

Theoretical Evidence and Rules of the Application of the Injunction for Personality Rights in Cyber Violence Cases

Ao Shi

School of Humanities and Law, North China University of Science and Technology, Tangshan,
063000, China

18762035795@163.com

Abstract. Cyber violence in the digital age features mass, concealment and diversity, which not only causes serious infringement on the personal and property safety of victims, but also brings new challenges to the existing network management order. The existing cyber violence governance mainly relies on the governance paths of individualism, organizationalism and nationalism. However, it is difficult to fully resolve the multiple risks triggered by cyber violence. The core function of the injunction system for personality rights established in the Civil Code is to provide a convenient and efficient protection mechanism for personality rights, and to build a protection mechanism for cyber violence governance that closely combines prevention in advance with timely infringement suppression, which to some extent makes up for the shortcomings of the traditional governance model with post-event relief as its essence. In terms of specific application, it is necessary to clarify the specific conditions and applicable procedures for embedding the injunction for personality rights into cyber violence governance. Meanwhile, it is of significance to distinguish between the application of injunction for personality rights and the safe harbor privacy principle, and improve the specific rules of blockchain electronic certificate deposit technology and platform responsibility, so as to provide technical support and platform connection for the embedding of injunction for personality rights into cyber violence governance.

Keywords: Cyber Violence Governance; Injunction for Personality Rights; Personality Rights Infringement.

1. Introduction

With the continuous innovation of Internet technology, the Internet has become an important medium for citizens to express opinions. In addition, with the characteristics of immediacy and convenience, the Internet has become the mainstream for citizens to express their standpoints. The data shows that the number of Internet users in China has reached 1.092 billion, and the Internet penetration rate has reached 77.5%. However, the surge in the number of Internet users has resulted in some negative effects, among which cyber violence is particularly prominent. Some related cases such as the "Pangmao incident" and "the incident of a mother who fell to her death for her child killed in the school by car" not only seriously violated the personal and property interests of the victims of cyber violence, but also challenged the cyberspace governance. To prevent all kinds of risks brought by cyber violence, the National Network Information Office has launched a nationwide campaign to purify the online environment and issued the Regulations on Information Governance of Cyber Violence, which provides a basis for further improvement of cyber violence governance.

However, the existing network governance mode often focuses on post-event relief. It is difficult to play an effective role in the rapidly changing network environment. Injunction for personality rights, as a protection mechanism that intertwines prevention in advance and timely infringement suppression, may provide a new institutional scheme for promoting the governance path of cyber violence. However, as a brand-new system in civil litigation, the specific applicable conditions and rules of the injunction for personality rights remain unclear. It is still controversial whether it is necessary to apply it to cyber violence governance and how to apply it. On the basis of sorting out the current situation of cyber violence, this paper will summarize the shortcomings of the existing model, demonstrate the necessity and feasibility of applying injunction for personality rights in cyber

violence governance, and propose the specific rules for embedding the injunction for personality rights in cyber violence governance.

2. Current Situation and Predicament of Cyber Violence Governance

(1) Cyber Violence and Its Risks of Harm in the Digital Age

Cyber violence refers to the anomie behavior that uses the Internet as a medium to infringe on the personal rights and interests of others and endanger the normal order of cyberspace through personal attacks such as insults, abuse, rumors and slander, and invasion of privacy. In cyberspace, cyber violence is mainly manifested in the form of wantonly publishing abusive insults, rumors and slander, privacy invasion and other information against individuals. Derogating personality, damaging reputation, and causing "social death" or even mental disorder, suicide and other serious consequences are also the manifestations of cyber violence.

As a product of the digital age, cyber violence has distinct characteristics of the times compared with traditional types of violence. First of all, cyber violence has group nature. The so-called a group nature means the trend that current participants in cyber violence show professionalization and industrialization, such as "cyber paid supporters", etc. Such paid supporters wantonly attack others by collecting "fees". Besides, its published content is seriously homogeneous with obvious subjective malice.

