Republic of China on Punishment for Public Security Administration.*

In China's criminal law system, the only offences related to cyberviolence are the offences of insult and defamation and the offence of violating personal information. In *Amendment VII to the Criminal Law*, offences such as illegally providing, obtaining or selling personal information were brought under the scope of criminal law. The liability of online platforms and online service providers has been clarified in *Amendment IX to the Criminal Law*. The provisions on cyberviolence in China's criminal law system are being gradually expanded in line with the development of the times.

Article 1 of *the Cybersecurity Law of the People's Republic of China*, which came into force in 2017, stipulates that this law is formulated to ensure cybersecurity, safeguard the sovereignty of cyberspace and national security, public interests of the society, protect the legitimate rights and interests of citizens, legal persons and other organisations, and promote the healthy development of economic and social informatisation. The newly promulgated *Provisions on Ecological Governance of Network Information Content* and *Measures for the Administration of Internet Information Servies* in 2020 provide for insults and defamation of others as well as the spreading of online rumours. The protection of the rights and interests of personal information has been strengthened in *the Law of the People's Republic of China on the Protection of Personal Information*, which was promulgated and implemented in 2021. In 2023, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security issued a circular on the *Guiding Opinions on Punishing Internet Violence and Illegal Crimes in accordance with Law*, which stipulates the rules applicable to the crimes of cyberviolence, including the identification of cyber-defamation, the determination of cyber-insults, the handling of the organisation of "human flesh searches", the handling of malicious speculation through cyberviolence, and the application of the offence of refusing to fulfil the obligation of information network security management. On the basis of the existing provisions, the specific application has been refined, which is conducive to punishing illegal and criminal activities of cyber violence in accordance with the law, and effectively safeguarding the rights and interests of citizen's personality and the order of the network.

3.2 The Dilemma of Regulating Online Violence

Difficulty in Regulating Mass Violations.

Cyberviolence is mass and blind, and the large number of cyberpublics involved in cyberviolence often makes it difficult to hold each individual involved in cyberviolence legally accountable. Restricted by the virtual nature of the network platform, network users in the network platform registration information is not the real identity information, network users published speech and behaviour is more shielded, the relevant authorities in the tracking is only able to lock the IP address, but can not be located to the specific individual, which results in the group infringement is difficult to regulate

and control, infringed upon is often difficult to bring a lawsuit against a clear defendant or to defend the rights of the person. The large base and uncertainty of Internet users make it more difficult for infringers to enforce their rights [15].

Existing Legal Remedies are Ineffective.

The penalties in China's current laws are not strong enough to have a deterrent effect. In China's civil law system, most of the ways of assuming responsibility for the infringement of cyber violence are stopping the infringement, compensating for the loss, apologising and eliminating the influence and so on. These ways of assuming responsibility are compatible with minor cyber violence, but for the serious consequences of serious cyber violence, such as serious damage to the infringer's reputation, serious detriment to the infringer's property, serious damage to the infringer's physical and psychological health or even the infringer's physical health, it is obviously inappropriate to regulate the consequences of serious online violence only with the civil law of the responsibility. Civil torts, where comments and criticisms exceed legal boundaries for the purpose of infringing on the rights to honour and privacy, are not sufficiently regulated by civil law and needed to be regulated by criminal law in the case of serious acts of cyberviolence [16]. Administrative regulations share the same remedial dilemma as civil law, with administrative law penalties mostly consisting of fines and administrative detention, which are difficult to match the consequences of serious cyber-violence and fail to produce a deterrent and remedial effect.

At the legislative level, not only is there a lack of specific, regulation in criminal law, but the criteria for recognition are vague. China's criminal law system does not directly provide for the regulation and application of rules on cyberviolence, and the only provisions relating to cyberviolence are the offences of insult and defamation, infringement of personal information, and provoking trouble. However, the offence of insult and defamation is a "pro-indictment" offence, which is dealt with only when told to do so, and it is often difficult to pursue criminal liability in judicial practice. The boundary between undesirable Internet speech and freedom of expression is relatively vague, but the current law does not provide clear standards for undesirable speech. In essence, it is difficult to judge whether Internet language is insulting or illegal because it is more abstract, and the Guiding Opinions on the Punishment of Illegal and Criminal Acts of Cyber Violence in accordance with the Law only differentiate between illegal and criminal acts of cyber violence and lawful acts, and stipulate that the criminal act of cyber insults and defamation will not be recognised as an illegal and criminal act of cyber insults and defamation.

