

Doi:10.11835/j.issn.1008-5831.fx.2024.10.003

欢迎按以下格式引用: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(2):267-279. Doi:10.11835/j.issn.1008-5831.fx.2024.10.003.



Citation Format: XU Wei, LI Ruiheng. The governance logic and optimization suggestions of network violence: Based on the grounded analysis of policy texts from 2009 to 2024[J]. Journal of Chongqing University (Social Science Edition), 2025 (2):267-279. Doi:10.11835/j.issn.1008-5831.fx.2024.10.003.

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

徐伟¹,李睿恒²

(1. 重庆邮电大学,重庆 400065;2. 公安部第三研究所,上海 201210)

摘要:依法规制网络暴力是新时代网络空间治理的核心目标。当前我国在这一领域的法律法规散见于各类不同性质和层级的立法文件中,导致了法律条文的碎片化、交叉重叠甚至相互矛盾的现象。这种法律体系的分散性和不一致性,不仅影响了法律的实施效果,还在具体操作中造成了责任不清、执行困难等问题。因此,系统梳理现有政策文本,分析其中的治理框架及其潜在问题,已成为提升网络暴力治理水平的当务之急。收集2009年至2024年间我国颁布的22份关于网络暴力治理的政策文件,运用程序性扎根理论对数据进行对比和分析,凝练出相关概念、范畴,最终构建了治理逻辑框架。研究表明,我国已经初步建立了三大网络暴力治理机制:综合治理机制、司法治理机制和长效治理机制。首先,在事中治理阶段,国家通过明确政府、平台和用户等主体的责任,形成了多层次、多方参与的综合治理机制。各方通过有效协作,推动网络暴力治理的全程参与和技术支持。这一机制在化解技术风险方面显示出较强的协同作用,但在社会风险的成因分析和应对方面尚有不足。其次,事后治理阶段的司法机制,通过精细化的法律解释,实现了民事、行政和刑事法律之间的有效衔接。该机制确保了网络暴力行为可以在不同法律框架下获得司法救济,但在具体实践标准上仍有待细化。尤其是在民事、行政和刑事诉讼之间,缺乏统一的实践理论,导致实践中可能出现衔接困难。最后,国家构建了以制度化为核心的长效治理机制,确保网络暴力治理可以持续、有效地应对不同情境下的网络暴力问题。通过流程化的安排,该机制能够对网络暴力问题做出迅速反应并提供长期的解决方案。然而,关于“平台权力”的监管仍然存在不足,尤其在如何有效监督平台履行其治理责任方面,法律条文尚不完善。总结而言,未来的治理方向应包括:强化对网络暴力的社会风险防控,进一步细化司法治理机制的实践标准以及完善对平台权力的监管机制,以推动我国网络暴力治理的法治化与现代化,构建更加完善的网络空间治理体系。

关键词:网络暴力;综合治理;司法治理;长效治理;网络空间治理

中图分类号:D922.16;D924.1 **文献标志码:**A **文章编号:**1008-5831(2025)02-0267-13

基金项目:国家社会科学基金重大项目“健全网络综合治理体系研究”(23ZDA086)

作者简介:徐伟,法学博士,重庆邮电大学网络空间安全与信息法学院特聘教授,Email:lawxuwei123@163.com。

一、问题的提出

网络空间已升级为一种全新的公共活动领域,孕育了多样化的公共参与方式^[1]。以网络空间为依托的数字经济已成为新质生产力形成和发展的重要一环^[2]。然而,传统空间中的暴力现象也以一种崭新的形式延伸至网络空间^[3]。网络暴力是指在网络空间中肆意利用言语信息诋毁、谩骂、攻击、伤害他人或者随意处置他人个人信息,从而给他人造成心理强制和精神压迫,情节严重的行为^[4]。网络暴力的发生和传播引发了网络空间的混乱,甚至导致一些悲惨的自杀事件。

习近平总书记强调,“网络空间是亿万民众共同的精神家园”,要“加快建立网络综合治理体系,推进依法治网”^[5]。在此背景下,最高人民法院、最高人民检察院、公安部、中央网信办等多主体接连出台了《关于切实加强网络暴力治理的通知》(以下简称《通知》)、《关于依法惩治网络暴力违法犯罪的指导意见》(以下简称《意见》)、《网络暴力信息治理规定》(以下简称《规定》)等多部政策文本,旨在加大网络暴力治理力度,完善网络暴力治理体系。然而,我国网络暴力治理领域的法律法规散见于不同性质和层级的立法文本中,存在严重的碎片化、交叉重叠甚至矛盾的现象^[6]。法规的碎片化和交叉状态不仅对网络空间治理的效果造成损害,也加大了治理的复杂性和成本^[7]。针对这一突出问题,本文以扎根理论为理论基础,对2009年至2024年22份关键法律法规文本进行深度质性分析,旨在全面梳理和构建我国网络暴力治理逻辑及相关问题。这不仅有助于解决法规碎片化和交叉规制问题,更为我国网络暴力的政策研究和治理实践提供了清晰而系统的政策图景。

二、网络暴力治理的文献回顾

围绕网络暴力治理政策和模式,学界开展了广泛研究,主要集中在三个方面。

第一,在分析网络暴力治理的法教义学框架方面,喻海松指出,现有框架形成了整体的民事、行政和刑事责任体系,但具体的衔接问题仍然存在疑难^[8]。为解决这一问题,蔡鹏程提出在法教义学框架内应用解释论,通过价值判断和比例原则来填补其不足^[9]。陈罗兰从立法论的角度建议通过设立新的网络暴力罪来完善法律框架^[10]。同时,石经海和黄亚瑞认为现行刑法对于新型网络暴力行为规制缺位,呼吁采用解释论明确个罪的界限,构建刑事规则限度理论^[11]。

第二,在涉网暴技术治理模式分析方面,技术治理被划分为限制“技术作恶”和运用技术治理网络暴力信息内容两个层面。路鹃和张君昌认为我国应完善技术思维和平台逻辑,夯实平台技术治理责任^[12]。赵韫淏和刘晶通过调研建议在实践中建立事前检测预防、事中干预处置、事后惩治救济的技术治理机制^[13]。张钦坤和曹建峰提出我国在技术监管层面需要明确“疏堵结合、包容审慎、敏捷灵活”的宏观理念,以平衡安全和发展的两大需求^[14]。

