Research on Whole-chain Criminal Law Regulation of Doxxing-Style Cyber Violence

Ruojin Li
Faculty of Law, Macau University of Science and Technology, Macao, China

Abstract: As a new form of cyber violence, doxxing-style cyber violence forms a complete black industrial chain by illegally obtaining and disclosing citizens' personal information and triggering secondary infringements, which seriously infringes on citizens' right to personal information and personality rights, and disrupts the order of cyberspace. Combined with relevant cases, criminal law provisions and judicial interpretations, after sorting out its whole-chain characteristics, it is found that the current criminal law regulation faces dilemmas such as obstacles to the application of miscellaneous provisions, vague responsibilities of multiple subjects, and lack of prevention and control mechanisms. Based on the principle of criminal law modesty and the principle of legality of crimes and punishments, we should optimize the application of charges, clarify the boundaries of responsibilities, and improve the prevention and control mechanisms to build a whole-chain criminal law regulation system, realize precise regulation and source prevention and control, balance the protection of citizens' rights and interests, cyberspace governance and the punishment function of criminal law, and create a healthy cyber ecology.

Keywords: Doxxing-style Cyber Violence; Criminal Law Regulation; Crime of Infringing on Citizens' Personal Information; Internet Service Providers

1. Research Background and Problem Statement

With the in-depth development of the digital economy, cyberspace has become an important field of social life, but the accompanying problem of cyber violence has become increasingly prominent. In 2024, public security organs across the country handled more than 8,600 cyber violence cases involving "doxxing", took criminal compulsory measures against more than 2,500 people in accordance with the law, and imposed administrative penalties on more than 8,500 people. Doxxing-style cyber violence (commonly known as "doxxing and targeting individuals online"), as a highly harmful new form among them, obtains others' personal information through illegal means and discloses it online, triggering a series of infringements such as online insults, offline harassment, and personal coercion, which causes devastating damage to the victim's personal dignity and peaceful life, and at the same time seriously disrupts cyber order and breeds cyber black and gray industries.

In recent years, public figures such as celebrities, anchors, and internet celebrities have become high-frequency victim groups of doxxing-style cyber violence. After public figures appear in live broadcasts or in the public eye, sensitive personal information such as personal ID numbers, home addresses, and phone numbers are illegally obtained and disclosed, and then they suffer from continuous phone harassment, SMS insults, and even some people come to their door to besiege and coerce them, leading to severe depression and termination of their careers, as well as chaos in social public order. Such cases expose the weak links in the current cyberspace governance and also pose severe challenges to criminal legal regulation.

Case Overview: From July 2023 to March 2024, six perpetrators including Zhou created and operated three communication channels specifically for implementing "online doxxing" on overseas social software. The perpetrators obtained citizens' personal information in batches through information exchange, illegal purchase, and retrieval with the help of "social engineering database" robots, and released more than 1,200 pieces of personal information involving unspecified subjects such as celebrities, online anchors, and parties to hot events in the relevant channels, with the cumulative views of relevant information

exceeding 4 million times. The six perpetrators increased the popularity of the channels by placing advertisements in the channels and recommending each other, attracting others to pay for querying and purchasing citizens' personal information, so as to realize illegal profits.

At the same time, when releasing the personal information involved in the case, the perpetrators attached insulting evaluation content, and organized and incited followers in the channels to carry out phone harassment, SMS insults and other acts against the doxxed targets, which seriously infringed on the personal information rights and interests of the unspecified majority and also caused substantial damage to social public interests. On April 30, 2025, the court sentenced Zhou to three years in prison, suspended for four years, and fined 4,000 yuan for the crime of infringing on citizens' personal information.