Unclear Responsibility for Network Regulation.

There is a lack of oversight of ISPs. Internet information departments at all levels should play an administrative supervisory role and carry out special governance of network service provision platforms. However, the Internet information department, the public security department and the judicial organs should clarify their respective responsibilities. At the present stage, the functions of the various departments in dealing with incidents of cyber-violence are relatively dispersed, and they tend to perform their

functions to provide relief only after incidents of cyber-violence have occurred, and there is a lack of prevention and regular supervision.

The regulation of online information by network service providers is ineffective. Article 1195 of *the Civil Code of the People's Republic of China* stipulates that ISPs have an obligation to supervise and manage and shall take the necessary measures upon notification by an Internet user, but the provision does not specify the scope of management by ISPs or the specific criteria for taking effective measures afterwards. The Provisions on Network Information Governance promulgated and implemented on 1 August 2024 made further detailed provisions on the prevention and warning mechanism, information and account disposal, and protection mechanism of network service provision platforms, but the assumption of legal responsibility for network service provision platforms remains vague. Most of the network service providers take commercial interests as their main consideration, and the regulation of network information is passive, therefore, clear legal provisions are needed to determine in detail the legal responsibility of network service providers, and urge them to fulfil their obligations and assume legal responsibility through regulation at the national level.

4 Suggestions for Regulating Cyber Violence in the Internet Environment of the New Era

4.1 Strengthening Active Guidance and Supervision of the Online Public

Strengthening Ideological Education for the Online Public.

Adhere to the guidance of Xi Jinping's thought on socialism with Chinese characteristics in the new era, thoroughly implement Xi Jinping's thought on the rule of law and General Secretary Xi Jinping's important thought on a strong network, and adhere to positive public opinion guidance. In 2021, the Central Internet Information Office issued *the Outline of Action for Enhancing Digital Literary and Skills of the Whole Population*, which seeks to strengthen publicity and education on civilised and lawful and healthy access to the Internet, and to raise the awareness of the Internet public in terms of rational thinking and social responsibility, as well as in terms of compliance with the rules of order in cyberspace.

Increasing Vigilance and Precautionary Awareness of the Cyber Public.

Be vigilant about the collection of personal information or other personal privacy in cyberspace, and reduce the release and registration of personal information on online platforms to avoid leakage of personal information. For infringements such as privacy leakage or human flesh search that you may suffer or have already suffered, you should promptly notify the online platform to take measures and request help from the relevant authorities, and dare to defend your rights.

The Online Public should Reject the Idea that the Law is not Accountable to the Public.

The online public should be responsible for their own online speeches, and *the Guiding Opinions on Punishing Internet Violence and Illegal Crimes in accordance with the Law* states that a zero-tolerance attitude should be upheld, the erroneous tendency of "not blaming the public for the law" should be effectively corrected, strict law enforcement should be adhered to, and responsibility should be seriously investigated in accordance with the law, with a focus on cracking down on the malicious initiators, organisers, and those who maliciously promoted and contributed to the crime as well. The online public should set up a correct cognition, reduce negative comments and retweets for hotly debated events on the Internet, and not just stand on the moral high ground and judge others, exporting their negative energy and dissatisfaction to unspecified people. With the increasing promotion of the real-name system on the Internet, the Internet public should take responsibility for their own words and deeds, participate in Internet activities and discussions sensibly, and jointly build a harmonious cyberspace.

4.2 Improving Legislation and the Judiciary

Criminalisation of Cyber Violence Offences.

