网络暴力型累积犯的刑法应对

张喆锐

【摘　　要】网络暴力行为所具有的累积犯的特点，使得针对网络暴力的刑法应对始终面临法益保护原则和刑法谦抑性原则的张力。只有将处罚对象限制为具有支配地位的责任主体，才能妥当化解来自责任主义原则和微罪不罚原则之质疑。应当根据不同网络参与者的角色定位确定不同网络参与主体对形成累积性结果的支配程度。总体而言，在刑事政策上，应当秉持弱化普通网络用户责任、强化具有网络影响力用户与网络服务提供者责任之立场；在此基础之上，还应根据不同主体参与具体网络传播方式之不同，进一步明确影响行为的刑事可罚性的因素。

【关 键 词】网络暴力；累积犯；角色义务；刑法谦抑性；微罪不罚

【作者简介】张喆锐(1995-)，男，东南大学法学院博士研究生，研究方向：刑法学(江苏 南京 211189)。

【原文出处】《东岳论丛》(济南)，2024.4.175～182

【基金项目】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”(项目编号：21&ZD209)。

一、问题的提出

网络暴力是数字社会中的严重失范行为，对民众日常生活造成显著消极影响。为有效防范和解决网络暴力、切实保障广大网民合法权益，2022年4月，中央网络安全和信息化委员会办公室(以下简称“中央网信办”)部署开展“清朗·网络暴力专项治理活动”，同年11月印发《关于切实加强网络暴力治理的通知》，要求切实加大网暴治理力度，维护文明健康的网络环境，并于2023年7月发布《网络暴力信息治理规定(征求意见稿)》(以下简称《征求意见稿》)。

以上专项行动和通知、意见，虽然客观上有助于抑制网络暴力、净化网络空间、优化网络生态，但不可否认，长期以来网络暴力治理难见成效。除了缺乏针对网络暴力行为之一体化的领域立法外[①]，作为最严厉制裁的刑法在处理该类问题时角色定位之模糊，也是造成治理失效的重要原因。一方面，刑法的目的是保护法益。处罚累积犯可以实现对法益的全面保护，但只要存在法益侵害或者能够抑制法益侵害的危险就介入刑法，很容易导致处罚范围被不当扩张[②]。另一方面，刑法具有谦抑性。作为具体个体实施的网络暴力行为，一般而言，都是没有对保护法益造成实质侵害的轻微违法行为[③]。倘若不加区分地肯定刑法之介入，刑法谦抑性原则将被架空，甚至造成刑法介入的道德危机[④]。前述问题导致刑法谦抑性和刑法法益保护功能之间的张力于网络暴力行为的刑法治理领域再次凸显。

刑法的法益保护机能和刑法谦抑性原则之间的张力只是表面现象，更为深层次的原因是，与一

般违法犯罪行为不同，网络暴力行为具有累积性特点[5]。“就行为与法益之间的关联性来看，从实害犯到具体危险犯，再到抽象危险犯，最后到累积犯，行为与法益的关联性越来越松弛，法益概念越来越抽象、模糊”[6]，在行为与法益关联已经较为模糊的累积犯情形中，即使有法益保护原则为之加持，刑法的轻易介入仍然面临来自刑法谦抑性原则之质疑。因此，明确累积犯对于刑法评价之意义是破解网络暴力型累积犯刑法治理困局的关键所在。

基于以上分析，本文从网络暴力为代表的新型累积犯所带来的刑法挑战出发，通过论证网络暴力型累积犯处罚的正当性根据，明确应对网络暴力型累积犯的刑法立场，并在此基础上提出针对网络暴力型累积犯的刑法应对。

二、区分网络暴力参与者的责任主体地位

(一)网络暴力型累积犯的刑法应对困境

发生于物理现实空间中的暴力，受制于物理时空的限制，通常表现为一对一的形式，即使存在多对一的情形，犯罪人的数量和其造成的社会危害也受到时空的限制。随着网络时代的到来，前述一对一的暴力模式已经被彻底改变，而多对一成为网络暴力之常态。网络空间的虚拟性以及匿名性导致的网络主体去责任化及群体极化问题，传播过程中“沉默的螺旋”导致的强势“民意”问题、舆情传播中羊群效应导致的盲目随从问题，共同触发了网络暴力[7]。相较于现实空间中的语言暴力，在多对一的网络暴力中，被网暴者往往面对海量负面信息，承受超乎寻常的精神压力[8]。通过前述对比可以发现，由集体非理性导致的个体走向集体过程中所形成的网络暴力的累积性效应，使得网络暴力能产生远超线下空间的社会危害性。

