·研究综述与前沿进展·

科学数据开放共享中的大模型应用：前景、风险与治理

王正超
（东南大学法学院，江苏 南京 211189）

摘 要：［目的/意义］探讨科学数据开放共享中大模型的应用及其限度，以期发挥大模型的技术赋能效应，助力科学数据开放共享数智化转型升级。［方法/过程］结合数据生命周期理论和利益相关者理论，梳理大模型应用于科学数据开放共享的逻辑理路，分析风险隐患并提出治理对策。［结果/结论］研究表明，首先，大模型能够从客体向度优化科学数据全生命周期形态、从主体向度激发利益相关者开放共享动力，从而有效驱动科学数据开放共享提质增效；其次，大模型应用带来脏数据与假数据的数据质量风险、内部威胁与外部攻击的数据安全风险、赋权与去权的数据权利保护风险；最后，应构建包含适应性治理理念、韧性治理机制和包容性治理工具在内的敏捷治理模式，以平衡促进应用与管控风险之间的张力，保障科学数据开放共享中大模型的妥善应用。

关键词：科学数据开放共享；大模型；开放数据；人工智能；敏捷治理
DOI：10.3969/j.issn.1008-0821.2025.07.015
〔中图分类号〕G203 〔文献标识码〕A 〔文章编号〕1008-0821（2025）07-0167-11

The Application of Large Models in Open Sharing of Scientific Data: Prospects, Risks, and Governance

Wang Zhengchao
（School of Law, Southeast University, Nanjing 211189, China）

Abstract: ［Purpose/Significance］ The study explores the application and limitations of large models in the open sharing of scientific data, with the aim of leveraging the technological empowerment effect of large models to assist in the digital-intelligent transformation and upgrading of open sharing of scientific data. ［Method/Process］ Combining data lifecycle theory and stakeholder theory, it outlined the logical path of applying large models to the open sharing of scientific data, analyzed the hidden risks and proposed governance measures. ［Result/Conclusion］ The study shows that firstly, large models can optimize the full lifecycle form of scientific data from the object dimension, and stimulate stakeholders' open sharing motivation from the subject dimension, thereby effectively driving the improvement of the quality and efficiency of scientific data open sharing; secondly, the application of large models brings data quality risks of dirty data and false data, data security risks of internal threats and external attacks, and data rights protection risks of empowerment and disempowerment; finally, it should be established an agile governance pattern that includes adaptive governance concepts, resilient governance mechanisms, and inclusive governance tools to balance the tension between promoting application and managing risks, and ensure the proper application of large models in the open sharing of scientific data.

Key words: open sharing of scientific data; large models; open data; AI; agile governance

收稿日期：2024-08-27
基金项目：国家社会科学基金重点项目“适合我国的企业行政合规制度构建研究”（项目编号：23AFX011）；江苏省社会科学基金重点项目“数字时代行政机关公开负面信息研究”（项目编号：23SFX021）。
作者简介：王正超（1999-），男，博士研究生，研究方向：行政法学，数据法学。

随着以 ChatGPT 为代表的 AI 大模型技术不断迭代升级，大模型的能力边界持续拓展，应用场景日益丰富。大模型在本质上是由大规模参数和复杂计算结构构成的深度学习模型，经过海量数据的预训练，大模型体现出强大的数据识别、分析、挖掘、关联等处理能力，在“数据为王”[1]的科学数据开放共享领域的嵌入式应用具有良好的耦合性。在价值理念层面，科学数据开放共享是开放科学运动的重要组成部分，而大模型正是得益于开放科学所倡导的开放获取(Open Access)主张才得以获得海量开源数据用于模型开发和训练，大模型“反哺”作为开放科学运动产物之一的科学数据开放共享具备内在价值的一致性，科学数据开放共享水平的提升又能进一步促进大模型获得更多的优质预训练数据，帮助其改善模型性能，实现二者之间的相互增益。在实现进路层面，大模型能够完成自然语言处理(NLP)、计算机视觉(CV)、多模态深度学习(MDL)等复杂数据处理任务，经过特定科学领域语料的预训练和指令微调后，便可以有效理解数据处理者的意图，迅速适应多样化的科学数据处理场景，且生成内容(AIGC)质量高、可用性强，能够有效满足科学数据采集生产、加工整理、存储共享等数据全生命周期提质增效的迫切需求。

大模型在科学数据开放共享领域展现出广阔的应用前景，但数据科学界对于这一技术的发展动向及其在本领域的应用缺乏足够的关注。目前，已有研究注意到大模型在科学数据管理与治理中的应用空间，但大多未能同科学数据开放共享的特殊性相结合，主要围绕大模型如何改变科学数据管理[2]、大模型在科研数据管理中的应用潜力[3]、大模型视域下的科学数据政策[4]、大模型驱动的数据治理技术[5]、科研智能化趋势下的科研数据形态[6]、人工智能与数据安全管理的融合发展[7]等展开研究。而针对大模型与科学数据开放共享的研究，虽然捕捉到二者之间的紧密联系及融合路径，但主要基于“AI for Science”(AI4S)视角考察大模型驱动科学研究所带来的潜在影响，侧重科学数据开放共享对大模型的被动适应，而非大模型对科学数据开放共享的主动赋能。这体现为，上述研究主张，作为科学数据开放共享的国际通用原则，FAIR 原则(Findable，Accessible，Interoperable and Reusable)在 AI 时代应当被赋予新的内涵——Findable and AI Ready[8]，即应当确保科学数据的可发现性并通过适当的数据预处理方案使其在结构和质量上满足 AI 的需求[9]。此外，有关科学数据开放共享中大模型应用风险的研究缺乏对各类风险进行体系化治理的探讨，这些研究主要涉及大模型应用所引发的科学数据开放共享安全风险[10]、图书馆科研数据服务版权风险[11]、学术期刊科学数据出版失范风险[12]等方面。基于此，本文拟对大模型在科学数据开放共享中的应用前景、风险隐患与治理对策展开系统研究，确保大模型以“科技向善”的价值底色助力科学数据开放共享数智化转型升级。