Secondly, cyber violence is concealed. The Internet provides a platform for every citizen to communicate. Because the network allows people to use false identities, the concealment of infringing subjects is enhanced, which makes it extremely tricky to track and identify infringers. In addition, opinions are individual remarks about things, events, ideas or characters. Opinions also have strong subjective attributes, and everyone has the right to express, that is, freedom of speech. Meanwhile, freedom of speech and reputation rights are mutually restricted with a boundary of insult between these two rights, while the determination of whether it constitutes insult is vague. From the perspective of infringement accountability, the combination of virtuality and reality of the network makes it difficult to identify causality with a high cost and difficulty of cyberspace governance and accountability, which makes it hard to control and punish network illegal acts.

Last but not least, the manifestations of cyber violence are diverse, including but not limited to publishing offensive and insulting remarks, disclosing the private information of cyber participants, and promoting social hatred and extreme thoughts. In addition to publishing insulting and offensive remarks through the Internet, private information exposure, causing others to suffer mental pressure, personal rights violation, and the use of the Internet to publish enmity speech and spread extreme thoughts should also be regarded as cyber violence.

Cyber violence featuring group nature and concealment has brought great challenges to the protection of personality rights and social governance. After suffering from cyber violence, most victims feel uneasy and stressed, fall into self-doubt and even overreact in the face of overwhelming negative remarks. In this state, it is difficult for victims to calm down and collect fixed evidence. From a social perspective, cyber violence disrupts the normal order of cyberspace, challenges the bottom line of social morality, causes social instability and undermines social harmony. Cyber violence is also detrimental to the protection of teenagers. Minors may virtually become participants or victims of cyber violence due to a lack of cognition and correct guidance.

(2) Governance Dilemma of Cyber Violence

First of all, the rapid development of information technology has broken the dual-subject relationship embodied in the traditional physical space identity. At present, the measures of cyber violence governance are mainly passive and post-event. In other words, after the violence occurs, the victim can lodge a complaint through legal channels or online platforms. However, it is difficult to identify the specific infringer in this process, and even if the specific individual is sued, it is hard to completely eliminate the social impact of cyber violence through litigation, and then make up for the damage to the victim's personal and property rights. The dilemmas faced by victims range from the

difficulties of stopping violence and eliminating adverse social impacts, the complexity of evidence collection to the difficulty of identifying liability, and the inadequacies of existing remedies in decreasing the consequences of violations.

Secondly, it is difficult to form a long-term mechanism for the regulation of group behavior by existing governance means. In recent years, the Interpretation of Several Issues Concerning the Application of Laws in Handling Criminal Cases such as Defamation through Information Network jointly issued by the Supreme People's Court and the Supreme People's Procuratorate stipulates that if the same defamatory information is clicked, viewed 5,000 times, or forwarded 500 times, it can be regarded as serious defamation. Since then, cyber violence has been controlled to some extent. However, on anonymous social platforms, the effect of legal governance is limited. At best, it can only regulate fewer central nodes and it lacks a strong binding force on those who participate in group language violence through comments and forwarding. The perpetrator may publish the infringing information on multiple platforms simultaneously, which makes it challenging for the victim to collect evidence. Moreover, the way the perpetrator hides, deletes or adds cyber violence information at any time will make the victim tired of coping, resulting in the difficulty of implementing the long-term mechanism.

Finally, the existing legal provisions are not perfect. Although the law is beginning to require network service providers to assume more regulatory responsibilities, the specific data compliance obligations have not been fully clarified in the newly introduced Data Security Law and Personal Information Protection Law. Meanwhile, the existing civil and administrative laws and regulations are weak in dealing with cyber violence. Although the Civil Code and relevant judicial interpretations stipulate the protection of civil rights, it is still difficult for victims of cyber violence to protect their rights in practice. Traditional crimes such as insult and libel can't fully adapt to the particularity of cyber violence, triggering the lag of the law and the inability to fully cover all kinds of acts of cyber violence. From the perspective of criminal governance, the applicable standards of crimes against serious cyber violence in criminal law are still unclear, which affects the role of criminal law in ensuring cyberspace security. The connotation and extension of cyber violence are constantly developing, which fails to be effectively regulated solely by the existing system. For example, group derogation and moral trial in cyber violence can't be properly handled through the existing crimes. Hence, some scholars believe that the existing crime system is no longer competent for the arduous task of cyber violence governance. It is necessary to add a special "cyber violence crime" to the criminal law sub-provisions.

