Typological Analysis of Network Violence and Research on Criminal Law Regulation

Rui Xu[1, a*], Yuxiao Quan[2, b], Bo Yuan[3, c]

[1]Shanghai University, Major in Law, Law School, Shanghai, 200444, China
[2]Donghua University, Major in English Literature, Foreign Language College, Shanghai, 441002, China
[3]Russian Speciality Yancheng Teachers University, School of Foreign Languages, Yancheng, 224002, China

[a*]1994572882@qq.com, [b]952723232@qq.com, [c]1710184086@qq.com

Abstract. In the information age, the Internet is increasingly connected with people ' s daily life and has become an indispensable part of people's social life. Network violence, as a new social phenomenon, has the characteristics of group-oriented, extreme, organized, young participants and great harm in reality, which poses a serious threat to social order and individual rights and interests. This paper first makes a type analysis of network violence, distinguishes between traditional network violence and new network violence, discusses its regulatory dilemma in the field of criminal law from macro and micro perspectives, and puts forward corresponding solutions, aiming at providing theoretical support at the legal level for the construction of a healthy network environment. In view of this, this paper introduces the comparative research method, draws on international experience, and puts forward strategies to solve the dilemma of cyber violence criminal law regulation. Specifically, this paper advocates the expansion and debugging of existing charges by the interpretation principle of criminal law, and explores the compatible path of existing charges to network violence, so as to build a more comprehensive and effective prevention and control mechanism of network violence under the legal framework.

Keywords: Network violence; Typification; Realistic dilemma; Criminal law regulation

1 Introduction

As of December 2023, the number of netizens in China has reached 1.092 billion. The Internet penetration rate climbed to 77.5 percent. Popularity of the Internet has greatly promoted social progress, but it also comes with multiple risks. The decentralized and anonymous nature of the Internet has weakened moral constraints and

[a] Both Rui Xu and Yuxiao Quan contributed the same amount and were the first authors.

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_17

made cyberspace a breeding ground for negative emotions [1]. Network violence called "hurting people by pressing buttons" and "killing people by pressing buttons" happens frequently, becoming a serious problem that needs urgent treatment in society. Although China has comprehensively regulated network violence through many departmental laws, judicial interpretations and relevant regulations, due to the characteristics of network language violence, its practical effect is limited, and it is still difficult to control network violence in practice. This paper sorts out the types and difficulties of network violence, and puts forward the strategies to deal with network violence to contribute to the harmony and stability of the Internet public space and safeguard the social public interests. Although there is a lot of discussion on network violence in the academic world, there is no unified definition of it. This paper discusses the types and governance of network violence on the basis of the ***Network Violence Information Governance Provisions*** (hereinafter referred to as the ***Regulations***), and the network violence referred to in this paper is also the "network violence information" referred to in the ***Regulations***.

2 The Characteristics and Hazard Analysis of Network Violence

2.1 Groupization and Radicalization

The collectivization and radicalization of network violence is reflected in the suppression of minority opinions by the majority [2]. Network violence is generated by the joint participation and promotion of many netizenson online platforms, and has significant group characteristics. First of all, on social media and other platforms, specific events are easy to arouse the emotional resonance of netizens and prompt them to gather quickly, which is the cornerstone of the group nature of network violence. Secondly, participants show a strong tendency to follow the crowd and imitate in their online behaviors. The anonymity and virtuality aggravate the psychology of "the law does not blame the crowd", leading individuals to blindly follow the opinions of the group and even make extreme remarks to seek group approval. The mutual imitation and reinforcement of this behavior further highlights the group nature of network violence. Moreover, there is often a certain degree of connection and interaction between the participants of network violence. They support and encourage each other by means of likes, comments and forwarding, forming a relatively stable group. In this group, individual voices may be amplified, while opposing or questioning voices may be ignored or suppressed. This kind of close connection and interaction mechanism within the group allows the influence and destructive power of network violence to expand rapidly.

To sum up, participants of network violence show significant group characteristics in terms of number, behavior pattern, internal interaction and emotional drive. This group nature not only intensifies the destructive power of network violence, but also increases the difficulty of governance. Therefore, when dealing with network vio-

lence, it is necessary to pay attention to the characteristics of group behavior and take targeted measures to effectively curb its occurrence and spread.

2.2 Organization and Professionalism

Organized cyberbullying usually involves a premeditated plan of action, orchestrated by a professional team, which is a conspiracy of capital and technology to attack individuals or groups through online channels to achieve specific commercial, political, or other selfish purposes. These teams may rally supporters through social media groups, forums, chat rooms and other online platforms, and disseminate offensive content through these cyberspace, rapidly amplifying the impact of cyberbullying. One of the most typical examples is the hiring of cyber mercenaries. As a result, the duration of network violence is lengthened, and the target of network violence is expanded, from individual stigma to group stigma. For example, experts become "experts" and rational speakers become "reasonable visitors" [3]. At the same time, the online water army's business covers a wide range, including the people's livelihood, the fight between fans in the rice circle, false praise, government control and evaluation, and malicious competition among large enterprises. These behaviors not only cause direct psychological and social harm to the victims, but may also cause serious damage to the online ecology and social order.

2.3 Juvenilization of Criminality

The emergence of the “Born-Digital” generation, alongside societal changes, such as the widespread use of smart devices and the shift to online education due to the COVID-19 pandemic, has led to a decrease in the age of both victims and offenders of network violence. On July 29, 2024, Hu Kaihong, full-time deputy director of the Central Civilization Office, said that survey data show that China has nearly 200 million underage Internet users, and the Internet penetration rate of minors has reached 97.2%. Among the different attributes of Internet users, almost all minors are covered by Internet connection. Although many minors are precocious nowadays, their age determines their level of understanding and depth of thought to some extent, and most of them do not have complete discrimination and control ability. When the voices of some key groups (such as opinion starters, opinion leaders, and human flesh searchers) become the mainstream, under the herd mentality, minors are prone to lose their rational judgment, adopt a blind attitude toward their remarks, and become the promoters of network violence incidents.

