

数据监管权横向配置的反思与重塑

刘权, 廖嘉林

(中央财经大学法学院, 北京 100081)

摘要:《网络数据安全条例》第47条规定国家数据管理部门网络数据安全职责,有助于优化数据监管权的横向配置,但并未根除“网信统筹+分业监管”的传统数据监管权横向配置的弊端。传统数据监管权横向配置存在过于分散和交叉重叠等缺陷,既增添不必要的监管成本,也造成过度监管或监管不足,在应对数字经济不确定性和数据处理活动特殊性中具有局限性。传统数据监管权横向配置有违功能适当原则,需细化构建“网信统筹+专门监管+分业监管”的横向配置结构。具体而言,强化网信部门的统筹协调职能以妥善处置监管权力纠葛,确定国家数据局为专门数据监管机构以实现监管的独立性和全局性,廓清部门分业监管的权责边界以达致数据监管的分工与合作。

关键词:数据监管权;国家数据局;数据安全;个人信息保护;功能适当原则

中图分类号:D922.1

文献标志码:A

文章编号:1672-7835(2025)03-0136-10

一、问题的提出

随着数字时代大数据、人工智能等新兴领域的迅猛发展,科学配置数据监管权,以实现该领域规范与发展并行至关重要。数据监管权是指法律设定的政府为履行数据监管事务所享有的公权力,监管内容包括数据安全和个人信息保护。《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)、《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)授予国家网信部门统筹协调职责及相关监督管理权,赋予工业、电信等主管部门在各自职责范围内的数据监管权,塑造出“网信统筹+分业监管”的传统数据监管权横向配置结构。2025年1月1日施行的《网络数据安全条例》第47条第3款规定在遵循传统数据监管权横向配置格局的基础上,规定国家数据管理部门在具体数据管理工作中履行相应的网络数据安全职责,这对解决传统数据监管权过于分散的缺陷具有重要意义。但是,《网络数据安全条例》第47条规定的适用范围有限,对国家数据管理部门的权限配置也十分有限,存在与数据法律规定较为抽象的类似问题,并未根除传统数据监管权横向配置的弊端,亟须在规范层面予以厘清与克服。

学界就数据监管权的配置问题展开了适量研究,主要从解剖数据多头合规问题^①、探讨构建个人信息保护机构^②、提出以法律限制数据监管权的创设^③、归纳域外数据监管经验^④等角度展开。上述探索为本文研究奠定了基础,但现有研究对于为何需要调整配置数据监管权的探讨不够深入,针对数据监管权

收稿日期:2024-11-11

基金项目:北京市社会科学基金一般项目(24FXB007);中央财经大学科研创新团队支持计划资助项目

作者简介:刘权(1982—),男,湖北随州人,博士,教授,博士生导师,主要从事行政法、数字法研究。

①参见黄志雄:《数据治理的法律逻辑》,武汉大学出版社2021年版,第181—214页;廖嘉林:《论数据监管权的规范配置》,《河北学刊》2025年第2期;廖嘉林:《公共数据要素市场化配置的主要困境与法治保障》,《宏观经济研究》2025年第3期。

②参见邓辉:《我国个人信息保护行政监管的立法选择》,《交大法学》2020年第2期;高秦伟:《论个人信息保护的专责机关》,《法学评论》2021年第6期;刘权:《风险治理视角下的个人信息保护路径》,《比较法研究》2024年第2期。

③冯洋,朱磊磊:《大数据监管权的法律限制》,《西安交通大学学报(社会科学版)》2023年第5期。

④参见陈统:《欧盟数据治理中的“一站式”监管:运行机制、实施困境及启示》,《学术探索》2024年第1期;米铁男:《俄罗斯网络数据流通监管研究》,《中国应用法学》2021年第1期。

的横向配置缺乏专门研究。本文将在检视传统数据监管权横向配置结构的基础上,论证重塑数据监管权横向配置的正当性,进而提出完善数据监管权横向配置的规范路径。

二、传统数据监管权横向配置的检视

“网信统筹+分业监管”分散化特征明显,一方面有助于减少信息不对称,利于各部门施展符合产业特点的监管技能;另一方面其弊端也日益显现,逐步沦为保障各方合法数据权益的牵掣。

(一) 传统数据监管权横向配置的构成

我国数据监管的横向配置经历了分业监管到“网信统筹+分业监管”的过程。数据分业监管是指根据数据控制者违法数据收集、处理行为所发生的领域确定数据监管机构的模式^①,其肇始于 2000 年全国人大常委会发布的《关于维护互联网安全的决定》。该决定首次在网络空间对个人数据进行保护,通过解释刑法在网络空间中的运用来保护个人数据,赋予政府机构一些数据监管权。2012 年全国人大常委会发布的《关于加强网络信息保护的決定》首次以法律形式建构个人数据保护制度,规定有关主管部门应当在各自职权范围内依法监管侵犯公民个人数据及其他危害网络信息安全的行为,塑造了分业监管的构造形态。为解决互联网及数据领域各自为政、协调性差的问题,2011 年国家成立网信办,负责互联网领域政策协调、法制建设和内容管理;2014 年成立中央网络安全和信息化领导小组及其办事机构,由网信办承担具体职责。经由数据法赋权,我国在横向层面已形成“网信统筹+分业监管”的数据监管配置结构。

