《学术界》(月刊)
总第243期,2018.8
ACADEMICS
No.8 Aug. 2018

维护网络意识形态安全的法治技术模式探析〔*〕

○ 李栗燕[1,2]
(1.南京师范大学　中国法治现代化研究院,江苏　南京　210097;
2.南京航空航天大学　人文与社会科学学院,江苏　南京　211106)

〔摘　要〕针对我国网络空间安全面临的挑战,引入网络安全学领域成熟的P2DR动态循环模型,在法治视野中构建起规则体系,探索维护网络意识形态安全的法治新路径。通过防护(P)、检测(D)、响应(R)三个环节的设计,实现维护网络意识形态安全的策略(P)。理论层面,剖析与分辨网络社会思潮(P),解读与提炼社会主义法治精神(D),渗透与弘扬社会主义法治精神核心内涵(R),以构建"防御、甄别、引导"三个功能的法治理论体系;实践层面,以"循序渐进"为重点完善信息"入口"制度(P),以"隐私保护"为重点健全信息"通过"制度(D),以"责任落实"为重点推进信息"治理"制度(R),构建"防御、控制、惩戒"三个功能的法治实践体系。

〔关键词〕网络意识形态安全;P2DR模型;法治创新;社会主义核心价值观
DOI:10.3969/j.issn.1002-1698.2018.08.013

互联网时代信息爆炸式发展,意识形态法治安全成为网络安全的新课题,随着各种网络思潮、"主义"冲击着主流意识形态,网络成为意识形态交锋的新战场。[1]网络本身的技术性、开放性、即时性、自由性给网络意识形态建设带来了挑战。[2]国际环境方面,西方国家凭借其强大的经济实力和话语霸权否定马克思主义意识形态的科学性和合理性,试图渗透消解主流意识形态主导地位;国内

作者简介:李栗燕,法学博士,南京师范大学中国法治现代化研究院博士后、特邀研究员,南京航空航天大学教授、博士生导师,研究方向:法政治学、网络安全法治。

〔*〕本文系中国博士后科学基金特别资助项目"新时代构建网络空间安全命运共同体的法治进路研究"(2018T110524)及"维护网络意识形态安全的P2DR法治路径研究"(2017M611860)、国家社科基金项目"维护网络意识形态话语权的法治路径研究"(17BKS135)的研究成果,并受中央高校基本科研业务费专项资金(No.NK2018008)资助。

环境方面,经济体制变革、社会结构变动、利益格局调整,社会的阶层化加速了利益主体的多元化和利益诉求的多样化,[3]公民自由权的异化消解着社会主义意识形态的合法性;理论上,“文革”时代马克思主义的“唯我独尊”,切断了与非马克思主义意识形态的交流与对话,造成后“文革”时代的失语,弱化了马克思主义理论软实力;实践上,马克思主义理论创新的滞后性使其对现实社会的解释力降低,学术理论大众化宣传的表象性使其对现实社会的适应性不足,网络意识形态安全面临诸多困境。不可否认的是,马克思主义话语的“理论彻底性”和“理论实践性”指引社会主义运动的进程,[4]我们需提升应对能力与方式,在梳理我国网络意识形态安全现状的基础上,分析其发展情势,探索维护网络空间的意识形态安全的新对策。

新挑战呼吁新路径,2016 年 12 月中共中央办公厅、国务院印发的《关于进一步把社会主义核心价值观融入法治建设的指导意见》中强调“加强互联网领域立法,完善网络信息服务、网络安全保护、网络社会管理等方面的法律法规。”这再次确认了,加强互联网法治建设是维护我国网络意识形态安全的重要实现路径。互联网时代我国意识形态安全法治建设要紧随互联网发展之步伐,积极地抓住机遇、应对挑战,必须在理论与实践两个层面上加强建设的力度与深度。

一、我国网络意识形态安全法治建设的路径选择

维护网络意识形态安全是一个跨越马克思主义理论、政治学、法学、计算机科学的新兴研究领域,对相关学科具有较高的系统创新要求。可是,目前的研究及创新与新时代的现实需求相比并不丰沛,研究成果重价值理性轻工具理性。如果,想要统筹好各学科之间的关系,最终有效落脚于法治路径,就首先要提炼出各关键领域对法治路径提出的新要求,其次再探寻能够有效响应这些新要求的法治新路径。

(一)网络技术领域对法治路径的层次化指向

网络空间是现实空间的投射,是法律个体的行为在网络环境下的总和。网络天然的开放性、碎片化以及去中心化等特征,使得网络安全的维护机制也呈现出多样化,国内外学界主要从治理的法治规范和技术防护、政府和社会协调监管、建立网络应急系统等方面对网络行为、语言进行分析,对法律和道德价值层面上的网络社会特质、个人行为方式等方面做出探讨。虽然国内外学界对于网络规制一直存在着诸多争论,而且这种争论也将伴随着互联网的发展持续下去,但“网络空间不是法外之地”已经成为共识。关于网络安全的立法模式,最具代表性的是全面立法理论,即将网络与现实社会等同看待,建立完备的网络管理的法律法规体系。从实践来看,各国在网络领域所不断呈现出的法治需求及其积极的立法态势,恰好是实践对理论共识的检验和印证,运用法治思维和法治方式维护网络安全与秩序,是现代社会治理的有效路径和必然趋势。

