Reconstruction of Subject Attribution in Criminal Governance of Cyber Harassment

Jingjun Wang
China University of Political Science and Law, Beijing, China

Abstract: This article examines subject attribution in the criminal governance of cyber harassment, focusing on the difficulties arising from rapid information dissemination, anonymity, collective participation, and the cumulative effects of online conduct. It reviews the attribution challenges associated with large numbers of participants and assesses the applicability of cumulative offense theory, arguing that the protection of individual legal interests requires differentiated analysis. Drawing on typological thinking and organizational dominance theory, the article proposes an attribution framework based on behavioral roles rather than identities. It distinguishes active conduct from failures to fulfill legally required duties and examines the respective responsibilities of initiators, instigators, ordinary participants, and platform operators. Initiators and instigators are assessed in relation to their organizational influence, while ordinary participants are evaluated according to the nature, frequency, and significance of their conduct. Platform responsibility is considered within the limits of legally prescribed supervisory obligations, knowledge of unlawful content, and the capacity to intervene. The article concludes that subject attribution should combine behavioral classification with differentiated responsibility and proportionate regulatory boundaries to protect legitimate rights and support orderly online interaction.

Keywords: Cyber Harassment; Collective Participation; Cumulative Offenses; Organizational Dominance Theory; Typological Thinking

1. Introduction

With the development of a new round of technological and industrial revolution, China's internet technology has developed rapidly, and the internet penetration rate has risen to a considerably high level. According to the 56th Statistical Report on internet Development in China released by China Internet Network Information Center on July 21st, 2025, as of June, 2025, the number of internet users in China was 1.123 billion, including 322 million in rural areas, and the Internet penetration rate was 79.7% [1]. More and more people are sharing the fruits of digital development. Internet and digital economy have added new vitality to people's material and spiritual life. Internet has replaced newspapers, television and other traditional media, and has become a new central media for transmitting information. People's work and life are increasingly integrated with the internet.

However, everything has its good side and bad side. On the one hand, the advancing digital era has brought convenience and rich experience to our lives, on the other hand, it has also created various problems. Cyberbullying is one of the most prominent problems. The platform of Self-media keeps the speed of spreading information, and a lot of information is soon known by more people. However, such information often lacks correctness and credibility. In addition, due to the anonymity of the internet, netizens can try the limit line of law with almost no risk. Thanks to the "low trust", "easy to spread incitement" and "anonymity" of the Internet, users can create and manipulate public opinion and incite violence at a low cost, and the cost is also very small. This is obviously contrary to the rules required for the high-quality growth of the internet.

Therefore, in order to purify the chaos of the Internet and make it develop well and healthily, those who abuse the Internet for cyber violence crime at will should be punished. The first problem is how to identify the object of punishment. This paper first introduces the research background and investigates the current situation and troubles of cyber violence crime. Then, think carefully and learn the existing idea of "the law does not punish the masses" and the theory of cumulative offenses. On this basis, the mechanism of investigating the responsibility of cyber violence crime is re-formulated, and an

attempt is made to find a solution from both legislation and judicial practice.

2. The Current Situation and Challenges of Cyberbullying Crime

2.1 Current Status of Cyberbullying Crimes

Internet has changed the way of communication before. Everyone is not limited by time and place, so they can express their opinions and spread information. With the expansion of internet and self-media platform, using the internet becomes very simple. Now everyone has their own place to express their opinions. The people who receive information are no longer limited to the previous circle of friends and family. The "no name" of the internet and the places where many people can participate make it difficult for people related to network events to find it correctly. There is also a side of reducing the possible adverse effects of people who participate in online chat. However, in the network environment, places where you don't need to name and places where you feel safe are also easy to expose uncomfortable parts. This is why cyberbullying was born.

With the development of Internet, the crime of cyberbullying is becoming more and more serious. Recently, criminal cases of insult and reputation damage have increased sharply, many of which are online insults and reputation damage. However, the crime rate is still low. Taking cases of reputation damage as an example, the number of first-instance cases accepted in 2022 was about four times that of 2013. Most of them are complaints filed by the victims themselves, and only 4.69% of the complaints filed by procuratorate. Among the libel cases concluded in that year, 46.17% were rejected, 18.74% were dismissed, 16.52% were revoked, and only 13.46% were convicted, and the conviction rate was even lower [2]. In 2024, the national public security organs handled more than 8,600 cyberbullying cases, took criminal compulsory measures against more than 2,500 people and imposed administrative penalties on more than 8,500 people [3]. These figures show that the crime of cyberbullying has reached a serious level, which needs to be dealt with as soon as possible, and the criminal law provisions in China are not effective enough for cyberbullying.

Cyberbullying crime is mainly the behavior of doing bad things to individuals in the network. For example, threats such as verbal bullying, slander, reputation damage, invasion of privacy, moral harassment, contempt or discrimination, making bad speculations, etc. All these will hurt the personality and reputation of others, cause "social death", cause great trauma to the soul, and even lead to suicide. There are many specific types of blue star crimes, including doxing, Internet rumors and language bullying. These three are not separate, and often appear together in a cyberbullying crime [4].

Doxing refers to using manpower to find other people's private information. In an era when it is difficult to obtain information, this action is often called "searching everywhere". However, with the rapid increase of people using the internet, the manpower used for this kind of investigation has also increased sharply, and the information and available means spread on the Internet have also increased, thus revealing privacy. Doxing is something that lets everyone know personal privacy, and verbal violence and physical violence may occur, causing great harm and affecting a person's life. "Although everyone can make moral judgments, not everyone can become a police officer", which is one of the main reasons for cyberbullying. To make matters worse, cyberbullying often escalates into a criminal act. "Criminals often use the Internet to do things to get personal information, expose personal information, and ultimately hurt others." In the end, netizens replaced public power to judge and punish others to some extent, which is a modern vigilante justice [6].

The so-called Online rumors are fictional stories that are not true on the Internet. Since the increase of self-media platforms, online forums have spread rapidly and reached many people. Whenever there is a hot topic in society, people who make and spread rumor will spread related rumor for themselves, disturb everyone and destroy the ordinary social order.

Verbal violence refers to the act of posting comments, images and videos that hurt or insult each other on the Internet. This kind of violence often has no logic and reason, but is just venting emotions. However, because it is obscene and offensive, there are many things that are very insulting, so it will cause serious harm. On the other hand, verbal violence is contagious. Some netizen's malice may deceive netizen who knows nothing and make him join the partner, which will become collective violence. On the other hand, verbal violence is prone to confrontation. The victims fight back and attack each other, and eventually both sides will be hurt. However, if the

victims are subjected to concentrated attacks for a long time, they will often be broken because of excessive internal pressure [5].