All in all, based on the dilemma of cyber violence governance, a new path of cyber violence governance should be explored. Introducing the injunction for personality rights into the cyber violence governance may provide a new solution.

3. Theoretical Evidence of Embedding Injunction for Personality Rights in the Cyber Violence Governance

For cyber violence governance, this paper puts forward a feasible way to embed the injunction system for personality rights. The existing ways to control cyber violence are not perfect. Their commonality lies in the fact that they all try to control cyber violence by legal means, relying on a certain force as the main body, and trying to limit and reduce cyber violence through legal norms. However, there are great differences in governance subjects, governance methods and governance effects. Comparatively speaking, the injunction system for personality rights has more advantages in solving cyber violence disputes. With a solid theoretical basis and clear characteristics and functions, it is legitimate and feasible to be embedded in cyber violence governance.

(1) Existing Cyber Violence Governance Paths and Their Shortcomings

Generally speaking, the existing cyber violence governance can be summarized into three governance paths, including individualism, organizationalism and nationalism. Individualism is to blame the responsibility of cyber violence on individuals. It believes that the problem can be solved

by directly punishing the initiator, which is a typical traditional idea. At present, the application of individualism in the cyber violence governance is reflected in the use of "habeas corpus", in which the victim applies and provides evidence, and the judicial organ promulgates it after verification, so as to safeguard the legitimate rights and interests of the victim and regulate the words and deeds of cyber participants. The core of organizationalism lies in the fact that the law sets up external regulatory laws aimed at self-regulation for Internet companies, and imposes specific governance responsibilities on online social platform organizations, which use their technical strength to restrict and delete all immoral speeches and accept government supervision simultaneously. Nowadays, western countries represented by the European Union mainly adopt an organizationalism model to control cyber violence. The characteristic of the nationalism model is that political power directly intervenes in the operation of the moral system in the "name" of law, thus injecting political rationality into moral communication.

The above models of cyber violence governance all have shortcomings. First, the existing governance models rely too much on the power of national legislation and administrative supervision. China's government directly intervenes in the management of Internet content through legislative and administrative means, such as Cyber Security Law and Personal Information Protection Law, etc. However, it is difficult to achieve cyber violence governance by relying solely on administrative supervision. As far as the state power system is concerned, the network platform is at the lower level. In other words, the network platform mainly provides services to users in accordance with relevant laws and regulations, and fulfills its due legal obligations. Its supervisory authority for bad information is also given by law, which is very limited.

Secondly, the existing governance path tries to improve the efficiency of governance by consolidating platform responsibilities. China's legal system has provisions that embody the principle of organizationalism, mainly adopting the safe harbor privacy principle. When cyber violence infringement occurs, the network service provider, that is, the network platform, is obliged to delete the speeches, pages, links, etc. that constitute the infringement. Hence, the platform is required to undertake more obligations. But this path has great defects. On the one hand, it is difficult for the platform to fulfill its responsibility for cyber violence governance. If the platform is required to bear too much responsibility, it will be overburdened, which is not conducive to the development of the digital economy. The platform is timid and will strictly control the speech of netizens under pressure, thus restricting the citizens' freedom of speech. On the other hand, the existing platform responsibility is mainly avoided according to the safe harbor privacy principle, and the platform only needs to take necessary measures to be exempted from liability, which is detrimental to cyber violence governance.

