

网络暴力行为的刑法规制研究

梅志娟

北京联合大学应用文理学院法律系，北京

发布日期：2026年8月24日

摘要

网络暴力已从个体失范演变为具有组织化、产业化特征的严重社会问题，现行以侮辱罪、诽谤罪为核心的刑法规制体系面临定义模糊、入罪门槛过高、因果关系认定困难、平台责任缺位等结构性困境。本文综合运用人格结构理论、传播学理论与刑法教义学方法，剖析网络暴力的成因、犯罪特征及现行规范体系的规制不足，比较借鉴域外立法经验，从法益保护与比例原则出发论证刑法介入的正当性，提出设立专门罪名、完善现有罪名构成要件、健全电子证据规则、强化平台刑事责任、完善自诉转公诉机关等路径，构建刑法与民事、行政、技术治理协同的多层次规制体系。

关键词

网络暴力；刑法规制；侮辱罪；诽谤罪；平台责任

Research on the Criminal Law Regulation of Cyber Violence

ZhiJuan Mei

College of Arts and Science of Beijing Union University, Beijing 100101, China

Abstract

Cyber violence has evolved from individual anomie into a severe social problem with organized and industrialized features. The existing criminal law regulation system, which centers on the crime of insult and the crime of defamation, is facing structural dilemmas including vague definition, excessively high criminalization threshold, difficulties in causation determination, and the absence of platform liability. Adopting personality structure theory, communication theory and criminal law dogmatics as research methods, this paper analyzes the causes and criminal characteristics of cyber violence as well as the regulatory shortcomings of the current normative system. By comparing and drawing on overseas legislative experience, this paper demonstrates the legitimacy of criminal law intervention based on legal interest protection and the principle of proportionality. On this basis, it puts forward targeted paths such as enacting a special criminal offense, improving the constitutive elements of existing crimes, refining electronic evidence rules, strengthening the criminal liability of online platforms, and optimizing the conversion mechanism

文章引用：梅志娟. (2026). 网络暴力行为的刑法规制研究. 法学年鉴, 1(3), 48 - 56.

ISSN Print: 3079-5389, ISSN Online: 3079-5397.

DOI: 10.63313/Law.8025

from private prosecution to public prosecution, so as to construct a multi-level regulatory system featuring the coordination of criminal law, civil remedies, administrative supervision and technical governance.

Keywords

Cyber Violence; Criminal Law Regulation; Crime of Insult; Crime of Defamation; Platform Liability

Copyright © 2026 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/>



1. 引言

随着互联网技术的深度发展，网络暴力已从零散的个体失范行为演变为具有组织化、产业化特征的严重社会问题。近三分之一的中国网民自称曾遭遇网络暴力，受害人抑郁、自杀等极端后果频发，其危害已从虚拟空间传导至现实社会，对公民人格权与网络公共秩序造成系统性破坏。

然而，我国现行规制体系呈现多法并行、条块分割的碎片化特征。刑事层面主要依托侮辱罪、诽谤罪、侵犯公民个人信息罪等传统罪名，存在法律定义模糊、入罪门槛过高、群体性攻击因果关系难以认定、平台责任缺位等结构性困境，导致处罚力度与暴力危害严重不匹配。民事赔偿与行政处罚等前置手段亦被实践证明难以有效遏制网络暴力蔓延。

在此背景下，刑法作为最后保障法的介入具有现实必要性与法理正当性。本文立足刑法教义学与比较法视角，剖析网络暴力的成因与犯罪特征，梳理现行规范体系的规制不足，论证刑法介入的正当性基础与基本原则，从立法、司法、执法及平台责任等维度提出系统性完善路径，构建刑法与多元治理手段协同的规制体系。