1 科学数据开放共享中大模型的应用前景

2023 年 12 月 31 日，国家数据局等十七部门联合发布《“数据要素×”三年行动计划(2024—2026 年)》指出，当前我国存在数据供给质量不高、流通机制不畅、应用潜力释放不够等问题。在此背景下，大模型有望充当突破制度瓶颈的抓手，激活科学数据开放共享机制，充分释放科学数据要素价值化红利。

1.1 科学数据开放共享的现实困境与大模型的纾困逻辑

近年来，从《科学数据管理办法》出台确立“开放为常态、不开放为例外”原则，到《中华人民共和国科学技术进步法》修订新增“推动开放科学发展”规定，我国一直致力于推动科学数据开放、共享与利用，但仍面临诸多发展难题。首先，科学数据开放共享体量不足、质量不高，难以发挥科学数据聚合价值。据中国科学院计算机网络信息中心等发布的《中国开放数据白皮书 2023》统计，虽然大多数中国数据受访者(78%)赞成将公开研究数据作为常规惯例，但只有较少的受访者(15%)会整理数据以便分享，而过半受访者希望得到关于科学数据管理与共享的培训和帮助。除成果抢发顾虑、学术认可不足等主观因素外，科研人员相应数据管理与共享能力的欠缺是当前科学数据供给匮乏、可用性不佳的重要原因。其次，科学数据基础设施建设薄弱，数据集成、存储、处理和访问效能亟待提升。数据规模不断扩大、多源异构和多模态数据的关联

融合难度不断上升，对数据整合集成机制、关联集成与语义搜索、存储系统等提出更高的要求，科学数据基础设施亟需技术升级。最后，科学数据开放共享管理与服务机制尚不完备，数据主权和话语权存在缺失。我国作为“后发国家”，在科学数据开放共享制度和实践上较欧美发达国家仍有一定差距，导致当前我国科研使用的科学数据 90%来自外资数据平台或出版机构[6]，产生的科学数据往往又由于国际期刊要求最先流向国外，科学数据面临“受制于人”和“无序外流”的双重困境。

引发上述困境的原因来自政策、科研环境、技术、管理、资金等诸多方面，而凭借强大的数据处理能力以及良好的泛化性能，大模型能够作为“发动机”为科学数据开放共享生态系统注入新的动能，通过技术变革引领制度瓶颈突破。一方面，相比以往的“小模型”[5]，大模型具备自动化、高效能、多模态数据处理能力，能够胜任丰富多样的数据处理任务，从而显著提升科学数据体量、质量和处理效率，实现科学数据开放共享的“量变”增长。随着数据处理场景日益复杂化，传统的“小模型”在大规模数据识别、多源数据融合和规范化等方面存在应对局限[5]，往往需要大量的标注数据或专家知识的支持，模型训练和数据处理效能低下。相比之下，大模型利用海量数据进行无监督预训练，能够为模型积累丰富的知识储备，并且通过少量的指令微调便能够快速掌握特定领域知识，节省了大量人工标注时间及学习成本，为模型的落地应用提供了极大便利。另一方面，大模型具备高度智能化和拟人化的内容生成能力，可以精准联结使用者需求，将其应用于数据产品与服务设计、策划等开发利用场景中，从而实现科学数据开放共享的“质变”升级。随着模型规模和训练数据的不断增长，大模型呈现出一定的“涌现”（Emergent）能力，譬如逻辑推理能力、内容创作能力，这将促成大模型在数据增值加工、数据出版服务等数据开发利用场景中的深度融合应用，从而超越数量的概念，发现隐藏在大数据洪流之下的“珍宝”[9]。

1.2 大模型驱动下的科学数据开放共享

总的来看，大模型应用于科学数据开放共享具备相应的开放科学基础和技术融合逻辑。更进一步地看，大模型对科学数据开放共享的驱动路径，可以从作为客体的数据和作为主体的利益相关者两个向度展开，如图 1 所示。

1.2.1 客体提质：大模型优化科学数据全生命周期形态

数据是科学数据开放共享的客体，也是数据科学的研究对象[13]，具有客观性和对象性的基本属性。虽然大模型自身尚不具备主体性，但借助于人类行动主体的应用，可以对科学数据形态施加显著影响。科学数据产生于科研活动过程，遵循数据生命周期规律，大模型对科学数据的改造路径便可以从科学数据生命周期的不同阶段切入。

具体而言，大模型被应用于数据采集生产、加工整理、汇交存储、增值处理、出版传播和再利用等科学数据开放共享全流程，全方位优化科学数据形态。第一，在数据采集生产阶段，高质量合成科研人员所需要的图像型、视频型等复杂数据或数据模型，从而拓展充实数据来源，提升高附加值数据供给水平。第二，在数据加工整理阶段，自动化完成海量数据异常值检测、错误校正和重复去除等数据预处理和元数据创建任务，使其满足数据存储或出版要求，从而降低科学数据开放共享的启动成本，提高数据流动性。第三，在数据汇交存储阶段，无缝接入数据平台的数据传输、集成和存储系统，实现对大规模、跨数据源的数据进行整合、解析和统一访问，优化数据存储结构，提高数据检索效率[14]。第四，在数据增值处理阶段，利用 AIGC“创造力”优势，充分挖掘科学数据潜力，开拓科学数据产品和服务种类与范围，提高数据增值效益。第五，在数据出版传播阶段，深度介入数据论文出版、数据独立出版和数据关联出版等科学数据出版模式，从选题策划、稿件筛选、审稿任务分配、同行评议、排版校对等多方面优化出版流程[15]，促进科学数据出版服务质效提升。第六，在数据再利用阶段，全面融入数据再利用生态，通过开放“大模型+科学数据开放共享”服务，拓展科学数据自动化检索、智能推荐、可视化交互和数据产品的一体化生成功能，进而提升科学数据再利用率及利用成效。

