Cyber violence governance on digital platforms: criminal compliance and public-private co-governance

Longyin Yang

School of Politics and Law,Northeast Normal University, Changchun130000, China.

yanglongyin@nenu.edu.cn

Abstract. Cyber violence is endangering the order of cyberspace with the characteristics of depersonalization and de-accountability, and the governance of digital platforms is facing challenges such as lagging response, lax implementation and conflict of interest. Platforms, as providers of online services, have a natural technological advantage and should be responsible for the governance of public cyberspace. There is an urgent need to establish a detailed criminal compliance plan to reduce the criminal compliance risk due to online violence through the whole process of prevention beforehand, timely disposal during the incident, and reflection after the incident, and a positive incentive function can be expected. In addition, the prudent involvement and appropriate intervention of public power are key elements in the governance of online violence. Under the framework of binary co-regulation, the public and private sectors complement each other and dynamically synergize to make up for the inadequacy of the current legal regulation.

Keywords: online violence, platform liability, criminal compliance, binary co-regulation.

1. Introduction

As a kind of "soft violence", cybercrime presents complex and diverse manifestations under the effect of the rapid development of information technology. Compared with general civil violations, cyber violence, because of its convenience and covert nature, has an ever-expanding group effect, and the harm caused to the victim and even the destruction of network order is significant and difficult to hold accountable.

China issued the *Guiding Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on the Lawful Punishment of Cyber Violence and Illegal Crimes* in September 2023, which defines the specific manifestations of cyber violence, classifying it as cyber defamation, cyber insults, and infringement of citizens' personal information. [1] In terms of the trend of legislative amendments in China, the academic field and practical departments have paid full attention to and discussed the relevant issues: in 2013, the two high courts issued the "*Interpretation of Several Issues Concerning the Application of Laws to the Handling of Criminal Cases of Using Information Networks to Commit Slander and Other Criminal Cases*"; in 2015, the "*Amendments to the Criminal Law (IX)*" added the "crime of infringing on the personal information of citizens" [2]; the *Cybersecurity Law of the People's Republic of China*, which has been officially in force since June 2017, explicitly provides for combating cyber violence [3]; and the National Internet Information Office drafted the *Provisions on the Governance of Information on Cyber Violence (Exposure Draft)* in July 2023, which clarifies the monitoring, warning, and disposal of information on cyber violence and proposes the establishment of a perfect protection function against cyber violence. Although existing legal norms and relevant judicial interpretations have regulated cyber violence to a certain extent, the assumption of responsibility by infringing subjects and digital platforms is still insufficient, and the remedies that should be implemented by the platforms are not yet clear.

In reality, the victim's rights against cyber violence exist in a cumbersome procedure, time-consuming and other problems, the objective status quo of network violence relief is not timely, making a considerable portion of the victims choose to remain silent, undoubtedly cutting the cost of cyber violence offenses. Digital platform as a "third party" to provide network services. It is necessary to assist in identifying the infringement subject and retaining evidence. With the construction of the

rule of law, the function of China's criminal law has gradually shifted from sanctioning crimes after the fact to actively and effectively preventing them. [4] As a result, the punitive function of criminal law should not be taken as the only means of managing network violence, and it is urgent to examine the network platforms that are on the front line of preventing network violence, actively fulfilling their duties of prevention and disposal, and playing the role of safeguarding the rights and interests of users and the ecological order of the information content in cyberspace, to construct a system of internal control of the industry's criminal compliance. It can effectively reduce the government's burden of regulating network enterprises and supplement the inadequacy of the existing legal system in regulation. In turn, it promotes binary co-rule in the regulation of cyber violence crimes and realizes the organic combination of national legal constraints and corporate autonomy.

2. Justification of criminal compliance on digital platforms

The concept of criminal compliance has its origins in the West and centers on the precautionary principle. A compliance program anticipates, detects and deters any potential criminal activity. [5] *Our Compliance Management System Guidelines*, which will come into effect on 12 October 2022, state that "Compliance means that an organization complies with applicable laws, regulations and regulatory requirements, as well as with relevant standard contracts, principles of effective governance, or ethical guidelines". [6] By establishing a compliance mechanism, digital platforms can identify and assess potential criminal risks and take preventive measures accordingly; the lower the risk, the less likely the enterprise is to be sanctioned. When an enterprise is involved in cyber violence, a written corporate compliance plan and the status of its implementation at the practical level will allow the platform to clarify unit and individual responsibilities at each stage of the process, and eliminate the limitations of the double penalty system as much as possible. In the long run, a sound compliance mechanism provides a soft guarantee for the development of platform enterprises. In the course of the industry's management services for handling massive data, updating and iterating technology, and responding to cyber violence, it has gradually adapted to the needs of protecting legal interests in the big data era.