2.4 The Naive Righteousness of the Initial Motive

Most cases of network violence involve controversial factors that violate basic ethics. Out of the simple desire to safeguard social justice and the moral bottom line, netizens will become so-called "moral guardians" and conduct moral trials on the parties concerned, hoping to urge the parties to return to the moral bottom line and maintain social justice and order through public opinion pressure. However, this simple sense

of justice is often easily distorted and abused in the complex environment of the Internet, and thus evolves into network violence against the parties. With the advance of public opinion, the simple justice of the initial motive of network violence is easy to be distorted and abused [4]. The anonymity of the network environment and the characteristics of fast transmission tend to cause netizens to lack rational thinking when expressing their opinions, and to follow the trend emotionally. Once the pressure of public opinion is formed, it is easy to cause irreparable harm to the parties. The mentality of blindly following the crowd will also make netizens gullible and spread false information without verification, further aggravating the degree of network violence. Sometimes netizens' sense of justice can be overly amplified or even abused, elevating personal grievances or private conflicts to the height of moral trial, and making groundless accusations and attacks on the parties involved. Such behavior not only goes against the original intention of justice, but also harms the healthy development of the online ecology.

2.5 Great Impact and Harm in Reality

Although network violence originates from the virtual realm, its substantial harm to the victims cannot be ignored. Such acts of violence not only damage personal reputation, but also cause profound psychological trauma, and may permeate the victims' real life and workplace, becoming the fuse of offline violence. When online violence extends offline, there are two main outcomes. One is offline vicious group behavior, which is mainly manifested by the masses spontaneously encircle and intercept the victims and interfere with the daily life of the victims. In group incidents, people's conscious personality has disappeared, and unconscious personality is dominant. The infection of emotions and ideas and the influence of suggestion make the cluster psychology develop in an extreme direction, and they have the tendency to immediately change the implied views into actions [5]. Second, the victim's suicide tragedy occurs frequently, and the compulsion of network violence lies in the great psychological pressure it causes to the victim [6]. Once the pressure of public opinion causes the victim to breakthrough the final psychological defense line, it will cause irredeemable serious consequences, such as the mother in the Wuhan campus incident, the female master who is criticized for her hair color, the teenager Liu and the female doctor in Deyang and other cases. All highlight the extreme harm of network violence. Given rising social uncertainty and challenges to national and social security, the role of criminal law in upholding security values has become increasingly critical. The serious consequences caused by network violence require astern response from the law to protect citizens' rights and maintain social stability.

3 Typological Analysis of Network Violence

The typology method aims to make up for the limitations of conceptual thinking, which is often closed and abstract. When legal norms are difficult to be fully displayed by abstract concepts and their logical systems, they need to be improved by

more open type thinking [7]. In view of the abstract and broad characteristics of network violence, this paper tries to define the specific connotation of various types of network violence more clearly through typology analysis, and then clarify its realistic motivation and goal.

3.1 Traditional Network Violence

From the traditional academic perspective, the behavior of network violence mainly includes human flesh search network violence, rumor-mongering network violence and verbal abuse network violence.

Privacy disclosure type of network violence refers to the network group through a variety of means to collect the victim's personal information, such as photos, family background, address, contact information, work unit, school, and so on, and publicly spread on the network, so as to cause psychological trauma to the victim. It uses the interpersonal communication mode of askingpeople and seeking people to constantly update the information of the parties, providing fresh materials for the network public opinion one after another, prompting the network public opinion to surge one wave after another, making the situation develop into an uncontrollable situation, and ultimately leading to the formation of network violence [8]. This kind of behavior exposes personal privacy, infringes on legitimate rights and interests, and involves moral judgment, which is equivalent to the abuse of lynching. In 2008, Jiang committed suicide by jumping from a building after her husband, Wang, cheated on her. Before she died, Jiang wrote a death blog on the Internet, recording her heart journey in the last two months of her life, telling how her husband Wang had an affair, asked for divorce and moved out of the house. The topic of "death blog" immediately detonated public opinion, and Wang was subjected to human flesh search, harassment and abuse by netizens. The event eventually changed from online abuse into real personal attacks and intercept from a crowd of people, and became the most serious public event on the Internet in 2008. The case pushed "human flesh search" and "network violence" into the judicial field, and gave birth to the first case of "human flesh search" in China.

The network violence of defamation and slander, means that the doers deliberately fabricates false information and wantonly defame the victim through the information network. Nowadays, with the rapid development of various social platforms, network rumors have become a social nuisance. By fabricating and spreading false information, this kind of behavior guides a large number of unknown netizens to slander the victims irrationally and maliciously, causing great psychological pressure to the victims, damaging their physical and mental health, and violating the legal interests of order in cyberspace. Especially when the victim is a woman, it often involves sexual privacy and stuff like that, which will cause serious psychological trauma to the victim. In "The Case of a Woman in Hangzhou Who Was Falsely Accused of Having an Affair while Collecting a Courier", the perpetrator defames the unknown woman by fabricating false information, which arouses wide attention of Internet public opinion, damages the reputation of the victim, and brings great troubles to her work and life.

Abusive network violence refers to the serious behavior of network groups who publicly humiliate, denigrate and abuse the victims by publishing insulting remarks and information through text, pictures, audio and video in cyberspace. Such acts, which are direct, public and insulting, bring mental and psychological harm to the victims, and may even lead to suicide or self-harm. In the "Deyang 'an Doctor Suicide case", the perpetrator posted insulting remarks through wechat, Weibo and other means, which triggered a large number of netizens to slander and abuse the victim, and finally led to the victim's suicide. Thus, it can be seen that verbal abuse network violence can cause serious consequences and bad social impact.

