·经济学研究·

DOI:10.20004/j.cnki.ujn.2024.02.007

数字经济背景下公共数据开放安全治理

李晓楠

(郑州大学 法学院,河南 郑州,450001)

[摘　要]公共数据类别多元化、开放方式多样性与普惠性要求与数据安全治理具有天然的紧张冲突。当前公共数据开放安全治理存在多重局限,包括强调公共部门而忽视社会主体的安全治理责任,安全保护义务的宣示化,技术规范的缺失,难以满足公共数据要素化下的安全治理需求。从消解公共数据开放与安全的冲突出发,针对公共数据开放的特征应注重回应性的安全治理。在方法论上强调合作治理、比例治理和技术治理;在治理机制上注重从公共数据梯度开放、安全义务的比例分配、技术治理的规范保障与安全合作治理的机制跟进等方面进行适应性的完善。

[关键词]公共数据开放;促进型行政;场景理论;数据安全

[中图分类号]F49;D912.29　　[文献标识码]A　　[文章编号]1671-3842(2024)02-0075-11

一、问题的提出

公共数据是国家机关、法律法规规章授权的具有管理公共事务职能的组织以及供水、供电、公共交通等公共服务运营单位,在依法履行职责或提供公共服务过程中收集、产生的数据①。公共数据开放即指向自然人、法人或者非法人组织依法提供公共数据的公共服务行为。2022年4月19日,中央全面深化改革委员会审议通过《关于加强数字政府建设的指导意见》,提出编制公共数据开放目录及相关责任清单,构建统一规范、互联互通、安全可控的国家公共数据开放平台,分类分级开放公共数据,有序推动公共数据资源开发利用,提升各行业各领域运用公共数据推动经济社会发展的能力。2022年12月19日,《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》(以下简称《数据二十条》)提出,要加强对各级党政机关、企事业单位依法履职或提供公共服务过程中产生的公共数据的汇聚共享和开放开发。由此可见,公共数据开放已成为激发数据价值,推动数字经济高质量发展的重要组成部分②。

然而,公共数据开放与安全之间存在天然的紧张冲突关系,数据开放扩大了数据风险敞口,可能诱发数据泄露风险、数据恶意破坏风险、数据违规使用风险和个人信息保护风险,威胁国家安全、经济安全和隐私安全。实践中就存在政府信息公开网站未对数据主体的敏感信息如医疗救助

[基金项目]司法部2022年度法治建设与法学理论研究部级科研项目"场景理论下数据出境安全监管规则研究"(项目编号:22SFB4028);2023年度河南省法学会研究课题"数字经济背景下国际金融服务法律治理研究"(项目编号:HNLS2023A10);郑州大学2024—2025年"双一流"建设项目"数字治理与中国式法治现代化"(项目编号:2024GJ020400039)。

[作者简介]李晓楠,郑州大学法学院经济法研究中心研究人员,法学博士后,邮箱:540356466@qq.com。

①冯洋:《公共数据授权运营的行政许可属性与制度建构方向》,《电子政务》,2023年第6期。

②张蕴萍,董超,栾菁:《数字经济推动经济高质量发展的作用机制研究——基于省级面板数据的证据》,《济南大学学报》(社会科学版),2021年第5期。

对象的住址、病情等进行脱敏处理,导致政务公开与个人隐私保护的冲突[①];“柠檬查”涉嫌垄断从全国车险信息平台获取的车险数据,破坏市场有效竞争[②];我国国内网络包括部分高校的网站近年来多次受到境外机构如美国国家安全局“特定入侵行动办公室”的网络攻击,被窃取的数据量超过140GB,损害了国家安全利益。里约热内卢政府系统超420GB的公共数据被黑客窃取,并面临着泄露数据的威胁。数据安全是公共数据开放的前提和条件,应始终“紧绷数据安全这根弦”。但公共数据具有数据类型多样、开放方式多维、开放参与主体多元等特征,显著增加了公共数据开放下的数据安全治理复杂度。

当前学界对公共数据开放背景下的数据安全治理研究仍处于初始阶段,且国内外学者的研究视角存在差异。国内学者侧重于对策性研究,或者从现象、原因到方案的线性思路,提出了公共数据开放中的安全风险防范策略[③]。或者直接从对策入手或聚焦于隐私保护,提出了完善数据安全保护制度的思路[④]。但普遍未充分结合公共数据开放的特殊场景,缺乏针对性。国外学者则多从“公共部门信息开放”的特征入手,将公平信息原则或个人数据保护规则等融入公共数据开放的安全治理当中[⑤],但更多聚焦于其本国的实践,难以直接为我国的公共数据开放安全治理所用。本文则从公共数据开放的特定场景入手,在厘清公共数据开放与数据安全紧张冲突的逻辑关系基础上,借鉴域外相关治理经验,并结合我国数据安全治理的立法和监管实践,有针对性地提出公共数据开放安全治理的完善路径,既弥补了当前研究的局限,又服务于公共数据开放安全治理实践。