2. 网络暴力成因的理论研究

2.1. 弗洛伊德人格结构理论的解释路径

人类本性中固有的攻击性与欲望冲动在网络空间找到绝佳释放渠道。根据弗洛伊德人格结构理论，人格可以划分为本我、自我和超我三个部分，其中本我作为人格结构中最原始、最基础的部分，完全处于无意识层面，遵循快乐原则，不断追求本能欲望的即时满足，特别是攻击本能和性本能的宣泄。[1]死本能作为本我的重要组成部分，表现为指向外部的破坏性和攻击性冲动，构成网络暴力的深层心理驱动力。超我则代表内化的道德规范和社会价值观，依据道德原则对本我冲动施加抑制；而自我作为调节者，需依据现实原则平衡本我与超我的冲突。然而，网络空间的匿名性与虚拟性极大地弱化了超我的道德监督功能，现实社会中的道德压力因“去现实化”情境而显著减弱，个体不再感受到“被凝视”的压力，超我无法有效唤起道德焦虑以抑制本能冲动，这使得本我的攻击本能得以肆意释放。当个体置身于网络群体中，这种本能释放更因责任分散效应而加剧，形成集体性的暴力宣泄。[2]

网民往往使用不成熟的心理防御机制，如投射和合理化，将自身无法接受的负面情绪或特质强加于他人，并通过道德包装使暴力行为正当化。将自身的嫉妒或挫败感通过虚拟身份转移表达，本质上是一种死本能的转移性宣泄。[1]这种心理机制与网络传播特性结合，造就了网络暴力特有的集体无意识现象，即个体在群体中丧失独立思考能力，成为暴力浪潮的推波助澜者。

2.2. 传播学视角下的异化机制

网络暴力本质上是一种异化的传播行为，其特殊传播机制助长了暴力升级。网络传播的即时性、交互性与去中心化特点，使得信息传播过程中出现严重失真与扭曲。[3]古典群体行为理论指出，个体在融入群体后会经历“去个性化”状态，即自我身份意识减弱和个人责任感消退，从而更易接受群体暗示并表现出非理性、情绪化与攻击性行为。社会认同模型进一步阐明，匿名性并非导致个体身份消失，而是促使个体从“个人身份”转向“社会身份”，即参与者会认同于“攻击者群体”这一临时形成的社会类别，并主动遵从该群体内部新兴的行为规范，如对特定目标进行集体贬损。[4]

传播内容的娱乐化倾向进一步加剧了这种异化，暴力行为被包装成娱乐消费产品，削弱了人们对暴力严重性的认知。[5]同时，网络传播的间接性特征使得施暴者无法直接感知受害者的痛苦，造成危害模糊性认知，从而降低道德约束。[3]社会传染理论为此提供了动力学解释：负面情绪和行为可通过社交网络节点快速渗透并感染大量用户，形成行为模仿与情绪共振的双重传染回路。[6]这种传播机制最终形成恶性循环：暴力内容获得更多关注与传播，平台算法进一步推送类似内容，不断强化暴力的扩散与升级。

2.3. 宏观社会结构的催化作用

我国特定的社会结构与环境为网络暴力提供了滋生土壤。社会转型期产生的结构性紧张与相对剥夺感，使部分群体积压大量负面情绪，网络成为其宣泄窗口。当前中国社会正处于深刻的社会转型期，其特征是社会结构发生整体性、根本性的变动，虽然推动了经济的飞速发展，但也必然伴随着各种社会矛盾的积累与结构性的张力。社会学家将这种状态描述为“风险社会”，即现代化进程本身产生了大量系统性、制度性的风险，这些风险的无序释放构成了社会不稳定的重要来源。[7]

传统社会控制机制在网络空间的弱化，使得道德与法律约束力显著降低，而新的网络行为规范尚未完全建立。与此同时，网络商业化运作模式客观上鼓励冲突与对立，因为极端内容往往能带来更高流量与参与。我国特有的城乡二元结构及其衍生的数字鸿沟也在网络行为中留下深刻烙印：城乡之间、代际之间以及不同教育背景的网民在数字资源获取、媒介使用能力和话语表达方式上存在显著差异，这种线上延展的社会分层不仅加剧了群体间隔阂与误解，也在特定议题讨论中易引发基于身份标签的攻讦和排斥。[8]这种宏观社会环境与个体心理机制的交互作用，创造了网络暴力滋生与蔓延的温床，使得冲突几乎不可避免。

