交大法学 SJTU Law Review
No. 3 (2024)

网络暴力治理：平台责任与守门人角色

王华伟*

目次

摘要 网络暴力不仅侵害个人法益，而且破坏健康的网络生态。网络暴力概念的失焦，群体聚合作用下个体责任的模糊，表达自由与网络监管的平衡需要，使得网络暴力的治理面临诸多困难。在网络暴力多元共治的基本前提下，除了个体责任的认定之外，应当重视对网络平台的法律规制。不论是从网络技术和传播学的原理还是从法律责任认定的角度，这都是合理的选择。在当下网络空间违法信息与内容的治理中，突出大型网络平台的守门人角色，已经成为国外代表性法案的做法，这也是我国网络暴力规制的重要制度设计方案。网络平台守门人角色的法理内涵，可以从技术措施和义务承担两个角度来具体展开。网络平台守门人制度应当符合我国网络监管模式的国情，重视民法、行政法、刑法等不同部门法的不同规范目标追求，为其合理构建层级性差异，并通过明确可操作的具体规定来落实。

关键词 网络暴力 平台责任 守门人 层级构造

一、问题的提出

近年来，网络暴力成为网络空间法律治理的重点难题。在杭州网络诽谤案、武汉小学生母亲坠楼案、粉色头发女孩自杀案、刘学州自杀案等事件中，网络暴力导致了严重的后果，引发社会高度关注。一方面，网络暴力侵害了公民个体法益，轻则损害他人名誉、侵犯个人信息，重则引发严重的伤害、死亡后果。另一方面，网络暴力也使得网络空间弥漫戾气，违法内容滋生蔓延，严重破坏了健康的在线环境和网络生态。然而，如何在法律上采取有效的治理策略，却是非常棘手的问题。尤其是，在个体责任的认定之外，网络平台应当发挥何种作用还有待深入探讨。

* 北京大学法学院助理教授、法学博士。

本文将首先深入分析网络暴力法律规制面临的困境及其形成原因，其后尝试通过规制重点的视角转换来寻求理论应对之道。在当下我们所处的网络平台时代，对于网络暴力的法律治理而言，网络平台实际扮演着非常重要的角色。在此背景下，本文将结合中外相关法律规范发展动态，主要围绕对网络平台责任的探讨，阐述守门人理论的适用空间和具体制度建构，寻求网络暴力治理的可行方案。

二、网络暴力的法律规制困境

虽然理论与实务都普遍认识到了网络暴力所带来的诸多危害，但是我国长期以来缺乏对其行之有效的法律规制路径，这一困境背后存在着一系列深层次的原因。

（一）网络暴力概念的失焦

当我们谈及法律规制时，明确规制对象是基本的前提。但是，网络暴力不仅并非规范的法律术语，而且即使在相对宽泛的人文社科领域也没有清晰的定义。2023年9月25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》（以下简称《惩治网暴意见》），该意见虽然专门针对网络暴力的惩治而制定，却没有对网络暴力进行明确定义。不过，该意见第1条对网络暴力行为进行了一定描述，即“在信息网络上针对个人肆意发布谩骂侮辱、造谣诽谤、侵犯隐私等信息”，这似乎有将网络暴力限定为发布违法信息行为的倾向。2023年7月7日，国家互联网信息办公室发布《网络暴力信息治理规定（征求意见稿）》，其第2条规定，网络暴力信息是指通过网络对个人集中发布的，侮辱谩骂、造谣诽谤、侵犯隐私，以及严重影响身心健康的道德绑架、贬低歧视、恶意揣测等违法和不良信息。虽然该条对网络暴力信息做出了直接规定，但是其边界无疑非常宽泛，尤其是“道德绑架”“恶意揣测”的内涵很难准确厘定。〔1〕

在理论上，对网络暴力概念的认定众说纷纭。有观点认为，网络暴力是网民对当事人实施的以制造心理压力为手段，以迫使当事人屈服的网络攻击性行为。〔2〕有的观点则强调，网络暴力的实质是一种语言暴力，具有明显的强制性、攻击性，主要体现为一种心理压力。〔3〕也有学者认为，网络语言的暴力特征在于语言数量的规模化、语言内容的攻击性以及伤害后果的现实化。〔4〕还有的观点则主张，网络暴力是通过网络针对个人或群体传播违法信息，反复、持续实施侵害的行为。〔5〕

然而，上述不同理论主张，虽然都具有一定的合理性，但也只是在特定语境下对网络暴力所进行的阶段性经验总结。例如，仅仅强调网民所实施的网络暴力行为的攻击性，可能没有细致考虑，网络暴力在一种复杂集群效应中的具体演化与生成方式。原本并不具有明显攻击性的虚假言论表达，经过社交媒体环境的发酵后，完全可能演变为人们所熟悉的网络暴力。再如，网络暴力是否

〔1〕 中央网信办于2022年11月2日印发的《关于切实加强网络暴力治理的通知》也间接对网络暴力进行了描述，但其中提到的“其他不友善信息”，同样属于非常笼统的概念。

〔2〕 参见陈代波：《关于网络暴力概念的辨析》，载《湖北社会科学》2013年第6期，第61页。

〔3〕 参见喻海松：《网络暴力的多维共治——以刑事法为侧重的展开》，载《江汉论坛》2023年第5期，第129页。

〔4〕 参见蔡荣：《“网络语言暴力”入刑正当性及教义学分析》，载《西南政法大学学报》2018年第4期，第64页。

〔5〕 参见敬力嘉：《网络暴力公私合作治理模式的反思与调试》，载《江汉论坛》2023年第5期，第137页。

必然需要满足语言数量的规模化、行为反复持续性等特征，也不无疑问。〔6〕某些规模较小、次数较少的网络语言表达行为，同样可能引发严重的后果。而且，随着媒介形式的发展和变化，基于现有现象归纳而来的网络暴力概念，可能很快便会过时。归根到底，网络暴力中的“暴力”只是一种修辞手法。这种意象性的概念，很难在法律规范意义上明确其具体构成要件。〔7〕

（二）网络聚合导致个体责任模糊

如果特定行为人在网络上通过散布信息的方式侮辱、诽谤他人，或者侵犯他人个人信息，通常在法律适用上并无太大疑问。网络暴力之所以引发争议恰恰在于，复杂的网络聚合效应使得个体责任在一种群体行为现象中难以被认定。