The current criminal law stipulates charges such as the crime of infringing on citizens' personal information, the crime of insult, the crime of defamation, and the crime of refusing to fulfill information network security management obligations for acts related to cyber violence. However, the whole-chain characteristics of doxxing-style cyber violence make it difficult for a single charge to fully evaluate its legal interest infringement. It can be seen from this case that only the principal offenders represented by the initial infringer Zhou bear criminal responsibility, while netizens participating in secondary infringements and internet service providers are often not convicted due to vague responsibility identification in practice, and even do not bear corresponding civil liabilities. Therefore, how to construct a comprehensive and precise criminal law regulation system based on the behavioral chain characteristics of doxxing-style cyber violence, and realize effective crackdown on infringements in all links, has become an important topic urgently to be solved in current criminal law research and judicial practice.

2. Whole-chain Interpretation of Doxxing-Style Cyber Violence — Taking the "Online Doxxing" Case of Zhou et al. as an Example

Doxxing-style cyber violence refers to a general term for a series of illegal acts in which actors, for improper purposes such as revenge and venting anger, malicious banter or illegal profit-making, illegally obtain a complete chain of natural persons' personal information through Trojan programs, phishing links, social engineering database queries and other means, and publicly disclose and disseminate it to the unspecified majority or specific groups, resulting in the infringement of personality rights and interests such as the right to privacy and reputation of the information subject, or triggering derivative risks such as personal safety and property safety. Its core feature lies in the relevance and chain reaction between the "doxxing" act and subsequent infringements, forming an infringement chain of "initial infringement – secondary infringement".

"Doxxing" forms a complete black industrial chain, which can be divided into three stages: upstream information acquisition, midstream information diffusion, and downstream secondary infringement [1]. The upstream is the basic link of the industrial chain, whose core is to illegally obtain and store massive citizens' personal information to provide data support for subsequent crimes. The subjects of the acts are mostly independent hackers or criminal gangs with network attack technology, who secretly commit crimes with the help of dark networks and encrypted communication tools. Subsequently, the original data is cleaned, associated, collided and deeply mined to form high-value intelligence products. Actors build and operate illegal "social engineering database" platforms, use credential stuffing attacks to achieve cross-platform data matching and improve information integrity; with the help of AI correlation analysis, portrait construction and other technologies, integrate multi-source fragmented information to generate complete personal digital files including identity, behavior, social interaction and other content, providing precise intelligence support for downstream crimes.

The midstream is the link where harm occurs. After obtaining citizens' complete information through illegal query platforms, actors publicly disseminate and diffuse information on public social platforms and targeted communities, inciting public opinion and implementing cyber violence. The downstream is the link where harm is realized. The midstream acts directly lead to the leakage of citizens' privacy and the derogation of reputation, and trigger group cyber siege, which is the final outbreak link of

the realistic harm of "doxxing" acts [2].

In this case, in the information acquisition link, Zhou obtained the victim's sensitive personal information such as ID number, home address, phone number, bank account information, and itinerary information through various means such as hacking the victim's social account and purchasing from the cyber black and gray industry. The core of the act in this link is "illegal acquisition", and the scope of information covers various types such as identity information, property information, and whereabouts information, most of which are sensitive personal information with stronger infringement.

In the information diffusion stage, Zhou disseminated the victim's personal information to multiple social platforms and live broadcast barrage areas, and set up special chat groups for information dissemination, triggering a large number of netizens to browse and forward, resulting in the victim's personal information changing from a private state to a publicly accessible state, creating conditions for subsequent secondary infringements, and the scope of infringement also extending from specific individuals to cyber public space.

In the secondary infringement stage, the doxxing acts involved in the case directly triggered continuous online infringements against the victim such as phone harassment, SMS insults and malicious reporting and banning of social accounts; offline, there were also real harassment acts such as door-to-door siege, tracking and coercion, which seriously affected the victim's normal life and work. The infringement patterns in this stage present diversified characteristics, including various types of acts such as insult, defamation, harassment, and coercion, and online infringements and offline harassment are intertwined and continuously amplified, eventually forming superimposed serious harmful consequences.

3. Current Situation and Dilemma of Whole-chain Criminal Law Regulation of Doxxing-Style Cyber Violence

At present, China's criminal law regulation of doxxing-style cyber violence mainly relies on relevant charges in the Specific Provisions of the Criminal Law, combined with judicial interpretations such as 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 such as Defamation Committed by Using Information Networks, the Guiding Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Punishing Cyber Violence Illegal Crimes in accordance with the Law, and 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 Infringing on Citizens' Personal Information, forming a preliminary regulation system.