2.1. Reconciling the public and commercial attributes of digital platforms

The take-off of the digital economy has strengthened the attributes of digital platforms as tools for the dissemination and exchange of information, and their participation in maintaining the order of the online environment through the provision of public services, content auditing, community regulation and other means is in fact "public power" in a specific space. In cases involving cyber violence, the extraction and disclosure of massive user information by digital platforms is the focus of attention, and over-extension of their public attributes may leave personal information databases in an unprotected state. Digital platforms should fulfill their information network security management obligations and assume responsibility for governing public space, rather than formally establishing a criminal compliance system merely for the sake of incrimination. Digital platforms are not only commercial entities providing services, but also managers and governors of cyberspace. The establishment of a criminal compliance mechanism is also a concrete manifestation of the platform's fulfillment of its social responsibility and maintenance of the rule of law and order.

Considered from a legal economics perspective, the construction of compliance mechanisms for digital platforms is a complex decision-making process involving a trade-off between costs and benefits. Most platforms, as for-profit business entities, are bound to consider cost-effectiveness. The establishment and operation of compliance mechanisms for online platforms requires the investment of a certain amount of resources, a comprehensive analysis and assessment of their own business characteristics, and the setting up of special systems at the management, operational and technical levels. However, compared to the legal sanctions, reputation loss and economic loss caused by criminal behavior, the investment in compliance mechanisms often has higher benefits and is an intangible asset within the enterprise. In addition, criminal compliance can create compliance

incentives for platforms, such as tax breaks and preferential market access, which contribute financially to their sustainable development.

2.2. Clarifying responsibility for the behavior of the unit and reflecting on the double penalty system

China's Criminal Law has gradually established a system of offenses against computer crimes and cybercrimes. At the legislative level, a set of legal frameworks for the accountability of cybercrime has been initially constructed through the adoption of three ways of attributing responsibility, namely, "treating the act of complicity as a positive offense", "treating the preparatory act as an act of execution" and "clarifying the platform responsibility borne by the network service provider". These three modes of attribution of responsibility have initially constructed a legal framework for pursuing responsibility for cybercrime offenses. The criminal liability of digital platforms as criminal entities is often closely related to the persons in charge and other directly responsible persons. In terms of legislative trends, the center of gravity of criminal law evaluation and sanctioning has gradually shifted from a single center of perpetrator responsibility to one that gives equal weight to perpetrator responsibility and platform responsibility. 7[The basic factual basis for this is that a small number of individual acts of cyber violence between the perpetrator and the victim are not enough to infringe upon the legal interests protected by the criminal law, whereas cyber platforms provide a centralized channel of expression on a scale large enough to amass a massive amount of violent speech in a short period of time, and cyber platforms are unlikely to stay out of the picture or to be completely "neutral".

At present, the determination of the responsibility of the unit in the dual penalty system adopted by China follows the theory of subrogated responsibility. This doctrine holds that the legal consequences of the expressed meaning and behavior of the person in charge of the unit should be directly attributed to the unit and that the unit bears responsibility for the individual's unlawful behavior. [8] The double penalty system highlights the deterrent strength and precision of punishment with the duality of responsibility, but there are limitations at the practical level. The principle of responsibility requires the subject to be responsible only for the behavior that is at fault, i.e. "no responsibility, no crime". Accordingly, even if the platform is not at fault, it will be forced to take responsibility for the illegal acts of its members under the dual penalty system perspective, which on the one hand actually weakens the principle of responsibility; on the other hand, it is contrary to the preventive goal of criminal compliance, no matter whether the platform establishes and implements an effective compliance program or not. Ultimately, all may face criminal liability.