2.2 Characteristics of Cyberbullying Crimes

Different from the previous cyberbullying, cyberbullying in the social media era can be said to have a fast attack speed and a more accurate "attacking effect". Because information is easy to spread immediately on social media, anything will soon become important on the internet and will be seen by many people in a few days. Moreover, because the network is virtual and anonymous, netizen don't care about the truth and the correctness of their speeches at all, and can comment and spread information at will. In the cyberbullying tragedy that happened one after another, it was "no snowflake is innocent". In order to prevent such a tragedy from happening again, it is necessary for us to carefully investigate and think about the characteristics of cyberbullying and find a solution.

2.2.1 The immediacy and breadth of information dissemination

Cyberbullying's crime spread is characterized by rapid growth. Using the fast and multi-person delivery mechanism of social media and short video platform, the information of cyberbullying will be delivered to millions of users in a few minutes. This is much worse than the "word-of-mouth" practice of reputation crimes in the past. The first reason why cyberbullying's crime has a great impact is that there are two forces: passive algorithm recommendation and user's own search. On the other hand, in order to let many people see it, the platform uses the method of trending topics to continuously expand the content worthy of discussion. On the other hand, users will keep forwarding the content with the feelings of "I think so" or "because everyone is doing it", so the content of the discussion will soon be expanded one by one, not just a platform. Unlike offline violence, which only affects people in the workplace, the scope of cyberbullying is constantly expanding. Victims often can't predict the cause and scale of the attack, and the anxiety of "being seen" and "being attacked" continues.

2.2.2 The concealment and anonymity of behavior

The virtual nature of cyberspace gives the abuser a natural shield. Most netizen use anonymous names on the Internet, and this ambiguity directly leads to the complete failure of moral rules-the perpetrators did not take the risk of their real names being exposed, so their behavior was more reckless. As managers, it conforms to the core logic of "depersonalization theory": when individuals think of "no one knows their own behavior", their inner social rules will weaken, but they will seek a sense of satisfaction from members of the group. This feature brings double difficulties to the prevention and collection of cyberbullying crimes.

2.2.3 The collectivization and conformity of the subject

Cyberbullying is rarely carried out by only one person. Rather, it is characterized by "team participation and reduced responsibilities." Participants in Cyberbullying crimes are often a group involving many people.

Cyberbullying crime is a common specific event, which begins with a person's attack, insult and reputation damage on a specific victim. However, with the spread of the Internet, the number of participants will increase rapidly. Social psychology says that if an deindividuation feels that his personality has disappeared in a group, de-indirection will occur, and his awareness and control of his behavior will be weakened. As a result, you will do behaviors that one can't do when one is young, that is to say, you will do unusual and unreasonable behaviors. Individuals want to be accepted by the group, even if they don't think about their actions carefully, it is easy to go along with the actions of the group. As a result, many unreasonable speeches and attacks will be made to the victims [8].

In the crime of cyber bullying, many netizens attack victims through comments and private message, and few people are finally held accountable by law. According to the theory of social loafing effect, it is easy for people to reduce their sense of responsibility when they think that their actions are part of a group. The more people cyberbullying, the shallower the sense of personal responsibility and the more serious cyberbullying.

2.2.4 The persistence and cumulative nature of damage

Unlike ordinary violent crimes, which only suffer once, cyberbullying has been going on and has a tendency to become more and more serious. The victim's personal information was pasted with malicious attacks and labeled as "bad" in the digital world. Moreover, if many netizens join the attack, the number of tags will increase and the damage will increase. At the same time, cyberbullying also has the phenomenon of "secondary violence". Even if the content of the

original attack is deleted, the third party will continue to expand in the form of screen short messages, transmissions or other Internet memories, forming a damage cycle. In other words, the psychological damage suffered by the victims of cyberbullying is easy to become something that can't be cured for life.

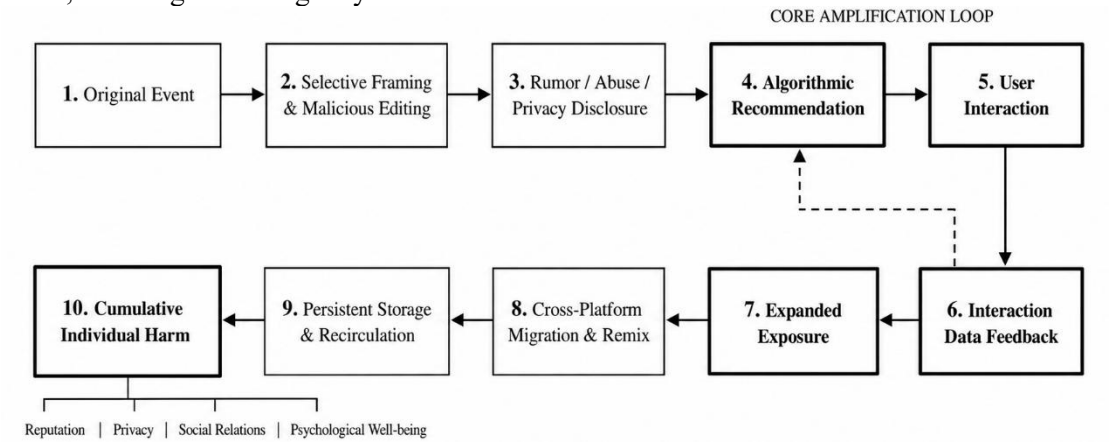


Figure 1. Mechanisms of Cyberbullying Information Dissemination, Algorithm Amplification, and Harm Accumulation.

As shown in Figure 1, the cyberbullying information includes event interception, malicious processing, algorithm recommendation, user interpretation and cross-platform migration. Then, the user interaction data is returned to the recommendation mechanism of the platform, and the state of "recommendation-interaction-feedback-expanded exposure" is displayed continuously or repeatedly, which will eventually cause complex harm to the victim's reputation, privacy, interpersonal relationship and mental health.

3. The Negation of "the Law Does not Punish the Masses"

3.1 The "Mass Mentality" in Cyberbullying Crimes

Everyone's understanding of "low cost" is that when an act involves or spreads many people, even if it violates low cost, it is difficult to punish it with low cost. The theoretical center of "the law does not punish the masses" is located in "mass". If many people do something, even if it is a violation of law or crime, it is difficult to hold everyone accountable because of the large number and complicated situation.