第三,在分析网络暴力的协同治理模式方面,周葆华和罗沛基于国家宏观治理功能、平台媒体等中观控制功能以及个人的微观调节功能,构建了一个多元共治体系^[15]。刘绩宏基于网络暴力演化机制认为,应发挥政府的信息澄清功能、社会的意见引导功能和个人的道德理性功能,在根源阶段阻止网络暴力的发生^[16]。冉连和张曦指出解决多元主体共治合力不足问题的关键在于完善多主体共建共治共享的治理模式制度设计,通过综合责任分配和功能协同构建一种互信互赖的合作共治模式^[17]。

综上所述,学术界在网络暴力治理领域的研究取得了显著进展。但其中大多数仍以当时新颁布的某一单独政策文本为分析对象,未能系统审视相关问题,缺乏体系化的深入分析。为弥补这一不足,有必要对现有零散的政策文本进行系统梳理,以清晰勾画网络暴力治理的体系脉络。

三、网络暴力治理的政策来源与研究方法

(一) 网络暴力治理政策来源

政策文本的筛选过程如下:在北大法宝、威科先行等数据库中以关键词“网络”“暴力”“造谣”“诽谤”进行检索。通过这一过程,筛选出的政策文本在一定程度上能够代表国家在多个领域对网络暴力治理的政策取向。根据上述政策文本收集标准,本研究选取了22份政策文本作为编码资料(详见表1)。

表1 编码政策文本列表

效力位阶(数量)	文件名称(发布年份)
法律(2)	《中华人民共和国未成年人保护法》(2024)、《中华人民共和国个人信息保护法》(2021)
行政法规(3)	《互联网信息服务管理办法》(2024)、《计算机信息网络国际联网安全保护管理办法》(2011)、《互联网上网服务营业场所管理条例》(2024)
部门规章(7)	《网络信息内容生态治理规定》(2019)、《关于加强网络直播规范管理工作的指导意见》(2021)、《互联网用户公众账号信息服务管理规定》(2021)、《网络表演经纪机构管理办法》(2021)、《网络主播行为规范》(2022)、《互联网跟帖评论服务管理规定》(2022)、《网络暴力信息治理规定》(2024)
党及组织文件(4)	《保护司法人员依法履行法定职责规定》(2016)、《新时代公民道德建设实施纲要》(2019)、《关于切实加强网络暴力治理的通知》(2022)、《关于进一步加强网络侵权信息举报工作的指导意见》(2023)
司法解释(5)	《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》(2013)、《关于审理编造、故意传播虚假恐怖信息刑事案件适用法律若干问题的解释》(2013)、《关于办理黑恶势力犯罪案件若干问题的指导意见》(2018)、《关于加强新时代检察机关网络法治工作的意见》(2023)、《关于依法惩治网络暴力违法犯罪的指导意见》(2023)
有关法律问题和重大问题的决定(1)	《全国人民代表大会常务委员会关于维护互联网安全的决定》(2009)

(二) 网络暴力治理研究方法

程序性扎根理论是在原始情境中获取原始资料并通过实证方法发现理论的方法论^[18]。对于“从零散的政策文本中勾勒出现有规制机制”这一研究命题,程序性扎根理论具有显著的方法论优势。因此,为更好地揭示网络暴力治理的制度逻辑,本文选择采用程序性扎根理论作为研究方法。

四、网络暴力治理政策的数据编码与检验

(一) 开放性编码

首先,对全部原始政策文本逐条逐段进行深入抽象和凝练,提取初始概念,使政策文本概念化、范畴化^[19]。鉴于政策文本的零散性,编码过程中容易出现重复概念和相似概念。因此,必须合并内涵一致的概念,进一步凝练相似的概念,形成上位副范畴。在确认没有新概念出现后,完成对政策文本的开放性编码。最终,本研究得到了共计303个初始概念和81个副范畴(详见表2)。

表2 开放性编码举例

政策文本内容	开放性编码	
	初始概念	副范畴
网站平台要建立网暴信息分类标准和典型案例样本库...	细化网暴信息识别标准	强化网暴信息识别能力
网络信息服务提供者应当建立健全网络暴力信息分类标准和典型案例样本库...	建立网暴信息分类标准	
	丰富网暴典型案例样本库	
网站平台要组织专门工作力量,及时收集网暴相关热点话题和舆情线索...	组织专门工作力量	完善涉网暴舆情应急响应机制
	及时收集网暴线索	
网络信息服务提供者应当优先处理涉未成年人网络暴力信息举报...	优先处理相关网暴举报	优先保护未成年人
发现未成年人用户存在遭受网络暴力风险的,应当立即处置违法违规信息,提供保护救助服务,并向有关部门报告...	立即处置相关网暴信息	
	特别提供保护救助服务	
.....	及时向有关部门报告	
	计 303 个初始概念	计 81 个副范畴

(二) 主属性编码

在开放性编码的基础上,对初始概念和副范畴进行更深入的整合,进一步凝练,形成高度概括性的主范畴。这一过程涉及归纳推理等方式,通过抽象总结,将初始概念和副范畴的内涵有机地整合在一起,形成主属性编码。最终总结出 26 个主范畴。这些主范畴对现有网络暴力治理政策文本进行了高度凝练,初步描绘了我国目前政策中蕴含的制度体系框架(详见表 3)。