Therefore, the compliance system is a refinement of the limitations of the double penalty system, which effectively achieves the division of responsibility for the behavior of the unit. If a member circumvents the compliance system that has been established and implemented by the enterprise and intentionally commits a wrongful act, the enterprise is not at fault; if there is a loophole in the enterprise's compliance system or the implementation of supervision is ineffective, it is considered to be a dereliction of duty on the part of the enterprise. For digital platforms, when encountering incidents of cyber violence, it is urgent to determine the subjective will of the unit crime within a short period of time, and to identify the causal link between insiders and the results of cyber violence legal infringement. Through the establishment of an effective criminal compliance mechanism, platforms can clarify internal responsibility at various stages, and determine the fault of the technical department, product department, operation department or management, which provides key information for the judicial authorities to determine whether the enterprise has legal responsibility or not. In addition, the criminal compliance system can also more effectively determine whether the platform has helped in online violence incidents and the nature of the helping behavior. Taking the "crime of assisting information network criminal activities" stipulated in Article 287 of *China's Criminal Law* as an example, a network service provider may be found to be a one-sided accomplice because it is aware that the user is using its platform to carry out unlawful activities but does not take any measures; technology providers and service providers who play a key role in cybercrime may also be evaluated as accomplices. positive criminalisation. [9]

2.3. Binary governance to create regulatory synergies between States and platforms

In Article 286 of the *Criminal Law of China*, "the crime of refusing to fulfill the obligation of information network security management", the prerequisite for the identification of this crime is "refusing to take corrective measures when ordered to do so by the supervisory authorities", and the corrective measures not only emphasize the active review obligation of the platform and the obligation to cooperate, but also require the supervisory authorities to have a legal and regulatory basis to specify the specific corrective measures and period of time. The corrective measures not only emphasise the obligation of the platform to take the initiative to review and cooperate, but also require that the supervisory department's order be based on laws and regulations, and that the enterprise's specific corrective measures and deadlines be clearly defined. [10] This clause incentivizes Internet enterprises to strengthen compliance management and promotes synergistic governance between the state and enterprises by strengthening accountability. For enterprises, it means the introduction of the mechanism of exoneration, i.e. the exemption of responsibility; for the state, it means the enhancement of the efficiency of crime control and the saving of judicial resources, and the pattern of public-private co-management is basically formed.

The subjective status of platforms is mainly manifested in two aspects: first, platforms exercise a quasi-legislative power through the formulation of internal regulations; second, platforms actually hold quasi-law enforcement and quasi-judicial powers when regulating user behavior, forming an internal systematic regulatory mechanism. In the case of online violence, the information asymmetry between the platform and other parties is extremely serious; incomplete implementation of the compliance system by the platform, or inappropriate behavior in the disposal process, will easily lead to the side effects of the platform's "law enforcement", which will make it difficult to comply with the principle of proportionality. The realization of power requires supervision, therefore, the binary governance between public and private is an inevitable trend. Under the guidance and constraints of public power, online platforms should move from passive compliance to active compliance.

It cannot be ignored that in this type of collaborative governance model, there exists a game relationship between the public power of the state and private subjects with different interests. On the one hand, some scholars have pointed out that "the development of public-private co-operation in cybersecurity governance model faces a large degree of threats from public institutions such as the government, rather than private institutions". [11] It is worthwhile to pay attention to how the regulator's guidance to online platforms in cases of cyberviolence can be put into practice and be effective, so as to avoid the administration's failure to fulfill its public mission and blame the platforms for their "refusal to perform". On the other hand, in order to fully meet the regulatory requirements, online platforms may over-regulate speech, which is not conducive to maintaining a healthy order of communication in cyberspace. In contrast, at the early stage of the development of the Internet industry, to encourage and protect the openness and innovation of the Internet, Safe Harbor Principle of the *Digital Millennium Copyright Act* of 1998 in the United States [12] did not require platforms to undertake the obligation of censorship beforehand. The Safe Harbor Principle does not impose an ex-ante censorship obligation on platforms, but rather requires them to take action only after they have been notified by regulators. This separation of the public and private sectors from the prior review process is obviously not suitable for today's situation of widespread cyber violence, which has led to the development of Red Flag Principle in legal practice. [13] The principle emphasizes that platforms should take the necessary measures to prevent the further spread of online violence and intervene in a timely manner with national governance tools to prevent platforms from escaping responsibility. It emphasizes the proactive nature of digital platforms' governance but also suggests that without state guidance or external regulatory mechanisms, corporate compliance can easily lead to paper compliance and ineffective compliance. In the early stages of a partnership, building mutual trust between the public and private sectors is an important prerequisite for maximizing the interests of both parties.

