

Determining Criminal Liability for Online Violence: Challenges and Legal Responses

Jinyi Shi

School of Law, Anhui University of Finance and Economics, Bengbu 233030, China
Email: anthony_sjy@163.com

How to cite this paper: Shi, J. Y. (2025). Determining Criminal Liability for Online Violence: Challenges and Legal Responses. *Law and Humanities*, 1(2), 84-99. ISSN Print: 3079-5117; ISSN Online: 3079-5125. <https://doi.org/10.63313/LH.9018>
Published: 2025-07-01

Copyright © 2025 by author(s) and Erytis Publishing Limited.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
<http://creativecommons.org/licenses/by/4.0/>



Abstract

Online violence, as a new social problem of the digital age, is characterized by group participation, anonymity, and rapid diffusion – posing a tremendous challenge to traditional criminal justice. In recent years, China has introduced a series of regulations and judicial guidelines to curb online violence. However, in practice there remain significant difficulties in the criminal liability determination for such acts, including ambiguous identification of responsible actors, challenges in proving subjective intent, complex issues of causation, and the inadequacy of traditional offenses to cover new online behaviors. This article examines the core dilemmas in attributing criminal responsibility for online violence, analyzes shortcomings in the existing legal framework, and proposes comprehensive measures – such as refining legislation, issuing clearer judicial interpretations, enforcing platform responsibilities, and leveraging blockchain technology for traceability – to build a clearer, more systematic and reasonable criminal law regime. The goal is to effectively balance the crackdown on egregious online abuse with the protection of freedom of expression, in line with the standards of rule of law.

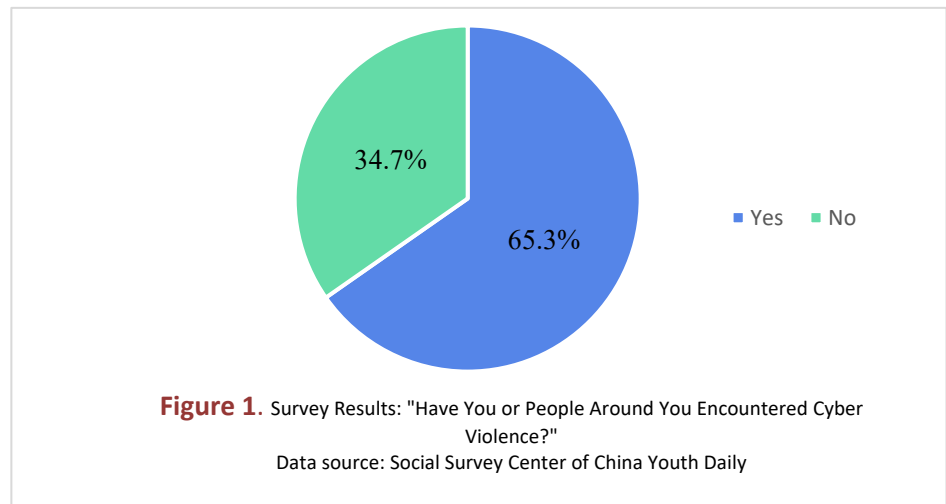
Keywords

online violence; criminal liability determination; application of law; platform governance; rule-of-law safeguards

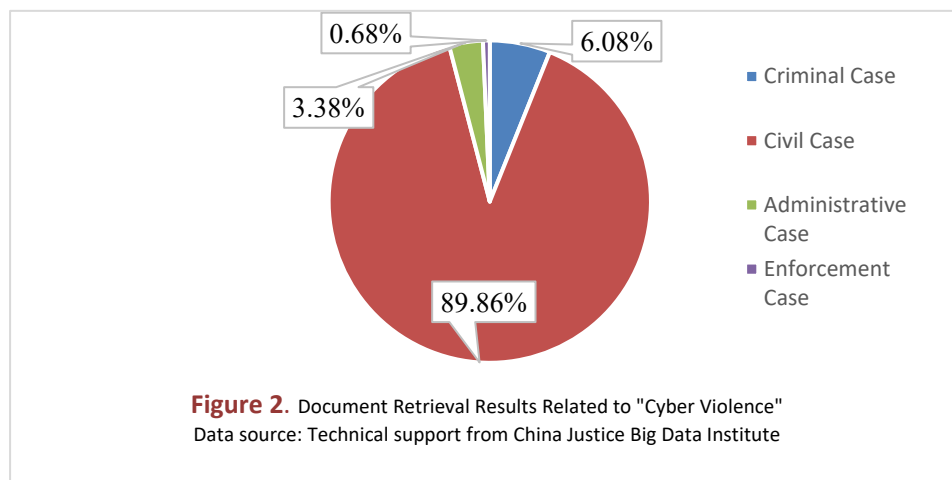
1. Introduction

The rapid proliferation of the internet has greatly facilitated information exchange, but it has also given rise to the serious societal issue of “online violence.” Surveys indicate that over 60% of young internet users in China have experienced or witnessed online violence, and some extreme cases have even resulted in victims suffering depression or committing suicide (Figure 1). Large-scale online harassment can inflict severe damage on social order and citizens’ rights. Online violence features lightning-fast spread, wide-ranging impact, and strong anonymity, enabling mobs of netizens to launch massive verbal attacks on victims. This phenomenon presents an unprecedented challenge to traditional legal frameworks for protecting

personal rights and maintaining public order.