从累积犯的最终效果看，网络暴力行为具有极大的社会危害性。与整体性观察相反，如果单独考察每一个具体行为主体实施的单一网络暴力行为，通常而言，其不具有对(通常是集体的)利益的完整性造成损害的具体危险[9]。在法益理论看来，值得处罚的行为是对法益造成实际损害或者危险之行为。随着全面保护法益的需要，危险的起点可以无限向前移动[10]，基于法益保护原则，很容易说明处罚网络暴力行为的根据。但是，植根于法益理论的理论进路仍将面临两个重要质疑。

其一，微罪不罚的问题。处罚累积犯的理论面临来自“微罪不罚”之质疑。一方面，在法益损害结果或者危险累积形成的过程中，即使在局部地区存在生成集体非理性的可能性，但由于各个轻微行为之间的关联性较为微弱，各个轻微行为与该集体非理性形成的证成是相当困难的。换言之，并没有某一方主体主导性地控制整个进程的发生。另一方面，法益理论的扩张本质导致对个体进行追责。正是由于一个总体性的集体非理性证成上的困难，导致无法找到适格主体来为此损害结果承担责任。法益理论内在的扩张本质逻辑在此显现。在传统累积犯理论的语境下，法益保护思想被表达为，为了避免大量同样轻微行为的发生从而最终损害法益，需要有主体来为未来的损害结果承担责任，哪怕这个主体所施行为的损害是微不足道的。可见，传统累积犯理论为了证明“微罪可罚”，只能向他人“寻求帮助”。单独的损害行为不可罚，正是因为他人也同样实施了相同的损害行为，共同累积造成了损害结果，通过对他人损害行为的“代偿”，获得对该轻微行为进行惩罚的理由。这也恰恰步入了另一个理论困境，即违反罪责原则。

其二，罪责原则的问题。累积犯面临的最大挑战是其违背了罪责原则。罪责原则坚持自己责任原则，反对团体责任或者说连带责任。单独看累积犯行为，其在很多情况下属于轻微不法行为。因为，其既不会对集体法益的完整性造成损

害,也不会具体地直接危及个人法益。只有当大量的个体实施相应行为时,才可能基于累积性效果产生法益损害或者法益损害的危险[11]。换言之,该类案件中的重大危险属系统性问题[12]。在法律评价上,如果以造成损害结果或者法益损害危险为由处罚累积犯,实质上将导致连带责任或者说团体责任。因为单独的累积犯行为仅是轻微不法行为,其并不能单独造成系统性的损害或者整体的损害,该损害是因为他人也同样实施了相同的损害行为,共同累积造成了损害结果。因此,处罚累积犯行为涉及连带责任(ex iniuria tertii)的问题,即个人不是因为自己,而是因为他人的行为受到处罚[13]。正如批评者所言,在累积犯的情境下,个体行为成了刑事归责的动因(Anlass),而不再是根据(Grund)[14]。这种不断降低轻微行为界限的理论,至少部分实现了整体结果归责的效果[15],涉嫌将整体责任归于个人,从而违反罪责原则。

(二)具有支配地位的责任主体与刑法应对困境的化解

基于法治国理念,责任主义原则和微罪不罚原则均应当得到遵守。但这不意味着网络暴力行为不受处罚。要克服传统累积犯理论面临的两大质疑,核心在于确认哪些主体可以被视为网络暴力累积性结果形成进程中占据支配地位的责任主体。

其一,将归责对象限于具有支配地位的责任主体,可以避免来自责任主义原则的质疑。责任主义原则强调每个主体仅对自己的行为造成的结果负责。从自己责任主义的角度看,符合责任主义原则的归责必须建立在结果是行为人的行为造成而非他人的行为造成这样的前提之上[16]。满足前述要求的因果流程,意味着在众多导致结果产生的条件中,行为主体对于累积性进程中因果环节具有支配力,其他的行为只不过是其所支配的因果环上的一环而已。在满足前述要求的情况下,由行为主体对其他行为人的行为造成的结果负责,也就是对自己支配的因果流程的整体造成的结果负责。