“网信统筹+分业监管”本质是分散化监管。根据数据法律法规以及《电信和互联网用户个人信息保护规定》等数十部规范性文本的规定,网信部门、工信部等多个部门在互联网、工业等领域均有监管权。数据分散化监管具有一定的合理性。由行业部门进行领域内监管,契合部门管辖的特征,有助于充分利用部门便利的监管条件,发挥熟悉数据处理活动的优势;有利于比较产业监管机构的行为,减少信息不对称,跟进互联网的快速演进与变革。但是,这种过于分散化的监管结构,其弊端也日益突出,桎梏公民与国家的数据权益保护,成为推进国家数据治理现代化过程中不容忽视的缺陷。

(二) 传统数据监管权横向配置的缺陷

1. 监管权力配置过于分散

数据监管权过于分散化主要表现为以下两个方面:一是数据监管机构设置较为狭窄,具有内在关联性的行业领域被割裂至不同监管部门管辖,数据监管缺乏专业性、综合性和全局性。在不少领域如交通安全领域的违法行为,网络部门、工信部门、公安部门等共享数据监管权。二是统一的数据监管权被分割于市场监管部门、工信部门等,数据监管权缺乏统合性,监管能力受到明显制约。网信部门作为统筹协调机构,并非专门的数据监管机构,却在执法实践中承担了过多的数据监管权。

数据监管权过于分散弊端丛生。数据监管权作为一种市场规制权,权力拥有者可以借此发挥市场影响力、控制市场资源甚至进行权力寻租,对监管部门而言具有天然的诱惑力。其一,滋生部门利益主义。各个监管部门形成单个权力中心,集决策、执行、监督权力于一身,可能导致部门系统封闭化、公共权力部门化。比如,在一起 APP 违法违规收集用户个人信息的案件中,检察院在办案前期竟找不到适当的行政主管部门^②。其二,造成过度监管或监管不足。数据监管权配置专业化有余而综合协调不足,相互牵制有余而相互配合不足^③。多头监管不利于稳定市场主体预期。相互竞争的监管机构导致监管过度,监管机构容易以“纳尔逊之目”方式选择性地评估监管所导致的成本^④。其三,不利于开展国际监

①黄志雄:《数据治理的法律逻辑》,武汉大学出版社 2021 年版,第 189 页。

②《浙江省杭州市余杭区人民检察院诉某网络科技有限公司侵害公民个人信息民事公益诉讼案》,最高人民检察院官网, https://www.spp.gov.cn/spp/jcgyssljgrxbh/202104/t20210422_527821.shtml。

③石佑启:《论法治视野下行政权力的合理配置》,《学术研究》2010 年第 7 期。

④克里斯托弗·胡德,科林·斯科特,等:《监管政府:节俭、优质与廉政体制建设》,陈伟译,高世楫校,译林出版社 2020 年版,第 150 页。

管与合作。随着电子商务、数据跨境流动的迅猛发展,各国依靠本国监管数据安全与个人信息侵害行为难以为继,其与国际标准经贸规则和国际组织对接合作的需求愈发强烈。《个人信息保护法》第12条规定国家应参与制定个人信息保护国际规则。过于分散的数据监管权导致对外的交流窗口、合作桥梁缺失,不利于体现我国政府对公民数据权益保护的高度重视和消除数据流通中的不合理障碍。

2.法定监管配置过于抽象模糊

现行数据法采用“有关部门”与“各自职责范围”的概括性表述界定监管主体权责,并未构建清晰的部门职权划分标准,亦未确立有效的跨部门协同治理机制,导致监管实践中存在职能交叉重叠与真空地带并存的悖论现象。网信部门虽然被赋予“统筹协调”职能,但其法定定位与实施效能之间存在一定落差。实践中,由于不同数据监管部门间法定职责界定不清,已有部门间配合不到位、检测标准和执法尺度不一致等问题,容易出现部门间竞争性监管执法的情形,影响个人信息保护监管执法的高效开展^①。

法定监管配置的语义模糊使所有数据监管机构均有法律解释权,可能导致监管成本加大、监管冲突、监管缺位、监管效率低下以及问责困难等问题。在2017年的支付宝年度账单未经同意搜集个人信息案件中,承担监管职能的网信部门和工信部通信管理局竟先后在2018年1月6日和11日约谈涉事企业负责人^②,重复监管导致消耗不必要的组织资源。在一起个人信息保护公益诉讼案件中,检察院发现某省通信管理局、某市公安局、某市互联网信息办公室均未履行个人信息保护监督管理职责,存在职能交叉、监管部门层级不同问题,导致放纵某款APP违法违规收集或使用公民个人信息的行为^③。网络通信公司的专营店侵害消费者个人信息的行为,究竟是市场监管部门予以监管,还是由工信部门展开监管,在执法实践中存在差异性^④。在某省级检察院办理的APP违法违规收集使用个人信息行政公益诉讼案中,相关行政机关反映,由于监管职权交叉、技术保障滞后等原因,导致监管缺乏系统性、有效性^⑤。