3. Responsibilities and paths for digital platforms to respond to online violence

In the process of cyberviolence governance, the responsibilities assumed by digital platforms should be carried out in an orderly and measured manner. Online platforms are both the objects to be regulated and the regulators within the system, i.e., "the State controls the platforms, and the platforms control the users". Especially in dealing with cyber violence, the alienation or abuse of the platform's function often brings great harm to the victims. In order to maintain order and reduce risk, the criminal compliance program established by online platforms not only helps to predict and prevent the occurrence of online violence in advance, but also provides a model for the vertical management of such incidents within the enterprise, transforming the management obligations conferred by laws and regulations into an enterprise system, and realizing the unity of the digital platform's internal control mechanism and the goals of criminal law.

3.1. Ex ante: improving internal compliance programs to prevent criminal risks

In building a criminal compliance system for digital platforms, it is important to adhere to a systematic and standardized methodology. Under the professional guidance of communications regulators, network security agencies and public security agencies, platforms should integrate the obligatory requirements of the criminal law into their operational mechanisms, management systems, operational guidelines and supervision systems to ensure that the obligations of the criminal law are implemented at the operational level of network platforms, thereby reducing the risk of criminal liability for the platforms. A comprehensive criminal compliance risk assessment should be carried out on all aspects of the platform's operation process using a combination of quantitative and qualitative methods. Based on the results of the assessment, detailed compliance guidelines and plans for dealing with cyber violence should be formulated. In addition, specialized training is held on a regular basis to improve the professional ethics and compliance quality of employees. Platforms should formulate clear and detailed rules and regulations against cyber violence before users enter the service, and indicate them in the user agreement and terms of service. Users need to fully understand the rules of cyberspace and be responsible for their own behaviors; platforms need to make every user aware of the "Notice to Users". Considering the limitations of network participants' professional knowledge and the difficulty in reading the terms and conditions of network service providers, platforms may consider transforming the "User Notice" into a "Consent Question and Answer", whereby the content of the User Notice is presented to the users in the form of a question and choice, or it may be incorporated into the "User Agreement" and the "Terms of Service". The platform may consider transforming the "User Information" into a "Consent Quiz" and presenting the content of the User Information to users in the form of question choices; or it may incorporate it into the "Credit Score" system, whereby correctly answering the questions and complying with the order will increase the number of points, which is conducive to promoting and motivating users.

With the help of technological means, the digital platform brings into play the advantages of information and improves the efficiency of monitoring and preventing illegal activities. The platform has established a dynamic and comprehensive evaluation system that takes into account such factors as the degree of maliciousness of the content of the speech, the scope of its impact, and the mental health of the target of the speech. For example, it has set up an AI intelligent detection assistant to conduct real-time searches for keywords closely linked to online violence and regularly update the search thesaurus, triggering manual checks and specialized audits once the detection results reach a certain threshold. Platforms handling powerful information flows under the condition of holding a large amount of user data, it is necessary to implement a real-name system and adopt a multi-factor authentication mechanism to enhance the security of accounts, while adopting strict security measures to protect users' personal information; for platforms that allow anonymous posting, set up content filters and additional monitoring mechanisms, and restrict the behavior of anonymous users, such as reducing the frequency of posting and the scope of visibility. In order to help victims and judicial authorities determine the identity of cyberviolence perpetrators for the first time after the occurrence of cyberviolence. Monitor user activities through user behavior analysis technology, take preventive

measures against potential cyber violence, establish a database of offending users, warn and educate first-time offenders, and gradually increase penalties for repeated offenders, including restricting posting privileges up to account bans. For the founders of emerging Internet groups, training should be strengthened by platform officials for users who have a duty to manage them.

3.2. During the event: specific procedures for responding to avoid the expansion of risks

In the face of incidents of online violence, digital platforms are required to immediately activate their contingency plans under their compliance frameworks, carry out preliminary risk assessments of the content in question, and swiftly implement technical intervention measures. These include content removal, access restriction or link disabling, etc., to pinpoint and control the source of online violence. At the same time, related discussion topics are promptly monitored and reviewed to prevent further expansion of the dissemination of violent content. Some scholars have pointed out that, according to the ecological governance requirements of the dominant position of online violent information dissemination, the substantive fulfillment of the obligation to deal with the incident needs to examine whether the social media platforms have effectively changed the hostage and monopoly of online violent information on online public opinion through the use of measures and governance tools, so as to bring the discussion of the controversial incident back to the normalized, diversified and healthy ecology. [14]