Finally, the over-reliance on the path of individualism aiming to strengthen personal awareness of the rule of law and relief means also has great defects. On the one hand, cyber violence is a "social addiction behavior", which is a "compulsive operation activity" where individual moral communications are systematically connected and then incorporated into the system. As the internal motivation of self-reproduction originating from the moral system, cyber violence is beyond self-consciousness and subject behavior, which is difficult for individuals to control. On the other hand, according to the personal safety protection order system applicable in civil litigation in China, the Anti-Domestic Violence Law of the People's Republic of China promulgated in 2015 embodies the functions of prevention and suppression, but the objects prohibited by the personal safety protection order are limited to domestic violence that infringes on citizens' physical health and personal freedom. The protection interest is also small, which makes it difficult to apply it to cyber violence governance. Moreover, the judicial procedure is too lengthy, inefficient and low in adjustment rate. Hence, it is difficult to quickly and fully relieve victims.

(2) Legitimacy Analysis of the Injunction System for Personality Rights Embedded in Cyber Violence Governance

Cyber violence features the group nature, concealment and diversity. In addition, the existing governance means are difficult to fully resolve all kinds of risks brought by cyber violence. However, the injunction system for personality rights can provide a protection mechanism for cyber violence

governance, which intertwines prevention in advance with timely stopping of infringement, making up for the shortcomings of the traditional governance model with post-event relief as its essence. Personality right injunction means that when a civil subject finds that his personality right has been infringed, he can apply to the court for an injunction, and the court will order the perpetrator to stop the infringement. The introduction of such a system plays an essential role in dealing with the particularity of personality rights infringement in cyberspace, such as fast diffusion time (group), wide scope and irreversible results.

On the one hand, the personality rights system can provide quick and effective relief for victims and avoid long-term litigation tug-of-war. Traditional cyber violence governance either relies on national law enforcement departments or platform relief, but both of them require a long period. Thus, it is difficult to provide timely protection for individuals. Given that once cyber violence fails to be controlled in time, mass cyber violence will follow. When individuals find it difficult to seek relief from the state or platform, their personal rights and property safety will be seriously threatened. The injunction for personality rights can provide the victim with a system of suppression and prevention with national coercive force, thus avoiding further harm to the victim.

On the other hand, the application for an injunction on personality rights is based on the premise that the infringement has been or is about to be carried out. The infringement about to be carried out emphasizes that the corresponding behavior has not yet happened but is very likely to happen. Traditional tort law usually does not pay too much attention to such behavior. However, the injunction for personality rights mainly aims at prevention, which takes the initiative to prevent the occurrence or damage expansion by the court issuing an injunction, thus preventing problems before occurrence and giving more adequate and reliable protection to personality rights. Instead of proving that the perpetrator is at fault and the damage results have been caused, the applicant only needs to prove the behavior being conducted by the respondent or the dangerous state of damage to the personality rights caused by the respondent, and the possibility that the applicant will suffer irreparable losses. Therefore, the specific application of the injunction for personality rights can show flexibility and adaptability in practice to respond quickly in different cases, which is of great benefit to preventing the concealment of cyber violence infringement and the diversity of infringement means. It also urges judicial departments to lay more emphasis on the immediate protection and psychological rehabilitation of victims when handling cyber violence, so as to avoid irreversible harm and promote the protection of personality rights under the existing legal order and the interaction of specific laws and regulations.

To sum up, by clarifying the independent procedures and substantive rules of the injunction for personality rights infringement, and reasonably setting the injunction period and procedural connection, the injunction for personality rights infringement can be effectively embedded in the cyber violence infringement, thus better protecting the legitimate rights and interests of victims.

4. Rule Construction for the Application of Injunction System for Personality Rights in Cyber Violence

To protect victims more comprehensively and reasonably, it is urgent to improve and clarify the injunction system of personality rights in cyber violence governance. The refinement of such a system covers the applicable conditions, detailed rules and the difference from the safe harbor privacy principle, so as to ensure that there are laws and rules to follow in the implementation, thus effectively reducing disputes and uncertainties. Meanwhile, special attention should be paid to the development of technical coordination and platform connection for applying the injunction for personality rights in cyber violence. The application of the injunction for personality rights should be developed and standardized through new technologies to effectively protect the legitimate rights and interests of victims.