从事实发生机理来看，网络暴力中的个体行为往往融合在集体行动之中，难以将其独立出来加以评价。网络暴力主要表现为一种集体暴力，是群体非理性的表现，也是网络群体极化现象的表现。〔8〕网络集体行为的形成机制非常复杂，斯梅尔塞（Neil Smelser）的价值累加理论，勒庞（Gustave Le Bon）的社会心理分析，以及布鲁默（Herbert Blumer）的循环反应理论等，对此从不同角度进行了深入阐述。〔9〕在网络暴力中，虽然通过事后调查也可能找到所谓“始作俑者”，但是实际损害后果是集体行为合力所致，个体的相互作用处在一种水乳交融的状态，最早的参与者并非一定负有最主要的责任。在无法进行群体归责的前提下，将个体责任予以剥离在事实认定上面临着很大困难。

从法律责任角度来看，网络暴力中个体责任的认定也存在一定障碍。一方面，由于网络暴力中的危害后果常常是在群体行为和各种复杂因素的共同作用下引发，确定离散个体与最终结果之间的因果关系并不容易。另一方面，在我国刑法罪名中，广泛地存在罪量要素，而大量个体行为可能很难达到这一要求。同时，这些离散个体往往匿名地分散在网络空间的各处，相互之间缺少共同的意思联络，要认定共同犯罪也相当困难。反过来，如果不考虑罪量要素，将网络暴力中数量庞大的个体统统纳入刑法规制范围，在刑事政策的妥当性上则值得斟酌。

（三）平衡表达自由与网络监管的需要

网络暴力治理的深层困境在于，如何平衡喧嚣背后的公民表达自由与网络监管。由于网络暴力边界的模糊性，再加之其本身也是从公共舆论中演化而来，网络暴力和正常网络言论的边界常常难以划定。网络舆论本身夹杂着诸多争议性内容，轻易将其界定为违法，则会压缩公众表达空间，甚至引发“寒蝉效应”。对“人肉搜索”进行法律评价乃至刑法评价的复杂性，便是其中最为典型的例证。理论与实务中通常认为，“人肉搜索”是网络暴力的一种典型形态。虽然早在十几年前，我国学界就已经对“人肉搜索”问题展开了较为广泛的讨论，但是实际上很少有学者对“人肉搜索”做出准确定义。有观点指出，理论上存在着广义的“人肉搜索”，也存在着狭义的“人肉搜索”，前者是指在网络社区通过求助、发问的方式获得众多网友的帮助和回答，后者则指社会层面的寻找具体的人和线索的搜索。〔10〕然而，即使是在狭义上理解“人肉搜索”，其是否违法也仍然很难

〔6〕有的观点将利用网络实施的猥亵儿童行为也纳入网络暴力的讨论范畴，这在很大程度上使网络暴力概念摆脱了对言论的依赖性。参见郭旨龙：《网络暴力刑法治理的解释原理》，载《江汉论坛》2023年第5期，第123页。

〔7〕当然，作为一种被讨论的违法现象，网络暴力概念本身具有重要意义。

〔8〕参见孙健、徐祖迎：《网络舆论监督及其规范》，载《中国行政管理》2011年第12期，第17页。

〔9〕参见朱力、卢亚楠：《现代集体行为中的新结构要素——网络助燃理论探讨》，载《江苏社会科学》2009年第6期，第84—85页。

〔10〕参见高巍：《略论“人肉搜索”的刑事规制》，载《法学杂志》2010年第3期，第67页。

判断。

关于“人肉搜索”是否入刑的问题，早在《刑法修正案（七）》制定之时就有所讨论，由于种种原因，其刑事可罚性没有被立法所确认。《惩治网暴意见》第4条已经明确地提出，组织“人肉搜索”，违法收集并向不特定多数人发布公民个人信息，情节严重，符合《刑法》第253条之一规定的，以侵犯公民个人信息罪论处。这一指导意见罕见地明确了“人肉搜索”组织者的刑事责任，具有相当的标志性意义。然而，仔细分析该条规定可知，组织“人肉搜索”入刑的基本条件仍然是符合侵犯公民个人信息罪的构成要件，而在此问题上，理论上仍处于完全开放的状态。有观点曾指出，“人肉搜索”同时包含善恶两面，难以对其进行整体性立法犯罪化。〔11〕另有观点则认为，按照我国《民法典》第1036条第2项的但书条款，此时属于“该自然人明确拒绝或者处理该信息侵害其重大利益”的情形，故仍然可以视情况纳入侵犯公民个人信息罪的规制范围。〔12〕但是，这种观点似乎已经默认了“人肉搜索”本身的侵害性前提，并且将视野局限在刑法与民法领域内。而在更宏观的视野中，学者们主张，作为一种信息搜寻方式的“人肉搜索”，是公民行使言论自由和信息自由的重要表现形式，是公民行使监督权、批评权的体现，但也可能带来网络暴力，因此体现出了隐私权和言论自由之间的冲突。〔13〕因此，仅仅依据上述《民法典》的规定来肯定“人肉搜索”行为的违法性，恐怕还值得更深入和细致的探讨。

三、网络平台责任与守门人角色

（一）规制重点的视角拓展

上述困境与争议表明，从个体网民着手的法律规制路径存在着重重障碍。网络暴力概念的模糊性，与刑法构成要件的精确性要求之间形成了抵牾。分布在各地的个体网民借助互联网参与集体行为，个体在网络暴力中发挥的实际作用难以准确评定，这也给精确的刑法归责带来了困难。而在网络平台责任的框架内可以采取更加综合性、宽泛性、早期性的措施予以应对，一定程度上缓解刑法构成要件精确性所带来的挑战。网络个体的言论本身亦构成公共舆论的组成部分，网络暴力中的表达自由和网络监管的平衡成为难题。由利弊兼有的“人肉搜索”可见，完全从刑法个罪的角度来追责，不仅困难而且可能过于严厉，不一定能达到预期的目的。而且，即使能够按照现有法律追究个别行为人的刑事责任，〔14〕这对作为一种社会现象存在的网络暴力的遏制效果也仍然相当有限。而从网络平台责任的角度予以引导和适度规制，社会效果可能相对更好。当然，值得强调的是，强化平台责任和治理，并不意味着完全放弃或不再重视个体追责路径，而是在此基础上从平台的角度拓展更加多元性、前置性的问题解决思路。换言之，面对频频出现的网络暴力，在网络暴力多元共治的基本前提下，除了个体责任的认定之外，应当重视对网络平台的法律规制。〔15〕

---

〔11〕 参见王立志：《出售、非法提供公民个人信息罪若干问题》，载《政治与法律》2010年第1期，第88页。

〔12〕 参见喻海松：《网络暴力的多维共治——以刑事法为侧重的展开》，载《江汉论坛》2023年第5期，第131页。

〔13〕 参见戴激涛：《从“人肉搜索”看隐私权和言论自由的平衡保护》，载《法学》2008年第11期，第40—42页；刘晗：《隐私权、言论自由与中国网民文化：人肉搜索的规制困境》，载《中外法学》2011年第4期，第870页。