表3 主属性编码举例

主范畴	副范畴	范畴内含
网暴传播扩散阻滞机制	评论环节管理	清理涉网暴评论,前置积极权威评论
	重点话题群组和板块管理	解散涉网暴群组、暂停新设相关话题群组
	直播管理	关停涉网暴直播间、管控受害者直播间
	短视频管理	清理涉网暴短视频、对相关新发视频审核前置
	权威信息披露	督促主体发布、加强推送转发
网暴受害者保护机制	优先保护未成年人	对涉未成年人网暴优先处置、特别救助
	加强用户真实身份核验	对相关主体进行登记识别+人工比对双重核验
	建立介入保护制度	系统主动提示防护、各主体积极协助防护
	设置一键防护功能	简化关闭转发、关闭评论等主动保护性功能
	完善私信规则	完善私信时间、数量、范围等被动保护性功能
	建立快速举报通道	优化涉网暴举报全流程程序设置
网暴协同监管机制	信息共享	各责任主体畅通涉网暴信息沟通共享机制
	会商通报	各责任主体建立重大涉网暴事件会商通报机制
	取证调证	各责任主体完善取证调证协作机制
	案件督办	网信部门强化案件督办机制
	监督检查	网信部门强化监督检查机制
.....
计 26 个主范畴	计 81 个副范畴	

(三) 选择性编码

通过对主属性编码内容的深入整合,最终得到了核心范畴,构建了初步的理论模型,揭示了政策文本中网络暴力治理的制度体系,主要体现在三个方面。第一,在网络暴力的事中治理中,通过明确主体责任,要求各主体切实履职,形成了网络暴力的综合治理机制。第二,在网络暴力的事后治理中,以法律解释为基础,协调民、行、刑的实体和程序,进行司法救济,形成了网络暴力的司法治理机制。第三,强调网络暴力在各个阶段的治理需要被制度化,建立了监测、预警、处置、阻滞、救济等全周期的连续机制,以实现长期的治理效果,形成了网络暴力的长效治理机制。

回顾全部 22 份政策文本,这三大治理机制不仅具有显著的核心性和解释力,而且在各个政策文本中频繁重现,它们之间存在动态联系和独立意义,符合选择性编码的效力要求^[20]。最终,在完成开放性编码、主轴性编码和选择性编码后,我们呈现了一个以核心范畴为中心、主范畴为提纲,由原始政策文本初步抽象形成的初始概念和副范畴为内容构成的理论模型(详见图 1)。

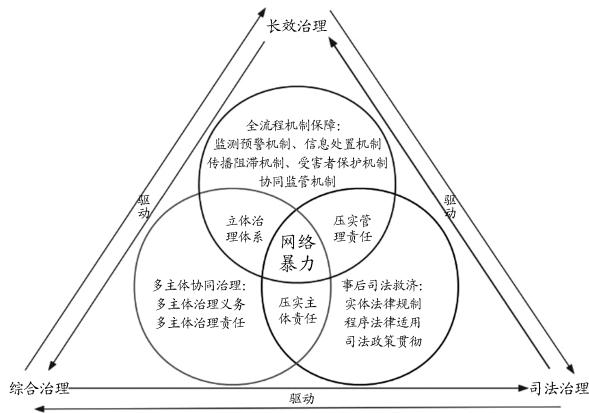


图 1 网络暴力治理的制度体系模型

(四) 理论饱和度检验

为确保研究成果的可信度,即编码结果的完整性,进行了理论饱和度检验。按照前文所述的政策文本筛选流程,最终选择了1份政策文本和7份典型案例^[21]作为检验材料进行检验。在对这些文本和案例进行编码方法的处理后,未获得新的初始概念、副范畴和主范畴,未超出前文获得的三个核心范畴的内涵范围,通过了理论饱和度检验。

五、网络暴力的治理逻辑分析

网络暴力作为一种日益严重的社会问题,其治理需要多方协同和综合施策。目前,我国已经建立了网络暴力的综合治理机制、司法治理机制和长效治理机制。首先,在网络暴力的事中治理阶段,我国着重强调各相关主体的责任分配和履行。通过明确政府、平台和用户等多方的职责,确保各方在治理网络暴力中各司其职,形成了一个多层次、多主体参与的综合治理机制。其次,在网络暴力的事后治理方面,国家建立了系统的司法治理机制。该机制基于对法律的细致解释,协调了民事、行政和刑事领域的实体法与程序法,使得网络暴力行为在不同法律框架下都能得到有效的司法救济。最后,为了确保网络暴力治理的长期有效性,我国构建了以制度化为核心的长效治理机制。通过这种制度化、流程化的安排,网络暴力治理得以实现全周期、全方位的覆盖,确保在不同时间点、不同情境下都能对网络暴力迅速作出反应,并提供持续的应对措施。在这三种机制中,综合治理机制为事中治理提供了组织和执行的基础,司法治理机制则为事后处理提供了法律保障和救济

途径,而长效治理机制通过制度化的安排,确保治理的连续性和持久性。这三者相互联系,彼此支撑,形成了一个有机统一的治理体系,构成了我国网络暴力治理的整体制度框架。

(一) 网络暴力的综合治理机制

网络暴力的发生关键在于网络空间的匿名性、超时空性等特征,形成了一个“主体多元、责任分散”的网络暴力场域,由此产生了失范效应^[22]。可见,网络暴力的成因复杂,不仅包括社会压力因素,还涉及管理缺位、执法不严、追责困难等多元因素。因此,有效的治理措施应该是协调多主体进行协同治理。新出台的《规定》新增第三条所确立的网暴信息治理原则即体现了网暴综合治理理念,即:源头防范、防控结合、标本兼治、协同共治。这一综合治理机制的建立有望在全方位、多层次上有效遏制和减少网络暴力的发生。

1. 网信部门履行监管责任,追究行政违法责任

网信部门作为网络信息服务和内容的监管主体,有责任积极执行监管职责,依照法律对未履行职责的网络服务提供者和网站平台进行处罚和处理。特别是,《通知》第四条第三款明确规定了网站平台双罚制,这一措施旨在强调对于网络平台及其主要负责人的双重追责,以保障网络信息服务和内容的合法、规范运行。