1.2.2 主体增能：大模型激发利益相关者开放共享动力

利益相关者是科学数据开放共享的主体，包括

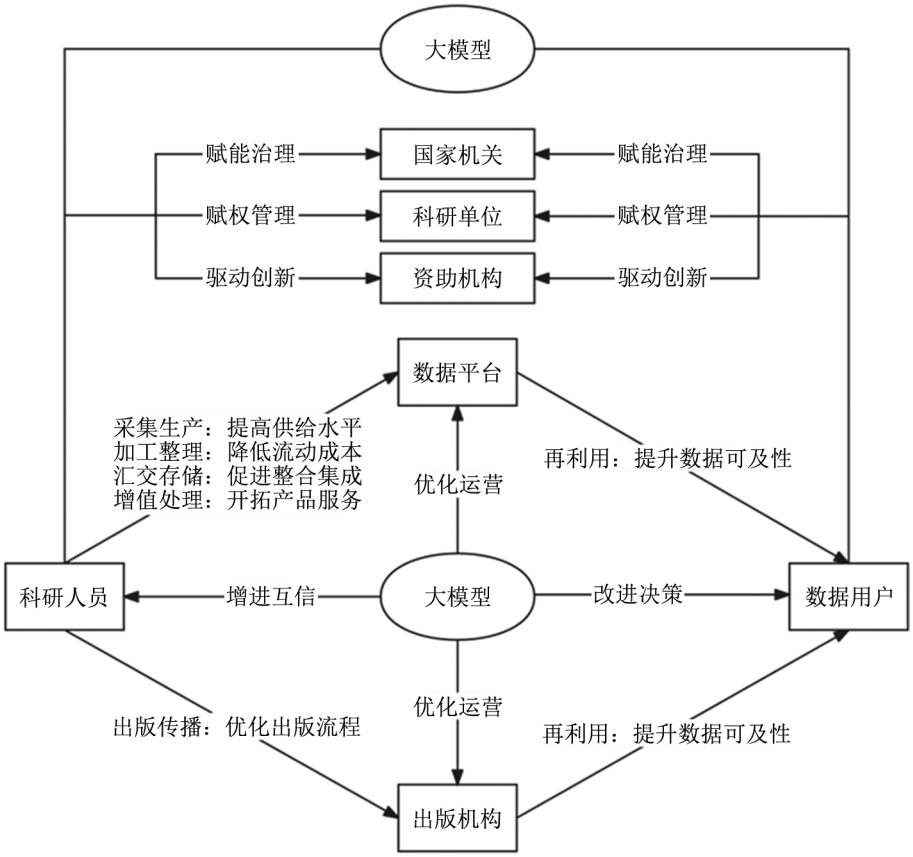

图 1　大模型驱动下的科学数据开放共享图景

Fig. 1　The View of Open Sharing of Scientific Data Driven by Large Models

科研人员、数据平台、出版机构和数据用户等直接参与主体，以及国家机关、科研单位、资助机构等监督管理主体。利益相关者理论认为，各利益相关者拥有不同的利益诉求，各类主体而非某一主体的利益最大化是系统追求的目标[16]。大模型应用能够增进科学数据利益相关者的主要利益，激发各类主体的价值动力，并使其相互作用以实现价值共创。

具体而言，大模型通过赋能治理、赋权管理、驱动创新、增进互信、优化运营、改进决策等方式全面提高科学数据利益相关者的利益满足度，促进各类主体积极采取行动。第一，国家机关的主要利益是提升科学数据治理水平，大模型作为一种“技术治理”[17]方式，具有高效率、易传导、可复制等优势，能够弥补政策法规等传统治理方式落地难、起效慢等缺陷，赋能科学数据治理“提速换挡”。第二，科研单位的主要利益是提升组织的科研竞争力，大模型通过增强个人的数据生产能力和组织的数据管理能力，在科研单位对内数据控制权和对外数据话语权方面发挥显著“赋权”作用。第三，资助机构的主要利益是推动可持续科研创新，大模型作为一种新兴数字技术，与科研创新具有天然融合性，AI4S 更是被视为科学研究“第五范式”，二者结合在驱动创新方面蕴藏巨大潜力。第四，科研人员的主要利益是获得学术认可与激励，大模型在提升科学数据开放共享影响力的基础上，也将促进相应学术成果评价、绩效考核管理等激励机制完善，从而增进科研互信，破解“囚徒困境”。第五，数据平台和出版机构的主要利益是提升品牌价值，大模型有助于优化数据运营服务，提升品牌知名度，打造新的盈利引擎。第六，数据用户的主要利益是利用科学数据为自身决策提供可靠参考，大模型能够增加数据获取机会，提高数据处理和分析能力，使数据用户在信息掌握更为全面和深入的基础上改进其科研决策。

2　科学数据开放共享中大模型应用的风险隐患

作为一把“双刃剑”，大模型在为科学数据开放共享生态系统释放技术动能、驱动科学数据开放

共享机制稳健有力运行的同时，也给科学数据治理带来一系列风险隐患，主要表现在数据质量、数据安全和数据权利 3 个层面。

2.1 “脏数据”与“假数据”：数据质量层面的风险隐患

数据质量是影响科学数据开放共享效果的关键，高质量数据是驱动科学发现的“加速器”，劣质数据则会给科学研究和应用造成巨大损失。虽然大模型具有改进数据质量、提升数据价值的功能，但囿于技术局限性或不当使用，可能会降低科学数据的准确性、完整性、可靠性等数据质量属性[18]，滋生新的数据质量风险。