〔14〕 对网络暴力中发起者、积极参加者刑事责任的分析，参见于冲：《网络“聚量性”侮辱诽谤行为的刑法评价》，载《中国法律评论》2023年第3期，第94—95页。

〔15〕 《惩治网暴意见》第20条已经明确肯定了“网络暴力综合治理”“网络暴力多元共治”的基本理念，并强调应当夯实网络信息服务提供者的主体责任。

其一，在网络技术层面，网络平台构成了网络社会中的关键节点，对其进行规制能够产生更加直接的效果。在网络中，虽然存在着无数分散的节点，但是其中少数连接数非常高的节点主导着网络的结构，它们被称为枢纽节点。这些少量枢纽节点，构成了复杂网络中的阿喀琉斯之踵；让少数几个枢纽节点失效，就可以使无尺度网络迅速分裂并形成级联效应。〔16〕随着网络平台的兴起，人们在网络中所进行的行为很多都需要首先连接网络平台来完成。例如，作为网络暴力的手段行为，不论是在微信还是微博等主流社交媒体发帖、转发、评论，登录网络平台是基本的前提。

其二，从传播学的角度来看，作为核心媒介的网络平台，不仅发挥了内容控制的守门人作用，而且还会影响用户的行为模式。有观点认为，网络平台之所以打败管道，是因为网络平台借助规模化消除了守门人，从而使得其规模更加有效。〔17〕这种观点只能说部分正确，因为网络平台虽然提供给了用户更加自由的信息交互空间，重新构建了网络空间的交往模式，但是网络平台本身并非完全中立，在数字时代，它作为大众媒介延续性地承担着“新型守门人”的角色。〔18〕目前，学界越来越多的观点认识到，所谓技术中立性实际是一个具有误导性的伪命题。〔19〕平台的运营者作为技术的开发者和使用者，不可能完全超然于社会系统之外。而且，“媒介即讯息”，因为媒介对人的协作与活动的尺度和形态发挥着塑造和控制的作用。〔20〕例如，主流搜索引擎的算法，实际上在很大程度上就决定了我们在网络中能够看到的内容，因而也就对个体的认知乃至大众媒介产生了深远影响。〔21〕换言之，在更深层的意义上，网络平台所制定的规则和搭建的行为框架，将会直接影响用户的举止。

其三，从法律责任来说，以网络平台作为规制重点既是更为务实的做法，也可以避免处罚泛化。鉴于网络暴力中个体参与者人数众多，其责任边界亦非常模糊，因此在追求法律责任时，常常面临难有抓手的困境。而网络平台的义务与责任边界相对明确，以此作为治理重点产生的规制效果辐射力强，且又不至于打击面过宽。

（二）守门人理论在网络法中的适用

随着网络空间法律规制重点的视角转换，网络平台的守门人角色逐渐浮出水面。守门人理论的来源要追溯到社会心理学家勒温（Kurt Lewin），1947 年他去世后，未完成的手稿被发表，其中第一次出现了守门的概念。其后，怀特（D.M. White）将守门人理论引入传播学，由此许多学者都开始使用守门人隐喻，对该理论的研究不断得到发展，并且突破学科界限在不同领域开枝散叶。〔22〕进入 21 世纪以后，网络社会加速发展，守门人理论在网络空间的法律治理中慢慢被接纳。尤其

〔16〕 参见[美] 艾伯特-拉斯洛·巴拉巴西：《链接：商业、科学与生活的新思维》，沈华伟译，浙江人民出版社 2013 年版，第 84、151 页以下。

〔17〕 参见[美] 杰奥夫雷·G. 帕克、马歇尔·W. 范·埃尔斯泰恩、桑基特·保罗·邱达利：《平台革命：改变世界的商业模式》，志鹏译，机械工业出版社 2018 年版，第 7 页。

〔18〕 参见白红义：《媒介社会学中的“把关”：一个经典理论的形成、演化与再造》，载《南京社会科学》2020 年第 1 期，第 111 页。

〔19〕 参见劳东燕：《“人脸识别第一案”判决的法理分析》，载《环球法律评论》2022 年第 1 期，第 157—159 页。

〔20〕 参见[加] 马歇尔·麦克卢汉：《理解媒介：论人的延伸》，何道宽译，译林出版社 2019 年版，第 19 页。

〔21〕 参见[英] 尼克·库尔德利：《媒介、社会与世界：社会理论与数字媒介实践》，何道宽译，复旦大学出版社 2014 年版，第 106 页。

〔22〕 参见[美] 帕梅拉·J. 休梅克、蒂姆·P. 沃斯：《把关理论》，孙五三译，中国人民大学出版社 2022 年版，第 3 页以下。

是，网络服务提供者和网络平台运营者的守门人角色，在中外文献中逐渐得到认可。〔23〕

强调网络平台的守门人角色，其本质就是强调网络平台应当承担更多义务，从而担负起更多法律责任。从20世纪90年代中后期开始，以德国《电信媒体法》、欧洲《电子商务指令》、美国《通信规范法》等为代表的法律和规范，构建了一套较为完整的网络服务提供者法律责任框架。在此时期，网络服务提供者的整体规模和影响力都较为有限，属于需要扶持的新生事物。为了更好地培育信息产业的发展，为新经济增长创造宽松的社会氛围，〔24〕法律更多地为网络提供者设置免责规范，明确其相对限缩的法律责任边界。“避风港原则”所包含的法律规则和程序，正是在这样的背景下逐渐发展完善。

然而近年来，国外的一些代表性法规，在一定程度上开始调整上述策略，体现出强化网络平台义务与责任的明显趋势。这种守门人角色的强调和平台责任模式的转变，背后有深厚的技术性、社会性、观念性原因。与二十多年前相比，当今的很多大型互联网平台公司具备了先进的信息网络技术，掌握了海量数据的支配权，控制着网络空间流量的分配，演变成为影响力极强的社会参与主体。在此背景下，不论是对于平台用户还是其他普通民众、机构或群体，在整个社会结构中，平台事实上形成了强大的“私权力”，〔25〕扮演了“把关”性的角色。如不对其加以引导、科以相对更多的义务，社会的良善治理将缺失重要的一环。因此，对大型网络平台的法律政策，逐渐从早期的“优待培育”转向了“引导规制”，强化网络平台的主体责任逐渐成为共识。例如，2017年，为了加强对网络空间仇恨犯罪的规制，德国议会通过了《网络执行法》，经过修订扩充后，其明确要求大型社交网络平台运营者承担起对违法内容及时处置、处置情况报告、相关违法内容传送警方等义务。如果违反这些义务，社交网络平台运营者将面临最高达五百万欧元的罚款。〔26〕此外，在全自动化运营网络平台中，按照传统共同犯罪理论来认定运营者的刑事责任可能存在处罚漏洞，因此，2021年《德国刑法典》新增设第127条运营互联网犯罪交易网络平台罪。〔27〕按照该规定，行为人在互联网上运营服务于促进实施违法犯罪行为的交易网络平台的，处5年以下自由刑；在加重的情形下，处1年以上10年以下自由刑。〔28〕

