

徐淋楠, 段美珍, 寇晶晶. 开放共享环境下科学数据安全治理路径[J]. 中华医学图书情报杂志, 2022, 31(6): 1-8.

DOI: 10.3969/j.issn.1671-3982.2022.06.001

· 研究与探讨 ·

开放共享环境下科学数据安全治理路径

徐淋楠¹, 段美珍^{2,3}, 寇晶晶⁴

[摘要]深入探究科学数据安全治理路径, 以期为我国数据安全战略的实施提供参考。基于信息生命周期管理模型, 从制度、技术、设施、人员 4 个要素出发对科学数据在存储、管理、应用 3 个层面的安全问题进行归纳, 并从科学数据治理主体出发探究治理路径, 进而提出我国政府应从宏观层面完善以数据安全为核心的基础性制度建设, 研究机构应从中观层面构建全面的科学数据安全机制, 科研人员应从微观层面提高科学数据安全素养等建议。

[关键词]开放获取; 科学数据; 数据安全; 治理路径

[中图分类号]G203 **[文献标志码]**A **[文章编号]**1671-3982(2022)06-0001-08

Research on the governance path of scientific data security in open access environment

XU Lin-nan, DUAN Mei-zhen, KOU Jing-jing

(1.School of Information Management, Nanjing University, Nanjing 210023, China; 2.Information Research Center of Military Sciences, Academy of Military Sciences, Beijing 100142, China; 3.Library of Academy of Military Sciences, Beijing 100039, China; 4.University of International Relations Library, Beijing 100091, China)

Corresponding author: DUAN Mei-zhen

[Abstract]To explore the scientific data security governance path, so as to provide reference for the implementation of data security strategy in China. Based on the information life cycle management model and considering the four elements of system, technology, facilities and personnel, the safety problems of scientific data storage, management and application were summarized and the governance path from scientific data governance subjects was explored. It is proposed that the government should improve the basic system construction with data security as the core at the macro level, research institutions should build a comprehensive scientific data security management mechanism at the middle level, and researchers should improve the scientific data security management literacy at the micro level.

[Key words] Open access; Scientific data; Data security; Governance path

[基金项目]国家社会科学基金青年项目“智慧图书馆建设评价模型与应用研究”(21CTQ009)

[作者单位]1.南京大学信息管理学院, 江苏 南京 210023; 2.军事科学院军事科学信息研究中心, 北京 100142; 3.军事科学院图书馆, 北京 100039; 4.国际关系学院图书馆, 北京 100091

[作者简介]徐淋楠(1998-), 女, 硕士研究生, 研究方向为数字图书馆技术、信息资源管理。

[通讯作者]段美珍(1992-), 女, 博士, 馆员, 研究方向为智慧图书馆、开放获取与信息资源建设。E-mail: duanmeizhen12@163.com

大数据时代, 数据已成为科学研究和产业发展的关键核心, 受到了世界各国的高度重视。在科学研究领域, 科学研究方法和知识生产的范式都发生了巨大变化^[1], 封闭式的科学研究已经不再适应时代的发展, 打破“信息孤岛”、消除数据闭塞已成为世界各国科研工作者的共识。尤其是在构建人类命运共同体的时代发

展背景下,跨地域、跨机构和跨学科研究成为常态,开放合作与数据共享成为使众多科学问题得以进一步深入探究与解决的关键,这一点在全球应对新型冠状病毒肺炎的问题上已经得到了充分的验证。作为推动开放科学发展的关键组成部分,科学数据开放共享不仅能够降低科研成本和投入,实现公众利益最大化,还能够为科学研究成果的可重复、可验证创造条件,有助于提升科研成果的透明性和准确性等,进而达到肃清学术风气的目的。但作为国家社会经济和科研创新发展的重要战略资源,科学数据在开放共享的过程中,也出现了许多数据安全问题。