3.1 Obstacles to the Application of Miscellaneous Provisions

The core obstacle to the judicial application of miscellaneous provisions lies in the unclear normative connotation and application boundary, which makes it difficult to achieve precise adjudication, and judicial personnel usually hold a cautious position and are unwilling to apply them easily. The first "doxxing" case among the typical cyber violence cases released by the Ministry of Public Security in 2024 directly reflects this dilemma.

In this case, Zhao, Cheng and others used hacking methods to illegally obtain citizens' personal information, disclosed the private information of more than 800 members of a virtual idol group and their fans online, and insulted and abused the victims, causing adverse social impact, and were taken criminal compulsory measures by the public security organ in accordance with the law. However, in the trial session, the court did not convict them of the crime of infringing on citizens' personal information, but sentenced them to the crime of illegally using information networks. The reasons for the judgment show that Zhao and Cheng, together with overseas personnel, set up communication groups for illegal and criminal activities and released relevant illegal information, with more than 30,000 group accounts, which is a serious circumstance and has met the constitutive elements of the crime of illegally using information networks.

From the facts of the case, there is nothing wrong with the court's determination of the crime of illegally using information networks, but what is worth discussing is that the core criminal acts of the two defendants are illegally obtaining and publicly exposing citizens'

personal information. Why were they not convicted of the crime of infringing on citizens' personal information at the same time? The core reason is that this case does not meet the conviction standards stipulated in Items 1 to 9 of Paragraph 1 of Article 5 of 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 Infringing on Citizens' Personal Information (hereinafter referred to as the Interpretation): According to media reports, although there are as many as 3,000 victims of doxxing in this case, according to the provisions of Item 5 of Paragraph 1 of Article 5 of the Interpretation, citizens' personal information other than those specified in Items 3 and 4 that are illegally obtained, sold or provided needs to reach more than 5,000 pieces to be deemed as "serious circumstances", and Item 6 of Paragraph 1 of Article 5 of the Interpretation clearly stipulates that if the quantity does not meet the standards of the preceding item, it shall be calculated in proportion to meet the standards accordingly. This case obviously does not meet the above requirements.

Although the relevant provisions of the Interpretation can be applied in Zhou's case, in the case of Zhao and Cheng, the judicial organ did not apply the miscellaneous provision of Item 10 of Paragraph 1 of Article 5 of the Interpretation to determine the crime of infringing on citizens' personal information, which is not due to lack of judicial courage. In the absence of clear and specific legal guidance, the ambiguity of miscellaneous provisions makes judicial staff need to make prudent judgments combined with specific circumstances in case handling, and their hesitation in application is reasonable. It is obviously beyond reasonable expectations to require judicial organs to generally apply miscellaneous provisions with substantive legislative attributes to handle most doxxing cases under the premise of bearing corresponding judicial risks. This status quo is also reflected in the rights protection dilemma of doxxing victims. If miscellaneous provisions can be easily applied, the difficulty of rights protection for doxxed people will be significantly reduced, and their helpless state will be effectively improved, which confirms the practical obstacles to the application of miscellaneous provisions from the side.

3.2 Vague Division of Responsibilities of Multiple Subjects

As for the initial infringer, as the initiator and core promoter of the doxxing act, he not only implements the basic acts of illegally obtaining and publicly disclosing citizens' personal information, but also often abets and induces other netizens to participate in secondary infringements through inflammatory remarks and guiding expressions, which directly promotes the expansion of harmful consequences. However, according to the joint crime theory of criminal law, to determine that the initial infringer is responsible for the consequences of secondary infringement, it is necessary to simultaneously prove that he subjectively has the intent of knowing or laissez-faire about the secondary infringement, and objectively there is a causal relationship in criminal law between his act and the consequences of secondary infringement.