In response to the spread of online violence, Chinese lawmakers and judicial authorities have steadily ramped up regulatory efforts. Notably, in September 2023 the Supreme People's Court (SPC), Supreme People's Procuratorate (SPP), and Ministry of Public Security jointly issued the Guiding Opinion on Lawfully Punishing Online Violence – the first comprehensive judicial policy document addressing the legal characterization, evidence collection, conviction, and sentencing of online violence cases. In June 2024, the Cyberspace Administration of China (CAC), together with several other agencies, promulgated the Provisions on Governance of Online Violence Information, further clarifying the definition of "online violence" content and setting out governance requirements, with the regulation taking effect on August 1, 2024. These developments signal a shift in China's legislative approach from cautious restraint to active intervention in curbing online abuse. However, despite these efforts, numerous difficulties persist in using criminal law to punish serious online violence: the identification of responsible parties is often unclear, online behaviors do not neatly fit existing offense definitions, causation between online conduct and harm is hard to prove, and there is a lingering conundrum of "the law not punishing the masses" when so many individuals are involved. Consequently, very few instances of egregious online violence have actually been subject to criminal sanctions (Figure 2). It is therefore imperative to examine in depth the issues surrounding the determination of criminal liability for online violence, with a view to providing clearer and more rational legal strategies for governing cyberspace in the digital era.



2. Defining Online Violence and Its Criminal Law Characteristics

2.1. Concept and Scope of "Online Violence"

"Online violence" is not a term of art in Chinese criminal law, but rather an umbrella label for a class of aberrant online behaviors. Broadly defined, online violence refers to acts whereby individuals rely on the internet – through words, images, audio/video, etc. – to commit aggressive, insulting, defamatory or threatening conduct against others, thereby infringing upon their lawful rights and possibly endangering their dignity, reputation, or mental and physical well-being. In a narrower sense, it specifically denotes sustained, concentrated, and group-based verbal attacks in cyberspace – essentially a new form of informational infringement akin to large-scale cyberbullying.

It is worth noting that authorities in China have offered a working definition of online violence. A 2022 notice by the CAC defined online violence as "*acts of centrally publishing insulting, abusive, defamatory, privacy-infringing or other unlawful and unfriendly information targeting an individual, which infringe others' lawful rights and disrupt normal online order.*" This definition highlights the typical forms of online violence (insults, defamation, privacy breaches, etc.) and the resulting harms (infringement of rights and disturbance of online order). In sum, online violence is not a single codified crime, but an umbrella term encompassing various unlawful or even criminal acts – including online insults, defamation, privacy invasion, "human flesh search" doxxing, and so on. Its legal nature usually manifests as an infringement on personal legal interests (such as the rights to reputation and privacy), and under the effect of online mob polarization it may further disrupt public order.

2.2. Key Characteristics of Online Violence

As a novel behavior distinct from traditional forms of violence, online violence exhibits several legal characteristics.

2.2.1. Anonymity and Concealment

The anonymity afforded by internet platforms – through pseudonyms or fake accounts – makes perpetrators difficult to trace and emboldens them by lowering their fear of legal consequences. Shielded by hidden identities, many netizens freely post vicious attacks, wielding the “keyboard” as a weapon to hurt others with impunity. This concealment means that once an online attack begins, it is often difficult to promptly halt, leaving victims isolated and helpless.

2.2.2. Group Dynamics and “Pile-On” Effect

Online violence typically takes the form of group mobbing. What may start as provocations by a few individuals can quickly snowball into a “cyber gang assault” involving many participants, fanned by social media amplification. From influential online figures (“Big Vs”) who incite or mislead, and media outlets that report out-of-context, to ordinary users who follow the trend by reposting and hurling insults – actors at all levels collectively fuel the fermentation and escalation of online violence. The diversity and sheer number of participants mean that any single act might seem negligible, but the cumulative effect is enormous. Indeed, the accumulation and amplification of countless comments can inflict harm far beyond that of any isolated remark, subjecting the victim to unrelenting psychological pressure.