3.2 Emerging Forms of Network Violence

With the development of social networks and the application of new technologies, new network violence methods are constantly updated, just like "opening a box to hang people", "cyber toilet", "online class explosion" and other such means are promoted through the network platform, forming a new organized network violence behavior.

“Opening the box to hang people” refers to the malicious disclosure of other people's personal privacy information in the name of disclosure, criticism, inciting netizens to attack and abuse, which is a kind of network violence. Different from the traditional human flesh search method of gradually exposing and spreading people’ privacy, "opening the box and hanging people" is the violence brought by technological development, which is worse than human flesh search. After the “box” is “opened”, not only personal information is leaked, but also more lawbreakers will use these privacy and information to unscrupulously harass "the box is opened".

“Hanging Toilet" refers to when a person's photos, behaviors, or statements are submitted by netizens to a "toilet number" on social media platforms. And "toilet number" is a type of account that is popular among fans of anime, celebrities, and gamers, where netizens can send private messages through the back-end to the account owner, who then posts the submissions anonymously. In its early stages, "online toilet" was simply a group of accounts that accepted anonymous submissions from netizens around certain interests, such as celebrities and anime, and posted them. Today, it has become a place where anonymous attacks and even cyberbullying are carried out without restraint, with a constant flow of negative content, leaks of personal privacy, accumulation of "dirty and messy" phenomena, and fermentation of negative and pessimistic emotions. If not properly regulated, it is easy to lead to the emergence of extreme cyberbullying incidents with disastrous consequences, and cause irreparable harm. The cyberspace is not a "lawless land", and the current state of "online toilet" goes against the goal of creating a clean and upright cyberspace. It is imperative to implement cyberspace governance to put an end to this strange phenomenon.

What is commonly known as "online classroom raids" can be simply described as "invasion" of online classes, cyberbullying of teachers and students, and disruption of teaching order. What is particularly terrifying is that this heinous act is even organized. It is a new type of online invasion, where participants in online classes leak the

conference number and password, allowing one or more outsiders to enter the live classroom and disrupt the teaching order by verbally abusing teachers and students, playing songs, spamming the chat, and even broadcasting obscene videos. These intruders are called "raiders". In 2022, a history teacher surnamed Liu from Xinzheng No. 3 Middle School in Henan Province died at home after an online class. According to the videos and pictures provided by his family, when Liu was teaching students online, a stranger broke into the broadcasting room. The intruder deliberately played harsh music to disturb the class order, and all kinds of insulting words were offensive. After the incident, the phenomenon of a new type of network violence, "online class explosion", has attracted wide attention.

Compared with traditional network violence, the emerging forms are more like wanton intrusion for no reason. And they are more dependent on technology and more disruptive to the social order.

4 Dilemmas and Causes of Criminal Law Regulation on Network Violence

Taking the connection of execution as the starting point, the criminal management dilemma of network verbal violence is mainly reflected in the physical dilemma of one-sided identification of the special behavior characteristics, sych as “serious circumstances”, "fabricating facts" and “social order”, and the procedural dilemma of low efficiency of criminal evidence transformation and private prosecution and public prosecution.

4.1 From the Macroscopic View:

The Group Nature of Network Violence Leads to the Dilemma of Criminal Law Regulation that "The Law often Turns a Blind Eye to Widespread Offenses".

The group nature of network violence causes the criminal law challenge of "law does not blame the public", which is a common problem in the field of criminal law and global social governance. The so-called "law does not blame the public" means that when the behavior is extensive or collective, even if it contains illegal or improper elements, it is difficult for the law to fully call to account [9]. Network violence often involves the participation of a large number of unspecified Internet users, and is manifested in continuous harassment, abuse, slander, threats, human flesh searches and the spreading of rumors. This kind of colonial and uncertain form of participation makes it difficult for criminal law to define the subject and responsibility of the crime.

The Misfocus of Public Discourse Drives it Difficult for Criminal Law to Pursue Criminal Responsibility for the Perpetrator through the Theory of Causality.

In the complex environment of "information cocoon", "limited public information reception" and "diversified discourse right on the Internet", Once the network information is released, it may be quickly disseminated by the self-media and various In-

ternet platforms. In this process, public opinion is dominated by various force, resulting in the focus deviating from the original issue, forming "public opinion out of focus" [10]. An in-depth analysis of the effect of "out- of-focus public opinion" shows that after information publishers publish content in cyberspace, it is often difficult to predict and control the subsequent evolution direction of public opinion. The intervention of many network participants may distort or even subvert the original intention of information publishers. Therefore, in the field of criminal law, how to establish the direct causal relationship between the information publishing behavior and the ultimate social harm becomes a difficult problem; How to reasonably attribute the social harm caused by the group behavior to a few individuals is also a major challenge in judicial practice; In addition, how to effectively prove or infer the subjective intention of the information publisher is also difficult.

4.2 From the Microcosmic View: the Special Behavior Characteristics of Cyber Violence Lead to the Failure of Traditional Charges to Match Network Violence

Crime of Insult and Defamation.

(1) Involving specific determination of "serious circumstances" -- Data absolutism.

According to the specific provisions of the first paragraph of Article 246 of the Criminal Law, the premise of the crime of defamation is that the perpetrator fabricates facts and spreads them, and the act must reach the degree of "serious circumstances". In ***the Interpretation of Several Issues concerning the Application of Law in Criminal Cases Involving Defamation through Information Networks*** jointly issued by the Supreme People's Court and the Supreme People's Procuratorate, Article 2 elaborates on what constitutes "serious circumstances", in which the number of page views and the number of retweets are particularly important factors to consider. However, it is worth noticng that due to individual differences, everyone's acceptance of information and psychological bearing capacity are not the same, so even if the number of page views and forwarding of defamation information is the same, the actual degree of harm to different victims maybe very different [11].