现阶段我国网络领域的法律规制尚处于矛盾暴露阶段和法律填补阶段,国

内学界普遍认为现阶段网络领域的法律规制应以完善立法为主，主要研究了网络信息安全法制的基本性问题、国外网络信息安全的立法实践活动、我国网络信息安全立法的现状及对其的概括性建议，但学界在“依法治网”领域的研究思路多延续了在法学其他领域的研究思路，目前在一定程度上还体现为“兵来将挡、水来土掩”的研究态势，研究结论集中于较零散的立法层面，对网络空间的特殊性和规律性缺乏系统性规划和预测性设计。对此，网络空间技术领域的分层治理理论值得关注，美国学者 T. L. 萨迪系统阐述了网络层次分析法的基础、原理及应用，展现出网络层次化研究的必要性及可行性。[5] 国内学者也提出了网络空间安全等级的层次划分，包含系统定级、系统备案、建设整改、等级评测和监督检查五个方面，分级实施保护以提高我国网络安全建设的整体水平；[6] 网络空间参与主体的层次划分，以网络空间运营者、网络空间参与者以及国家网络空间安全管理者的不同身份，系统论述网络安全技术在保护关键基础设施、个人信息安全、网络安全监管预警和信息通报制度、应急处理机制等方面的具体应用。[7] 可以看出，网络领域的法治路径不可能脱离网络技术，网络的分层系统规制有其应然性。

（二）意识形态领域对法治路径的务实性要求

中国社会主义发展已经进入新时代，就国别关系来看，意识形态仍然决定着国家利益与价值取向；就社会制度来看，资本主义与社会主义两种异质的制度之间的对立与冲突仍然存在，由此决定的意识形态斗争仍然以一种更温和与隐匿的方式在强劲地开展；就文化层面来看，文化差异的存在是一种基本事实，意识形态的差异就是这种文化差异的重要因素与表征。就当代中国而言，意识形态仍然在人们的社会生活中扮演着突出的行动指南与策略武器的角色。这不再是一个唯意识形态的时代，然而意识形态仍然会深刻影响人们的思维、抉择与行动。因此，意识形态问题绝不仅仅只是思想领域的问题，是一个具有重大时代意义的多学科综合性研究课题。

面临意识形态领域的新较量，学者们纷纷建言献策，提出构建“网语体系”，[8] 彰显主流意识形态在理论上的“高势位”，[9] 将核心层、中间层的理论与外围层的实践语言充分融合[10] 等新建议。但究其实质，这不免又流于另一种表象性宣传下话语结构的更新。不正视现实矛盾，仅更新话语结构的思想政治教育，终将难以触动精神思想深处，终将难以捍卫意识形态安全。意识形态安全面临现实的困境和理论的徘徊，重提与再思法律意识形态正是对法律实践生活中一个具有时代意义课题的尊重与自觉。就理论而言，法治本身就是意识形态中不可分割的组成部分，社会主义法治精神的理论逻辑及意蕴与社会主义意识形态内核在本质上趋于一致；就实践而言，市场经济是法治经济，经济基础决定上层建筑，法治手段对经济活动的协调和规制，终将映射于作为思想上层建筑核心部分的意识形态领域。由于意识形态的抽象性，意识形态研究容易陷入多务虚而缺乏切实路径措施、纲领性强而操作性弱的僵局，“法治”作为工具性手段，其

规则性、操作性和务实性正是意识形态领域新的要求和期望,法治模式的构建和法学方法在意识形态领域的运用,构建起立体法治体系,拓展了意识形态领域的研究视野、思路及方法。

(三)法治路径在网络意识形态安全领域的选择与革新

全面依法治国与加强网络意识形态工作是相辅相成的辩证关系,两者并不矛盾。在网络意识形态斗争中,坚持全面依法治国,体现在对涉及网络意识形态斗争案件的执法中,就是能否落实法治精神,有效减少犯罪,最终实现公平正义。而加强网络意识形态工作,也有利于全面依法治国战略工作的开展,有利于进一步推动社会公平正义,有利于促进网络法治建设顺应新时代的诉求进入一个新的阶段。维护网络意识形态安全,需要权力与民主的共生、自由与秩序的博弈、法律与他律的平衡,如何在网络主体的权利设定中处理好国家权力同公民权利的关系、信息共享同信息专有的关系、隐私权与知情权的关系,都落脚于法治路径的选择与革新。