In practice, the abetting and inducing acts of initial infringers are mostly concealed and indirect, and the netizens participating in secondary infringements are autonomous, so it is difficult to accurately define the scope of subjective knowledge of initial infringers and the causal force, resulting in it being difficult to fully determine their criminal responsibility for the consequences of secondary infringements, and they can often only be held accountable for their own acts of information acquisition and diffusion, weakening the evaluation of their core leading role.

For ordinary netizens participating in secondary infringements, the dilemma of responsibility identification is more prominent. Such subjects are numerous and highly anonymous, and most of them participate in cyber violence by forwarding, commenting, insulting and other ways. The act of a single subject seems to be less harmful, and it is difficult to individually meet the "serious circumstances" standard of criminal crimes. At the same time, people relatively despise invisible violence and invisible harm (mainly mental harm) represented by cyber violence. Therefore, when applying traditional theories to judge the causal relationship between serious consequences such as suicide and cyber violence acts, it is easy to draw a negative conclusion [3]. In the "avalanche" infringement scenario formed by group cyber violence, the identification of

responsible subjects falls into a dilemma, which is essentially a structural impact and normative dissolution of the traditional criminal law's principle of individual responsibility by the collective behavior mode in the digital age [4]. Modern criminal law takes individual responsibility as the core basis of imputation, and the investigation of criminal responsibility takes the causal relationship in criminal law between the actor's act and the result of legal interest infringement as a necessary prerequisite. However, the harmful consequences of cyber violence are usually formed by the superposition and aggregation of a large number of individual acts without intent connection. It is neither possible to determine the intent of joint crime nor apply the traditional principle of "partial perpetration, full responsibility" for joint crime imputation, which ultimately makes it difficult to accurately define the scope and size of responsibility of each participating subject, and the accountability system is difficult to operate effectively [5].

In practice, the participation of most ordinary netizens is spontaneous and scattered, lacking clear intent connection, so it is difficult to prove that they have common criminal intent; at the same time, due to the excessive number of participants, it is difficult to trace their identities one by one and distinguish the role of each subject's act, resulting in either no accountability for all participants or inappropriate scope of accountability, making it difficult to achieve the compatibility of crime, responsibility and punishment.

The core controversy over the criminal responsibility identification of internet service providers focuses on the boundary of information network security management obligations and the judicial identification standard of "knowing". According to the criminal law and relevant judicial interpretations, internet service providers have security management obligations such as blocking the spread of cyber violence information, deleting infringing content, and retaining case-related data. Those who neglect to perform such obligations and the circumstances are serious may constitute the crime of refusing to fulfill information network security management obligations; if they form a joint criminal intent with the initial infringer, they may establish a joint crime.

However, in judicial practice, the security management obligations of internet service providers lack clear definition, and it is difficult to determine the reasonable limit of their review and deletion obligations for "doxxing" infringing information. At the same time, the identification standard of "knowing" is relatively vague, and it is difficult for judicial organs to prove that the platform has exact cognition of infringing information, nor can it prove that the platform has intent connection with the initial infringer, which leads to the dilemma of determining the platform's criminal responsibility.

Taking Zhou's case as an example, after receiving the victim's report, the involved social platform did not delete the publicly disclosed personal information and insulting remarks in time, which objectively allowed the harmful consequences to expand. However, due to the lack of clear judgment standards, it is impossible to determine that its inaction has reached the level of "serious circumstances", nor can it prove that it has criminal intent. In the end, the platform was not held criminally responsible, which fully highlights the practical problem of identifying the responsibility of internet service providers.

More prominently, some platforms themselves may provide assistance for cyber violence by infringing on citizens' personal information, and search engines are typical. On the one hand, search engines infringe on citizens’ personal information rights and interests and the public’s right to information choice through traffic control, bidding ranking, information screening and content control, giving birth to the logic of "surveillance capitalism" in cyberspace; on the other hand, their improper handling and abuse of personal information cause governance problems such as information fairness, accessibility and accountability, and form destructive innovation formats in the name of "technological innovation", further exacerbating the institutional dilemma of personal information protection and cyber violence governance [6].