2.2.3. Compound Harmful Consequences

The direct harm of online violence is to personal interests such as an individual’s dignity, reputation, and privacy. However, when an online campaign escalates and spills over, it can trigger offline harassment, doxxing (“human flesh searches”), or even real-life retaliation, thereby endangering public order and safety. In other words, the legal interests harmed by online violence often intertwine personal and public interests. Whether a given online violence incident has damaged public order depends on its scope and consequences, but it is certain that severe online violence transcends mere civil torts or administrative violations and necessitates criminal law intervention.

3. Challenges in Determining Criminal Liability for Online Violence

Compared to traditional one-on-one offenses, online violence often involves numerous perpetrators and complex speech acts, creating unique challenges for assigning criminal responsibility. The main difficulties can be summarized as follows.

3.1. Difficulty in Identifying Responsible Parties

Online violence is usually perpetrated collectively by an indeterminate multitude of netizens, and the old adage “the law cannot punish everyone” often leads to many offenders escaping legal sanctions. In a major cyber mob incident, participants might include the initial rumormongers or malicious agenda-setters (the “organizers”), those who repeatedly post insulting or harmful comments (the

“direct perpetrators”), others who simply chime in or fan the flames (“general participants”), and even the internet service providers that amplify the abuse through algorithms or traffic promotion. All these diverse actors together contribute to the harm inflicted on the victim’s legal interests – yet in imposing criminal liability, it is difficult to hold each one to account. Who should face criminal charges, and how to distinguish principal culprits from accessories? If every one of the thousands of users who posted offensive comments were treated as perpetrators, it would be unfeasible in practice and offend the principle that punishment should be proportional to personal culpability. But if only a very few ringleaders are punished, it hardly seems just or deterrent. This “offender identification” dilemma leaves judicial authorities in a quandary when deciding whom to prosecute.

3.2. Difficulty in Proving Subjective Intent

Criminal prosecution requires establishing that the perpetrator acted with the requisite guilty mind (*mens rea*). Yet the mental states of online abusers are often complex and do not fit neatly into classic categories of intentional crime. Many participants in online violence may be acting out of momentary anger, curiosity, thrill-seeking or herd mentality. Believing themselves to be dispensing justice, they follow the crowd in commenting, without genuinely intending or recklessly disregarding that their actions could drive someone to serious harm. Even if some comments objectively contribute to a victim’s severe outcome (such as suicide), it is hard to conclude that the multitude of commenters all harbored an intent to cause injury or death.

3.3. Difficulty in Establishing Causal Link

In criminal law, an act must be causally linked to a harmful result in order to impose liability for that result. But online violence is typically a process-based harm committed by a multitude of comments, where the causal chain between any single act and the ultimate serious outcome is highly complex. On one hand, the victim’s psychological harm or reputational damage is the cumulative result of numerous statements, making it nearly impossible to tie a specific comment to a specific injury. On the other hand, the online public opinion environment is fast-changing and often exhibits a “loss of focus” phenomenon – the topic shifts, truth and falsehood intermingle, and the eventual serious consequence may not stem from any one remark but rather from the prolonged pressure of public scrutiny. In extreme cases, a victim’s decision to end their life may involve their own psychological fragility and other factors, with online bullying being only one contributing cause.

3.4. Conflicts and Gaps in Applying Offense Provisions

China's Criminal Law currently has no specific offense called "online violence." Prosecutors must resort to traditional offense provisions to charge acts of online violence, which leads to ambiguities and overlap in the application of different crimes. Several issues arise in this context.

3.4.1. Overlap of insult vs. public order offense

For online abusive speech, there is confusion over whether to apply the crime of insult or the crime of "picking quarrels and provoking trouble." Under Article 246 of the Criminal Law, openly insulting another person, if circumstances are serious, constitutes the crime of insult. However, a 2013 judicial interpretation by the SPC, SPP, and MPS on handling online defamation and related cases stipulates that using the information network to curse or intimidate others, in an egregious manner that disrupts public order, should be charged as the crime of picking quarrels and provoking trouble (寻衅滋事罪). This creates a legal overlap: when a netizen goes on a tirade of abuse online, if one views the primary harm as an infringement of personal reputation and it's serious, it falls under insult; but if one views it as disrupting public order, it could be prosecuted as picking quarrels. In practice, there is no clear guideline for distinguishing the two, and similar conduct has been charged differently in different jurisdictions, undermining consistency in the law's application.