1. 理论层面:以层次化系统性设计为框架

国内学术界将维护意识形态安全的视角从思想政治教育领域逐渐拓展,虽并没有将法治运用于网络意识形态维护的直接研究,却可以梳理出以“依法治网”促进网络意识形态建设的基本观点:一是选择统一的立法模式,建立多元化的网络立法渠道。二是培养网络技术领域人才,提升网络管理法治化的实践水平,提出“法计算机学”。[11] 三是以“硬法为主、软法为辅”为治理原则,提出了“混合法治理”的新路径,进行全方位防护。[12] 四是坚持网络文化法治建设与道德建设相结合,进行网络文化的检测与法律规制,形成网络监管机制与网络施教机制相结合的网络舆论机制。[13] 五是培育大众网民的“法治”理念,响应信仰危机,对一定的主观过失或故意行为追究相应的侵权责任;对歪曲事实、结群炒作网络舆论的,还应及时介入法律行业自律职能,祛除消极舆论意识形态生活化的趋势。[14] 虽然可能囿于在网络这一虚拟空间缺乏进行规制的有效抓手和经验方法,学界还没有以法治视角对网络意识形态问题进行系统性研究的成果,但是“法治”在网络意识形态安全维护中的重要性已经凸显。网络空间具有其自身的整体性和动态性,网络环境瞬息万变,继续采用以往“兵来将挡、水来土掩”的研究思路,已不符合新时代网络意识形态安全维护的迫切需要。如今,将研究重点从零散的立法修补层面向系统的模式设计层面转移,把握网络空间的发展规律,把握网络意识形态冲突的主要矛盾,进行层次化、系统性研究是法治理论思路革新的关键。

从网络技术领域对法治路径的层次化要求中我们可以得出结论,网络领域的法治路径需要顺应网络技术的发展规律。在网络安全领域,为了网络安全而构建的网络安全模型,国际上有两个发展阶段,第二阶段就是以 P2DR 为代表的动态安全循环模型,即 Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)模型。[15] 其在网络安全领域运用广泛,可以转换为多种有效模

型来应对网络安全问题,如有学者提出利用蜜罐技术改进 P2DR 模型,并实现其在公安网络上的应用;[16]通过构建策略部署、引入策略自适应管理、添加统一管理控制台的方式来改进模型,[17]并针对我国当前企业园区网络发展与应用过程中面临的网络安全问题,提出基于 P2DR 模型设计方案可以极大地缓解新技术应用与企业隐私权限的矛盾,[18]以及运用网络安全模型为我国未来的校园网络安全技术的研究与应用构画蓝图和设想。[19]在网络技术领域,P2DR 模型早已成为一种应用灵活的成熟模型,虽然其在社会科学领域的应用尚待挖掘,但从以上研究网络法治建设的观点梳理中已经可见"防护、检测、响应"在网络法治建设中的重要性,两者不谋而合,亦是遵循网络空间规律的殊途同归。因此,围绕网络基本法,对法律规制进行"防护、检测、响应"的层次化立法设计和制度设计契合了国际上以 P2DR 为代表的动态网络安全循环模型的理论思路。

2. 实践层面:以具体化务实性立法为填充

在我国的法治征程中,全面依法治国与加强网络意识形态工作相辅相成。法治不仅是社会主义核心价值观的内容之一,也是坚持和发展中国特色社会主义的重要落脚点。在全面推进依法治国基本方略的指引下,秉承中国特色社会主义法治精神,能够为网络意识形态的健康发展保驾护航。一方面,法律是定纷息争的理性工具,能够通过规范化的方式来解决网络意识形态领域的矛盾;另一方面,法律思维也是一种理性的思维引领工具,能够引领人们用更为理性的思维和态度净化信息时代纷繁复杂的思想言论,同各种错误的思想与社会思潮交锋,凝聚人们的共识,维护主流意识形态。

然而,网络意识形态的管控并非易事,若网络监管懈怠,将引发社会主义意识形态发声无力,然网络监管过严,又会引发民众对言论控制无据可依的不满。究竟言论自由与话语权管控的边界该如何掌握,程序如何规范,都是亟需法治解决的问题。但在当前该领域法治建设中,总体战略设计较为缺乏,面临着一系列的困境。在立法层面,科学健全的立法体系尚未形成,法律法规兼容性差、滞后性强;法律法规条款模糊,缺乏实践性和可操作性;网络立法程序的不完善影响了法律法规制定的科学性;立法价值失衡,重管理轻权利,责任体系与救济制度不完善。在执法层面,多头管理,职能混乱,各部门各自为政,跨区网络执法难以协调,交叉和缺位管理的现象严重。在司法层面,维护国家意识形态安全行为界定的定罪量刑不甚清晰,维护国家意识形态安全案件查处中司法与执法之衔接不甚完善,以及司法运行机制在网络运行体系中的缺位,也使得维护网络意识形态安全的实效难以彰显。在守法层面,互联网行业自律性差,网络主体守法意识、安全意识淡薄,不利于推进网络意识形态领域的法治建设。

近年来,我国维护网络意识形态安全的法治建设取得了初步成效,管理领导体制中法治的核心作用凸现,执法行动成效初现,国内规范性提升,国际认同度增强。2014 年 2 月 27 日,中央网络安全和信息化领导小组成立,着眼研究制定网络安全和信息化发展战略、宏观规划和重大政策,致力推动国家网络安全和信

