

网络安全行政处罚的归责原则

尹培培*

内容摘要:基于网络平台表达机制的特殊性,《网络安全法》以“发现违法信息”为前提课予运营者以网络安全监管处置义务,确立了主观归责原则,要求网络安全行政处罚以运营者具有“主观过错”为前提。实践中,由于惯常的专项治理逻辑以及对《网络安全法》所承载的积极促进目的的忽视等因素,行政机关在对运营商是否违反网络安全保护义务的界定过程中,并未将法定的主观要素考虑在内,导致了处罚行为的随意性,对于未来秩序之可控性的过度追求也弱化了法治的约束。基于网络安全保护之实效性 with 网络法治秩序之平衡,应当通过“区分信息种类和内容”建构主客观相结合的归责路径。

关键词:网络安全法 行政处罚 主观归责 归责路径

一、问题与研究进路

信息技术给社会结构带来了最深刻的变革,“因为不断伸张和密织的互联网,确实在相当大的程度上瓦解了由电话公司、出版社、报刊编辑部等建构起来的人工秩序,实现了哈耶克所设想的那种分散而自律的构想。可以说,无论对不对、好不好,某种无组织、无目的、无计划的‘自生秩序’已经出现在电脑世界,并且开始占优势”。^[1]此种变革也为法治提出了新的任务。正是在“网络技术迅猛发展,网络问题日益凸显,网络安全已成为关系国家安全和发展的重大关系,关系人民群众切身利益的重大问题”^[2]这一背景之下,《网络安全法》应运而生。

《网络安全法》为网络运营者设定了网络安全保护义务。通过对条文的解读可以发现,该法以“发现违法信息”为前提课予网络运营商及其直接责任人以具体处置义务,从规范层面排除了运营商对于“未被发现”以及“未能被发现”的违法信息所应承担的法律后果,将主观要素纳入到网络安全行政处罚的责任要件。那么,该规定在实际运行中的状况如何呢?因为《网络安全法》刚刚颁布不久,这一

* 南京师范大学法学院讲师,法学博士,中国法治现代化研究院研究员,江苏区域法治发展协同创新中心副研究员。

本文系国家社科基金青年项目“网络空间治理的行政处罚问题研究”(项目批准号:18CFX054)、江苏省哲学社会科学基金项目“网约车的法律规制研究”(项目批准号:17FXC002)的阶段性研究成果。

[1] 季卫东:《大变局下的中国法治》,北京大学出版社2013年版,第115页。

[2] 参见《《中华人民共和国网络安全法》(草案)的说明》。

问题尚未引起学界的充分关注,已有的研究大多基于纯粹的理论层面,对我国应当在行政处罚领域确立主观归责原则进行浅尝辄止的探讨和呼吁,^[3]而忽视了这一制度本身的实效性。对于实践层面运行状况的关注不足或许无助于对主观归责原则确立和运行机理的理解,进而不可避免地对其在今后各个领域的适用产生影响。

笔者以《网络安全法》生效后的部分行政执法事例为研究对象,试图从规范和事实两个层面,对网络行政处罚主观归责原则的实际应用状况作一个考察,进而尝试在我国行政管理机构独特的执法逻辑以及风险社会的语境之下,对其中存在的问题进行解释。规范层面,本文通过对《网络安全法》相关责任条款及关联规定的分析,尝试归纳出立法机关将主观要素纳入网络安全行政处罚的制度机理,进而探究其在现有行政执法体制下的效力问题。事实层面,笔者将以“腾讯、新浪微博等违反网络安全法被重罚”事件以及“58同城、赶集网等因违法违规发布‘大棚房’租售信息被约谈”等事件为分析对象,试图从执法机构的处罚行为及处罚措施中探究网络安全行政处罚主观归责原则在具体行政执法事例中的适用状况。笔者尝试将问题置于我国行政执法系统“政策实施型”行为逻辑的背景下,在当前风险社会这一语境中,对《网络安全法》中的责任条款进行剖析,在规范分析的基础上,明确其适用要件,并尝试对其背后的法理依据加以梳理,同时对网络安全主观归责原则在实践运作中存在的问题进行剖析和解释,以此折射出网络安全处罚的内在逻辑,揭示其运行原理,并尝试提出可能的解决路径。

二、网络安全行政处罚主观归责之学理梳理与规范解读

通过对《网络安全法》中涉及网络运营者责任的条款分析后发现,广义上的网络安全保护义务可以细分为防范义务^[4]、发现后的处置义务^[5]以及配合义务。^[6]狭义上,即通常意义上的网络安全保护义务仅指网络运营者“发现后的处置义务”。笔者采狭义上的“网络安全保护义务说”。《网络安全法》第47条规定:“网络运营者应当加强对其用户发布的信息的管理,发现法律、行政法规禁止发布或者传输的信息的,应当立即停止传输该信息,采取删除等处置措施,防止信息扩散,保存有关记录,并向有关主管部门报告。”该条课予了网络运营者加强对网络环境管理的义务,具体表现为发现违法信息后应当立即采取的系列处置行为。同时,为确保其实效性,该法亦明确了网络运营者违反法定义务的法律后果。第68条规定:“网络运营者违反本法第47条规定,对法律、行政法规禁止发布或者传输的信息未停止传输、采取删除等处置措施、保存有关记录的,由有关主管部门责令改正,给予警告,没收违法所得;拒不改正或者情节严重的,处十万元以上五十万元以下罚款,并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照,对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

根据《网络安全法》第47条的规定,网络运营商负有“发现违法信息”后的具体处置义务。第68条规定,违反该义务的,由有关部门责令改正的同时处以警告、没收违法所得等行政处罚。对这一规定进行文义解释便可得知,网络运营者负有该义务的前提条件是必须已经发现了违法信息。因此,“发现违法信息”可以作为其履行法定义务的必要条件推导出来。对这一规定进行反向解释,也就意味着《网络安全法》从规范层面排除了运营商对于客观上“未被发现”以及“未能被发现”的违法信息所应承担的法律后果,将主观要素纳入到网络安全行政处罚的责任要件,在对违反网络安全保护义