3.3 Lack of Ex-ante Prevention and In-process Intervention

China's current criminal law regulation system for doxxing-style cyber violence has a significant structural imbalance, which generally presents a governance pattern of emphasizing post-punishment, insufficient ex-ante prevention,

and weak in-process intervention. It is difficult to effectively block and control the complete infringement chain of "illegal information acquisition – information public diffusion – secondary infringement occurrence", nor can it curb the breeding and spread of such acts from the source.

On the one hand, in the source link of information acquisition, the intervention of criminal law has significant lag. The current focus of criminal regulation mostly focuses on the acts of illegally obtaining and providing citizens' personal information that have caused actual harmful consequences, while there is a lack of normalized monitoring, early identification and front-end regulation mechanisms for prepositive and preparatory acts such as batch crawling of citizens' personal information in the cyber black and gray industry, illegal query of sensitive information using technical interfaces, and layer-by-layer resale of information through underground channels. It is difficult to form a penetrating and whole-process crackdown on the cyber black and gray industry, resulting in a large amount of sensitive personal information continuously circulating in the illegal industrial chain, providing convenient conditions for the high-frequency occurrence of "doxxing" acts. Judicial organs often can only start prosecution procedures after the information is disclosed and the infringement consequences appear, making it difficult to achieve source prevention and control.

On the other hand, in the transmission link of information diffusion, the in-process intervention obligations of internet service providers have not been effectively compacted. In practice, most network platforms adopt the mode of passively accepting victim complaints and reports for information content with clear cyber violence orientation and high risk such as "doxxing", "targeting individuals online" and "human flesh search", and their capabilities of active monitoring, rapid identification and timely disposal are seriously insufficient. Even if relevant infringing information is found, due to imperfect review mechanisms, cumbersome disposal procedures and low response efficiency, the information spreads rapidly and fissionably in multiple scenarios such as social platforms, chat groups, and live broadcast barrages. When the platform takes disposal measures such as deletion, shielding, and disconnection of links, personal information has been leaked on a large scale, and the harmful consequences have initially formed and are difficult to reverse.

More prominently, the ex-ante early warning and immediate protection mechanisms for secondary infringements are seriously lacking. After citizens' personal information is illegally disclosed, a cross-platform and cross-departmental linkage mechanism of rapid early warning, emergency disposal and personal protection has not been established for the possible real personal safety risks of victims such as online phone bombing, SMS insults, malicious intimidation, as well as offline tracking, siege, harassment, and coercion. Judicial organs, network platforms and relevant functional departments are difficult to form a joint force for prevention and control, and cannot effectively block risk transmission before the escalation of infringement acts, resulting in the continuous extension of online cyber violence to real space, further highlighting the prominent shortcomings of whole-chain criminal law regulation in ex-ante prevention and in-process intervention.

4. Improvement Paths of Whole-Chain Criminal Law Regulation of Doxxing-style Cyber Violence

4.1 Optimize the Charge Application System to Realize Whole-Chain Precise Punishment

For cyber violence cases with serious circumstances, we should abide by the basic principle of legality of crimes and punishments, and complete the conviction evaluation based on the criminal law interpretation theory. The author believes that under China's existing criminal law normative system, the necessity of independently adding new crimes for doxxing cyber violence is not sufficient, and the application system can be optimized through the following two aspects [7].

First, adhere to the principle of unity of subjectivity and objectivity to comprehensively evaluate the degree of social harm of the act [8]. The principle of unity of subjectivity and objectivity requires that judicial determination must take into account subjective culpability and objective harm, abandon the one-sided judicial thinking of purely subjective imputation or objective imputation, and ensure the neutrality and fairness of criminal responsibility evaluation.

At the subjective level, it is necessary to examine the motives and purposes of the actors in committing cyber violence: either venting dissatisfaction due to personal grudges, or deliberately harming others out of jealousy, or intending to mentally control the victim, or deliberately creating topics to gain traffic and hype for profit, or simply following the trend to vent emotions. The more obvious the subjective malignancy and infringement intent, the higher the condemnability and harmfulness of the act.