If this theory is applied to cyberbullying crime, it will be clearer and more complicated.

On the other hand, there is no special crime about cyber violence in our country. On the contrary, we use crime such as insult and damage to reputation to ban cyber violence. Therefore, it is a bit difficult for victims to protect their rights [7].

On the other hand, it is also difficult to clarify the responsibility of cyberbullying crime. Because many people have done bad things, it is difficult to know the relationship with the victims. Among thousands of bad guys, it is not clear who should bear how much responsibility, whether they are the first to do bad things or those who joined later. It is difficult to confirm the relationship with the victim, and it takes an incalculable amount of money and time to investigate everyone's responsibility.

First of all, the basis of modern criminal law theory is "personal responsibility". To determine the criminal responsibility of suspects, it is necessary to confirm the relationship between their actions and the final result. Individuals are only responsible for the results of their actions. However, the crime of cyberbullying involves many people, and it is difficult to find the relevant people correctly. Secondly, the crimes of cyberbullying often come from the natural behavior of the group, so it is difficult to determine the responsibility by using the principle of "partial execution of full responsibility" by accomplices. Third, the result of cyberbullying crime is often produced slowly, during which various obstacles may occur. For example, suicide because of that person's inner reasons, etc. Therefore, it is difficult to decide what kind of result the prisoner should be responsible for [9].

3.2 The Negation of the "Law Does Not Punish the Masses" Approach to Cyberbullying Crimes

As mentioned earlier, due to the combined effects

of limited criminal law regulation, a large number of perpetrators, and weak causal relationships, the "avalanche" of cyberbullying crimes caused by numerous small acts of cyberbullying seems difficult to punish, making cyberbullying appear to have truly become an act of "the law does not punish the masses." [19] However, in order to provide effective legal remedies for victims, protect the legitimate rights and interests of the people, and maintain social and online order, it is necessary to regulate cyberbullying crimes, and not allow the principle of "the law does not punish the masses" to exonerate the perpetrators hiding behind the scenes.

On the one hand, at the legal level, China has issued the "Guiding Opinions on Punishing Cyber Violence Crimes According to Law" (hereinafter referred to as the "Cyber Violence Guiding Opinions"), which stipulates the legal application of cyber violence crimes. This includes: fabricating and spreading rumors will be punished as defamation; insulting others through wanton abuse, malicious slander, or disclosure of privacy will be punished as insult; organizing "doxxing" and illegally collecting and disseminating citizens' personal information to an unspecified number of people will be punished as infringement of citizens' personal information. Malicious marketing and hype carried out under the guise of cyber violence will be punished as illegal use of information networks. However, the definitions of degree and behavior are somewhat vague, and there is overlap in the behaviors, making accurate application difficult [10].

On the other hand, regarding causal attribution, China currently adopts a more moderate stance in some interpretations, clarifying that even if the time span is long and the causal relationship is weak, even the initial perpetrator must be held responsible for the final serious consequences. The "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Defamation and Other Crimes Committed Through Information Networks" (hereinafter referred to as the "Interpretation on Online Defamation") stipulates that situations such as high click-through rates, suicide or self-harm by the victim or their close relatives are considered "serious circumstances" as stipulated in Article 246, Paragraph 1 of the Criminal Law, thus establishing the crime of insult and defamation [11]. Traditional theory generally holds that defamation infringes upon a person's rights to reputation and privacy, but does not directly cause serious harm to their person. It is generally believed that Cyberbullying is only one reason for serious consequences such as suicide and self-mutilation. In addition, such behavior will also be influenced by external factors, such as a person's psychological and physical condition. Suicide and self-harm are often regarded as intermediary factors and excluded from the scope of responsibility. However, "Interpretation of Cyberbullying" shows that if serious consequences are caused by using the Internet to damage others' reputation or engage in Cyberbullying, it should be the object of the corresponding criminal law. Therefore, he indirectly admitted that there is a causal relationship between cyber bullying and suicidal self-harm behavior.

Therefore, it is clear that China's position on causal attribution is calmer. The center of moderate attribution theory is to go beyond the strict provisions of the previous causal relationship, and blame the results on the people who act in certain circumstances. Different from the past causal relationship theory, moderate attribution theory relaxes this standard, because there is a very definite direct connection between behavior and result. If there is a basic correlation between the behavior and the result-usually, the behavior is a necessary condition for the result to occur-it can be blamed on the person who acts as the result. "Moderation" can be expressed as two points: First, we relaxed the conditions for blaming people for the results. Basically, if there is any conditional relationship, it will blame the result on that person's behavior and let that person bear the responsibility for the result. Second, it is a mild thing to blame the result on the criminal liability that was investigated after that person [12].

"Guiding Opinions on Cyberbullying" and "Internet Slander and Slander Interpretation" to some extent deny the idea that there are too many perpetrators of cyberbullying crimes, so there is no need to punish them. Today, with the serious spread of cyber bullying, it is necessary to punish some perpetrators. On the other hand, the Guiding Opinions on Cyberbullying clarifies the legal provisions used in cyberbullying crimes and provides a legal basis for using rules to restrain this behavior. On the other hand, Interpretation on Internet Defamation clarifies the idea of the relationship between cause and effect. He

believes that even if there are many participants, the relationship between the reasons is very long, and there is nothing wrong with linking the results with the people who cause them. Even if the crime of cyber bullying worsens and various external factors influence it, I still think that the serious consequences that happened to the victims were caused by the initial cyber bullying. This can prevent the perpetrators of cyber bullying from evading responsibility and punishment for various reasons, such as "others' instigation" and "their mental state was not good at that time".

When cyberbullying is serious, publishing, forwarding information and instigating people to spread it will eventually hurt the victim's body and mind. Criminals, especially those who started cyberbullying, those who called everyone together and those who helped others, have clear bad feelings, whether for money or for hurting others. However, these actions are all aimed at attacking others and undermining social rules. The guiding opinions and interpretations have already answered the questions of which crime should be used to regulate these acts and what consequences the perpetrators should be held responsible for. The principle of "the law does not punish the masses" is no longer a "get-out-of-jail-free card."