二、公共数据开放与安全治理的紧张冲突

(一)公共数据多样化特征提高安全治理复杂度

从安全维度出发,以数据遭到篡改、破坏、泄露或非法获取、利用,对国家安全、公共利益或者个人、组织合法权益等造成的危害程度,可将数据区分为一般数据、重要数据和核心数据三类[⑥]。科层制社会治理结构下,公共部门构成了社会有效运行的关键环节,而公共数据作为公共部门履行管理职责或提供服务的“附带产品”,几乎涵盖了以上所有的数据类型。例如,全国车险信息平台依职能收集的车险承保、理赔数据等可能归于一般数据;医疗机构在提供医疗服务过程中掌握的个人尤其是政治人物的健康信息就可能隶属于重要数据或核心数据。其他诸如行业发展数据、企业经营数据、交通数据、地理数据等,既可能属于一般数据,又可能属于重要数据或核心数据[⑦]。

公共数据的多样性显著增加了数据安全管控的难度。一是,不同种类和量级的数据可能表征差异化的利益,包括国家安全、公共利益和经济价值等,并最终体现为差异化的安全治理策略。具言之,依据“风险为本”的治理原则,难以“一刀切”的对所有类型或数量级的公共数据适用一套完全通用的治理工具。与国家安全和公共利益密切关联的公共数据开放通常会受到更为严格的管

①吴姗,甄子锐:《政府网站泄露隐私受关注 各地整改升级保护机制》,https://www.rmzxb.com.cn/c/2017-12-05/1888996.shtml,2023.10.23.

②苑苏文:《中国超2.7亿车购买商业险,你的车险信息或正在被滥用》,https://www.chinanews.com.cn/cj/2022/11-15/9894687.shtml,2023.10.23.

③肖冬梅,苏莹:《我国政府数据开放中的安全风险及其防范对策》,《现代情报》,2022年第6期。

④宋华琳,郑琛:《论政府数据开放中的数据安全保护制度》,《中国司法》,2022年第3期。

⑤FREDERIK Z. B., JONATHAN G., MIREILLE V. E., Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework, *Berkeley Technology Law Journal*, Vol. 30, No. 2, 2015, p. 2073.

⑥张敏,魏伟,谭天怡等:《数据分类分级及其发展路径研究》,《网络安全与数据治理》,2022年第7期。

⑦李晓楠,宋阳:《国家安全视域下数据出境审查规则研究》,《情报杂志》,2021年第10期。

控;个人隐私数据开放较之于企业经营数据开放又会受到额外的安全规制。如何针对不同的数据类型配备适应性的安全治理规则,进而实现层次化的精细治理,构成了公共数据开放安全治理的挑战。二是,公共数据的类型存在转化的可能,一般数据存在因数量级变化或数据处理技术介入而转化为重要数据或核心数据的可能,致使公共数据开放安全治理既要关注数据自身的性质,又要针对数据量级作出回应,还要对数据处理行为作出规范,提升了安全治理的复杂度。

(二)公共数据开放的普惠性增加数据安全控制难度

公共数据开放具有普惠性特征,即符合一定条件的社会主体均可以利用公共数据,以使公共数据利益惠及社会大众,实现公共数据"取之于民,用之于民"。如果说公共数据种类多样化带来的安全治理挑战来源于公共数据的利用端,那么公共数据开放的普惠性就是从数据利用端出发的安全治理挑战观察,并主要表现为以下两个方面:

一是公共数据开放的普惠性意味着利用主体的多样化和普遍化,要求厘清公共数据开放过程中所涉不同主体的安全保护义务[①]。由于数据利用主体的多元性及利用目的的差异性,需要依据不同的利用目的对不同的数据利用主体确立有区别的安全保护义务。例如,相较于商业目的,出于公益目的的公共数据利用主体可能部分豁免数据用于"指定目标"的限制,以在隐私保护与公共利益之间达成平衡。又如,相较于大型平台企业,中小企业、组织或者个人作为公共数据利用主体在数据安全管理和技术保障能力上显著不足,如果设置相同的安全义务,或者导致难以全面落实而形成安全保护漏洞,或者实质阻碍公共数据开放普惠性的实现。但差异化的安全义务治理模式,必然加大了规则制定的难度。

二是公共数据开放的普惠性意味公共部门通常并不从数据开放中获取额外经济利益[②]。例如欧盟2019年《开放数据和公共部门信息复用的指令》规定用户可以免费对高价值数据集和(受到公共资助的科学研究活动所产生的)研究数据开发利用;其《数据治理法案》规定了公共部门可以以不高于成本的价格收取相关数据提供的费用,收费设置应当合理、透明、公开且无歧视。尽管公共部门固有的"利他主义"本质,其义务的配置不是基于利益而是基于职权,但在公共数据开放具备对外赋能作用的情况下,如果要求公共部门与公共数据利用主体承担同等的数据安全治理义务就可能存在过度增加公共部门负担、导致利益失衡问题。但如果弱化公共部门的数据安全治理责任又将导致公共数据开放安全源头治理缺失,不符合数据全生命周期安全的原则性要求。为此,在强调公共部门规制职能的传统安全治理模式下,如何在公共数据开放普惠性与公共部门安全管理责任之间进行平衡,无疑构成了治理效能的挑战。

(三)公共数据开放模式挑战安全治理能力

公共数据开放的内容包括数据资源和数据服务,开放的方式包括场内方式和场外方式[③]。尽管当前公共数据开放模式还处于探索阶段,但总体体现出两个趋势。一是开放公共数据资源到开放公共数据服务的内容转变。《数据二十条》明确鼓励公共数据按照"原始数据不出域、数据可用不可见"的要求,以模型、核验等产品和服务等形式向社会提供,以保障个人隐私和公共安全。广州市数据交易所完成的首个公共数据运营产品"企业经营健康指数"即是将公共部门掌握的企业经营数据进行隐私保护计算后加工而成的数据产品。二是开放的方式从场外向场内转变。当前各地数据交易所如上海数据交易所、北京数据交易所等也纷纷上线公共数据产品,而公共数据利用方直接从公共部门或其授权的运营机构处获取公共数据的情形则较为少见。

---

①RAZVAN D. , Policy Recommendation Regarding the Interface between the Protection of Commercial Secrecy and the Re-use of Public Sector Information, *Masaryk University Journal of Law and Technology*, Vol. 6, No. 3, 2013, p. 321.