At the objective level, the actual harmful consequences caused by the act should be comprehensively considered, including the number of clicks, views and dissemination coverage of illegal information, whether the victim and his close relatives have serious consequences such as mental disorders, self-harm, suicide, and whether group public opinion incidents or public order chaos are triggered. The more serious the objective harm caused by the act, the higher the degree of social harm.

Second, fully take into account the particularity of the online discourse environment, and avoid mechanically applying literal interpretation to improperly compress the application boundary of charges. Insult acts in the sense of criminal law usually manifest as aggressive expressions with obvious derogation, ridicule and defamation attributes. However, semantic connotation is not static, and it constantly derives new meanings with the changes of context.

The cyber field has diverse cultures and special contexts. Some words are neutral or even commendatory on the surface, without explicit insult, but can form implicit derogation, ridicule and personal attack effects relying on specific contexts, which have substantial insult attributes. For example, in the "Zhou et al. online doxxing infringement case", some netizens commented on the victim's words and deeds in the form of questions, statements and ironies, and there were no vulgar swear words and explicit attack language in the relevant expressions. However, combined with the background of the tragic incident and the spread effect of online groups, the continuous superposition and fermentation of such metaphorical and suggestive expressions formed strong psychological pressure and mental infringement on the victim who was in grief, and finally induced the serious consequence of the victim's suicide. It can be seen that the determination of the crime of insult should not be limited to the intensity of the surface attack of language, but must comprehensively judge the substantial derogation value behind the expression combined with the specific online context [9].

4.2 Clarify the Responsibility Boundaries of Multiple Subjects to Realize Whole-Chain Collaborative Accountability

As the initiator and core actor of doxxing-style cyber violence, the initial infringer runs through key links such as illegal acquisition of information, batch disclosure, and incitement of dissemination, and plays a decisive role in the formation, diffusion of the infringement chain and the expansion of harmful consequences, and shall be given a heavier punishment in accordance with the law.

For actors who organize and plan "doxxing" acts, lead the theft and public dissemination of personal information, and abet and induce others to commit secondary infringements, even if they do not directly participate in specific acts such as insults and harassment, they shall be identified as the principal offender in accordance with the joint crime principle and bear criminal responsibility for the harmful consequences of the whole chain. Especially for actors who implement "doxxing" relying on the cyber black and gray industry for the purpose of illegal profit-making, their acts seriously infringe on citizens' personal information rights and interests and disrupt the management order of cyberspace. Judicial organs should increase the intensity of punishment, strengthen the application of property penalties such as fines, resolutely cut off the black industrial chain of illegal acquisition, trading and dissemination of citizens' personal information, and curb the criminal drive of profiting from "doxxing" from the source.

For ordinary netizens participating in secondary infringements, we should adhere to the principle of compatibility of crime, responsibility and punishment and stratified imputation, to avoid "the law does not punish the multitude" or excessive accountability. For those who actively commit acts such as insults, defamation, intimidation, malicious reporting, and offline harassment, with wide dissemination scope and serious harmful consequences, which have reached the criminal conviction standard, shall be identified as accomplices in joint crimes and

given lighter, mitigated or exempted punishment in accordance with the law. For those who only follow the trend to comment, participate slightly and do not cause serious consequences, criminal responsibility may not be investigated, and instead they shall be regulated by administrative penalties, platform disciplinary measures, social credit constraints and other ways, to realize a reasonable distinction between criminal punishment and social governance.

The compacting of the responsibility of internet service providers is an important fulcrum of whole-chain regulation. At the legislative and judicial levels, the information network security management obligations should be further refined, and the specific standards and performance requirements of platforms in content review, risk early warning, rapid disposal, evidence retention and other aspects should be clarified. If the platform fails to take necessary measures such as deletion, shielding, current limiting, and disconnection of links in time after discovering or receiving reports of "doxxing" infringing information, resulting in large-scale dissemination of illegal information and continuous expansion of harm, it shall be held criminally responsible for the crime of refusing to fulfill information network security management obligations in accordance with the law.