息化法治建设。党的十九大提出的网络强国、法治强国的战略方针和《网络安全法》的实践,为构建维护网络意识形态安全的法律制度提供了总纲性的保障。

2017 年 6 月生效的《网络安全法》第六条指出,“国家倡导诚实守信、健康文明的网络行为,推动传播社会主义核心价值观,采取措施提高全社会的网络安全意识和水平,形成全社会共同参与促进网络安全的良好环境”。可见,作为网络安全领域的基本法,《网络安全法》已提出了网络意识形态安全法治建设的立法旨归,但尚限于概念的提出缺乏具体制度,维护网络意识形态安全的目标难以有效落地,面对意识形态领域对法治路径的务实性要求,法治路径的设计与革新任务日益紧迫。这并不意味着将《网络安全法》打造为一部事无巨细的行为指南,《网络安全法》作为网络安全领域的宪法性法律,其价值在于为网络安全提供了统领性立法思路和基础性制度框架,从《网络安全法》的框架入手,寻觅适宜的思路方法来梳理、细化、衔接《网络安全法》在维护网络意识形态安全方面的相应细则规范与理论保障,是将网络意识形态保护落实到法治实践革新的关键。

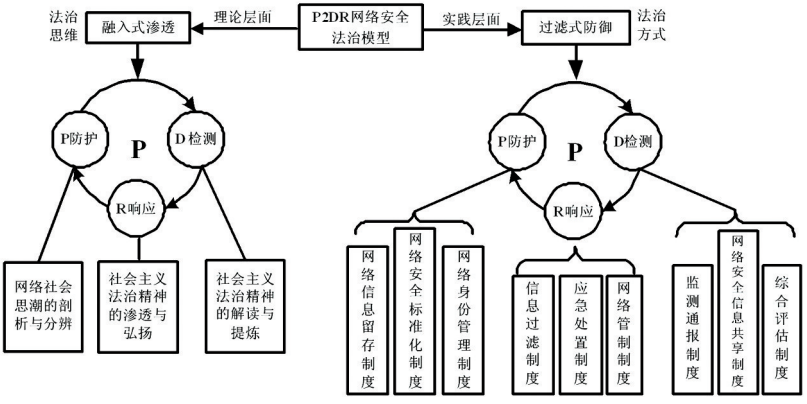
3. 理论与实践之结合:P2DR 网络安全法治模型应需而生

由上述分析可知,在网络意识形态安全领域进行法治路径革新具有充分的可行性和迫切的必要性,综合把握法治理论思路革新与法治实践路径革新的关键点,即是维护网络意识形态安全法治建设的突破点,由此,P2DR 网络安全法治模型的设计应需而生。通过引入网络安全学领域成熟的 P2DR 动态循环模型,通过防护、检测、响应三个环节的设计来维护网络意识形态安全,以网络技术手段对弈网络战场,避免坐而论道。在 P2DR 法治模型的宏观思路下,逐步落实网络安全策略,与《网络安全法》的制度构建相衔接,将网络技术手段固化为现实社会规范,以法治路径调适网络意识形态安全的监管,实现社会主义网络意识形态的融入和推进。

二、P2DR 网络安全法治模型的构想及制度设计

为了网络安全而构建的理论框架就是网络安全模型,20 世纪 90 年代末,随着完整闭环、动态循环的 P2DR 模型在网络安全学领域的提出,标志着静态安全模型向动态安全模型的转变,自此国际上的网络安全标准初步建立。作为网络安全学领域成熟的理论,P2DR 模型在计算机科学与技术等领域获得了广泛运用,但在社会科学领域的应用尚未充分挖掘。本文沿其核心思路,提出 P2DR 网络安全法治模型的构建(见图 1)。P2DR 模型在网络安全学领域的证成,首先为此法治模型的科学性奠定了基础。其次,同在网络安全的研究场域下,也避免了水土不服的后顾之忧。通过防护(Protection)、检测(Detection)、响应(Response)三环节的设计使网络平台实现良性循环运转,与社会主义法治精神的弘扬相契合,与《网络安全法》中具体制度的运转相衔接,且形成动态、开放的发展态势,保障其时效性,以期有效驾驭意识形态领域的复杂局面,在法治视野中构建起网络空间的规则秩序。

图 1　P2DR 网络安全法治模型示意图



(一)P2DR 网络安全法治模型在理论层面的构建与调适

意识形态是一种社会意识形式,法治本身就是意识形态的一个部分,因此法治精神、理念、意识、思潮本身就属于网络平台中传播的重要客体之一。在理论层面实现安全策略,是通过 P2DR 网络安全法治模型从“防护、检测、响应”三个环节实现“防御、甄别、引导”三个功能的法治理论体系。

1. 防护环节(P):对网络社会思潮的剖析与分辨

该环节需要对中西方法治思想进行辨析,去伪存真。对新自由主义、网络民粹主义、民主社会主义、宪政民主论、消费主义等充斥网络的社会思潮进行剖析,卸其伪装,明其实质,晓其目的,构筑起对网络错误思潮、阴谋思潮的防御体系。