②刘语,曾燕:《论有偿使用制度推动公共数据开放发展》,《西安交通大学学报》(社会科学版),2023年第4期。

③江小涓:《数据交易与数据交互》,https://new. qq. com/rain/a/20231127A06KJT00, 2023. 12. 05.

尽管公共数据服务化和场内交易更利于安全的标准化管控,但也至少在两方面对数据安全治理带来了挑战。一是,公共数据开放要求公共部门或其授权部门具备较强的数据安全处理能力。具言之,在公共数据服务化的场景下,公共部门首先对数据进行安全计算技术处理形成密文"计算因子",公共数据运营机构则以密文"计算因子"为基础应用特定算法进行融合计算,最终由数据商进一步开发成进场交易的公共数据产品。但是公共部门自身通常缺乏数字技术能力以应对层出不穷的数据安全风险,如何实现治理转型无疑成为新挑战。二是,场内交易模式下,公共数据开放流程变得更为冗长。公共数据开放不再是公共部门—数据利用主体之间的直接流转,而是可能表现为公共部门—授权运营机构—数据商—数据利用主体之间的多环节流动,自然考验着数据安全的多流程管控能力。

三、公共数据开放安全治理的当前局限

目前我国公共数据开放安全治理还呈现出"实践先行、立法滞后、文件治理、政策推动"的特征。在国家层面主要通过《数据安全法》《个人信息保护法》《政务信息资源共享管理暂行办法》等规范进行公共数据开放安全治理。在地方层面如河南省、江西省、上海市等也逐步制定了地方公共数据安全的规范性的文件,探索公共数据开放安全治理的地方实践。综合来看,现有的安全治理还存在强调公共部门义务而弱化合作治理、数据开放安全规则缺位、技术规制工具不足的局限,难以应对公共数据开放背景下的数据安全问题。

(一)强调公共部门而忽视社会主体的安全治理责任

现有公共数据开放安全治理通常强调公共部门的数据安全保护义务,而忽视社会主体的治理参与。例如《数据安全法》第五章"政务数据安全与开放"中主要规定了国家机关的保密义务以及安全保护责任。又如《政务信息资源共享管理暂行办法》尽管确立了"谁经手,谁使用,谁管理,谁负责"的政府信息管理原则,但其适用对象也仅仅局限为政府部门。再如地方性规范《河南省政务数据安全管理暂行办法》尽管确立了"谁使用谁负责"的原则,但也主要局限于政府或其相关部门确定的政务信息系统建设、运维运营等单位。还如《上海市公共数据开放暂行办法》在谈及数据安全保护时着重强调政府及其相关部门的管理义务,尽管试图通过将安全保障条件融入开放条件、明确开放平台的安全管理责任等方式尽可能的将利益关系主体纳入安全治理体系,但主要还是将非公主体作为被动接受治理的对象。

尽管《个人信息保护法》《数据安全法》通过"数据处理者"的概念可以将数据安全保护的内部的风险管理机制如制定内部管理制度和操作规程、权限管理和安全教育、制定并实施应急预案等加诸公共数据开放的广泛利益关系主体,似可弥补社会主体数据安全治理的缺位和不足。但"场景理论"已经表明数据安全保护应当与具体的社会交互关系相适应,将数据安全的一般治理要求施加于公共数据开放下的相关社会主体或者导致权利义务失衡,或者导致安全治理漏洞,而无论哪一种都会造成公共数据开放整体社会价值的减损[①]。

(二)公共数据安全保护义务的宣示化

现有公共数据开放安全治理存在安全义务原则化、抽象化的问题,导致难以落实和监督。以公共部门的数据安全保护义务为例,《数据安全法》《政务信息资源共享管理暂行办法》等规范也仅仅表现出更多的宣示意义,并不具有较强的操作意义。例如《数据安全法》在"政务数据安全与开

①HELEN N. ,Privacy as Contextual Integrity,*Washington Law Review*, Vol. 79,No. 1,2004,p. 119.

放”一章下也仅仅是笼统地规定了国家机关应当按照法律和行政法规的规定建立数据安全管理制度，落实安全保护责任，保障政务数据安全。又如《政务信息资源共享管理暂行办法》在“共享信息的提供与适用”和“信息共享工作的监督和保障”等章节中也只是原则性地提出数据安全保护要求，即国家机关加强共享信息使用的全过程管理，国家网信办建立政府信息资源共享网络安全管理机制，共享平台管理单位要加强公共数据共享交换时的安全防护等。但数据安全管理义务的具体细节却并未过多涉及。