保障科学数据安全,是开放共享的基础和前提^[2]。为此,多个国家和地区出台了相关政策以推进科学数据安全保障的落实。仅 2018 年一年就有欧盟《一般数据保护条例》(General Data Protection Regulation, GDPR)^[3]、英国《2018 数据保护法》(Data Protection Act 2018)^[4]、我国《科学数据管理办法》^[5]等政策的出台。2020 年 9 月,我国在主题为“抓住数字机遇,共谋合作发展”的国际研讨会上提出了《全球数据安全倡议》,呼吁各国秉持发展和安全并重的原则,保护好涉及本国国家安全、公共安全、经济安全和社会稳定的重要数据^[6]。2021 年 6 月,我国出台了第一部专门针对数据安全的法律《中华人民共和国数据安全法》^[7]。这些政策和倡议的提出充分体现了科学数据对国家科技创新的重要性,也充分说明了各国政府对科学数据安全问题的重视。数据作为与劳动、资本等生产要素比肩的核心生产要素,已成为国家之间竞争的焦点。谁掌握了和占有了更多的科学数据资源,谁就更有可能在新一轮的科技竞争中掌握话语权。因此,我国必须重视关于开放共享下科学数据安全问题的研究,建构出与时代发展相契合的安全战略和治理路径以应对激烈的国际竞争和博弈。

关于数据安全的讨论,国内学术界主要集中在“政府公共数据”^[8-11]、“个人隐私数据”^[12-14]、“健康医疗数据”^[15-17]等方面,专门针对科学数据安全问题的讨论相对较少。现有的科学数据安

全研究主要包括对科学数据共享后隐私保护的政策解读^[18-20]和方法探析^[21]、对科学数据知识产权方面的法律探讨^[22]、对保障科学数据开放安全的技术研究^[23],以及对影响科学数据开放安全程度的因素分析^[24]等方面。除此之外,有一些学者从不同角度对开放共享环境下科学数据安全的治理路径提出了建议。如有学者从科学数据的机密性、完整性、可用性角度提出了针对科学数据安全的治理对策^[25],有学者从制度、基础设施、数据素养、实施 4 个层面构建了高校安全数据的治理框架^[26],还有学者从研发人员、作者、我国政府、外国政府 4 个主体的角度提出了云环境下科学数据的治理范式^[27]。本文则主要基于信息生命周期理论,从科学数据的存储、管理、应用 3 个层级由下至上展开讨论,进而从宏观、中观和微观的视角提出开放共享环境下科学数据安全治理路径。

1 研究框架

科学数据安全问题贯穿在数据管理的每一个流程和环节中,各环节又受多重因素的影响。结合有学者提出的信息生命周期管理的层次模型与科学数据管理实践^[28],本文认为可以从存储、管理、应用 3 个层级和阶段对科学数据管理中可能存在的安全问题进行梳理提炼。

根据 WSR 系统方法论,即“物理(Wuli)—事理(Shili)—人理(Renli)方法论”,在分析某一个对象或解决某一问题时通常会涉及物理、事理、人理 3 个方面的要素和内容。其中,“物理”主要是指在分析某一个对象或解决某一个问题时人所面对的物质客观存在。在科学数据安全治理过程中,“物理”主要涉及设备和技术等客观的物理存在。“事理”主要是指改变物理层面的客观存在及其规律时所应用的有效方式和对策。在科学数据安全治理过程中,“事理”主要指治理主体制定的相关制度规范和策略。“人理”是指在分析某一对象或解决某一问题时涉及到的主体(人、人群和团体)及其之间的关系和变化,使人们能根据可接纳的道理实现项目或达成问题的原定目标。在科学数据安全治理过程

中，“人理”主要涉及政府、科研机构和科研人员等科学数据安全治理的利益相关主体。在具体安全问题分析的过程中，本文结合现有研究成果和实践中存在的问题，按照制度、技术、设施和人员的要素分析思路，对存储、管理、应用 3 个不同层级和阶段中可能出现的科学数据治理问题及成因进行详细梳理。