2. 网络服务机构主体履行管理责任,追究内部违规责任

网络服务机构包括网络信息服务提供者、网络平台及MCN机构,作为网络暴力场域的管理主体,应主动履行管理职责,依法强化内容治理和处置。《规定》第七条明确网络信息服务提供者有责任贯彻管理主体责任,提升工作手段和处理能力;《规定》第十一条、第十二条、第十五条等规定网络平台要完善预防和处理处罚机制,为牵涉网络暴力的信息、账号和利用网络暴力进行炒作的账号设定惩罚体系,并设立罚款记录公示和报告制度;《网络表演经纪机构管理办法》第八条要求MCN机构要对旗下签约主体履行管理责任,增强成员的法律和道德意识,并根据法规处置违规成员。通过自上而下为服务提供者、平台和MCN机构分别赋予治理义务,这一机制有助于限缩网络暴力责任主体,依规处置处罚。

3. 司法机构履行法律治理责任,推动民行刑衔接治理

司法机构作为提供最终法律救济的主体,应加强职能衔接配合,完善溯源治理。根据《意见》第二十条等相关规定,司法机构首先要立足司法职能,统一司法理念,完善民、行、刑及自诉公诉程序衔接,以确保为个案提供有效的法律救济。同时,司法机构还需立足社会治理,展开理论研究,深入分析网络暴力发生的现实根源,提出司法检察建议,向相关责任主体提供有效的指导,从而实现对网络暴力的溯源治理。

4. 加强公众法治宣传,弘扬社会道德风尚

公众作为网暴事件中的亲历者、旁观者或潜在的参与者,应当加强法治和道德建设,从而消解网暴的参与及传播主体。网络暴力的参与者和传播者往往基于朴素的伦理道德观念,在情感发酵中逐渐走向失范表达^[23]。在道德培育方面,新出台的《规定》相较征求意见稿,新增第六条,明确网络信息服务提供者和用户均应坚持社会主义核心价值观,尊重社会公德和伦理道德,维护良好的网络生态。在法治宣传方面,根据《意见》第十九条要求,应建立以规则为引领、以价值为导向的法治宣传制度,贯彻普法责任制,加强案例普法教育。从而在微观层面重建德法理性,化解网暴风险。

(二) 网络暴力的司法治理机制

近年来,社会和学界对于通过立法解决网络暴力问题的呼声不断。对于此类立法论的治理观

点,全国人民代表大会宪法和法律委员会在相关议案审议结果报告中表示会对增设“网络诽谤罪”“网络暴力罪”的议案予以考虑。然而,目前这些立法方案尚未得到立法机关的正式采纳。相反,在2013年和2023年,司法机关分别颁布了《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》(以下简称《解释》)和《关于依法惩治网络暴力违法犯罪的指导意见》(以下简称《意见》),对前者进行了解释和填补。而全国人大监察和司法委员会在议案审议报告中则回应称“已有相关法律法规或者规范性文件作出规定,建议有关部门做好法律实施工作,及时总结经验成果”^①。因此,可以认为目前我国立法和司法机关更倾向于在司法实践中运用解释论填补法律空白,而不是支持立法论的治理观点^[24]。

通过对编码结果的梳理,可以看出我国在网络暴力治理方面尚未形成综合的立法体系,但已初步构建了以专项立法为核心、以法律适用为抓手的法律框架。2013年和2023年颁布的《解释》和《意见》共同为网络暴力的法律适用提供了全面的规定。其中《意见》更为综合和全面。基于对网络暴力的社会危害性,《意见》从行为外延出发明确了网络暴力法律规制的对象和边界,进一步明确了网络暴力的司法治理路径。

1. 实体法律的规制

在刑事法律层面,现有政策体系回应了学界关于“从构成要素相当性角度进行解释”和恪守刑法价值的学理要求^[25]。《解释》及《意见》分别对诽谤罪、侮辱罪、侵犯公民个人信息罪、寻衅滋事罪、故意毁坏财物罪、拒不履行信息网络安全管理义务罪以及从共同犯罪的角度对现有刑法条文进行了解释参照适用。值得注意的是,《意见》中的规则建构表述均为“符合刑法第……条规定的,以……罪定罪处罚”。虽然这一规定可能使一些网暴行为不为刑法所规制,削弱刑法治理的效力^[26]。但这一方面体现了罪刑法定原则和刑法的谦抑性,另一方面也为行政法与民法的协同治理留下了适当的法律空间^[27]。

网络暴力作为一个复杂的社会学概念,其内涵广泛,外延多样。虽然其以严重的社会危害性引发了刑法学界广泛和深入的关注,但正如“法不责众”问题所反映的,刑法的谦抑性对于含有主体集散性的网络暴力具有天然的治理困境。故而《意见》等政策文本中同时规定了行政法律救济和民事法律救济制度,形成民、行、刑三法共治的网络暴力治理法律保障格局。《意见》第七条规定“依法惩治网络暴力违法行为……尚不构成犯罪,符合治安管理处罚法等规定的,依法予以行政处罚”。第九条规定,“依法做好民事维权工作……被害人请求行为人承担民事责任的,人民法院依法予以支持”。从而,司法治理机制中刑法作为最终救济手段,对最严重的网络暴力行为及其责任主体进行规制;对于尚不构成犯罪的一般情形和普通参与者,符合行政法律规定的依法予以行政处罚;对于日常生活中较为微弱的情形则由受害者依法提起民事诉讼,司法机关依法予以支持。

2. 诉讼程序的适用

当下网络暴力司法治理困境一方面体现为实体法上“法不责众”,另一方面体现为程序法上个人取证困难,当事人诉讼成本高昂。2015年《刑法修正案(九)》对刑法第二百四十六条作出修订,新增第三款:“通过信息网络实施侮辱诽谤行为,自诉人提供证据确有困难的,人民法院可以要求公安机关予以协助”。时至今日,网暴司法治理机制进一步完善了网络暴力案件的程序法救济。

在刑事诉讼领域,《意见》通过明确侮辱诽谤案件公诉标准,落实公检法依法支持自诉转公诉完

^①详见《全国人民代表大会监察和司法委员会关于第十三届全国人民代表大会第五次会议主席团交付审议的代表提出的议案审议结果的报告》。

善公诉救济程序;通过协助调证取证,依法支持自诉完善自诉救济程序。在行政诉讼领域,新增涉网暴情形作为提起行政公益诉讼的法定情形。在民事诉讼领域,法院应根据受害人申请依法作出人格权侵害禁令;新增涉网暴情形作为提起民事公益诉讼的法定情形。在诉讼程序保障层面,司法机制以加强公权干预为抓手,在刑事自诉、行政救济和民事诉讼中加强公力介入以弥补私力的能力局限和成本失衡,从而提升司法救济的实效性,推动提升受害者维权积极性。