Taking the guiding case issued by the Supreme People's Procuratorate, the Prosecution Case No. 138 Yue's insult case, for example, the number of views of defamatory information in this case was only more than 600 times, far lower than the threshold of 5,000 views stipulated in the Interpretation. However, this limited range of dissemination has led to the serious consequences of the victim's tragic death [12]. This case highlights a problem: if the actual serious injury to the victim is ignored only because the formal pageviews are not up to standard, it may cause that the victim cannot obtain legal relief in time, and even need to wait until the situation deteriorates to the point of no return before the judicial organ intervenes, which obviously runs counter to the public's basic expectations for fairness, justice and the original intention of the law.

(2) Involving the determination of "fabricating facts"--The crime of defamation.

Article 246 of the Criminal Law clearly defines the constituent elements of the crime of defamation, that is, defamation involving fabricating facts and reaching a serious degree of circumstances. Among the various manifestations of network violence, fabricating and spreading rumors have become the most easily identified and qualitative forms by law because of their direct malicious nature and relatively clear evidence chain. However, digging into the actual situation of network violence, we find that not all defamation acts are entirely based on fabrications out of the air. On the contrary, in many cases, the perpetrators are often selective quoting or exaggerating existing information (such as media reports), so-called "taking information out of context" or "adding the trimmings", in order to incite public sentiment and launch mass attacks against specific individuals. Such acts, although they contain true information to a certain extent, they distort and mislea facts just as seriously as fabrications out of the air, and often cause incalculable social harm.

In the face of this kind of network violence which is not completely fabricated but contains subjective assumptions, the judicial practice has encountered difficulties in applying the requirement of "fabricating facts". Due to the strict definition of "fabrication" in legal provisions and the consideration of "serious circumstances", it has become a difficult problem to accurately define the legal nature of defamation acts that are partially true but have obviously exceeded the reasonable limit.

In view of this, it is necessary for us to re-examine the criminal standards of the crime of defamation, so as to better adapt to the new situation and new problems in the network era. If the relevant legal provisions are not adjusted and improved in time, a large number of network violence acts that defamate others and cause serious consequences by fabricating some facts and spreading misleading information may be outside the regulation of the criminal law, which is undoubtedly a severe challenge to legal justice and social order.

(3) The procedure dilemma of private prosecution and public prosecution.

In China, the crime of insulting and defamation belongs to the private prosecution case which is handled only after telling. The traditional insults and defamation mostly happen among acquaintances, so the victim's willingness to sue will be greatly reduced for the maintenance of interpersonal relationship. Based on respect for the victim's choice of litigation and personal will, China's criminal law classifies it as a private prosecution case, giving the parties more options to resolve the conflict. However, with the development of technology and the popularization of the Internet, the characteristics of network violence are completely different from those of traditional language violence. Due to the anonymity and multi-person participation of network violence, victims often cannot determine the perpetrator and their real identity only by their own strength. Also, Online information is easy to be tampered with and deleted, and it is also extremely difficult for victims to collect and retain evidence. According to the investigation, only 24.3 percent of the private prosecution cases of insults and defamation by network violence were found guilty. Compared with it, the rate of guilty verdit in the public prosecution cases is 100 percent. In the above cases where the courts made substantive judgments, the defendants were acquitted in 31.6% of the

private prosecution cases [13]. This figure is not only far from the overall acquittal rate of 0.083% in the past five years [14], but also significantly higher than the acquittal rate of 5.59% in private prosecution cases from 2008 to 2012 [15]. This indicates that in the network violence insult and defamation cases, only relying on the victim's private prosecution of crimes, may have no way to meet the needs of punishing crimes. It can be seen that in the current situation, the private prosecution procedure has not only failed to achieve the original intention of ensuring the victim's procedural choice, but has strictly restricted it. To some extent, the private prosecution procedure has become a burden for the victims of network insults and defamation cases.

In order to prevent the victim from being trapped in the private prosecution procedure, China's criminal law also stipulates that the insulting defamation case, which "seriously endangers social order and national interests", can be prosecuted by the procuratorial organ. However, the threshold of public prosecution is not clear enough. Although ***the Guiding Opinions on Punishing Crimes of Internet Violence according to Law*** provide several cases deemed as "seriously endangering social order", its wording is still vague and broad, which is difficult to grasp in judicial practice.

The Ambiguity of Personal Information Definitions in the Crime of Infringing Citizens' Personal Information.

Article 253 of the Criminal Law stipulates that anyone who sells or provides citizens' personal information to others in violation of relevant state regulations with serious circumstances, shall constitute the crime of infringing citizens' personal information. In 2017, the "Two High Schools" issued the "Interpretation on Several Issues concerning the Application of Law in Handling Criminal Cases involving Infringement of Citizens' Personal Information" (hereinafter referred to as the "Interpretation"). Article 1 of the Interpretation stipulates that "citizen's personal information" in the crime of infringing citizen's personal information refers to all kinds of information that can identify the identity of a specific natural person or reflect the activities of a specific natural person, either alone or in combination with other information. Article 2 of the Interpretation stipulates that anyone who violates laws, administrative regulations or departmental rules on the protection of citizens' personal information shall be identified as "violating the relevant provisions of the State." Article 3 of the Interpretation stipulates that those who publish citizens' personal information through information networks or other channels, or provide lawfully collected citizens' personal information to others without the consent of the person collected, shall be identified as "providing citizens' personal information" in the crime of infringing citizens' personal information. According to the contents of the Criminal Law and the Interpretation, the main legislative purpose of the crime of infringing citizens' personal information is to protect citizens' privacy rights. However, in a large number of network violence incidents involving human flesh search, the victims' personal information such as photos and social updates that are picked up and disseminated by netizens are all information that the victims voluntarily post on social software such as Weibo. According to Article 1 of the Interpretation, the photos and other information disclosed by the victims are "personal information of citizens"; According to Articles 2 and 3 of the Interpretation, forwarding others' disclosed personal information is

"providing citizens' personal information," but not "violating relevant state regulations." This is because there is no clear provision in the current legal system to prohibit such online dissemination. Although the behavior may be without the consent of the information owner, it does not touch the core of the crime of infringing citizens' personal information -- illegal collection or profit-making.