Cyber violence, as a product of the development of the new era, is difficult to regulate in the traditional sense of the law. Most scholars in the academic world have a positive attitude towards the criminalisation of cyber violence offences. Professor Zhang Mingkai is of the view that China's current efforts to satisfy protected legal interests by adopting the creation of new offences should take full account of the principle of legal interest protection, clarify the setting of constituent elements, and allow the new offences to supplement the inadequacies of the existing criminal law system [17]. Professor Chen Xingliang is of the view that if the cyber behaviour cannot correspond to the real behaviour, exists only in cyberspace and its influence is mainly in cyberspace, it cannot be criminalised by traditional crimes and a separate new offence has to be created [18]. In judicial practice, cyber-violence crimes are new forms of crime, and the provisions on cyber-violence in existing laws are vague and fragmented, making it difficult for judicial staff to identify and judge cyber-violence, and it is very easy to end up with acquittals in practice, which is not conducive to the punishment of cyber-violence crimes. Therefore, it is not only necessary but also urgent to create a new offence in the criminal law for cyber violence crimes.

Refinement of Concepts Related to Cyber Violence.

To clarify the concept of cyberviolence, including the constituent elements of cyberviolence offences, such as the subject of infringement, the object, the subjective and objective factors, to clarify that cyberviolence offences are unlawful, and to distinguish between cyberviolence offences and traditional offences. Clarify the responsibilities of online service provision platforms by refining the relevant legal provisions. Network service provision platforms pursue profits, so they should assume legal responsibilities that match the benefits they receive, provide early warning and remedies, and closely

monitor network information. It is necessary to refine the determination criteria and defamation; uniform standards should be established for the determination of the main acts of aggression and the results of the acts, which are stipulated in *the Interpretation of Criminal Cases of Online Defamation*. However, with the development of the Internet era, this provision is still subject to many limitations and should be adjusted in keeping with the times. For the determination of the number of clicks and views, invalid data should be deleted from the statistics and considered in conjunction with the number of people who actually use the platform.

Giving Full Play to the Functions of the Judiciary.

At the legislative level, the legislature should promote the process of criminalising cyberviolence offences, summarise and refine the legal provisions on cybercrime, clarify the responsibilities of all parties, and establish by law the responsibilities of the platforms that provide online services, the cyberpublic, and the relevant authorities with regard to cyberviolence offences, so that cybergovernance can be based on the law.

At the law-enforcement level, public security and Internet information departments should fulfil their respective responsibilities in accordance with the law, establish a coordinated sharing mechanism, provide advance warning of incidents of cyberviolence, file and investigate cases of cyberviolence that they have already occurred, and collaborate with each other. For incidents that either department determines to be cyber violence, they should work together to notify the other department in a timely manner. For complaints received by the Internet information department, the public security department should be notified in a timely manner, and the person concerned should be informed that he or she can report the case to the public security authorities, which, upon receipt of the report, should open a case in a timely manner, and the Internet information department should assist the public security authorities in conducting the investigation, and work together to establish avenues for the person concerned to safeguard his or her rights.

In the area of trials, the training of trial staff should be strengthened for new forms of cyberviolence offences. With the increasing number of cases of cyber-violence crimes, trials of cyber-violence crimes should be more specialised, and new forms of evidence collection and identification of cyber-violence crimes should be adopted to strengthen the extraction and analysis of evidence and clues.

4.3 Deepening Regulatory Responsibility

Strengthening Joint Supervision of Online Platforms by Relevant Departments.

As the main department to fulfil the administrative supervisory responsibility for network service provision platforms, the Internet information department should implement the supervision of network service provision platforms. In addition, the regulation of online service provision platforms should be regularised alongside specialised governance.

A joint multisectoral regulatory system should be established to monitor and govern in collaboration with public security and judicial authorities. Each department has its

own responsibilities, assists and co-operates with each other, establishes an information-sharing platform, establishes a governance system of early warning and remedies for network service providers, provides infringers with a smooth avenue to defend their rights, and implements effective supervision of network platforms in an all-encompassing and multi-dimensional manner.

Strengthening the Supervision and Management Responsibilities of Network Service Providers.

The Civil Code of the People's Republic of China provides for the supervisory responsibility of ISPs, but only stipulates that ISPs are only required to take measures upon receipt of notification, which only covers post-event remedies. Network service providers should assume the responsibility of supervision in the whole process, and before the occurrence of network violence, network service providers should use computer algorithms to establish an intelligent detection system to spontaneously supervise the content of network information, and take measures such as blocking and deletion of undesirable remarks in a timely manner, so as to avoid the occurrence and expansion of network violence. At the same time, in the course of day-to-day supervision, the Internet public should be reminded in a timely manner and prompted to comply with the provisions of the Internet order through pop-up windows or other forms. After the occurrence of an incident of cyber violence, the accounts of the facilitators as well as the participants of cyber violence should be counted and locked in a timely manner, the accounts concerned should be disposed of, the cyber public should be correctly guided in a timely manner, and the results of the disposal should be made known to the public.