3.4.2. Defamation thresholds and procedural hurdles

In cases of online rumormongering or defamation, the requirements of the defamation offense (also in Article 246) and its procedure limit effective enforcement. By law, defamation is ordinarily a private prosecution offense – the victim must bring charges – unless the offense "seriously endangers social order or national interests," in which case public prosecution is allowed. A 2013 judicial interpretation attempted to define "serious circumstances" for online defamation by setting quantitative thresholds (for example, a false rumor viewed 5,000 times or reposted 500 times was deemed serious enough for a criminal case). While this provided a useful benchmark at the time, a decade later in the era of ubiquitous social media those numbers are extremely low. Today, it is not uncommon for even trivial posts to exceed 5,000 views or 500 shares. Rigidly applying those thresholds would imply nearly every online rumor meets the criminal standard, raising concerns of over-criminalizing speech. Conversely, if the outdated standard is ignored and not updated, many new forms of vicious rumor-mongering cannot be timely punished under criminal law. In addition, the private prosecution requirement itself presents a high barrier: victims of defamation often find it difficult to gather evidence and endure a protracted lawsuit on their own, and many give up, meaning perpetrators go unpunished.

3.4.3. Privacy violations ("human flesh search") and legal gaps

A common aspect of online violence is the doxxing of victims – illegally obtaining and exposing someone’s personal information (home address, phone number, ID number, etc.), which gravely violates the right to privacy. China’s Criminal Law Article 253(1) (added in 2009, and amended in 2015) criminalizes the infringement of citizens’ personal information, targeting those who illegally obtain, sell, or provide others’ personal data when circumstances are serious. In principle, a typical “human flesh search” scenario – where perpetrators gather and spread a victim’s private information without consent, leading to the victim being harassed or targeted offline – *could* be prosecuted under this provision. If the perpetrator had a malicious motive (such as revenge or profit) and the consequences are severe, it likely meets the “serious circumstances” threshold for the crime. However, in practice there are debates and loopholes. For one, the law requires the act to involve citizens’ personal information that is *illegally provided or obtained*; if doxxers share information sourced from public records or post less sensitive data (say, merely someone’s workplace or social media handle), it may fall outside the statute’s scope. For another, if the doxxing was not done for profit – for example, an offender publishes someone’s info ostensibly in the public interest or as free expression – it can blur the lines, and enforcement must carefully balance privacy rights against claims of freedom of information.

3.4.4. Offense coverage gaps

Finally, the scope of current offenses is limited in covering every harmful behavior emerging from online violence. Beyond insult, defamation, and personal information crimes, some malignant online conduct does not squarely fit any existing criminal provision. For example, if masses of netizens maliciously “pile on” in a way that throws the online public sphere into chaos, yet without a specific individual target for insult or defamation, can this scenario be brought under the crime of picking quarrels (which traditionally punishes public disturbances)? Another example: if an online platform knowingly permits a large-scale bullying campaign to run rampant on its service and responds passively, the only applicable offense in current law might be “refusing to fulfill information network security management obligations” (Article 286(1)), which has a high bar (it requires the platform to ignore government orders to act, resulting in very serious consequences) and is rarely invoked. In short, there is a disconnect between traditional criminal provisions and the new reality of online violence. Some egregious forms of cyber abuse still evade criminal punishment entirely, creating a difficult choice between a regulatory vacuum and potentially stretching existing laws to cover novel situations.

4. Current Legal Framework and Regulatory Approaches

Despite the absence of a standalone “online violence” offense, China’s criminal law

framework does contain various provisions that can be applied to acts associated with online violence. This section reviews the main applicable offenses, evaluating how they have been used to address online violence and where the challenges remain.

4.1. Crime of Insult: Application and Limitations

The crime of insult (Article 246 of the Criminal Law) is designed to protect citizens' personal dignity by punishing those who openly use violence or other methods to insult others. In online contexts, a perpetrator who uses the internet to post degrading, abusive statements that malign another person's character ostensibly meets the basic elements of this crime. However, applying the traditional insult statute to cyber scenarios raises several questions. First is the requirement of publicness – the offense requires that the insult be made “openly.” Statements on public social media feeds, comment sections, or forums would clearly qualify as public insults. But what about insults made in a semi-private group chat or a niche online community? There is a gray area in determining whether certain online venues count as “public” for purposes of the statute.

4.2. Crime of Defamation: Application and Evolution

The crime of defamation is also set forth in Article 246, targeting the fabrication and dissemination of false facts that damage another's reputation. In the internet age, rumors can spread with unprecedented speed and reach, making the social harm of defamation greater than ever. The judicial interpretation issued in 2013 (by the SPC, SPP, and MPS) specifically addressed online defamation, introducing a quantitative threshold for “serious circumstances” – notably, the criterion of a false rumor being viewed over 5,000 times or shared over 500 times. This was a pioneering effort to adapt enforcement to the online context, and it served its purpose in a period when such numbers indicated a significant impact.

However, reaching 500 shares is no longer an exceptional indicator of harm. It cannot be assumed in today's environment that crossing that numeric threshold alone equates to grave harm – doing so risks sweeping up virtually all instances of online rumor-spreading as criminal defamation. On the other hand, cunning offenders have adapted to avoid detection: instead of outright falsehoods, they might spread insinuations or scatter the rumor across multiple forums and platforms, complicating the determination of both falsity and impact.