而欧盟委员会于2022年批准生效的《数字服务法》实际上也在朝着同样的方向前进。《数字服务法》第二章大体维持原有《电子商务指令》关于网络服务提供者的责任框架，第三章则逐层递进地规定了不同主体的勤勉义务，包括适用于所有网络中介服务提供者〔29〕的条款，适用于存储服务提供者的条款，适用于在线网络平台提供者的条款，以及适用于超大型在线网络平台和超大型搜索引擎运营者的条款。例如，其中第16条规定的存储服务提供者（包括网络平台运营者）对违法内容设立通报和响应机制的义务，与德国《网络执行法》非常相似。〔30〕违反《数字服务

〔23〕 参见单勇：《数字看门人与超大平台的犯罪治理》，载《法律科学》2022年第2期，第79页。

〔24〕 参见王华伟：《德国网络平台责任的嬗变与启示》，载《北大法律评论》第19卷第1辑，北京大学出版社2019年版，第122—123页。

〔25〕 参见刘权：《网络平台的公共性及其实现——以电商平台的法律规制为视角》，载《法学研究》2020年第2期，第46页。

〔26〕 Vgl. § 2, § 3, § 3a, § 4 Netzwerksdurchsetzungsgesetz.

〔27〕 Vgl. Bundestags-Drucksache 19/28175, S.1.

〔28〕 Vgl. § 127 StGB.

〔29〕 英文原文为 provider of intermediary services，为便于理解，此处翻译为网络中介服务提供者。

〔30〕 Vgl. Redeker, IT-Recht, 8. Aufl., 2023, Rn. 1129; see Council Regulation (EC) No 2065/2022 of 19 October 2022 on A Single Market for Digital Services, Art.16.

法》的相关规定，网络中介服务提供者最高有可能被处以其前一财政年度全球营业额6%的罚款。〔31〕

（三）网络平台责任的制度设计

对于网络暴力的治理，强化网络平台所扮演的守门人角色，将成为法律规则设计的基本方向之一。网络暴力本质上是一种网络内容的传播行为，在本体上通过信息传输来完成。而网络平台作为信息传输和内容传播的关键枢纽，具有致力于防止网络暴力发生的充分理由。一方面，从网络平台的实际技术控制性来看，网络平台能够最为及时地预测、处置网络暴力信息。大型的网络平台实际上控制着流量的入口，对其支配空间内的信息和内容具有较高的控制可能。虽然实名制本身在理论上存在较大争议，〔32〕但是在实名制实际已经在各大网络平台推广以后，运营者对网络平台中内容的管控能力客观上提升了。同时，大型网络平台拥有雄厚的财力、先进的网络技术，采取一定措施对网络暴力内容进行控制，并非负荷很重、难以完成的工作。另一方面，网络平台本身享受了用户集聚效应带来的红利，业务规模迅速发展，由此，为防治网络平台模式内存风险而承担相应义务，符合权利义务对等的基本原理。而对于网络暴力的防治，网络平台守门人角色的制度设计应从技术措施与义务承担两个角度来展开。

在技术措施层面，对网络暴力的防治可以分为事前技术措施与事后技术措施。事前技术措施可以包括设立网络暴力识别标准，设立网络暴力预警机制，设立应急预案，制定网络平台文明公约，定期发布网络暴力处置评估报告等；事后技术措施可以包括设立一键防护机制，〔33〕设立透明便捷的投诉机制，及时屏蔽、删除违法内容，查封违规账号，移送违法信息，配合执法机制等。这些技术措施大部分都已经被规定在《关于切实加强网络暴力治理的通知》以及《网络暴力信息治理规定（征求意见稿）》中。不过，上述技术措施虽然得到了普遍认可，其具体落地仍需行业标准和技术共识予以支持。技术治理有助于矫正和克服法律治理的滞后性和模糊性，〔34〕对于网络暴力具体个案能发挥更加直接的作用。例如，在前文提到的杭州网络诽谤案、武汉小学生母亲坠楼案、粉色头发女孩自杀案、刘学州自杀案等案件中，如果能够从技术上及时切断网络暴力信息对被害人的影响，那么灾难性的后果则很可能能够避免。

在落实技术措施的过程中，明确网络暴力的识别标准尤为困难，它也构成采取其他技术措施的基本前提。相对可行的做法是根据网络暴力侵害的法益类别来对行为和内容进行分组，这样可以适当回避目前形成完全统一概念所面临的难题。其一，侵害人格权的网络侮辱、诽谤行为。这类行为属于最为典型的网络暴力类型，结合侮辱罪、诽谤罪的构成要件及其教义学理论加以认定即可。值得注意的是，对公众人物、公众话题发表网络评论，构成人民参与国家公共事务的重要途径，因而就其在侮辱、诽谤性质的把握上应当相对严格，甚至其可能构成违法阻却事由。〔35〕其二，侵害个人信息权的信息处理行为。例如，未经允许，通过网络擅自公开或散布他人个人信息，这也

〔31〕 See Council Regulation (EC) No 2065/2022 of 19 October 2022 on A Single Market for Digital Services, Art. 52, Art. 74.