最后，从利益相关者角度出发，按照政府、科研机构和科研人员等参与主体分类，探究开放共享环境下科学数据安全的治理路径（图 1）。

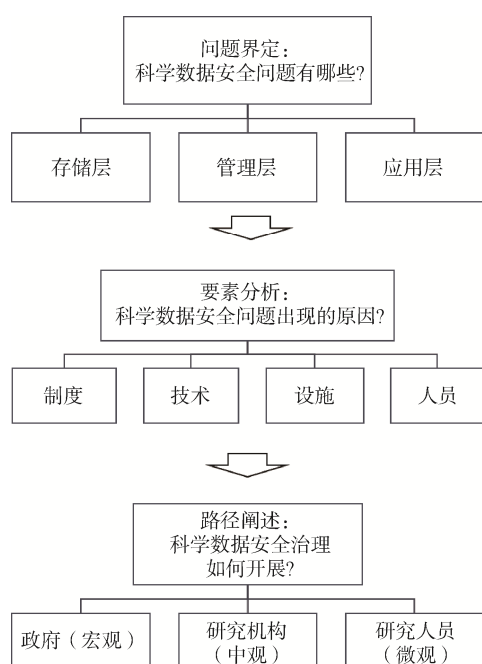


图 1 开放共享环境下科学数据安全研究框架

2 开放共享环境下科学数据安全问题及成因

2.1 科学数据存储层面的安全问题及成因

科学数据的保存和存储是科学数据管理的第一步，在这一过程中可能会出现存储数据丢失、数据存储格式不规范、数据版本不完整等数据安全问题。

2.1.1 存储数据丢失

存储数据丢失通常涉及设施、技术和人员 3 个方面的问题。设施设备方面，如用于存储的硬件设备可能会由于超出容量等各种突发原因崩溃、损坏或丢失，造成存储的部分甚至全部数据丢失；技术方面，如存储系统在存储操作过程中可能会被病毒入侵或操作失误使数据遭到损坏或

丢失但无法复原等；人员方面，如科研人员未及时上传相关研究数据或未进行充分的数据备份，以及其他管理人员误操作等都会导致相关数据缺失或丢失。

2.1.2 数据存储格式不规范

数据存储格式问题受制度规范影响较大。目前国际和国内还未形成标准化的科学管理规范，不同机构对同一学科甚至同一类型科学数据的存储要求都大相径庭。各种主客观原因导致数据存储格式多样，数据与软件不兼容，原始数据无法访问和互操作。在这种情况下，即使数据按规定上传和共享，也不具备通用性，无法供其他研究人员使用。

2.1.3 数据存储版本不完整

存储版本不完整、存储数据有误等操作性问题通常与实施数据操作的人员有较大关联。在实际研究过程中，科研人员可能缺乏数据版本保存意识，仅上传最终科研成果中涉及的数据。然而，得出实验结果的前置数据也同样具有较高的存储价值，如果仅上传最后的结果数据，则其他研究人员无法重复进行实验以验证实验结果的有效性，也无法利用已有实验数据得到更多的科学发现。对于长期受资助的项目，如果科研人员未按研究机构规定定期上传和管理科学数据，那么造成的损失和后果将更为严重。除此之外，一些有价值的科学数据被创建后，可能被研究人员误认为无须保存导致被删除等，从而影响后续的科研工作。

2.2 科学数据管理层面的安全问题及成因

科学数据集中存储后需要对其进行合理、高效的管理，在这一层面可能面临统一的数据安全分级标准缺失、数据泄漏和数据窃取等数据安全问题。

2.2.1 缺乏统一的数据安全分级标准

不同阶段的科学数据的价值和保密程度不同，因此需要根据不同价值和密级制定对应的保密管理和审查策略。在国内，虽然国务院办公厅发布的《科学数据管理办法》提出了科学数据要分级分类管理，但目前国内仍然没有较为统一规

