网络暴力的生成逻辑及治理路径研究

黄钰惠

湖北大学 法学院，湖北省武汉市，430000；

摘要：网络暴力是数字时代亟待解决的社会风险，其危害已从个体心理创伤延伸至经济秩序破坏及国家安全威胁。基于犯罪学、社会学与传播学的交叉视角，系统解构网络暴力的生成逻辑，提出多维度治理路径。

关键词：网络暴力；生成逻辑；协同治理

DOI：10.64216/3080-1486.25.03.036

1 问题的提出

随着元宇宙技术的爆炸性发展与 AI 智能的兴旺，网络暴力的危害性已突破个体层面，衍生出复杂的社会问题。心理创伤层面，日本学者田中直树的追踪研究表明，网络暴力受害者出现抑郁、焦虑等心理障碍的概率是普通人群的 4.3 倍，且心理创伤的持续时间较传统暴力事件长 3-6 个月。社会秩序层面，群体性网络暴力事件可能引发公众恐慌，干扰正常舆论生态，甚至威胁国家安全与企业商誉。政策治理层面，全球形成了差异化的应对路径。我国于 2024 年构建的“法律规制+平台责任+社会协同”三维治理框架，将网络暴力行为纳入刑法、治安管理处罚法等法律体系，但存在规制范围局限的问题。现行法规主要聚焦个人受害者，对国家、民族、企业等群体的保护存在空白。反观国际社会，欧盟《数字服务法案》依赖平台自律的治理模式，被批评为过度赋予企业内容审查权，导致大量灰色地带的网络暴力行为缺乏有效规制。随着网络恐吓、网络跟踪等新型暴力形态不断涌现，现有治理体系在应对跨平台、跨国界的暴力传播时，暴露出响应迟缓、协同不足等问题。

网络提供的表达空间满足各类网民的需求，而在暴力表达中，言论自由权与名誉权的冲突僵持不下，随着暴力事件的升级将名誉权的损害推向高潮。因此，深化网络暴力研究已成为维护数字时代社会稳定的关键课题。

1.1 网络暴力概念

在国际通行语境下，网络暴力（cyber violence）通常被定义为“通过计算机、手机等电子渠道故意并重复地对他人实施的伤害行为”，其核心特征包括重复性、故意性、持续性与线上匿名性。

我国现行法规中，由于概念较新、立法分散，“网络暴力”尚无统一法律定义。《关于切实加强网络暴力治理的通知》和《网络暴力信息治理规定》对网络暴力分别采用“其他不友善信息”和“不良信息”进行界定，导致法律术语不统一，且仅聚焦于针对个人的侮辱、诽谤等，范围过于狭小，忽视了当代社会，国家、民族和企业等特定的社会群体都能成为网络暴力受害者。其概念在法律规范中也呈现出封闭性特征，难以应对现实社会中网络暴力行为的新发展。

据《辞海》解释，“暴力”泛指通过武力侵害他人人身、财产等权利的强暴行为，可见“暴力”在传统语境中具有明显的身体性、强制性与组织性特征，其结果往往表现为肉体损伤、财产损失或直接的社会冲突。而网络暴力本质更趋近于对受害人的舆论摧毁与心理影响，而非直接物理强制，不能简单将“暴力”的传统定义直接套用于“网络暴力”，将线下所有与网络相关的施暴行为统归于“网络暴力”之列。

结合社会失范理论，网络暴力是社会失范在虚拟空间的具体体现，即“网络失范行为”的一种具体类型。“网络失范行为”指的是“网络行为主体违背了一定的社会规范和所应遵循的行为准则要求，而在‘虚拟的电子网络空间’里出现行为偏差，以及因为不适当地接触和使用互联网络而导致行为偏差的情况。”因此，网络暴力既可能是在网络空间中的个体偏差行为，也可能是非组织化的群体极化行为，其虽不具备传统社会动员意义上的组织性，但却依靠网络情绪的共振机制与传播算法的推波助澜，形成了事实上的暴力集群。据此，本文将“网络暴力”定义成网络技术风险与现实社会风险，通过网络媒介由网络行为主体的交互行动形成双重风险交织，进而侵害当事人合法权益的网络失范行为。

1.2 网络暴力的成因

1.2.1 网络暴力的社会学根源

德国著名社会学家乌尔里希·贝克认为“现代社会实际上已经进入一种风险社会”，风险社会特点是风险

具有不可预测性。社会目前仍存在贫富差距较大、性别对立激化、步入老龄化社会等矛盾，且网民来自五湖四海、出身各行各业，迥异的社会背景和认知上的巨大差异决定了网民在看待同一问题时极易出现分歧，为冲突和网暴埋下隐患。