4. The Denial of "Repeated Cybercriminals"

4.1 Definition of cumulative offenses

As mentioned earlier, cyberbullying crimes do not occur overnight; they are caused by the accumulation of hundreds or thousands of small acts, through individual acts of malice, which eventually break down the victim's psychological defenses and cause harm. Therefore, some scholars have noted the cumulative nature of cyberbullying crimes and proposed using the principle of cumulative offenses. If all people who use the internet do bad things together, they will be considered as cyberbullying. Based on this, everyone who participates has the overall characteristics of cyberbullying, and the behavior of all people who use the network in cyberbullying is also regarded as a kind of cyberbullying.

To use the theory of cumulative crime, we must first understand its meaning. The so-called cumulative crime means that an action poses little threat to society and is not punished as a crime. However, if this action is repeatedly accumulated to a certain extent, the danger will become greater, and the increase in quantity will cause a change in nature and become a crime that must be tried by law.

The subjective factor of repeated crime must be that prisoners have the same or general criminal intention. In other words, don't give up and go on knowing that actions may accumulate harm. In other words, knowing that there may be illegal results, the prisoner is holding the gambler's mood and thinking that "his actions will not have such results" and continues to act. The objective elements of repeated crimes are as follows. There are several criminal acts of the same nature in the same kind of behavior. The action lasted for a long time, and there was no big gap between them, and it continued to cause harm. The accumulation of results and the overlapping of actions make the size of the injury reach the legal standard-for example, in the case of multiple fraud, the total amount must be "a particularly large amount". If the accumulation of behavior exceeds a certain standard, the harm to the legally protected interests will change from "possible" to "actual"-for example, environmental crimes must reach the level of "serious deterioration". [13]

From this point of view, cumulative offenses seems to be in line with the criminal characteristics of cyberbullying: the damage caused by an act is very small, only the respective acts do not constitute a crime, or only have a little damage, but after repeated times, the idea of common liability will change. In the past, criminal law was based on everyone's behavior, but in cumulative offenses, the person who went must be responsible for the "assumed overall result". For example, a person who pollutes must be partly responsible for environmental disasters caused by the actions of other people who may pollute.

4.2 Negation of Cumulative Offenses

However, it is inappropriate to use the theory of cumulative offenses as the basis for attributing the consequences of cyber violence.

First, the application of cumulative offenses mainly focuses on situations where collective legal interests are infringed [14]. The theory of cumulative offenses was first proposed by German scholar C.H. Kuhlen in 1986 based on Article 324 of the German Criminal Code, concerning water pollution. It refers to a special form of crime where a single act is insufficient to cause substantial harm or threat to a legally protected interest; only through the accumulation

of numerous similar acts can a substantial harm be caused. This principle arose because traditional criminal law theory categorizes crimes into actual harm offenses, specific danger offenses, and abstract danger offenses based on the nature of the damage caused to legally protected interests by the acts committed in specific crimes. However, with social development, some acts, when viewed individually, do not possess the potential to harm legally protected interests (environmental crimes being typical), but when combined with the actions of others, they can lead to irreversible and serious consequences. Based on the principle of individual responsibility, in the absence of communication and agreement among the perpetrators, the damage resulting from the accumulation of multiple acts cannot be attributed to any single specific subject. To prevent people from recklessly discharging pollutants and severely damaging the ecological environment due to the lack of explicit prohibitions in criminal law, the theory of cumulative offenses emerged.

The basis for punishing repeat offenders lies in the infringement of collective legal interests. However, cyberbullying primarily infringes upon specific individual legal interests such as the right to reputation and the right to privacy [15]. Therefore, under the current criminal system, unless a "cyberbullying offender" is established, there is no room for applying the theory of repeat offenses.

Secondly, regulating cyber violence through criminal law based on the theory of cumulative offenses carries the risk of being unconstitutional. In the theory of cumulative offenses, cumulative danger is not a necessary prerequisite for constituting a crime, but rather a motivation for legislative consideration. The environmental interests initially subject to cumulative offenses are often irreversibly damaged. Regulating individuals' illegal pollution behavior in advance through criminal law to prevent it from combining with similar behavior by others and ultimately causing damage to environmental interests has a certain degree of rationality. In contrast, the standards for identifying cyberbullying are relatively subjective, and the boundary between freedom of speech and cyberbullying is rather blurred. If we stop or punish the behavior of cyberbullying in advance according to the cumulative crime theory, it is likely to restrict the freedom of speech of citizens too much [16], which is in danger of violating the constitutional principle of protecting the freedom of speech of citizens. In addition, the relationship between similar behaviors in cumulative crimes is fundamentally different from that in cyberbullying.

Taking environmental pollution as an example, there is no causal relationship between different people's pollution behaviors, but they are independent behaviors, and the accumulation of total amount will cause damage to the environment. However, similar behaviors in cyberbullying are generally directly related. In cyberbullying, many netizen gather on a specific event or topic and often launch attacks in a similar way. These behaviors are not only closely linked in time, but also very consistent in content and goal. Participants in cyberbullying often generate new statements in response to previous malicious remarks, creating a chain reaction. In other words, the harmful consequences of cyberbullying are actually caused by the collective behavior of the initiator, malicious netizens, and "spectator" netizens. The causal relationship between the specific subject and the harmful consequences is clearer than that of typical cumulative environmental crimes, therefore, there is no need to apply the theory of cumulative crimes to determine the attribution of the harmful consequences.

The theoretical basis of cumulative offenses lies in the fact that a single act cannot independently cause substantial harm to a legally protected interest; only the accumulation of multiple acts can create an effect sufficient to harm that interest. Therefore, the key to cumulative offenses is that all acts collectively contribute to the final harmful result, and individual acts cannot bear full responsibility alone. Its essence is the infringement of collective legal interests by collective actions; the allocation of responsibility is not based on the dominant position or leading role of any individual actor, but rather on the fact that each participating act contributes to the harm to the legally protected interest. According to the theory of cumulative crime, people who have participated in the adverse consequences to some extent, regardless of whether they are in a dominant position, should be held accountable.

In other words, if we know that one or more perpetrators play a leading role in the occurrence of the result, we don't need to use the theory of cumulative crime for analysis and discussion. Although we can use the theory of cumulative crime to explain cyberbullying, we should know

that not all the perpetrators of cyberbullying should be held accountable, but the responsibility for the consequences should be attributed to those who play a leading role [18].