其二,将归责对象限于具有支配地位的责任主体,可以避免来自为微罪不罚的质疑。如前所论,累积犯的特点是:在孤立看待单个网络暴力行为时,该单个行为不具有严重社会危害性,只有众多行为累积才能产生严重的社会危害性。因此,倘若将单个的暴力行为与累积犯的整体社会危害性关联考察,在能肯定单个暴力行为在导致整个结果的因果流程中起到支配作用时,就可以肯定该行为具有较大社会危害性。因此,在能肯定网络暴力累积性进程中占据支配力的责任主体时,对之加以处罚并不违背责任主义原则和微罪不罚的要求。

其三,将归责对象限于具有支配地位的责任主体,符合网络犯罪的底层逻辑。网络暴力行为以大量个体实施的轻微损害行为为构成基础。如前所论,每一个具体主体实施的网络暴力行为通常仅是轻微不法行为。其之所以最终造成严重的社会危害性,在于众多网络暴力行为累积而成。虽然在线下空间,单一的网络暴力行为受制于时空限制很难形成累积性效果,但是在整个网络暴力进程当中,由于互联网信息传播的底层逻辑,大概率存在着能实质性影响甚至支配事件发生的关键因素。换言之,在网络暴力当中能够找到为此负责的核心主体。

(三)具有支配地位责任主体的确定标准

最高人民法院、最高人民检察院与公安部联合印发的《关于依法惩治网络暴力违法犯罪的指导意见》(以下简称《指导意见》),根据行为主体行为模式之不同,将重点打击对象区分为“恶意发起者”“组织者”“恶意推波助澜者”以及“屡教不改者”。以行为模式为标准的划分,难以反映网络暴力中多方主体间的结构关系。与此相对,《征求意

见稿》根据不同参与主体的角色定位之不同，将网络暴力结构关系中的参与主体划分为网络用户与网络服务提供者。根据主体功能不同或者说角色不同进行分类较为妥当。因为不同主体往往体现不同的支配力。孤立地看发生于网络空间中的每一个单独个体实施的侮辱、诽谤、侵犯隐私行为等与现实社会中的对应行为并无差异；而且由于网络暴力发生于虚拟空间之中，单一个体的网络暴力行为并不像现实暴力行为[17]那样，直接对被害人造成侵害。加之，在“信息大爆炸”时代下网民对于“无足轻重”的“网络暴力”一般并不关心。因此，单个个体的网络暴力行为通常不会对被害法益造成实质侵害。换言之，网络暴力行为之危害不在于单独个体实施的网络暴力行为，而在于相应暴力行为因非理性之契机累积而成的整体损害。从这样的角度看，在网络暴力社会危害的形成之中，关键不在于网络暴力所传达的信息而在于相应信息之传播。“传播属性”较“事件属性”而言具有更关键的作用，特别是借助算法技术的助推、各方媒体的参与、公众人物及意见领袖的二次扩散等[18]。

在互联网信息传播过程中，不同主体虽然传播同样的信息，但因其在信息传播过程中所具有的角色定位不同，必然意味着其对信息传播的影响也不同。相较于普通网络用户，掌握流量密码的网络“大V”、网络平台可能更容易引导乃至主导信息之传播，使得普通互联网用户在群体压力之下会产生顺从行为，即使不是由于群体压力，少数群体也会在社会顺从心理的影响下潜移默化其决策[19]。因此，《征求意见稿》基于用户角色区分网络参与主体的逻辑是妥当的。但其对网络用户的规定还较为模糊。鉴于网络暴力行为的危害在于其所形成之累积性后果，而累积性后果之形成与信息之传播密切相关。因此，在《征求意见稿》的基础上，应当根据网络用户的职能定位与资源支配的不同，进一步将其区分为普通网络用户与网络影响力用户。

