

网络暴力治理的法治化转型 及立法体系建构

刘艳红^{*}

内容提要：网络暴力问题是新时代国家治理过程中的重大性、交叉性、领域性难题。当前我国治理网络暴力的相关法律规定内容分散且缺乏协调配合，在权责主体、制裁措施、救济方式等方面存在制度疏漏，无法有效回应当前网络暴力问题的治理需求。积极推进网络暴力治理的法治化转型及立法体系建构，是纾解我国网络暴力治理困局之关键。推动网络暴力治理的法治化转型，既要树立协同共治理念，实现多元治理主体的协同以及法律与技术的协同，也要确立系统性法治模式，充分发挥部门法的协同共治功能。在协同共治理念与系统性法治模式的指引下，应遵循领域性立法思维，制定反网络暴力法，搭建网络暴力治理的基本法律制度框架，完善网络暴力治理配套法律法规制度，构建起网络暴力治理领域的专门性立法体系，全面实现我国网络暴力治理的法治现代化转型。

关键词：网络暴力 反网络暴力法 领域法 协同共治

网络技术重塑了现代生活，并在现实社会之外构建了一个虚拟网络空间。在网络技术与社会生活深度融合的过程中，各种现实社会问题和现实矛盾进入网络空间，演变成为“网络暴力”的重要源头。网络暴力是以网络为媒介，通过诽谤侮辱、煽动滋事、公开隐私等人身攻击方式，侵害他人人格权益、危害网络正常秩序的行为，它在网络空间中的公民之间产生，是虚拟化、数字化、具有群体属性、跨越双重空间的新型暴力模式。网络科技的飞速发展推动了社会的进步，也为网络暴力的泛化与蔓延提供了条件。“被撞学生妈妈因网暴坠亡”、〔1〕“粉

^{*} 中国政法大学刑事司法学院教授。

本文系国家社科基金重大项目“数字经济的刑事安全风险防范体系建构研究”（21&ZD209）的阶段性成果。

〔1〕 2023年5月，武汉某学校老师驾车误撞一名小学生并致其死亡。当天，遇难学生的母亲接受了有关媒体采访并在网上发布受访视频，部分网友对其穿着和长相进行恶意评价，实施了侮辱、诽谤等网络暴力。其后，学生母亲跳楼身亡。参见《武汉小学生“校内被撞身亡”后，其母坠楼身亡》，https://www.thepaper.cn/newsDetail_forward_23341084，2023年8月30日最后访问。

发女孩被网暴后轻生”、〔2〕“河南女教师遭网暴后猝死”〔3〕等恶性网络暴力事件引起了全社会的高度关注,网络暴力已然严重危害到公民的合法权益和网络空间的健康生态。中央网络安全和信息化委员会办公室(简称“中央网信办”)于2022年4月发起“清朗·网络暴力专项治理行动”,并于同年11月印发《关于切实加强网络暴力治理的通知》,要求加大网络暴力治理力度,完善网暴问题治理的长效机制。然而,立法层面的不足是网络暴力治理面临的首要困境。我国现有法律法规尚未搭建起足够完善的网络暴力治理框架,网络暴力治理的法治路径存在制度规范疏漏、法治理念滞后与制度运行不畅等弊端,导致重大网络暴力风险问题无法得到有效遏制。面对现代社会中的网络暴力治理难题,本文立足于我国网络暴力治理的法治化困境,主张应确立网络暴力治理的协同法治理念,推行适应于数字技术跨域发展的系统性法治模式,在领域法治思维的指导下制定治理网络暴力的专门性立法,并推动相关立法体系建构,以全面实现我国网络暴力治理的法治化转型。

一、国家治理现代化视域中网络暴力治理的法治困境

国家治理现代化追求的是良法善治之目标。将体现良法要求的公平正义价值融入国家治理体系之中,是国家治理现代化的题中应有之义。规则之治是网络暴力治理的根本遵循,网络暴力治理应该建立在系统完备的法治规范体系的基础上。要实现我国网络暴力治理的法治化转型,首先应在国家治理现代化的时代背景下,对我国网络暴力治理的法治困境及时检省。

(一) 网络暴力治理的法律框架存在规范疏漏

面对愈加复杂的网络暴力现状,我国的网络暴力治理日渐暴露出规范供给不足的结构性问题。在我国当前的法律制度框架中,能够对网络暴力发挥治理作用的制度规范,散见于民法典、刑法、个人信息保护法、网络安全法以及相关部门规章、司法解释之中。对于网络暴力行为的规制,主要通过关联现有制度规范中对侮辱、诽谤、寻衅滋事等行为的调整间接实现。由于存在规范上的疏漏,在许多场合中,不仅无法实现对网络暴力违法犯罪行为的依法治理,也难以为受害者提供全面有效的保护。

首先,现行法律主要将发生在线下的隐私侵害、侮辱、诽谤等传统不法行为作为调整对象,〔4〕而没有对网络跟踪、网络恐吓、网络造谣、网络欺凌等网络暴力行为进行专门规制。虽然民法典、刑法、个人信息保护法、网络安全法等,从理论上讲都可以作为网络暴力治理的规范依据,但相关规范并未将网络暴力行为本身作为调整对象,而是通过惩治关联行为的方式附带规制网络暴力。例如,适用民法典、个人信息保护法关于隐私权、个人信息保护的规定规制网络暴力,其前提是行为人在实施网络暴力的过程中泄露了他人隐私或个人信息。这意味着,如果行为人并非以泄露隐私、个人信息等方式,而是单纯通过网络跟踪、网络造谣、网络

〔2〕 郑某某被成功保研到某知名高校后,在爷爷病床前分享喜讯,却因其染了粉色头发,遭到部分网友、网络营销号的辱骂和诽谤。郑某某遂患上严重的抑郁症,最终选择轻生离世。参见《“粉发女孩”离世,网暴悲剧何时终结》, https://www.thepaper.cn/newsDetail_forward_22044976, 2023年8月30日最后访问。

〔3〕 2022年10月某日晚,多名网暴者进入刘某某的网课直播间,通过语音辱骂等方式干扰其上课,刘某某最终因心脏病发而猝死。参见《女教师上网课后去世,谁在进行“网课爆破”》, <https://news.sina.com.cn/s/2022-11-03/doc-imqmmthc3115907.shtml>, 2023年8月30日最后访问。

〔4〕 参见刘艳红:《网络时代言论自由的刑法边界》,《中国社会科学》2016年第10期,第145页以下。

欺凌等方式实施网络暴力,则无法适用民法典、个人信息保护法中的相关规定。

针对当前理论和实务中争议较大的网络暴力参与人的规制范围问题,已有制度规范并未作出明确规定。从形式上看,网络暴力参与人都可能涉嫌侮辱、诽谤、寻衅滋事等违法甚至是犯罪行为。然而,如果对所有人都因此加以规制,容易出现“全民违法”的后果;^[5]如果限定规制范围,对于应当限定到何种程度,也需要相应的规范依据。在相关法律法规的具体适用中,受“法不责众”倾向的影响,有关部门往往只处罚网络暴力的发起者、组织者,而忽略对其他参与者的规制。当前,司法机关也意识到这种做法并不妥当。为了有效规制网络暴力,最高人民法院、最高人民检察院、公安部共同起草了《关于依法惩治网络暴力违法犯罪的指导意见(征求意见稿)》,于2023年6月9日向社会公开征求意见。该征求意见稿提出,要切实矫正“法不责众”倾向,对网络暴力的恶意发起者、组织者、推波助澜者以及屡教不改者予以重点打击。然而,在民事裁判和行政执法领域,这种“法不责众”倾向仍然存在。2023年8月3日,北京互联网法院发布了一批涉网络暴力典型案例。^[6]在其中的“刘某与孙某网络侵权责任纠纷案”中,孙某因与网络“大V”刘某存在不同观点,发私信辱骂刘某及其家人。随后,刘某在微博上公开“挂人”,将二人的私信截图、孙某个人照片及其微博账号截图等通过多条微博发布,引发许多网友评论和转发。对于发布负面评论侮辱孙某的网友,原本可追究其民事侵权责任和扰乱网络秩序的行政责任,但在司法和执法实践中,这种非发起者、非组织者实施的行为普遍被放过,本案最终也只追究了刘某微博“挂人”发起网暴的民事责任。