5. Reconstruction of Attribution of Responsibility in Cyberbullying Crimes

5.1 Introduction of Typological Thinking

In order to find out the responsibility of cyberbullying's crime, we need to find out who is involved. Different standards, these people are classified in many different ways. However, if we want to separate all the people involved in cyberbullying crime without omission, we need clear classification standards. This standard is generally based on identity or action. Because if it is such a standard, it can be targeted at everyone. In the daily stories about cyberbullying crimes, the true identities of "instigator" and "segregator" are often mentioned, which becomes an important clue to determine the responsibility. This shows the tendency to investigate the responsibility of those who have played a special role in the crime of cyberbullying, which is the performance of typological thinking. Typological thinking in law is a way for law makers to divide legal phenomena, social relations and related personnel with similar nature, work and behavior into groups according to the essential characteristics, inherent rules and social needs when making legal rules. They decide the legal rules, rights and obligations and legal consequences suitable for each group. This is not a simple classification, but to go deep into the essential level of legal objects, find the differences and commonalities between different groups, and establish a scientific, reasonable and targeted legal mechanism [17].

However, if status has nothing to do with determining the illegality of its behavior, it cannot be classified by status. For example, bribery refers to the behavior of state employee who uses his position to extort money or illegally accept goods from others without seeking benefits for others. Because of the status of state employee, you can't trade the behavior about work, so you will be punished according to this status. If it is a normal life, it is just a transaction of "exchanging one's own behavior for reward". What makes this behavior illegal is status. However, in cyberbullying crimes, the status we usually talk about does not necessarily make its behavior illegal. People who don't have a specific status can also become bad people, and the illegal content is still the same.

Therefore, for cyberbullying crime, we can't just focus on identity when considering it separately. We should pay attention to the behavior itself and punish those who have done certain behaviors and those who have not. This is not based on insults, reputation damage, personal information disclosure and other behavior content to divide the responsible person, but based on the role of behavior in cyberbullying crime and "division of responsibilities" to determine the responsible person.

5.2 Organizational Domination Theory

According to the previous theory of indirect perpetratorship, for the purpose of committing crimes, only those who use people who are incapable of committing crimes or who are not in the mood to commit crimes are indirect Perpetrators. This is to control the development trend of crime by means of intimidation and deception, and treat the people who are used as tools of crime. Accordingly, in the crime of cyberbullying, the first person to create an opportunity, even if objectively dominated to make cyberbullying happen, actually did not control the swearing person. People who do cyberbullying, such as language attacks, act entirely according to their own wishes. Therefore, we can't hold them accountable with the theory of indirect perpetratorship.

However, organizers are indeed indispensable for the occurrence of crimes. The basis for a perpetrator to ensure the achievement of their illegal purposes is the large number of potential perpetrators. As long as some of them follow their instructions, cyber violence crimes can be guaranteed to occur.

Based on the autonomy of perpetrators of cyber violence and the guiding role of initiators and instigators, the theory of indirect perpetrators' organization and control will form the basis for constructing a theory of liability in cyber violence crimes.

The theory of organizational control arose from the need for judicial trials of Nazi war criminals after World War II. Traditional criminal law theory struggled to explain how high-ranking Nazis like Hitler and Himmler could commit crimes by issuing orders without directly participating in their execution. Therefore, Roxine proposed that such leaders, while not directly controlling the executors, ensured the execution of orders through organizational power

structures, thus constituting indirect perpetrators [21]. This theory was accepted in the 1990s by the German Federal Court during the Berlin Wall shooting trial, demonstrating the criminal responsibility of both the East German soldiers who carried out the shooting and the state organization behind them.

Roxine argues that the leaders of organized power structures do not coerce or deceive those directly carrying out the crimes. The executors have complete free will and can refuse to carry out criminal orders without hindering the leaders from achieving their criminal goals.

Unlike instigators and traditional indirect perpetrators, leaders of illegal organizations do not directly decide or control the occurrence and progress of events according to their own will. The organizers and implementers are relatively independent.

However, this weak control is compensated for by the sheer number of members and the organizational structure, ensuring the successful achievement of the criminal objectives. Faced with a powerful organizational machine, grassroots members "do not play the role of free and responsible individuals, but rather anonymous, replaceable figures… merely replaceable cogs in the power machine." The refusal or failure of individual members to carry out the organizer's expected behavior does not prevent other members from correctly implementing the organizer's demands. Therefore, the sheer number of members allows for errors in execution, and the arbitrary replaceability of executors, along with the large number of grassroots members, jointly ensures the smooth execution of the organizer's criminal plan, independent of whether the members' free will obeys the organizer. Furthermore, the replaceability of specific executors makes them more likely to accept orders than specially selected executors, because individuals may think, "Even if I don't do this, someone else will," thus eroding their conscience and moral burden based on group behavior.

In cases of organized control, the direct perpetrator is not coerced or deceived, or a normal, rational person would not have compelled to commit a crime under clearly unreasonable demands; therefore, they possess full criminal responsibility and should be punished for personally committing the principal act. The organizer is a principal behind the principal, and a fully responsible principal behind the principal; they should be held responsible for their intentional guidance and exploitation of the perpetrator, and for macroscopically orchestrating the entire situation [20].

Based on the organizational control model, we can better analyze and determine the principal responsibility in cyberbullying crimes. In cyberbullying crimes, according to typological thinking, we can roughly divide the "division of labor" into three categories: initiators/instigators, general participants, and passive administrators. In this criminal act, initiators/instigators are responsible for instilling specific ideas and guiding the behavior from the outset; general participants intentionally or unintentionally join the attacks on the victims as desired by the initiators/instigators; and passive administrators de-escalate the situation. These three categories can be considered an "organization," which includes leaders and lower-level executors. The organizers and instigators of cyberbullying crimes are the "organizational" leaders who guide the occurrence of cyberbullying. Given the large number of netizens, as long as a small portion participates in cyberbullying—that is, general participants—it is possible to ensure that harm is inflicted on the victims; the substitutability of this action is relatively strong.

Therefore, based on the theory of organizational control, ordinary participants in cyber violence crimes will be punished as fully conscious subjects who directly carry out the crimes; initiators and instigators should be sanctioned for their organizational control and guidance of the situation. This is the theoretical basis for constructing the subject of responsibility for cyber violence crimes.

5.3 Responsibility for Positive Behavior

Active behavior refers to the act of instigating cyber violence and spreading false or insulting remarks in cyber violence crimes, knowing that it may cause harm to others. Those who engage in active behavior mainly include instigators and general participants.