Platforms should implement appropriate management measures for user accounts suspected of cyberviolence, such as warnings, functional restrictions and even account bans, in accordance with established user behavioral and community guidelines. The most important tool for victims of online violence is the activation of a one-click protection mechanism by the platform. At this stage, various online platforms, such as Weibo and Shake Tone, have established preliminary protection mechanisms based on "mutual shutdown comments", but lack a systematic detection system and evidence retention system. For users who have successfully applied for protection or met the conditions for protection, platforms should record them in real-time, form a complete chain of evidence, and carry out procedures for fixing and preserving the evidence to ensure the completeness and availability of all relevant data, so as to facilitate subsequent legal analyses and possible judicial proceedings. While melting down violent public opinions, the platform should also correctly guide public opinions, which can be done by combing through the entire timeline of the incident and focusing on experts' scientific interpretations of similar incidents, calling on netizens to discuss and analyze the incident rationally and draw lessons from it, so as to avoid the situation from becoming more serious and expanding.

In addition, the platform should promptly activate the internal compliance review process and consultation mechanism, and set up dedicated personnel to analyze in depth the causes, scope of impact and potential deficiencies of the control system. As scholars have pointed out, corporate compliance management should not stand outside the business process and act only as an external supervisor, auditor and vetter, but should be embedded in the "whole business process" of the enterprise, and should find the corresponding compliance control points and implement targeted compliance control measures in response to the compliance risk points existing in the business process. [15] Accordingly, digital platforms should actively assume the role of "gatekeeper" [16] in dealing with cyber violence, actively controlling and actively responding to the instructions of the regulatory authorities, in order to protect the rights of users and the order of the platforms from cyber violence.

3.3. Ex post facto: taking stock of criminal compliance experience and rationalizing risk avoidance

Digital platforms should systematically review and analyze the entire process of responding to cyberviolence cases in order to identify and refine effective compliance management strategies. By revising and strengthening the criminal compliance mechanism, combined with upgrading and improving the technical means, the platforms will be able to enhance their prevention and response

capability to cyber violence more significantly. At the same time, cooperation and exchanges with enterprises in the same industry have been strengthened. Platforms can share their experience in technology prevention and control and in stopping harm, or they can reach an agreement to block the speech of abusers and track information in real-time when responding to incidents of cyber violence, forming a strong regulatory synergy within their own ecological domains. At this stage, the supervisory and guiding role of national public authorities should also be emphasized. For platforms that refuse to fulfill their information network security management obligations, the supervisory authorities should formulate detailed acceptance charters focusing on strengthening the platform's own operations, to avoid platforms shifting their responsibilities to employees through criminal compliance; for platforms suspected of aggravating the problem of cyber-violence through improper means such as data monopoly and abuse of dominant market position, etc.

The Antitrust authorities should investigate according to the law and provide guidelines to promote industry self-regulation and compliance. In the process of correcting problems with the compliance system, platforms should simultaneously assess risks with the help of compliance risk identification tools, to achieve preventive and avoidance effects.

The summary reflections of the senior leadership of the digital platform at this stage play an important role in the improvement of the compliance system. In company law doctrine, corporate leaders have a holistic obligation (Gesamtverantwortung) to guarantee corporate compliance and are non-delegable. [17] As a result, the obligation of compliance of the enterprise as a proposed subject is naturally passed on to the enterprise leaders. China's Supreme People's Procuratorate's Measures for *Compliance Construction, Evaluation and Review of Enterprises Involved in Cases (for Trial Implementation)*, issued in April 2022, states that the highest level of an enterprise can play the following major roles in carrying out compliance rectification: first, "enterprises involved in cases should generally establish a compliance construction leading group, consisting of its actual controller, principal person in charge and supervisory personnel directly responsible for it, etc. Composition. [18] The compliance management leadership team needs to further develop specialized compliance strategies and establish corresponding internal norms and regulations based on a comprehensive review and assessment of the potential compliance risks of the enterprise. In establishing relationships with legal advisors, industry experts and regulators, online platforms emphasize the value of positive incentives for criminal compliance, ensuring that there is an effective communication mechanism between the compliance team and senior management, and leveraging the positive impact of senior-level commitment to build a more robust and adaptable criminal compliance system.