其次,关涉网络暴力治理的法律责任条款不完整。法是一种强制秩序,有效的法应当对违反法秩序的行为附加确定的法律责任,不附法律责任的法律义务,以及不确定、不完整的法律责任,都有损法的规范效力。^[7]然而,当前与网络暴力治理相关的法律责任条款大多不完整,降低了立法的可适用性与可操作性。自2011年开始,我国形成了以中央网信办为中心的互联网立法及治理格局,中央网信办出台的部门规章及其他规范性文件,成为划定网络暴力治理中各方权责的重要依据。这些规范性文件虽然均设有“法律责任”章节或法律责任条款,但相关章节或条款的具体内容与针对一般违法行为的行政处罚别无二致,没有考虑到网络暴力治理的特殊性及其制度需求。例如,《关于切实加强网络暴力治理的通知》强调网络平台要健全网暴预警预防机制、强化对网暴当事人的保护、严防网暴信息传播扩散,但这些规定都较为空泛,没有明确网络平台是否应对网络暴力进行全流程监控,也没有规定网络平台违反相关义务应当承担何种法律责任。

最后,针对网络暴力的一体化评价机制缺位。由于缺失网络暴力治理的专项法律与配套制度,现有法律体系未能完全覆盖网络暴力的治理需求,直接对适法和守法环节产生了负面影响。在当前的网络暴力治理范式中,一般需要先行分解网络暴力行为,将其拆分为侮辱攻击、网络造谣、“人肉搜索”等不同类型,然后再分别对它们进行独立评价,才能勉强实现网络暴力治理的有法可依。这种治理范式难以顾全网络暴力的所有类型。如果将碎片化的网络暴力危害行为简单直接相加,则难以展示网络暴力的整体轮廓;如果对孤立的网络暴力行为进行单独评价,则难以对行为的情节性质与危害结果予以全面评价,无法精准打击网络暴力违法犯罪行

[5] 参见秦前红:《宪治审视下“全民违法”现象的产生及破解之策》,《政治与法律》2022年第4期,第2页。

[6] 参见《严惩网络暴力!北京互联网法院发布涉网络暴力典型案例》, <https://new.qq.com/rain/a/20230803A09HM800>, 2023年9月5日最后访问。

[7] 参见[奥]汉斯·凯尔森、[德]马蒂亚斯·耶施泰特:《纯粹法学说》,雷磊译,法律出版社2021年版,第65页。

为。由于缺乏专门立法,针对网络暴力的一体化评价机制缺位,不同法律规范囿于局部治理视角,既可能因遗漏重要违法类型而形成处罚漏洞,也可能出现对同一事实的重复评价或二次处罚。网络暴力治理的配套制度不健全,也是阻碍网络暴力治理体系现代化的关键因素。目前,从前端的网络素质教育、网络暴力预警,到中端的网络暴力行为识别与监管,再到末端的网络暴力行为处置与救济,都在一定程度上存在配套立法不足的问题。网络暴力治理是涉及多元主体的系统性工程,任何环节配套立法的缺位,都会致使治理链条运转滞涩不畅,难以保证法治化治理的顺利推进。

(二) 网络暴力治理的法律体系矛盾

当前,我国有关网络暴力治理的法律规范之间缺乏有机衔接,难以形成系统协调的网络空间治理秩序与全面有效的权利保护机制。法律体系分为内部体系与外部体系,内部体系是诸多法律规范一致认可的价值判断体系,外部体系是由实在法规范及其相互关系构成的体系。^{〔8〕}信息化发展与网络安全不可避免地会发生价值冲突,网络暴力治理的上位立法缺失也影响到法律外部体系的整合,这些都在不同程度上影响着整个网络法治秩序的统一和对网络暴力的法治治理效果。

1. 网络暴力治理的法律内部价值体系矛盾

法律内部体系,也称为法律内部价值体系,是具有目的意义或价值标准的法律原则体系。按照法律的整全性理论,现行法律规则(准则)所构成的体系性框架,是综合考虑了国家的管理秩序、社会公共利益与公民的道德生活等形成的有机价值整体,立法者应当努力将法律的、政策的、道德的价值准则融为一体,避免法律内部价值体系出现冲突。^{〔9〕}网络暴力治理的核心价值追求,是保护公民的基本权利、维护网络空间公共秩序(网络安全价值),但同时也要兼顾信息技术发展催生的数字经济利益(信息化发展价值)。在对网络暴力的治理过程中,既要防止网络安全价值或信息化发展价值的单极扩张,也要承认网络安全与信息化发展的彼此相容。于是,网络安全与信息化发展之间的价值选择,就构成了网络暴力治理的法律内部体系矛盾。

在网络空间中,安全、发展、秩序、自由等多元价值交叠互补,不同价值目标在网络暴力治理中相互竞逐。在此趋势下,试图以某种单一价值去引领网络暴力治理的方向,必然会因违背社会发展的客观规律,而无法真正地回应网络暴力治理需求。在网络技术助推国家和社会全面发展的过程中,信息化的高速发展引发了个人信息泄露、网络攻击、网络欺凌等方面的安全风险,人类在某种程度上受技术操控,以至于偏离了人的理性和目的论主体地位。在现象发生层面,网络暴力的滋生和蔓延,总体上可视为网络空间中安全价值与发展价值不协调的结果,是法律内部价值体系冲突的表现。在社会治理层面,既然网络暴力的形成源于法律内部体系矛盾,对此类社会失范行为的有效治理,首先需要对网络空间的安全与发展进行再平衡。网络暴力治理中的价值体系本身处于对立统一的辩证关系之中,安全价值与发展价值的冲突,是法律在调整网络关系的过程中经常需要面临的问题,二者的相容共存则是法律在理性衡平网络关系各方主体权利义务后的结果。2020年党的十九届五中全会审议通过《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》,提出坚定不移建设网络

〔8〕 参见〔德〕卡尔·拉伦茨:《法学方法论》,陈爱娥译,商务印书馆2003年版,第316页。

〔9〕 参见〔奥〕恩斯特·A.克莱默:《法律方法论》,周万里译,法律出版社2019年版,第140页以下。

强国，统筹发展和安全。为此，有必要科学确立网络暴力治理的价值理念，明确“统筹发展和安全”的网络暴力治理价值立场，避免网络安全保障与信息化发展两者之间陷入失衡格局。

2. 网络暴力治理的法律外部规范体系矛盾

法律外部体系是法律规范的集合，也称为法律外部规范体系，其强调法秩序的统一性，要求所有的法律形式具有规范逻辑上的一致性。法律只有尽可能做到规范上的和谐一致，才不至于因为规范相互矛盾而自我推翻，才能为理性人所理解和接受，并用于规范和预测人们的行为。^{〔10〕}

在网络暴力治理的规范体系层面，直接规制网络暴力的法律制度规范离散性较强，且缺乏基础性的法律制度支撑，难以形成相互联结的结构体系。根据凯尔森的规范等级理论，在一国的法秩序内部，法律应该表现为阶层有序的法律体系架构，高级规范调整着低级规范的创造，低级规范的内容根据高级规范创造而来。^{〔11〕}法律体系作为规范的等级体系，必须符合法秩序中的阶层关系。当前，网络暴力治理的法律外部规范体系主要由相关法律与下位的部门规章与规范性文件组成。其中，民法典、刑法、网络安全法、个人信息保护法等法律，只能对网络暴力进行附带调整和间接规制；下位的部门规章与规范性文件，如《网络信息内容生态治理规定》（2019）、《互联网跟帖评论服务管理规定》（2022）等，由于缺乏统一的上位法依据，在网络暴力治理中“各自为政”，对于网络暴力的概念范畴、责任主体、义务内容、责任形式等表述不一。