Cyberbullying crimes are characterized by their mass and cumulative nature, representing a typical pattern of mob crime. Mob crime is a special type of crime under criminal law, its core feature being the joint commission of illegal acts by multiple individuals, with the acts themselves possessing a mob-like, public, or socially harmful nature. These crimes not only infringe upon specific legal interests but also often impact

public order and social management. In mob crime, the general attitude of legislators is to punish the ringleaders. Although current Chinese regulations governing cyberbullying crimes such as insult, defamation, and infringement of citizens' personal information do not stipulate punishment only for ringleaders and active participants, this article discusses the issue of determining the responsible party in cyberbullying crimes. Given the structural similarities between the two, it is appropriate to determine the responsible party by referring to the handling mechanism of mob crime. Furthermore, in general principle, punishing the ringleaders is essential for any crime; in cyberbullying crimes, the ringleaders are generally the organizers and instigators.

5.3.1 Initiators and instigators

The people who started cyberbullying are mainly people who make online rumors and swear words and spread them. Usually, these people are the first to post false information or attack with difficult language on the Internet. Their purpose is to let many people see it on the online platform, spread the lying information and swearing words quickly, and hurt the reputation, self-esteem and mental health of the victims. People who are the foundation of cyberbullying have a great role in this bad thing. In terms of legal troubles, compared with many participants, it is a little easier to find the person who sent the information first and confirm whether the information is bad or not.

"In the online world, it is very common for information to be clicked, viewed and forwarded. Therefore, the actual clicking, viewing and forwarding of the swearing information must all be attributed to the behavior of the swearing person. Simultaneously, as long as the perpetrator disseminates fabricated information online, they are aware that others will click, view, or forward it." [22] These initiators and instigators know and should know that their controversial and inflammatory remarks on online platforms may trigger other netizens to follow suit and imitate, thereby exacerbating the negative impact of their statements. Furthermore, they at least subjectively harbor an attitude of indifference. Therefore, from a legal liability perspective, those who initiate and instigate cyberbullying not only bear direct responsibility for the inappropriate information they disseminate but should also foresee the potential chain reaction of their actions and bear the corresponding legal consequences. Thus, in cyberbullying incidents, the initiator of cyberbullying should be considered the primary target of criminal liability. Meanwhile, it's worth considering whether all acts of initiating or instigating cyberbullying should be punished. Cyberbullying crimes such as network insult and reputation damage belong to the category of abstract dangerous crimes. If "serious situation" is taken as the criterion of conviction, it should be decided whether its actions will increase the risk of reputation damage. However, because the Internet has a strong ability to expand time and space, the content of Cyberbullying can be kept in the form of text and images. Therefore, it should be considered that insulting and damaging reputation on the Internet is a serious crime, which will bring great threat to personal reputation and physical and mental health. Doxing, spreading rumors, swearing and other behaviors have a strong threat to the victim's reputation and will bring greater psychological pressure and adverse effects. We should pay attention to the protection of victims, rather than taking countermeasures after serious consequences.

The conclusion is that no matter how bad the situation is, those who initiate or instigate the crime of cyberbullying must bear the responsibility. In the actual cyberbullying incident, this kind of person is usually the actual instigator and the first person to have a certain degree of influence. They are organized, with the purpose of launching the cyberbullying incident and expanding the results.

However, I want to clarify one thing here. Our target is cyberbullying, not all inappropriate speeches. The reasons are as follows. First of all, legal and illegal information accounts for all the contents of free speech. If inappropriate information is strictly classified as illegal, citizens' freedom of speech will be severely restricted. Secondly, the general criterion for judging cyberbullying is "the effect of actual personal attack", but the feeling of personal attack varies from person to person, so it is impossible to take actual harm as the criterion. Inappropriate speech should be judged according to its subjective malicious and inflammatory nature, and the potential harm it may bring to ordinary people. If the speech has the nature of malicious instigation and the potential result can be predicted, it should be considered as cyber bullying [23].

5.3.2 General Participants

"General participants" refers to individuals who actively participate in spreading false or insulting information or attacking victims in cyberbullying crimes. According to the model of mob crime, generally, except for a few crimes where only the ringleaders are punished, most mob crimes also punish active participants, those with significant involvement, and repeat participants. Therefore, in the case of cyberbullying crimes, there is no reason to exclude participants from punishment. Although the impact of a single unfriendly comment may not be significant in isolation, the accumulation of thousands of unfriendly comments in a short period can still create enormous psychological pressure on victims. Punishing general participants is a necessary measure to deal with this kind of unfriendly comment that is "not so bad when scattered, but overwhelming when gathered," and is a crucial issue that cannot be ignored in the governance of cyberbullying. Punishing general participants serves two purposes: firstly, their actions seriously infringe upon legal interests; secondly, it serves as a warning and educational tool, preventing future occurrences and clarifying the boundaries of freedom.

If participants are to be punished, it is necessary to identify who should be punished. Clearly, punishing all of the tens of thousands of participants in cyberbullying would be too costly and unnecessary under criminal law. The law needs to select those whose actions warrant criminal punishment. China's criminal law specifies the number of offenses required for certain crimes. In these crimes, a single act is insufficient to meet the elements of the crime; only repeated acts of similar behavior are sufficient. A typical example is the provision for "repeatedly and secretly stealing public or private property" in theft. A similar principle can be applied to assigning responsibility in cyberbullying crimes. Those who repeatedly spread false information and play a prominent and significant role in cyberbullying cases should be given appropriate criminal penalties. This regulation should, on the one hand, emphasize their significant role and importance; otherwise, it risks expanding the scope of criminal prosecution. On the other hand, their primary actions should be dissemination, such as liking and forwarding, to distinguish them from the instigator role of key figures.

Punishing general participants is based on their role as accomplices in cyberbullying, which aligns with the principle of the unity of the legal order. Minor acts of online insults, defamation, and infringement of citizens' personal information can be considered illegal, but the application of criminal penalties requires careful consideration. The frequency of such acts plays this role; by examining factors such as the number and extent of participation, the necessity for prevention can be assessed. In real-world cyberbullying cases, general participants typically include prominent individual netizens and important public figures involved. Whether misled or acting intentionally, they all contribute to the occurrence of cyberbullying, making prevention necessary.