3. 网络暴力犯罪的特征分析

3.1. 道德伪饰下的暴力本质

网络暴力最显著的特征在于其伪正义性，施暴者往往自以为站在道德制高点。这种自以为是的“正义”对“非正义”的讨伐，实质上是对个体展开的大型围剿活动。施暴者通过道德标签化手段，将被攻击对象置于道德对立面，从而合理化自身的暴力行为。这种道德伪饰机制与弗洛伊德理论中的心理防御机制高度吻合，即通过投射和合理化将自身攻击欲望包装成道德追求。在实际操作中，施暴者常采用“替天行道”的话语框架，将私人恩怨上升为道德审判，使得暴力行为获得某种形式的精神合法性。[9]例如，在“粉色头发女孩”事件中，网民以“维护传统”为名，对当事人进行道德审判和人身攻击，实则是对异己者的排斥本能和现实挫败感的转移表达。这种表面正义实则暴力的行为，借助群体声势掩盖其施虐本质，形成一种集体伪善的暴力狂欢。道德脱离机制在此过程中发挥关键作用：个体通过责任转移——将暴力归因于“群体行为”、道德辩护等方式，解除内在道德约束，使暴力行为得以持续和升级。

3.2. 群体暴力中的原始恶意释放

网络暴力呈现出多对一的攻击模式，散发着人类最原始的集体恶意。这种群体暴力具有明显的去个体化特征，个体在群体中丧失自我识别和自我约束能力，表现出平时不会有的极端行为。群体极化和群体思维效应进一步加剧了这种恶性发展，使得群体成员观点不断趋向极端，并形成对内一致对外排斥的封闭思维模式。勒庞所描述的“群体心理”在此得到充分体现：个体在群体中变得冲动、易受暗示且缺乏判断力，情绪与行为在“循环反应”中不断相互刺激并强化。而今网络暴力已呈现组织化、黑产化发展趋势，形成完整的暴力产业链条，包括人肉搜索、信息贩卖、有组织谩骂等专业化分工。[10]这种有组织的群体暴力不仅危害性更大，而且更难追溯和规制。根据《第52次中国互联网络发展状况统计报告》，近三分之一的中国网民自称曾遭遇网络暴力，这种有组织的群体暴力不仅危害性更大，而且更难追溯和规制。

3.3. 从虚拟伤害到现实后果的传导

网络暴力最致命的特征在于其能够造成切实的物理伤害和心理创伤，带来惨烈后果。虚拟世界的暴力通过多种途径向现实世界传导：一是直接导致受害者心理健康问题，如抑郁、焦虑甚至自杀倾向；二是影响受害者的社会关系与职业发展，造成社会性死亡；三是引发线下暴力事件，如网络暴力引发的现实冲突和报复行为。这些后果的严重程度往往远超预期，且具有不可逆性。事件发生频次之高与后果之严重触目惊心，显示出网络暴力绝非隔靴搔痒的暴力手段，而是具有实质破坏性的社会问题。[11]

从刑法学视角审视，网络暴力所致危害结果呈现显著的精神性和弥散性特征。被害人因遭受持续贬损和舆论审判而产生严重心理创伤、社会评价急剧降低，甚至引发抑郁或自杀等极端后果。然而，尽管损害结果切实发生，在刑法归责上却难以确立具体行为与损害后果之间的因果关系。一方面，群体性攻击呈现“多因一果”的形态，单一网络言论与最终危害——比如被害人自杀之间往往无法通过传统因果关系理论进行独立和充分的法律评价；另一方面，其间常介入被害人自身心理特质、其他环境因素或其自由意志决定，进一步复杂化因果链条的判断。司法实践中即便出现严重后果，亦常因无法将结果归责于特定行为人的具体行为，而只能将严重后果作为量刑情节予以考量，反映出当前刑法框架在面对新型数字暴力行为时存在的结构性困境与规制限度。[12]

4. 网络暴力规制的规范体系梳理

4.1. 我国现行法律规制框架

我国对网络暴力行为的规制呈现多法并行、条块分割的特征，尚未形成有机统一的规范体系。在刑事法律层面，《刑法》主要通过第二百四十六条侮辱罪、诽谤罪、第二百五十三条之一侵犯公民个人信息罪等罪名对网络暴力进行规制。侮辱罪和诽谤罪要求行为必须达到“情节严重”方可入罪，2013年《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》明确了“情节严重”的认定标准，如诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上。侵犯公民个人信息罪则针对非法获取、出售或提供公民个人信息的行为，为打击“人肉搜索”提供了法律依据。