这种数据安全保护义务的宣示化固然可以增强相关条款的包容性和张力，但同样可能导致责任主体难以精准履行安全保护义务，难以实现不同场景下的风险精细化管理，并给责任归结带来依据不足的困境。即便是《数据安全法》《个人信息保护法》已对政府信息安全作出规制的情况下，依然存在政府信息泄露等侵犯个人隐私和商业秘密的行为，有地方政府网站的负责人就认为主要是因为现有规范不够明确具体，基层往往难以精准把握和操作落实[①]。对于非公共主体包括数据利用主体、数据经济人、数商和数据交易所等固然也可以准用《数据安全法》《个人信息保护法》下的一般安全义务如数据分类管理、数据加密或脱敏等，但在公共数据开放的场景下，仍未解决不同参与主体的安全义务精细化分配问题，且缺乏整体和系统化的治理视角。为此，有学者认为应加强公共数据开放领域的专门安全立法，明确数据安全保护标准，强化不同主体间的安全义务的适应性分配与协调[②]。

（三）公共数据安全技术规范缺失

现有涉及公共数据开放下的数据安全治理偏向于通过社会规范进行，而忽视技术规范的跟进和融合。具体来说，《数据安全法》《政务信息资源共享管理暂行办法》等规范在数据安全治理上依然采取的是义务—责任的传统人防模式，也即给相关主体包括公共部门、平台运营者、数据利用主体等施加一定的数据安全保护义务，并通过责任追究督促义务的落实。此种以关键人为对象的治理方式在社会交互关系较为简单的场景下基本满足了治理需要，原因在于关键人往往在社会交互的风险预防和控制上发挥着主导作用，通过对行为人的苛迫使行为人进行负责任的安全治理，最终达到社会秩序的稳定。但在公共数据开放场景下，仅仅通过人防难以实现数据安全治理目标。

一是在数据开放的全生命周期中，后一流程的数据安全依赖前一流程的数据处理，公共数据的流转又依赖安全的数字环境，不同参与主体的安全责任往往具有重叠性，在安全事故发生时难以准确厘清[③]。即便可以通过精确的义务分配廓清不同参与主体的安全义务边界和内容，但责任固有的事后性救济特征也难以弥合国家安全、公共利益和个人隐私利益的损害。二是公共数据开放下的数据流转过程介入了技术因素，单纯依靠社会规范本就难以实现预期的治理效果。尽管《数据安全法》明确了国家推动数据安全标准的体系化建设，实际上构成了技术标准安全治理的法律依据，但对为何进行技术标准治理、技术标准的具体内容、技术标准如何与法律规范对接等问题却鲜有提及。虽然部分地方已经陆续出台了公共数据安全的技术标准，如北京市的地方标准《政务数据分级与安全保护规范》、深圳市的地方标准《公共数据安全要求》，但一方面不能完全适用于公共数据开放的场景，另一方面也造成了规制的碎片化，亟需体系化和系统化。

---

①吴姗，甄子锐：《政府网站泄露隐私受关注 各地整改升级保护机制》，https://www.rmzxb.com.cn/c/2017-12-05/1888996.shtml，2023.10.23.

②庄国波，韩惠：《5G时代政府数据开放共享的安全风险及防范》，《理论探讨》，2020年第5期；戚建刚，兰皓翔：《基层治理视角下的知识产权行政保护能力研究——以机构改革后湖北省W市13个区的市场监管局为样本》，《北京行政学院学报》，2022年第2期。

③张勇进，章美林：《政务信息系统整合共享：历程、经验与方向》，《中国行政管理》，2018年第3期。

四、公共数据开放安全治理的回应性逻辑

现有规范层面体现的公共数据开放安全治理局限实际上反映了治理理念上的偏差。在数字技术变革带来的社会生产关系破坏性创新下,风险社会的复杂性、不确定性进一步加剧,公共数据开放下的安全问题正是风险社会在特定情景下的反映。从风险社会的回应性规制出发,公共数据开放安全治理在组织上应强化合作治理,在规则上应强化层次性和适应性,在工具上应注重主动性和预测性,以化解公共数据开放与数据安全的紧张冲突[①]。

(一)公共数据开放安全的合作治理

合作治理强调利益相关方的治理参与和互动,从而与强调公共部门的监管权力及被监管对象的服从的传统治理模式相区别。合作治理主要体现为公共部门与非政府部门共同制定、执行公共政策,管理公共事务的治理安排[②]。合作治理倡导治理与被治理者之间的角色融合,将单一的线性权力治理转化为多元的分布式治理,强调社会主体的治理介入。合作治理下,行政权力的外向功能受到削弱,而由自我规制以及社会监督进行补强,以应对政府和市场的双重失灵困境[③]。

在公共数据开放的场景下,通过合作治理实现公共数据的安全保障有其内在逻辑。首先,利益平衡考量下需要合作治理。公共数据开放具有普惠性的特征,让公共数据供给端即公共部门承担过重的数据安全保障义务就可能导致利益失衡。而合作治理所立基的特定互惠性目标,在公共数据开放中恰恰存在。一方面公共数据利用主体从公共数据开放中获得了经济利益,另一方面公共数据供给主体通过数据开放促成了服务型政府的建设,在促进数据利用主体利益实现的同时又反射地实现了自身的行政利益。其次,公共数据开放的模式也要求合作治理。公共数据开放的全生命周期中涉及多类性质不同的主体,既包括传统的公共部门,也包括准公共部门如公共数据授权运营机构,还包括数据利用主体、数据中介,合作治理有助于充分调动参与主体的治理潜能,弥补公共部门在人才、技术、财政等方面的约束,还有助于提升治理的透明度和效能[④]。