[3]从理论层面对行政处罚归责原则所作的研究,可参见彭爽:《论行政处罚的归责原则》,《中南林业科技大学学报(社会科学版)》2010年第5期,第58—60页;刘席宏:《行政处罚主观归责研究》,《黑龙江省政法管理干部学院学报》2015年第1期,第28—31页。

[4]《网络安全法》第21、25、59条。

[5]《网络安全法》第47、68条。

[6]《网络安全法》第69条。

务的处罚上采主观归责原则。该条责任规定所采取的不完全罗列构成要件的准用性规范方式,在适用上需要结合其他相关法规范以及具体状况进行解释,由此留下了从规范以及法理层面对其归责原则进行探讨的空间。

(一)主观归责原则

主观归责原则关注的重心在于行政相对人实施违法行为时所具有的主观心理状态,即刑法学上的“罪过”。此种“罪过”意味着“任何犯罪行为都是基于一定的罪过心理实施的;罪过在犯罪中的重要性表现为:没有罪过的行为,不是犯罪行为;除严格责任犯罪之外,不能够证明罪过的存在,也就不能证明犯罪的存在。”^{〔7〕}已有的行政法基础理论,无论是传统的亦或是现代的,对于行政处罚的主观要件究竟应当如何确定和安放,都不曾有过较为深入的论证。然而,这一问题在行政法实务当中往往事关“罚”与“不罚”,因此,对其研究具有理论和实践层面的双重意义。^{〔8〕}

行政处罚的归责原则,是行政法的一个基础理论问题,它决定着行政处罚责任的构成与配置,对于整个归责体系的建构起着基础性的指导和统帅作用。与归责原则直接相关的一个概念是责任要件。责任要件的具备与否直接取决于一国有关行政处罚的法律规定中所确立的归责原则。所谓责任要件,主要系指行为人的主观犯意,即行为人能对其行为有一定之意思决定,因此,若其决定从事违反行政法上义务之行为,即得对其非难,要求其承担责任,此种责任要件主要有两种,即故意与过失。^{〔9〕}以法律后果的承担是否需要具备主观上的故意或过失这一责任要件为标准,可以区分主观归责原则和客观归责原则。

具有总则性质的《行政处罚法》第3条规定:“公民、法人或者其他组织违反行政管理秩序的行为,应当给予行政处罚的,依照本法由法律、法规或者规章规定,并由行政机关依照本法规定的程序实施。”这意味着,行政处罚的基本功能在于维护社会正常发展所需要的“行政管理秩序”。而这一基本的功能定位体现在行政处罚的归责原则上即表现为,通常情况下,是否承担行政处罚法律责任并不要求相对人主观上存在故意或过失的心理状态。^{〔10〕}

比较法上,或许是基于行政处罚与刑罚皆为国家公权力对不法行为制裁的手段这一同源性之故,世界各国对于行政处罚责任要件的规定通常与刑罚并无二致,基本以主观上存在故意或过失作为行政处罚的“入罪”要件。比如,德国《违反秩序罚法》第10条规定:“只有故意行为方可作为违反秩序行为处罚,但是法律明确规定对过失行为应当处以罚款的情形除外。”据此,德国在行政罚领域确立了主观归责原则,以处罚故意行为为原则,过失行为为例外,且对于过失行为仅能给予罚款处罚,排除了罚款以外的处罚种类。即,只有故意行为和法定的过失行为具有可罚性。而对于究竟何种情形构成“故意”,德国《违反秩序罚法》尽管没有直接对其含义进行界定,但通过体系解释和反向解释的方法可以从相关条文中获得。该法第11条第1款规定:“实施行为时未意识到一种情形属于法定事实构成,不是故意行为。过失行为的可处罚性不受影响。”由该条文可推出,所谓故意行为,是指实施行为时明知该情形属于法定事实构成而继续为之的情形。因此,德国法上的故意以“行为时的明知”为判断标准。奥地利早在1925年颁布的《行政罚法》中就明确了主观归责原则,^{〔11〕}此后,“无过错即无责任原则与法无明文规定不处罚、禁止溯及既往等基本理论一样,均成为行政处罚适用上确定不移的法律原则”。^{〔12〕}

〔7〕刘生荣:《犯罪构成要件原理》,法律出版社1997年版,第187页。

〔8〕崔建远:《合同责任研究》,吉林大学出版社1992年版,第50页。

〔9〕翁岳生:《行政法(上册)》,中国法制出版社2009年版,第847页。

〔10〕关于行政处罚的归责原则,学界并未形成通说。尽管多数学者认为《行政处罚法》确立了以客观归责为主的归责原则,但该法第25、26条亦包含主观归责要素的考量。

〔11〕除了故意和过失外,奥地利《行政罚法》还确立了“推定过失”原则,但该原则的适用有着严格的法定要件,体现在《行政罚法》第5条第1项:“于行政法规无关于责任条件之特别规定时,过失行为已足为处罚之理由,仅系违反禁止命令或作为命令之行为,而无须以引起损害或危险作为违反行政义务行为之构成要件者,如行为人不能证明其无法避免行政法规之违反,应认为有过失。”章剑生:《现代行政法基本理论(上卷)》,法律出版社2015年版,第364页。