面对刑法的规范性期待，普通网络用户应当履行作为一般性规范接受者，即普通公民，所具有的一般守法义务。譬如，在互联网中，普通网络用户应当履行不侮辱、诽谤、侵犯他人个人信息的守法义务。而网络影响力用户由于其定位与资源整合支配能力的不同，考虑到其在互联网当中所享受的流量资源红利以及所产生影响的广阔性，应当负担更高的审慎义务。而作为网络服务提供者，其所负担的更多是监管义务。但是，上述义务边界仍过于模糊，以下将尝试进一步明确该边界。

三、网络暴力型累积犯责任主体的类型与刑法应对立场

根据网络用户责任主体地位之不同，在网络暴力累积犯之法律评价选择上，应采取弱化普通网络用户责任、强化网络影响力用户责任与强化网络服务提供者责任的立场。

(一)弱化普通网络用户责任之根据

弱化普通网络用户在网络暴力中的答责可能性首先源于，在通常情况下普通用户对累积性后果的形成不具有支配性地位。普通网络用户并不掌握流量密码，不但通常不具有引导或者主导信息传播的能力和资源，在很多情况下反而受制于“信息茧房”，在信息获取和传播中处于被支配地位。所谓“信息茧房”，是指在现代互联网环境中，个人或群体因被包含在信息壁垒之内，其接受或者传播之信息常被固定为特定种类信息[20]。有研究表明，在一般情形下，当有影响力用户传播同类型信息收益高于传播异类型信息收益时，无论普通用户选择接受同类型信息抑或异类型信息，都容易形成信息茧房[21]。此时普通用户不仅传播力有限，其选择的空间也十分有限[22]。其所谓的个体自由决断，只不过是基于信息“偏见”所作出的。一般情况下，不能认定此时网络个体的认知是“自

由”的,换句话说,其意志的形成与意志的实现都不是自由的[23]。因此,与其说普通网络用户可以主导信息之传播,不如说普通用户在信息传播和形成过程中受制于信息茧房而始终处于被支配的地位。

除此之外,限制对普通用户之归责符合罪责原则和微罪不罚原则的要求。众多网络暴力行为累积形成的损害结果虽然极其严重,但归责对象终究是个人而非群体。而单个的网络暴力行为所造成的损害结果极其微量,网络暴力型累积犯归责的重点是那些制造或加剧集体非理性效应的主体,而并非受集体非理性所影响的普通网络用户。换言之,由于普通用户对累积犯结果之出现不具有支配性,此时,再将结果归责于普通用户将违背责任主义原则和微罪不罚的要求。为了避免违反责任原则,在一般情况下,普通网络个体应当仅仅为自己的行为承担责任,不能因为与“相关”他人共同造成了恶劣结果就扩张性地对其进行惩罚。

(二)强化网络影响力用户责任之根据

之所以应强化网络影响力用户在网络暴力中的答责,是因为其在累积性效果形成过程中居于支配地位。

其一,网络影响力用户具有公共属性。技术发展和制度共同为网络影响力用户的产生提供土壤。在传播学中,网络影响力用户往往被称为“意见领袖”。而个体能替代传统媒体成为具有网络影响力的用户,正是由去中心化的自媒体时代所成就的。作为社会表演者的意见领袖,他们的身份想象有赖于其他网络用户的认同[24]。这使得网络影响力用户具有不同于普通网络用户的公共属性一面。分析网络影响力用户在信息传播中的作用时,我们不能单纯强调其个人属性,更应当重视其角色所蕴含的公共属性一面。正是后者导致网络影响力用户拥有引导乃至主导信息传播的能力。

其二,网络影响力用户在网络暴力累积效应形成中具有重要作用。最终决定传播力大小的重要因素仍然是事件的传播过程,网络影响力用户对事件发酵的作用要大于事件本身。正如研究所示,网络影响力用户往往能够在网络暴力累积效应中成为重要变量。例如,作为意见领袖的网络用户在其粉丝那具有信任基础,在价值观念上其粉丝一般与之具有相似性,因此,粉丝群体容易与网络影响力用户达成共识。此外,受群体极化效应的影响,即使作为非粉丝群体的少数异见群体也可能受其影响而转变态度立场。因此,网络影响力用户通常能使事件得到二次传播,从而进一步扩大事件本身的传播力。如果再与“算法助推”以及“首发内容具有明显倾向性”相结合,则会共同构成具有最高传播力的网络暴力事件的最显著途径[25]。