3.授权性监管职能过于宽泛

以《个人信息保护法》为例,其中存在大量监管授权性条款,给监管部门留有巨大的裁量空间。《个人信息保护法》第62条规定网信部门统筹协调有关部门开展个人信息保护工作,授予监管部门广泛的监管创制范围。类似的授权条款还有《个人信息保护法》第45条、第52条和第58条的规定。以上条款均未明晰授权的事项、目的、范围、期限及被授权机关实施授权决定应当遵循的原则。这些授权性规范为应对复杂的个人信息处理活动提供了灵活的监管工具,有助于形成激励相容的数据治理模式。但是,极为宽泛的监管性授权可能存在合法性风险,监管部门几乎享有不受范围和内容限制的规则制定权,将加剧《个人信息保护法》实施后不同时期的差异化适用,形成一种实质上的“法律适用不平等”或者“执法不平等”^⑥。在监管处罚权限配置上,《个人信息保护法》设定了十分宽泛的裁量空间。《个人信息保护法》第66条规定将该法中所有个人信息处理的权利义务关系条款纳入行政处罚的制裁后果,并未凸显对不同权利义务配置类型的差别。总之,过于宽泛的授权性监管职能可能助长数据监管的恣意行为。

三、重塑传统数据监管权横向配置的正当性

“网信统筹+分业监管”在应对日益纷繁复杂的数字经济与数据处理活动中愈发捉襟见肘,有必要

①崔聪聪:《个人信息保护的行政监管及展开》,《苏州大学学报(哲学社会科学版)》2022年第5期。

②参见《国家互联网信息办公室网络安全协调局约谈“支付宝年度账单事件”当事企业负责人》,国家互联网信息办公室官网, http://www.cac.gov.cn/2018-01/10/c_1122234687.htm? mtype=group;《工业和信息化部信息通信管理局就加强用户个人信息保护约谈相关企业》,工业和信息化部官网, https://www.miit.gov.cn/jgsj/xgj/gzdt/art/2020/art_188834d379ac47b0837324db21fcf10d.html。

③《检察机关个人信息保护公益诉讼典型案例》,最高人民检察院官网, https://www.spp.gov.cn/xwfbh/wsfbt/202104/t20210422_516357.shtml#2。

④参见湖北省荆州市中级人民法院(2015)鄂荆州中行终字第00063号行政判决书;北京市西城区人民法院(2020)京0102行初127号行政判决书;北京市第二中级人民法院(2020)京02行终1338号行政判决书。

⑤《检察机关积极维护个人信息安全 2021年办理个人信息保护领域公益诉讼案件2000余件》,最高人民检察院官网, https://www.spp.gov.cn/spp/xwfbh/wsfbh/202202/t20220227_545967.shtml。

⑥蒋红珍:《〈个人信息保护法〉中的行政监管》,《中国法律评论》2021年第5期。

嵌入专门数据监管机构,并厘清其与网信部门、分业监管部门之间的分工与关系,这样才能契合功能适当原则。

(一) 重塑传统数据监管权横向配置的必要性

1. “网信统筹+分业监管”的局限性

“网信统筹+分业监管”植根于网信办主导的信息网络安全监管结构。20 世纪 90 年代以来,我国为应对互联网的快速发展和挑战,力求超越单一主管部门集中控制的传统管理模式,在互联网领域形成多部门、去中心化的社会化管理体系。互联网“九龙治水”的监管结构经历了 1994—1998 年邮电部、电子部、信息办和中科院四部门共管,1999—2004 年信息产业部主导,2005—2013 年国务院新闻办主导,2014 年起由网信办主导的阶段^①。网信办在 2011 年成立时被定位为管理国家互联网信息的办事机构,负责落实互联网信息传播方针政策和推动互联网信息传播法制建设,并无独立的监管职权。随着大数据时代的到来,为应对日益突出的数据安全和个人信息保护问题,在当时并无专门数据监管机构的情况下,2014 年国务院授权与数据监管内容较为贴近的网信办负责互联网信息内容管理,网信办开始逐步关涉数据方面的监管职责。但是,网信办主导的信息网络安全监管体制的核心职能并非数据监管,其将数据监管作为组织的次要工作,有效应对数据处理活动存疑。

数据处理活动相比网络活动具有特殊性。基于数据处理活动的特殊属性、数据的重要程度以及数据的不同应用场景,数据安全风险呈现的内容与网络安全风险并不一样,二者之间紧密关联的同时差异悬殊。数据安全主要受到数据泄露、数据损坏、数据丢失、数据滥用等威胁,而网络安全主要受到黑客攻击、网络病毒、网络钓鱼、网络诈骗等威胁。数据安全主要关注数据的安全性,包括数据的保密性、完整性、可用性和可控性等;网络安全主要关注计算机网络的安全性,包括网络的保密性、完整性、可用性和可控性等。数据安全与网络安全的交集,在于网络数据的自身安全。传统信息安全范式的保密性、完整性、可用性对于数据价值周期某一节点的数据自身安全仍适用,但对流动性数据的利用安全而言,传统信息和网络安全范式下静态的安全边界防护方法已难以为继^②。网络安全审查制度和数据安全审查制度在实践中经历了一个逐渐清晰分化的过程,表明信息网络安全监管体制与数据安全监管体制应当具有各自的边界与独立性。

进言之,在互联网发展初期,莫基于信息网络安全监管体制的“网信统筹+分业监管”尚能对数据安全、个人信息保护风险形成有效防控。但是,随着数字经济的深入发展,现有数据监管结构无力全面应对人工智能新技术、公共数据开发利用、数据跨境流通等有关大数据引发的新问题。从信息网络安全监管体制剥离并构造相对完整、独立的数据监管结构,是适应数据处理活动规律的必然选择。