在网络暴力治理的规范衔接层面，参与网络暴力治理的部门法之间联动不足，在体系融贯上存在阻碍。法律体系是规范的秩序体系，相同位阶的规范之间必须保持和谐融洽关系。^{〔12〕}在实体法上，不同部门法在对网络暴力的违法性评价标准上缺乏清晰界限，导致网络暴力治理的规范体系协调不畅。尤其是，受刑民不分和以刑为中心的传统法制影响，这种分散性的法治模式导致民事层面存在网络暴力治理短板，在刑事层面却出现了网络暴力治理过度现象。在程序法上，网络暴力执法的取证环节缺乏统一的标准和程序，民刑之间、行刑之间均未建立明确的程序转换机制，这也导致法律衔接适用困难，难以发挥整体性治理功能。

（三）网络暴力治理的法治效能不彰

当前网络暴力治理的法治效能不彰，根源在于法律规范与技术发展之间存在张力。进入数字时代以来，法律的发展经常无法与计算机网络的发展同步。当立法机关或者司法机关刚刚决定如何应对一个新产品或者新服务的时候，技术又发生了变化。^{〔13〕}网络暴力发生在虚拟化、数字化的网络空间中，是具有明显的群体属性、跨越双重空间的新型暴力模式，网络暴力相对于传统暴力的特殊性，导致传统的法律治理模式陷入失效困境。

1. 网络暴力治理的法律规制范围存在局限性

在瞬息万变的科技社会中，法律概念的科学滞后性愈加明显。^{〔14〕}网络暴力依托于信息技术支撑的网络平台，不仅涉及多元的参与主体，也呈现出复杂的因果关系，因而网络暴力风险

〔10〕 参见张志铭：《法律解释学》，中国人民大学出版社2015年版，第122页。

〔11〕 参见〔德〕凯尔森：《法与国家的一般理论》，沈宗灵译，中国大百科全书出版社1996年版，第150页。

〔12〕 参见陈清秀：《法理学》，中国台湾元照出版有限公司2017年版，第398页。

〔13〕 See William Jeremy Robison, *Free at What Cost: Cloud Computing Privacy under the Stored Communications Act*, 98 Georgetown Law Journal 1197 (2010).

〔14〕 参见郭春镇：《生成式AI的融贯性法律治理——以生成式预训练模型（GPT）为例》，《现代法学》2023年第3期，第99页。

具有不确定性,超出了既有法律规则的应对能力。

网络暴力行为呈现虚拟性与现实性相结合的特点。从行为方式来看,网络暴力是利用网络信息的传播功能对当事人实施侮辱、诽谤、攻击、谩骂等不法行为;从行为后果来看,网络暴力会给现实生活中人们的合法权益造成各种负面影响。这种虚拟性与现实性相结合的特点,会给法律上的因果关系认定造成困难,导致大量的网络暴力行为难以被纳入传统的法律规制范围。网络暴力实施者利用新技术手段,借助文字、语音、图片、视频等对受害人进行全方位侵害,具有识别难、提告难等特质,增加了网络暴力因果链条在事实上的认定难度。^[15]网络暴力事件中的因果关系大多具有间接性,难以适用传统的因果关系理论。以刑法为例,传统刑法理论重视有形暴力和有形伤害,对于以网络暴力为代表的无形暴力、无形伤害相对较为轻视。在适用传统理论判断诸如自杀等恶性后果与网络暴力之间的因果关系时,易得出否定的结论。然而,越来越多的证据与案例显示,网络暴力与精神障碍、自杀自残等恶性后果间存在切实关联。现代脑神经科学研究表明,当受害者遭受言语威胁或情感虐待时,他们的大脑产生的生理变化与遭受物理伤害时产生的生理变化是一致的,因而精神伤害也是一种身体伤害。^[16]受限于传统归责理论对精神损害的轻视,网络暴力案件中的法律因果关系很难得到认定,这不利于对被网暴者展开全方位的法律保护。

网络暴力行为的特殊性还表现在参与主体的群体性上。用传统的法律规制方式应对群体性网络暴力侵权行为,很难取得理想的治理效果。当前的网络暴力现象呈现出明显的职业化、产业化趋势,“网络水军”“黑公关”“键盘侠”等,都是聚众实施不法行为的职业性个体或群体的代名词,蓄意发起、煽动滋事类的网络暴力行为亦具有极强的组织性、群体性。例如,张某某为发泄个人情绪,画了侮辱和讽刺江歌母女的漫画,并使用多个微博账号传播,其中一个账号发布的微博被转发一千五百余次,被点击浏览一千余万次。^[17]网络暴力牵涉网络空间中的海量个体,而传统法律预设的行为类型主要以单个行为主体为中心,在治理网络暴力方面难以发挥应有作用。

2. 网络暴力治理的法律责任缺乏威慑性

与线下语言暴力的危害后果相比,网络暴力的危害后果往往更为严重。这主要体现在以下方面:(1)网络暴力造成的危害后果具有系统性。网络暴力对个人权利和社会公共秩序都具有侵害性。在个人权利层面,网络暴力既损害被害人的身心健康,也会因网络信息泄漏而危及个人财产安全。在社会与国家层面,网络暴力既荼毒互联网健康生态,也影响一国的国际形象。(2)网络暴力的危害具有持续性。网络暴力能够持续较长时间且会不断重复,尤其是针对一些公众人物,网暴的持续时间能够达到数月乃至数年,这将给被害人的情感与心理造成巨大伤害。(3)网络暴力造成的危害具有不可逆性。网络暴力因其数字属性而具有内容留痕性,施暴者可以利用网络不断扩大信息传播的受众面,并留下永久性的数字内容,使被害人所受身心摧残无法得到彻底治愈。^[18]

现行法律对网络暴力行为施加的处罚整体较轻,不具有实际的震慑效果,难以发挥长期治理功效。在行政处罚中,治安管理处罚法是网络暴力治理的主要法律依据。根据该法第42条,

[15] 参见王静:《数字公民伦理:网络暴力治理的新路径》,《华东政法大学学报》2022年第4期,第30页。

[16] 参见徐颖:《论“网络暴力”致人自杀死亡的刑事责任》,《政法论坛》2020年第1期,第138页。

[17] 参见张剑:《“画”地为牢:淮南女子侮辱江歌母女获刑》,《安徽商报》2021年5月18日第8版。

[18] 参见吴进娥:《性犯罪网络传播行为刑罚裁量的功能主义诠释》,《东南法学》2022年第2期,第178页。

如果网络暴力行为涉及公然侮辱他人、捏造事实诽谤他人、散布他人隐私,就应受到行政处罚。但是,即使这类网络暴力行为达到“情节较重”的程度,行政机关也仅能给予行为人10日以下的行政拘留和500元以下的顶格罚款。在刑事处罚中,针对网络暴力犯罪行为施加的刑罚同样过轻。我国现行刑法中虽有侮辱罪、诽谤罪、侵犯公民个人信息罪、寻衅滋事罪等罪刑条款,但它们都是围绕传统违法犯罪的法益侵害性进行的立法设置,在追究网络暴力的刑事责任方面往往力度不够。^[19]例如,根据刑法第246条的规定,即使是严重影响被害人生活、给被害人造成重大精神损害的侮辱、诽谤行为,也只处3年以下有期徒刑或拘役;如果存在认罪认罚等其他量刑减免情节,施暴人所受刑罚将更加轻微,与其行为的法益侵害性无法匹配。