Therefore, even if human flesh search involves widespread dissemination of the victim's personal information, it is difficult to be directly defined as a crime of infringing citizens' personal information due to the lack of evidence that directly violates relevant state regulations and fails to meet the requirements of illegality in judicial interpretation.

5 Legislation on Network Violence in Some Countries

Cyber violence is not only happening in China's Internet field, but has become a global problem. Many countries regulate this through legislation. Its regulatory experience can provide useful reference for China's management of cyber violence.

5.1 The United Kingdom: Focus on Protecting Minors

At the end of October 2023, the UK successfully passed the landmark Online Safety Act, which is regarded as a key piece of legislation in the field of cyber protection. Its core objective is to strengthen safeguards for online users, especially vulnerable groups such as children, to ensure that their safety and privacy are fully respected and protected in cyberspace. The core principles of the Act are to adopt a zero tolerance policy for harmful behavior in cyberspace, to protect children from online violence, and to give adults more freedom of choice over online content.

Specifically, the bill clarifies the legal responsibility of technology companies in preventing and promptly removing illegal content, such as terrorist information. It not only sets a general framework for social media, but also sets out more detailed requirements for child protection [16]. For example, it emphasizes that enterprises must take effective measures and conduct "child risk assessment" on relevant social media software; Implement differentiated risk management strategies according to the characteristics of children of different ages; In the formulation of policies, children's reading comprehension ability should be fully considered. At the same time, provide convenient online reporting channels, so that children and parents can easily report problems and get help quickly. These measures reflect the comprehensiveness and depth of the Act in protecting children's Internet safety. Businesses that fail to comply with these strict rules will face hefty fines from Ofcom, as well as severe penalties for their failure to comply.

Data for 2022 shows that smartphone ownership among five - to seven-year-olds in the UKhas risen to 17 per cent, up 12 per cent from 2019. Ninety-seven per cent of 12- to 15-year-olds now own a smartphone, up 14 per cent from three years ago. In the UK, the smartphone penetration rate among 16- and 17-year-olds has reached 100% [17]. The British government is considering legislation to restrict underage

smartphone use in a bid to reduce the risk of cybercrime and its links. The latest proposal to ban the sale of smartphones to under-16s has been welcomed by parents as an effective shield against the potential harm social media can do to children, including threats such as cyberbullying, access to pornography and hacking. Meanwhile, the government has issued guidance on mobile phone use in schools to encourage schools to take steps to limit mobile phone use in school, with the aim of reducing distraction and promoting positive changes in pupils' behaviour.

The UK has maintained a high level of pressure on violent online crimes and strengthened its control over cyberspace. The Public Order Act 1986, the Communications Act 2003 and the Anti- Terrorism Act 2006 have all identified network violence as a crime and regulated it under criminal law. In September 1996, the UK government promulgated the first industry-wide regulation of the Internet, R3 Safety-Net (3R Safety). The "3R" stands for "Rate", "Report" and "Responsibility" respectively [18]. Clarify the responsibilities of the platform and give play to its supervisory and management role.

5.2 Germany: The Responsibility of Network Platform.

In June 1997, Germany passed the Multimedia Law, the world's first comprehensive law regulating the Internet. The Multimedia Law imposed relatively strict restrictions on Internet service providers, requiring them to take necessary technical measures to restrict the dissemination of certain publications and be responsible for the content they provide. The law establishes such basic principles of Internet legislation as the principle of free access [19], the principle of responsibility for the classification of content transmitted, the principle of the protection of citizens' personal data and the principle of the protection of minors. In addition, the law introduced the network real-name system, which requires users to provide necessary personal information when accessing the Internet so that legal tracing and investigation can be carried out if necessary.

In January 2018, Germany introduced the Internet Enforcement Law. The law requires online platforms to block or delete online information that is clearly illegal within 24 hours; And within 7 days, block or delete Internet information that is generally illegal. At the same time, platforms must also designate people responsible for handling user complaints and regularly submit quarterly reports to the German Federal Ministry of Justice on combating illegal speech. The law also requires social media platforms to quickly delete or block illegal content after receiving complaints from users, and sets hefty fines of up to 50 million euros for mishandling. The essence of the "Network Enforcement Law" covers three main points: first, clearly defining the scope of illegal content (Article 1, Paragraph 3); second, establishing a mechanism for handling complaints about illegal content within a limited time (Article 3); and third, stipulating the legal reporting responsibility for specific complaint content (Article 2)) [20].

With the progress of society, the phenomenon of network violence has become increasingly prominent, and its complexity and multiplicity require more powerful legal responses. To this end, Germany has taken an innovative initiative in 2020 to system-

atically integrate all the laws and regulations related to cyberviolence in the current legal system, and adopt the strategy of "package legislation" (that is, to achieve an overall legislative purpose, the relevant provisions scattered in multiple laws are "packaged" in one legal document.) [21]. This comprehensive legal framework aims to prevent and punish network violence more effectively, build a solid legal protection network for the public, and ensure a safe and harmonious online environment.