《治安管理处罚法》则对尚未构成犯罪但具有社会危害性的网络暴力行为进行行政处罚，如第四十二条规定对公然侮辱他人或捏造事实诽谤他人的行为，处五日以下拘留或五百元以下罚款；情节严重的，处五日以上十日以下拘留，可以并处五百元以下罚款。在专门立法方面，《网络安全法》第四十七条确立了网络运营者的“通知-删除”义务，要求其加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散。《个人信息保护法》则为个人信息保护提供了专门法律依据，明确任何组织、个人不得非法收集、使用、加工、

传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

此外，最高人民法院、最高人民检察院和公安部联合发布的《关于依法惩治网络暴力违法犯罪的指导意见》试图细化网络暴力的认定标准和处罚原则，明确规定在“严重危害社会秩序”情况下，网络侮辱、诽谤案件可以由检察机关提起公诉，特别是“造成被害人或者其近亲属精神失常、自杀等严重后果的”等情形属于“严重危害社会秩序”。2024 年施行的《网络暴力信息治理规定》作为首部专门性部门规章，首次对“网络暴力信息”作出定义，并系统设定平台的事前预防、事中响应和事后处置义务。然而，这种多法并存的规制模式存在明显的碎片化和重叠性问题，缺乏统一的适用标准和实践框架。

4.2. 规制实践中的困境与不足

现行规制体系在实际运行中面临诸多困境，导致处罚力度与暴力行为强度严重不匹配。首要问题在于网络暴力的法律定义模糊，缺乏明确的概念界定和构成要件标准。虽然在《网络暴力信息治理规定》中将网络暴力信息定义为“通过网络对个人集中发布的，侮辱谩骂、造谣诽谤、侵犯隐私等违法和不良信息”，但这一定义仅停留在部门规章层面，未被上升至法律层面，导致司法实践中认定困难，不同法院对类似案件可能作出截然不同的判决。

刑事门槛设置过高，如侮辱罪、诽谤罪的入罪标准难以适应网络暴力的危害特性。尽管 2013 年司法解释设定了“500 转、5000 点击”的入罪标准，但在群体性网络暴力中，单一行为的传播量可能不足，但整体危害却极其严重，这使得刑事追责面临结构性困难。再次，取证难、溯源难等技术性障碍使得许多网络暴力行为无法得到有效追责。网络匿名性和跨平台传播特性使得侵权主体难以特定化，证据固定高度依赖技术手段与平台协助，而受害者往往缺乏相应的技术和资源支持。[13]平台责任界定不清导致事前预防机制缺位，平台往往缺乏主动干预和防止网络暴力的动力。虽然《网络安全法》和《网络暴力信息治理规定》明确了平台的内容管理义务，但实践中平台审核标准不一，执行力度差异较大，缺乏统一规范的标准指引。

4.3. 国外法律实践的对比借鉴

对比国外网络暴力规制实践，我国现行方式显得相对保守和滞后。美国通过《通信规范法》第 230 条为网络平台提供责任豁免，规定互动计算机服务的提供者或用户不应被视为另一信息内容提供者所提供的任何信息的发布者或发言人，这为平台提供了广泛的免责保护。但同时，美国通过《反网络欺凌法》等专门立法强化对特定网络暴力行为的规制，部分州还通过了针对网络骚扰和欺凌的刑事立法，如加利福尼亚州刑法第 653.2 条将通过电子通讯设备重复实施骚扰行为规定为犯罪。