一是“脏数据”[19]（Dirty Data）风险。大模型存在“数据污染”“幻觉”“算法黑箱”等问题，使用者对大模型输出结果的准确性和可靠性疏于考察，直接加以运用，将产生不符合科学要求或标准规范的“脏数据”。首先，在大模型预训练阶段，原始数据质量瑕疵、缺陷以及算法偏见，都将导致大模型输出结果出现偏差，难以满足科学数据精确性和标准化等方面的特定要求。即便能够保证数据源选取和预训练质量，大模型也可能遭受指令攻击或提示注入产生“二次污染”[12]。其次，当预训练数据集中存在特定情况缺失时，大模型将根据概率分布关系作出最符合提示语要求的“推断”，这种时常表现出“自信而错误”的“推断”被称为大模型的“幻觉”。“幻觉”使得大模型在数据处理上缺乏稳健性，与科学数据的高度严谨性要求相背离。最后，大模型“黑箱”式的数据处理机制透明度不足，输出结果的可解释性差，且有赖于进一步的人工审查和验证，导致数据的用户接受度不高。因此，大模型在科学数据开放共享中的应用，可能使得数据可用性“不升反降”。

二是“假数据”[20]（False Data）风险。大模型在“合成数据”方面具有“深度伪造”（Deepfake）特性，使用者将其应用于捏造、伪造、歪曲和篡改科学数据，很难被现行科学数据开放共享流程发现，进而产生不具有可信度和可用性的假数据。在科学数据开放共享中，CARE 原则（Collective Benefit，Authority to Control，Responsibility and Ethics）被视为 FAIR 原则的重要补充[21]，强调科学数据的公益、权威、责任和伦理，旨在确保科学数据的生产、收集、共享及使用都应符合科研伦理和学术道德等要求。然而，大模型使用者为了追求自身利益，可能利用其实施科学数据学术不端行为。例如，一篇发表在《美国医学会眼科杂志》（JAMA Ophthalmology）的论文使用 GPT-4 的高级数据分析功能（Advanced Data Analysis，ADA）生成虚假的实验数据集，发现其能创造出看似真实合理的数据，并且准确支撑作者错误的论文观点[22]。期刊编辑和评审专家在审稿阶段很难判别数据的真实性和有效性，数据平台往往更加难以对此及时、准确地作出反应。这种“恶意投毒”[7]式的数据造假行为是对数据质量的毁灭性打击，由此产生的链式反应将严重影响科学数据可信共享。

2.2 内部威胁与外部攻击：数据安全层面的风险隐患

数据安全是科学数据开放共享的基础，包含机密性、完整性和可用性等数据安全属性[23]。大模型数据安全问题是其实际应用中的一大掣肘，OpenAI 的技术报告显示，即便是最新版本的 GPT-4，仍可能被黑客入侵[24]，引发数据泄露、窃取、篡改和毁损等数据安全风险。根据风险来源不同，科学数据开放共享中大模型应用的数据安全风险可以划分为以下两类。

一是内部威胁型数据安全风险。研究显示，80% 的数据安全风险是由内部原因造成的[25]，包括硬件或软件故障、内部人士滥用权限泄露或窃取数据、疏忽操作导致数据丢失或毁损等，大模型带来的内部威胁型数据安全风险主要涉及前两者。第一种情形表现为大模型需要处理规模更大、复杂性更高的数据集，对系统性能、可扩展性和灵活性提出更高要求[7]，但现有科学数据基础设施往往难以满足其要求，导致技术接入的适配性和稳健性不足，从而埋下数据安全隐患。譬如，大模型的接入使得基础设施之间及其与数据处理者之间交互增强，数据开放接口增多，若缺乏健壮的通信接口和安全的数据传输机制，将增加数据泄露或丢失风险。第二种情形表现为大模型控制者和处理者等内部人士违反身份认证、授权和访问控制机制，未经授权或滥用权限获取和利用科学数据，导致数据窃取或泄露，进

而可能对国家安全、行业秩序和个人隐私造成严重危害。此外，内部人士能够凭借其身份，利用大模型深度挖掘、交叉碰撞、相互验证数据集之间的联系，对已经脱敏加密的隐私数据或涉密数据实施“反向工程”和“数据拼图”，引发隐性数据安全风险[26]。

二是外部攻击型数据安全风险。由大模型遭受科学数据开放共享生态系统外的攻击引发的数据安全风险被归为外部攻击型数据安全风险，攻击者可能是黑客组织、犯罪团伙或者国家(地区)，攻击动机包括政治或军事目的、商业竞争、复仇或泄愤、获取经济利益等。在国家层面表现为，大模型“技术主权”安全威胁带来数据主权安全风险。“技术主权”是指一国自主开发利用技术的创新能力[27]。当前，大模型技术主要由欧美发达国家(地区)掌握，面对国外技术断供、封锁等限制围堵，我国海量科学数据将处于失控状态，给数据主权乃至政治、经济主权增加不稳定因素。在行业层面表现为，大模型遭受黑客攻击导致科研组织机密数据损毁、篡改以及秘密披露、系统中断、数据截获，对科研秩序造成冲击。除科学数据外，科研组织所持有的诸如编辑部审稿流程数据等内部数据也可能被窃取或泄露，造成科研组织利益受损，扰乱行业公平竞争秩序。在个人层面表现为，大模型在用户数据隐私保护上有所欠缺。ChatGPT 曾被曝出泄露用户姓名、邮箱、聊天记录标题和信用卡最后四位数字[28]，用户数据被不法分子攫取可能导致个人隐私受到侵犯，滋生用户画像分析等个人数据安全风险。