〔12〕城仲模:《行政法之基础理论》,台湾三民书局1994年版,第197页。

因此,在行政处罚领域确立主观归责原则,即以行政相对人是否存在主观过错作为行政违法的责任要件,是符合现代行政处罚理论的发展趋势的。此外,将行政相对人主观过错纳入到责任要件当中亦为行政相对人提供了接受处罚的心理基础,由此可以提升行政相对人对行政处罚的可接受程度,否则,行政处罚便难以产生预期的法律效果。与此同时,对于主观要素的充分考量可以收缩行政机关在认定行政相对人行政违法行为构成上的自由裁量权。如果在行政法理上不强调行政违法行为构成的主观要件,可能会导致行政机关根据“需要”认定违法行为。^[13]

(二)网络安全主观归责原则之确立机理:基于处罚目的与互联网之特性

任何制度的产生都有其特定的机理,主观归责原则的确立也不例外。网络安全领域主观规则原则的确立亦是基于《网络安全法》的处罚目的以及互联网相对于传统规制领域的特殊性而生成的。

1.处罚目的解读

行政处罚与刑罚同为国家对于不法行为的制裁手段,两者对于违法行为的制裁仅存有量的不同,并无质的差异。^[14]因此,于制裁目的而言,两者的差异本身并不能阻断刑事制裁原理在行政处罚领域的参考适用。在刑事领域,制裁处罚之目的功能有如下三种:^[15]

(1)衡平(对等)正义:报应理论(因果报应法则,以牙还牙),属于绝对刑罚理论。采取报复原则,要求罪责平衡,亦即罪责与处罚间的绝对平等。所处制裁处罚与其行为产生侵害他人或社会国家法益之程度,亦即所产生危害结果,应维持衡平,以符合“责罚相当性原则”。由此实现个别案件正义。

(2)分配正义:特别预防功能(改过自新功能),属于相对的刑罚理论。按照行为人之个人人格标准处罚,以再社会化,警告以及排除危险,所处罚款应能防止违规行为人嗣后再犯之可能性。由此实现个别案件正义及社会正义。

(3)法律正义:一般预防功能(以儆效尤功能)。按照社会需要的标准处罚,以使社会恢复原状,维持社会秩序不被破坏。包括积极的一般预防(以使社会稳定,防卫法律秩序);以及消极的一般预防(一般性的威吓)。

上述三种见解各有其合理性,但是每一种见解本身又都不足以全面证成制裁目的正当性。对于报应理论,正如费因伯格所认为的那样,所谓“刑罚,就是各种类型违法行为的价格标签”。^[16]由该理论所衍生出的制裁正当性在于,应当根据违法行为造成的危害来判定其应付出的代价。因此,“责罚相当性原则”自然应当得到如铁律般的遵守。而分配正义和法律正义理论所强调的预防功能其实是异曲同工的,两者均强调对于个案本身进行的制裁应当同时能够关注到社会层面所产生的后果,以此为基础强调惩罚所具有的预防功能。然而实际状况是,处罚本身就是对不法行为人所施加的不利影响,即便不刻意加以强调,此种因“限制、剥夺权利”对当事人本身乃至社会所产生恐吓作用也是不言而喻的,唯需注意的是惩罚程度的不同对于预防功能实效性发挥的影响。由此观之,在考量制裁的正当性问题时,既要充分遵循“责罚相适应”原则,亦应当考虑到处罚手段、程度的强弱对于个案当事人乃至社会的影响,从而尽可能地增强行政处罚预防功能的有效性。

《网络安全法》以“保障网络安全、维护网络空间主权和国家安全、社会公共利益”为立法目的。立法目的作为一部法律的灵魂指引着具体制度规则的建构,由此形成的规则最终服务于立法目的的落实。法律于互联网是“张力”性的存在。一方面,法律应当对网络空间所产生的负面效应进行规制,但另一方面,亦须通过此种规制促进互联网的有序发展。《网络安全法》所欲达成的目的主要在于“保障网络安全”和“维护网络空间主权和国家安全以及社会公共利益”。然而,对于法律目的的探寻而言,

[13]参见章剑生:《现代行政法基础理论》,法律出版社2015年版,第363页。

[14]关于此观点论证,可参见尹培培:《不予行政处罚论——基于〈行政处罚法〉第27条第2款规定之展开》,《政治与法律》2015年第11期。

[15][德]亚图考夫曼:《法律哲学》,刘幸义等译,法律出版社2011年版,第162页。

[16]Report of the Royal Commission on Capital Punishment, London, 1953, pp. 17—18.

除了目的条款本身之外,似应包括个别法条、个别制度的规范目的。^[17]通过《网络安全法》的第二章可以看到,其立法目的之一还在于“促进经济社会信息化健康发展”。因此,该法在消极保障之外,还担负有积极支持与促进网络发展这一目的。将主观过错纳入其中一方面有力维护了网络安全管理秩序,同时也避免了如同客观归责那般严厉的制裁可能会带来的阻断运营者积极性的后果,因而兼顾了《网络安全法》“消极维护”和“积极促进”的双重目的。

2. 互联网平台的特性

互联网平台相较于现实空间具有怎样的特殊性,进而使得在网络安全行政处罚领域确立主观归责这一原则成为必要?在四通八达的网络信息时代,传统组织架构中部门间的壁垒被打破,“以上传达为主要内容的中间管理层可以逐步被缩减乃至最终被取消,行政机构可以在一定程度上得到精简,因信息传递不及或错误所造成的内部消耗可以大大减少,行政流程进一步简化”,^[18]从而加速信息在横向和纵向上的流动效率以及提高信息传递的精准性。中间层级的弱化使得现代组织结构向中空化方向发展。此种根本性的变化一方面避免了传统组织架构之下经过层级传播导致信息失真的弊端;但另一方面,信息源与决策层之间的人为阻隔的消除也意味着在某种程度上充当缓冲功能的中间层级的失灵,从而直接削弱了管理层对于信息本身的控制能力。在某种程度上而言,网络运营者并不具备如同现实世界那样通过层级汇报制度来管控信息发布的能力。