欧盟则通过《通用数据保护条例》确立严格的数据保护原则，并从源头减少网络暴力依赖的个人信息泄露风险。《通用数据保护条例》要求数据控制者和处理者实施严格的数据保护措施，违反者将面临高达全球年营业额 4% 的罚款。此外，欧盟《数字服务法》引入了平台问责制，要求大型在线平台采取风险缓解措施并接受独立审计。日本和韩国等亚洲国家则更注重平台责任和事前预防，要求平台建立完善的举报和处理机制。日本 2014 年通过的《网络欺凌对策推进法》要求学校和地方政府采取防止网络欺凌的措施，并为受害者提供支持。韩国则实行网络实名制，并通过《信息通信网利用促进及信息保护法》对网络暴力行为进行规制，要求平台及时删除有害信息并向当局报告。这些域外经验显示，有效的网络暴力规制需要专门立法、平台责任和司法救济等多管齐下，而我国目前在这些方面均存在明显不足。特别值得注意的是，许多国家已经认识到网络暴力的特殊危害性，并通过降低入罪门槛、强化平台责任等方式加大规制力度，这与我国相对保守的规制手段形成鲜明对比。[14]

5. 网络暴力刑法规制的完善路径

5.1. 刑法介入的正当性基础

网络暴力行为的社会危害性已远超一般违法范畴，必须通过刑法这一最后保障法进行规制。从法益保护角度深入分析，网络暴力呈现出复合性法益侵害特征：它不仅直接侵害公民个人的名誉权、隐私权、个人信息权等具体人格权，更对网络空间公共秩序与社会安全感造成系统性破坏。这种法益侵害的广泛性与深刻性完全符合刑法所保护的法益范畴。具体而言，刑法中的法益保护原则要求对重大社会利益提供最强有力的保障，而当某项利益具有重要社会价值且面临严重威胁时，刑法的介入就具有正当性。网络暴力导致的部分案件中出現受害人自杀、严重精神疾病等不可逆的损害后果，其危害程度与传统犯罪行为相当，甚至因其传播范围的无限性和损害的持续性而显得更为严重。[11]

从比例原则视角审视，刑法介入的必要性得以进一步证成。比例原则作为公法领域的黄金原则，要求国家权力的行使必须适当、必要且合乎比例。在网络暴力规制领域，当民事赔偿、行政处罚等前置法律手段已被实践证明无法有效遏制网络暴力蔓延时，作为最后保障法的刑法介入就显示出其必要性。值得注意的是，网络暴力往往具有跨地域、隐蔽性强、证据易消失等特点，传统法律救济手段面临举证难、追溯难等现实困境，这使得刑法介入更具有紧迫性。[15]

随着互联网技术的深度发展，网络暴力已经呈现出明显的组织化、产业化发展趋势。这种新型网络暴力已不再是简单的个体失范行为，而是演变为具有完整产业链条的黑产模式，包括专业化的信息搜集团队、内容制作群体和传播推广组织。这种组织化特征使得网络暴力的危害性呈几何级数增长，也使其完全符合犯罪行为的本质特征。刑法作为社会控制的重要手段，必须对这种新型犯罪行为作出及时回应。从比较法视角观察，世界各国对网络暴力的刑法规制呈现出不断加强的趋势。这些立法动向都反映了国际社会对网络暴力危害性的共识。我国刑法作为社会主义法律体系的重要组成部分，应当与时俱进地完善对网络暴力的规制，这既是保护公民合法权益的需要，也是维护网络空间秩序的必然要求。[14]

此外，从刑法理论的发展演变来看，现代刑法正在经历从传统法益保护向风险预防功能的转型。网络暴力作为一种新型社会风险，其潜在危害具有不可预测性和广泛扩散性，这就要求刑法适当提前介入时点，建立预防性的刑法规范体系。当然，这种预防性刑法的构建必须严格遵循法治原则，避免过度犯罪化倾向。通过设置适当的危险犯形态，将具有严重社会危害性的网络暴力行为纳入规制范围，既符合刑法发展的时代要求，也能够有效应对网络暴力带来的新型社会风险。[16]