〔32〕 质疑性的观点，参见杨福忠：《公民网络匿名表达权之宪法保护——兼论网络实名制的正当性》，载《法商研究》2012年第5期，第37—38页；周永坤：《网络实名制立法评析》，载《暨南学报（哲学社会科学版）》2013年第2期，第1页。

〔33〕 参见贺剑：《能不能建立一种网络暴力事前隔离机制？》，载微信公众号“中国法律评论”，2022年1月28日。

〔34〕 参见王燃：《论网络暴力的平台技术治理》，载《法律科学》2024年第2期，第125页。

〔35〕 参见张明楷：《刑法学》（第6版），法律出版社2021年版，第1197页。

是网络暴力中常见的行为样态。2017年6月1日起施行的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件若干问题的解释》第3条已经明确，该种情形属于侵犯公民个人信息罪的非法提供公民个人信息行为。其三，侵害性自决权的网络性侵行为。我国刑法理论和司法实务对强奸罪的犯罪构成设置了较为严格的性器结合条件，故该罪在网络空间的适用相对较窄。然而，强制猥亵、侮辱罪和猥亵儿童罪则并没有这样的限制，因而发送电子图片、网络视频等行为方式都存在构成前述两项犯罪的空间。其中，较为典型的形态是借助信息网络来实施猥亵儿童的行为，对此，最高人民检察院发布的指导性案例也已经予以确认。〔36〕实践中，此类网络性侵的案例数量在持续增加，〔37〕可以将其作为网络暴力的一种类型予以确立。其四，侵害身体健康、生命法益的行为。通常而言，通过信息网络实施人身暴力犯罪的情形较为罕见。但是，实务中也可能存在个别特殊的行为，即借助信息网络实施语言暴力来给被害人形成心理强制，引发被害人实施自伤或自杀。〔38〕其五，侵害他人私人生活领域以及行为与意志自由〔39〕的网络跟踪、骚扰(Cyberstalking)行为。在外国刑法中存在着跟踪骚扰类的犯罪，而近年来这类行为进一步朝着网络化、信息化的形态发展。正因如此，《德国刑法典》第238条跟踪骚扰罪(Nachstellung)最近增加了若干项借助信息网络实施的骚扰行为类型。〔40〕这类行为尚未完全被我国现行《刑法》所覆盖，但是仍然需要对其进行适当的规制。需要说明的是，上述网络暴力行为类型并非完全互斥，实务中完全可能存在同时符合多种情形的行为。

在责任承担层面，同样应当通过类型化的思维，来梳理网络平台在网络暴力治理中的义务。纵览中外相关代表性法律规范和司法实践，网络平台的守门人角色主要通过如下几种大的义务类型来体现。

其一，适当强化违法内容处置义务。现有建立在“通知—删除”规则之上的网络服务提供者责任体系，主要就是以违法内容的合理处置作为基本目标。在当下的网络空间中，网络平台往往不仅仅提供一种纯粹的信息传输通道，而是以存储和处理一定信息为前提，提供相关网络服务。因此，在绝大部分情况下，网络平台运营者可以被归类为存储服务提供者。〔41〕按照现有中外的代表性法律规则，对作为存储服务提供者的网络平台运营者而言，如果其认识到了网络暴力违法内容的存在，则通常负有义务及时采取措施，对违法内容予以封锁或删除。而且如上文所述，不论是德国的《网络执行法》还是欧盟的《数字服务法》，在上述“通知—删除”规则框架的基础上，都通过明确违法内容删除期限、设立有效的违法内容投诉机制、发布违法内容处置报告等要求，进一

〔36〕通过信息网络传播的方式对儿童实施猥亵行为构成猥亵儿童罪既遂的判决，参见《最高人民检察院第十一批指导性案例 骆某猥亵儿童案(检例第43号)》，载中华人民共和国最高人民检察院网2018年11月18日，https://www.spp.gov.cn/xwfbh/wsfbt/201811/t20181118_399386.shtml#2。

〔37〕参见邵守刚：《猥亵儿童犯罪的网络化演变与刑法应对——以2017—2019年间的网络猥亵儿童案例为分析样本》，载《预防青少年犯罪研究》2020年第3期，第49页。

〔38〕司法实务中已经出现了通过网络交流，教唆、帮助被害人自杀的案例。参见郭树合、郝祺之：《网上“帮助”他人自杀如何定性》，载《检察日报》2023年8月8日，第4版。

〔39〕Vgl. Gericke, in: Münchener Kommentar zum StGB, Band 4, 4. Aufl., 2021, § 238, Rn. 1.

〔40〕例如，通过滥用他人个人数据来进行商品下单，或使第三人与其联系；通过实施数据窥探、截获等犯罪行为来侵扰被害人；传播或公开被害人的相关图像信息(如Revenge Porn，即复仇式披露含有他人色情内容的图片)；假冒作者身份传播或公开能使被害人受到贬低评价的内容等。Vgl. § 238, Abs.1, Nr.3, 5,6,7 StGB; Heger, in: Lackner/Kühl/Heger (Hrsg.), Strafgesetzbuch Kommentar, 30. Aufl., 2023, § 238, Rn. 4a.

〔41〕See Council Regulation (EC) No 2065/2022 of 19 October 2022 on A Single Market for Digital Services, Art. 3 (i).

步强化了内容处置义务。这些比较法的经验，应当通过适当的制度安排被我国的相关法律框架所吸收。

首先，违法内容的识别，原则上应当由网络平台来进行。网络平台处在信息和内容处理的最前线，和用户存在最直接的联系，易于发现违法信息也便于接受违法内容的投诉。况且，网络平台从信息处理中直接或间接地获得利益，不论从技术可行性的现实角度还是权利义务平衡的法律角度，由其承担违法内容识别的任务都是相对合理的安排。不过，为了避免违法内容治理的过度“私有化”现象，网络信息安全主管部门应当和网络平台建立起顺畅的沟通衔接机制，保障主管部门可以及时介入，发挥适当的监管职能。

其次，网络平台应当建立起便捷、透明、快速响应的违法内容投诉机制。网络平台虽然具有强大的信息网络技术，但是在面对海量的数据和无数的信息源时，仍然无法完全独立完成违法内容处置的任务。更何况，鉴于公民信息自由的考量，网络平台本身不应过度积极地介入用户生成信息内容的审查。在此背景下，用户对网络暴力等违法内容的投诉在治理中发挥了举足轻重的作用。为了避免流于形式，违法内容投诉机制应当设置在网络平台中易于访问的位置，同时其操作流程不能过于复杂。尤为重要的是，网络平台应当对具体违法内容的处置结果进行通报，对处置流程予以公示，尽可能实现机制透明。此外，网络平台应定期（如每月）发布违法内容处置报告，以更好地实现对违法内容处置机制的事后监督。网络平台在发现违法内容后，应当快速响应。具体删除期限的设置，各国的标准有所不同。例如，德国的《网络执行法》规定，网络平台对“明显违法内容”应当在 24 小时内删除，而对其他违法内容则应当在 7 天内删除。〔42〕法国的《阿维娅法案》规定，网络平台在收到基于种族、性取向、身体残疾、煽动仇恨等网络暴力言论投诉后，应当在 24 小时内删除，但对恐怖主义或儿童色情相关的内容则应在 1 小时内删除。〔43〕考虑到目前信息流通的速度和效率极高，7 天标准已经难以契合有效治理违法内容的需要，24 小时标准是相对妥当的做法。同时，针对高度敏感的违法信息或违法性表征非常清晰的内容，可以在严格类型化的基础上设置更高要求的时间标准。在前述杭州网络诽谤案、武汉小学生母亲坠楼案、粉色头发女孩自杀案、刘学州自杀案等事件中，网络平台最终都采取了措施删除和屏蔽了大部分的网络暴力内容。然而，这种平台的响应机制如果能够更为及时地启动，很可能能够避免很多类似悲剧性后果的发生，这种情形出现的原因之一就在于目前的治理规范没有提出明确的响应时间要求。