(1) Conditions of Applying Injunction System for Personality Rights in Cyber Violence

By dismantling and sorting out the relevant provisions in the Civil Code, the conditions of applying injunction for personality rights can be refined as follows. The applicant is qualified with a clear respondent and specific requests. Corresponding evidence should be provided to prove that damage is or is about to occur, and failure to take measures will lead to irreparable damage. The court accepting the application shall have jurisdiction according to law. These conditions prove that the application for an injunction for personality rights is indeed based on actual and urgent needs, rather than an abuse of rights. In view of the concealment of cyber violence and the innovative and diversified means of digital violence, it is necessary to give all-round consideration to the technical types, transmission characteristics and damage consequences of cyber violence when pursuing accountability, so as to ensure the accurate crackdown on cyber violence crimes.

In the operation process, how to determine that the damage is or is about to occur, and failure to take measures will lead to irreparable damage? The application of the injunction for personality rights requires that the infringement is going on, and the behavior of the perpetrator has an apparent appearance of infringement. Cyber violence is manifested in the fact that the perpetrator spreads remarks that damage the victim's personality rights on the online platform. Once the victim is found, he can apply to the court with jurisdiction for an injunction of personality rights and ask the perpetrator to delete relevant information to prevent the further expansion of the infringement influence.

It should be noted that the injunction for personality rights is different from the cessation of damage. As the way of the perpetrator's responsibility, the cessation of infringement should be taken as a precondition by the relevant judgment of the court. However, the application of the injunction for personality rights is not preconditioned by litigation procedure. It is a relatively independent order that can be obtained without completing the litigation judgment procedure. Its purpose is to stop the infringement of personality rights in time, provide efficient relief for victims, and avoid irreparable damage to the subject of personality rights. Its application scope includes the infringement of others' rights to life, health and body, as well as the infringement of others' personality rights, etc. The targeting perpetrators are not limited to family members, let alone natural persons, including any subject that infringes on personality rights, such as legal persons or unincorporated organizations. In addition, when applying the injunction for personality rights, the court does not need to consider the applicant's success rate when examining the application, nor should the application of the notification rule be regarded as a standard. In ordinary civil procedure, because rapidity gives way to fairness, if the personality right injunction advocated by the applicant passes the defense of the respondent, once the personality right infringement occurs in the domain of cyber violence, it may be infinitely expanded, resulting in immeasurable consequences. The prohibition on infringement of personality rights no longer adopts the prudent and formal trial method of ordinary civil litigation, but is replaced by simple and rapid trial and judgment to realize temporary relief.

(2) Differential Application of Injunction for Personality Rights and Safe Harbor Privacy Principle

Because both the injunction of personality rights and the safe harbor privacy principle can play protect personality rights and interests, some scholars advocate that there is no need to introduce the injunction system of personality rights, but only rely on the safe harbor privacy principle. However, the two different mechanisms in the Civil Code used to quickly stop the infringement of online personality rights are two important legal concepts. There are obvious differences in their application, which enables the injunction for personality rights to give full play to its unique advantages.

First of all, the application scope of the injunction for personality rights mainly solves disputes in which the safe harbor mechanism is difficult to function, including difficult disputes and repeated infringement disputes involving multiple platforms. In legislation, it should be clear that difficult disputes should be handled by the injunction mechanism of personality rights. In addition, the injunction procedure for personality rights can be divided into "blocking" and "stopping infringement", so as to improve the efficiency of network service providers' assistance in enforcement.

Secondly, the difficulty of building the injunction mechanism of personality rights is much higher than that of the safe harbor mechanism, which has a lower threshold, making it easier for the right

holder to file an application and play a role faster. However, as a compliance exemption mechanism mainly applicable to cyberspace, the safe harbor privacy principle has a limited scope of action. It is slightly weak in the face of repeated cyber violence by infringers. Meanwhile, it is challenging to resolve the victims' risk of cyber violence from the root cause.