2.3 “赋权”与“去权”：数据权利层面的风险隐患

完善的数据权利保护体系有利于激发科学数据开放共享利益相关者的积极性，促进科学数据向生产要素转化。大模型凭借其出色的数据加工处理能力，有助于科学数据在内容选择或编排上体现独创性而获得著作权保护，但是，由于 AIGC 的可版权性存在争议，对大模型的过度使用可能导致科学数据不被视为作品而无法获得著作权保护，因此呈现出大模型对科学数据著作权保护“赋权”与“去权”的双重效应，使得数据权利保护局面进一步复杂化。一方面，“赋权”效应体现为，大模型能够利用其深度学习的高级架构，重新解析和组织数据，生成与原始数据密切相关但表达方式全新的内容[11]，实现科学数据的“二次创作”，进而满足作品独创性要求，取得著作权保护。事实上，现实中存在大量的科学数据因数据库编排方式有限，以及考虑用户体验、设计成本与难度而无法满足独创性要求，因此被排除在著作权保护范围之外。大模型能够有效帮助这些科学数据摆脱作为“非独创性”数据库或数据集处于权利保护真空地带的困境，将更多的科学数据纳入著作权保护范围。另一方面，“去权”效应体现为，对于大模型的使用可能滑向“机器主导”的自主生成模式，导致人类在科学数据创作中的智力贡献严重不足，由于人类创作者贡献是可版权性的核心判断标准之一，科学数据可能失去成为作品而获得著作权保护的资格。在北京互联网法院作出的“AI 文生图著作权侵权国内第一案”判决中，法院强调原告的智力投入和个性化表达是构成作品的关键[29]。美国版权局在 AIGC 版权登记问题上要求作者表明有“至少最低限度的人类创造性努力”(At Least Minimal Human Creative Effort)的存在[30]。而在使用大模型处理科学数据的场景中，可能会出现大模型自主运行生成、人类参与创作的程度和创造性低于“最低限度”的情形，导致科学数据丧失可版权性，引发大模型对数据权利保护由“赋权”到“去权”的异化风险。

3 科学数据开放共享中大模型应用的治理对策

要规制大模型应用于科学数据开放共享所滋生的风险隐患，必须对其展开体系化治理。在大模型治理策略研究中，敏捷治理(Agile Governance)作为一套具有柔韧性、流动性、灵活性或适应性的行动或方法，一种自适应、以人为本以及具有包容性和可持续的决策过程[31]，被越来越多地认可和接受。敏捷治理最先在 2018 年“世界经济论坛”上被提出，我国《新一代人工智能治理原则——发展负责任的人工智能》将其引入人工智能治理领域。因此，构建科学数据开放共享中大模型应用的敏捷治理模式既是“发展负责任的人工智能”的题中应有之义，又能够作为高度不确定性和复杂性风险背景下的一种新型治理方式[32]，凭借灵敏迅捷、联通共识、双向反馈等特性[33]，有效应对科学数据开放共享多元链式运行所带来的大模型应用风险泛在化和

弥散化趋向，达成促进技术应用和规制潜在风险之间的动态平衡。

在具体的模式建构上，敏捷治理一般被认为包含“理念—机制—工具”三重进路[34]，三者相互融通、层层递进，旨在实现对传统治理模式的目标理念重塑、统筹能力提升和行动逻辑调适[35]。面对科学数据开放共享中大模型应用风险的复杂多变性、随机突发性和结果不可控性等特点，传统治理模式存在价值理念滞后、运行机制低效、工具选择单一的应对局限。相较而言，敏捷治理强调根据不断变化的情况灵活调整治理策略[36]，更加契合未知且难以预测的风险应对需求。这包括：秉持适应性治理理念，从“被动回应风险”到“主动适应风险”；构建韧性治理机制，从“单方主体集中监管”到“多元主体协同参与”；运用包容性治理工具，从“刚性规制”到“柔性引导”。从而以“价值性”“制度性”“工具性”三维敏捷寻求科学数据开放共享中大模型应用治理的“最优解”，如图 2 所示。

图 2 科学数据开放共享中大模型应用的敏捷治理框架

Fig. 2 Agile Governance Framework for Large Models Application in Open Sharing of Scientific Data

3.1 秉持适应性治理理念，注重风险防治结合

敏捷治理以适应性为核心特征和关键优势，适应性强调治理措施应足够灵活以适应复杂系统的细微差别，提倡差异化、风险预防和主动安全的治理理念[37]，是敏捷治理的“价值性”维度表征。大模型技术发展的不确定性以及科学数据开放共享多元链式运行的特点，决定了科学数据开放共享中大模型的应用风险具有较强的复杂性、多变性、突发性和不可控性。在适应性治理理念指引下，应建立一套预防和应对并重的动态适应的风险防控机制。

第一，应当建立灵活有效的大模型风险识别分析机制，根据大模型自身所处的环境和影响范围，并与参与主体充分沟通协调，形成共同的风险认知和行动准则。大模型滋生的风险隐患涵盖整个科学数据生命周期流程，应通过向各环节的参与主体收集和整理充足的信息，采用跨学科的方法分享知识、交流见解，从而对可能发生的不利后果加以预判和预防。这包括：一是建立大模型开发训练者等技术专家与科研领域知识专家联合的数据质量风险研判机制，及时、准确识别由大模型技术导致的数据真实性、可靠性等质量风险。二是建立大模型技术专家与国家安全、网络安全、数据安全等安全专家联合的数据安全风险研判机制，全面、详尽掌握潜在的数据安全风险点。三是建立科研领域知识专家与知识产权专家联合的数据权利保护风险研判机制，从专业角度辨识、防范由大模型引发的数据版权保护风险。

第二，应当建立差异有序的大模型风险评估控制机制，按照风险发生可能性和危害严重程度对大模型引起的数据质量、安全和权利保护风险加以分级分类，并采取不同的控制措施。适应性治理理念追求将风险控制在可以接受的范围之内，而非绝对的“零风险”，比例原则和风险分级分类成为大模型监管的主流选择。譬如，欧盟《人工智能法案》将人工智能系统划分为不可接受的风险、高风险、有限风险和最小风险 4 种级别，并规定不同程度的控制措施。大模型在科学数据开放共享中的风险也因不同应用场景而存在差异，应对其展开相应的定量或定性评估，并将评估结果按照不同的标准或维度进行分组或排序，以便分别采取规避、减轻、转移或承担等风险控制措施[38]。值得说明的是，大模型风险评估控制机制不是一次性或静态的，而应随着大模型技术、环境和影响范围进行动态、有序地调整和应变。