2. 数据产业具有特殊性

数据违法行为的技术性、专业性和复杂性以及数据产业的融合对传统数据监管横向配置构成悬殊挑战。数据交易活动具有较强的技术性,要求推进专门数据监管组织配置的专业化^③。以个人信息保护为例,该领域应用极广、对象极多,在部分领域如 APP 违规收集个人信息具有较强的隐蔽性和危害性,挑战分散式执法,要求监管具有全局性与独立性。由于网信部门、工信部门等均非专门数据监管机构,在开展数据监管执法时难免会受到本部门利益及外界因素的影响,可能滋生“监管俘获”“权力寻租”“选择性执法”等问题。譬如,某家装企业违法收集、处理个人信息的行为并未获市场监管部门立案及支持^④就颇具争议。

数据产业具有融合发展的趋势。随着数字技术与实体经济的不断发展,传统的数据产业界限愈发

^①方兴东:《中国互联网治理模式的演进与创新——兼论“九龙治水”模式作为互联网治理制度的重要意义》,《人民论坛·学术前沿》2016 年第 6 期。

^②刘金瑞:《数据安全范式革新及其立法展开》,《环球法律评论》2021 年第 1 期。

^③廖嘉林:《论数据监管权的规范配置》,《河北学刊》2025 年第 2 期。

^④重庆市第一中级人民法院(2020)渝 01 行终 850 号行政判决书。

模糊,传统数据产业划分下的特定数据产业监管机构之间容易出现政策冲突^①。产业融合成为数据资源市场发展的一个规律和特征,客观要求将原来过于分散的监管执法职能进行适当整合,将其交由具有全局视野与独立性的机构行使,这在诸多传统事项领域中亦为鲜明例证。譬如,国务院迄今开展了9次大部制改革,通过统一反垄断执法权、合并保监会和银监会等进行监管职权适当集中,体现了适应监管事项领域发展变化的规律,具备特殊性的数据产业更应推行监管职权适当集中。2024年12月,国家发展改革委等六部门发布的《关于促进数据产业高质量发展的指导意见》强调推动数据应用创新和产业融合。数实融合、数据产业融合是数字经济与数据处理活动的发展趋势,客观要求数据监管事异则备变。

总之,快速变化的数字经济环境以及数据处理活动与传统的权力结构在时效性、覆盖性和有效性等方面的划分存在冲突,新技术新业态带来的监管空白冲击着缺乏专业性、全局性的传统数据监管结构。即使网信部门具有统筹协调职权,也无法摆脱临时组织的性质及多头监管的弊端^②。

(二) 重塑数据监管权横向配置契合功能适当原则

从“网信统筹+分业监管”模式中嵌入专门数据监管机构,构建“网信统筹+专门监管+分业监管”的整体监管模式,契合功能适当原则。功能适当原则是指以国家效能和治理能力为导向,将各种国家任务的职权配置给在组织、结构、程序、人员上具有优势,从而可能作出最优决定的机关^③。功能适当原则赞成权力的适度混合即必要分工和均衡,反对简单机械地拘泥于权力相互掣肘与削弱,最终目标在于实现国家权力行使的理性化和国家任务完成的最优化,进而保障人民的生存与发展权益。

其一,设立专门数据监管机构契合数字经济的运行机理,体现了行政组织法为适应技术变革而进行的制度创新,已被全球多数国家采纳。欧盟要求成员国建立独立监管机构,并设置欧盟数据保护委员会以协调成员国遵守实施《通用数据保护条例》^④。澳大利亚设置信息管理办公室开展数据安全和个人信息保护监管。专门数据监管机构相比主管部门模式抑或统筹协调模式,具备独立性、专业性和国际性,能有效平衡隐私保护和数据流通。设置专门数据监管机构有助于摆脱历次机构改革中行政组织的惯性思维,构成行政组织中的分殊现象^⑤。

其二,有助于捋顺“网信统筹”的法定功能,促进“网信统筹”职权行使的理性化。由于国家网信部门承担了过多的关乎数据领域的微观监管执法权,职能过于宽泛,导致其偏离“统筹协调和相关监督管理工作”的法定本职,难免影响其开展以信息安全监管为主业的监管工作。嵌入专门数据监管机构,有助于矫正网信部门“事事躬亲”的不良倾向,厘定和夯实其统筹协调的职能定位,推动其专责解决监管部门间信息沟通不畅、协同执法难度大的问题。

其三,有助于克服“分业监管”的过度分散性问题。行政目标的实现取决于行政权的范围是否合理明确,要求行政组织的整体设置简洁、协调和统一^⑥。一方面,通过适度整合网信部门、工信部门及分业监管部门的监管权,构建监管权相对统一的专门数据监管机构,能够迅速解决多头合规问题。另一方面,保持一定的分业监管并厘清分业监管的边界,可以满足刑事犯罪领域、国家安全等特殊领域、特别禁制的需求,持续为公民与企业提供合理的预期。

可靠的数据保护和执行机制是保障行业和个人利益的有效措施^⑦。《中共中央关于进一步全面深化改革 推进中国式现代化的决定》明确强调要“提升数据安全治理监管能力”。整体监管模式综合考量数据监管任务的特殊性、职能、组织、机关结构等诸多关联因素,进而达于整体监管组织结构以及内部

①周汉华:《基础设施产业政府监管权的配置》,《国家行政学院学报》2002年第2期。

②邓辉:《我国个人信息保护行政监管的立法选择》,《交大法学》2020年第2期。

③张翔:《我国国家权力配置原则的功能主义解释》,《中外法学》2018年第2期。

④参见《通用数据保护条例》第51条。

⑤高秦伟:《论个人信息保护的专责机关》,《法学评论》2021年第6期。

⑥应松年,薛刚凌:《行政组织法研究》,法律出版社2002年版,第11页。

⑦Bharwaney M, Marwah A. "Personal Data Privacy in the Digital Age", *Hong Kong LJ*, 2013(43):801-834.