5.4 Responsibility for Negative Behavior

Passive behavior refers to actions taken when one could have prevented the escalation of cyberbullying but failed to fulfill their due obligations. Those primarily engaging in passive behavior are internet platform providers and operators. As platform managers, internet service providers (ISPs) have a management obligation to control areas where danger arises. However, ISPs often indulge in the escalation of controversies and even cyberbullying in order to attract users. Maintaining a healthy and peaceful online environment is a social obligation of ISPs. ISPs that fail to prevent or condone the escalation of cyberbullying should also bear responsibility for the harm suffered by the victims.

Of course, emphasizing the regulatory obligation of the platform does not mean that the platform should manage everything, but has the obligation to take necessary and limited management measures.

There are two reasons to cherish "limited things". First, because the internet platform is a folk thing, we should protect our right to operate freely. If the state interferes too much, its original nature may change. Second, most of the bad information on the internet is annoying and distorted, and its illegality is lower than that of aggressive language. If the platform is required to manage these words, it will adopt the practice of "mixing them all together" and ban all the contents that may cause criticism and discussion, which is in danger of damaging freedom of speech. If suppressed, it will only rebound even more, which is inconsistent with the true nature of the internet, which is "open, shared and free".

Therefore, the monitoring obligation of internet platform must abide by the principle of "balance".

Platform should choose the method that has the least impact on everyone while controlling the serious cyberbullying. Generally, a tiered management system should be adopted for internet content, meaning stricter control or even deletion measures should be taken for cyberbullying information with strong illegal characteristics and obvious insults and attacks; more lenient regulatory measures should be taken for "harmful information" with less obvious illegality, controlling it only when necessary. At the same time, internet platforms also have a regulatory obligation to monitor behaviors that clearly aid and abet cyberbullying crimes [24].

The Ninth Amendment to the Criminal Law added the crime of refusing to fulfill information network security management obligations, indicating an attitude that platforms need to manage cyberbullying, rather than treating them as accomplices. Punishing network service providers as accomplices to cybercrime would result in an excessively low threshold for conviction, which is detrimental to the development of the internet industry. Network service providers' failure to promptly delete illegal information is usually not due to shared intent with cyberbullying or criminal behavior, but rather influenced by practical factors such as operating costs. If treated as accomplices, platforms could easily be convicted due to inadequate management. While network service providers, as technology platforms, have a management obligation for information dissemination, they are fundamentally different from direct perpetrators of crimes; they do not directly plan or actively participate in crimes. Therefore, they cannot be simply regarded as accomplices to cybercrime, but rather regulated separately.

Theoretically, it is also agreed that online platforms only bear a criminal obligation to take positive action regarding obviously illegal information. Only when an online platform fails to properly fulfill its supervisory obligations under criminal law can it potentially face criminal penalties. Specifically, if an online platform subjectively and clearly knows of the existence of information involving cyberbullying and clearly illegal, yet still fails to act; and objectively speaking, if this inaction promotes the initiation, organization, or incitement of cyberbullying that has reached the level of a crime, then the law should hold the internet platform accountable for its inaction, and the internet platform should bear responsibility for its inaction that has contributed to the cyberbullying [25].

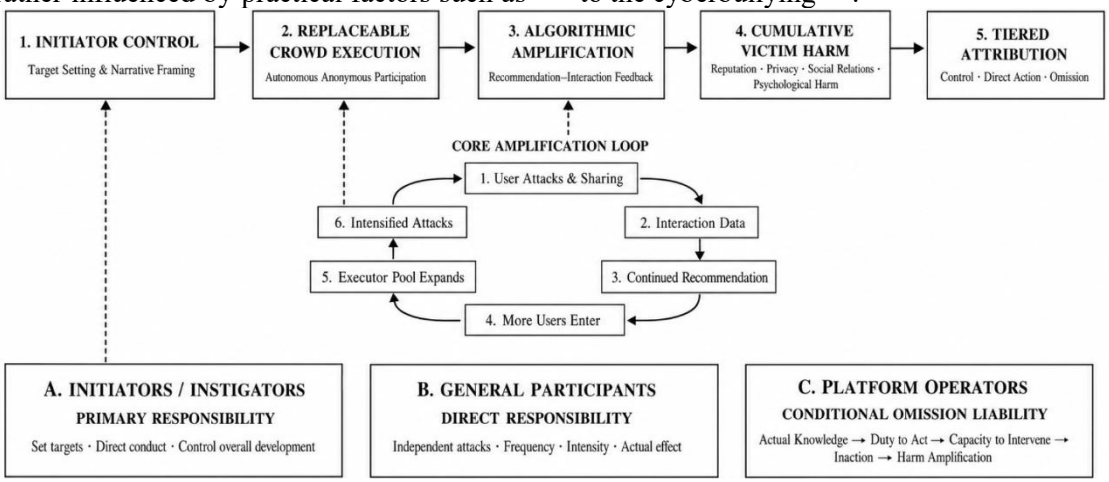


Figure 2. Subject Relationships and Hierarchical Accountability Mechanism in Cyber Violence Crimes Under the Organizational Dominance Theory.

As shown in Figure 2, the initiators and instigators do not directly control each participant. Instead, they macroscopically promote the continued occurrence of cyberbullying by setting attack targets, shaping narrative frameworks, and leveraging the large number and substitutability of anonymous participants. Ordinary participants, acting on their own independent will, should bear responsibility for their direct actions such as commenting, forwarding, and doxing. Platform operators bear corresponding responsibility only when they knowingly fail to act despite having the knowledge of illegal information, a duty to address it, and the ability to intervene, and thus actually contribute to the expansion of harm. Therefore, the principal responsibility for cyberbullying crimes should be stratified according to overall control, direct execution, and passive inaction.

6. Conclusion

While the digital age brings convenience to life, it has also given rise to the prominent problem of cyberbullying. Cyberbullying, with its anonymity, widespread dissemination, and low-cost ability to create public opinion, severely infringes upon the legal rights of victims, including their right to reputation and privacy, and can even lead to serious consequences such as "social death," psychological and physical harm, and suicide. When investigating the case of cyberbullying, it is important to find out who is in charge before adding the correct charges. Therefore, it is very necessary to rethink the decision method of cyberbullying's criminal responsibility to guide the healthy growth of the Internet and abide by social rules.

This article first investigates the current situation and difficulties of cyberbullying crime. The information immediately spreads to many people, and the action is hidden without knowing the name. The perpetrators are easy to act in groups, and the losses are getting bigger and bigger. Then criticize the idea that "many people can't be punished by law" and the idea of "accumulated cyberbullying". The first idea is that the responsibility in cyberbullying crime is scattered and the relationship between cause and result is complicated, so it is difficult to use it. The second idea is that cyberbullying is unreasonable mainly because it hurts the important rights of individuals and may violate the constitution, and the relationship between cause and effect is easy to change.