范的数据安全分级标准。此外,不同类型科学数据的开放尚未统一参考标准,这就导致各科研机构开放程度差异较大。有的科研机构过于谨慎,封锁绝大多数科学数据使其难以共享;有的科研机构则对科学数据的重视程度不够,随意公开科学数据,导致科研成果被窃取等。即使在科学数据管理实践发展较好的国家,不同机构的数据安全分级标准也难以统一规范。以美国高校为例,加利福尼亚大学伯克利分校根据数据的敏感性提出了 3 级科学数据分级标准,哈佛大学基于其信息安全准则制定了 5 级科学数据分级标准^[29]。

2.2.2 数据泄露

数据泄露现象的产生受科学数据利益相关主体多方面主客观因素的影响。科学数据管理过程中涉及的环节和人员较多,数据泄露风险较大。从科研人员和数据管理人员的角度来说,部分人员数据安全保护意识不强、数据安全级别识别能力不足等都会导致数据泄露。从政府和机构层面来说,现行科学数据的安全等级划分不够明确、数据管理系统的安全性能和技术保障能力不足等,都不利于科学数据安全工作的开展。此外,国内法律法规对科学数据泄露和侵权的惩处力度较低,会存在部分科研机构的数据管理人员受到利益诱惑主动将重要的科学数据泄露给其他科研机构的现象。

2.2.3 数据窃取

科学数据被窃取是引发科学数据安全问题的又一关键因素,并且这一现象时有发生。如 2021 年,英国开放大学发现其开放获取知识库中的大量博士论文被挂在亚马逊上售卖,影响较为恶劣。为了保护学生的著作权益,英国开放大学被迫停止了其机构知识库的开放获取。涉及国家安全层面的科学数据被窃取问题尤为突出。部分国家为了在国际上获取更多的话语权,以高科技技术手段大规模窃取、监视他国的重要科学数据,这对构建共建共享、合作共赢的世界数字经济体系产生了极大的损害。数据窃取造成的数据安全问题虽然对科学数据管理的利益相关者而言属于不可抗力,也非其主观意愿,但仍应从技术设备等

要素出发对数据安全问题进行排查和反思,以避免数据窃取风险^[30]。

2.3 科学数据应用层面的安全问题及成因

科学数据开放共享的最终目的是为了应用,科研人员在实际应用中可能会遇到数据所有权模糊、数据篡改和数据滥用等安全问题。

2.3.1 数据所有权模糊

缺乏明确规范的科学数据产权界定制度是导致数据所有权模糊,进而引发科学数据安全应用问题的关键因素之一。如科研人员在获取科学数据后由于权利边界的不确定性,可能存在不敢使用或过度使用的现象;当数据的所有权为多个主体时,数据开放带来的权益分配也可能引发纠纷。因此,在推进科学数据开放共享的进程中,必须要正视数据权益问题,明确数据主权和治权。

2.3.2 数据篡改

信任是开放科学数据的基础,也是开放科学环境下科学合作的基石。无论是开放前数据的篡改,还是开放后数据应用的篡改,对科学研究的发展都会产生严重的影响。科学数据应用阶段的数据篡改不仅涉及数据安全问题,还是违反学术诚信和学术道德的表现。如在实际科研过程中,部分科研人员会存在不标明数据来源,将他人的科研成果占为己有,篡夺他人的知识产权的现象;有些科研人员甚至会在论文引用后篡改原始数据,使其强行符合自己的研究结果等。

2.3.3 数据滥用

有一些学科领域和研究课题所涉及的科学数据通常包含了个人和机构等不宜随意公开应用的数据信息。尤其是在医药卫生领域和统计学领域,较多临床数据和调查数据包含了个人隐私信息,这些数据信息在开放共享后,使用者获取的门槛和成本降低,容易导致隐私数据的泄漏和滥用。

3 开放共享环境下科学数据安全的治理路径

政府、科研机构及科研人员是科学数据开放共享过程中最为核心的主体,在科学数据的生产、资助、组织、管理、利用过程中扮演着不同的角色。其中,政府是科学数据的宏观层面的管理者,主要承担了研究资金资助和政策法律制定