因此,网络平台区别于现实组织的特殊性恰恰在于其责任人与行为人的严重分离。从表面来看,政府要规制的是网络平台,但平台本身只是一个媒介,其监管的重点实质上是平台背后数以亿计的网络用户,法律规定给运营商的监督义务实际上是在行政机关(网络监管部门)与运营商之间进行责任分配的结果。在互联网时代,由于行政执法部门身负监管压力,又受资源和预算的约束,比如跨地域取证困难,网络的匿名性等特征使得传统上基于管辖权划分的行政执法体系难以适应网络环境下的复杂状况,在此种情形下,监管部门自然希望扩张平台注意义务的范围,促使其帮助甚至替代自身去履行监督审查义务,从而减轻监管压力。^[19]

那么,对于此种行为人与责任人分离的状态,对运营者进行处罚是否欠缺妥当性呢?譬如,一些运营商为扩展信息的流动性和开放性,在页面中设置了可以直达其他平台的网页链接以方便网络使用者能够更加快捷地获取其所关注的内容,然而,该运营商本身对于这些“外部信息”的合法性是无从控制的。此种情形之下,倘若将此种链接按照“自身发布的信息”进行处罚,那么是否会造成运营商因惧怕处罚而使得一些虽然于网络发展大有益处但却存在违法风险的信息发布行为被遏制呢?如前文所述,《网络安全法》的主要目的之一就在于“保障网络安全”,结合《〈网络安全法〉(草案)的说明》可知,该法是在“网络技术迅猛发展,网络安全已成为关系国家安全和国家安全,关系人民群众切身利益的重大问题”这一背景之下应运而生的,其中“加强网络主权的维护以及对于个人信息的保护”等需求更是具有相当的迫切性。因此,出于此目的的实现,确有必要落实网络运营者责任,以提高法的威慑力和实效性。而面对行为人与责任人相分离的情形,该法以“发现违法信息”为前提课予网络运营者以具体处置义务,从规范层面排除了运营商对于“未被发现”以及“未能被发现”的违法信息所应承担之法律后果,将主观要素纳入到网络安全行政处罚的责任要件,已经在相当程度上消除了此种疑虑。

三、网络安全行政处罚主观归责的实践样态及其解释

《网络安全法》生效后,与之相关的执法实践迅速展开。很快,一则题为《腾讯新浪微博等违反〈网

[17]王泽鉴:《民法实例研习·基础理论》,中国政法大学出版社2003年版,第144页。

[18]邓集文:《网络与政治:二元互动发展》,《株洲工学院学报》2003年第1期。

[19]赵鹏:《网络平台行政法律责任边界何在》,《财经杂志》2016年4月20日。

络安全法》被重罚》的新闻标题就出现在了公众的视野。广东省、北京市网信办根据《网络安全法》第47条和第68条的规定,分别对腾讯公司、新浪微博作出“最高罚款”的处罚决定,对百度贴吧作出“从重罚款”的处罚决定。紧接着,“58同城、赶集网等因违法违规发布‘大棚房’租售信息被约谈”,北京市网信办、北京市规划国土委同样根据《网络安全法》第47条和第68条作出处理,但处理结果是“下达行政执法检查记录,责令网站落实整改”。对上述两则执法事例进行剖析,可以从实践层面呈现出对网络运营者进行网络安全行政处罚的客观运行样态。

(一)实践样态:违反网络安全保护义务的“罚”与“不罚”

上述执法事例发布后,简单对比后便不难发现,同样是违反《网络安全法》第47条所设定的“发现法律、行政法规禁止发布或者传输的信息的,应当立即停止传输该信息,采取消除等处置措施,防止信息扩散,保存有关记录,并向有关主管部门报告”这一法定义务,在实践当中却直接事关“罚”与“不罚”的问题。

1.从重处罚

据“网信广东”^[20]微信公众号发布的消息称,广东省网信办于2017年8月11日对腾讯公司微信公众平台存在用户传播暴力恐怖、虚假信息、淫秽色情等危害国家安全、公共安全、社会秩序的信息问题依法展开立案调查。调查结果显示,腾讯公司对其微信公众平台用户发布的有关法律法规禁止发布的信息未尽到管理义务,其行为违反《网络安全法》第47条的规定。根据《网络安全法》第68条,广东省网信办对腾讯公司作出最高罚款的处罚决定。几乎与此同时,北京市网信办也依据《网络安全法》就新浪微博对其用户发布传播“淫秽色情信息、宣扬民族仇恨信息及相关评论信息”未尽到管理义务以及百度贴吧对其用户发布传播“淫秽色情信息、暴力恐怖信息帖文及相关评论信息”未尽到管理义务的违法行为作出从重罚款的处罚决定。

从基本案情来看,两起事例均将网络运营者未尽到对其用户发布传播“淫秽色情信息、宣扬民族仇恨信息及相关评论信息”以及传播“淫秽色情信息、暴力恐怖信息帖文及相关评论信息”行为的管理义务视为“情节严重”这一法定从重处罚情形,且由主管部门直接依照《网络安全法》第68条规定的“拒不改正或情节严重”所对应的法律后果分别进行了顶格罚款和从重罚款。就公布的事实来看,两者尽管在论证环节存在区别,即广东省网信办进一步将“淫秽色情信息、宣扬民族仇恨信息及相关评论信息”界定为“危害国家安全、公共安全、社会秩序的信息”,但这一认定并未对双方所应承担的法律后果产生实质性影响。