Finally, in terms of institutional functions, the safe harbor privacy principle is mainly to encourage network platforms to provide services, promote the free dissemination of information under the premise of complying with the law, and focus on the liability limitation of network service providers. The injunction for personality rights focuses more on the immediate protection of victims. According to some scholars and the actual solution paths, the safe harbor rule mainly deals with all kinds of online infringement cases, while the injunction for personality rights is mainly responsible for solving difficult disputes and repeated infringement disputes involving multiple platforms.

To sum up, the injunction for personality rights and the safe harbor rule has their own advantages and disadvantages in application. Victims of cyber violence can make a choice based on their circumstances. Courts should also flexibly use these two mechanisms when dealing with related cases to effectively protect personality rights from cyber violence.

(3) Technical Collaboration and Platform Connection for the Application of Injunction for Personality Rights in Cyber Violence

There is still a prominent problem in controlling cyber violence and safeguarding the personality rights and interests of victims. In other words, the cost of obtaining evidence and safeguarding rights for the parties is high and difficult. The evidence collection of cyber violent infringement mainly involves online electronic evidence, including screenshots, links, videos and other evidence materials. These evidences are easy to tamper with and lose. It is also difficult for victims to collect and fix them by virtue of their abilities. Often, they can only choose notarization and evidence preservation to obtain evidence. However, these two methods require much time and high costs. The procedures are also quite cumbersome, which undoubtedly increases the difficulty of application.

To meet this challenge, China's judicial system has taken the initiative to explore the use of "blockchain technology" for electronic data storage in recent years. Through this technology, the victim can grab the infringing web page in real time and store it as electronic data spontaneously or with the help of a third-party certificate storage platform. Then, the victim can perform an encryption operation to generate a unique hash value, which is uploaded to the court-led blockchain certificate storage platform. Once a network infringement dispute occurs, the victim can submit these electronic evidence to the court for verification. The court will use the blockchain certificate storage platform to compare the hash values of these electronic data. If the comparison results are consistent, these data have not been tampered with since they were uploaded to the blockchain. This process simplifies the evidence collection procedure and reduces the cost of evidence collection, providing victims with a more convenient and economical way to defend their rights.

From the perspective of platform responsibility, the platform should clarify its security obligations in cyber violence governance. By strengthening the management of comment links, we can prevent and manage topics that may involve cyber violence in advance, efficiently screen and clean up illegal and illegal comments, and strictly control the spread of unfriendly comments. In addition, the platform should strengthen the publicity and education of typical cases of cyber violence, publish the judgment results and expose the words, deeds and motives of the perpetrators, so as to form public condemnation of cyber violence.

At the national level, introducing the data power of the network platform and strengthening its security management obligations is helpful to realize the collaborative governance of cyber violence. Relevant laws and regulations have clarified the key position and important role of network platforms in cyber violence governance, and stipulated specific security management obligations. If the network platform fails to fulfill these obligations, it will face civil liability, administrative punishment and even criminal liability. Therefore, the network platform should fully realize the importance of its responsibility and earnestly fulfill its security management obligations to maintain the health and harmony of the network environment.

5. Conclusion

The rapid development of digital technology and Internet industry triggered the transformation of traditional verbal violence into cyber violence, a new form of violence, which poses a great challenge to the existing network governance system. In the face of endless and increasingly fierce cyber violence, all the existing cyber violence governance paths have significant shortcomings. However, the injunction system for personality rights can provide a protection mechanism for cyber violence governance, which intertwines prevention in advance with timely stopping of infringement, and makes up for the shortcomings of the traditional governance model with post-event relief as its essence. It is obviously legitimate and necessary to embed injunction for personality rights into cyber violence governance. To ensure the accuracy and scientificity of applying the injunction for personality rights, it is necessary to clarify the conditions of applying injunction for personality rights in the cyber violence governance, and make normative measures on its applicable procedures, so as to avoid unclear application and norms in the regulation of cyber violence. In addition, the injunction for personality rights is different from the traditional remedies, which can provide timely protection to victims and avoid the fermentation of cyber violence, stop perpetrators through preliminary evidence examination and provide measures with national coercive force to further protect victims' rights and create a clear cyberspace.