4. Roles and functions of governance of public-power collaborative digital platforms

Since the end of the nineteenth century, there has been a gradual "socialization of law", which has led to the emergence of the notion of the integration of the public and private spheres and of collaborative governance. In this process, the traditional framework of the dichotomy between the individual and the public interest has been reshaped, giving rise to a new type of social value that emphasizes the importance of the overall interest of society and the public interest. It is an inherent necessity of the public attributes of digital platforms to assume a certain degree of public responsibility in managing the order of a particular space on the network. Excessive responsibility objectively cannot be fulfilled by the platform, and is also prone to lead to the expansion of power, making the enterprise overstep its limits. Some scholars have pointed out that the governance model of public-private cooperation of cyber violence not only exists in the mix of private subjects and public sector subjects, but also exists in the mix of administrative supervision and crime risk prevention and control functions. [19] In the event of cyber violence, the personal dignity of the victim is often violated, and is also an important fundamental right protected by our constitution, the intervention of public power in the whole process and at all stages is necessary. Its role in digital platform governance should be multidimensional and all-encompassing. When the platform's

criminal compliance system is flawed, public power guides it to shape the correct corporate culture and improve it; when the platform's response to handling cases involving online violence lags or fails, public power follows up and urges it to fulfill its duties on time. The binary interaction achieves dynamic balance in a virtuous circle. Public power does not monopolize the platform's governance activities, but plays the role of "guide", "co-operator" and "regulator", and authorizes some of the management functions to the platform. It can authorize part of its management functions to the platforms, and its moderate intervention is conducive to keeping cyberspace active and promoting the development of the digital economy.

4.1. Follow-up on platform developments and review of internal compliance systems

Supervisory authorities should pay close attention to the dynamics of platforms and conduct occasional monitoring and spot checks on their mode of operation, content auditing and user behavior. The platform's operation mechanism is directly related to its strength in regulating information dissemination and its influence on user activities. The regulator focuses on assessing whether there are risk points on the platform that may trigger cyber violence, such as whether the algorithmic recommendation system is biased and whether the user interaction mechanism is prone to lead to group conflicts. Currently, China has established a relatively complete normative system in the areas of personal information protection and cybersecurity, which provides a normative basis for companies to develop special compliance programs. [20] At the practical level, China's Central Internet Information Office has asked localities to establish channels for the rapid disposal of reports of online violence, strengthen the service functions of reporting platforms, and provide a set of "report complaints", "reporting guidelines", "typical cases", "laws and regulations", "guidelines", "guidelines", "laws and regulations", and so on. " "Laws and regulations" and other multi-functional in one of the reporting service products [21]. The aim is to promote platform compliance through external supervision, but implementation is not yet widespread. An example of an organization that can follow up on suspicious developments on platforms in real-time is already in place in Germany - the Centre for Unsuspicious Investigations in Data Networks, which is part of the Federal Criminal Police Office (Bundeskriminalamt) and is tasked with cyber-policing. At the Länder level, 16 Länder have set up "cyberpolice" or other forms of regulatory bodies that have the authority to monitor developments on the Internet around the clock and can quickly analyze and respond to information on the Internet and take the necessary measures. In addition, in their daily reviews, administrative and law enforcement authorities should focus on whether the platforms have set up a feasible and effective compliance system in accordance with the standards for the fulfillment of the obligation to manage information on cyber violence. In the event of a case involving online violence, the judiciary will first review the functionality of the compliance programme before examining the behavior of members within the platform. Continuous improvement is still needed at the legislative level to adapt to new cyberviolence crime trends and digital technology developments. The cybercrime department should also strengthen cooperation with academia, drawing on academic research results to guide practice, provide complete compliance guidelines as much as possible, and improve the scientific nature of the guidance.

4.2. Provision of necessary services and establishment of good cooperation

2022 *The Notice on Effectively Strengthening the Governance of Cyber Violence* issued by China's Central Internet Information Office does not address the obligation of network service providers to assist the public sector. With the high incidence of vicious incidents of online violence, not only does the assistance relationship need to be taken seriously, but more critically, the public and private sectors need to establish long-term and effective cooperative relationships and smooth communication mechanisms. The cooperation should be based on mutual trust and a common goal, i.e. to maintain online order and protect users' rights and interests. Long-term cooperation can also help ease the conflict between platforms as profit-seeking commercial entities and their responsibility for public governance. Internet information departments should provide the necessary services and

support, and organise regular compliance training seminars and legal advice for enterprises. Promote platforms to establish an effective content audit process, including but not limited to a mechanism combining manual and technical auditing, a training and assessment system for auditors, and a complaint and review mechanism for audit results. Under the guidance of public power, the two sides will jointly study and formulate strategies and measures to deal with online violence; carry out public education and publicity to raise the public's awareness of online violence and its prevention; and promote cross-platform collaboration to jointly combat online violence. In addition, the *Personal Information Protection Law*, passed in August 2021, specifically establishes provisions for public interest litigation, followed by the Supreme People's Procuratorate's issuance of the *Circular on Implementing and Enforcing the Personal Information Protection Law to Promote the Prosecution of Public Interest Litigation on Personal Information Protection*. It is evident that the procuratorate can play a huge role in the relief mechanism, further uniting platforms to protect the legitimate rights and interests of victims in online violence cases.