2. 检测环节(D):对社会主义法治精神的解读与提炼

要将马克思主义理论融入到法治精神的提炼与建设中,针对网络社会从不同角度提出的具有代表性的观点,运用马克思主义科学的世界观、价值观、方法论来完成对网络文化资源的甄别检测。分别从对社会发展规律、社会主义建设规律、共产党执政规律的深入认识中;从社会主义发展的历史与现实以及国家治理体系和治理能力现代化实践中;从国外法治文明建设的有益成果、经验中;从马克思主义经典文本、中国传统文化资源中,提炼符合社会主义发展要求的法治精神内涵。

3. 响应环节(R):对社会主义法治精神核心内涵的渗透与弘扬

通过上一步的检测与提炼,寻求较为完整的社会主义法治精神的学理解读。将其核心理念融入到网络意识形态安全维护的理论构建中,将其思想内涵渗透到网络主体大众的意识形态中,“对话”具有意识形态指向性的社会思潮,与社会现实同频共振,实现引领与弘扬。

(二)P2DR 网络安全法治模型在实践层面的构建与规制

意识形态的防护工作落实到法治实践,最终需要通过具体的制度设计来实现,P2DR 网络安全法治模型从“防护、检测、响应”三个环节实现“防御、控制、惩

戒”三个功能的法治运转体系。[20]

1. 防护环节(P):以“循序渐进”为重点完善信息“入口”制度

“入口”制度的设计包含网络安全标准化制度、网络信息留存制度、网络身份管理制度。《网络安全法》第十五条概括了网络安全标准化制度,[21]在技术层面为后续网络威胁信息的检测提供了标准化依据,从源头规范网络环境。第二十一条明确了网络信息留存制度,要求网络运营者对网络运行状态、网络安全事件等进行监测并记录,以备查验。时间上,明确了六个月的留存期限,地域上,明确了境内储存的要求,增强了制度的可操作性。第二十四条诠释了网络身份管理制度,实际上是网络实名制的扩大和创新。第一,追求更加全面的网络实名制,涵盖网络接入、电话入网、域名注册、信息发布,实行全方位的实名验证;第二,不仅要求电子身份和现实身份之间的关联性,还推动电子身份的互认,建立电子身份之间的关联性,形成严密的网络身份体系。完善网络身份管理制度,是从信息发布者和传播者的层面对网络安全隐患进行预防,完善了网络使用者的信息链条,减少了因为网络隐秘性带来的网络安全风险,使网络使用者的行为在现实社会可被审查、可被监督、可被追究。这些制度并不直接干预网络意识形态威胁信息的传播,但是其在 P2DR 网络安全法治模型中发挥着基础性的不可替代的作用,构建起了防护阶段网络意识形态平台有据可依、寻查有迹、追责有人的法治防御体系。

防护制度体系的构建有利于强化网络参与者的义务意识、责任意识,以及正确行使权利的意识。然而,全面信息防护网的建立,促使网络话语必留痕迹、网络行为无处隐匿,责任承担的危机感打破网络社会“畅所欲言”的和谐,一定程度上为制度的推行带来重重阻力。当前阶段,防护制度的构建必须以“循序渐进”为重点,把握合理尺度,层次化、阶段性地进行推广。相应提出如下建议:

在网络安全标准化制度完善过程中,实现推荐性标准向强制性标准的平缓过渡。现阶段,在我国已出台的国家网络安全标准中,大多为推荐性国家标准,根据《网络安全法》的要求及网络安全工作的需求,强制性国家安全标准的数量增长成为必然。[22]在推荐性标准向强制性标准的转化过程中,应以审慎性为原则,谨慎考查强制性标准的必要性,避免强制性标准脱离网络安全实际需要,造成网络运营者权利的限缩;同时,应确保为网络运营者留有充分的过渡调整期限,确有及时调整必要的,由全国信息安全标准化技术委员会分批次指导进行。

在网络信息留存制度完善过程中,随着制度的稳进推行,可进一步考虑扩大网络信息六个月的留存期限,考虑其与法律诉讼时效的期限之间的关系,进一步满足法律诉讼过程中通过网络手段调查取证的需求。

在网络身份管理制度完善过程中,网络实名制可首先在一些大型的、正规的门户网站或商务网站率先强制实行、严格实行,对一些规模较小、开放性的论坛网站则可暂时宽松管理、逐步推进,缓冲以言论自由为旗号的消极势力对防护制度产生的冲击。再者,《网络安全法》第二十四条提到“用户不提供真实身份信

息的,网络运营者不得为其提供相关服务”,但对于已开通网络服务的在网客户,未及时进行身份验证的,应首先明确网络运营者的通知义务,其须告知网络消费者可能面临的停网风险,网络消费者仍未在固定期限内完成身份认证的,可附条件给予一定的宽限期,最大限度地保障网络消费者的权益与网络服务的安全稳定。