综上,由于网络影响力用户自身的公共属性以及在累积效应中的重要作用,应当对其科以更多的审慎义务。

(三)强化网络服务提供者责任之根据

看门人理论为强化网络服务提供者的答责提供了理论支持。强化网络服务提供者责任的理由在于两个方面,即网络服务提供者在网络暴力中的重要影响与监督保证人身份地位。

其一,网络服务提供者在网络暴力累积性效应形成中具有关键作用。学界认为,“看门人”理论可以为网络服务提供者不法的成立提供支撑。在前互联网时代,传统媒体是人们接收信息的主要渠道,传统媒体作为新闻资讯的看门人,在极大程度上能够影响甚至决定受众群体的认知和价值观念。而在互联网时代,网络成为人们获取信息的主要途径。人们逐渐习惯通过算法程序来获取信息、认识世界,而算法偏见则成为人工智能时代社会偏见的一种体现[26]。算法偏见使算法程序在

信息生产与分发过程中失去客观中立立场，造成片面或与客观实际不符的信息，影响公众对信息的客观全面认识[27]。这种算法偏见所带来的法律风险不在于作出不利于人的决策，而是能代替或参与人的决策[28]。换句话说，算法助推机制很大程度上会形成算法偏见，而网络服务提供者在算法偏见中起到了助推作用[29]，使得公众陷入信息茧房之中。因此，在当前自媒体时代，看门人地位的实质内核仍未改变，改变的只是信息传播和接受方式以及承担看门人职责主体之扩展。由此，作为信息传播者的网络服务提供者，负有对危险源的监督义务。

其二，网络服务提供者具有监督保证人地位。监督保证人对于某些特定的危险源具有特别的安全保障义务，其必须保证这个危险源不会扩散和伤害他人，而需要被监管的危险源不仅包括物，也包括人[30]。这种监管义务首先是一种民法上的交往安全义务，那些拥有一栋房子和一块土地的人必须保护居住者和拜访者不会因为不充足的安全措施而受到损害[31]。同理，网络服务提供者应当对其所提供的网络服务负有安全监管责任，保证网络服务的使用者不会因为提供者的不充分的网络安全保障措施而受到损害。“在网络社会中，网络服务提供者对于危险源的监督，产生了保护他人法益不受来源于自己控制领域的危险威胁的义务……该保证人义务的根据在于，复杂社会系统中的秩序必须依赖于处分权人所管理的特定空间和特定控制领域的安全。”[32]当网络平台不履行该义务时，客观上会促进违法行为的发生、信息的传播，甚至导致刑事追诉证据灭失。因此，网络服务提供者虽不直接实施网络暴力行为，但基于其角色地位，其不但有责任保障其服务使用者在限度内发表言论，而且在用户违反自身的言论自由界限时，也需要网络服务提供者履行监督义务。

四、影响不同类型网络暴力型累积犯刑法评价的具体因素

为贯彻刑法谦抑原则，避免在累积犯情形下不当扩大处罚范围，下文将以网络暴力中的三方角色关系为基础，以具体情形为例，进一步明确弱化普通网络用户责任、强化网络影响力用户与网络服务提供者责任的具体标准。

(一)影响普通网络用户刑事可罚性之因素

基于普通网络用户认知上的“信息茧房”效应以及个体损害结果上的微量性，在普通网络用户仅实施简单的侮辱、诽谤、人肉等其他个体性网络暴力行为时，应当实现刑事治理的升维化打击，不应轻易将之评价为犯罪行为。换言之，此类违法行为所创设的风险极其轻微尚未达到需要刑法禁止之程度，哪怕相应行为意外造成严重损害结果，也不能认为该损害结果是相应行为所创设风险的现实化。除非普通网络用户所实施的行为对于累积性网络暴力的形成具有支配力，或者其对该支配力具有直接因果作用力，才可以考虑其刑事可罚性。以下列举三种典型情形。