2.仅责令整改

据新华社北京2017年8月17日电,北京市网信办、北京市规划国土委就违法违规发布“大棚房”租售信息一事,联合依法约谈58同城、赶集网、百度等网站。对此,北京市网信办、北京市规划国土委两部门要求,“不得发布‘大棚房’信息广告,发布农业大棚信息时不得含有可居住等信息内容;不得发布含有生活设施的农业大棚房源照片;各网站要严格遵守《网络安全法》《互联网新闻信息服务管理规定》,不得发布违法违规信息,更不得通过发布谣言、标题党等行为误导网民,对违法违规从事互联网新闻信息服务业务的网站将予以相应的行政处罚”,^[21]进而根据《网络安全法》第47条及《互联网新闻信息服务管理规定》第16条^[22]相关规定下达了行政执法检查记录,责令网站落实整改。

事实上,《网络安全法》和《互联网新闻信息服务管理规定》对于网络运营者、互联网新闻信息服务提供者未尽到对于违法信息管理义务的规定并不完全一致。前者对一般违反义务的情形规定了“责令改正,给予警告,没收违法所得”这一法律后果;而后者仅规定了“给予警告,责令限期改正”。尽管规定

[20]该公众号系广东省互联网信息办公室注册的官方微信公众号,发布的信息具有官方权威性。

[21]58同城、赶集网等因违法违规发布“大棚房”租售信息被约谈,载新华网:http://news.xinhuanet.com/2017-08/17/c_1121500789.htm,2018年1月2日。

[22]参见《网络信息服务管理规定》第16条规定。

不尽相同,但两者均不存在免于处罚的仅责令改正的情形,^[23]而是均要求给予警告处罚。但从北京市网信办的决定来看,其并未对相关部门发布传播违法信息的行为给予处罚,仅仅是责令整改。与此同时,北京市规划国土委执法总队相关负责人在论证这一网络发布行为的违法性时进一步指出,“‘大棚房’是利用大棚结构将农业生产用地改造成居住生活用地,其行为违反土地管理、城乡规划法律法规,属于违法用地违法建设,对耕地及基本农田造成严重破坏。按照要求,北京市严禁建设‘大棚房’,现有的‘大棚房’也要坚决予以拆除。相关网站发布的‘大棚房’租售信息,给不了解情况的网民造成错误引导,极易产生经济损失,并引发后续不良社会影响”。^[24]结合上述意见发现,在完成了对违法事实,即相关网站发布的信息内容系属于违法信息,并造成误导网民进而极易产生经济损失并引发不良社会影响的后果的论证后,主管部门却并未按照相关法律规定赋予该法律事实对应的法律效果。

3.因忽略主观状态导致处罚的随意性

综合上述执法事例可以发现,执法机关基于类似的法律事实——网络运营者未能尽到对用户发布的违法信息的管理义务,分别赋予该法律事实以“罚”与“不罚”的法律后果,处罚决定的作出似乎具有相当的随意性。在重罚运营者的事例中,并未看到行政机关对于从重理由的说明,而是在对法律事实进行简单阐述后,直接进行了法定处罚的升格,对网络运营者顶格处罚和从重处罚。而在“约谈案”中,在对违法事实及其危害后果进行明确认定后,却转而作出“责令改正”这一决定,并未对该违法行为予以处罚。

关于从重处罚,《网络安全法》并无明确规定。与之相关联的《行政处罚法》第38条第2款规定:“对情节复杂或者重大违法行为给予较重的行政处罚,行政机关的负责人应当集体讨论决定。”该条款尽管涉及“较重行政处罚”,但也仅仅从处罚决定作出的程序视角来规范处罚行为。尽管我们无法从上述执法事例中看出该从重处罚决定的作出是否经过了行政机关负责人集体讨论这一程序,但就这一规定本身而言,很显然意味着“较重行政处罚决定”的作出应当坚持审慎的义务。即,只有在充分论证出基本的法律事实情节复杂或者违法行为达到“重大”程度,且经过较为严格的程序方能作出。此外,根据《行政处罚法》第25、26条的规定,在决定是否对违法行为人从轻处罚、减轻处罚甚至是不予处罚时,相对人违法时的主观状态亦是重要的考量要素之一。从体系解释出发,得出是否从重处罚亦需要将违法者的主观状态考虑在内这一结论应当并不存在方法论上的障碍。在腾讯、百度被重罚的事例当中,根据主管部门所依据的《网络安全法》第68条的规定,对于一般的违法行为,仅仅对应“警告,没收违法所得”这一法律后果,只有存在“拒不改正或情节严重”的情形时才可作出“罚款”处罚。从“当然解释”的角度出发,仅适用“罚款”这一处罚种类况且需要“情节严重”这一论证过程,直接作出顶格处罚或从重处罚则当然不可缺少更加有力的论据支撑,其中亦应当包括对于网络运营者是否尽到管理义务的主观状态的考量。

同样,在对58同城、赶集网等违反网络安全保护义务却不予处罚的事例中,对于相关网站履行监管义务的主观状态的忽略使得整个论证过程呈现出逻辑上的混乱和断裂。

上述实践情形意味着,在网络安全行政处罚的执法实践当中,执法机构缺乏对网络运营者在实际层面上是否尽到管理义务的论证和考量,而是在发现违法信息后,直接认定网络运营者未尽到网络安全保护义务,并未将法定的主观要素考虑在内,导致了处罚行为的随意性。

(二)网络安全处罚实践忽略主观状态审查的原因

1.审查动力不足

(1)专项治理的执法逻辑。

现代行政法下的行政权是一种需要严格依法行使的有限权力。然而,与有限制的行政权相并列

[23]无论是互联网领域的行政处罚,抑或是传统领域如《安全生产法》中,都存在大量责令整改、责令改正等规定。尽管学界对于责令改正究竟是否属于行政处罚存在争议,但本文认为,除法定的责令停产停业外,责令改正并非处罚行为,仅仅作为行政管理的手段或措施而存在。