2. 检测环节(D):以“隐私保护”为重点健全信息“通过”制度

“通过”制度的设计包含监测通报制度、网络安全信息共享制度、综合评估制度。在网络空间,对信息传播及内容的控制关系到社会安全和国家安全,一些虚假捏造的恶意言论严重干扰到网络秩序,其负面影响延伸至现实社会,对扰乱社会秩序埋下隐患;一些“西化”“分化”思潮的涌入,对当今社会的主流思想甚至是意识形态造成冲击,对国家安全造成严重威胁。因此,网络意识形态安全检测环节的关键在于维护互联网信息的传播及内容的可控性,然而,网络信息传播速度快,受众面广,且具有可存储和再传播的特点,使得其可控难度加大。通过构建网络意识形态安全秩序的第二层保护屏障,以及时发现有悖于良性对话原则的网络信息,集合问题信息,缩小关注范围。

《网络安全法》第五十一条、五十二条体现了监测通报制度,要求有组织地对网络安全状态进行监测、对网络安全信息进行收集、分析、通报和预警,便于及时检测信息安全的实时动态和存在风险,及时调整和制定对策加以控制,为信息检测行为提供了合法依据。此外,《网络安全法》在“关键信息基础设施的运行安全”专节中规定了“促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享”,第二十九条规定“国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作,提高网络运营者的安全保障能力”,触及了“网络安全信息共享制度”的宏观概念,体现出以关键信息基础设施体系内的共享为主,以网络运营者之间的共享为辅的整体思路,但尚未进行具体的立法衔接和制度设计。

综合看待检测体系下的现有相关制度,都主要是从约束“被检测方”的视角来进行制度设计。一定程度上,检测环节是公权力基于国家安全对私人主体信息进行的窥探和排查,在安全监测过程中,个人网络信息的保密性受到威胁。不可否认,约束“被检测方”影响着检测阶段审查能否取得实质性的成果,但是也不可忽略对“检测方”的法律规范。因此,透明、审慎当为该制度规范的重要原则,使检测环节有依据、有程序、有限制,防止“检测”初衷的扩大和异化,须把握好审查的范围和尺度,对网络安全的检测环节进行更加理性、规范地保障。[23]具体来看,《网络安全法》在监测通报制度中,重点规范了网络运营者的操作规则,[24]但对公权力机关、其他个体的审慎义务仅以原则性条款进行了明确,[25]有必要进行细化,实现依据合法、程序正当、救济充分的闭环制度设计。在网络安全共享信息制度的进一步规划中,网络安全信息共享的范围决定了信息收集触角的延伸范围,必须紧密围绕“网络意识形态安全威胁”这个指标展开。[26]建

议在专业意见和调查评估的基础上严格框定共享信息的范围,采用列举式方法界定,限制共享信息范围的开放度。

除以上对现有立法框架内的专门制度进行完善和细化之外,设立综合评估制度以实现模型系统内的动态平衡和自我修复也是模型持续发展的必然要求。评估内容主要包括两个方面,即对隐私保护情况的评估和对言论威胁程度的评估。第一,通过对隐私保护情况的评估保障法之透明,建议由国家网信部门统筹对网络信息安全检测过程中公民隐私等权利自由受影响的程度、隐私保护政策和程序的实施效果等进行评估和监督;第二,通过对言论威胁程度的评估保障法之自由,通过听证会、讨论会等形式,逐渐明晰威胁网络意识形态安全的言论与自由言论之间的界限,从而审慎界定网络意识形态安全威胁信息的范围,充分保障公民的话语自由。

3. 响应环节(R):以"责任落实"为重点推进信息"治理"制度

"治理"制度的设计包含信息过滤制度、应急处理制度、网络管制制度。防护环节抵御网络意识形态安全威胁因素的进入,检测环节控制网络意识形态不安全信息的通过,其目的一方面是预防问题、控制问题,另一方面也是发现问题、聚焦问题,从而进行有针对性的具体响应。日常情况下的响应措施主要体现为信息过滤、责任落实,紧急情况下则包括应急处理、网络管制。通过落实"治理"制度,及时应对处理具有意识形态威胁性的网络信息,恢复网络平台的"最大安全"和"最低风险"状态。

信息过滤制度首先体现于《网络安全法》第四十七条、第四十八条,对于危害国家意识形态安全的相关信息,网络运营者、电子信息发送服务提供者、应用软件下载服务提供者有义务采用停止、消除、报告等措施进行主动控制,《网络安全法》第五十条规定网信部门等监管部门也有二次过滤的监督义务,从而避免危险信息进一步的传播和扩散。然而,第五十条对有权限喊停网络信息传输的主体仅进行了半开放式的规定,即"国家网信部门和有关部门",须进一步界定"有关部门"的范围以及喊停的程序。此外,《网络安全法》条文中有 12 处涉及应急处理制度,[27]明确了网络运营者、关键信息基础设施的运营者、国家网信部门、负责关键信息基础设施安全保护工作的部门等各方主体的制定应急预案及定期演练的义务。安全事件真实发生时,通过启动紧急预案、调查评估、采取措施、发布警示信息等措施加以应对。《网络安全法》第五十八条还明确了网络管制制度,在突发紧急情况下,为维护国家安全和社会稳定,可依法谨慎采用网络管制制度,经国务院决定或者批准,在特定范围内限制网络通信,这是网络安全最后也是最彻底的一道防线,但在一定程度上,这也对网络安全所要求的可用性产生了攻击,影响到网络使用者对网络信息进行访问、浏览、存取等正常需求,是特殊情况下秩序对自由的压制。[28]但是从长远来看,只有建立起良好有序的网络秩序,有效抵制网络安全风险,保持网络环境的持续稳定,才能长久地保障网络安全的可用性。尽管如此,对自由的约束仍应更为审慎,自由是相对的,对