【情形一】利用“深度合成”等生成式人工智能技术发布涉及社会敏感谣言信息的。深度合成技术是基于对抗式生成网络模型建立起来的。其所生成的虚假信息逼真程度之高，譬如人脸替换、人脸合成、语音合成等，往往以十分令人相信的方式呈现给社会公众[33]。正如丁汉青教授的研究所展现的，除“算法助推”外，“首发内容倾向性”与“是否存在谣言”两个条件变量也对网络暴力事件的高度传播具有重要催化作用[34]。而诽谤型网络暴力往往同时具有上述两个条件变量。深度合成技术所生成的虚假信息具有高度逼真性，普通网络用户通常缺乏辨别该类信息真假的辨识能力，容易因误信而传播，使得此类诽谤行为往往具有引发后续网络暴力的高度可能性，换言之，该行为具有引发集体非理性的高度支配可能性。同理，与

该类行为相类似的行为，例如恶意篡改聊天记录、拼接照片、裁剪视频等行为，同样具有高度逼真性，若相关内容同时具有高度社会敏感性，很容易引起信息广泛传播，引发后续网络暴力。因此，对于前述由普通网络用户实施的网络暴力行为，应当肯定其刑事可罚性。

【情形二】恶意为网络暴力信息购买热搜或以其他方式广泛扩大其影响的。如前所述，算法助推是高传播力网络暴力事件得以发生的充分条件之一。以新浪微博购买热搜为例，该服务旨在短时间内扩大微博发文的推广度和曝光度。虽然在受众群体上，普通网络用户与其受众群体之间缺乏有影响力的网络用户与其粉丝之间的信任关系，但该服务与网络影响力用户转发或发布微博具有一定相似性，都对微博发文的影响力具有扩大作用。而之所以强化对网络影响力用户的责任，恰恰在于其利用粉丝对其之信赖，可以影响相应信息之传播。因此，考虑到购买热搜行为对于扩大网络暴力信息具有实质推动作用，积极促使高传播力网络暴力事件的形成，应当肯定该行为具有刑事可罚性。

【情形三】积极收买网络影响力用户推动网络暴力信息传播。该情形是在共犯的语境下进行讨论的，但仍然需要注意限制该情形处罚范围。对于仅仅与网络影响力用户以例如私信的方式达成联系，简单将相关信息告之网络影响力用户的，一般情形下应否认该行为的刑事可罚性。除非在该过程中，其通过其他方式能影响网络影响力用户之选择。如通过支付报酬或者给予其他酬谢等方式收买网络影响力用户推动网络暴力事件传播的，才应当考虑其刑事可罚性。

(二)影响网络影响力用户的刑事可罚性之因素

在社交媒体中，网络影响力用户具有个人性与公共性双重属性。在涉及日常事项的表达当中，网络影响力用户与普通网络用户没有本质上的不同，享有与后者等同的言论自由权。但是，在涉及社会敏感问题的讨论上，由于其形成过程中的公共性与在高传播力网络暴力事件中的重要地位，要求网络影响力用户负有更高的审慎义务。不过，在涉及公共事项监督问题时，基于社会整体利益之考虑，对其谨慎义务之要求应区别于一般社会敏感问题讨论。譬如，当公民的言论关涉政治、公共管理、公共人物等公事时，即使其言论具有一定的虚假或者夸大成分，其可罚性也要受到必要的限制[55]。在其他社会敏感问题讨论上，网络影响力用户的刑事可罚性主要基于未履行必要的审慎义务之程度。此处的审慎义务是一项积极义务，具体表现为信息的审查义务与表达的慎重义务。

首先是信息审查义务。此种审查义务主要表现为对信息内容真实性的审查。一是对于那些已经被网络平台标识为“可能不实”的推文，应当尽到最高的审查义务，除非确有证据证明推文的真实性，否则不应进一步扩散。二是对于那些未被平台标识，但关键信息缺失，行文前后逻辑矛盾，可能是虚假信息的，应当尽到一般理性人的审查义务。譬如，要求投稿者补充信息，或者在转发时以突出方式强调原推文的关键信息缺失等漏洞，提醒网友理性慎重对待。三是对于那些明显不实的推文，不得进行二次扩散。