组织分工形态的最妥当性,促使数据监管权限争议解决内部化,有效降低行政成本和提升组织运行效能。整体监管模式能够克服传统监管模式中独立性、专业性与全局性不足的缺陷,因应数据供给规模化、多元化和数据流通市场化、国际化的需求^①,适应数据安全治理监管的现代化趋势,具备深刻的正当性。

四、数据监管权横向配置重塑的展开

在配置路径上,需要以数据监管任务为导向,在政府职能配置中体现事务的“同质性分工”原理^②,强化网信部门的统筹协调职能,将国家数据局塑造为专门数据监管机构,并实现监管部门之间的高效分工与合作。

(一) 网信部门:强化统筹协调功能

1. 统筹监管部门的监管范围与程序

其一,统筹数据监管权力二次配置方案。明确“相关监督管理工作”的解释权归网信部门,强化网信部门在组织、结构、程序、人员方面的“统筹协调”权能。在数据行业领域借鉴大部制改革经验,实施监管职权相对集中。遵循《国务院行政机构设置和编制管理条例》,应由网信部门统筹拟定数据监管权的二次配置方案,由国务院机构编制管理机关提出具体方案,报国务院决定。譬如,在金融数据领域,网信部门可以推动统筹整合相关部门的金融数据监管权,适度配置给金融监管机构,并与专门数据监管机构做好协调衔接。金融对电子信息技术依赖度极高,数据是金融系统最为核心的资产,数据安全隐患使金融系统变得脆弱,极易引发经济动荡、秩序混乱^③。相较于网信部门,金融监管机构在保护金融消费者合法权益和防控金融数据安全风险方面具有更强的专业监管优势,应由金融监管部门主要负责互联网金融用户信息保护工作^④。具言之,由国家金融监督管理总局统筹负责金融消费者个人信息保护权益和金融集团数据监管,央行和证监会根据各自监管的证券业市场承担相应的重要数据监管职责。

其二,统筹监管职责体系与执法规范。针对现行授权监管职能边界模糊的问题,应重点完善数据安全与个人信息保护的监管制度框架。由网信部门牵头构建协同监管机制,建立跨部门职责清单,明确各机构监管范围、执法权限和救济机制。在数据安全领域,细化动态数据分类标准,实施差异化精准监管,强化风险分级管控。在个人信息保护方面,通过制定配套实施细则,从信息处理标准等实体规范、执法流程等程序规则构建分层监管机制,提升制度执行效能。

2. 协调监管部门的监管职权与冲突

其一,构建以网信部门为核心的双层矛盾协调机制。明确网信部门作为数据监管争议的法定裁决主体,联合相关部门构建全国统一的监管协作框架,明确其具备听取汇报、提出整改指令等法定权限,确保监管争议得到及时有效的处置。在正式协调机制层面,建立专项执法联席会议制度,由网信部门主导协调跨部门执法争议并制定联合行动计划;非正式协调机制层面则通过建立常态化研讨机制,由网信部门组织监管部门定期交流,解决基层执法中出现的普遍性和特殊性问题。

其二,构建执法数据共享机制。欧盟通过升级内部市场信息系统,实现监管机构间高效数据互通,其“一站式”协作模式值得借鉴^⑤。由网信部门牵头构建执法数据信息协同共享平台,建立跨部门数据对接标准,制定分类分级信息共享规范。实施线索双向通报机制,要求各行业监管部门实时上传涉及个人信息及数据安全的违法线索。构建智能分案系统,通过预设的数据分析模型自动匹配监管机构,疑难案件则由网信部门启动多部门联合商会机制,从而形成线索发现—流转处置—协同执法的监管闭环。

①李兴腾,朱敏:《数字中国视域下数据监管的现实困境与完善路径》,《数字经济》2024年第11期。

②宋华琳:《政府职能配置的合理化与法律化》,《中国法律评论》2017年第3期。

③马颜昕:《数字政府:变革与法治》,中国人民大学出版社2021年版,第354页。

④黄志雄:《数据治理的法律逻辑》,武汉大学出版社2021年版,第211页。

⑤De Wachter J, Peeters C. “Advocate General Rules on the One-Stop Shop Mechanism”, *Eur. Data Prot. L. Rev.*, 2021(7): 129–133.