自由的约束也理应是相对的,网络管制制度仅设定“经国务院决定或者批准”这一个限定条件尚显单薄,须进一步细化提请机构、实施机构、监督机构以及临时措施种类、限制范围、限制期限等要件。

除了相关制度的细化和完善外,责任落实是响应环节的关键,在《网络安全法》的“法律责任”专章中,对具体责任的承担方式有较为细致的规定,但尚有两个方面模糊不清。一方面,对不同主体之间的责任界分尚不清晰,“《网络安全法》中使用了‘网络产品和服务提供者’‘关键信息基础设施运营者’‘网络运营者’等多个概念,却缺乏对这些网络活动主体概念明确而规范的界定”,[29]以致在责任的设定上踌躇无据。《网络安全法》作为国家实施网络空间管辖的第一部基本法律,构建起网络安全领域新的制度框架,体现出新的立法趋势,对网络领域各法律主体的义务、责任提出了新的要求。因此,有必要以系统性、发展性的眼光重新统筹相关立法文件中关键主体的责任问题表述,从而减少实践争议,统一责任体系。例如,通过考虑《网络安全法》影响下网络服务提供者的义务与责任,调整《侵权责任法》中具体条文之表述,从而统一立法思路、凝聚立法旨归、实现立法意图。另一方面,对不同等级责任的划分界限尚不清晰,较多呈现出“尚不构成犯罪的”“情节较重的”之类的模糊表达,有必要对威胁意识形态安全的责任等级界限进行明晰,明确民事责任、行政责任、刑事责任之间界分的标准,协调抽象意识与具体责任之间的关系,完善责任追究的制度与程序。对此,建议参考如下思路(见表1),完善威胁网络意识形态安全的法律责任阶梯。

表1

责任类型 / 行为类型	民事责任	较轻的行政责任（警告、责令改正、小额罚款）	较重的行政责任（其他行政责任）	刑事责任
过失	违反法律法规，给其他民事主体造成损害的。	✓	拒不改正或造成严重后果。	拒不改正且造成严重后果，考虑追究刑事责任。
重大过失		\	✓	造成严重后果，考虑追究刑事责任。
故意		\	✓	未造成严重后果，根据行为危险性考虑追究刑事责任；造成严重后果，追究刑事责任。

其他行政责任主要包括:责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照、计入信用档案、从业禁止等。

三、结　语

P2DR 网络安全法治模型的提出,将网络安全领域的奠基式理论在法治领域加以创新。理论层面,法治思维的 P2DR 模型构建促进网络意识形态融入式渗透,完善社会主义意识形态的科学内涵,提升网络时代主流意识形态的对话实力;实践层面,法治方式的 P2DR 模型构建促进网络意识形态过滤式防御,在意识形态对话的渗透与防御中维护网络意识形态安全,形成科学的事前防御、事中控制、事后惩戒的法治体系,切实保障了意识形态问题在网络领域进行法律规制的可行性实效。本文围绕模型设计的具体制度在《网络安全法》立法思想中均有迹可循,是针对维护意识形态安全的细化性研究,期冀能为立法机关提供关于网络安全法等相关法律法规立法完善的建议,为执法机关提供执法依据,为全面落实依法治国以及网络强国战略的实施贡献绵薄之力。

正如《网络安全法》通过之时,"推动传播社会主义核心价值观"这一法律条文曾备受争议一样,对于网络意识形态安全的维护,学界也同样顾虑其立法的法理基础缺失、实践操作困难。但对于网络空间这个与社会现实同频共振的社会,其规则之治应该与现实社会的要求一致,方法上更需要摸索创新。将法治模式和法学方法在意识形态领域予以运用,挖掘探讨新时期维护我国意识形态安全的新路径,分层设计规制,将维护网络意识形态安全从思想领域的教化之治拓展到行为领域的规则之治,为切实保障意识形态问题在网络领域进行规制的实效做出了探索。

注释:

〔1〕Moyer Michael,"Internet Ideology War.", *Scientific American*, Vol. 302, No. 4, 2010.

〔2〕Paul Duguid,"Open Standards and the Internet Age: History, Ideology, and Networks by Andrew L. Russell (review)." *Business History Review*, Vol. 89, No. 2, 2015.