5.2. 刑法规制的基本原则构建

构建网络暴力刑法规制体系必须建立在坚实的刑法基本原则基础之上。罪刑法定原则作为刑法的基石原则，要求对网络暴力的界定必须明确、具体，避免使用模糊性表述导致刑罚权的滥用。具体而言，应当在立法层面明确网络暴力的概念界定、构成要件要素和法律效果，确保法律规定的明确性和可预测性。这种明确性要求不仅体现在实体规范的制定上，也需要在程序规则层面作出相应安排，包括证据认定标准、侦查取证程序等都需要符合法治原则的要求。在网络环境下，罪刑法定原则的实现面临新的挑战，因为网络行为的多样性和复杂性使得法律规范的明确性难以完全实现。这就需要立法者采用概括性规定与示例性列举相结合的方式，既保持法律规范的适应性，又确保其具有足够的明确性。

法益保护原则要求刑法介入必须建立在确切的法益侵害基础之上。就网络暴力而言，需要准确识别和界定其侵害的法益类型和程度。个人法益方面包括名誉权、隐私权、个人信息权以及心理健康权等；超个人法益方面则包括网络空间公共秩序、社会安全感等集体法益。在平衡保护不同法益时，需要特别注意处理刑法保护与言论自由之间的关系。言论自由作为宪法保障的基本权利，其限制必须谨慎而合理。

刑法对网络暴力的规制应当针对那些明显超出言论自由边界的恶意行为，而非一般性的网络表达。这就需要建立明确的界限区分标准，通过类型化的方法将网络暴力行为与正当的网络表达区分开来。

比例原则在网络暴力刑法规制中具有特殊重要性。这一原则要求刑事立法和司法必须遵循适当性、必要性和相称性三个子原则。适当性原则要求刑法措施必须能够有效实现规制网络暴力的立法目的；必要性原则要求在多种可选的规制手段中选择对公民权利限制最小的方式；相称性原则则要求刑法介入的强度必须与网络暴力的危害程度相匹配。在网络暴力刑法规制中，应当根据行为的社会危害性设置梯度化的刑罚体系，从罚金、社区服务到有期徒刑形成层次分明的法律责任体系。特别是在设置法定刑时，需要充分考虑网络暴力的特殊危害性，避免刑罚过轻导致威慑不足，也要防止刑罚过重违背罪责刑相适应原则。

谦抑性原则要求刑法保持适当克制，仅对具有严重社会危害性的网络暴力行为进行规制。这一原则强调刑法的补充性地位，即只有当其他法律手段无法有效规制时，刑法才能介入。在网络暴力治理中，应当建立“民事救济-行政监管-刑事处罚”的三层治理体系，刑法仅作为最后保障手段发挥作用。同时，谦抑性原则也要求司法实践中对网络暴力犯罪的认定采取审慎态度，避免刑法过度介入网络空间而抑制正常的网络交流与表达。在具体案件中，需要严格区分网络暴力与网络纠纷、网络暴力与不当言论等相似但性质不同的行为，确保刑法只在必要范围内发挥作用。[11]

责任主义原则在网络暴力语境下的适用。这一原则要求刑事责任的承担必须以行为人具有主观罪过为前提。在网络暴力案件中，由于参与主体众多、行为方式复杂，准确认定各行为人的主观故意程度具有较大难度。这就需要司法实践中发展出适合网络环境的责任认定标准，既不能过度扩大打击范围，也不能轻纵具有严重恶意的行为人。对于网络暴力中的帮助行为、教唆行为等参与形态，也需要建立明确的刑事责任认定标准，确保罪责认定符合个人责任原则。

考虑程序正当原则在网络暴力案件中的适用。网络暴力案件往往涉及大量电子证据，这些证据的收集、固定和运用都需要遵循严格的程序规范。特别是在跨境取证、技术侦查等特殊侦查手段的运用上，必须严格遵守法律规定，保障当事人的合法权益。同时，网络暴力案件的审理也需要考虑被害人的特殊保护需求，建立适合网络环境的新型诉讼程序，确保案件审理既公正高效，又能充分保护各方当事人的合法权益。[12]