3. 司法政策的贯彻

司法政策是指导司法实践过程的策略和原则^[28]。面对变动不居的社会现实,运用司法政策可以缓和法律规范的稳定性与网暴形态变化间的张力。司法治理机制中的司法政策主要体现在:其一,严格控制网暴认定标准。《意见》第十条规定,非故意明知不认定诽谤、非谩骂诋毁不认定侮辱,从而在复杂多变的网暴形态中,为法律所保护的言论自由和法律否定评价的不法提供根本性区分标准,为正常的网络秩序提供理念保障。其二,重点打击四类主体。《意见》第八条规定要重点打击恶意发起者、组织者、恶意推波助澜者、屡教不改者,从而破解网暴参与人数众多、主体集散性强导致的“法不责众”困境,将法律责任落到实处。其三,依法严惩六类情形。《意见》等规范性文件具体规定网络服务提供者发起组织的、利用生成式人工智能技术实施的、编造“涉性话题”的、有组织实施的、涉及黑恶势力的和针对未成年人、残疾人实施的情形应依法从重处罚,针对性地回应了网暴新形态、新手段。

通过落实司法政策,可以调和违法犯罪和言论自由、执法必严和“法不责众”等问题间的复杂关系。在对最具危害性的情形予以重点打击的同时,维护法律规范的稳定性与网暴形态变化间的张力,实现更好的司法治理效果。

(三) 网络暴力的长效治理机制

正如2022年全国人大监察和司法委员会在议案审议报告中所强调的,我国在网络暴力治理方面的关键问题不在于法律的不足,而在于法律的实施。尽管我国已经在加大网络执法力度方面取得了一些成就,通过“清朗”“净网”等系列专项行动取得了一定成果,但这种“运动式执法”也常常伴随一些负面效果和学界的批评^[29]。一些学者指出,专项行动在实践中固然有其合理性和有效性,能够快速整合治理资源、迅速回应社会需求,但也可能导致执法过程中的不规范行为,并因其短期性而引发事后反弹^[30]。将监管与执法从“运动式执法”过渡到“常态化”“规范化”执法,是推进国家治理体系和治理能力现代化的重要实践^[31]。长效治理机制的建立旨在使网络暴力治理措施常态化、制度化,确保治理按照设定的程序和模式持续运行。这一长效治理机制包含了从事前监测预警、事中信息处置、事后传播阻滞、受害者保护到协同监管的全周期治理体系。

1. 网暴的事前监测预警

当前舆情的规模和发展速度已使依赖人工巡查的传统监测方法难以实现对网暴迅速有效的监测预警。随着大数据与人工智能技术的不断发展,基于数据集训练的算法模型已经能够实现智能文本语义识别、情感分析等复杂工作,为网暴监测预警提供了新型技术支持^[32]。在这一新形势下,最新出台的《规定》第十二条对原征求意见稿第九条作出修改,要求网络信息服务提供者采用人工智能等技术手段和人工审核相结合的方式加强网暴治理。网络信息服务提供者需要建立专业的网暴治理团队、组织专业人才使用技术手段收集网暴线索、识别网暴行为,并按照政策要求构建网暴信息的识别和分类标准。同时,网络信息服务提供者应根据管理实践积累丰富的典型案例样本库,加强基础的网暴信息识别能力以适应新型的网暴表现形式。此外,相关主体可以从库中提取事件

类别、主体特征、参与人数、信息内容等特征信息,结合后台历史数据(例如信息发布者的举报记录等),构建适用于具体网络服务场景的网暴技术识别预警模型,有助于网暴信息进行更深入的分析和研判。

2. 网暴的事中信息处置

对于类型多样、严重程度迥异的网络暴力信息及相关主体,应当根据法律规定设置多种处置手段予以规范。《规定》第十五条规定,对涉网暴不良信息应采取停止传输、删除、屏蔽、断开链接等处置措施。但在现阶段的众多专项行动通报中,“删帖次数”“封号数量”等被视为网络治理成效的首要标志。但是一味地“以删代管”有碍于网暴治理的法治化和常态化^[33]。网暴信息的处置需要根据不同情况适用不同严厉程度的规制手段,建立宽严相济的规制体系以符合回应性规制理论中的规制金字塔模型,实现更为经济高效的监管和治理。对于轻微的网暴信息,可采取限制传播、拦截过滤等措施限制其传播范围而无需删除;对于超过轻微范畴的网暴信息,可采取删除屏蔽、断开链接等方式进行处置。对于发布信息的账号主体,也应根据情况采取警示教育、停止流量支持、限制账号功能,最终封停账号的处置方法。《通知》第四条第一款规定,对于发布不友善信息的账号,可以提示理性发言;对于参与网暴的账号,可以进行警示教育、限制功能等;对于首发多发煽动的账号,依法采取关闭账号、全网禁止注册新账号等措施;如果涉及违法犯罪,则需将账号控制主体移交相关部门依法追责。如果该主体存在运营机构,也应根据客观情况进行相应的处置,以实现对网暴信息的合法有序处置。