二、网络暴力治理的法治理念与模式

党的二十大站在全面建设社会主义现代化国家的战略高度,提出推进国家安全体系和能力现代化的关键命题,对完善社会治理体系作出重要部署,要求防控化解网络安全风险等重大风险。国家治理现代化的核心要义在于制度之治,它要求实现从法律体系向法治体系的全面转向,通过法治改革推进治理革命,进而实现从前现代向现代化的根本转型。^[20]网络暴力问题是新时代国家治理过程中的重大性、交叉性、领域性难题,必须运用现代法治思维予以应对。明确网络暴力治理的法治理念与法治模式,是推动网络暴力治理在法治轨道上有效运行的前提。

(一) 网络暴力治理法治理念的确立

为了适应网络空间自身的技术演化规律,为网络暴力治理提供有效的法治方案,我国应积极调整网络暴力治理的法治理念,实现从分散治理向协同共治的转型,打造网络空间的良法善治。中共中央印发的《法治社会建设实施纲要(2020—2025年)》要求,要完善党委领导、政府负责、民主协商、社会协同、公众参与、法治保障、科技支撑的社会治理体系,打造共建共治共享的社会治理格局。我国网络安全法第7条规定“推动构建和平、安全、开放、合作的网络空间”,“建立多边、民主、透明的网络治理体系”,也表达了网络空间治理的协同共治理念。在网络暴力治理领域确立协同共治理念,一要实现多元治理主体的协同,二要促进法律规制与技术治理的协同。

1. 多元治理主体的协同共治

网络暴力治理是一项系统性的风险治理工程,离不开广泛的民主参与和多元主体的协同共治。社会协同理论研究显示,越复杂的社会系统越需要协同,政府、社会组织与公众之间的有效协同,对复杂社会系统治理具有正面积极的作用。^[21]网络暴力风险在诸多方面迥异于传统社会的风险类型,其具有隐蔽性、虚拟性、不确定性等特点。并且,网络技术的更新、用户规模的增长和网络产业的勃兴,也使网络暴力呈现出利益驱动化、组织产业化、专业分工化与群体对立化的复杂发展态势。传统的风险管理理念,强调的是公权力的单向管控,注重以行政命令的方式解决社会矛盾,并不适应网络社会的利益格局,无法满足网络暴力治理现代化的发展需求。风险治理理念强调权力与权利的双向互动,注重市场主体的多元合作,有助于建立网络

[19] 参见石经海、黄亚瑞:《网络暴力刑法规制的困境分析与出路探究》,《安徽大学学报(哲学社会科学版)》2020年第4期,第78页。

[20] 参见汪习根:《论中国式法治现代化的理论体系》,《政法论坛》2022年第6期,第13页。

[21] 参见范如国:《复杂网络结构范型下的社会治理协同创新》,《中国社会科学》2014年第4期,第107页。

空间命运共同体。^{〔22〕}在网络暴力治理中引入风险治理理念,旨在充分激发多元主体在网络暴力治理中的作用,形成公权力与私权利有机协同的治理体系。

首先,网络暴力治理需要在政府部门之间实现内部协同共治。在网络暴力治理中,监管部门发挥着核心导向作用,各个监管部门的职能配置,关系到网络暴力治理的整体功效。按照网络安全法第8条的规定,国家网信部门负责统筹协调网络安全工作和相关监督管理工作,国务院电信主管部门、公安部门和其他有关机关依法在各自职责范围内负责网络安全保护和监督管理工作。网络安全治理的权力配置呈现“九龙治水”特征,这将为网络暴力监管权力运行的部门主义和碎片化埋下隐患。着眼于权力运行的功能和效率,权力应当配置给组织结构最优的职能部门。^{〔23〕}为实现最佳的治理效果,应当建立一种相互依存、功能有序的权力配置体系,使网络暴力治理监管部门在职能分工的基础上相互合作,实现功能协同。

其次,网络暴力治理需要在政府与社会主体之间实现外部协同共治。在治理现代化视域下,通过整合与协调公私主体,可以实现网络规制与网络自治、国家管制与技术革新、国家利益与网络用户利益的平衡发展。目前,以多元共治模式建构网络空间秩序已逐渐成为各界的共识性主张,^{〔24〕}网络暴力治理体系同样需要政府、平台企业、社会组织、广大网民共同参与,共筑网络安全防线。具体而言,政府应当发挥统一引导功能,积极搭建网络暴力治理的宏观框架,包括明确治理的基本理念与基本方向,在整体治理政策制定、立法工作推进、行业监管中发挥主导作用。平台企业应发挥在网络暴力治理中的基础性作用。网络平台所拥有的技术架构,使其在网络暴力治理中具有天然优势。为激发网络平台的治理活力,应持续优化平台的信息监管技术,赋予并充分信任平台对网络暴力行为的处置权。在共建共治共享的社会治理格局下,网络暴力治理需要各行业各领域积极参与。行业自治是网络社会治理法治实施体系的重要内容。^{〔25〕}推动互联网行业组织形成关于网络暴力治理的行业规范公约,为各平台的协同治理工作提供可以共同参考的标准,有助于行业内部形成网络暴力治理共识并展开普遍自治。公民作为网络空间治理的主力军,应当积极参与网络暴力治理,既要全方位提升自身的网络素养,严格遵守网络行为规范,也要积极监督不良网络言行,为净化网络空间贡献力量。

2. 法律与技术的协同共治

随着网络技术革命的发生及网络技术应用的普遍化,我国的社会形态已发生结构性变革。网络空间兼具社会性与技术性双重特质,技术自始便参与了网络空间的社会建构,技术治理也顺势成为网络暴力治理的重要手段。然而,网络技术变革也会对传统社会治理及其法律规范体系造成冲击,^{〔26〕}信息技术发展的变动性与法律规范的安定性之间也存在一定的紧张关系。正因如此,网络空间治理体系强调整体性和协同性,在网络暴力治理的过程中,应当遵循法律规制与技术治理相互协同的共治理念,协调好法律与技术的关系。

其一,以技术驱动网络暴力治理范式的现代化转型。网络暴力治理需要跳出单向度的制度性治理思维,在技术辅助论理念的指引下,遵循网络技术发展规律,融入技术思维,提升网络

〔22〕 参见周佑勇:《社会主义核心价值观融入网络空间治理现代化的法治逻辑》,《江苏行政学院学报》2022年第1期,第125页。

〔23〕 参见〔英〕马丁·洛克林:《公法与政治理论》,郑戈译,商务印书馆2002年版,第189页。

〔24〕 参见童建明:《最有利于未成年人原则适用的检察路径》,《中国刑事法杂志》2023年第1期,第6页。

〔25〕 参见于冲:《网络“聚量性”侮辱诽谤行为的刑法评价》,《中国法律评论》2023年第3期,第96页。

〔26〕 参见徐汉明:《我国网络法治的经验与启示》,《中国法学》2018年第3期,第65页。

暴力治理效能。首先,技术治理具有自主更新能力,能够形成与网络暴力风险适配度更高的治理措施。技术工具具备“跟随开发”“及时完善”的功能优势,可以与网络空间的技术架构、网络平台的功能、网络内容的传播形式等同步发展,从而更高效地应对新型网络暴力风险。其次,技术工具可以弥补法律规则的滞后性。法律规制属于“被动型”治理策略,技术防护则是“主动型”治理策略。通过发挥网络暴力治理技术在实时监测、精准研判、动态防御、常态威慑等方面的功能优势,能够提升对网络暴力风险态势的实时感知和反应能力,充分保障网络空间安全。

其二,以法律制度促进网络暴力治理技术向善发展。网络暴力治理应建立在法治逻辑基础上。技术治理主要以技术编码与自治伦理为基础,与以规范为核心的法律治理方式不同,技术治理是自成体系的治理方式。^[27]技术治理具有突破制度调控的自主发展趋势,不仅直接影响网络空间治理权责的重新界定,也存在潜在的治理风险。例如,网络平台的暗箱操作与技术霸权等,直接威胁到网络暴力治理的公正性。网络暴力治理中的技术治理,仍需接受法治的规范监管。为此,必须配置完备的法律监管制度,依托法治理性明确网络技术的发展边界,确保先进的网络安全技术在法治轨道上充分发挥防治网络暴力风险的功能。