Another significant problem with defamation cases is the difficulty of initiating public prosecution. As noted, most defamation cases require the victim to file charges, and only when a rumor triggers broad public panic or disorder will authorities step in. This means many online falsehoods that cause serious personal harm but do not clearly undermine public order may still not see a government-led prosecution. Given that online rumors often poison the general information environment and can indirectly affect public interests, some commentators argue that when a rumor disseminated via internet causes a major social impact, it should be construed as “se-

riously undermining social order,” thus allowing prosecutors to pursue the case *ex officio*. Expanding the scope of public prosecution in this way could significantly improve the enforcement against viral defamation.

4.3. Personal Information Infringement and the “Human Flesh Search”

In the context of online violence, a typical doxxing scenario might be: someone gathers a victim’s sensitive personal data (home address, phone number, ID number, etc.) without permission and disseminates it online, leading to the victim being subjected to harassing calls, stalking, or even vigilante attacks in real life. If such conduct results in significant harm, it likely fits the criteria of “illegally providing personal information” in serious circumstances, thus constituting the crime. Especially if the perpetrator acted with clear malicious intent (such as seeking revenge or notoriety) or for profit, and the victim suffered real damage, criminal liability should ensue.

Of course, applying this crime to doxxing has its limitations and contentious points. One limitation is that the law is aimed at *illegally obtained or provided* personal data – if the information shared by the mob is actually scraped from public sources (for instance, posting the victim’s publicly listed workplace or a social media profile), it may not fall under the statute’s protection of “personal information.” Likewise, if the information shared is not particularly sensitive (perhaps just a name combined with publicly available details), some may argue the threshold for criminal protection isn’t met. Another contention comes from the perspective of free expression: perpetrators sometimes defend doxxing as a form of public supervision or claim that they are merely sharing “open secrets.” In cases where the doxxing is non-commercial, defendants might argue they didn’t “provide information illegally” but were exercising a right to share news. Enforcement must carefully navigate these claims, weighing the privacy rights of individuals against any purported public interest or speech rights.

4.4. The Catch-all Crime of “Picking Quarrels and Provoking Trouble”

Picking quarrels and provoking trouble (寻衅滋事罪, Article 293 of the Criminal Law) has emerged as a catch-all offense to maintain public order, traditionally covering acts like random assaults, stalking and obstruction, forcible taking of property, and creating disturbances. In the context of online violence, if a large-scale campaign of online abuse transcends an attack on a particular individual’s rights and rises to the level of disrupting public order, this offense may be invoked as a last-resort characterization. This has been especially relevant when online violence goes offline or triggers broader unrest. For example, if netizens are incited to congregate offline and cause trouble due to an online controversy, or if an online harassment case results in mass incidents or panic, picking quarrels becomes a necessary legal tool to address the situation.

Indeed, the 2013 judicial interpretation on online rumors included a provision that *“using the information network to insult or intimidate others, with egregious circumstances, thereby disrupting social order”* should be punished as picking quarrels. This interpretive extension has provided a means to deter rampant online abuse. However, it has not been without controversy. Some observers worry that elevating conduct which primarily infringes personal reputation into an offense against public order may represent an unwarranted expansion of criminal law, potentially infringing upon freedom of expression. There is concern that what is essentially personal cyberbullying could be punished as a more serious crime simply by recharacterizing it as a public order issue.

Therefore, in practical application, authorities exercise caution and demand strict conditions for using this charge. The rule of thumb is that only if an online violence incident leads to a significant breakdown of public order should it be prosecuted as picking quarrels; ordinary cases of online group harassment should revert to charges like insult or defamation. A case-by-case analysis of consequences is necessary. For instance, if a particular online harassment incident causes widespread public outrage, triggers offline chaos (such as group gatherings, vigilante actions, or public panic), thus clearly extending beyond a private dispute and materially disturbing social order, it can be deemed as *“seriously disrupting public order,”* warranting the use of the picking quarrels offense. On the other hand, if the impact is confined to the online sphere – say, a localized social media uproar that does not spill into real-world disorder – it is generally not appropriate to up-charge it to a public order crime, lest the net of punishment be cast too broadly.

5. Legislative Reforms and Policy Recommendations

In view of the difficulties discussed above and the shortcomings in the current legal regime, it is necessary to adopt a multi-pronged approach spanning legislation, judicial interpretation, and broader social governance to improve the criminal law response to online violence.

5.1. Clarify Legal Definitions and Refine Criminalization Criteria

First, lawmakers or the judiciary should establish clear definitions related to online violence to guide enforcement uniformly. Consider incorporating a definition of online violence into a Criminal Law amendment or a new judicial interpretation – for example, a provision describing *“using the information network to commit acts of insult, defamation, privacy infringement, etc., which harm others’ rights”* – thereby delineating the scope and boundaries of punishable online violence. Additionally, it is crucial to sharpen the line between mere illegality and criminality by formulating detailed thresholds for what constitutes a crime in the online context.