5.3 South Korea: Network Real-name System

South Korea occupies a leading position in the global Internet field. From the establishment of the Network police system in 2003 to the implementation of the "real name system" in 2007, its rich practical experience has provided valuable reference for the application and governance of the Internet in China. In the network management system of South Korea, the network real-name system occupies a pivotal position and constitutes the cornerstone of its network security system. In 2007, South Korea officially established the network real-name system through legislative means, and in the Law on the Promotion of the Use of Information and Communication Networks and the Protection of Information, it clearly established a statutory clause on "restrictive personal identity verification". The clause stipulates that websites with daily visits of 300,000 or more must require Internet users to register their real names. Those who violate the regulation will be fined up to 30 million won and liable for legal disputes arising therefrom [22].

As a common system design in real life, the real-name system plays a bridging role, strategically connecting virtual identities and real individuals, and enhancing netizens' sense of self- responsibility. Its essence is to introduce the legal framework and moral standards of the real society into the online world, and encourage netizens to maintain self-discipline and be careful about their words and deeds in cyberspace [23].

However, in the process of its implementation in cyberspace, the real-name system has triggered a wide range of disputes and discussions. As the first country in the world to enforce the network real-name system, the policy issued by South Korea has gone through a complicated process from preparation, implementation, adjustment, termination, and now conditional application [24]. How to properly set the weight of netizens' participation in the negotiation to ensure the effective integration of opinions from multiple parties? At the same time, how to properly resolve the boundary between public and private rights, so as to encourage netizens to express themselves responsibly while resolutely protecting their privacy and information security? We still need to deal with these problems in the localization study of South Korea's real name system, explore the balance between management and development, and draw the boundary line between public rights and private rights.

Comparatively speaking, China's network legislation is relatively lagging behind, no matter in the amount of legislation or in the level of legislation, there is a big gap with the real needs. In the maintenance of national network information security, strengthen network content management and so on, we still face the difficulty or em-

barrassment of imperfect legal system. Strengthening network legislation has increasingly become one of the urgent tasks of our country's legislative work.

6 Solutions to the Dilemma

This paper proposes to explore the compatible path of existing charges to network violence, expand and debug existing charges by applying criminal law interpretation principles, and identify serious network violence by applying criminal law interpretation principles such as objective interpretation and purpose interpretation. Specifically, in terms of entity, the penalty criteria should be improved, a single number of identification should be abandoned, a multi-dimensional identification method of "criminal quantitative standards + substantive legal interest " should be adopted, and it should be clear that the order of cyberspace belongs to social order. In terms of procedures, it emphasizes the responsibility of each subject to assist in investigation and evidence collection, and increase the opportunity for victims of network violence cases to initiate the investigation procedure.

6.1 Learning from the Experience of other Countries

Drawing insights from foreign countries' countermeasures against cyberbullying, including South Korea's real-name system, Germany's platform responsibility, and the United Kingdom's protection of minors, we endeavor to provide solutions tailored to China's specific national conditions. On this foundation, we actively propose measures and relevant suggestions aimed at better resolving the issues identified within the realm of cyberbullying.

The core crux of the enforcement difficulties in criminal law arising from the notion of "the law does not punish the majority" lies in the ambiguity of criminal subjects and the definition of responsibility. To address this dilemma, it's a good idea to draw on the successful experience of South Korea's online real-name system to enhance users' sense of responsibility and behavioral constraints. By implementing the online real-name system, various online platforms can optimize their user management systems, making the accountability and crackdown on cyberbullying more precise and efficient. Specifically, the real-name system requires users to provide their authentic identity information during registration, which not only facilitates law enforcement agencies to quickly identify responsible individuals through database comparisons, simplifying the investigation process and reducing enforcement costs, but also ensures that online behavior records are more complete and traceable, covering users' basic information and activity trajectories, providing a solid evidential foundation for combating cyberbullying. This aids in accurately defining the cause, development, and scope of influence of incidents, providing sufficient grounds for judicial decisions.

As for the challenge of causality determination caused by "misdirected public opinion," strengthening platform responsibility and clarifying opinion guidance are the crucial breakthrough points. Germany's practices in platform responsibility manage-

ment offer valuable insights. Firstly, platforms should be encouraged to establish advanced information identification and early warning systems for cyberbullying, leveraging technological means to assess potential risks from multiple dimensions to achieve precise warnings. Secondly, a convenient and efficient reporting mechanism should be established, with quick reporting entry points prominently displayed on platforms to simplify the reporting process and ensure that users can promptly feedback on cyberbullying behaviors. Platforms must respond promptly to reports, taking swift measures such as deletion and blocking to curb the spread of violent information. Lastly, the platform accountability system should be improved, with accounts involved in cyberbullying subject to classified dispositions based on the severity of the offense, ranging from educational warnings, functional restrictions, to account suspensions. For those with extremely heinous conduct, measures such as banning them from accessing the entire network should be implemented to serve as a deterrent.

6.2 On the Determination of "Fabrication"

"Fabrication" in abroad sense includes complete fabrication and partial fabrication. As for the word "fabrication" in the crime defamation, the theory generally holds that it only refers to specific facts created out of nothing and false out of thin air, that is, only complete fabrication but not partial fabrication. In the author's opinion, misinterpreting facts and spreading them wildly, such as Interpreting words out of context, circulating erroneous reports. and adding decorative embellishment, seem to fabricate only part of the facts, but this does not absolutely deny the possibility of the relevant acts turning into complete fabrications. With all kinds of Internet information so dizzying, it is difficult for netizens to directly judge the authenticity of Internet information. In order to attract people's attention, people take media reports out of context, add facts made up by themselves, and then repost and spread them wildly. If it causes serious damage to others' personality and reputation, it should constitute a case of "fabricating facts to slander others". According to purpose interpretation, fabricating some facts to slander others and cause serious damage to the personality and reputation of others should be a crime; According to the literal interpretation, the act of fabricating part of the facts does not exceed the maximum textual range of "fabrication". Therefore, misinterpreting key facts in cyberspace, such as taking words out of context or adding decorative embellishment, and spreading them wildly to cause serious consequences fall into the category of "fabricating facts to slander others", and thus constitute the crime of defamation.