(二) 网络暴力治理的法治模式之选择

良法善治是新时代网络暴力治理现代化的价值根基,^[28]而网络空间的良法之治主要表现为规则之治,它要求“构建完善的网络空间治理规则体系,为网络空间运行提供规则指引,为网络安全风险提供规制工具,为信息化发展提供强制保障”。^[29]为了建构中国网络暴力治理的良法善治路径,需要推动网络暴力治理的法治模式由分散性法治模式向系统性法治模式转型。“智能时代的法律秩序将与传统社会的法律秩序截然不同,要求改变传统法律观念,构建完善的法律供给机制与法律保障体系。”^[30]网络暴力是复杂社会问题在网络空间的“镜像”,网络暴力风险属于新型重点领域风险。相应地,网络暴力治理的法治模式也应适应网络技术治理跨领域、交叉性的客观规律。分散性法治模式属于碎片化的部门法治,其缺乏体系性和协同性,对于网络暴力的整体规制能力不强。系统性法治模式对应于集成化的领域法治,其强调法治的整体性与协调性,能够充分发挥立法的合力作用。为提升反网络暴力立法的治理能力,网络暴力治理宜采取系统性法治模式,即充分发挥民法、行政法与刑法治理网络暴力的协同配合功能,并在此基础上制定领域性的反网络暴力专门法。

1. 分散性法治模式的局限性

中国目前的网络暴力治理法治格局呈现分散性,主要表现为由多个部门法共同承担反网络暴力的治理功能。分散性法治模式以部门法为基础,其优势在于,能够结合网络暴力发生的具体环节与场景作出有针对性的规定。并且,相关部门法的修正较为容易。但是,这种法治模式的缺点也十分明显。我国可用于规制网络暴力的法律规定散见于民法、行政法、刑法等部门法领域的多部法律法规、部门规章及司法解释中,这种法治资源配置带有明显的部门法主义倾向,难以产生整体性的社会治理效果,甚至会严重影响网络暴力的治理效能。

首先,分散性法治模式制造了大量的重复性立法,且能够发挥实际作用的规范数量较少,

[27] 参见冀洋:《“网络空间不是法外之地”的刑法分析》,《中国法律评论》2023年第3期,第109页。

[28] 参见张文显:《习近平法治思想的政理、法理和哲理》,《政法论坛》2022年第3期,第13页。

[29] 前引[22],周佑勇文,第123页。

[30] 周佑勇:《论智能时代的技术逻辑与法律变革》,《东南大学学报(哲学社会科学版)》2019年第5期,第70页。

多数规范被束之高阁,“立而不用”或“立而少用”,造成“法律贬值”。在我国目前的法律制度体系中,民法典、刑法、个人信息保护法、数据安全法、网络安全法,以及诸多部门规章、司法解释,都与网络暴力治理存在间接关联。这些法律法规或司法解释的数量看似很多,但在网络暴力的治理过程中,能够真正发挥作用的立法资源却较为匮乏。究其原因,一是上述法律法规或司法解释,在网络暴力规制方面存在大量的重复性规定;二是面对愈加复杂的网络暴力发展态势,各个部门法在网络暴力的调整范围、追责方式等方面衔接不畅,导致法律适用过程中矛盾与分歧频发;三是从条文具体内容上看,多数立法仅对网络暴力行为作出了禁止性规定,却没有为之匹配具体的责任条款。

其次,分散性法治模式变相增加了法律系统的运行成本,导致执法部门的职责界限难以清晰划分,容易滋生法律适用的文牍主义及选择性执法。^[31]职责清晰是有效执法的重要前提。由于网络暴力间接关联了大量法律规范,而不同法律规范的执法主体各异,假如各执法主体之间缺乏协调和配合,针对网络暴力的执法就会出现权责不清的问题。由此,当国家重点打击网络暴力时,不同的执法部门可能相互竞争;当网络暴力治理进入常态化时期,执法部门之间又可能相互推诿。前一情形会造成执法资源的浪费,后一情形则会降低执法效率,二者都将影响网络暴力治理的实际效果。

最后,网络暴力治理的部门法治资源分配不成比例,刑事制裁手段在整个网络暴力治理体系中占据绝对优势地位,而前置的预防性行政管理措施、相对柔和的民事制裁手段相对缺位。过度依赖刑法治理网络暴力,既不符合网络发展的技术性特质,又会带来诸多附随问题。譬如,网络暴力治理缺乏对网络空间自身的契约规制与技术规制的认识和尊重,刑罚模式等国家强制力过多干预,将导致治理机制短效等问题。在尚未完善网络暴力治理的相关前置法规定时,如果直接动用刑事立法扩大处罚范围和惩罚力度,将会陷入“只能治标,难以治本”的形式法治困局。^[32]

总之,分散性法治模式固守传统治理思维,具有明显的滞后性,难以针对数字社会的新型网络暴力问题进行回应性调整,不宜作为我国网络暴力治理的法治模式。

2. 系统性法治模式的功能优势

在重点专项领域进行专门立法,实现从分散性法治模式向系统性法治模式的转型,是法律系统复杂化背景下的科学选择。在多元化的现代社会,立法必须及时关注“社会发展的关键节点”,通过出台领域性专门立法,对信息网络、人工智能等领域的关键问题作出个性化回应。^[33]一些大陆法系国家自20世纪60年代开始就通过解法典化运动开启了这一历程。所谓解法典化,是指在法典之外,针对不同领域制定大量的特别法。这些特别法在规范内容上超越了“一法一部门”的立法格局,并以“领域”作为区分标准,对民事、行政及刑事法律规范进行一体化整合,形成针对某一类型的关系进行持久且有机调整的规范体系。这样的特别法,实质是关于某一制度或者整个事项的一般法。^[34]近年来,我国立法机关也开始反思分散性治

[31] 参见黄籍:《为什么选择性执法?——制度动因及其规制》,《中外法学》2021年第3期,第786页。

[32] 参见喻海松:《网络犯罪黑灰产业链的样态与规制》,《国家检察官学院学报》2021年第1期,第54页。

[33] 参见[意]艾伯特·马蒂内利:《多元现代性与中国式现代化道路》,《中国社会科学报》2021年10月15日第12版。

[34] 参见[意]那塔利诺·伊尔蒂:《解法典的时代》,薛军译,载徐国栋主编:《罗马法与现代民法》第4卷,中国人民大学出版社2004年版,第97页。

理模式的缺陷，并对基于领域性立法的系统性法治模式作出了积极尝试。例如，2021年12月24日，全国人大常委会通过反有组织犯罪法，该法内容涉及有组织犯罪的预防和治理、涉案财产认定和处置、国际合作等多方面，对于有组织犯罪的防治发挥着一般法的功能。又如，2022年9月2日，全国人大常委会通过反电信网络诈骗法，从电信治理、金融治理、互联网治理等方面，对电信网络诈骗的防治作出专门规定，对反电信网络诈骗工作起到统领全局的重要作用。

从分散性法治模式到系统性法治模式，从“一法一部门”到“一法一领域”，这种变化将带来治理效能的根本提升。在规范层面，领域性专门立法对分散性立法进行了批判性吸收，消除了同一事项被不同部门法分散规制所产生的分歧，也创造了更具适应性的新规范与新制度。例如，反有组织犯罪法设有专章，对有组织犯罪涉案财产的认定和处置作出特别规定，纠正了以往有组织犯罪涉案财产处置中的“同案不同判”现象。又如，反电信网络诈骗法设专章规定“金融治理”，明确银行在发现有电信网络诈骗风险时，有义务采取紧急止付等能够有效保护被害人财产的措施，否则需要承担相应的责任。这些富有特色的制度安排，调整的是反有组织犯罪、反电信网络诈骗工作领域的特殊事项，在以往的分散性立法中很难发展出来。领域性专门立法会更加充分地考虑本领域的特殊情况，也更有机会发展出具有创新性且富有实效的特色制度。在法律适用层面，相较于分散性立法，领域性专门立法一体整合了民法、行政法、刑法等部门中的关联法律规范，实现了领域内的法秩序高度统一，能够最大化提升特别领域的治理效能，达到“尽可能用一个法律解决所有相关问题，以方便机关的执法、司法的用法和民众的守法”的效果。^[35]