5.3. 具体规制路径的完善建议

完善网络暴力刑法规制需要从立法、司法和执法三个层面进行系统性的制度设计。在立法层面，当务之急是考虑设立专门的网络暴力罪名，构建符合网络暴力特征的构成要件体系。基于网络暴力的复合性特征，新罪名应当采用概括性规定与具体行为类型列举相结合的方式。概括性规定明确网络暴力的本质特征是对他人实施网络欺凌、骚扰或恐吓，造成严重后果或具有严重危险的行为；具体行为类型则应当包括人肉搜索、网络诽谤、恶意举报、虚拟追杀等典型网络暴力形式。在构成要件设计上，应当充分考虑网络环境的特殊性，适当降低入罪门槛，如将“情节严重”的标准从现实世界的物理损害扩展到心理创伤、社会评价降低等非物质性损害。

对现有罪名的修订完善同样重要。就侮辱罪而言，应当明确网络环境下“公然”要件的认定标准，将具有一定关注度的网络空间纳入公然范畴；对于诽谤罪，需要完善虚假信息的认定标准，建立专门的技术鉴定机制。侵犯公民个人信息罪则需要进一步扩大个人信息保护范围，将网络暴力中常见的社交关系、行为偏好等信息纳入保护范围。同时，应当考虑增设网络平台刑事责任条款，明确平台在明知或应知网络暴力发生时的作为义务。平台作为网络空间的重要管理者，应当承担起相应的安全管理责任，对于怠于履行管理职责导致网络暴力扩散的，应当承担相应的刑事责任。

司法层面的完善需要重点关注证据规则的适应性问题。网络暴力案件中的电子证据具有易篡改、易消失的特点，需要建立专门的电子证据收集、固定和认定规则。建议最高人民法院出台网络暴力案件证据规则司法解释，明确电子证据的取证程序、鉴定标准和证明力认定规则。同时，应当探索建立技术专家陪审员制度，在复杂网络暴力案件审理中引入专业技术人士参与事实认定。在证明标准方面，可以考虑采用差异化的证明标准，对于主观故意等难以直接证明的要件，允许通过间接证据进行推定，但必须设置严格的推定条件和反驳机制。

统一裁判标准是司法实践中的另一个重要议题。目前各地法院对网络暴力案件的定罪量刑存在较大差异，影响了法律适用的统一性和权威性。建议最高人民法院发布网络暴力犯罪典型案例，通过指导性案例的方式统一法律适用标准。特别是对“情节严重”、“造成严重后果”等规范性构成要件要素，需要明确具体的判断标准和考量因素。可以考虑建立网络暴力案件量刑指导系统，通过大数据分析和技术手段，为法官提供量刑参考，促进量刑规范化。[17]

执法层面需要加强公安机关的网络执法能力建设。网络暴力案件侦查涉及电子数据提取、网络身份溯源、跨地域取证等专业技术要求，需要配备专业网警队伍和技术侦查设备。建议在网安部门设立专门网络暴力查处科室，建立快速响应机制，防止证据灭失。同时，需要完善跨区域警务协作机制，解决网络暴力案件管辖冲突和取证难问题。对于跨境网络暴力案件，还需要加强国际执法合作，通过司法协助条约等机制解决跨境取证和犯罪嫌疑人引渡等问题。

平台责任机制的完善是遏制网络暴力的关键环节。应当通过立法明确网络服务提供者的安全管理义务，包括内容审核机制、投诉处理机制和证据保存机制等。对于未履行必要管理义务导致网络暴力扩散的平台，应当承担相应的行政责任乃至刑事责任。同时，建立平台与司法机关的协作机制，要求平台在发现涉嫌犯罪的网络暴力行为时，及时向公安机关报告并保存相关证据。平台还应当建立用户信用评价体系，对实施网络暴力的用户采取限制功能、暂停服务直至永久封号等措施，形成平台内部的自律机制。