Such standards should be both quantitative and qualitative. On the quantitative side, the outdated benchmarks for *“serious circumstances”* (like the number of views/reposts for rumors) should be updated to reflect the current scale of internet

activity, perhaps raising the numeric thresholds or contextualizing them (e.g. considering proportion of false information spread or speed of dissemination). But numbers alone should not be decisive; qualitative factors must also be emphasized – for instance, the malicious nature of the content, the severity of the consequences (did the victim suffer clinical psychological harm? did the incident spark wider disorder?), and the victim’s own experience of harm. By codifying such criteria, the law can resolve the current ambiguity at the margins of illegal and criminal behavior, enabling more precise targeting of truly harmful online conduct.

5.2. Optimize Judicial Interpretations to Unify Application

In tandem with legislative refinement, judicial authorities should make full use of judicial interpretations and guiding cases to fill in gaps and ensure consistent application of the law. It is advisable that the Supreme People’s Court and Supreme People’s Procuratorate issue updated guidance or an interpretation based on recent case experiences with online violence. Such guidance should focus on resolving practical uncertainties.

5.2.1. Distinguishing insult vs. public order offenses

Clearly articulate criteria for when online abusive conduct should be characterized as the crime of insult versus when it crosses into “picking quarrels and provoking trouble.” The interpretation could list typical scenarios that fall under insult (e.g. targeted harassment causing personal harm but no wider disturbance) and the exceptional scenarios that warrant treating it as a public order offense (e.g. harassment triggering large-scale public chaos). This would reduce the inconsistencies in charging decisions across different regions.

5.2.2. Updating defamation standards

Revisit the 2013 online defamation interpretation and adjust the quantitative metrics. In light of current internet usage, higher thresholds or additional factors should be introduced. For instance, specify that the existing view/share numbers are no longer ironclad indicators by themselves; instead, incorporate factors like *the context of dissemination, whether the rumor caused substantial public panic or directly resulted in severe victim harm*. Importantly, it should be stated that if an online rumor leads to extremely serious outcomes (such as the victim’s mental collapse or suicide), the case should be treated severely regardless of the precise click or share counts.

5.2.3. Interpretation on privacy breaches

Formulate a dedicated explanation for handling online privacy-invasion behaviors. This should clarify how “human flesh search” doxxing can meet the elements of the personal information crime. It might detail what constitutes “illegally obtaining/providing information” in an online context (for example, emphasizing lack of consent and method of acquisition) and flesh out the meaning of “serious circumstances” – considering factors like the sensitivity of the information exposed, the

extent of its spread, and the harm caused (e.g. tangible threats or losses suffered by the victim). Providing concrete benchmarks here will aid prosecutors and courts in tackling doxxing cases.

5.2.4. Addressing the prosecution of insults

Tackle the problem of under-enforcement due to procedural barriers by expanding the role of public prosecutions in serious online violence cases. The interpretation could establish that whenever online insults or defamation result in grave consequences – such as the victim suffering mental disorder, attempting suicide, or when the incident incites significant public disorder – those cases *should be* handled as public prosecutions by the procuratorate. By doing so, the burden on victims to initiate cases would be alleviated in the most severe instances, overcoming one of the key limitations of the current law.

Through such targeted judicial interpretations and by publicizing guiding cases that illustrate these principles, courts nationwide would have a clearer playbook when adjudicating online violence-related criminal cases. This would promote uniform evidentiary standards, conviction criteria, and sentencing ranges, thereby enhancing the timeliness, fairness, and authority of the judicial response to online abuse.

5.3. Refine Legislation to Balance Free Speech and Rights Protection

Governing online violence requires walking a fine line between safeguarding freedom of expression and protecting individuals' rights from egregious abuse. Lawmakers should uphold the principle of restraint in criminal law (*ultima ratio*) – meaning that not every offensive or intemperate online remark should be criminalized, to avoid chilling legitimate discourse or public supervision. The legal framework must not become a tool to suppress normal online criticism or satire that, while harsh, remains within socially tolerable bounds. For such general cases of rude speech, solutions should lie in ethical guidance, self-regulation, or administrative intervention, rather than criminal punishment. At the same time, for behavior that exceeds what the law can tolerate – sustained harassment, vicious personal attacks, or rumor-mongering that causes serious harm – the legal system must demonstrate zero tolerance and ensure that “the net of justice” does not let the perpetrators escape. To articulate this balance, legislative documents or judicial policy statements can reiterate that ordinary online speech, even if sharp-tongued, should not be subject to criminal sanctions, whereas malicious infringement of others' rights via the internet that causes major damage will be met with firm legal consequences.