从国际经验看,合作治理已经成为公共数据开放安全的普遍选择。一方面,公共部门积极与公共数据开放流程外的社会主体进行安全合作,如美国政府与Code For America等组织合作举办“公民黑客日”等活动,充分利用社会技术力量为美国当前面临的各类挑战包括政务数据安全问题提供解决方案[⑤]。另一方面,充分发挥数据开放平台、数据中介等的安全治理职能。如欧盟为解决安全可信的公共数据共享,一方面依托统一的公共数据开放平台,构建确保数据安全交换的技术环境和治理机制,另一方面通过数据中介机构如数据交易结算所、数据商、第三方专业服务机构采取适当的技术、组织和法律措施,确保数据的存储和传输的高度安全性[⑥]。

(二)公共数据开放安全的比例治理

比例治理倡导所采取的措施与所欲达成的目的之间应当相称。尽管脱胎于行政法,更多是用来限制行政权力,但随着治理对象复杂性的不断提升,比例治理兼具精细化治理的意味,并暗含着不同对象差异化治理的思维逻辑。从比较的视角看,比例治理与“以风险为本”的治理方法也有共通之处,强调根据不同场景下风险的大小采取符合比例的治理措施。

在公共数据开放场景下,通过比例治理实现公共数据安全有其自身的逻辑。首先,比例治理

①杨炳霖:《回应性监管理论述评:精髓与问题》,《中国行政管理》,2017年第4期。

②徐国冲:《合作治理研究的理论脉络及其发展》,《厦门大学学报》(哲学社会科学版),2022年第6期。

③王伟:《数字经济治理体系的运行逻辑——以合作治理为视角的考察》,《电子政务》,2023年第10期。

④贾开:《数字治理的反思与改革研究:三重分离、计算性争论与治理融合创新》,《电子政务》,2020年第5期。

⑤黄如花,陈阅:《美国政府数据开放共享的合作模式》,《图书情报工作》,2016年第19期。

⑥王轶:《欧盟促进公共数据流通利用四大机制和特点趋势》,《数字经济》,2023年第Z2期。

有助于厘清不同主体的义务边界，实现有差别的共同责任。例如欧盟GDPR在序言中就明确，保护个人数据不是一项绝对的权利，必须依据比例原则考虑其社会功能以及与其他基本权利的平衡。这里的比例原则实际上就是要求在施加保护数据安全义务时，应当针对具体的场景，进行多种利益或价值的衡量，避免权利（力）义务、成本与收益之间的不平衡。具体反映到公共数据开放下，一是要处理好数据开放与数据保护的关系，避免为了数据保护而过度限制开放；二是在公共数据开放链条不同主体间分配数据保护义务时应当考虑不同主体的权利义务平衡，避免一刀切的要求，实现保护义务、保护能力、利用利益等多重要素的平衡。

其次，比例治理有助于指导精细化管理，促进义务的遵守和落实。比例治理要求不同场景下主体的差别义务本身就表明数据安全治理由原则性的规定走向了具体细节。这些可操作性的规则可能通过公共数据安全的具体指南、标准等体现。例如工信部就发布了《车联网网络安全和数据安全标准体系建设指南》，构成车联网场景下数据安全治理的具体遵循。尽管目前在国家层面上还未有针对公共数据开放下的安全指南或标准，但在比例治理理念下，具有可操作性的规则体系已经成为治理的必然选择。实际上地方性规范如《江苏省公共数据开放与安全管理细则》《浙江省公共数据开放与安全管理暂行办法》已经区分公共数据开放主体与利用主体分别确立了监督管理义务与合规利用义务。规则的精细化对于公共数据的利用者来说，有利于对照实施，以避免安全责任；对于公共数据开放安全的监管者来说，又可以便于监督的落实。

（三）公共数据开放安全的技术治理

在数据安全的治理中，“技术治理”与“法律治理”的结合已经成为应对公共数据开放安全风险的基本方法[①]。与法律治理偏向于调整人与人之间的行为关系不同，技术治理偏向于调整技术与行为之间的关系，通过特定技术的部署和应用实现公共数据安全。技术治理强调通过数据安全技术如匿名化处理技术、加密技术、AI智能检测为公共数据开放提供安全可信的环境。例如我国采用“数据安全沙箱”，确保“公共数据不出域”“数据可用不可见”，满足公共数据运营单位对外安全供数。欧盟GDPR提出“经过设计的数据保护”，强调将技术措施集成到数据处理活动中，实现全生命周期的数据保护。

从公共数据开放的全生命周期安全出发，技术治理至少应当包括以下三个方面。一是公共数据的静态安全技术治理，也即通过技术保障公共数据的存储安全，构成了公共数据安全开放的环境基础。二是公共数据的处理安全技术治理，也即从原始公共数据到公共数据产品形态转换过程中的技术安全，构成了公共数据安全。三是公共数据的交换安全技术治理，也即公共数据对外交互的环节的技术安全。从技术内容出发，技术治理至少应包括以下五个方面。一是可信计算技术，公共数据开放（交易）平台应以可信计算基（TCB）为基础，实现软硬件计算资源可信，营造可信的公共数据开放流程控制链。二是强制访问控制，数据开放或交易平台在通信网络、操作系统、应用系统各方面实现访问控制标记和策略，实现不同访问控制点之间的访问控制关联。三是审计追查技术，公共数据开放或交易平台应建立事件分析模型，发现并追查威胁路径、定位威胁源头，有效防范和应对攻击行为。四是数据安全处理技术，公共数据授权运营主体、数商等对外提供公共数据时应当通过技术处理保证数据不可被篡改和非法获取。五是多级互联技术，即在不破坏公共数据开放平台、公共数据授权运营平台、交易平台正常安全的前提下，实现不同级别安全主体之间的安全互联。当然这里的安全技术应与被保护对象的安全风险等级匹配，在通用安全技术要求外，可以针对高级别安全风险对象额外采用安全扩展技术要求。