社会治理“要更加注重联动融合、开放共治，更加注重民主法治、科技创新，提高社会治理社会化、法治化、智能化、专业化水平，提高预测预警预防各类风险能力”。^[36]网络暴力属于综合性社会问题，仅靠单一部门法不足以完成法治化治理任务，需要统筹整体法秩序予以系统应对，构建一体化的网络暴力法律治理体系。^[37]面对网络暴力及其带来的负面影响，法律体系积极参与治理的重心，应调整为主动促成各部门法的有效衔接，及时转变以往网络空间治理的刑法依赖模式，实现前置的预防性法律和相对柔和的制裁手段的先行治理。网络暴力治理涉及网络空间中的矛盾预防与化解等多个方面，网络暴力犯罪只是其中危害性最大的问题，相应地，刑事法治方式也只是治理的重要手段之一。在网络暴力治理法律体系中，刑法应该作为严重性后果的保障性的制裁手段。民法典、网络安全法、个人信息保护法等前置法律规范提供的治理手段，应当更加丰富、更有针对性，以促成“从事后追责转向事前预防”的模式转型。例如，“网课爆破”这种蓄意的有组织的网络暴力事件，可能造成网络空间公共秩序受损并危害公民生命健康安全，在平台监测到相关信息后，需要从法秩序的整体角度来评析网络暴力的行为性质与法益损失，通过民行刑共治来处理。

系统性法治模式的重要特征在于立法的系统性。传统立法范式构造出的是泾渭分明的“一法一部门”格局，难以为跨部门法领域的网络暴力治理提供整全性规制。数字时代的立法

[35] 苏永钦：《寻找新民法》，北京大学出版社2012年版，第78页。

[36] 《习近平就加强和创新社会治理作出重要指示强调 完善中国特色社会主义社会治理体系 努力建设更高水平的平安中国》，《人民日报》2016年10月13日第1版。

[37] 参见黄文艺：《推进中国式法治现代化 构建人类法治文明新形态——对党的二十大报告的法治要义阐释》，《中国法学》2022年第6期，第24页。

范式强调交叉融合,其以领域性立法为导向,聚焦于重点领域的风险治理。2023年2月,中共中央办公厅、国务院办公厅印发的《关于加强新时代法学教育和法学理论研究的意见》,明确提出要推动学科交叉融合发展,其用意也在于进一步推动领域法学的发展,构建适应数字时代技术治理规律的领域法治。在领域法治思维的指导下,国家应当制定专门的反网络暴力法,统领其他具有网络暴力治理功能的部门法规范,形成以反网络暴力法为核心的网络暴力治理立法体系。

三、网络暴力治理的立法体系构建

我国已经进入反网络暴力的法治治理阶段,但由于核心制度尚未形成,反网络暴力治理难以提升质效。立法是法治之基础。确立科学的立法体系,明确有效的立法路径,避免立法的无序化、低效化,是加快推进我国反网络暴力立法的前提。^[38]传统法律体系无法回应数字时代的网络暴力治理需求,为营造健康有序的网络暴力治理生态,必须统筹推进反网络暴力立法体系构建,推动网络暴力治理法治模式由分散性向系统性转型。

(一) 制定反网络暴力法的意义与功能

制定反网络暴力法,是国家治理体系现代化视域下完善网络空间治理法律体系的重要之举,也是重构网络暴力治理法律秩序的体系根基。当前我国治理网络暴力的相关法律规定内容分散且缺乏协调配合,难以应对日趋泛滥的网络暴力问题,故应考虑推进集预防、遏制和惩治网络暴力于一体的反网络暴力法出台。由反网络暴力法针对防治网络暴力相关问题作出专门性、领域性、体系性规定,以提高反网络暴力法律规范的适用性、衔接性和可操作性。

在协同共治理念与系统性法治模式的指引下,宜遵循领域性立法思维来制定反网络暴力法,以深化网络暴力治理的领域法治路径。领域法立足于对经济社会发展变化中的许多交叉联动的新兴领域和重要现实问题的关切,试图找到一条开阔的立法进路解决从传统的学科理论到社会现实应用的融通问题,其既能够对领域之外的新型社会问题保持灵活性与开放性,又能够在领域之内维持法律体系的稳定与统一。^[39]相较于部门法,领域法在结构上具备适当的开放性,能够积极适应数字时代社会关系的复杂变迁并及时作出调整。领域法采取的是一种整合性的立法路径。在立法技术上,通过把整个领域内具有共通性的法律问题以提炼公因式的方式加以规定,^[40]能够发挥概念涵摄与体系统合的功能;在立法内容上,就某个领域内的一般性制度规定,提取出一个纲领性的结构框架和原则性的法律秩序,将具体详细的法律内容交由领域内的部门法来完成,能够为领域内部门法律制度的独立发展预留足够的裁量空间,从而保证整个领域性法律体系的开放与灵活。领域内的部门法可以随着技术条件的发展与社会形势的变更,随时作出调整和应变。这样既能增强整个领域法体系的弹性,也可为领域法治革新注入社会活力。领域法是在多元复杂的法律规范的集聚基础上形成的结构稳定、体系完整的复合型法律,能够保证领域内法律系统的稳定与统一,使某个领域的法律制度不至于朝令夕改。法律的作用在于形成并维护普遍的社会秩序,法律的内容必须在一定程度上具有普遍性。^[41]领域法

[38] 参见郭旨龙:《网络暴力刑法治理的解释原理》,《江汉论坛》2023年第5期,第126页。

[39] 参见侯卓:《领域法思维与国家治理的路径拓补》,《法学论坛》2018年第4期,第100页。

[40] 参见周佑勇:《中国行政基本法典的精神气质》,《政法论坛》2022年第3期,第65页。

[41] 参见[日]川岛武宜:《现代化与法》,王志安等译,中国政法大学出版社2004年版,第266页。

具有广泛的适用空间和充分的解释余地，其通过将某个领域内所有实质上相同的规范内容与调整对象统一起来，按照一定的逻辑结构和体系编排，形成了一个可以普遍适用的有机领域法整体。

反网络暴力法是中国网络暴力治理迈向法治化的体系支点，属于网络暴力治理领域的基础性法律，在网络暴力治理法律体系中居于领域法地位。网络暴力问题属于网络空间中的重点风险领域，该领域所涉问题的综合复杂性与法律交叉性，决定了很难通过修改一两部法律来达到源头治理的目的。领域性立法思维要求整合相关学科的法治资源，促进各个部门法交叉融合发展，以回应网络时代的重大领域性风险问题。伴随着现代公共治理模式的崛起，“传统的法范式陷入了严重危机之中，一种与公共治理相适应的回应型法开始取而代之”。^{〔42〕}立足于回应型立法的开放性与变革性理念，为适应新时代科技高速发展的要求，网络暴力领域的立法必须以解决重大网络暴力风险问题为导向，而不是以部门法为依托。反网络暴力法作为专门应对网络暴力问题的领域法，在治理范围上具有充分的涵摄性，能够贯通网络社会与现实社会中的网络暴力问题，构建全面系统的网络暴力治理制度。基于反网络暴力法的领域法性质，网络暴力治理亦可跳出部门法的思维局限，实现横跨公私法秩序的协同治理。