1.2.2 网络暴力的心理学因素

从众心理诱发网络暴力，主要体现在以“带节奏”，“跟风”为特征的网络暴力中。当某一热点舆情发生后，几名意见领袖的转发评论，粉丝便趋之若鹜展开群体性攻击。盲目迷信权威性话语，在从众心态驱使下沦为制造网暴的“乌合之众”。看客心理催化网暴问题恶化，以旁观看戏的姿态置身事外，对当事人缺乏基本的理解与共情。主观上未必抱有很大恶意，但在围观看戏过程中出于无聊、冷漠、自私、麻木不仁等心态不断煽风点火。

1.2.3 网络暴力发生的新媒体传播规律

沉默的螺旋理论，出于对被孤立的恐慌，大多数的个体会尽力避免因单独持有某些态度和观点而陷入孤立境界。当其作用于互联网时，表现为持有较为弱势观点的网民为了防止自身受到孤立和攻击，在强大舆情力量面前或保持沉默或选择苟同。

1.2.4 网络暴力传播的环境犯罪学原理

网络时空条件为潜在网暴者创造了作案机会。网络空间高度延展性与流动性既为网暴者提供了活动便利，也强化了环境隐蔽性，降低事实真相的可见度。网络环境强化了受害者遭受网暴侵袭的风险，青少年网络群体自我保护能力弱、社会经验不足，对负面消息具有较强敏感性和感知力。现有网络暴力问题缺乏有效的社会控制机制，缺失犯罪防范，网络的空间化发展直接导致监管难度跃升，隐蔽在暗处的网暴者借助境外服务器、多级跳转等方式躲避审查，仅对于预先设置的代码、图片、符号进行过滤已难以阻止相应的网络不法行为。

1.3 网络暴力治理法治化的现实困境

1.3.1 立法规定滞后模糊

我国现有针对网络暴力问题的治理形式是分散性法治模式，即以《民法典》《刑法》等实体法为主干，结合《网络安全法》《个人信息保护法》等单行法，再以部门规章和规范性文件为补充，形成一套相对完备的法律规范体系。审视我国现行的法律框架，针对网暴行为的治理体系仍面临诸多挑战，核心在于法律责任的界定模糊与强制约束力不足。群体性是网络暴力主要特征，本身就牵涉甚广，若入罪门槛设置过低，将导致人人自危，冲击言论自由，也不利于网络的发展。目前，针对网暴行为的主要处理方式往往停留在警告、约谈、责令改正等行政层面，或者需要“按照有关法律、行政法规的规定予以处理”，强调“依法从严处置处罚”。落实到具体处罚上，却常常显得力度轻微，难以匹配网暴行为的严重危害。行政处罚方面，主要依据《治安管理处罚法》，其顶格处罚仅为 10 日以下拘留及 500 元以下罚款，且侧重个人信息保护，对于更广泛的网暴形式针对性不足。刑事层面，受严格的罪刑法定原则限制，许多具有巨大社会危害性的网暴行为，常因缺乏明确对应的罪名或其构成要件难以完全符合，导致无法有效追究刑事责任，最终难以认定为犯罪。这种违法评价不当、惩罚力度不足的状况，使得法律对潜在施暴者的震慑力大打折扣。更深层次问题在于立法体系本身的衔接不畅与规范体系的离散性强。当前，对网络暴力进行治理的主要依据，大量分散在部门规章和各类规范性文件之中，虽然数量众多，但存在法律位阶低、内容易变、过于关注短期治理成效等特点，规制内容往往繁琐且相互之间可能存在重叠或冲突，导致法律依据的不稳定性和权威性不足。从实体法角度看，不同部门法之间，对于何种网暴行为应承担何种性质的法律责任，民事侵权、行政违法还是刑事犯罪，缺乏稳定、清晰的区分标准和评价体系，容易导致同案不同判或法律适用混乱。程序法角度，民事、刑事、行政程序之间的衔接与转化机制非常不清晰。当一个网暴案件可能涉及刑事犯罪时，如何从行政处理或民事纠纷顺畅地转入刑事侦查和诉讼程序在实践中存在诸多障碍。

1.3.2 执法取证溯源困难

电子证据存在收集保全困境，电子证据具有虚拟性、时效性、易损性的特点，容易被灭失篡改。同时，证据需有真实性和合法性，电子证据容易违背取证及时、全面、客观连续性、合法性原则。且其证明效力存疑，电子证据既要建立同案件事实间的关联，也要建立电子证据载体与当事人或其他诉讼参与人之间的关联。

2 网络暴力治理对策

2.1 政府权责

完善网络暴力治理的法治规范与法律规则体系。依据网络空间治理法治原则，结合网络暴力实践问题与信息化发展规律，完善互联网运行、网络信息内容管理、账号处置等法律规范，确立网络安全可信身份查验制度，督促网络服务使用者合法合理使用网络。构建基础法律体系，制定专门性的《反网络暴力法》预防、检测、处置、制裁、救助的全链条治理框架。同时，细化不确定