其次是表达慎重义务。此种表达慎重义务主要表现为表达的价值中立性。一是对于可能导致网络暴力的社会敏感事件的讨论，不得采取可能引起群体侮辱的措辞。譬如，不得在转发热点事件时发表侮辱性言论或者鼓励、怂恿表达侮辱性言论。二是对于涉及“道德审判”的社会敏感事件，可以就事件本身进行一般性讨论。但是当讨论对象指向具体个人时，应当进一步分析是否会对被指向个体造成伤害。若违反上述审慎义务，

则视为创设了法所不允许的危险。

(三)影响网络服务提供者刑事可罚性之因素

网络服务提供者的责任主要是一种安全管理责任。

其一,作为前置法的行政法对网络服务提供者的安全管理义务进行了明确规定。作为网络领域的“基本法”,第9条规定“网络运营者开展经营和服务活动,必须遵守法律、行政法规……,履行网络安全保护义务,接受政府和社会的监督,承担社会责任。”《网络安全法》第10条规定“建设、运营网络或者通过网络提供服务,应当依照法律、行政法规的规定和国家标准的强制性要求,采取技术措施和其他必要措施,保障网络安全、稳定运行,有效应对网络安全事件,防范网络违法犯罪活动”。此外,《网络安全法》第三章和第五章分别对“网络运行安全”和“监测预警与应急处置”做出的相对具体的安全义务管理规定,为《刑法》第286条之一拒不履行信息网络安全管理义务罪提供了明确的前置法基础。在具体的网络暴力治理领域,《征求意见稿》对网络服务提供者针对网络暴力信息治理的管理义务进行了更加详尽且更具针对性的规定。

其二,不宜将网络服务提供者评价为具体网络暴力行为的共犯。一方面,网络服务提供者所负担的监督保证人义务是一种一般性的安全保障义务,对一般性危险源而不是具体危险源的监管义务。一般性危险源表现为一种制度性缺陷,指的是在网络媒介不再是一种纯粹中立的工具反而塑造人的行为方式时[39],服务提供者所提供服务中的制度性或技术缺陷成为网络暴力形成的支配性原因,此时,网络服务提供者有义务对该危险源进行监管,对制度性或技术缺陷进行修补。对具体危险源(即个体网络暴力实施者)的监管无非是对网络服务提供者科以一种无法承受的监管负担。另一方面,网络服务提供者所提供的服务一般情形下并非专门用于促进网络暴力。此处涉及的是中立帮助行为的问题。如果该服务只是偶尔被不法者用于实施违法犯罪,不宜将其认定为客观上的帮助行为。

五、结语

基于互联网底层逻辑的差异,网络暴力型累积犯的刑法应对面临时代难题与挑战。对累积犯进行处罚具有教义学上的正当性,因为任何网络暴力行为对结果的发生都具有因果力。但是大范围处罚累积犯可能违背微罪不罚的原则。在构建轻罪体系的过程中,应当将“治罪与治理并重”,才能实现中国式法治现代化所追求的善治目标[59]。因此,在对处罚累积犯的观点持肯定态度的基础上,仍然应当坚持刑法谦抑原则。在处罚累积犯的同时,明确言论自由的范围,明确不同类型行为人的自由界限及其各自的保证人义务,以期完成对累积犯处罚路径的构建。

注释:

①参见刘艳红:《网络暴力治理的法治化转型及立法体系建构》,《法学研究》,2023年第5期。

② Vgl. Pawlik, Das Unrecht des Bürgers, Tübingen: Mohr Siebeck, 2012, S. 139.

③参见孙国祥:《论累积犯的正当性及其限度——兼谈累积犯对污染环境罪构成的影响》,《法学》,2023年第9期。

④参见李礼:《网络暴力的道德批判与规制》,《晋阳学刊》,2020年第6期。

⑤参见张凌寒:《“不良信息”型网络暴力何以治理——基于场域理论的分析》,《探索与争鸣》,2023年第7期。

⑥孙国祥:《论累积犯的正当性及其限度——兼谈累积犯对污染环境罪构成的影响》,《法学》,2023年第9期。

⑦李华君,曾留馨,滕姗姗:《网络暴力的发展研究:内涵类型、现状特征与治理对策——基于2012-2016年30起典型网络暴力事件分析》,《情报杂志》,2017年第9期。

⑧参见喻海松:《网络暴力的多维共治——以刑事法为侧

重的展开》,《江汉论坛》,2023年第5期。

⑨ Vgl. Wohlers, Deliktstypen des Präventionsstrafrechts, Berlin Duncker & Humbolt, 2000, S. 318.