的责任。科研机构是中观层面的管理者，负责制定符合科研诚信和学术道德的科学数据管理规范，管理科研人员受资助项目的实施，提出科学数据向公众开放的策略，保障开放共享下科学数据的安全。科研人员既是科学数据的生产者和利用者，也是微观层面的管理者，需要按照规定及时公开计划内应共享的科学数据，遵守科学数据的管理规范和相关的法律法规。

3.1 完善以数据安全为核心的基础性制度建设

政府在完善和优化科学数据的安全治理工作中首先应解决我国数据安全顶层设计不完备的问题。虽然目前我国已有包括《科学数据管理办法》在内的多项数据管理政策，但相关政策缺乏系统性，完备、细致的制度框架还未形成，不能很好地解决当前科学数据所面临的安全问题。因此，我国政府需持续细化和完善相关制度。

3.1.1 建立健全科学数据的产权制度

针对科学数据所有权模糊的问题，我国尚无明确的法律法规出台。因此，应在国家层面推进科学数据产权制度的建立，厘清科学数据的所有权边界，明确科学数据的认定、转让、使用规则，规范科学数据各利益相关主体在保护科学数据上所应承担的责任，健全科学数据知识产权的保护制度。除此之外，对数据窃取、泄漏、滥用等数据侵权问题，除了《数据安全法》中提出的加大惩处力度、提高违法成本、细化惩处机制外，还应加快健全个人信息的授权保护制度，通过强制明示授权许可等方式切实保护用户的权利。

3.1.2 制定科学数据分级保护制度

《中华人民共和国数据安全法》第三章第十九条提出要对数据实行分级分类保护，但并未制定出详细的数据分级保护指导标准。因此，我国政府需要细化制定科学数据安全分级管理的具体准则，在鼓励依法合规使用非敏感科学数据的同时，保护敏感科学数据的安全，避免可开放的不开放及不可开放的被泄漏等情况。在科学数据的分级上，已有部分大学及科研机构进行了实践。如美国国家航空与宇宙航行局（National Aeronautics and Space Administration, NASA）对地观测数据信息

系统（Earth Observing System Data and Information System, EOS DIS）将科学数据处理层级分为 level 0、level 1A、level 1B、level 2、level 3、level 4 共 6 个层级以辅助海量科学数据的处理^[31]。美国加利福尼亚大学伯克利分校将科学数据划分为极低（公共信息）、低（非公开、不敏感和去身份的信息）、中（中度敏感的个人可识别信息）、高（非常敏感的个人可识别信息）4 个级别^[32]，以实现严格的科学数据保护。我国政府也应基于现实需要和已有经验完善科学数据的分级保护制度。

除此之外，科学数据安全分级规则的制定还要考虑学科和行业的特点，数据处理的程度受到数据用途、数据价值及数据采集等多个因素的影响。如果是宇宙理论方面的探索，则需要对仪器产生的异常值、缺失值数据进行加工处理后将其纳入分析进程，但如果是探究宇宙生命的可能性，则需要尽可能地保存原始的、全面的、完整的信息。因此，科学数据分级不能一概而论，需要具体问题具体分析。

3.1.3 通过关键主体将制度政策落到实处

国内科研资助机构通常是政府实施科研资助与管理等的关键主体，在科学数据安全治理方面发挥重要的作用。因此，在科学数据安全政策落实过程中，政府宏观管理部门应充分发挥所辖机构和组织的主体作用，根据其职能权力赋予相应的职责和任务。同时，相关主体应在国家和政府宏观政策和法律的指导下，积极制定既符合国家和政府诉求，又能够保障科研机构、科研人员等其他相关者利益的细则和要求。如科研资助机构可通过制定科学数据管理指南等，强制要求受资助的科研机构和科研人员按照科研项目资助的周期阶段，对科学数据进行管理和提交，并将受资助的科研项目的数据安全管理作为项目完成的指标之一进行审核。国家科学数据管理平台作为数据管理的实际操作者，要从数据管理具体实施机制的制定、技术设施和人员的配置等更加微观的层面提升系统平台的数据安全管理能力和数据可重用水平等，以期为中观和微观层面科学数据的安全治理提供借鉴和补充。