[24]前引[21]。

的是有效率的行政权。“行政需要效率是行政的生命,现代社会中的行政权对效率尤其渴望。”^[25]基于这样的理念,行政权的行使尽管离不开法律的严格控制,但同时也要求法律同行政一道,高效率地、积极主动地介入社会各领域,协调复杂的利益关系,从而在最大限度内确保公民基本人权的实现。

然而,“随着立法规模的扩大,行政机关所承担的执法职责也随之增加。执法任务与执法资源之间的矛盾是客观存在的。从理论上说,行政机关应当将所有的执法资源平等地分配到每一部法律的执行中。但是,立法往往对这一问题未置可否。因此,如何分配执法资源成为裁量的事项。实践中,轻重缓急是由行政机关独自拿捏的。选择取舍中的顾此失彼、厚此薄彼也不可避免地成为不同法律以及同一部法律不同事项实施中的常态。”^[26]在运动式治理、专项治理模式模式一直被视作公共政策高效推行的中国经验这一背景下,^[27]某种程度上,对法律的实施是通过制定政策开展专项治理的方式加以推进的。《网络安全法》制定实施后,各部门紧接着下发了学习《网络安全法》的通知,并同时制定了“加强网络安全管理,净化网络环境”等具体的工作要求,全方位地按照上述目标开展相关工作。“公安部会同有关单位组织开展了大型互联网企业专项保卫行动、网站安全和互联网电子邮件安全专项整治行动,发现整改了一批网络安全深层次问题和隐患。各地也通过开展‘扫黄打非’、‘剑网’等系列行动,对互联网站、应用程序、论坛、博客、微博、公众账号、即时通讯工具、网络直播中宣扬恐怖暴力、淫秽色情等信息及时清理。”^[28]如同一位大数据领域的创业者所感受到的那样,“《网络安全法》正式实施前后,像一场寒流,席卷了整个大数据行业”。^[29]在以专项整治的方式推进《网络安全法》的实施过程中,网络环境的确在相当短的时间内达到了政策推行的目标,亦保证了《网络安全法》第8条“县级以上地方人民政府有关部门的网络安全保护和监督管理职责”的实现。此种专项治理下追求治理效率和效果的执法逻辑必然导致行政执法机构对于法条本身规定的主观状态的审查动力不足,而仅仅根据“违法行为—法律后果”这一客观归责模式,力求在最短的时间内实现专项整治的打击目标。

(2) 忽视《网络安全法》所承载的“积极促进”目的。

如前文所述,《网络安全法》具有“网络安全之保障”与“网络信息化发展之促进”的双重目的。但无论是《网络安全法》出台后各部门为配合法律的执行所制定的相关配套法规,抑或是开展的各项专项整治行动来看,其偏重点均在于打击违法行为这一突出的问题导向。从上述文件中不难发现,其规范和强调的重点均在于构建严密的规范体系以应对网络安全日趋复杂的严峻形势,至少从规范层面几乎未见对于促进网络信息化发展这一积极目的的考量。在执法实践上,“各地各有关部门认真落实法律要求,扎实做好网络意识形态工作,坚决清理各类违法违规信息;法律实施主管部门还建立了网络信息巡查机制和公众举报平台,及时清理违法违规信息”。^[30]尽管从实用主义的角度来讲,对于违法行为打击当然有助于促进网络信息化的健康发展,但作为法律之灵魂存在的立法目的这一核心条款直接指引着具体制度规则的建构。因此,对《网络安全法》所承载的“积极促进”目的的忽视也不可避免地引导执法者单纯专注于打击违法行为的实质性效果上,使得执法机构在实践中对规范层面所要求的主观过错审查的动力严重不足。

2. 过度的预防性规制使得处罚行为脱离法治框架

当下已经进入风险社会。在这一急剧转型时期,个人言行失范、脱序的现象与社会正常发展之间一直处于紧张状态之中。作为行政机关,其首要任务在于维系社会秩序的稳定,这是其他一切活动得

[25]章剑生:《现代行政法基础理论》,法律出版社2015年版,第93页。

[26]林彦:《全国人大常委会如何监督依法行政?——以执法检查为对象的考察》,《法学家》2015年第2期。

[27]参见贺东航、孔繁斌:《公共政策执行的中国经验》,《中国社会科学》2011年第5期。

[28]王胜俊:《全国人大常委会执法检查组关于检查〈中华人民共和国网络安全法〉〈全国人民代表大会常务委员会关于加强网络信息保护的決定〉实施情况的报告》,2017年12月24日在第十二届全国人民代表大会常务委员会第三十一次会议上。

[29]《网络安全法》实施一个月,大数据创业进入迷茫期,载腾讯网 <http://tech.qq.com/a/20170710/020821.htm>,2018年1月5日。

[30]古承宗:《风险社会中与现代刑法的象征性》,《(台湾)科技法学评论》2013年第1期。

以开展的前提。现行法律规范中大量“罚”则的存在也多少可以说明这一点。但另一方面,这种紧张状态往往成为了执法者僭越立法的正当理由,也极其容易获得社会公众道义上的支持。因为社会公众也迫切地需要政府来整合不稳定的社会秩序,以此在风险社会当中求得更多的安全感。“风险社会的规范议题不再是强调国家统治权力过度集中,或是自由如何分配等,而是聚焦在社会持续处于一种高度信赖社会控制机制的氛围,亦即要求国家积极采取行动排除或降低风险(恐惧),或是实现安全保证之需求。”^[31]因此,个人的生存风险亟待通过国家层面的具体制度举措获得消解,否则,个人出于本能对风险的抵御很有可能通过危害社会秩序的极端方式进行,以此便会进一步加剧其他生存者的焦虑和不安。这样的现实亦对风险社会下的政府治理提出了新的要求。