⑩ Vgl. Jakobs,"Kriminalisierung im Vorfeld einer Rechtsgutsverletzung", ZStW, 1985, S. 753.

⑪ Vgl. Wohlers, Deliktstypen des Präventionsstrafrechts, Berlin: Duncker & Humbolt, 2000, S. 318.

⑫Vgl. Silva Sánchez, Die Expansion des Strafrechts, Frankfurt am Main: Klostermann, 2003, S. 76.

⑬ Vgl. Roxin Greco, Strafrecht Allgemeiner Teil, Bd. 1, Nördlingen: C. H. Beck, 2020, § 2 Rn. 82.

⑭ Vgl. Saliger, Umweltstrafrecht, München: Vahlen, 2020, S. 118.

⑮ Vgl. Samson,"Kausalitäts- und Zurechnungsprobleme im Umweltstrafrecht", ZStW, 1987, S. 635.

⑯蒋太珂:《因果力比较规则的刑法理论构造》,《法学研究》,2023年第1期。

⑰此处所指与网络暴力行为相对应的现实行为类型。

⑱参见丁汉青,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)》,《广州大学学报》(社会科学版),2023年第1期。

⑲参见周曼,郭露:《自媒体时代的网络暴力群体极化效应成因研究:结构方程模型的证据分析》,《江西师范大学学报》(哲学社会科学版),2021年第4期。

⑳参见崔春梦:《网络交往"信息茧房"的意识形态效应及其治理》,《北京交通大学学报》(社会科学版),2023年第3期。

㉑参见杨芳芳,宋雪雁:《自媒体平台信息传播中信息茧房形成的演化博弈研究》,《情报科学》,中国知网网络首发,发布时间:2023年10月23日。

㉒参见[美]凯斯·R.桑斯坦:《信息乌托邦:众人如何生产知识》,毕竞悦译,北京:法律出版社,2008年版,第8页。

㉓参见朱奇伟:《故意体系地位变更的方法论意义》,《法律方法》,2023年第2期。

㉔参见吴迪:《微博"意见领袖"的形成机制及其思考》,《北京邮电大学学报》(社会科学版),2016年第2期。

㉕参见丁汉青,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)》,《广州大学学报》(社会科学版),2023年第1期。

㉖参见岳平,苗越:《社会治理:人工智能时代算法偏见的问题与规制》,《上海大学学报》(社会科学版),2021年第6期。

㉗参见郭小平,秦艺轩:《解构智能传播的数据神话:算法偏见的成因与风险治理路径》,《现代传播》,2019年第9期。

㉘参见刘艳红:《生成式人工智能的三大安全风险及法律规制——以ChatGPT为例》,《东方法学》,2023年第4期。

㉙参见丁汉青,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)》,《广州大学学报》(社会科学版),2023年第1期。

㉚Vgl. Rengier, Strafrecht Allgemeiner Teil, Nördlingen: C. H. Beck, 2021, S. 510.

㉛ Vgl. Roxin, Strafrecht Allgemeiner Teil, Bd. 2, Nördlingen: C. H. Beck, 2003, S. 747.

㉜皮勇:《论新型网络犯罪立法及其适用》,《中国社会科学》,2018年第10期。

㉝参见万志前,陈晨:《深度合成技术应用的法律风险与协同规制》,《科技与法律》,2021年第5期。

㉞参见丁汉青,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)》,《广州大学学报》(社会科学版),2023年第1期。

㉟参见刘艳红:《网络时代言论自由的刑法边界》,《中国社会科学》,2016年第10期。

㊱参见王华伟:《网络空间正犯与共犯的界分——基于特殊技术形态的考察》,《清华法学》,2022年第3期。

㊲参见刘艳红:《民刑共治:中国式现代犯罪治理新模式》,《中国法学》,2022年第6期。