5 Conclusion

Cyber violence is a product of the development of the Internet, and is the impact of the new era of criminal behaviour on the traditional legal regulation. The problem of cyber violence is a hot issue of concern in countries all over the world. The public is subject to increasing social pressure, and the emergence of the Internet has provided the public with an outlet for catharsis, and social hostility has gradually intensified, in which the public has committed acts of cyber-language violence, cyber-moral judgement, human searches or provocations against unspecified parties to the incident, and the public has been subjected to the domination of group and blind obedience that has gradually evolved into cyber-violence incidents. The provisions on cyber violence in China's existing laws are scattered and vague, with no unified and exhaustive system, thus giving rise to the dilemma that group infringement is difficult to regulate, the existing legal remedies are ineffective, and the responsibility for cyber supervision is unclear. In response to these dilemmas, improvements can be made in three major areas, including strengthening guidance and supervision of the online public, improving legislation and justice, and deepening regulatory responsibility.

By optimising the regulation of cyber violence crimes, cyber order can be better maintained, which is conducive to building a clear and orderly cyberspace. However, the recommendations in this paper for improving the criminal law system for cyber

violence offences still need to be studied in depth, and need to be combined with judicial practice to make further explorations.

References

1. Peter K. Smith, Jess Mahdavi, Manuel Carvalho, Sonja Fisher, Shanette Russell, and Neil Tippett. (2020). Cyberbullying: itsnature and impact in secondary school pupils.UK: Goldsmith University of Londaon.
2. John Chapin. (2016). Adolescents and Cyber Bullying: The Precaution Adoption Process-Model. Education and Information Technologies.
3. Huang, Y. (2021). Research on the Criminal Law System of "Cyber Violence". Master's thesis, Southwest University of Political Science and Law.
4. Wang, J. (2022). Ethics of Digital Citizenship. Journal of East China University of Political Science and Law.
5. Shi, J., & Huang, Y. (2020). Analysis of the Dilemma and Exploration of the Way Forward in the Criminal Law System of Cyber Violence. Anhui University Journal.
6. Huang, Y. (2021). Research on the Criminal Law System of "Cyber Violence". Master's thesis, Southwest University of Political Science and Law.
7. Hou, Y., & Li, X. (2017). An Analysis of the Motivations and Influencing Factors of Internet Violence among Chinese Netizens[J]. Journal of Peking University (Philosophy and Social Science Edition).
8. Feng, L., & Fu, W. (2021). The Causes and Corrections of "Social Death" in the Age of Social Media. Young journalist.
9. Luo, G. J. (1989). Ethics. People's Publishing House.
10. Zheng, G. (2009). Ethical reflections on the moral judgement of the mass media. Journal of Zhejiang University (Humanities and Social Sciences Edition).
11. The Constitution of the People's Republic of China. (2023). Beijing: China Legal Publishing House.
12. Fu, L. (2017). Human Search: the operation of fluid dynamic social power and its path to normativity. Doctoral dissertation, East China University of Political Science and Law.
13. Wu, Y. (2022). Study on the "Pocketisation" of the Offence of Picking Quarrels and Provocations. Journal of Shanxi Politics and Law Management Cadre College.
14. Wang, G. (2023). Criminal Law Principles of Cybercrime[M]. Beijing: Law Publishing House.
15. Chen, X. (2021). The Regulatory Path of Personal Information Protection under the Perspective of Cyber Violence. Application of law.
16. Yang, L. X. (2013). Civil Law Empire. China Legal Publishing House.
17. Zhang, M. (2020). The Concept of the Creation of New Offences----Support for a Positive View of Criminal Law. Modern Jurisprudence.
18. Chen, X. (2021). Types of Cybercrime and Their Judicial Recognition[J]. Rule of Law Research.