3. 网暴的事后传播阻滞

长效治理机制应涵盖对网暴行为的全周期治理,其中阻滞网暴信息的无序传播是遏制网暴负面影响的至关重要的环节。研究表明,谣言信息因其零时滞的首因效应、算法助推和受众情绪诉求等因素影响,导致其传播力大于辟谣信息的传播力,从而造成了“辟谣失灵”的现象^[34]。因此,阻滞谣言、诽谤等网络暴力的关键在于降低网暴信息的传播力,增强正面信息的传播力^[35]。阻滞传播的具体策略可分为“删帖策略”与“辟谣策略”两种^[36]。基于“删帖策略”,当网暴发生时,相关主体应依规在评论环节、重点话题群组和板块、直播间、短视频等场域迅速进行有效管控。对新发内容进行严格审核,对涉网暴言论采取限制传播、拦截删除等措施依规处置。基于“辟谣策略”,相关主体应在上述场域中优先展示正面信息,赋予正面信息更高的流量推送权重等;还应督促权威信息在权威渠道及时发布,同时加强权威信息推送转发,从而增强辟谣信息的可信度,强化传播效果^[37]。《规定》第十三条规定,网络信息服务器对存在网络暴力风险的,应采取限制流量等措施;新增第十六条规定,互联网新闻信息服务器发布转载涉网暴信息时,应立即公开更正,消除影响;第十八条规定,网络信息服务提供者应及时采取删除、屏蔽、关闭评论、停止提供相关服务等处置措施。可见,《规定》旨在综合“删帖”和“辟谣”策略,多措并举阻滞网暴信息传播。

4. 网暴受害者保护机制

网络暴力的长效治理机制不仅涵盖了对网络暴力行为的打击,还包括对网络暴力受害人的全方位保护。除了法律提供的事后救济之外,相关主体可在事前和事中积极采取措施,以预防网络暴力行为造成的严重后果。根据《通知》第四条第二款规定,相关主体通过加强用户真实身份核验,消除网络匿名性和超时空性,有效阻断网络暴力的实施。根据《通知》第二条,相关主体还应提供一键防护、私信限制规则以及快速举报通道,建立被动防护机制。此外,按照《规定》第二十三、二十四条,相关主体还需要建立介入保护制度,当发现网络暴力风险时,积极提示防护,在风险实现时主动

协助防护。同时,根据《规定》第二十七条,应树立优先保护未成年人的治理原则。当发现涉及未成年人的网络暴力事件时,相关主体应优先处理相关举报,立即处置相关信息,提供特别救助,并及时向有关部门报告。

5. 网暴协同监管机制

网信部门统筹监管是网络暴力长效治理的关键。自2014年国务院发布《关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》以来,我国已经形成了基于属地管理架构的网信办监管体系^[38]。然而,在实践中,互联网信息内容监管职能表现出分散和碎片化的特点。网信办、公安、广电等多个部门都具有监管职能和权力,导致协调成本高、治理效率低^[39]。在网络暴力信息治理领域,核心政策文件如《通知》和《规定》系由网信办牵头出台,实际上确立了由网信办担任监管主体的协同监管机制,其中明确了“坚持由网信部门进行监督检查、案件督办,各相关主体间建立信息共享、会商通报、取证调证便利制度”的原则。

六、网络暴力治理政策的优化建议

本研究以包括最新出台的《网络暴力信息治理规定》在内共22份网络暴力治理的政策文本为基础,采用扎根理论作为定性研究方法,深入分析了当前网络暴力治理零散政策文本中所隐含的制度逻辑与体系。研究发现:《规定》《通知》和《意见》及其余涉网暴治理法律法规以网络暴力的社会、技术、心理成因为抓手,针对网络暴力发生规律构建了三机制治理策略,即综合治理机制、司法治理机制和长效治理机制,完善网络暴力的事前事中事后治理。这三者相互交融、互为补充,形成了一个相对完整的网络暴力治理的制度框架,为全面营造清朗网络空间提供了坚实法治力量。然而,尽管已经建立了治理的制度框架,但当前网络暴力治理的制度体系仍存在一些缺陷,亟须在后续工作中进行深入的补充和完善,以更有效地应对复杂多变的网络暴力现象。

第一,综合治理机制在化解网络暴力中的技术风险方面表现出协同作用,但对社会风险成因的关注相对不足。网络暴力浮在网上却根于网下^[40]。尽管技术性风险如匿名性、超时空性、网络技术的便捷性直接导致了网络暴力的多发,然而网络暴力往往基于网民的道德情感经由激化而得以扭曲表达。其中虽有技术风险的催化,但究其根源仍是现实社会矛盾、社会风险的一种表现方式^[41]。如网课爆破案背后是传统教育中被压抑的师生关系矛盾;粉发女孩案则反映了当下传统道德与新式审美间尚未调和的冲突等,而那些庞大的网暴参与者则多因现实压力而借技术风险之便,以道德审判之名行发泄之实^[42]。因此,毋庸置疑的是治理网络暴力的根本之策仍是调节社会矛盾,控制社会风险。然而,在网络暴力治理机制中,社会风险治理责任仅分配给了司法系统的诉源治理机制和司法建议机制。诉源治理只是宏观社会治理机制的一部分,而社会治理并非司法系统可以主导甚至独立实现的目标。网络暴力的社会风险治理需要国家层面的其他社会政策予以应对。首先,应完善“政府主导,多方协商”的治理模式。这样既可以保障政府的决策地位和实施效力,又能吸取多方主体的意见和建议,以便更及时地发现和预防风险。其次,应建立对现有治理体系的监测评估机制。面对快速发展和变化的社会现实,及时评估、修正和反馈既有治理体系有助于在微观层面及时消解风险。此外,还可以引入更多第三方机构进行社会风险评估,拓展多方视角,从而增强风险发现、识别和处置的能力。

第二,虽然司法治理机制规定了实体法衔接治理,但仍缺乏具体实践标准和民、行、刑统一理论。刑事犯罪、行政违法、民事侵权间的界分主要依靠“情节”的严重程度。这在“交织地带”给司法

实践带来区分难题^[43]。面对网暴易发多发的急迫现实,实践中司法机关首先应恪守《意见》第十条,从严解释网络暴力违法犯罪情形,保障言论自由不受侵犯的红线。其次,司法机关在实践中应严格区分违法犯罪和民事侵权,进而在司法实践中落实《意见》等政策文本中规定的民事责任承担及民事公益诉讼、人格权侵害禁令等其他救济方式,积极协助进行民法救济。相应地,司法机关应在实践中严格限缩刑法适用,刑罚是“社会政策的最后手段”,在法益保护中作为最后的、补充性的手段。当民法、行政法无法弥补受害人的损失时才考虑予以介入,消极谦抑进行刑事救济^[44]。在积极和消极间的部分适时运用行政责任对超越民事范畴而不足刑事犯罪的“准犯罪”予以救济。根本上而言,法律适用理念不能解决民行刑衔接,尤其是行刑衔接的客观困境。对于如何区分和调和刑事不法与行政不法、民事不法间的差异,依然亟待构建一个法秩序统一框架下的解释理论^[45]。或通过立法论明确网络暴力情境下的行政处罚前置性要件,从而实现行政与刑事间梯度有序救济。