最后，强化违法内容处置义务，应当通过明确违法内容的认定标准来实现。长久以来，关于违法信息的范围，包括《互联网信息服务管理办法》《电信条例》等在内的我国多项法律和相关规范确立了“九不准”的宽泛标准。〔44〕2020 年生效的《网络信息内容生态治理规定》进一步将违法信息的范围拓宽到“十一不准”，新增了歪曲、丑化、亵渎、否定英雄烈士事迹和精神，侵害英雄烈士姓名、肖像、名誉、荣誉的信息，以及宣扬、煽动恐怖主义、极端主义的信息。然而，上述范围中的诸多概念都相当模糊，在实践中很难把握。以拒不履行信息网络安全管理义务罪为例，该罪中网络服务

〔42〕 Vgl. § 3 (2) Netzwerksdurchsetzungsgesetz.

〔43〕 参见石佳友：《网络暴力治理中的平台责任》，载《法律科学》2023 年第 6 期，第 20 页。

〔44〕 “九不准”信息具体包括：反对宪法所确定的基本原则的；危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；损害国家荣誉和利益的；煽动民族仇恨、民族歧视，破坏民族团结的；破坏国家宗教政策，宣扬邪教和封建迷信的；散布谣言，扰乱社会秩序，破坏社会稳定的；散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；侮辱或者诽谤他人，侵害他人合法权益的；含有法律、行政法规禁止的其他内容的。

提供者应当删除的违法信息的认定标准，在理论上就存在各种不同的理解。〔45〕本文认为，对于违法内容的认定，应当在部门法领域予以区分。考虑到刑法的最后手段性特征，拒不履行信息网络安全管理义务罪中的违法信息宜采取相对严格的标准，原则上应当以信息内容符合《刑法》分则相关构成要件作为违法性认定依据。〔46〕但是在民事法、行政法等领域，违法内容的标准可以参照上述“十一不准”规范，进行相对宽松的具体判断。同时，对于违法性表征不够清晰的内容，辨识过程往往相对复杂，此时不应课予平台过高的义务。

其二，确认不同程度的数据和信息保护义务。通常认为，数据和信息是一对相互关联的概念，前者侧重数据本体，而后者侧重数据所承载的内容。对数据和信息的滥用与非法处理（如非法的“人肉搜索”），往往构成网络暴力行为的重要手段和前提。网络平台作为数据和信息处理者，常常控制了大量数据和信息，应当担负起保护数据和信息的义务。我国《数据安全法》第27条规定，开展数据处理活动应当建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。按照《数据安全法》第21条的规定，我国根据数据在经济社会发展中的重要程度，以及一旦遭到非法处理对国家安全、公共利益或者个人、组织合法权益的危害程度，对数据实行分类分级保护。我国《个人信息保护法》第二章第二节对敏感个人信息做出了专门的规定，对其处理的合法性设置了更高的要求。较之于一般的个人信息处理者，《个人信息保护法》第58条更是对大型网络平台运营者设置了更为严格的个人信息保护义务。总的来说，在网络暴力的防治过程中，数据和信息越重要、性质越敏感，对网络平台的数据和信息保护义务要求就越高。在刑法层面，网络平台对用户信息（数据）的保护义务，已经在我国《刑法》第286条之一拒不履行信息网络安全管理义务罪中得到了确认。

其三，配合执法义务的确立。网络平台处在各项网络活动的最前线，直接为用户提供网络服务，处理相关数据。如果没有网络平台的配合，执法机关的法律治理行为很难实现。因此，很多代表性的法律都在一定程度上确认了网络平台的配合执法义务。例如，德国《网络执行法》在2020年进行了修订后补充规定，社交平台运营者在处置投诉过程中所获悉的违法内容，如果符合特定犯罪构成要件的，出于促进追诉犯罪的目的，必须提交给联邦刑事警察局。〔47〕欧盟《数字服务法》第10条规定，网络中介服务提供者在收到执法机关要求提供特定用户特定信息的命令时，应当及时予以回应。〔48〕该法第18条甚至进一步要求，网络平台提供者在发现涉及威胁他人生命或安全的刑事犯罪线索时，应当及时通知执法机关，这一条在理论上格外引人注意。〔49〕我国《数据安全法》第35条也规定，公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，有关组织、个人应当予以配合。而且，我国《刑法》第286条之一拒不履行信息网络安全管理义务罪也明确了违反义务“致使刑事案件证据灭失”这一行为的后果，实际上也间接确立了网络服务提供者的配合执法义务，包括对网上信息和网络日志信息记录进行备份和留存，并在国家有

〔45〕参见陈洪兵：《拒不履行信息网络安全管理义务罪条款“僵尸化”的反思》，载《学术论坛》2022年第3期，第8页。

〔46〕相关的理论主张和域外立法，参见孙禹：《论网络服务提供者的合规规则——以德国〈网络执行法〉为借鉴》，载《政治与法律》2018年第11期，第55页；Vgl. § 1 (3) Netzwerksdurchsetzungsgesetz。

〔47〕Vgl. § 3a Netzwerksdurchsetzungsgesetz.

〔48〕See Council Regulation (EC) No 2065/2022 of 19 October 2022 on A Single Market for Digital Services, Art. 10.

〔49〕Ibid., Art. 18.