其三,构建综合执法协同机制。“数据处理具有明显的电子化场景性、跨区域性、空间不确定性。”^①数据处理活动所需的扁平化组织趋势与现有科层组织体系相冲突,强化了监管机构执法协调沟通的必要性。因此,在构筑权力衔接协调机制的基础上,注重发挥各监管部门联合决策与执法的优势,构建综合性执法体制,节约行政成本^②。由网信部门牵头健全执法协调联络机制,开展专门、集中的监管执法或整治,有助于高效解决纠纷,抑制监管部门不当的利益冲动,增强企业和个人的法律保护预期。

(二)国家数据局:专门数据监管机构

1.现有专门数据监管机构的构建方案省思

现有方案针对专门数据监管机构的设计众说纷纭,均有一定合理性,但是有违功能适当原则,均非最优的选择。其一,设立完全独立的数据监管机构缺乏制度环境和现实条件。传统的政府监管体制对当前数据监管模式的塑造形成了路径依赖。完全独立的数据监管机构需要健全的行政体制、发达的市场经济与极高的监管标准,这与当前我国科层制下的分业监管土壤存在冲突。数据处理活动场景极为丰富,具有较强的复杂性和专业性,完全依靠单一的数据监管机构可能杯水车薪,无法承担严峻而繁重的监管任务,保持一定的分业监管具备必要性。

其二,于网信部门设立专门数据监管机构的专业性不足。政府监管机构承担政府的职能,应当具有专业监管性^③。国家网信部门的职责定位是负责全国互联网信息内容管理工作及监督管理执法,偏重网络信息内容和意识形态健康治理,并不主要聚焦数据安全、个人信息保护,而且在区县层面缺乏行政执法力量。网信部门囿于自身的职能定位和特点,无法满足数据处理活动的特殊性需求,需要从其主导的传统信息网络安全监管范式中剥离并构造相对独立的数据安全监管体制。

其三,由通信管理局、公安机关、国家安全机关等部门作为专门数据监管机构的主体和能力不适格。工信部门的主要职责为监测工业行业日常运行、推动重大技术装备发展和自主创新,个人信息保护只是其推进信息化建设中非中心职责的延伸,无法合理分化行政监管任务。虽然通信管理局具有个人信息保护相关职权,但是其机构仅设置在省一级,区县、市无通信管理部门。公安机关仅能对违反《中华人民共和国治安管理处罚法》侵犯个人信息的行为进行执法或者对构成犯罪的侵犯公民个人信息的行为立案侦查^④。公安机关和国家安全机关作为维护社会与国家安全的侦查机关,较难以客观中立的态度开展数据监管活动^⑤,不具备承担处置高度的技术性、专门性和复杂性的数据处理活动的基础功能。

其四,设立国家数据保护委员会需要极为丰富的组织资源保障。设立国务院个人信息保护委员会要求通过提升行政级别来实现职能更加明确、机构更加规范、运行更加稳定、组织更加健全的高级组织形态^⑥,实际上是对传统全方位管理和高度集权体制的盲目崇拜,不利于培育真正具有法治精神的专门监管机构。行政资源的有限性决定了增设行政机构或提升独立监管机构行政级别都不可行,这与社会对独立监管机构日益增大的需求产生尖锐对立^⑦。通过攀比行政级别构造的独立监管,不符合数字法治政府的建设目标,长此以往可能会沦为国家机构改革的对象。

2.国家数据局为专门数据监管机构的可行性

功能适当原则要求数据监管任务的实现与组织设置相吻合。将国家数据局塑造为专门数据监管机构契合功能适当原则与整体监管制度框架,具备可行性。

其一,国家数据局与网信部门之间具备良好的内在兼容性。网络数据安全是数据安全的主要领域,《网络数据安全条例》第47条规定的网络数据安全管理制度,对塑造类似数据安全管理制度具有

①王锡锌:《个人信息国家保护义务及展开》,《中国法学》2021年第1期。

②贺荣兰:《政府市场监管权的法律配置及其优化》,《甘肃社会科学》2019年第6期。

③马英娟:《政府监管机构研究》,北京大学出版社2007年版,第33页。

④浙江省杭州市余杭区人民检察院办案组:《以检察公益诉讼促进个人信息长效保护》,《中国检察官》2021年第12期。

⑤郑曦:《刑事诉讼数据处理的全流程监管》,《中国法学》2024年第5期。

⑥黄勇:《论个人信息保护执法机构的设置及其职能》,《山西煤炭管理干部学院学报》2020年第1期。

⑦吴敬琏:《比较(26)》,中信出版社2006年版,第83页。

重要推动作用。近年来在地方数据监管制度的实践探索中,不少地方数据立法条例和规章明确规定数据部门在网信部门的统筹协调下开展数据安全和监督管理工作^①,明确规定由数据部门专责或者牵头负责数据安全监管工作^②。譬如,《广州市数据条例》第42条明确规定数据交易场所如不配合日常监管工作,由市数据主管部门责令改正,并由有权机关对责任人员依法给予处理。这一规定反映了数据部门可能逐步演化为专门数据监管机构的趋势,表明数据局和网信统筹机构之间具备良好的内在兼容度和互补性。国家数据局专责监管数据安全和个人信息保护,有助于网信部门专注履行统筹协调职责、弥补数据监管分散化缺陷和适应数据法规的配置逻辑。

其二,国家数据局具有相对独立性。“独立性是监管机构能否扮演好公共利益维护者角色的关键性因素,是监管机构的核心特征。”^③国家局虽然设立于主管部门之下,但具备监管机构在法律授权、人事、职权、经费来源方面的独立性要件,能够针对特定复杂行业开展科学监管。例如,国家市场监督管理总局管理的国家药品监督管理局能够对药品生产、储存、流通、销售等环节开展有效监督,实现药品领域的良善监管。国家数据局作为国家发展改革委管理的国家局,具有一定客观、中立、超然的特点,由其针对数据这一特定产业领域实施监管,可以提升监管的公正性。国家数据局通过制定科学的监管标准,做出公正的价值分配,有助于规范行使授权性监管职能,推进个人信息保护国际监管交流与合作。