第三，应当建立及时有力的大模型风险应急响应机制，明确各利益相关者在大模型风险事件应对中的主体权责，完善大模型风险事件的事前预警、事中报告、事后调查总结等处置程序，确保风险的快速、协调和有效应对。一方面，要明确大模型开发者、提供者、使用者的责任分配，根据“利益之所在，风险之所在”原则，确定各利益相关者承担的风险与责任，推动科学数据开放共享行业自律和规范化发展。另一方面，及时完善的大模型风险事件处置程序是机制有效运转的关键，包括预案与流程、通知与报告、处理与恢复、信息共享与合作、媒体与公众关系、事后总结与改进、培训与演练、法律合规等系统性措施[37]，从而在大模型风险事件发生时，能够及时、有效控制风险事件的影响范围，遏制危害后果的蔓延。

3.2 构建韧性治理机制，加强风险协同共治

敏捷治理具有高度柔韧性，柔韧性强调治理框架在应对风险冲击时展现出良好的抗击、恢复和转型能力[39]，是敏捷治理的“制度性”维度表征。与适应性侧重快速响应以应对动态风险不同，柔韧性侧重弹性运行以应对长期风险，而治理主体协同配合、形成合力，是治理框架具备柔韧性的关键[40]。科学数据开放共享中大模型应用的治理是一个涉及国家机关、科研单位、资助机构、数据平台、出版机构、科研人员、数据用户等诸多利益相关者在内的复杂过程，为确保大模型能够承受住各种压力和挑战，应构建多元主体协同参与的韧性治理机制。

第一，国家机关在韧性治理机制中以其权威主体的身份扮演主导性角色，应当通过强调不同主体的广泛参与和有效互动，积极深入了解大模型的技术特征和应用模式，在对其风险充分前瞻、动态跟踪的基础上制定监管方略。一方面，国家机关应鼓励各利益相关者之间的合作，协调不同主体的需求，确保治理过程的协同性。另一方面，国家机关应及时、敏锐地捕捉大模型的应用风险，通过制定相应的政策法规，引导大模型的规范应用。譬如，开展

大模型科研不端监管立法，合理界定并有效规制利用大模型伪造、篡改科学数据等科研不端行为及其责任；加强对大模型技术自主研发的政策支持力度，确保技术主权安全；强化对大模型实施黑客攻击等行为的打击力度，完善相应的刑事、行政和民事制裁体系；规范 AIGC 版权保护监管尺度，明确利用大模型处理科学数据的权利保护边界。

第二，科研单位、资助机构、数据平台和出版机构等科研组织是科学数据开放共享中大模型应用的积极推动者，在韧性治理机制中扮演主体性角色，应当加强与国家机关的互动合作，并通过行业自治、内部合规等形式促进大模型治理体系的完善。一方面，科研组织应尽快与监管部门达成合作，制定具体应用指南。在科技部的指导和支持下，中国科学技术信息研究所联合爱思唯尔等发布《学术出版中 AIGC 使用边界指南》，相关科研组织可以参照制定“科学数据开放共享中大模型应用指南”，从而促成大模型应用的集体行动，克服科研组织“经济人”属性带来的“各自为政”的弊病。另一方面，科研组织应强化大模型内部合规建设，压实风险主体责任。譬如，加强对科研人员使用大模型处理科学数据的质量审查和版权把关，从安全策略、组织建设等方面完善大模型内部安全管理制度[10]，有效控制自身风险。

第三，科研人员、数据用户是韧性治理机制的重要一环，既可能是大模型应用风险的开启者，也可能是受害者，应当提升其使用大模型的风险意识和规避能力，以此奠定大模型应用治理的良好起点。一方面，通过监管部门的宣传引导、科研组织的培训教育等形式提高其大模型使用素养，包括注重对 AIGC 准确性、可靠性和可版权性的考察，避免处理机密或隐私数据。另一方面，应着重强化科研伦理教育，包括禁止使用大模型从事数据造假行为、实施“反向工程”还原国家秘密和个人隐私，以及进行用户画像分析等恶劣行径，并通过相应惩戒措施提高威慑力，确保大模型在遵循科研伦理前提下的健康应用。

3.3 运用包容性治理工具，推进风险审慎监管

包容性是敏捷治理的重要特征，强调审慎运用治理工具，给予治理对象必要的发展时间和试错空间，不宜提早或过度干预治理进程，是敏捷治理的“工具性”维度表征。为鼓励和支持大模型的创新应用，在治理“工具箱”中，传统的“命令—控制”型规制工具虽然不可缺少，但其适用顺位应适当后移，而优先采取技术供给、软法规范等具有支持性、指导性的包容性治理工具。

第一，对于能够通过大模型技术或配套技术发展而化解的应用风险，应当鼓励技术不断发掘和拓展，无需引入规范约束，避免为技术发展设限，从而提升治理的可持续性。一方面，应通过大模型自身技术优化弥合与科学数据开放共享之间的罅隙。譬如，在大模型预训练阶段“投喂”高质量科学数据，采用专业人士监督和反馈，持续改进大模型处理科学数据的专业性能，有效降低大模型脏数据风险；同时，通过大模型自身技术改进，促进基于大模型技术的 AIGC 检测技术加快发展，妥当控制大模型假数据风险。另一方面，应充分吸纳其他先进技术，作为“他山之石”攻克大模型风险防控的痛点和难点。譬如，采用零信任技术对主体身份、网络环境、终端状态等要素“持续验证+动态授权”，有效控制利用大模型处理科学数据的访问行为；利用同态加密、差分隐私和联邦学习等隐私计算技术保障科学数据“可用不可见、可用可计量”，在满足数据处理需求的同时确保数据机密性和隐私性得到控制[10]。

第二，对于单纯依靠技术发展无法规避的大模型应用风险，当风险尚不足以采用强制性规制工具时，应当运用国家标准、行业自律规范等软法规范工具，通过引导式、自愿式的柔性治理，在不波及大模型创新应用的前提下，将风险影响范围最小化。在国家标准层面，我国已于 2019 年国家重点研发计划“国家质量基础的共性技术研究与应用”重点专项设立“科学数据安全技术及基础技术标准研究”项目，目前《科学数据安全要求通则》《科学数据安全分类分级指南》等国家标准正处于批准阶段，应在继续推进国家标准体系研究的基础上，细化大模型适用相关国家安全标准的实施方案，为大模型应用提供具体遵循。在行业自律规范层面，对于一时难以界定风险性质及级别的大模型应用行为，应通过赋予行为人相应的行业软法义务，逐步探索