At the same time, the protection of victims' rights should be strengthened, and the public security organ's assistance in evidence collection mechanism should be improved. For cases where the victim has difficulty in producing evidence, the public security organ shall carry out work such as identity verification, electronic data fixation, and behavior trace tracing in a timely manner to provide support for accountability. In addition, clarify the legal obligation of internet service providers to cooperate in evidence collection, require them to provide account information, dissemination data, background logs and other evidence in a timely manner during case handling, and provide technical support and assistance, to build an efficient and smooth evidence supply system and provide solid procedural guarantee for the whole-chain criminal law regulation of doxxing-style cyber violence.

4.3 Improve Ex-Ante Prevention and In-process Intervention Mechanisms to Realize the Closed Loop of Whole-Chain Regulation

The core value of criminal law regulation lies not only in post-accountability, but also in ex-ante prevention and in-process loss stopping. Combined with the whole-chain characteristics of doxxing-style cyber violence, it is necessary to take "source prevention and control, process blocking, and tilted protection for victims" as the core, improve ex-ante prevention and in-process intervention mechanisms, realize front-end regulation of cyber violence acts, and reduce the expansion of harmful consequences. This is not only the embodiment of the principle of criminal law modesty, but also an important path to connect criminal regulation with civil and administrative protection. However, whether in the stages of ex-ante prevention, in-process control or post-accountability, network platforms are required to implement standardized management and compliant disposal of evidence collection work [10].

At the level of ex-ante prevention, the core is to strengthen the information network security management obligations of internet service providers and promote them to establish a special early warning and prevention mechanism for doxxing-style cyber violence. According to the Cybersecurity Law, the Personal Information Protection Law and relevant provisions of the criminal law, internet service providers, as managers of cyberspace, have the statutory responsibility to prevent cyber crimes and protect citizens' personal information and personality rights and interests, and their ex-ante early warning obligation is the core extension of this responsibility.

Specifically, in the face of the "online doxxing" acts that have occurred, network platforms should cooperate with relevant departments to fix evidence, and perform the obligation of evidence collection and fixation in a timely manner based on their own technical advantages [11]. Internet service providers should be promoted to use artificial intelligence, big data and other technical means to build a special monitoring model for doxxing acts, to conduct real-time monitoring, intelligent identification and precise interception of obscure keywords such as "doxxing", "social engineering database", "information query" on the platform, behavior patterns of illegally obtaining personal information, and abnormal trajectories of batch dissemination of private information, so as to block the channels of information theft and

dissemination from the source.

At the same time, the monitoring obligation standards of internet service providers should be clarified, and the early warning thresholds, interception scopes and disposal procedures should be refined, to prevent them from evading obligations on the grounds of "limited technology". For those who fail to perform early warning and prevention obligations resulting in the occurrence of doxxing acts, administrative responsibilities may be investigated in accordance with the law, and those with serious circumstances shall be included in the scope of criminal accountability, to force them to implement the main responsibility.

At the level of in-process intervention, it is necessary to build a comprehensive victim protection mechanism to realize timely loss stopping of infringement acts and rapid relief of victims' rights and interests, and make up for the shortcoming of "emphasizing accountability and neglecting protection" in the existing mechanism.

On the one hand, a rapid reporting channel for doxxing-style cyber violence should be established, and the reporting acceptance standards, verification time limits and feedback mechanisms should be clarified. Internet service providers need to verify, delete and shield the infringing information immediately after receiving the report to prevent further diffusion of information; at the same time, strengthen the protection of the victim's identity information, and strictly prohibit the platform from leaking the victim's reporting information to avoid secondary infringement.