3.2 构建全面的科学数据安全管理机制

科研机构作为中观层面的管理者担任了承前启后的责任,既是政府制定相关法律政策的具体实施者,又是科研人员是否履行科学数据安全保护责任的监督者。因此,作为海量科学数据的集中地,科研机构需在精进数据安全保护技术的基础上,构建全面的数据安全管理机制。

3.2.1 建立科学数据隐私保护机制

科研机构首先应对包含隐私信息的科学数据进行处理,通过数据匿名、限制准入、资格审查等手段对科学数据进行保护。以苏格兰纵向研究(The Scottish Longitudinal Study, SLS)^[33]对敏感数据的处理为例,SLS 拥有人口普查数据、重大事件数据(出生、婚姻、死亡)、教育数据、卫生数据等信息,用来审视和解决一系列社会经济问题,是宝贵的社会决策信息来源。为了保护个人隐私和数据安全,SLS 采取了如下措施:一是数据集以匿名形式存在,调查中涉及到的个人会模糊掉姓名和地址;二是数据存储在有密码保护的独立网络上,用户只能在特定的受保护位置访问数据;三是负责维护和督导的理事会审查每一个研究申请,并进行风险评估,不授权任何需要确认个人数据的研究;四是严格控制访问程序,如果科研人员需要远程分析数据,则由现场相关人员代为运行统计程序。我国科研机构应参考已有成功经验,依据数据特性完善科学数据的隐私保护机制。

3.2.2 制定科学数据使用管理机制

科学数据格式、标准的不统一对数据的完整性和通用性造成了阻碍,因此需要对科学数据的上传和引用标准进行规范。在科学数据标准化方面,Open AIRE 为我国提供了很好的参考。Open AIRE 作为欧盟委员会开放政策的基础支撑机构,为科研人员提供了覆盖所有科学数据类型标准指南^[34]。在数据引用方面为科学数据制定了唯一的引用标识,使其能够如其他文献资源一般自由、规范地流通。我国可参考德、英、澳等国家联合建立的 DataCite 机构的运行程序来构建此类机制。DataCite 等机构专门用于登记科学数据并

为其分配永久标识符,使科学数据可作为独立的、可应用的、唯一的科学对象被使用^[35]。

3.2.3 完善科学数据备份容灾机制

建立科学数据的备份容灾机制是应对科学数据遗失的重要手段。科研机构需采用合适的数据库备份介质和策略,以应对供电中断、硬件崩溃等突发情况。当然这一机制也需要科学数据存缴者的配合,如美国地震科学注册研究中心(Incorporated Research Institutions for Seismology, IRIS)在其数据提交协议中规定^[36],数据提交者必须周期性地将科学数据转录到新媒体中,通过对数据的定期管理来保证数据的安全性和永久可用性,维护数据集的多个副本以防止单个数据集的丢失或物理损坏。

3.2.4 强化科学数据追踪防御机制

开放共享科学数据对当前的信息技术提出挑战,必须开发满足共享机密、敏感数据的安全技术来防止意外事故和蓄意攻击。当前我们不能仅通过对源代码和安全系统架构保密的方式保障数据安全,还需要开放源代码等信息,在攻击者分析漏洞并攻击后对系统进行更为彻底的测试,这种“开放性最终形成更好的安全性(openness ultimately breeds better security)”的做法可以帮助我们更好地保障数据安全。除了对现有系统的测试,科研机构还应重视数据溯源技术应用,以达到防篡改、防泄露、防攻击、防病毒的目的。

3.3 提高科学数据安全管理素养

科研人员作为生产和利用科学数据的重要主体,受到政府和科研机构的双重管理,是上述政策和机制的践行者。从这一层面维护科学数据安全,需要科研人员遵守法律和道德的双层约束。