行为的容错边界，促成行业监管的包容审慎。譬如，对大模型使用者课予透明度义务，要求其披露和说明科学数据处理中大模型的使用情况，并对相应科学数据的可用性和可版权性进行检测和验证，当对大模型的应用风险积累足够的经验共识时，进而上升为国家政策或立法，形成一个动态、完善、可持续的规范体系。

4 结 语

大模型为人类社会发展带来新机遇，科学数据开放共享领域有望借此迎来重大革新契机。结合数据生命周期理论和利益相关者理论，研究发现，大模型有助于纾解科学数据开放共享面临的现实困境，释放强劲的价值共创潜能。然而，正如价值与风险是“一枚硬币的两面”，大模型也带来科学数据质量、安全和权利保护等层面的风险隐患。在大模型应用治理上，敏捷治理能够有效应对高度不确定性和复杂性的应用风险，合理平衡促进应用与管控风险之间的张力。通过构建包含适应性治理理念、韧性治理机制和包容性治理工具在内的敏捷治理模式，以“价值性”“制度性”“工具性”三维敏捷促进传统治理能级升维。受限于大模型实践应用进展，本文仅是从宏观系统层面讨论其在科学数据开放共享中的应用，对微观操作性问题讨论较少，未来将在大模型应用模式不断成熟的基础上继续细化和深入研究。

参 考 文 献

[1] 赵丽梅. 科学数据共享的价值及其表征——基于主体性的分析视角 [J]. 自然辩证法研究，2022，38（5）：116-122.

[2] Hatch V. Deciphering the Data Deluge：How Large Language Models Are Transforming Scientific Data Curation [EB/OL]. [2023-11-15]. https://www.embl.org/news/embletc/issue-101/deciphering-the-data-deluge-how-large-language-models-are-transforming-scientific-data-curation/.

[3] Azeroual O，Schöpfel J. New Developments in Research Data Management-The Potential of AI [EB/OL]. [2024-01-01]. https://doi.org/10.1016/B978-0-323-95689-5.00253-4.

[4] 丰佰恒，杜宝贵. 大模型视域下大数据政策生态链研究——以科学数据政策为例 [J]. 现代情报，2024，44（10）：41-51.

[5] 李直旭. 大模型驱动的数据清洗与数据合规技术展望 [EB/OL]. [2024-07-24]. https://datascience.fudan.edu.cn/6e/d0/c13525a683728/page.htm.

[6] 张婧睿，孙蒙鸽，韩涛. 科研智能化趋势下科研数据研究 [J]. 科学观察，2023，18（4）：49-61.

[7] 张昊星，赵景欣，岳星辉，等. 全生命周期数据安全管理和人工智能技术的融合研究 [J]. 信息安全研究，2023，9（6）：543-550.

[8] Scheffler M，Aeschlimann M，Albrecht M，et al. FAIR Data Enabling New Horizons for Materials Research [J]. Nature，2022，604（7907）：635-642.

[9] 李新，苏建宾. 走向数据善治：以地球科学数据治理为例 [J]. 科学通报，2024，69（9）：1149-1155.

[10] 廖方宇，李婧，龙春，等. 开放科学背景下科学数据开放共享安全挑战及我国对策思考 [J]. 农业大数据学报，2024，6（2）：146-155.

[11] 闫宇晨. ChatGPT 应用背景下图书馆科研数据服务版权风险研究 [J]. 国家图书馆学刊，2024，33（3）：25-36.

[12] 刘娴. AIGC 技术赋能学术期刊数据出版的应用研究与思考 [J]. 编辑学刊，2024，（4）：31-37.

[13] 朝乐门，张晨，孙智中. 数据科学进展：核心理论与典型实践 [J]. 中国图书馆学报，2022，48（1）：77-93.

[14] 范淼. 人工智能与数据管理共同支撑新质生产力发展 [J]. 图书与情报，2024，（2）：8-11.

[15] 张智雄. 在开放科学和 AI 时代塑造新型学术交流模式 [J]. 中国科技期刊研究，2024，35（5）：561-567.

[16] Blair M M. Ownership and Control：Rethinking Corporate Governance for the Twenty-First Century [M]. Washington，D. C.：Brookings Institute，1995.

[17] 刘秀秀. 新时代国家治理中技术治理的双重维度及其出路 [J]. 行政管理改革，2019，（10）：65-70.

[18] 盛小平，田婧，向桂林. 科学数据开放共享中的数据质量治理研究 [J]. 图书情报工作，2020，64（22）：11-24.

[19] 翟军，李晓彤，苗珍珍，等. 我国开放政府数据“脏数据”问题研究及应对——地方政府数据平台数据质量调查与分析 [J]. 图书馆，2019，（1）：42-51.

[20] 刘文奇. 中国公共数据库数据质量控制模型体系及实证 [J]. 中国科学（信息科学），2014，44（7）：836-856.

[21] Carroll S R，Garba I，Figueroa-Rodríguez O L，et al. The CARE Principles for Indigenous Data Governance [J]. Data Science Journal，2020，19：1-12.

[22] Taloni A，Scorcia V，Giannaccare G. Large Language Model Advanced Data Analysis Abuse to Create a Fake Data Set in Medical Research [J]. JAMA Ophthalmology，2023，141（12）：1174-1175.

[23] 盛小平，郭道胜. 科学数据开放共享中的数据安全治理研究 [J]. 图书情报工作，2020，64（22）：25-36.

[24] OpenAI（2023）. GPT-4 Technical Report [R/OL]. [2024-04-15]. https://cdn.openai.com/papers/gpt-4.pdf.

[25] 司莉，邢文明. 科学数据管理与共享的理论与实践 [M]. 武汉：武汉大学出版社，2017.