4.3. Protecting fair competition and promoting the healthy development of the industry

Large digital platforms have a monopoly position due to their size and market influence, and they have greater control over the dissemination of information, the regulation of user behavior and the review of content. Without effective regulation and corresponding anti-monopoly measures, such control may indulge or even promote the spread and intensification of online violence in the pursuit of traffic and profits. Public power should, on the one hand, protect the rights and interests of users and prevent digital platforms from abusing their dominant market position and infringing on user privacy and data security. At the same time, it should also protect legally operating platforms from unfair competition and illegal interference. In the public regulatory system, *the Antimonopoly Law* has greater institutional tension than *the E-Commerce Law*, and the relevant problems can be solved one by one by following the logic of the Antimonopoly Law regulation. [22] Regulators need to ensure that platforms do not use their dominant market position to restrict competition, inhibit freedom of expression, or avoid legal liability. Antitrust authorities should encourage fair competition within the digital platform industry, guide industry associations and enterprises to establish self-regulatory mechanisms, formulate industry standards and codes of conduct, and promote self-regulation and healthy development within the industry. In short, fair competition in the digital platform market can incentivize platforms to innovate their governance models and seek more effective strategies for online violence governance. With the incentive of competition at the national level, platforms are more motivated to develop new content review mechanisms, user education programs and cooperative governance models, thereby enhancing the overall health of the online environment.

5. Conclusion

How platforms can cope with increasingly complex online violence, enhance the level of regularised supervision and promote the standardization of compliance systems is a major issue that cannot be ignored in today's digital interconnected era. Guided by the positive criminal governance mindset, online platforms should develop a set of comprehensive mechanisms that can prevent, identify, respond to and eliminate online violence, and implement a series of multi-dimensional strategies such as technical monitoring, content filtering, user behavior analysis and education and advocacy. Effective criminal compliance systems are used to prevent, detect and stop illegal and criminal behavior within the platform, and special review mechanisms are performed by dedicated personnel so that responsibilities can be more clearly implemented when risks arise. Digital platforms enjoy advantages in terms of technology and professionalism, while the corresponding public power has limitations in intervening and improving the internal management of the platform. In case of infringement of users' rights and interests, platforms should take the initiative to cooperate with public authorities to establish a binary and collaborative remedial mechanism to more effectively protect and remedy the legitimate rights and interests of users. Under the framework of collaborative public-

private governance, the State should fully respect the pursuit of profitability of online platforms as commercial entities, and coordinate and balance the goals between the need for autonomy in the private sphere of online platforms and the development of the macro digital economy.

References

[1] The types of offenses listed in the guidance also include "malicious marketing hype through cyberviolence", which is not cyberviolence per se, but an extension of cyberviolence.

[2] Article 253 of the Criminal Law originally stipulated that the offenses of selling or illegally providing citizens' personal information and of illegally obtaining citizens' personal information are offenses. Illegal Acquisition of Citizens' Personal Information was special subjects, i.e., they were limited to State organs or financial, telecommunication, transport, educational, medical, and other units and their staff. Amendment (IX) to the Criminal Law has changed the scope of the above two offenses to include the following Offences The criminal subjects of the above two offenses were originally limited to state organs or units of finance, telecommunication, transport, education, and medical care and their staff, and have been expanded to general subjects and units.

[3] See the Cybersecurity Law of the People's Republic of China: Article 12 Any individual or organisation using the Internet shall abide by the Constitution and the law, comply with public order, respect social morality, shall not jeopardise cybersecurity, and shall not use the Internet to engage in activities that endanger the security, honour and interests of the State, incite subversion of State power or overthrow of the socialist system, incite secession of the country or undermine national unity, advocate terrorism or extremism, disseminate violent, obscene and pornographic information, fabricate and disseminate false information that disrupts economic order and social order, and infringe upon the reputation, privacy and intellectual property rights and other legitimate interests. , promote ethnic hatred and discrimination, disseminate violence, obscene and pornographic information, fabricate and disseminate false information to disrupt the economic and social order, and infringe upon the honour, privacy, intellectual property rights and other legitimate rights and interests of others.