3.3.1 遵守科学数据管理规范

科研人员作为科学数据的生产者时,一方面要配合科研机构的备份容灾机制,按规定程序制定数据管理计划,定时上传管理科学数据,做好科研项目全流程的数据记录及备份,积极履行数据公开和共享的责任,在数据出现突发问题时,及时向负责机构报告并就此紧急事件快速作出反应;另一方面,提交数据时应按照科研机构的统

一标准进行上传,遵守科学数据管理规范,保证数据的可用性和完整性。

3.3.2 增强科研诚信道德意识

科研人员作为科学数据的使用者时,首先要遵守政府制定的各项法律法规,以我国《科学数据管理办法》和《中华人民共和国数据安全法》为参考,对科学数据的存储、管理、应用进行谨慎处理,不因经济利益等做出数据泄漏、篡改、窃取等数据侵权行为,遵守学术道德。当然,在个人数据权益被侵犯时,也应运用法律武器追究侵权行为,维护自己的合法权益。其次要遵守科研机构数据获取程序,按准入和使用要求合规利用数据,规范科学数据处理行为,促进科学数据的开放共享。

4 结语

科学数据走向开放共享是大数据时代的主流趋势,保障这一趋势下的科学数据安全对降低科研成本、推动学科创新、肃清学术风气、增强科研实力具有重要意义。本文基于制度、技术、设施、人员等要素对科学数据存储、管理、应用中可能存在的安全问题进行分析,并从政府、科研机构 and 人员等利益相关主体的角度提出了开放共享环境下科学数据安全的治理路径,有一定的指导价值。但本文研究还存在一定的不足,后续将研究和制定更加具体的实施细则,助力中国数据安全战略的构建和实施。

【参考文献】

- [1] 陈传夫,李秋实.数据开放获取使科学惠及更广:中国开放科学与科学数据开放获取的进展与前瞻[J].信息资源管理学报,2020,10(1):4-13.
- [2] 李宜展,刘细文,李泽霞,等.科学数据安全边界概念模型研究:基于利益相关者视角[J].中国科学基金,2022,36(2):339-347.
- [3] ESRF. General Data Protection Regulation(GDPR)[EB/OL]. [2022-04-14]. <http://www.esrf.eu/GDPR>.
- [4] Department for Digital, Culture, Media& Sport and Home Office. Data Protection Act 2018[EB/OL]. [2022-03-14]. <https://www.gov.uk/government/collections/data-protection-act-2018>.
- [5] 国务院办公厅关于印发科学数据管理办法的通知[EB/OL]. [2022-03-14]. http://www.gov.cn/gongbao/content/2018/content_5283177.htm.
- [6] 全球数据安全倡议(全文)[EB/OL]. [2022-04-07]. http://www.gov.cn/xinwen/2020-09/08/content_5541579.htm.
- [7] 中华人民共和国数据安全法[EB/OL]. [2022-04-07]. <http://www.npc.gov.cnnpc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>.
- [8] 陆莉.“数据资产框架”视角下我国政府公共安全数据开放现状、问题与对策[J].情报杂志,2020,39(11):104-110.
- [9] 庄国波,韩惠.5G时代政府数据开放共享的安全风险及防范[J].理论探讨,2020(5):48-54.
- [10] 佟林杰,刘博.信息生态视域下政府数据开放中的数据安全和隐私保护问题研究[J].图书馆理论与实践,2020(5):67-72.
- [11] 冉连,张曦.地方政府数据开放中的数据安全风险研究:基于全国33个地级市政策文本的内容分析[J].情报杂志,2020,39(11):96-103.
- [12] 祝阳,李欣恬.大数据时代个人数据隐私安全保护的一个分析框架[J].情报杂志,2021,40(1):165-170.
- [13] 宋阳,张崧,张志勇,等.物联网+大数据环境下个人信息安全防范与保护措施研究[J].情报科学,2020,38(7):93-99.
- [14] 陆康,刘慧,任贝贝,等.智慧图书馆用户数据隐私保护研究:基于《中华人民共和国网络安全法》和《一般数据保护条例》的文本启示[J].图书馆理论与实践,2020(3):17-21.
- [15] 肖瑗,卢雅雯,吕智慧,等.生物医疗大数据隐私安全保障机制研究[J].计算机应用与软件,2021,38(2):318-322.
- [16] 周正强,陈玉玲,李涛,等.基于联盟链的医疗数据安全共享方案[J].应用科学学报,2021,39(1):123-134.
- [17] 冯涛,焦滢,方君丽,等.基于联盟区块链的医疗健康数据安全模型[J].计算机科学,2020,47(4):305-311.
- [18] 魏来,李思航.国内外科学数据隐私保护政策比较研究[J].新世纪图书馆,2020(12):17-23.
- [19] 秦顺,邢文明.开放·共享·安全:我国科学数据共享进入新时代:对《科学数据管理办法》的解读[J].图书馆,2019(6):36-42.
- [20] 姜鑫,马海群,王德庄.国外科研机构开放科学数据与个人数据保护的政策协同研究:基于爱丁堡大学《数据保护政策》的案例分析[J].档案学研究,2020(4):135-143.
- [21] 朱贝,王传清.我国科学数据共享中的隐私治理探析[J].图书情报工作,2020,64(22):37-47.
- [22] 许燕,麻思蓓,郑彦宁,等.科学数据的法律属性与知识产权管理[J].科技管理研究,2020,40(22):177-182.
- [23] 魏银珍,邓仲华,关玉蓉,等.一种基于区块链与智能合约的科学数据安全溯源方法[J].现代情报,2021,41(1):32-38.
- [24] 刘晓婷,佟泽华,薛晓娜,等.科研协同中数据安全共享的博弈分析及仿真研究[J].新世纪图书馆,2020(5):40-47.
- [25] 盛小平,郭道胜.科学数据开放共享中的数据安全风险治理研究[J].图书情报工作,2020,64(22):25-36.