关机关依法查询时予以提供等。〔50〕在网络暴力发生后，如果网络平台拒绝或怠于履行该类义务，引发严重后果，满足其他构成条件时则可按照该罪进行追责。

四、网络平台守门人角色的层级构造

虽然强化网络平台的守门人角色已经得到越来越多的认可，但是如何明确其具体适用条件仍然值得格外注意。简单过度地强调课予网络平台更多的义务和更严的责任，最终会使网络平台失去生存空间，背离制度设计的初衷，也并不真正有利于网络暴力的治理。

其一，在符合国情的监管模式中理解守门人角色。不论是德国的《网络执行法》还是欧盟的《数字服务法》，其显著强化大型网络平台的义务与责任，实际上对欧盟内部企业影响不大，因为活跃在欧洲的大型网络平台主要都来自欧盟之外；而与此相对，美国虽然也有强化网络平台责任的诸多动议，但是采取欧盟“强监管”模式的可能性不大。〔51〕而中国的网络平台虽然市值规模很大，但是实际上已然背负了来自不同规范的多重义务和来自不同部门的各种监管，网络治理一直面临着“九龙治水”的状况。〔52〕在此背景下，至少不宜再过于激进、粗糙地强化守门人角色。就网络暴力而言，大型网络平台固然应当采取更多有效的事前事后技术措施，承担更加有针对性的内容管理义务，发挥相对更加积极的作用，但是治理网络暴力的主要责任并未直接从执法部门转移给大型网络平台这一私主体。过去二十年来，我国的网络平台和信息产业得到了迅速发展，其体量和规模达到了空前的程度，在法律治理过程中出现了诸如垄断、数据违规处理等问题。〔53〕然而，在当下我国大力发展数字经济的时代背景下，信息产业成为新的支柱性产业，仍需重点培育，而在其中，网络平台将继续扮演非常重要的角色，过度严苛的法律规制框架并非理性选择。因此，强化网络平台守门人角色，需要在基本国情、产业政策、网络监管等多重因素中来进行平衡和制度设计。通过网络平台的义务强化来优化网络暴力治理，也同样需要在这一基本框架中进行整体思考。

其二，网络平台在不同部门法领域扮演的守门人角色存在差异。在现有的很多法律规范和理论文献中，守门人已经成为非常关键的概念。例如，在欧盟委员会同时提出的《数字市场法》中，守门人不仅仅是一种理论概念，而且存在明确的法律定义和认定条件，〔54〕并作为一种核心规制理念贯穿在整部法律之中。我国《个人信息保护法》第58条对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者设立了更为严格的义务，被认为是个人信息保护领域的守门人条款。〔55〕但是，在不同部门法领域，守门人的要求存在很大差异，相关义务和责任也相应形成不同层级，应当根据部门法本身的性质与任务以及特定的目标追求谨慎进行

〔50〕 参见王爱立主编：《中华人民共和国刑法解读》，中国法制出版社2018年版，第699页。

〔51〕 参见王天凡：《数字平台的“阶梯式”监管模式：以欧盟〈数字服务法〉为鉴》，载《欧洲研究》2023年第2期，第71—73页。

〔52〕 参见王华伟：《避风港原则的刑法教义学建构》，载《中外法学》2019年第6期，第1454页。

〔53〕 参见《国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问》，载中国网信网2022年7月21日，http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm。

〔54〕 See Council Regulation (EC) No 1925/2022 of 14 September 2022 on Contestable and Fair Markets in the Digital Sector, Art. 2-8.

〔55〕 参见周汉华：《〈个人信息保护法〉“守门人条款”解析》，载《法律科学》2022年第5期，第36页。

认定。

《数字市场法》更多的是着眼于数字市场中超大型网络平台与其他网络平台之间竞争力失衡的问题，旨在避免不正当竞争，创造更加公平的商业环境，〔56〕因此其对网络平台守门人角色的强调几乎达到了前所未有的程度。而与之不同，《数字服务法》则相对侧重于维护一个安全、可预测和值得信赖的在线环境，突出对网络平台中违法内容的治理，〔57〕其难度更大，所以它对网络平台义务的强化仍然是相对克制的。虽然《数字服务法》明显强化了网络中介服务提供者的义务，但是对《电子商务指令》所设计的网络中介服务提供者基本免责框架仍然大体予以维持。例如，《数字服务法》第8条还是明确规定：网络中介服务提供者对于其传输、存储的信息，没有一般性的监控义务，也没有积极寻找表明违法活动事实或情况的义务。基本的理由在于，恰恰是过去上述免责框架提供的法律确定性，才使得新的网络服务形式迅速成长起来。〔58〕类似地，虽然德国《网络执行法》明显强化了社交网络平台提供者的义务和责任，但是一方面它本身在理论上受到了很多批评，另一方面其仍然大体与《电信媒体法》所设定的免责框架保持一致。〔59〕

理论上，有观点认为，由于网络平台在网络空间扮演着守门人的角色，因此应当肯定网络平台的犯罪控制义务，对非法内容的控制也应当从被动审查转向主动审查。〔60〕还有观点指出，《互联网信息服务管理办法（修订草案征求意见稿）》第16条要求互联网信息服务提供者建立信息发布审核制度，也是此种主动审查立场的体现。〔61〕但是，网络平台企业毕竟不是执法者，对此可能还需要全面考虑主动审查将给网络平台企业、信息产业所带来的沉重负担以及背后的正当性问题。同时，对他人内容进行主动审查的背后，实际上还潜藏着侵犯他人信息权利和言论自由的风险。虽然在一定程度上强化网络平台的守门人角色乃大势所趋，但是在各种因素的综合权衡之下，网络平台所承担的违法内容管理义务不宜整体转向主动审查。

同样，网络暴力的治理实际上主要涉及违法内容的管理。网络平台对此所扮演的守门人角色，应当在不同的部门法领域中体现出层级性的构造。在民事法领域，涉及平等主体之间的法律关系，网络平台对网络暴力的管理没有尽到应尽的义务因而引发损失时，网络平台承担民事责任的条件和范围可以相对较为宽松。在行政法领域，涉及行政权力的行使，鉴于网络平台对其所管理空间的支配性以及怠于配合网络空间监管的现状，可以有条件地强化其义务及其相应的行政处罚，欧盟的《数字服务法》和德国的《网络执行法》便是在这个方面的努力，我国亦可在一定程度上效仿。

在刑法领域，由于刑罚本身的高度严厉性以及附随的诸多消极后果，则应当极为慎重，不应将前置法中的义务轻易上升为刑法义务，转化为刑事责任。科处网络平台刑事责任，不仅会对平台企业造成毁灭性的打击，而且存在震慑整个行业的“溢出性”风险。纵观国际范围内一些代表性的法案，虽然强化网络平台责任是大势所趋，但是很少直接将其上升为认定刑事责任的依据。虽然

---

〔56〕 参见赵精武：《从“超大型平台”到“守门人平台”：欧盟〈数字市场法〉的制度逻辑与监管特征》，载《数字法治》2023年第2期，第195—196页。

〔57〕 See Council Regulation (EC) No 2065/2022 of 19 October 2022 on A Single Market For Digital Services, Whereas: (3), (9).

〔58〕 Ibid., Whereas: (16), Art.2(3), Art. 4 - 6, Art. 8.