6.3 On the Determination of "Serious Circumstances"

The actual impact on reputation should be the criterion for judging "serious circumstances," following the principle of combining criminal quantitative standards with substantive legal interest infringement standards. The author points out that the definition standard of the volume of defamatory information dissemination in the "Interpretation of Defamation Issues" appears rigid in dealing with complex real-world situa-

tions. The core issue lies in the fact that the judgment standard for "serious circumstances" is too single and lacks flexibility. Regarding the consideration of the volume of dissemination and page views, a more refined evaluation method should be pursued rather than relying solely on the quantification of a single indicator. More importantly, it is necessary to combine the actual situation and conduct an in-depth analysis of how these dissemination behaviors specifically affect the social reputation and personal evaluation of the victim, thereby conducting a substantive assessment.

Some scholars further suggest that in order to enhance the applicability and comprehensiveness of the Interpretation on Defamation Issues, it should be clearly included in the consideration of the results of external damage to the right of reputation. Specifically, the quantitative standard in the existing Article 2 (1) should be adjusted to a more dynamic judgment standard, that is, it is required to reach a degree that "significantly leads to a substantial decline in the victim's social evaluation or serious damage to his reputation". Such a revision is intended to more accurately reflect the actual harm to an individual's reputation caused by defamation, rather than merely judging by the formal amount of communication.

6.4 The Adjustment of the Constitutive Requirement of Existing Crimes or the Legal Punishment:

For network violence that is difficult to be dealt with through interpretation, the constitutive requirements of existing crimes or legal punishment should be adjusted through the amendment to the Criminal Law at an appropriate time, so as to effectively deal with new crimes. The author believes that the act of providing and spreading others to disclose personal information and causing serious consequences is stipulated as "the crime of infringing citizens' personal information".

First of all, focusing on the specific provisions of some crimes, the author thinks that the crimes of infringing on citizens' personal information should be revised. Specifically, human flesh search, which is prevalent in the current network environment, is characterized by the illegal use and dissemination of personal information that may have been known to the public, and often leads to serious consequences. Although the initial acquisition of such information may be based on legal means, such as the public information bulletin board of the work unit, but without the consent of the right holder or in the case of its explicit opposition, unauthorized dissemination and provision of such disclosed personal information, and cause serious consequences, should be regarded as a new form of infringement of citizens' personal information.

The current law mainly focuses on the act of "selling or providing" personal information, but the nature and scope of objects of "disclosure" information in the network environment are completely different from those of "providing". The former is aimed at generally, unspecific audience, while the latter tends to target specific individuals. Therefore, it is logically inappropriate to simply equate "disclosure" with "provision."

To this end, we propose to directly amend the provisions of the Criminal Law on the crime of infringing citizens' personal information, and explicitly include the act of "releasing citizens' personal information through information networks or other means" as one of the types of criminal acts of the crime. In this way, anyone who

disseminates undisclosed personal information without permission or discloses disclosed personal information without authorization, and causes serious consequences, will be punished by the criminal law, so as to realize a more comprehensive and effective protection of citizens' personal information. Such a revision cannot only adapt to the new situation of the Internet era, but also better reflect the justice and deterrence of the criminal law.

In network violence cases, the majority of the cases are decided around the charges of insulting and defamation [25]. Relevant scholars hold different views on the determination of the crime of insult and defamation in the process of judgment. In actual judgment, the court often separates the crime of insult and the crime of defamation. According to the traditional view, the most obvious distinction between the crime of insult and the crime of defamation is the identification of "facts". If the facts are fabricated, even if the fabricated facts have harmed the victim's reputation, we cannot identify them as the crime of insult. On the contrary, if the facts exist objectively, and the defendant takes advantage of the existing facts to insult the victim, then the crime of this crime is the crime of insult. The scholar believes that, on the one hand, from the content of Article 246 of the Criminal Law, the conjunctive word "or" should bean inclusive relationship or a parallel relationship, which is more conducive to the protection of the victim by law. On the other hand, the scholar elaborates from the legislative purpose that no matter the "fabricated" factor the "real" fact, as long as the defendant uses the "fact" to harm the reputation and personality of the victim, we should allconsider the act as an insult. If the fabricated fact happens to exist, and to use the fabricated facts to insult the victim's reputation and personality, it is suggested that the crime of insult and libel should be imposed, rather than only the crime of libel, which is more conducive to a comprehensive evaluation of the case.

6.5 Enable True Program Selection

It is necessary to give the victim the right to choose, which means to give the victim different choice of procedure. In the scope of the object of telling, the victim should be allowed to choose to tell the public security organs, procuratorial organs or courts. This breaks through the previous restriction that the court is the only object of telling in the case handled by telling, distinguishes "telling" from "private prosecution" in the procedure, and establishes the independent status and important significance of "telling". Only if the victim chooses to tell the court, it can be handled as a private prosecution case. If the victim chooses to tell the public security organ, the case should be handled according to the public prosecution procedure; In the order of telling, if the victim tells multiple judicial organs, the judicial organ that first receives the victim's telling should handle it and determine the result of the victim's choice of proceedings.

7 Conclusion

With the science and technology advance, cybercrime has become a serious threat to society. The lack of effective legal regulation has allowed cybercriminals to operate

with impunity, posing a great challenge to law enforcement agencies [26]. As a pervasive "undercurrent" in the digital age, the governance of network violence still need shoulder heavy responsibilities and traverse a protracted journey. While this paper endeavors to delineate the comprehensive overview of network violence, analyze the intricate dilemmas confronting criminal law regulation, and delve into potential avenues for resolution, the complexity and ever-evolving nature of cyberspace underscore the perpetuity of the study on its governance. In the future, advancements in technology and shifts in societal norms are likely to further transform the forms and characteristics of network violence, necessitating a continuous deepening of our regulatory exploration. The enhancement of criminal law regulation not only requires precise definitions and punishments of network violence; but also it necessitates the establishment of a supple legal framework that accommodates the unique traits of the Internet era, thereby offering a robust legal foundation for upholding order and justice within cyberspace.