References

- [1] Liu, Y. H. (2022). Strengthen research on the realization of cyber violence governance and creation of a positive and healthy cyber ecology. *Legal Daily*, (5).
- [2] Tian, S. B. & Liu, J. (2020). Identification and regulation of cyber violence from perspective of social governance. *Journal of South Central Minzu University (Humanities and Social Science Edition)*, 40(03), 168-173.
- [3] Wang, J. G. (2024). Cyber remedies for cyber violence infringement: Dilemmas and paths. *Journal of Henan Polytechnic University (Social Science Edition)*, 25(01), 7-13.
- [4] Shi, J. Y. (2023). Responsibility of the platform in the cyberviolence governance. *Legal Science (Journal of Northwest University of Political Science and Law)*, 41(06), 14-23.
- [5] Cai, W. Z. (2011). *Network communication revolution: Power and regulation*. Shanghai: Shanghai People's Publishing House, 20-21.
- [6] Li, H. J. et al. (2017). Research on the development network violence: Intension and type, status characteristics and governance measures—An analysis based on the cases of network violence during 2012-2016. *Journal of Intelligence*, 36(09), 139-145.
- [7] Jing, L. J. & Hu, J. (2021). The perfect path of legal regulation of cyber violence. *Journal of People's Public Security University of China (Social Science Edition)*, 37(05), 142-149.
- [8] Shi, J. H. & Huang, Y. R. (2020). An analysis of the dilemma of criminal regulations on cyber violence and its solutions. *Journal of Anhui University (Philosophy and Social Science Edition)*, 44(04): 78-89.
- [9] Wu, D. Z. (2024). Cyber violence and moral constitutionalism: An analysis based on system theory. *Politic Science and Law*, (05), 63-80.
- [10] Yin, J. G. (2015). On the government management mechanism of Internet information. *China Legal Science*, (01), 134-151.
- [11] Jiang, W. & Xiao, J. G. (2018). *Civil procedure law*. Beijing: China Renmin University Press, 56-66.
- [12] Liu, X. Z. & Zhao, B. B. (2022). Prohibition of personality right infringement: Legislative background, orientation and procedure construction. *Social Sciences in Guangxi*, (03), 105-112.
- [13] Wu, Y. Z. (2021). Study on the procedure of personality rights and injunction. *Legal Science (Journal of Northwest University of Political Science and Law)*, 39(02), 133-144.
- [14] Zhu, X. F. (2022). On the normative application of the injunction for the protection of personality right in the Civil Code. *Journal of China University of Political Science and Law*, (03), 145-157.

- [15] Liu, Y. H. (2022). Idea, logic and path: A study on the rule of law governance of cyber violence. *Jiang-Huai Tribune*, (06), 21-30+2.
- [16] Wang, L. M. (2019). On preliminary injunction for infringing on personality rights. *Law and Economy*, (04), 3-15.
- [17] Cheng, X. (2021). On the injunction in personality rights protection in Civil Code of China. *Journal of Comparative Law*, (03), 138-151.
- [18] Dai, S. C. (2023). Litigation commentary on Article 997 of the Civil Code (Injunctive relief for personality rights infringement). *Social Science in Yunnan*, (01), 131-143.
- [19] Xie, D. K. (2023). The public and private collaborative governance model of cyber violent crime. *Legal Science (Journal of Northwest University of Political Science and Law)*, 41(05), 92-101.
- [20] Zheng, Y. M. & Chen, D. S. (2022). On the application of the injunction for the protection of personality rights in using information network to infringe personal rights and interests. *Journal of University of South China (Social Science Edition)*, 23(03), 97-105.