①鲍静，张勇进：《政府部门数据治理：一个亟需回应的基本问题》，《中国行政管理》，2017年第4期。

五、公共数据开放安全治理的机制完善

(一)公共数据分级下的安全有序开放

公共数据分级是基于数据发生泄漏、篡改、丢失或滥用后的影响对象包括国家安全、公共利益、个人和其他组织利益,影响程度包括一般影响、严重影响和特别严重影响,影响范围包括较小范围、较大范围、强可控、弱可控,进行的综合判断后,安全风险由小到大可分为一至四级。公共数据分级是公共数据类别多样化的必然要求,也是公共数据开放安全治理的基础,决定了哪些数据可以开放、以什么方式及要求进行开放等[①]。

就哪些公共数据可以开放而言,《数据安全法》已规定了国家应制定政务数据开放目录。实践中一般将公共数据区分为无条件开放类、受限开放类和禁止开放类三类。禁止开放类通常包括国家秘密,可能危及国家安全、公共安全、经济安全与社会稳定的数据,涉及商业秘密、知识产权或获取协议保护、个人隐私的数据。当然,部分禁止开放类数据经过脱敏、脱密等技术处理可以转化为受限或无条件开放类数据。受限开放类数据通常包括经过权利人同意开放的涉及商业秘密、个人信息的数据,开放将严重挤占基础设施资源,开放后预计带来特别显著的经济效益但安全风险难以评估的。无条件开放数据则是除了禁止开放类和受限开放类外的其他公共数据。

从域外实践看,美国《联邦信息和信息系统安全分类标准》根据保密性、完整性、有效性等要素对公共数据进行了细分,以确定不同的访问级别或条件。并针对虽不属于国家秘密但应受到一定信息安全措施保护的联邦公共数据专门制定了名为《受控非密信息》的行政令,并陆续出台了受控非密信息识别指南、标志指南、保护方法等规范文件,将受控非密信息分为20大类、124子类,作为有必要限制公开或控制传播的公共数据类型[②]。欧盟《开放数据指令》以及《数字治理法案》并未直接规定公共部门可以开放哪些数据,而是将决定权留给各成员国[③]。

我国一方面有必要借鉴受控非密信息的数据分类进一步完善和细化数据开放目录,而不是仅仅依据数据的性质进行概括地分类,以增强公共数据开放安全管理的精确度和可预见性;另一方面应当将公共数据开放目录的构建与公共数据的安全风险级别对应,构建基于风险的开放管理机制,原则上公共数据安全风险一级及以下的应当无条件开放,二级或三级及以下的应当有条件开放如脱敏后开放,四级及以上的应当不予开放或者提供可用不可见的有条件开放。

就公共数据以什么方式及要求进行安全开放而言,实际上需要回答两个问题。一是直接下载数据、接口调用、通过算法模型获取结果数据或服务等开放方式在安全管控能力上依次递增,是否可以适用于不同风险的公共数据。原则上来说,对于无条件开放数据可以通过上述三种方式对外开放,对于受限开放类数据不得通过直接下载的方式提供,对于禁止开放类数据只能通过数据服务的方式提供。但在通过算法模型获取结果数据或服务时,由于已经对原始数据进行了安全处理,实质上改变了开放的安全风险级别,故有必要对结果数据或服务进行新的安全评估或审查。二是数据利用主体的安全利用条件。欧盟《数字治理法》在第2章"重新使用公共部门持有的某些类别的受保护数据"第5条就对公共数据"重用的条件"进行规定,包括个人数据的匿名化处理,保密商务数据的披露控制处理,安全处理环境等。如果数据利用主体不具备该等条件或能力,公共部门就不应允许数据的重用。当然在考虑公共数据的类别、性质和利用的目的的情况下,安全许

---

①MIRIAM M. B., Commercializing Public Sector Information, *Journal of the Patent and Trademark Office Society*, Vol. 97, 2015, p. 412.

②周亚超,左晓栋:《美国受控非密信息分类与安全控制解析》,《网络空间安全》,2020年第3期。

③LUKAS D., GREGOR L., The Data Governance Act: Promoting or Restricting Data Intermediaries, *Competition and Regulation in Network Industries*, Vol. 23, No. 4, 2022, p. 270.