- [26] 刘桂锋, 阮冰颖, 包翔. 数据生命周期视角下高校科学数据安全内容框架构建[J]. 情报杂志, 2021, 40(2): 146-153.
- [27] 肖冬梅, 孙蕾. 云环境中科学数据的安全风险及其治理对策[J]. 图书馆论坛, 2021, 41(2): 89-98.
- [28] 粟湘, 郑建明, 吴沛. 信息生命周期管理研究[J]. 情报科学, 2006, 24(5): 691-696.
- [29] 杜宇骁, 龚城, 伏安娜, 等. 哈佛大学 Datatags 数据分级系统研究及启示[J]. 图书馆杂志, 2019, 38(8): 17-26.
- [30] 博士论文被盗卖, 谁让开放获取成为开放盗窃? [EB/OL]. [2022-03-19]. <https://c.m.163.com/news/a/GF22P67H05119GS3.html>.
- [31] 吴培中. 美国地球观测数据和信息系统的宏观结构[J]. 国际太空, 2000(8): 23-29.
- [32] Berkeley Information Security Office. How to classify research data[EB/OL]. [2022-03-14]. <https://security.berkeley.edu/education-awareness/best-practices-how-tos/how-classify-research-data>.
- [33] Scottish Longitudinal Study Development & Support Unit. What data are included?[EB/OL]. [2022-03-14]. <https://sls.lscs.ac.uk/guides-resources/>.
- [34] Príncipe P, Rettberg N, Rodrigues E, *et al.* Open AIRE guidelines : Supporting interoperability for literature repositories, dataarchives and CRIS[J]. *Procedia Computer Science*, 2014, 33: 92-94.
- [35] Brase J. Data Cite-A global registration agency for research data[EB/OL]. [2022-03-14]. <https://ideas.repec.org/p/rsw/rswwps/rswwps149.html>.
- [36] Incorporated Research Institutions for Seismology(IRIS), Data Services. Data Provider Agreement for contributors of data to the IRIS DMC[EB/OL]. [2022-03-14]. https://www.iris.edu/hq/files/programs/data_services/policies/Data_Provider_Agreement-V1.5.pdf.

[收稿日期: 2022-04-28]

[本文编辑: 孙伟娟]