其三,国家数据局专业化程度高。“具有正当性的监管以效率和消费者选择的最大化为目的。”^④国家数据局作为数据产业发展的推动型部门,职责范围包括整合共享和开发利用数字经济和数据资源,相较传统部门更具全局视野,更为熟谙数据处理活动和数字经济发展规律。国家数据局在制定规则、监督执法的过程中,能够更好地实施包容审慎监管理念,更好地平衡数据产业发展和数据执法行为,更好地处理政府与市场的关系。国家数据局通过对数据不当处理行为做出明智、快速地审议与裁决,能够带给社会合理的交代并较好地平息数据产业秩序纠纷^⑤,最大化减少对数据处理活动的不当干预,培育数字经济发展必需的制度环境,进而推动数字经济规范与发展并重。

需要指出的是,国家数据局作为统筹数据基础制度建设的政策制定部门,在有利于实施包容性监管职能的同时,可能存在与监管职能相混合的不足。如果政策职能与监管职能过于聚集,则容易受到利益部门的牵制与影响,可能导致政监不分、政事不分,有损政府监管威信,进而动摇市场投资者的信心。因此,需要扬长避短,于监管配置上进行精巧的平衡。

3. 国家数据局专门数据监管权的配置

《网络数据安全管理条例》仅规定了国家数据管理部门的网络数据安全职责,配置其行政检查权、要求暂停和整改权,但并未赋予其数据监管的行政处罚等权限。基于数据违法行为的特殊性,监管与执法之间难以分割。数据违法行为从研判、认定、发现、处置到反馈环环相扣,需要前端政策制定、日常监管部门与后端执法部门密切协作。如果监管权与执法权分割,行业主管部门缺位和退出,将导致后端执法部门陷入“孤立无援”“独木难支”的境地^⑥。欧盟《通用数据保护条例》赋予独立监管机构调查权、矫正权、干预权、行政处罚权等诸多权力^⑦。需明确国家数据管理部门为国家数据局,将分散于网信、工信等部门的数据安全、个人信息保护的执法权适当配置给国家数据局,健全其监管职权。

其一,坚持监管职能与政策职能适度分离的原则,于国家数据局内部设立数据监管司。数据监管司秉持客观公正性,依法独立开展监管,不受任何行政机关、团体和个人的干涉,但是并不意味着与政策部

①参见《江苏省数据条例》第64条等。

②参见《贵州省数据流通交易促进条例》第34条、《新疆维吾尔自治区数据条例》第5条、《广州市数据条例》第3条和第42条、《太原市大数据发展促进条例》第5条、《青岛市公共数据管理办法》第41条等。

③马英娟:《政府监管机构研究》,北京大学出版社2007年版,第34页。

④托尼·普罗瑟:《政府监管的新视野:英国监管机构十大样本考察》,马英娟、张浩译,孙娟娟、苏苗罕校,译林出版社2020年版,第15—16页。

⑤马英娟:《政府监管机构研究》,北京大学出版社2007年版,第34页。

⑥骆梅英,黄柳建:《市场监管综合行政执法改革中的权限配置》,《苏州大学学报(哲学社会科学版)》2021年第6期。

⑦参见《通用数据保护条例》第58条。

门等主体毫无瓜葛。一方面,数据监管司应与国家数据局内外部宏观政策制定部门以及相关从业者、各种利益团体有所区隔并保持适当距离,免于各方面的不当干预,不被个别利益或好恶所围猎与俘获,如规范监管机构负责人任免程序,建立独立预算保障机制,明确监管人员任职资格并建立离职从业限制制度。另一方面,监管过程难免涉及数据监管标准、检查与执行等监管政策的制定,因此数据监管司需要畅通与政策部门等主体的沟通交流机制,能够广纳各方合理意见并接受公众监督,确保监管与决策过程的透明化公开化,避免因监管机构的独立造成行政系统的封闭、混乱乃至政策协调实施的不切实际。

其二,配置专业化的监管队伍,丰富监管的灵活性。监管队伍涉及社会、技术、法律和经济多专业领域,需要提升自主性与专业化程度,以适应数字经济环境与数据处理活动场景的变化。

其三,赋予国家数据局规则制定、行政执法与争议调处职能。明确其主导制定数据跨境流动等规则制定的权限,提升政策稳定性与公信力。强化数据处理全流程审查监管权,通过细化裁量权行使标准和技术指南防范监管权力滥用。完善争议解决机制,建立专业数据行政复议委员会,健全行政申诉与司法救济衔接程序,保障公民的救济权利。

其四,规范国家数据局的责任配置。明确监管目标、工作流程、监督机制和绩效评估等问责指标,实现其监管权责配置清晰。国家数据局需要对其监管行为的合法性、正当性与科学性承担法律及技术责任,在保持职能相对独立性的同时建立权力制约机制,防止监管失范或技术垄断导致的权力异化问题。当配置条件逐步成熟时,将由国家发展改革委管理的国家数据局调整为国务院直属机构,强化其专门监管职责。