On the other hand, the diversified support system for victims should be improved, which not only provides victims with free psychological assistance and legal consulting services to help them cope with mental damage and rights protection dilemmas, but also gives full play to the ex-ante prevention and in-process loss stopping functions of the personality right infringement injunction. According to the Civil Code and relevant judicial interpretations, for doxxing-style cyber violence acts that are being implemented or about to be implemented, the victim may apply to the people's court for a personality right infringement injunction in accordance with the law, requiring the actor to stop the infringement, delete the infringing information, and prohibit the dissemination of private content. The people's court shall review quickly and make a ruling in a timely manner, to block the infringement act in advance through civil relief means, avoid further expansion of harmful consequences, and realize the effective connection between civil protection and criminal regulation.

5. Conclusion

In the digital age, doxxing-style cyber violence, with the whole-chain characteristics of "illegal acquisition – information diffusion – secondary infringement", seriously infringes on citizens' right to personal information and personality rights, breeds cyber black and gray industries and disrupts cyber public order. The current criminal law regulation faces practical dilemmas such as blocked application of miscellaneous provisions, vague responsibilities of multiple subjects, and lack of front-end prevention and control mechanisms. A single charge evaluation and the governance mode of "emphasizing post-event and neglecting front-end" are difficult to achieve precise regulation.

For the criminal law regulation of doxxing-style cyber violence, we should adhere to the principles of legality of crimes and punishments and criminal law modesty, based on the existing normative system, optimize the application of charges through criminal law interpretation theory, construct a social harm evaluation standard with the unity of subjectivity and objectivity, take into account the particularity of the online discourse environment, clarify the responsibility boundaries of initial infringers, participating netizens, and internet service providers, and realize the compatibility of crime, responsibility and punishment. At the same time, relying on its whole-chain attributes, we should promote the forward shift of governance focus, compact the network platform's obligations of information security management and early warning disposal, and build a multi-collaborative ex-ante prevention and in-process intervention mechanism to form a closed loop of criminal law regulation.

Only by building a deeply integrated whole-chain governance system can we build a legal defense line in cyberspace, balance the relationship between rights and interests protection, industrial development and order maintenance, create a clear and orderly cyber ecology, and contribute to the construction of the rule of law in the digital society.

References

[1] Liu Xianquan. Criminal Law Regulation of Deepfake Behavior in the Era of Artificial Intelligence. Journal of Political Science and Law, 2025, (11): 52.

[2] Li Guangjie, Li Xiaobo. Research on Multidimensional Risks and Governance of Online "Doxxing": A Perspective Based on Actor-Network Theory. Journal of Beijing Police College, 2026, (2): 4-5

[3] Liu Yanhong. The Rule-of-Law Transformation of Cyber Violence Governance and the Construction of Legislative System. Chinese Journal of Law, 2023, 45(5): 84.

[4] Xiao Chenzhang. Reconstruction of Imputation Logic and Norm Iteration in Criminal Governance of Cyber Violence. Journal of East China University of Political Science and Law, 2025, 28(4): 179.

[5] Tian Hongjie. The Dilemma of "the Law Does Not Punish the Multitude" in Criminal Law Governance of Cyber Violence and Its Resolution. Law Science Magazine, 2024, 45(1): 32.

[6] Yang Zhiqiong. Legal Risks of Search Engines Processing Personal Information and Corresponding Countermeasures. Legal Forum, 2023, 38(6): 55.

[7] Wang Huawei. Criminal Law Regulation of Human Flesh Search in the Context of Cyber Violence. Journal of Comparative Law, 2025, (3): 144-145.

[8] Liu Xianquan. New Approaches to Criminal Law Regulation of Crimes in Metaverse Space. Journal of Comparative Law, 2022, (3): 135.

[9] Cai Yongcheng. The Criminal Governance Logic and Path of Cyber Violence. Research on Rule of Law, 2025, (5): 141.

[10] Xie Shu. Towards Three-Dimensional Collaboration: Evidence Supply in Cyber Violence Criminal Cases. Journal of Political Science and Law, 2025, (7): 149-150.

[11] Liu Yanhong. Systematic Governance of "Online Doxxing" in the Digital Age. People's Tribune, 2025, (19): 85-86.