可条件本身应当是非歧视的、透明的、相称的和客观合理的，不能通过排他性质的许可限制竞争[①]。

（二）公共数据安全义务的层次化分配

为应对公共数据开放多主体参与带来的安全义务分配难题，在“比例”义务的实现上原则上应以“控制”为标准。“控制”意味着在公共数据开放的全周期中可以影响公共数据的流转，通常是公共数据的持有者如公共部门、公共数据的授权运营机构，处理者如数商、数据开放（交易）平台、数据利用者等。“控制”本身意味着可苛责性，由控制者采取行动保护公共数据安全既有可能性又有效率，且控制者往往在公共数据开放中享有利益，由控制者承担安全义务也符合权利义务对等的基本价值追求。当然，不同主体在控制能力和控制范围上存在差异，控制能力强、控制范围广的主体相较而言应承担更多和更严格的安全义务，也就体现为差异化的比例安全义务。

尽管公共数据开放模式存在多样性，但公共数据开放过程的全生命周期中通常涉及三类主体：公共部门、公共数据开放（交易）平台、社会利用主体。这三类主体均负有《数据安全法》规定的普遍数据安全保护义务，包括依法合规开展数据处理活动，建立健全数据安全管理制度，采取技术安全措施等。但从“控制”标准出发，按照公共数据供给、流通、利用等不同的控制范围，不同主体也有区别于其他主体的专属义务，并在义务内容上表现出层次性。

公共部门控制数据供给，对公共数据开放安全具有源头的管理义务。为此，公共部门应当承担数据合规鉴别、分类分级、开放目录管理、公平和安全利用保障等义务，进而从公共数据开放的源头实现数据安全。首先，公共部门应当保证在日常业务中收集的数据满足合规要求，包括数据来源合法、数据质量合规，以保障公共数据处于可用的状态；其次，公共部门应当按照法律规定及时对持有的公共数据进行分类分级，并及时纳入开放目录管理；再次，公共部门在开放公共数据时应当维护“公平利用”秩序，禁止排他性安排，避免限制数据竞争。此外，公共部门应建立公共数据利用安全审计机制，定期核查数据利用者对公共数据处理的过程、手段和结果，及时制止不安全的利用行为。

公共数据开放（交易）平台控制公共数据的流通，对公共数据开放安全具有过程管控义务。一是应提供安全技术支持。为数据开放主体提供各类数据归集、数据治理、清单编制、分级分类、申请审核、工单处理等功能，并提供相应的技术能力保障，协助数据开放主体更好履行开放职责；为数据开放主体提供开放数据的统计分析、风险判断、质量评估、合规服务等功能，为相关政策制定提供决策参考；对数据开放和利用行为进行全程记录，为数据开放和利用的日常监管提供支撑；探索隐私计算、沙箱验证等功能，提供安全空间。二是接入控制。公共数据开放（交易）平台对数据利用主体的接入或访问数据申请进行审核或者协助公共部门审核，负有身份认证、访问控制、安全传输等安全控制义务，保障数据交换过程中的实体信任、数据传输安全以及交换记录的可溯源。

公共数据利用主体控制着公共数据的后续处理方式。这里的数据利用主体不但包括公共数据需求方，在公共数据交易等场景下还可能包括公共数据授权运营主体和数商。其在数据安全上的义务主要体现在三个方面。一是不得随意改变公共数据使用的方式和范围。有条件开放的公共数据通常需要经过申请—审核程序，并签订数据利用协议，为此公共数据利用主体一般不得随意变更公共数据的使用方式和范围，以避免数据安全风险敞口的随意扩大。但是，数据利他主义者即为公共利益目的而利用公共数据的主体可以豁免数据利用协议下的特定利用目的约束[②]。二是配合公共部门和开放平台做好数据安全的维护。在公共数据存在许可利用期限过期、安全等级变更等情况下，公共数据利用主体应当根据公共部门或数据开放平台的要求及时停止公共数据的

①MARIATERESA M.，Policy Recommendation on the Competition Law Issues of the Re-use of Public Sector Information（PSI），*Masaryk University Journal of Law and Technology*，Vol. 6，No. 3，2012，p. 373.

②倪楠：《欧盟模式下个人数据共享的建构与借鉴——以数据中介机构为视角》，《法治研究》，2023年第2期。

处理行为,并配合履行公共数据的销毁,重新取得利用许可等安全管理义务。此外,应定期向公共部门报告公共数据利用情况,并在必要情况下接受定期审计。

(三)技术治理的规范保障

技术介入固然可以改善公共数据开放下的安全治理,但仍需要通过制度化的方式实施,在完善技术治理要求的同时,推动技术的规范应用。为此,技术治理下的规范保障主要体现为完善公共数据安全治理的技术规范。

技术规范本身构成义务符合性和行为人可责性的前提,缺少技术规范必然影响社会规范功能的发挥。此外,技术规范构成技术治理的制度基础,其灵活性和及时性可以适应公共数据开放的复杂场景,提高治理的应对能力。技术规范的制定和修改通常不受繁琐的立法程序约束,可以适应数据安全技术的发展,避免规则的僵化。技术规范通过融入社会规范,提高了规则的确定性和可执行性。公共数据安全的技术规范主要包括三个层次的内容:一是技术规范的内容,主要解决具体场景下数据安全的义务标准问题;二是技术规范的制定,主要解决技术规范的组织启动、程序保障问题;三是技术规范与治理的衔接,主要解决技术规范的实施问题。

就技术规范的内容而言,应结合公共数据开放不同阶段的技术需要来确定,具体包括以下几个方面。一是公共数据收集过程中的安全要求,包括收集过程中应用身份鉴别、数据源认证等确保开放数据的真实性。二是公共数据的分级分类,包括数据安全等级标记、管理等。三是公共数据开放目录管理标准,包括公开目录的内容如对应公共数据的类别、安全级别及共享方式,公开目录的管理如更新、审核、发布等。四是公开数据的安全控制标准,包括质量控制、存储加密、数据更新、安全审计等。五是公共数据交换阶段的安全技术标准,具体又包括用户管理、授权管理、数据脱敏或加密、身份识别、访问控制、安全传输、操作溯源、接口安全等。六是公共数据使用阶段的安全技术标准,主要又包括身份认证、访问控制、数据脱敏或加密等。