The governance of network violence represents not merely a competition between technology and law but also a profound discourse encompassing humanity, civilization, and the future. In this endeavor, we find ourselves simultaneously as challengers, confronting the intricacies of this multifaceted issue, and as shapers, molding the contours of a safer and more equitable cyberspace. Let us embark on this journey, armed with wisdom and courage, transforming the societal challenge of network violence into a catalyst for the progression of cyber civilization. Our collective efforts shall strive to render cyberspace a verdant haven for all humanity, envisioning a future cyber society brimming with light and promise.

References

1. Cui Shixiu & Zhang Rui (2023). Typological Analysis and Evaluation of Cyber violent Crimes. Journal of Liaoning Public Security Judicial Management Cadre College (06), 75-84
2. Cao Lin. "Internet Dependence" Promotes Online Violence [N]. Oriental Morning Post, 2007-7-9. Cao Lin. "Internet Dependence" Promotes Online Violence [N]. Oriental Morning Post, 2007-7-9
3. Cui Shixiu & Zhang Rui (2023). Typological Analysis and Evaluation of Cyber violent Crimes. Journal of Liaoning Public Security Judicial Management Cadre College (06), 75-84
4. Li Huajun, Zeng Lioxin & Teng Shanshan. (2017). Research on the development of cyber violence: Connotation types, current characteristics and governance Countermeasures: Based on analysis of 30 typical cyber violence incidents from 2012 to 2016. Journal of Information (09), 139-145.
5. Le Pen. The Crowd: A Study of Popular Psychology [M]. Translated by Feng Keli. Beijing: Central Compilation and Translation Press, 2014:125-136
6. Chen Daibo (2013). Analysis of the Concept of Online Violence. Hubei Social Sciences (06), 61-64. doi: 10.13660/j.cnki. 42-1112/c.012243
7. Refer to Karl Lorenz's book "Methodology of Law" translated by Chen Ai'e, Beijing: Commercial Press, 2003 edition, page 337

8. Liu Lihong (2009). Analysis of the Causes of Online Violence Caused by "Human flesh Search". Southeast Transmission (01), 100-101
9. Gong Yifan, Liu Shan, Zheng Jiezhong, Song Xiao & Wang Jingyi (2024). Practice, difficulties, and improvement suggestions for criminal law regulation of online violence. Qin Zhi (04), 43-45. doi: 10.20122/j.cnki. 2097-0536.2024.013
10. Sun Yuhua (2015). Constitutional Review of Judicial Interpretation on Internet Defamation. China Law Review (04), 126-136
11. Jian Chang & Yang Zongke (2023). Legal regulation of online violence in public opinion. Media (09), 94-96
12. Liu Xianquan & Zhou Zijian (2023). The dilemma of criminal law regulation of online violence and its solutions. Rule of Law Research (05), 16-27. doi: 10.16224/j.cnki. cn33-1343/d.202230905.012
13. Chu Chen City (2023). The evolution and basic stance of criminal law in response to online violence. Chinese Journal of Criminal Law (04), 35-52. doi: 10.19430/j.cnki. 3891.2023.04.001
14. Bao Wanchao (2013). Implementation Status and Reform Thoughts of Administrative Litigation Law: Analysis Based on the "China Law Yearbook" (1991-2012). China Administrative Management (04), 48-55
15. He Jiahong (2015). From Investigation Center to Trial Center - Improvement of China's Criminal Procedure System. Social Sciences in Chinese Universities (02), 129-144+159
16. Li Zhongdong (2024). The UK's Online Safety Act focuses on protecting children. Prosecution Storm (01), 48-49
17. Nicholas Negroponte. Digital Survival [M]. Translated by Hu Yong and Fan Haiyan. Haikou: Hainan Publishing House, 1997:269-272.
18. Fan Weiguo (2015). Legal Governance of Online Rumors: UK Experience and China's Path. Academic Exchange (02), 94-100
19. (2012). Strive to Build a Legal Barrier for the Healthy Operation of the Internet (continued) - Review of Foreign Internet Legislation. China Business Administration Research (05), 26-29
20. Sun Yu (2018). On the Compliance Rules of Network Service Providers - Taking the German Network Enforcement Law as a Reference. Politics and Law (11), 45-60. doi: 10.15984/j.cnki. 1005-9512.2018.11.005
21. Chen Yike & Song Jiangtao (2022). Cyberbullying Governance in Germany and Its Implications for China. Leadership Science (05), 127-130. doi: 10.19572/j.cnki. ldkx. 2022.05.017
22. Sang Ruijiao, known to Bei & Wang Yanyang (2023). Legislation and Practice of Anti Cyberviolence in South Korea. Modern World Police (07), 66-73
23. Yue Ning (2023). Comparative Analysis of Legal Regulations on Cyberbullying at Home and Abroad. Cyberspace Security (06), 107-112
24. Dong Junqi (2016). Inspiration from the Subject Game in South Korea's Cyberspace for China's Information Security Governance: Taking South Korea's Real Name System Policy as an Example. Intelligence Science (04), 153-157. doi: 10.13833/j.cnki. is. 2016.04.032
25. Luo Xiang (2024). Path selection and reflection on criminal law regulation of online violence, starting from the breakdown of the crime of insult. Chinese and Foreign Law (02), 285-30685-306.
26. Chen Mengjia, Wang Ziping & Wu Han. (2024). Practical Dilemmas Facing Criminal Legislation on Network Violence and Ideas for Responding to Them. Journal of Politics and Law (2),43-43.