In refining the law, caution must also be taken to prevent negative side-effects of over-expanding criminal law. Some scholars have warned that creating new offenses in reaction to each transient social phenomenon can lead to an incoherent criminal code and may result in symbolic legislation that is difficult to enforce. Thus, any move to criminalize online violence further should be based on thorough research and deliberation, ensuring it meshes well with the existing offense structure. For example, rather than introducing a broad and vague “online violence crime” which could overlap with multiple current crimes, a more measured approach would be to amend relevant provisions in the

Special Part of the Criminal Law – such as adding aggravating circumstances for crimes committed through networks, or adding specialized sub-clauses for typical online behaviors under existing articles. This approach conveys a clear message that the law will severely punish online violence, while preserving the internal consistency and logic of the criminal law.

5.4. Enforce Platform Responsibility and Leverage Technological Tools

Online platforms act as both amplifiers of harmful content and gatekeepers that can curb abuse; accordingly, they should bear commensurate legal and social responsibility in preventing and responding to online violence. It is recommended to strengthen platform obligations through both regulation and enforcement, as well as harness technology to aid governance:

On the regulatory side, existing laws like the Cybersecurity Law and the Personal Information Protection Law should be supplemented with more detailed requirements for platforms regarding online violence. For example, specify that when a platform detects a large-scale harassment incident, or receives a victim's complaint or a notice from authorities about such an incident, it must promptly take measures: delete or block infringing content, suspend or ban offender accounts, preserve evidence, and cooperate with investigations. Failure to timely fulfill these duties should expose the platform to administrative penalties and, in serious cases, criminal liability (via the refusal to perform network management duties offense discussed above). Recent rules, such as the 2024 CAC Provisions, already move in this direction by outlining content management and emergency response obligations for platforms. These need vigorous implementation.

On the enforcement side, regulatory agencies should institute routine oversight mechanisms. Major social media companies and forum hosts could be required to regularly report their handling of online violence incidents. Supervisory bodies can conduct inspections and, where a platform has had multiple serious incidents of online violence, summon its executives for warnings or publicize the platform's lapses. In egregious situations, regulators might impose joint sanctions (for instance, fines, suspension of certain features, or even temporary shutdowns) to press the point that negligence in curbing online abuse will not be tolerated. Internally, platforms ought to refine their community standards and invest in proactive monitoring and content moderation, using both human reviewers and AI algorithms to detect and filter out content that constitutes insults, defamation, or incitements to mob behavior.

In sum, reinforcing platform accountability and embracing technological solutions can significantly improve the effectiveness of online violence governance. Platforms are urged to actively act as the “first line of defense,” while regulators and law enforcement leverage advanced tools to supplement traditional methods. By combining strict legal liability for negligence with cutting-edge tech for evidence and tracing, the goal of more targeted and timely enforcement against online violence becomes attainable.

6. Conclusion

The challenge of determining criminal liability for acts of online violence shines a light on the novel tests facing legal systems in the digital age. This study has traced the concept and characteristics of online violence, analyzed the current predicaments in applying criminal law, and put forward targeted proposals for legislative reform and governance enhancements. In summary, the criminal justice approach to online violence must strike a balance: maintaining the restraint of criminal law while promptly expanding legal tools to address new forms of offenses. On one hand, it is essential to break the misconception that “the law will not hold the multitude accountable,” and to signal a stance of zero tolerance for egregious online abuse. On the other hand, overreach must be avoided – criminal law should not intrude too far into the domain of ordinary online expression, and citizens’ legitimate space for speech must be protected. Achieving this equilibrium requires legislators and judges to finely calibrate legal rules and standards: through improving offense provisions and issuing nuanced interpretations, scientific and reasonable thresholds for criminalizing online violence can be established.

In judicial practice, continuous experience and precedent-building will be invaluable. Courts and law enforcement should actively summarize lessons from typical cases, using them to clarify decision rules and unify the criteria for evidence, culpability, and sentencing. Over time, a body of jurisprudence can develop that lends greater predictability and fairness in handling online violence cases.

Looking to the future, the line between cyberspace and physical society will only continue to blur, and the manifestations and impact scope of online violence may further evolve. This implies that criminal law governance must also keep pace with the times. Advances in technology offer new avenues for precision prevention and control of online violence – for example, big data analytics to monitor public sentiment and identify brewing mob incidents, or blockchain tracing as discussed, to pinpoint the sources and spread of harmful posts. Such innovations can provide powerful support to law enforcement, making interventions more timely and evidence-based.