的法律概念，如虚假信息、淫秽色情信息、民族仇恨信息等。

优化网络暴力治理的监管机构职能与监管能力。明确网络暴力监管机构的核心职能分配，加强网络暴力监管机构的信息共享与协商沟通。监管主体间的分散性权力配置模式，导致职权重合与推诿不作为。需充分利用信息技术提升网暴监管智能化水平，网络数据加工处理技术，在整合分析网暴数据基础上，描述网暴发生背景、特点，进而发现规律和构建模型，建立科学有效及时的防范与应对网暴机制。制定切合网暴实际的网络安全技术标准，网络暴力分级分类应对技术标准。

2.2 平台权责

治理前端搭建平台规则体系。以应急机制响应网暴舆情。建立健全舆情监测机制、舆情预警机制、应急响应机制、技术与人员保障机制。以数字技术完善审核机制，规制宽容原则，压实平台责任、投诉举报机制、人工审核机制、第三方标记实名机制。

治理中端释放平台处置活力。完善分类分级裁量标准，根据信息内容、危害程度、扩散范围区分疑似网暴信息、一般网暴信息和严重网暴信息。保障双方举证申辩权利。利用避风港原则“通知——删除”规则与“反通知——终止”规则。加强网暴信息内容管理，主动或被动清理、严控传播评论，重点话题组和板块严加管控。信息披露方面开设辟谣专区、专门辟谣账号、配合机关账号发布权威消息。倡导跨平台间合作机制，打通合作关隘，构成跨平台合作机制与外部监督保障。

治理末端盘活平台多元效能。建立健全辟谣机制，网暴受害人心理辅助机制，优化搜索算法，针对重点保护群体提供倾斜性保护。设定信用管理制度，账号发文前警示提醒，参与网暴账号警示教育，首发多发煽动发布网暴信息账号关闭账号，情节严重全网禁止注册新账号，借网暴营销盈利行为暂停权限，涉及违法犯罪移交相关部门。认可并将平台进经验上升为行业规范甚至纳入行政法规规范供给源当中，重视平台技术优势，积极赋予治理权限，借助平台数字技术立法试验田，发挥平台行业优势适时整合具有普遍意义的上位规范。

2.3 公民权责

由于存在行为主体以主观上不具有故意犯罪意图为由，逃避承担相应刑事责任的情形，尤其是对于网络中侵犯他人名誉的行为，通常网民仅凭借着所看到的信息便盲目地跟随多数人的观点，对他人恶语相向、人身攻击等，在主观上并不具有明确的犯罪意图。但不能以无法明知所传播信息的真实性为由完全否定其主观的过失心理。因此，可根据行为所造成的后果严重情况，增加过失损害他人名誉罪的规定。在此鞭策之下，公民会更加注重全方位提升自身网络素养，时刻规范网络信息内容的发布，主动举报与监督网暴行为。在这种背景下，当遭遇网络暴力时网民们就能够理性维权，及时获得救济。

我国亟需构建网络暴力治理政府、平台、公民的三方权责机制，建立严格的责任制度，实现对网络暴力的全方位、多层次治理，提高治理的针对性和实效性，化解网络空间的矛盾纠纷，从而营造健康、文明、有序的网络环境，保障网络空间的良性发展。

参考文献

[1]梁丽莉：《法律规制视角下的网络暴力现象研究》，重庆大学 2013 年硕士论文。

[2]参见 PeterK.Smith，TheNatureofCyberbullyingandWhatWeCanDoaboutIt，JournalofResearchinSpecialEducationNeeds15，176-184，（2015）.

[3]叶青：《坚持全面依法治国推进网络暴力治理现代化》，《法治日报》2025 年 2 月 5 日。

[4]李一：《网络行为失范》，社会科学文献出版社 2007 年版，第 92 页。

[5]参见姜方炳：《“网络暴力”：概念、根源及其应对——基于风险社会的分析视角》，《浙江学刊》2011 年第 6 期。

[6]参见陈代波：《关于网络暴力概念的辨析》，《湖北社会科学》2013 年第 6 期。

[7]周凯、刘伟、凌惠：《社交媒体、“沉默螺旋”效应与青年人的政治参与——基于25位香港大学生的访谈研究》，《现代传播（中国传媒大学学报）》2016 年第 5 期。

[8]参见侯玉波、李昕琳：《中国网民网络暴力的动机与影响因素分析》，《北京大学学报》2017 年第 1 期。

[9]王秀平：《网络暴力成因及理性法律规制》，《山东师范大学学报（人文社会科学版）》2010 年第 4 期。

[10]刘晓航：《网络暴力的刑法规制困境及应对》，《北京社会科学》2023 年第 5 期。