This paper puts forward a method to re-examine the previous ideas and re-formulate the way of giving responsibility to cyberbullying crime. First of all, I'm introducing typological thinking. When deciding the responsibility, look not at the person's identity, but at the action itself, and tell him that the action is very important on cyberbullying crime. Secondly, separate positive behavior from passive behavior, and give different weights to the people who started, instigated and ordinary participants. The first person and the instigator should bear the heaviest criminal responsibility because they will become the root of cyberbullying. The behavior of ordinary participants will also seriously damage the interests protected by law, so we should consider the nature, frequency and severity of the behavior as an accomplice and be held accountable. Finally, regarding passive behavior, he believes that the supervision obligations of providers and operators of internet platform are very important. They said that limited necessary management countermeasures must be taken, and the principle of balance must be observed. If the supervisory obligations are not fully fulfilled, they should bear criminal responsibility.

Finally, to reshape the responsibility mechanism of cyberbullying, many things need to be considered, including how to distinguish behaviors, the difference between active behaviors and passive behaviors, and the obligations of the monitoring platform. Defining the responsible party, deeply judging the misconduct and enhancing the platform responsibility can well prevent the spread of cyberbullying. Safeguard the legitimate rights and interests of victims and maintain the healthy development of social order and network environment. In the future, with the continuous development of internet technology, banning cyberbullying will face more problems, but separate consideration is still a practical method to establish a more scientific and reasonable mechanism for banning cyberbullying.

References

[1] China Internet Network Information Center, The 56th Statistical Report on China's Internet Development, https://www.cnnic.cn/n4/2025/0721/c88-11328.html (in Chinese).

[2] Wang, J., Breaking the "Law Does Not Punish the Masses" Dilemma in Cyberbullying: "Two Supremes and One Ministry" Demand Strict Legal Accountability for Cyberbullies, 21st Century Business Herald, September 2023, 1st ed. (in Chinese).

[3] Ministry of Public Security: Public Security Organs Handled More Than 8,600 Cases of Cyberbullying in 2024, People's Daily Online, http://society.people.com.cn/n1/2025/0110/c1008-40399408.html (in Chinese).

[4] Fu, Y., Breaking Out of the Dilemma of "The Law Does Not Punish the Masses": Criminal Law Regulation of Insult and Defamation-Type Cyberbullying Crimes, Hebei Vocational Education of Law 3, no. 2 (2025) (in Chinese).

[5] Miao, X., An Analysis of the Causes of Cyber Linguistic Violence, People's Tribune (Bimonthly), no. 12 (2014) (in Chinese).

[6] Yang, T., Three Prerequisites Must Be Considered Before "Human Flesh Search"

Can Be Criminalized, Procuratorial Daily, August 26, 2008 (in Chinese).
[7] Jiang, T., The Convergence of Criminal, Administrative, and Civil Liabilities in Cyberbullying Governance, Legal Science 39, no. 5 (2023) (in Chinese).
[8] Chen, Y., Wang, S., & Liu, X., Adolescent Relatedness Need Satisfaction and Deindividuated Online Behavior: A Moderated Mediation Model, Chinese Journal of Clinical Psychology 27, no. 6 (2019) (in Chinese).
[9] Tian, H., The Dilemma and Resolution of "The Law Does Not Punish the Masses" in the Criminal Law Governance of Cyberbullying, Law Science Magazine 45, no. 1 (2024) (in Chinese).
[10] Ministry of Public Security of the People's Republic of China, Guiding Opinions on Lawfully Punishing Cyberbullying Illegal Crimes, https://www.mps.gov.cn/n6557558/c9221769/content.html (in Chinese).
[11] Supreme People's Procuratorate of the People's Republic of China, The Supreme People's Court and Supreme People's Procuratorate Issue Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Such as Online Defamation, https://www.spp.gov.cn/zdgz/201309/t20130910_62417.shtml (in Chinese).
[12] Zhang, M., On Mitigating Result Attribution, China Legal Science, no. 3 (2019) (in Chinese).
[13] Leng, B., Criminal Law Governance of Cumulative Dangerous Behavior in Collective Cyberbullying, Rule of Law Research, no. 5 (2023) (in Chinese).
[14] Roxin, C., New Developments in the Discussion of Legal Interests (translated by Xu, S.), Yueda Law Journal [Taipei University Law Review], no. 12 (2012) (in Chinese).
[15] Zhang, M., Criminal Law Protection of Collective Legal Interests, Law Review, no. 1 (2023) (in Chinese).
[16] Kreß, P., On the Justification of Cumulative Offenses (translated by Tong, Y.), Nanjing University Law Review, no. 2 (2024) (in Chinese).
[17] Xiao, C., Reconstruction of Attribution Logic and Normative Iteration in the Criminal Governance of Cyberbullying, Journal of East China University of Political Science and Law 28, no. 4 (2025) (in Chinese).
[18] Zhang, Z., Criminal Law Response to Cumulative Offenses of Cyberbullying, Dongyue Tribune, no. 4 (2024) (in Chinese).
[19] Li, M., Regulatory Difficulties and Criminal Responses to "The Law Does Not Punish the Masses" in Cyberbullying Crimes, Contemporary Law Review, no. 5 (2024) (in Chinese).
[20] Yuan, G., The Logic of and Reflection on the Theory of Organizational Domination in Criminal Law, The Jurist, no. 6 (2020) (in Chinese).
[21] Roxin, C., Straftaten im Rahmen organisatorischer Machtapparate, Goltdammer's Archiv für Strafrecht, 1963, S. 199 ff.
[22] Zhang, M., Exploration of Controversial Issues in Online Defamation, China Legal Science, no. 3 (2015) (in Chinese).
[23] Wang, X., & Huang, J., Cyber Righteousness or Cyberbullying: The Boundaries and Legal Control of Online Reporting and Supervision Behaviors, Law Forum, no. 5 (2024) (in Chinese).
[24] Zhang, L., How to Govern "Bad Information"-Type Cyberbullying: An Analysis Based on Field Theory, Exploration and Free Views, no. 7 (2023) (in Chinese).
[25] Shi, J., Platform Responsibility in Cyberbullying Governance, Legal Science (Journal of Northwest University of Political Science and Law), no. 6 (2023) (in Chinese).