就技术规范的制定而言,应当充分发挥社会主体参与数据安全治理的作用。具体来讲,在标准的制定的过程中,一方面可以由全国信息安全标准化技术委员会作为标准制定的牵头机关以保证标准的连贯性、统一性和权威性,以破解当前技术标准碎片化的趋势;另一方面也要广泛吸收数据安全研究机构、高校、数据安全行业公司及团体协会、公共数据开放平台运营机构等主体参与标准的起草和制定,以最大限度地保证标准的先进性、科学性和可操作性。此外,对于公共数据利用阶段的技术规范而言,除了出台国家和地方标准外,还可以考虑制定行业标准和团体标准,充分调动公共数据利用机构及其所属行业协会等的自律监管功能,形成治理合力。

就技术规范融入治理的方式而言,可以认为是通过准用性规范的方式发挥作用。例如《数据安全法》第二十七条要求开展数据处理活动应当采取相应的技术措施或其他必要措施。其中的技术措施或其他必要措施的基准就主要来源于相关的技术规范如国家标准。但是,由于《数据安全法》等并未明确指向某一或某类技术标准,且由于技术规范并不一定具有法律强制效力,相关的数据安全技术规范大多以推荐性标准的方式存在,因此实际上导致了技术规范难以发挥治理工具的作用。此种情况下,宜在相关法律规定如《数据安全法》"政务数据安全与开放"一章中明确相关技术规范在判断相关主体履行数据保护义务情况上的基准作用,为技术规范融入公共数据安全治理体系提供制度通道。

(四)安全合作治理的机制跟进

数字政府建设的大背景下,合作治理的实现同样需要机制保障,并服务于协同治理体系的形成。一是构建互利共赢的公共数据开放模式,在实现公共部门治理责任相对减轻的同时,充分调动社会主体参与公共数据开放当中,形成责任补位;二是完善合作治理的激励机制,构建回应式的安全治理机制,发挥合规豁免的作用。

首先,推动公共数据定价和交易机制的构建。尽管公共部门通常不从公共数据开放中获得额

外收益，但可以通过公共数据定价和交易机制吸引有安全能力的主体参与到公共数据的授权运营当中。授权运营主体可以在对应的技术环境“授权运营域”内对公共数据进行加工处理，也可以将社会数据导入授权运营域，与公共数据进行融合计算形成数据产品和服务，并在数据交易平台进行公开交易。这一方面可以通过授权运营准入避免因公共数据普惠性而导致公共部门需要直接面对众多数据利用主体而带来的治理复杂性，另一方面授权运营主体可以与公共部门共同分担安全治理责任。当然，公共数据授权运营机构在对外提供公共数据产品时，仍应满足市场竞争性要求，禁止排他性安排，同时在产品定价上可考虑实行“准许成本加合理收益”的政府指导价，并可以参考资源补偿收费机制，在公共数据属于公共产品的基本定位基础上，补偿公共部门的治理支出。

其次，拓宽政企、政民合作治理的渠道。除了传统征询立法建议的方式，我国还可以通过开展创新应用竞赛、合作建立试点项目等方式进一步提升公私合作治理安全的广度和深度。针对公共数据开放安全治理中的治理挑战如“公共数据可用不可见的技术实现”“公共数据开放平台安全沙箱的设计”“公共数据处理留痕的技术机制”“公共数据安全的监管和监督科技部署和实现”等可以通过在线公开或定向邀请的方式征集解决方案，并给予适当的奖励，以促进公民和企业参与政府治理。公共部门可以与企业开展基于数据共享的合作项目[①]，例如建立监管沙盒，可以让掌握安全技术企业在沙盒中充分验证公共数据安全处理技术，实现公共部门与企业的监管互动。

再次，构建公共数据处理主体安全合规责任豁免机制。在公共数据开放的安全责任设置上，可以充分借鉴回应性治理理论，一是充分发挥公共数据处理主体的自我规制，在安全风险可控的范围内可以放缓监管部门的主动接入，而优先依靠公共数据处理主体的内部纠错和风险管理机制，塑造公共数据处理主体的安全治理角色；二是适当软化公共数据处理主体的安全责任，可以将是否建立起完善的数据安全风险自我治理机制如在法定的安全义务外采取额外的组织、管理和技术保障措施，作为责任减轻或豁免的重要考量因素，进而充分利用社会主体的安全能力服务于公共数据开放安全的治理。

六、结语

数字经济背景下，公共数据已经成为推动社会经济发展的重要生产要素，公共数据开放已成为必然趋势和选择。数据安全是公共数据开放的前提和基础。但从当前实践看，我国公共数据开放的安全治理还存在安全规则宣示化、技术治理工具应用不足、合作治理缺位等问题亟待破解，严重影响了公共数据开放的安全有序进行。从回应性治理出发，强调公共数据的分类分级和许可利用机制、细化相关参与主体的安全管理义务、引入制度保障下的安全技术、拓宽公私合作安全治理机制已成为公共数据开放安全治理的应有之义。但安全本身是整体的、系统的和动态的，尽管本文试图从理论上廓清公共数据开放安全治理的全貌，但难免挂一漏万，值得进一步体系化的持续跟进研究。

[责任编辑：袁朋伟]

①张敏：《包容审慎监管：数据交易的平台监管进路研究》，《河北学刊》，2023年第1期。