第三,目前的网络暴力长效治理机制着眼于落实网络暴力信息监管处置责任,但未就“平台权力”监管和执法监督做出完善规定。《网络暴力信息治理规定》第十五条等虽然规定了处罚记录上报制度,纳入了由网信部门主导的监督检查机制。但从整个机制的价值导向可以发现,监督检查机制旨在规制网络服务提供者等管理主体怠于履责类情形。现有机制未对压实主体责任过程中可能出现的超过法定限度而“自我阉割”式过度审查、过度执法作出考量^[46]。进而,监测预警措施在运行中易成为事实上的网络监控措施^[47]。平台主体在政府授权自我规制中实际完成了权力的增能与兴起^[48]。故而,在将来对长效治理机制的完善中,首先应将对“平台权力”监管机制予以纳入。如平台在相关标准库建设和完善中既要纳入“处罚标准案件”,也要纳入“不处罚标准案件”;在作出处罚和申诉反馈过程中,应明确处罚的具体法律依据和事实依据,摒弃“依据相关法律法规……”式的粗犷执法,使被处罚者申诉有据可依;网信办在监督过程中也既要监督相关主体是否履行了积极的查处义务,也要监督相关主体是否履行了消极的权利保障义务,从而将平台、用户、网信部门三方纳入,由多方协同进行平台权力监管。其次在治理过程中,网信等政府部门应在根本上把握好授权与分权、安全与发展间的动态关系^[49]。在过程中通过约谈等政策工具把握平台权力边界,从而更好地落实主体责任,实现对网络暴力的有序治理。

参考文献:

- [1] 门豪. 互联网“吃瓜”的意义构成:集体欢腾新面孔[J]. 天府新论,2022(1):143-150.
- [2] 翟绪权,夏鑫雨. 数字经济加快形成新质生产力的机制构成与实践路径[J]. 福建师范大学学报(哲学社会科学版),2024(1):44-55,168-169.
- [3] 王艺. 网络虚拟空间中的“非理性互动”类型及影响因素[J]. 现代传播(中国传媒大学学报),2018(10):63-67.
- [4] 周立波. 网络暴力犯罪的刑事法治理[J]. 法治研究,2023(5):38-51.
- [5] 新华网. 习近平谈打造清朗的网络空间[EB/OL]. (2021.09.07)[2024.06.25]. http://www.news.cn/politics/2021-09/07/c_1127836264.htm.
- [6] 储陈城. 刑法应对网络暴力的流变及其基本立场[J]. 中国刑事法杂志,2023(4):35-52.
- [7] 陆益龙. 纠纷解决的法社会学研究:问题及范式[J]. 湖南社会科学,2009(1):72-75,80.
- [8] 喻海松. 网络暴力的多维共治:以刑事法为侧重的展开[J]. 江汉论坛,2023(5):128-135.
- [9] 蔡鹏程. 网络谣言刑事归责限度理论的构建:兼论网络谣言与网络暴力的界分[J]. 阅江学刊,2023(5):58-75,169-170.
- [10] 陈罗兰. 网络暴力的刑法治理与罪名增设[J]. 法律科学(西北政法大学学报),2023(5):115-123.
- [11] 石经海,黄亚瑞. 网络暴力刑法规制的困境分析与出路探究[J]. 安徽大学学报(哲学社会科学版),2020(4):78-89.
- [12] 路鶴,张君昌. 技术路径下网络暴力治理的共治模式探究[J]. 青年记者,2023(15):86-88.