Ultimately, it will take the concerted effort of legislation, justice administration, regulatory oversight, and societal education to weave a tight net of rule of law against online violence. Under a continuously improving legal framework, online behavior will be more orderly and governed by clear norms, and citizens’ personal rights will enjoy genuine protection even in the virtual space. We have reason to expect that, with the safeguard of rule-of-law principles, a healthier and cleaner cyberspace will gradually take shape, and criminal law will fully play its role in upholding social order in the digital era.

These preventive and educational “soft measures” complement the “hard law” of criminal sanctions, working on the principle of addressing problems at the source. This echoes the spirit of the modern “Maple Bridge Experience,” which advocates resolving conflicts and risks at the grassroots level before they escalate. In the

online context, applying multiple strategies in concert – early prevention, self-regulation, community intervention, and then legal punishment as needed – is likely to yield better outcomes than relying on after-the-fact punishment alone. Only when legal regulation, industry self-discipline, and public oversight form a united front can online violence be effectively curbed at its roots.

Acknowledgements

This research was supported by the Anhui University of Finance and Economics Graduate Student Research Innovation Fund (Grant No. ACYC2023296). The author sincerely appreciates the financial support and resources provided by this fund, which significantly contributed to the successful completion of this research

References

- [1] Shi, J.-H. (2023) On the Essence of Cyber-Violence and Improvement of Criminal-Law Application Rules. *Legal Science (Journal of Northwest University of Political Science and Law)*, 41 (5), 69–82.
- [2] Feng, M.-Y. and Jiang, T. (2023) Criminal Regulation of the Abuse of Deepfake Technology. *Hubei Social Sciences*, 4, 127–135.
- [3] Li, W.-J. and Zhou, Y.-T. (2024) Criminal Regulation of Cyber Violence under the Trend of Petty-Offense Legislation. *Journal of Liaoning University (Philosophy & Social Sciences Edition)*, 3, 97–106.
- [4] Ouyang, B.-Q. (2024) Criminal Regulation of Cyber Violence from the Perspective of Victim Protection. *Jiangxi Social Sciences*, 1, 67–78.
- [5] Chen, R.-L. (2023) Criminal Governance of Cyber Violence and the Addition of New Offences. *Legal Science (Journal of Northwest University of Political Science and Law)*, 41 (5), 115–123.
- [6] Yu, C. (2023) Criminal Evaluation of Accumulative Online Insults and Defamation. *China Law Review*, 3, 87–98.
- [7] Tong, Y.-F. (2024) An Information-Propagation Crime Model for the Criminal Regulation of Cyber Violence. *Journal of Huazhong University of Science and Technology (Social Science Edition)*, 4, 46–59.
- [8] Liu, X.-Q. and Zhou, Z.-J. (2023) Difficulties and Solutions in the Criminal Regulation of Cyber Violence. *Legal Studies*, 5, 16–27.
- [9] Zhang, M.-R. (2025) On the Application of Criminal Law to Cyber-Violence Offenses. *Journal of Pingdingshan University*, 1, 29–34.
- [10] Chen, X. (2024) Difficulties and Relief of Criminal Regulation of Cyber Violence. *Journal of Qingdao Ocean Shipping Mariners College*, 45 (4), 17–22.
- [11] Li, M.-L. (2025) Alleviating the Dilemmas of Criminal Governance of Cyber Violence: Essence, Concepts and Pathways. *Chinese Journal of Maritime Law*, 36 (2), 105–117.
- [12] Li, S.-T. (2024) Criminal Regulation of Cyber Violence and Innovative Governance Paths in the Digital Era. *Jiangnan Forum*, 5, 56–65.
- [13] Zhang, J.-H. (2024) Criminal Governance of Cyber Violence in the Digital Age. *Jiangnan Forum*, 5, 45–55.
- [14] Wang, H.-W. (2024) Cyber-Violence Governance: Platform Responsibility and the Gatekeeper Role. *Jiaoda Law Review*, 3, 78–90.
- [15] Zhou, L.-B. (2023) Criminal-Law Governance of Cyber Violence Offenses. *Legal Studies*, 5, 38–51.
- [16] Leng, B.-Y. (2023) Criminal Governance of Accumulative-Danger Conduct in Group

Cyber Violence. *Legal Studies*, 5, 28–37.

- [17] Chu, C.-C. (2023) Evolution of Criminal-Law Responses to Cyber Violence and Its Fundamental Position. *Criminal Law Review of China*, 4, 35–52.
- [18] Zhang, Y. (2023) Criminal Responses to Offenses in Virtual Space. *Henan Social Sciences*, 26 (5), 66–71.
- [19] Sun, G.-X. (2023) On the Legitimacy and Limits of Accumulative Offenses. *Law Science*, 9, 64–80.
- [20] Liu, X.-H. (2023) Dilemmas and Countermeasures in the Criminal Regulation of Cyber Violence. *Beijing Social Sciences*, 5, 106–117.