刑事自诉转公诉机制的完善对保护受害人权益具有重要意义。网络暴力受害人往往面临取证难、维权成本高等困境，自诉方式难以有效维权。建议修改刑事诉讼法，明确网络暴力案件可以适用公诉程序的情形和标准。对于造成被害人自杀、精神失常等严重后果的案件，或者涉及组织化、产业化的网络暴力行为，即使被害人未提起自诉，检察机关也可以直接提起公诉。同时，应当完善被害人援助制度，为网络暴力受害人提供法律咨询、心理疏导等全方位支持，帮助其更好地维护自身权益。建立网络暴力犯罪记录制度，将网络暴力犯罪纳入行为人犯罪记录系统。这对于预防重复犯罪和累犯具有重要作用。同时，可以考虑建立网络暴力犯罪行为入教育矫正制度，通过强制参加网络法治教育课程、社区服务等方式，帮助行为人认识错误、改正行为，预防再次犯罪。对于未成年人实施网络暴力的，应当建立专门的教育矫正机制，侧重教育和挽救，避免简单的惩罚性措施。还需要加强网络暴力刑法规制的监督评估机制。建立网络暴力案件数据库，定期对网络暴力犯罪的趋势、特点和处理效果进行分析评估。通过立法后评估等方式，及时发现和解决法律适用中的问题，不断完善网络暴力刑法规制体系。同时，建立公众参与机制，通过网络问卷、专家论证等方式，广泛听取社会各界对网络暴力治理的意见建议，确保刑法规制措施既有效又适当。

5.4. 刑法与其他治理手段的协同

刑法规制并非万能，必须与其他治理手段形成协同效应。民事赔偿制度应作为刑法的重要补充，为受害人提供经济救济。行政监管应发挥事前预防作用，通过平台监管、内容审核等手段减少网络暴力的发生。技术治理应成为基础性手段，通过算法优化、内容识别等技术措施主动防范网络暴力。行业自律同样不可或缺，网络平台应建立行业标准和最佳实践，形成自我约束机制。最后，社会教育是根本之策，

应加强网络素养教育和道德建设,从源头上减少网络暴力的产生。这种多层次、全方位的治理体系才能真正有效应对网络暴力这一复杂社会问题,而刑法在这一体系中扮演着不可或缺的最后保障作用。

参考文献

- [1] 陈选华,寇杰,高翩.精神分析视角下的社会网络暴力行为主体分析[J].湖南行政学院学报,2019,(4):73-78.
- [2] 谭婷.基于精神分析理论探析网络暴力事件成因——以乔任梁死亡事件为例[J].西部广播电视,2017,(14):80-81.
- [3] 陈长松,陆虎成.“网络爆破”的特征、危害与治理初探[J].教育传媒研究,2023,(5):69-71.
- [4] 兰玉娟,佐斌.去个性化效应的社会认同模型[J].心理科学进展,2009,17(2):467-472.
- [5] 葛宸希.网络暴力问题的法理分析及治理对策[J].佳木斯大学社会科学学报,2022,40(6):51-54.
- [6] 张宝生.地方政府网络舆情综合治理体系构建及治理能力提升策略研究.黑龙江省,哈尔滨师范大学,2022-12-03.
- [7] 陈小强.中国转型期网络信息不确定性现象的社会学研究[D].中共中央党校,2015.
- [8] 侯玉波,李昕琳.中国网民网络暴力的动机与影响因素分析[J].北京大学学报(哲学社会科学版),2017,54(1):101-107.
- [9] 刘紫川,桂勇,黄荣贵.“暴”亦有“道”?青年网暴实践的特征及价值基础[J].新闻记者,2023,(9):3-18+96.
- [10] 袁韬.自媒体时代网络暴力行为的刑法规制及其完善[J].河南开放大学学报,2024,37(2):48-53.
- [11] 黄亚瑞.“网络暴力”刑法规制研究[D].西南政法大学,2021.
- [12] 蔡荣.“网络语言暴力”入刑正当性及教义学分析[J].西南政法大学学报,2018,20(2):63-72.
- [13] 王子晨,汤艳君,潘奕扬.面向取证的网络攻击者溯源分析技术研究综述[J].信息安全研究,2024,10(4):302-310.
- [14] 李俣然.网络暴力犯罪规制研究[D].南京财经大学,2023.
- [15] 肖圣乾.网络暴力行为刑法规制的实证研究[D].青海师范大学,2024.
- [16] 劳东燕.风险社会与功能主义的刑法立法观[J].法学评论,2017,35(6):12-27.
- [17] 徐伟,李睿恒.网络暴力的治理逻辑与优化建议——基于2009—2024年政策文本的扎根分析[J].重庆大学学报(社会科学版),2025,31(2):267-279.