(1)从行为控制转向源头控制。

复杂交互的网络技术、匿名化的网络环境都意味着风险的不可避免性,面对铺天盖地的“违法行为”,应当建构一种整体性的治理与规制策略,在此指导之下,考虑如何从源头开始,对导致危险现实化的相应环节进行必要控制,构建新的归责机制,以避免无人负责现象的蔓延。^[32]但与此同时,若是规制举措本身超出了“必要控制”的范畴进而过度追求对于未来秩序的可控性,那么新的风险源便伴随而来,即政府本身的管制行为规避了法治框架的约束。

(2)预防性规制策略本身蜕变为新的危险源。

“在传统的规制领域,任何政策执行点上,行政权都会有立法者无法控制的政策回旋空间存在,包括执行工具的选择、标准的制定、甚至是政策价值间的优先设定与选择等,”^[33]在牵涉到复杂的互联网技术变革的网络空间更是如此。然而“预防总是与无限制相联系,具有不确定性和难以捉摸的特性,具有与生俱来的‘越早越好’的内在扩张逻辑”,^[34]基于这样的逻辑,行政机关也因此获得了巨大的权力行使空间。当预防性规制策略抑制了规制对象发展的内在动力,那么此种规制手段可能会导致的后果就在于,借由对未来秩序之可控性的追求这一看似正当的目的而弱化法治的约束,进而使得为控制风险所采取的预防性规制手段本身蜕变为新的危险源。《网络安全法》实施后,为尽可能保障网络安全,行政执法机构对于网络安全管理秩序的维护进行了积极介入与干预,一旦发现违法行为便迅速进行处置。此种高效率的执法行为一方面在短时间内获得了突破性的执法成果,但与此同时,也不可避免地规避了《网络安全法》中关于主观要件的规定,产生了弱化法治约束这一新的风险。

四、通过“区分信息种类和内容”分别建构主客观归责路径

尽管网络安全行政处罚主观归责原则实效性危机的存在有着深刻的原因,但并不能以此减免行政执法弱化法治框架约束的正当性拷问。就《网络安全法》的现行规定而言,主观归责原则的“一刀切”也的确给执法实践带来了一定的障碍。一方面,该原则的确立充分考虑了网络安全领域违法行为的特殊性及《网络安全法》的立法目的,因而有其合理性;但另一方面,此种“一刀切”式的规定使得行政执法机构出于执法效率的考虑,在应当考量主观要素的场域对该要件作出选择性忽略。因此,基于网络安全保护的实效性、网络法治秩序的平衡,对于网络运营者的网络安全保护义务应当通过“区分信息种类和内容”分别建构主客观归责路径。

(一)法定监督义务之类型区分

《网络安全法》要求网络运营者加强对网络用户的发布和传输行为的监管,但并未就信息的种类和内容本身作出规定。但发布和传输这一界分本身就意味着网络运营者所要监控和管理的信息在内

[31][32]参见劳东燕:《风险社会与功能主义的刑法立法观》,《法学评论》2017年第6期。

[33]叶俊荣:《环境行政的正当法律程序》,台湾三民书局1997年版,第15页。

[34]何荣功:《预防刑法的扩张及其限度》,《法学研究》2017年第4期。

容上是存在不同的。尽管信息源头均来自网络用户,但用户发布和传输的内容可能是终极信息,亦有可能是中间层信息,即不直接显示内容的链接信息。倘若如此,在不区分信息内容和种类的情况下要求网络运营者行使监督职责是否具有期待可能性呢?

在比较法上,德国在1997年即颁布了《多媒体法》,是世界范围内首个制定互联网规制法律规范的国家。该部法律对运营商的责任作了分层处理,其基本原则在于,网络服务提供者对其自身提供的信息负责;对于来源于第三方的信息,只有在运营商了解并掌握了该信息的内容并且在技术上存在阻止其传播的可能性的情形下才负有责任;对于只是通过该平台促成对第三方信息的使用的情形不负有责任。尽管该规定出台于20世纪,但其中的分层处理方式于今天的网络空间规制仍然有借鉴意义。即,在认定运营商责任时,需要区分平台本身所发布的信息和以该平台充当中介所发布的来源于第三方的信息,即运营商和信息来源之间的关系问题。

新加坡在《互联网行业准则》中明确了网络内容的主要责任人是信息的作者,而非运营商,但是明确了运营商在政府调查过程中的协助义务。因此,新加坡网络规制立法的特殊性在于,在管制过程中,仅对运营商设定了较为宽松的配合义务,而并未为其设定事先审查以及事中监控互联网内容的义务,一方面体现了政府在网络治理中与运营商进行共治的协作模式,另一方面尽可能地为网络的发展减轻阻碍和提供充足的空间。同时,《准则》为了保证运营商提供服务的积极性,还规定了相应的免责条款,包括按照政府的要求取消对于包含违禁内容的网站的订阅以及立即消除对于此类网站的链接等。因此,新加坡总体而言所采用的是一种较为柔性的治理方式,在保障国家和公共利益的基础上,尽可能低限度地限制互联网的使用以保障民众的言论自由,同时也赋予了运营商足够的发展空间,从而达到促进信息技术发展的目的。同时,对于违反法律规定的平台责任人,在政府对其进行处罚之前,先行给予一次自行纠正的机会。

由此观之,在新加坡和最早进行互联网规制立法的德国,均以区分信息来源作为对运营商创设义务的前提。除了为运营者及其平台负责人设定了较为宽松的监督和配合义务之外,^[35]新加坡《互联网行业准则》更是追根溯源,直接从源头上对信息的作者进行处罚。此外,亦有一些国家通过与运营者签订协议的形式来实现对互联网的规制,而政府在此过程中会不断为运营者提供技术支持,如过滤软件等。^[36]