[26] 周毅，郭朗睿. 公共数据开放中隐性数据安全风险治理机制的

构建及其实现［J］. 情报理论与实践，2024，47（12）：63-71.
［27］ March C，Schieferdecker I. Technological Sovereignty as Ability，Not Autarky［J］. International Studies Review，2023，25（2）：viad012.
［28］ Vigliarolo B. Italy Bans ChatGPT for“Unlawful Collection of Personal Data”［EB/OL］.［2023-11-02］. https://www.theregister.com/2023/03/31/italy_bans_chatgpt_for_unlawful/.
［29］ 中国法院网. 破冰：首例人工智能文生图案生效——北京互联网法院探索为“AI 文生图”著作权划定边界［EB/OL］.［2024-02-05］. https://www.chinacourt.org/article/detail/2024/02/id/7796864.shtml.
［30］ THALER v. PERLMUTTER，1：22-cv-01564，（D. D. C. Feb 07，2023）ECF No. 17［EB/OL］.［2024-07-15］. https://www.courtlistener.com/docket/63356475/17/thaler-v-perlmutter/.
［31］ 薛澜，赵静. 走向敏捷治理：新兴产业发展与监管模式探究［J］. 中国行政管理，2019，（8）：28-34.
［32］ 沈费伟. 数字乡村敏捷治理的实践逻辑与优化路径［J］. 求实，2022，（5）：96-108，112.
［33］ 张桂蓉，王雨晴. 数智赋能推进敏捷化应急情报体系研究［J］. 现代情报，2024，44（4）：3-10，31.
［34］ 朱国伟，周妍池，刘银喜. 敏捷治理推动数字政府建设：发展趋势与实现路径［J］. 电子政务，2024，（2）：55-64.
［35］ 胡贵仁. 模糊应对、数字赋能与敏捷治理——超大城市风险防控的逻辑转向及困境超越［J］. 城市问题，2022，（9）：87-94.
［36］ 王英，卢国强. 负责任的社会科学数据治理的内涵、特征与层次［J］. 现代情报，2025，45（1）：124-134.
［37］ 赵梓羽. 生成式人工智能数据安全风险及其应对［J］. 情报资料工作，2024，45（2）：30-37.
［38］ 张涛. 人工智能治理中“基于风险的方法”：理论、实践与反思［J］. 华中科技大学学报（社会科学版），2024，38（2）：66-77.
［39］ 张欣. 面向产业链的治理：人工智能生成内容的技术机理与治理逻辑［J］. 行政法学研究，2023，（6）：43-60.
［40］ 王静，王鹏. 智慧图书馆生成式 AI 大模型风险治理机制研究［J］. 情报杂志，2024，43（8）：190-197.

（责任编辑：郭沫含）

（上接第 99 页）

略。同时，对新加坡数据治理体系的研究体现出立足全球视野，对不同国家和地区数据治理体系建设模式、关键导向、内容要点等展开深入调查的丰富空间，也需要确认在保持个体特质的前提下如何实现相互融通的方法和策略，更要深入我国实际积极洞察数据治理体系建设的应有内涵与不同模式、从中央到地方的数据治理体系的构建逻辑和推进策略、建设成效与存在局限的原因、不同数据治理维度如何深化设计与落实等，这些都呈现为未来的研究空间。

参 考 文 献

［1］ 夏义堃. 试论政府数据治理的内涵、生成背景与主要问题［J］. 图书情报工作，2018，62（9）：21-27.
［2］ 王翔，郑磊.“公共的”数据治理：公共数据治理的范围、目标与内容框架［J］. 电子政务，2024，（1）：2-9.
［3］ 安小米，郭明军，魏玮，等. 大数据治理体系：核心概念、动议及其实现路径分析［J］. 情报资料工作，2018，39（1）：6-11.
［4］ Alhassan I，Sammon D，Daly M. Data Governance Activities：A Comparison Between Scientific and Practice-Oriented Literature［J］. Journal of Enterprise Information Management，2018，31（2）：300-316.
［5］ Thompson N，Ravindran R，Nicosia S. Government Data Does Not Mean Data Governance：Lessons Learned From a Public Sector Application Audit［J］. Government Information Quarterly，2015，32（3）：316-322.
［6］ 董焕晴，何树坤，曹高辉. 数字健康产业数据治理体系研究［J］. 现代情报，2024，44（9）：131-141，153.
［7］ 黄璜，孙学智. 中国地方政府数据治理机构的初步研究：现状与模式［J］. 中国行政管理，2018（12）：31-36.
［8］ 左美云，王配配. 数据共享视角下跨部门政府数据治理框架构建［J］. 图书情报工作，2020，64（2）：116-123.
［9］ 马广惠，安小米，宋懿. 业务驱动的政府大数据平台数据治理［J］. 情报资料工作，2018，39（1）：21-27.
［10］ Mao Z J，Wu J Y，Qiao Y L，et al. Government Data Governance Framework Based on a Data Middle Platform［J］. Aslib Journal of Information Management，2022，74（2）：289-310.
［11］ 赵蕊蕊，陈俊蕾，张潇月.“周期—工具—主体”协同视角下我国公共数据治理政策解析［J］. 情报资料工作，2024，45（9）：51-63.
［12］ 安小米，王丽丽，许济沧，等. 我国政府数据治理与利用能力框架构建研究［J］. 图书情报知识，2021，38（5）：34-47.
［13］ 夏义堃. 政府数据治理的维度解析与路径优化［J］. 电子政务，2020（7）：43-54.
［14］ 夏义堃. 试论数据开放环境下的政府数据治理：概念框架与主要问题［J］. 图书情报知识，2018，35（1）：95-104.
［15］ 孙建军，马亚雪. 面向多元场景的数据治理：进展与思考［J］. 图书与情报，2023（4）：1-11.
［16］ 黄璜，孙学智. 中国地方政府数据治理机构的初步研究：现状与模式［J］. 中国行政管理，2018（12）：31-36.
［17］ Open Data Watch. Singapore Open Data［EB/OL］.［2024-09-11］. https://odin.opendatawatch.com/Report/countryProfileUpdated/SGP?year=2022.

（责任编辑：杨丰侨）