反网络暴力法在整个网络暴力治理领域中具有体系整合功能，可以统摄分散在各个部门法中的法律条文，整合具有关联性的具体制度，解决法律之间的协调不足和矛盾冲突问题，从而实现网络暴力治理的法治融贯统一。领域法是在部门法的基础上制定的综合性规定，具备“公私兼顾”的属性。反网络暴力法作为国家网络暴力治理领域的基本法，立足于从各个部门法中提炼出的涉及网络暴力治理的基本原则、管理体制与法律责任等纲要性内容，以基础性、专门性与特色性法律制度为框架，针对网络暴力形成更具主动性、系统性、协同性的治理理念与机制，可以统领网络暴力治理的整体法律秩序。反网络暴力法作为网络暴力治理体系的关键枢纽，将能在网络暴力治理法治体系中发挥沟通作用，其不仅是对网络安全法中具体要求的贯彻和落实，也可以强化自身与民法、刑法等部门法的衔接，系统性推进网络暴力治理的立法体系建构。

（二）框架秩序：创设网络暴力治理的基本法律制度

传统的网络治理法律规范体系无法有效回应新型网络暴力问题的治理需求，关键原因在于其在网络暴力治理的权责主体、制裁方式、救济措施等方面存在制度疏漏。故而，反网络暴力法应从基本概念、管理体制、治理机制、法律责任等方面，明确网络暴力治理的基本法律制度，为网络暴力治理提供系统全面的规范支撑。

首先，反网络暴力法作为治理网络暴力的基本法，应将明确网络暴力的判断标准、对网络暴力内容进行科学分类分级作为首要立法重点。纵观我国立法及理论流变，关于网络暴力的界定主要存在以下观点：（1）狭义界定。这种观点认为网络暴力仅仅涵盖对被害人的中伤或直接侵害，网络侮辱、网络诽谤等属于典型的网络暴力；^{〔43〕}（2）广义界定。相较于狭义界定，这种观点将滋扰行为也纳入到网络暴力中，认为网络暴力包括各种类型的网络软暴力；^{〔44〕}

〔42〕 罗豪才、宋功德：《软法亦法：公共治理呼唤软法之治》，法律出版社2009年版，第8页。

〔43〕 参见前引〔19〕，石经海等文，第79页。

〔44〕 参见魏汉涛、陈心哲：《四步认定法：化解“软暴力”扩大化风险的路径——基于230份裁判文书的分析》，《中南民族大学学报（人文社会科学版）》2022年第1期，第109页。

(3) 最广义的界定。这种观点将未被受害人所感知的行为也纳入到网络暴力的范畴。^[45]笔者认为,法律概念应具有开放性,应能适应时代的变化而不断扩大其外延,并且,网络暴力作为客观事实,其存在与否不以被害人感知为前提。因此,笔者提倡对网络暴力作最广义的界定,并以此为基础对网络暴力进行分类。当前,被各国纳入治理范围的网络暴力主要包括网络欺凌、网络诽谤侮辱、网络仇恨言论、网络跟踪、网络恐吓等类型,这些均可作为我国反网络暴力法的调整对象。

其次,在管理体制上,反网络暴力法应确立政府监管、行业自律、企业规范、公民参与的协同治理体制。中央网信办的成立有助于垂直领导网络暴力治理,但由于各个监管部门的职能配置并不明确,不利于及时高效地应对风险泛在的新型网络暴力事件。如何进一步强化中央网信办在信息内容治理中的主导作用,如何使各行业主管部门形成监管合力,是反网络暴力法要着力解决的问题。基于此,有必要在反网络暴力法中细化网信部门的主导职责,明确电信、公安、文化、教育等相关部门的协助职责,制定网络暴力治理部门的权力清单和责任清单。互联网环境复杂且技术性强等特点,给政府监管带来一定困难。网络行业自律是互联网治理不可或缺的部分。政府可以引导行业协会制定网络暴力治理技术规范,将技术标准融入治理过程中,以标准化带动技术规制健康发展,提升网络暴力治理水平。网络平台是信息内容管理的第一责任主体,其不仅作为网络服务提供者或网络暴力的发生场所而存在,更应主动充当网络暴力的积极治理者之角色。反网络暴力法应进一步压实网络平台的主体责任,赋予网络平台在网络暴力治理的监测预警、信息传播扩散、当事人保护、应急处置等环节的管理职能,并严肃处罚失职失责的网络平台。网络暴力治理人人有责,公民亦应积极参与网络暴力治理。反网络暴力法可以从公民层面出发确立源头治理目标,为公民养成良好的网络文明素养、培育数字公民伦理、强化公民的法律意识和法治思维等提供条件,以促进公民严守言论自由的义务边界、规范自身网络行为。

再次,在治理机制上,反网络暴力法应针对网络暴力建立预防、监测、处置、救助的全链条治理框架,形成常态化的全流程治理机制。在事前预警阶段,反网络暴力法应注重从网络信息内容审查与加强技术设置等方面来预防网络暴力行为。尤其是网络平台应确立网络暴力预警预防机制,即建立内容审核过滤机制,构建网暴技术识别模型、网络暴力应急响应机制和首发溯源机制。在过程监测阶段,反网络暴力法应明确要求监管部门和网络平台对网络暴力进行监测与识别,并及时报告、通报、公布正在发生的网络暴力行为。在事后响应阶段,反网络暴力法应确立相关网络监管部门可以对网络暴力行为采取的应急处置措施类型,并规定相关机构应对网络暴力受害人提供法律援助和社会援助,以降低网络暴力的后续影响。另外,在网络暴力治理的长效机制中,应突出对未成年人和妇女等重点人群的保护,并在反网络暴力法中设置专门的预防与应对机制。

最后,有必要在反网络暴力法中设置“法律责任”专章,综合考量网络暴力行为的危害程度、施暴者的主观恶性以及社会影响等多重因素,合理配置施暴者所应承担的民事责任、行政责任和刑事责任,并理顺三者的界限与联系,构建起层次分明、轻重适当、衔接顺畅的网络暴力责任追究体系。反网络暴力法可以通过引致性条款来配置相应的法律责任,根据网络暴力行为严重程度的不同,指向各部门法针对各类违法犯罪行为规定的责任条款,实现整体法秩序

[45] 参见储陈城:《刑法应对网络暴力的流变及其基本立场》,《中国刑事法杂志》2023年第4期,第46页。

的有机联动。此外,为扩大对网络暴力的法律规制范围,在刑事责任方面,建议作如下调整:适度扩大责任主体范围,对恶意发起者、组织者、推波助澜者、屡教不改者以及其他积极参与人员追究相应的刑事责任;区分核心行为与外围行为,上述人员之外的参与者可视为外围行为人,对其应优先适用非刑罚处罚措施,确保行为与责任相适应;将造成被害人自杀、自残或罹患精神疾病等作为对涉案人员从重处罚的情节。

(三) 系统协调:完善网络暴力治理的配套法律制度

网络空间中的暴力行为深受社会环境和技术发展的复杂影响,相应地,网络暴力治理也是一项复杂的系统工程。反网络暴力法只能确立法律规制的总体框架与原则性内容,在反网络暴力法的基础上,还需要制定一系列配套制度,为执法和司法部门提供明确的规则指引。完善网络暴力治理配套法律制度的关键,是要鼓励各个职能部门和地方政府从立法执法司法守法各个维度,全方位构筑反网络暴力制度体系,形成以反网络暴力法为中心、授权性立法为辅助、配套性制度相结合的内容完备、层级分明的网络暴力治理法律规范体系。

首先,建议国务院制定“网络暴力防治条例”。反网络暴力法只能针对防治网络暴力的一般性问题和重要性问题作出概括性规定,在网络暴力治理实践中,还有许多具体问题需要通过制定其他法律或制定实施细则来解决。由国务院先行制定“网络暴力防治条例”,有助于积累实践经验,为制定更高位阶的法律规范奠定基础。^[46]在具体内容上,该条例可以对网络暴力的多元共治机制、监测预防机制、干预处置机制、制裁救济机制等作出详细的制度安排,实现网络暴力治理从粗放式治理到靶向式精准治理的转变。在多元共治机制上,需要细化政府监管、网络平台协助、社会多元主体参与的机制安排。例如,可为公民参与网络暴力治理提供具体的法治渠道。在监测预防机制上,为在网络暴力形成前期做好网络信息审查与舆论监测工作,有必要建构信息分级与审查机制、网络暴力识别与预警机制,还可考虑对一些重点平台或重点人群进行动态监测。在干预处置机制上,在网络暴力行为持续期间,为避免网络暴力危害后果的扩大化,有必要及时阻止相关暴力言论,为当事人权利提供实时保护,并通过教育引导、信息公开等方法,及时澄清谣言,平息网民情绪,进行舆论引导。在制裁救济机制上,除了应当明确民事、行政、刑事等责任衔接机制,还应细化政府、学校、家庭、平台等各方面义务与责任,建构对网络暴力受害者的帮扶与救济体系。