(二)通过区分信息种类和内容实现监督义务的期待可能性

相比较之下,我国对于互联网的规范制度较为严格,这样的规定是与当前较为严峻的网络安全环境相适应的,尽管如此,倘若在不对信息种类和内容加以区分的状况下为责任主体设定监督义务,此种义务很有可能会因为不具有期待可能性而根本无从履行。

期待可能性理论产生于德国,同时也是我国刑法理论中的重要问题。德国学者威尔泽尔认为:“人总是预先确定目标并选择达成此目标的手段,进而使用选择的手段而向达成目标的方向努力,此种目的性才是行为的本质要素。”^[37]尽管这句话是对于“规范责任”的阐述,但该理论以期待可能性为核心,使得我们能够从中窥知一二。日本学者大塚仁教授曾经对期待可能性理论作过如下评价:“期待可能性正是想对在强有力的国家法规范面前喘息不已的国民的脆弱性倾注刑法的同情之泪的理论。”^[38]期待可能性对于法律规范设定的限制在于,对于不具有可实现性的义务,不应当作为入罪的责任要件。作为同为国家制裁违法行为的行政处罚,该理论亦可为其所用。实践中,尽管网络运营者投入了大量的人力、物力从事信息的审核以及不良信息的处置工作,但面对海量的互联网信息难免

[35]事实上,绝大多数国家关于互联网规制的法律都仅规定了运营商的协助义务,对于网络安全的维护仍然由政府部门充当技术和监管主力。

[36]澳大利亚对网络管理的法规由政府、行业和受众代表共同制订。澳大利亚网络服务提供商与政府传播和媒体管理局签署协议,保证不传播谣言、垃圾邮件等。传播和媒体管理局还向网络服务商提供过滤软件,以保证协议的有效执行。

[37]陈兴良:《期待可能性问题研究》,《法律科学》2006年第3期。

[38]冯军:《刑事责任论》,法律出版社1996年版,第245页。

挂一漏万。出于网络安全保护之实效性与网络法治秩序之平衡,应当以“区分信息种类和内容”分别建构主客观归责路径。当然,此种区分无需如同新加坡那般过度追溯,直接将责任落实于信息作者头上即可,否则会架空运营商的监督义务,使得《网络安全法》的规定形同虚设。此外,在区分的基础上需要附加一定的说明义务,即运营商在发布该外部信息时的确不知晓或者在技术上不存在鉴别的可能性,此种情形下当然不能再期待其监督义务的实现。

(三)基于区分信息种类和内容这一前提分别建构主客观归责路径

基于网络安全保护的实效性与网络法治秩序的平衡,应当通过区分“能够直接获取实际内容的终极信息”与“通过该运营平台发布的中间信息”,以及“高度敏感性信息”和“模糊性信息”分别设定不同程度的监督义务。具体可分为两个步骤进行:对该信息作“终极信息”与“中间信息”的区分,若是后者,则因具体内容的不可控性而采主观归责原则;若是前者,则进一步对该信息作“高度敏感性信息”抑或是“模糊性信息”的界分。对于前者,由于此类信息的传播可能产生的重大危害后果,因而应当采取较为审慎的态度,采客观归责原则;对于后者,应当采过错推定原则,即若是运营者能够证明自己已经尽到管理义务,即用尽技术措施及监控手段均无法发现或判断的,可免于处罚责任。具体如下:(1)对于“通过该运营平台发布的中间信息”,因具体信息内容具有变动性和不可控性,因此采主观归责原则。(2)对于“能够直接获取实际内容的终极信息”,若是其内容属于“高度敏感性信息”,网络运营者应当负有审慎的处置义务。应当在发现后立即删除;若是属于“模糊性信息”,一方面,对信息作出是否具有违法性的判断势必导致删除行为的滞后性;另一方面,对模糊性信息本身的违法性界定亦存在主观性。因此,对此种情形应当采过错推定原则。

根据《网络安全法》第47条和68条之规定,法律为网络运营者设定了采取对违法发布或传输信息的具体处置义务。按照上述判断步骤,若是所涉违法信息属于终极信息中的模糊性信息,网络运营者若是未履行对此种信息的处置义务,则可推定其主观上具有过错,依法处“警告,没收违法所得”等处罚。但如前所述,网络运营者履行这一义务的前提条件在于其能够发现违法信息,故而应当排除对于“未被发现”以及“未能被发现”的违法信息的处置义务。由此,网络运营者能够证明其已经穷尽技术手段、且并未违反事前的“防范”义务时,即无需承担违法责任。

此时,尽管运营者可以免受第68条规定的“警告、没收违法所得”等处罚,但这并不意味着正常的网络秩序无法得到修复。《网络安全法》对网络秩序的规范举措是多方位的,除了监管处置义务外,亦包括配合义务,^[39]同时创设了约谈、^[40]警告等多种方式作为辅助手段来实现对网络安全秩序的保护。另外,《刑罚修正案(九)》亦专门增设了拒不履行网络安全管理义务罪。

结 语

互联网技术的发展日益推动着行政法学领域知识形态的改变。尽管在实践和学说领域都不乏对于互联网规制以及行政处罚归责原则等话题的探讨,但如何将互联网规制中的具体责任条款整体嵌入甚至覆盖到行政处罚法益当中,则是一个需要我们以全新的视角去看待的问题。必须明确的是,在讨论互联网规制的诸多问题时,仅在现实世界中既定法律规范的“螺狮壳里做道场”固然不可行,但若是仅仅将目光流连于现实中已经改变的格局,片面沉溺于信息技术的汪洋大海当中随波逐流的做法亦不可取。因此,本文将视线聚焦于规范与事实之间,着眼于信息技术的发展对于现实规制所提出的要求进行阐释,以期有裨于网络安全行政处罚归责原则的进一步具体建构和完善。

[39]参见《网络安全法》第69条的规定。

[40]参见《网络安全法》第56条的规定。