- [13] 赵韫湜,刘晶.“规则+技术”:互联网平台针对“网络暴力”现象的数字化治理[J].北京文化创意,2023(2):75-84.
- [14] 张钦坤,曹建峰.从《网络信息内容生态治理规定》看互联网新技术的治理[J].信息安全与通信保密,2020(2):12-18.
- [15] 周葆华,罗沛.网络暴力:概念情境、类型聚焦与协同治理[J].青年记者,2023(17):68-70,74.
- [16] 刘绩宏.网络谣言到网络暴力的演化机制研究[J].当代传播,2016(3):83-85.
- [17] 冉连,张曦.网络信息内容生态治理:内涵、挑战与路径创新[J].湖北社会科学,2020(11):32-38.
- [18] GLASER B G, STRAUSS A L. *The discovery of grounded theory; strategies for qualitative research* [M]. Chicago: Aldine Pub. Co, 1967.
- [19] 杜晓君,刘赫.基于扎根理论的中国企业海外并购关键风险的识别研究[J].管理评论,2012(4):18-27.
- [20] 贾旭东,谭新辉.经典扎根理论及其精神对中国管理研究的现实价值[J].管理学报,2010(5):656-665.
- [21] 依法惩治网络暴力违法犯罪典型案例[N].人民法院报,2023-09-26(003).
- [22] 姜方炳.“网络暴力”:概念、根源及其应对:基于风险社会的分析视角[J].浙江学刊,2011(6):181-187.
- [23] 王静.数字公民伦理:网络暴力治理的新路径[J].华东政法大学学报,2022(4):28-40.
- [24] 陈堂发.强化法律适用:网络暴力的法治途径[J].人民论坛,2022(9):96-99.
- [25] 郭旨龙.网络暴力刑法治理的解释原理[J].江汉论坛,2023(5):119-127.
- [26] 石经海.论网络暴力的实质与刑法适用规则的完善[J].法律科学(西北政法大学学报),2023(5):69-82.
- [27] 姜涛.网络暴力治理中刑事责任、行政责任与民事责任的衔接[J].法律科学(西北政法大学学报),2023(5):102-114.
- [28] 刘顺峰.司法政策概念论[J].济南大学学报(社会科学版),2023(5):129-140.
- [29] 程琥.运动式执法的司法规制与政府有效治理[J].行政法学研究,2015(1):75-81,128.
- [30] 陈柏峰.党政体制如何塑造基层执法[J].法学研究,2017(4):191-208.
- [31] 刘鹏.运动式监管与监管型国家建设:基于对食品安全专项整治行动的案例研究[J].中国行政管理,2015(12):118-124.
- [32] 李明德,邝岩.大数据与人工智能背景下的网络舆情治理:作用、风险和路径[J].北京工业大学学报(社会科学版),2021(6):1-10.
- [33] 靖鸣,江晨.网络删帖行为及其边界[J].新闻界,2017(7):44-53,108.
- [34] 王超.辟谣何以失灵:一个信息传播效果视角的解释框架[J].情报杂志,2019(5):123-129.
- [35] 丁汉青,韩玥.事件与传播:网络暴力事件传播力影响因素分析:基于49例网络暴力事件的定性比较分析(QCA)[J].广州大学学报(社会科学版),2023(1):183-192.
- [36] 粟盛玉,郭凤海.应对网络政治谣言需要“删帖策略”[J].电子科技大学学报(社科版),2019(2):53-59.
- [37] 刘于思,徐煜.在线社会网络中的谣言与辟谣信息传播效果:探讨网络结构因素与社会心理过程的影响[J].新闻与传播研究,2016(11):51-69,127.
- [38] 卢超.互联网信息内容监管约谈工具研究[J].中国行政管理,2019(2):41-46.
- [39] 周汉华.论互联网法[J].中国法学,2015(3):20-37.
- [40] 姜方炳.污名化:“网络暴力”的风险效应及其现实隐喻:以“李刚门”事件为分析个案[J].中共浙江省委党校学报,2012(5):50-57.
- [41] 姜方炳.空间分化、风险共振与“网络暴力”的生成:以转型中国的网络化为分析背景[J].浙江社会科学,2015(8):52-59,157-158.
- [42] 王苑岭.“打抱不平”的人肉搜索:相关网络暴力问题探析[J].重庆邮电大学学报(社会科学版),2009(3):127-130.
- [43] 史立梅,孙若尘.“情节恶劣”的适用语境与判断标准之研讨:以《刑法修正案(十一)》经核准负刑事责任条款为例[J].青少年犯罪问题,2022(1):149-160.
- [44] 张红昌.体系与问题交融下民刑交叉案件的谦抑性研究[J].中国人民公安大学学报(社会科学版),2023(4):15-23.
- [45] 赵宏.网暴案件中的民行刑责任与一体化衔接[J].北方法学,2023(5):5-20.
- [46] 支振锋.网络安全风险与互联网内容治理的法治化[J].改革,2018(1):44-46.
- [47] 贾健,王博文.打击犯罪视域下网络监控的措施定位及其法律规制[J].重庆邮电大学学报(社会科学版),2024(6):31-42.
- [48] 孙逸啸.网络平台自我规制的规制:从权力生成到权力调适:以算法媒体平台为视角[J].电子政务,2021(12):69-79.
- [49] 朱垚颖,谢新洲,张静怡.安全与发展:网络内容审核标准体系的价值取向[J].新闻爱好者,2022(11):27-33.

The governance logic and optimization suggestions of network violence: Based on the grounded analysis of policy texts from 2009 to 2024

XU Wei¹, LI Ruiheng²

(1. Chongqing University of Posts and Telecommunications, Chongqing 400065, P. R. China;

2. The Third Research Institute of Ministry of Public Security, Shanghai 201210, P. R. China)

Abstract: Regulating cyber violence according to law is the core goal of cyberspace governance in the new era. At present, China's laws and regulations in this field are scattered in various legislative documents of different natures and levels, which leads to the fragmentation, overlapping and even contradictions of legal provisions. The dispersion and inconsistency of this legal system not only affect the implementation effect of the law, but also cause problems such as unclear responsibility and difficult implementation in specific operations. Therefore, it is urgent to systematically sort out the existing policy texts, analyze the governance framework and its potential problems, and improve the governance level of cyber violence. This paper collects 22 policy documents on cyber violence governance issued by China from 2009 to 2024, compares and analyzes the data by using procedural grounded theory, condenses relevant concepts and categories, and finally constructs the logical framework of governance. The research shows that China has initially established three major network violence governance mechanisms: comprehensive governance mechanism, judicial governance mechanism and long-term governance mechanism. First of all, in the stage of in-process governance, the state has formed a multi-level and multi-party participation comprehensive governance mechanism by clarifying the responsibilities of the government, platforms and users. Through effective collaboration, all parties promote the full participation and technical support of cyber violence governance. This mechanism shows a strong synergy in resolving technological risks, but there are still deficiencies in the analysis and response to social risks. Secondly, the judicial mechanism in the post-governance stage has realized the effective connection between civil, administrative and criminal laws through refined legal interpretation. This mechanism ensures that cyber violence can obtain judicial relief under different legal frameworks, but it still needs to be refined in specific practical standards. Especially between civil, administrative and criminal proceedings, the lack of a unified theory of practice may lead to difficulties in convergence in practice. Finally, the state has constructed a long-term governance mechanism with institutionalization as the core to ensure that the problem of cyber violence in different situations can be dealt with continuously and effectively. Through process-oriented arrangements, the mechanism can respond quickly to cyber violence and provide long-term solutions. However, there are still deficiencies in the supervision of platform power, especially that the legal provisions are not perfect in effectively supervising platforms' fulfillment of their governance responsibilities. In summary, the future governance direction should include: strengthening the prevention and control of social risks of cyber violence, further refining the practical standards of judicial governance mechanism and improving the supervision mechanism of platform power, so as to promote the legalization and modernization of cyber violence governance in China and build a more perfect cyberspace governance system.

Key words: network violence; comprehensive management; judicial governance; long-term governance; cyberspace governance

(责任编辑 刘琦)