〔59〕 见前注〔24〕，王华伟文，第130—132页。

〔60〕 参见单勇：《论互联网平台的犯罪控制义务》，载《现代法学》2022年第3期，第76页。

〔61〕 参见程宝库、李俊辉：《非法内容审查的平台责任研究——欧盟〈数字服务法〉的分析与借鉴》，载《中国市场监管研究》2023年第2期，第22页。

《德国刑法典》专门增设了第127条运营互联网犯罪交易网络平台罪，但是其适用边界较窄，而且所谓填补立法漏洞的功能也受到了广泛质疑。〔62〕而在美国，由于特别强调对言论自由的保护，即使是对明确仇恨言论的规制，都没有体现出在欧洲那样的积极性，〔63〕因此平台刑事责任也就显得更加宽松。在我国《刑法》中，直接涉及平台刑事责任的罪名主要是拒不履行信息网络安全管理义务罪，其为网络平台的守门人刑法义务提供了实定法依据。〔64〕该罪在司法实践中适用极少，但是整体来看这种现象并非必然被负面评价。重要的原因之一在于，该罪构成要件中隐形内嵌了诸如责令改正程序这样的“避风港原则”，既对网络平台形成了较强的刑事合规压力，同时又对其设置了较为明显的出罪机制。同时，责令改正程序也有利于确保从行政不法到刑事不法的递进与过渡，〔65〕促进了行刑衔接模式的建立。相反，主张扩张该罪信息网络安全管理义务或弱化责令改正程序的做法，往往使得司法判决逻辑异化。〔66〕

其三，强化网络平台守门人角色应当通过明确的规则设计来具体实现。换言之，强化网络平台在网络暴力治理中的义务，应当以清晰且具有可操作性的规定来呈现。目前，虽然我国诸多法律规范和文件都强化了网络平台的法律责任，但是往往仅予以概括性规定，相关条款的实际可操作性不强。例如，网络平台对包括网络暴力在内的违法内容投诉的处理报告，具体多久发布一次，发布在何种渠道，都应当予以明确。网络暴力如何进行类型化判定，判定不明时如何审查和处理，都应当有规范性的办理流程。再如，网络平台发现包括网络暴力在内的违法内容后，具体应在多长时间内予以屏蔽或删除，进行更为细化的规定也有必要。类似的问题，在《数字服务法》和《网络执行法》等规范中都有值得参考的做法，上文笔者也据此对我国的制度建设提出了相应的建议。如果不对网络平台扮演守门人角色所承担的义务予以细化，要么将使得制度目标落空，要么意味着网络平台将面临捉摸不定的法律责任风险。

五、结　　语

网络暴力成为网络空间治理的顽疾，这在很大程度上考验着管理者的法律治理策略。在现有的规制框架下，网络暴力的法律治理面临一系列难题。网络暴力并非规范的法学概念，其中的“暴力”具有意象性的特征，目前仍然难以对其内涵形成广泛共识。网络暴力的聚合性特征，使得其中个体参与者的责任边界非常模糊。网络暴力的治理，还面临着表达自由和网络监管之间的平衡难题。面对网络暴力规制的困境，在网络暴力多元共治的基本前提下，应当在个体责任的认定之外，强化对网络平台的法律规制，这不仅符合网络技术和传播学的原理，而且也是一种相对务实合理的法律责任追究方案。在当下的网络时代背景下，强调大型网络平台在网络空间治理中所扮演的守门人角色，已经成为国外代表性法案的基本做法，这也将成为我国规制网络暴力的重要制度设

〔62〕 Vgl. Eschelbach, in: Kindhäuser/Neumann/Paeffgen/Saliger, Strafgesetzbuch Kommentar, 6. Aufl., 2023, § 127 Rn. 2.

〔63〕 See Patrick Zurth, *The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability*, 31 Fordham Intellectual Property, Media and Entertainment Law Journal 1084, 1138(2021).

〔64〕 参见喻浩东：《网络空间中信息安全守门人的刑法义务》，载《财经法学》2023年第4期，第118页。

〔65〕 参见王帅：《拒不履行信息网络安全管理义务罪中的“责令采取改正措施”解读——基于行刑联动的思考》，载《法律适用》2022年第8期，第76页。

〔66〕 参见王华伟：《网络犯罪的司法认定》，中国人民大学出版社2022年版，第118—120页。

计方案。网络平台守门人角色的法理内涵，可以从技术措施和义务承担两个角度来展开。作为守门人的网络平台，在对网络暴力进行类型划分的基础上，应当对网络暴力采取一系列事前、事后的防治措施，并通过形成行业标准和惯例等方式固定下来。在网络暴力的治理中，网络平台的义务承担主要体现为违法内容管理义务、数据保护义务和配合执法义务三个方面。但是，网络平台的守门人角色应当在符合我国国情的监管模式中来加以理解。不同的部门法语境下网络平台所扮演的守门人角色也存在很大差异，从民法、行政法到刑法应当呈现层级性的结构。同时，强化网络平台守门人角色应当通过具体明确的规定来落实，不宜仅仅停留在宏观的制度设计之上。

网络暴力的法律治理是一项非常复杂的议题，其不仅需要多方合力协作，而且也呼唤新的网络空间治理思路。守门人理论为网络暴力的规制带来了新的思考路径，但是其并非一味地加重网络平台的责任，而是在原有法律责任框架下适当提升网络平台的义务，同时在不同利益诉求之间审慎地进行平衡。

Abstract　Cyber violence not only infringes upon personal legal rights, but also destroys a healthy online ecology. Many factors make the legal governance of cyber violence face great difficult, such as the ambiguity of the concept of cyber violence, the blurring of individual liability in group behavior, and the need for balancing freedom of expression and network regulation. Under the basic premise of pluralistic and co-governance of cyber violence, in addition to the identification of individual liability, attention should be paid to the legal regulation of online platforms. No matter from the principles of network technology and communication, or from the perspective of legal responsibility determination, this is a reasonable choice. Currently, in the governance of illegal information and content in cyberspace, highlighting the gatekeeper role of large-scale online platforms has become a representative legal practice abroad. This is also an important institutional design for the regulation of cyber violence in China. The legal connotation of the gatekeeper institution of online platforms can be elaborated from two perspectives: technical measures and obligations undertaking. The gatekeeper institution of online platforms should be in line with the national conditions of online regulation in China. Attention should be paid to the different normative goals of different departmental laws, such as civil law, administrative law, and criminal law, so as to build a reasonable hierarchical structure for the gatekeeper institution. The gatekeeper institution of the online platform also needs to be implemented through clear, concrete and operable stipulations.

Keywords　Cyber Violence, Platform Liability, Gatekeeper, Hierarchical Structure

（责任编辑：樊传明）