[4] See Zhou Guangquan, "The Establishment of the Positive Criminal Law Legislation View in China", in Legal Studies, 2016, 38(04):23-40.

[5] See: [U.S.] Philip Weller, "Effective Compliance Programs and Corporate Criminal Proceedings", translated by Wan Fang, in Finance and Economics Law, Vol. 3, No. 3, 2018, p. 144

[6] See: Compliance Management System Requirements and Guidance for Use (GB/T35770-2022).

[7] See Yu Chong, "The Delimitation of Criminal Liability for the Inaction of Network Service Providers under the Vision of "Dichotomy", in Contemporary Jurisprudence 2019, 33(05):13-26.

[8] See Li Benchan et al., eds: Compliance and Criminal Law: An Examination from a Global Perspective, China University of Political Science and Law Press, 2018 edition, p. 232

[9] There are controversies in the academic community about the division of this evaluation, such as Zhang Mingkai in the article "On the Crime of Helping Criminal Activities in Information Networks" in which he rejected the theory of independence of accomplices, and believed that the nature of the crime is not the formalization of helping criminals, but rather, the sentencing rules of helping criminals. In Politics and Law,2016,(02):2-16.DOI:10.15984

[10] See: Amendments to the Criminal Law (IX), formally implemented on 1 November 2015; Interpretation of Key and Difficult Issues in the Interpretation by the Supreme People's Court and the Supreme People's Procuratorate of the Interpretation of Several Issues Concerning the Application of the Law in Handling Criminal Cases of Illegal Use of Information Networks, Helping Criminal Activities in Information Networks, etc., released on 25 October 2019

[11] Kristen E. Eichensehr, Public- Private Cybersecurity, Texas Law Review, Vol. 95:467, p. 468 (2016).

[12] See U.S. Digital Millennium Copyright Act, 1998.

[13] The Red Flag Doctrine: emphasises that when it is clear that an OSP knew or should have known of the existence of illegal or infringing content on its platform, it should take the necessary measures to prevent the distribution of such content. Under the DMCA, if an OSP has actual knowledge or it is clearly inferred

from the facts (i.e., a red flag) that copyright infringement is occurring, they will lose the protection from liability afforded by the safe harbor doctrine.

[14] See Zhu Xiaoyan, "From content regulation to ecological regulation: the reshaping of platform obligations in the governance of online violent information", in Journal of Nanjing University (Philosophy-Humanities-Social Sciences), 2024, 61(01):76-91+163-164.

[15] See Chen Ruihua, "The Basic Principles of Effective Compliance Management", in Journal of Shanghai University of Political Science and Law (Rule of Law Series), 2024, 39(01): 14-31. DOI: 10.19916.

[16] Alex Lemaire, "La régulation équitable des plateformes", in Xavier Delpeche (dir.), L'émérgence d'un droit des plate-formes, Dalloz, 2021, p. 48.

[17] Vgl. Frank G. Schmidt-Husson, in:Christoph E. Hauschka (Hrsg.), Corporate Compliance, Verlag C.H. Beck, 2007, §7 Rn.2 ff; Metin Konu, Die Garantenstellung des Compliance-Officers, Duncker & Humblot, 2014, S.44

[18] See: Measures for Compliance Building, Assessment and Review of Case-Related Enterprises (for Trial Implementation), published by the General Office of the All-China Federation of Industry and Commerce, in conjunction with the General Office of the Supreme People's Procuratorate and nine other units and nine other departments, April 2022

[19] See Jing Lijia, "Rethinking and Debugging the Public-Private Partnership Governance Model of Cyber Violence," in Jianghan Forum, 2023, (05): 136-144.

[20] See Jing Lijia, "System Construction of Personal Information Protection Compliance", in Legal Studies, No. 4, 2022.

[21] See Office of the Central Committee for Network Security and Informatisation: Guiding Opinions on Further Strengthening the Work of Reporting Online Infringement Information. [EB/OL]. (2023-09-15) [2024-04-17]. https://www.cac.gov.cn/2023-09/15/c_1696347685563097.htm

[22] See Sun Jin, "Public Regulation of Digital Platforms' "Choose One or the Other" Behaviour under the Antimonopoly Law", in Journal of Political Science and Law, 2024(02):51-62.