其次,加快“未成年人网络保护条例”出台进程,强化对未成年人的网络保护。常见的网络欺凌是严重的网络暴力行为,会给未成年人的身心健康带来巨大伤害,对未成年人加强保护的必要性自不待言。在网络暴力事件中,未成年人也可能是暴力实施者,其隐私和个人信息也需要受到保护。当前,网络暴力的实施主体呈现低龄化趋势,^[47]但我国现行法律法规尚未针对未成年人的网络欺凌问题作出专门规定,未明确未成年人遭受网络欺凌时监护人、学校、平台企业的强制报告义务、救助方式、救助程序、失职责任等,无法为未成年人提供较为全面、立体的保护。目前,“未成年人网络保护条例”已列入2023年度国务院立法工作计划,建议在该条例中设置“网络欺凌防治”专章,对参与未成年人网络欺凌治理的各方主体的权利(力)、职责以及常态化协作机制作出明确,尤其要建立校园网络暴力防范、干预和救济机

[46] 参见支振锋:《治理网络暴力还需综合施策》,《中国党政干部论坛》2022年第7期,第77页。

[47] 参见施鑫:《犯罪场域下网络暴力行为的控制路径》,《哈尔滨工业大学学报(社会科学版)》2018年第1期,第34页。

制。例如,《关于切实加强网络暴力治理的通知》提出要“坚持最有利于未成年人的原则,优先处理涉未成年人网暴举报”,2023年7月7日中央网信办发布的《网络暴力信息治理规定(征求意见稿)》也在“保护机制”一章中特别强调为未成年人提供特殊、优先保护。未来的“未成年人网络保护条例”可以吸纳这些具有特色的制度安排。此外,该条例还应细化未成年人保护法第5章“网络保护”中的规范内容,在预防和规制网络暴力问题上进行有效协调,加快形成未成年人网络暴力治理领域的梯次化规范体系。

最后,建议最高人民法院、最高人民检察院修订网络暴力治理相关司法解释。为促进精准打击网络暴力违法犯罪行为,司法机关可以根据实际情况适时出台司法解释。在民事司法解释方面,建议在网络暴力事件中加强对公民人格权利的保护。公民遭受网络暴力或者面临遭受网络暴力的现实危险时,其人格权利经常会受到侵害,且难以获得及时充分的救济。民法典第997条规定了人格权侵害行为禁令制度,这种高效快捷的人格权请求权的程序实现机制,能够及时制止侵害人格权的行为,避免权利人受到更为严重的侵害。^[48]因此,建议最高人民法院在制定“人格权侵害禁令司法解释”时,将网络暴力事件中公民遭受的人格权损害纳入保护范围。当行为人在网上散播严重毁损他人名誉的言论时,受害人应有权申请法院颁行禁令,要求网站采取封锁账号、屏蔽信息、断开链接等措施,以防止损害后果的扩大。

在刑事司法解释方面,将造成严重危害后果的网络暴力案件纳入公诉案件范围,更有助于提升网络暴力治理的绩效。例如,“杭州女子取快递被造谣出轨案”从自诉转为公诉,^[49]在一定程度上震慑了“法不责众”的施暴者心理,有助于维护网络空间秩序。基于网络暴力愈演愈烈的态势,2023年6月9日最高人民法院、最高人民检察院、公安部联合发布《关于依法惩治网络暴力违法犯罪的指导意见(征求意见稿)》,规定“对于网络侮辱、诽谤是否严重危害社会秩序,应当综合侵害对象、动机目的、行为方式、信息传播范围、危害后果等因素作出判定”。造成被害人精神失常、自杀等严重后果;随意以普通公众为侵害对象,相关信息在网络上大范围传播并引发恶意评论;侮辱、诽谤多人;多次散布或组织指使他人散布诽谤、侮辱信息等网暴情形,都有可能被认定为刑法第246条第2款规定的“严重危害社会秩序”,从而实现由自诉转为公诉。相较于2013年9月6日最高人民法院、最高人民检察院发布的《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》,上述征求意见稿明显扩大了自诉转公诉的范围,加大了刑法对于网络暴力的打击力度。此外,该征求意见稿也对公安机关协助取证等问题作了规定。不过,由于“指导意见”重在指导,上述征求意见稿对于被害人提起自诉时可能面临的被告人难以确定、调查取证困难等问题,尚未给出解决方案。

健康有序的网络暴力治理生态有赖系统完备的法治保障,只有在领域性立法思维的指导下制定反网络暴力法及其相关配套制度,确保立法的系统性、整体性与协调性,才能充分发挥相关法律规范的合力作用,推动中国网络暴力治理迈向法治化。

结 语

中共中央印发的《法治社会建设实施纲要(2020—2025年)》将“依法治理网络空间”

[48] 参见程啸:《论我国民法典中的人格权禁令制度》,《比较法研究》2021年第3期,第138页。

[49] 参见最高人民法院第34批指导性案例之“郎某、何某诽谤案”(检例第137号)。

作为当前法治社会建设的重点内容之一。为维护健康有序的网络空间环境，需要防范化解各类网络安全风险，加强对网络暴力违法犯罪行为的法治化治理。网络暴力治理的法治化，是全面依法治网的必然选择。推动网络暴力治理的法治化转型及其立法体系构建，是国家治理现代化的必然要求。

在法治理念上，网络暴力治理应在科学把握网络暴力发生规律和发展态势的基础上，引导社会多元主体通力协作，利用法律规制与技术治理的相互协同，全面塑造良好网络生态。在法治模式上，为了构建网络暴力治理的良法善治路径，需要推动网络暴力治理由分散性法治模式向系统性法治模式转型。系统性法治模式注重发挥民法、行政法、刑法等部门法的协同配合功能，强调防治重大网络暴力风险的问题导向，主张依托领域性专门立法，建构全面系统的网络暴力治理法律体系。在立法路径上，建构与国家治理现代化水平相适应的反网络暴力立法体系，是中国网络暴力治理法治转型期需要着力解决的重大难题。反网络暴力法作为一部专门规制网络暴力的领域性法律，可以通过明确网络暴力治理的基本原则与框架制度，统摄相关部门法中的分散性条文，促进网络暴力治理迈向协同高效的法治化之路。

Abstract: Cyber violence is a significant, intersectional and domain-specific challenge faced by China in the process of state governance in the new era. The current legal provisions on the control of cyber violence in China are scattered and poorly coordinated. With institutional loopholes in terms of the responsibility subjects, sanction measures and relief approaches, they are unable to effectively cope with cyber violence. The key to getting out of this dilemma is to bring the cyber violence control system under the rule of law and establish a corresponding legislative system. To this end, China should, on the one hand, establish the concept of collaborative management to realize the coordination among multiple control entities and between law and technology and, on the other hand, establish a systematic rule of law model to give full play to the collaborative management function of branch laws. Guided by the concept of collaborative management and systematic rule of law model, China should follow the domain-specific legislative thinking and formulate an anti-cyber violence law, so as to build a basic legal framework for the control of cyber violence and, on this basis, improve the supporting legal systems, establish a specialized legislative system and ultimately modernize the cyber violence control system and bring it under the rule of law.

Key Words: cyber violence, anti-cyber violence law, domain law, collaborative management