此外,就网信部门和国家数据局的角色关系而言,网信部门行使统筹数据相关法律政策的制定完善与监督落实职能,国家数据局进行数据监管和负责数据相关政策的制定、协调和实施。针对重大决策和跨领域协同监管事项,网信部门发挥统筹协调功能,构建跨部门联合执法协同机制。在国家数据局及其他监管部门在数据监管政策的制定、实施过程中,由国家网信部门进行统筹协调,以免政策执行“各自为政”。国家网信部门尊重国家数据局的日常监管权,避免介入微观执法,而在涉及数据安全底线与系统性风险处置时,则须通过顶层把控和政策校准实施战略性指导,实现监管效能与专业自主的动态平衡。

(三) 其他监管部门:分业监管的边界与合作

1. 厘清专门监管与分业监管的关系

“从提高效率的角度考虑,权责配置的理想状态是将管辖权配置给符合条件的唯一部门,实现同一事项同一部门管辖。”^①基于数据监管事务涉及的专业知识和信息的多质性,理想配置状态无法在所有数据事项领域中统一实现,一定程度的分业监管具备现实性与必要性。国家数据局作为具有全局视野的专门数据监管机构,定位为侧重对全局性数据风险的控制,也在行为监管上对数据安全、个人信息保护进行统一执法。专门监管并不意味着对各个领域中的数据事项展开完全监管。专门监管与数据法律所设定的分业监管并不必然冲突。

进言之,国家数据局作为基础性监管主体,统筹实施数据安全、个人信息保护等一般性监管规则,开展多领域常态化执法。各行业主管部门则基于产业特性制定专项数据治理规范,履行垂直领域监管职能。针对刑事侦查、国家安全等高敏感场景,则由公安、国安机关依法行使数据安全监管权,地方及部门严格落实属地、属事管理责任。因此,需要处置好国家数据局与分业监管部门之间的张力,构建国家数据局与分业监管部门的职权衔接与沟通机制,明晰国家数据局与分业监管部门的监管事权和监管范围边界,避免监管空白或监管重叠。对于国家数据局与分业监管部门之间出现的争议,必要时由国家网信办统筹协调解决。

2. 构建分业监管的合作机制

其一,类型化构建统一监管原则和制度规则。例如,网信部门与国家数据局在国家标准《信息安全技术 个人信息安全规范》的基础上,可以统筹相关主管部门制定类型化、场景化的个人信息保护规则和

^①朱新力,余军:《行政法视域下权力清单制度的重构》,《中国社会科学》2018年第4期。

标准,构建个人信息保护执法裁量基准制度。其二,构建跨行业、跨部门、跨区域的协同监管机制。数据行业监管包括对行业内的数据收集、使用、流通的监管职能,涉及数据收集、处理、存储、传输和共享等环节。政府监管实践中促进部门间的沟通与协调有利于部门间的信息共享与高效协作,实现综合治理^①。《贵州省数据流通交易促进条例》第34条规定体现了对该类监管机制的尝试,通过建立健全数据流通交易跨部门协同监管机制,提升防范与应对数据流通交易风险的系统性和专业性。其三,构建数据分业监管和专门监管相结合的监管机制。行业监管可能忽视数据生产要素的市场属性,不当的监管措施容易产生反市场偏误和行业垄断问题,而专门监管侧重全局性监管,可能容易忽视数据的其他价值。因此,需要构建数据分业监管与专门监管相结合的监管机制,以实现推动数据产业发展与维持市场公平竞争秩序之间的平衡。

结语

在行政组织法和监管改革的背景下,面对大数据、人工智能等新兴领域的挑战与发展,需要深刻检视传统数据监管权横向配置的弊端,构建“网信统筹+专门监管+分业监管”的横向配置结构,以实现公民数据权益保障与政府权力规范行使的平衡。本文从横向层面对于如何优化数据监管权的配置做了初步探讨。欲真正实现数据领域的良善监管,还需理论界与实务界努力从纵向层面研究并厘清数据监管权在不同层级政府之间所进行的分配问题。

Reflection and Restructuring of the Horizontal Allocation of Data Regulatory Authority

LIU Quan & LIAO Jialin

(School of Law, Central University of Finance and Economics, Beijing 100081, China)

Abstract: Article 47 of *The Network Data Security Management Regulations* stipulates that defining the cybersecurity data oversight responsibilities of national data management authorities helps optimize the horizontal allocation of regulatory powers, yet fails to fundamentally resolve the inherent drawbacks of the traditional “cybersecurity coordination+sectoral regulation” framework. The conventional horizontal allocation of data governance authority suffers from issues such as excessive fragmentation and overlapping jurisdictions. These deficiencies not only increase unnecessary regulatory costs but also lead to over-regulation or regulatory gaps, demonstrating limitations in addressing the uncertainties of the digital economy and the unique nature of data processing activities. This traditional governance structure contravenes the principle of functional appropriateness, necessitating the establishment of a refined “cybersecurity coordination + specialized oversight + sectoral regulation” framework. Specifically, this entails strengthening the cyberspace administration’s coordinating role to resolve jurisdictional conflicts, establishing the National Data Administration as a specialized regulator to ensure independence and holistic oversight, and clarifying departmental responsibilities under sectoral regulation to achieve coordinated governance through division of labor and collaboration.

Key words: data security; National Data Administration; data regulatory authority; personal information protection; the Principle of Distribution of the State Powers

(责任校对 曾小明)

^①和军,杨慧:《ChatGPT类生成式人工智能监管的国际比较与借鉴》,《湖南科技大学学报(社会科学版)》2023年第6期。