〔3〕李栗燕、高清军:《试论新时期我国意识形态对话平台建设》,《毛泽东邓小平理论研究》2012 年第 8 期。

〔4〕侯惠勤:《意识形态的历史转型及其当代挑战》,《马克思主义研究》2013 年第 12 期。

〔5〕〔美〕T. L. 萨迪:《网络层次分析法原理及其应用:基于利益、机会、成本及风险的决策方法》,鞠彦兵、刘建昌译,北京:北京理工大学出版社,2015 年,第 299 – 306 页。

〔6〕夏冰:《网络安全法和网络安全等级保护 2.0》,北京:电子工业出版社,2017 年,第 107 – 151 页。

〔7〕马民虎:《网络安全法适用指南》,北京:中国民主法制出版社,2018 年,第 21 – 23 页。

〔8〕王永贵、张晓丽:《推动马克思主义大众化的对策思考——以网络时代为背景》,《人民论坛》2011 年第 32 期。

〔9〕钟明华、洪志雄:《维护我国意识形态安全的路径思考》,《思想理论教育》2016 年第 1 期。

〔10〕聂筱谕:《西方的控制操纵与中国的突围破局——基于全媒体时代意识形态话语权争夺的审视》,《世界经济与政治论坛》2014 年第 3 期。

〔11〕徐世甫:《网络管理法治化的问题域》,《上海大学学报(社会科学版)》2006 年第 4 期。

〔12〕秦前红、李少文:《网络公共空间治理的法治原理》,《现代法学》2014 年第 6 期。

〔13〕胡长生、黄勇:《论网络文化的旨趣及其治理》,《江西教育学院学报(社会科学版)》2010 年第 5 期。

〔14〕陈堂发:《当前网络意识形态四大特征与四大规制措施》,《唯实》2016 年第 4 期。

〔15〕P2DR 安全模型给网络安全下了一个全新定义:“及时的检测和响应就是安全”,“及时的检测和恢复就是安全”。在整体安全策略的控制和指导下,在综合运用防护工具(如防火墙、操作系统身份认证、加密等)的同时,利用检测工具(如漏洞评估、入侵检测等)了解和评估系统的安全状态,通过适当、及时的响应将系统调整到“最安全”和“风险最低”的状态,防护、检测、响应组成了一个完整的、动态的安全循环,保证信息系统的安全。

〔16〕太史雁峰、万定生、陈军冰:《利用蜜罐技术改进 P^2DR 模型及在公安网络上的应用研究》,《福建警察学院学报》2006 年第 2 期。

〔17〕韩锐生、徐开勇、赵彬:《P2DR 模型中策略部署模型的研究与设计》,《计算机工程》2008 年第 20 期。

〔18〕徐均、周泓宇、徐婧、杨灵运:《P2DR 网络安全模型在企业园区网中的研究与应用》,《中国新技术新产品》2013 年第 16 期。

〔19〕袁文光:《职业院校的网络安全风险分析》,《电子技术与软件工程》2014 年第 14 期。

〔20〕本模型中涉及的多数制度在《网络安全法》中均有迹可循,有的只触及了宏观概念,有的仅限于对网络系统安全整体的监管。此外,综合评估制度在我国《网络安全法》中并未有直接的体现,笔者受 2015 年美国《网络安全信息共享法案》中的隐私保护评估机制启发,参考适用。

〔21〕《网络安全法》第十五条规定:“国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责,组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。”

〔22〕例如《网络安全法》第十条、第二十二条、第二十三条对建设、运营网络以及通过网络提供产品和服务的行为提出了遵循强制性标准的要求。

〔23〕赵丽莉:《基于过程控制理念的网络安全法律治理研究——以“风险预防与控制”为核心》,《情报杂志》2015 年第 8 期。

〔24〕《网络安全法》第四十一条规定,网络运营者收集信息时须明示信息主体,信息的收集、使用及其范围、方式都必须得到信息主体的允许。

〔25〕《网络安全法》第三十条规定:“网信部门和有关部门在履行网络安全保护职责中获取的信息,只能用于维护网络安全的需要,不得用于其他用途。”第四十四条规定:“任何个人和组织不得窃取或者以其他非法方式获取个人信息,不得非法出售或者非法向他人提供个人信息。”

〔26〕方婷、李欲晓:《安全与隐私:美国网络安全信息共享的立法博弈分析》,《西安交通大学学报(社会科学版)》2016 年第 1 期。

〔27〕《网络安全法》条文中“应急”字样出现 12 处,主要涉及的法条有:第二十五条明确了网络运营者制定网络安全事件应急预案的义务;第三十四条明确了关键信息基础设施的运营者制定网络安全事件应急预案的义务;第五十三条明确了国家网信部门协调有关部门健全应急工作机制,制定网络安全事件应急预案的义务。

〔28〕《网络安全法》第七十六条第二款规定:“网络安全,是指通过采取必要措施,防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力。”

〔29〕敖力嘉:《信息网络安全管理义务的刑法教义学展开》,《东方法学》2017 年第 5 期。

〔责任编辑:刘　鎏〕