情报视角下科技论文数据泄露风险的研判、规避与阻断*

王育英[1)] 王群燕[2)]

1)《情报杂志》编辑部,710054;2)中共陕西省委党校(陕西行政学院),710061;西安

摘 要 大国竞争使科研成果成为国外智库或情报机构收集情报的重要信息源之一,以科技论文为载体的科技交流数据泄露风险进一步增加。开展科技论文数据泄露风险研究,可为出版工作提供警示与参考。通过实例和定量分析阐释科技论文数据泄露风险防范的必要性,结合大数据特点分析数据泄露风险发生原因,指出数据泄露风险识别难点,运用知己知彼的情报学方略,从对内对外2个方面研判数据泄露风险,反向推理风险规避关键点,探寻出一条数据泄露风险溯源性阻断路径,即科技期刊出版单位应切实履行对作者的告知义务,创新告知形式方法,提高实效,同时细化对科技论文数据泄露风险的审查。

关键词 情报;科技论文;科技期刊;数据风险;数据泄露

Assessment, avoidance and blocking of data leakage risk in scientific papers from an intellegence perspective//WANG Yuying, WANG Qunyan

Abstract Great power competition makes scientific research achievements become one of the important information sources for foreign think tanks or intelligence agencies to collect intelligence, and the risk of data leakage during scientific and technological exchanges based on scientific papers has further increased. Conducting research on the risk of data leakage in scientific papers provides warnings and references for publishing work. This paper explains the necessity of preventing data leakage risk in scientific papers through examples and quantitative analysis, analyzes the causes of data leakage risk in combination with the characteristics of big data, points out the difficulties in identifying data leakage risk, applies the strategy of knowing oneself and the other in infomatics to judge the data leakage risks from both internal and external aspects. It reverses the key points of risk avoidance, explores a path to block the traceability of data leakage risk, namely, sci-tech journal publishers should effectively fulfill their obligation to inform authors, innovate the form and method of notification, improve the effectiveness, and refine the disclosure risk review of scientific papers content.

Keywords intelligence; scientific paper; scientific journal; data risk; data leakage

First-author's address Editorial Office of Journal of Intelligence, 710054, Xi'an, China

DOI:10.16811/j.cnki.1001-4314.2024.02.003

*2024年陕西省科学技术情报学会研究课题(2024KTF-06)

在大国科技竞争日趋激烈的背景下,每个国家都有各自的国家安全和利益,传统意义上"本身并无泄露问题可言"的科研成果有可能会被卷入大国竞争博弈中,成为竞争对手追踪的对象;原来"认为安全"的论文数据也有可能会通过出版渠道被国外智库或情报机构摄取,并经大数据关联分析,被提取出具有情报价值的信息。由此可见,以科技论文为载体的科技交流数据在大国博弈中泄露风险提高了,从情报视角看,科技论文数据已成为重要的开源情报源。随着我国保密管理相关法律条例的颁布和不断完善,尽管除了具有明确涉密性质的科研成果外,科技论文中一般较少出现涉密内容,但论文字里行间涉及一些敏感问题的表达还是有可能的。在大数据时代,这些隐匿在海量数据中的碎片化信息在技术加持下极有可能成为有价值的情报。因此,科技论文在出版前必须注意对相关问题做合理规避和处理,避免其出版后成为国外智库或情报部门的决策参考依据。

目前,学术界关于期刊、论文信息安全和泄密研究主要聚焦以下几方面:1)科技论文出版信息安全。王珏等[1]解析了开放科学环境下科技论文发表中的安全隐患与风险。张晶晶等[2]分析了农业科技期刊论文发表中的信息安全关键点。段尧清等[3]总结了目前我国科学论文发表中存在作者个人信息安全意识薄弱、内部人员信息泄密风险较大、技术进步加大安全监管难度和行业政策标准缺失4个信息安全问题,并提出了科学论文发表中信息安全水平的五维一体提升路径。2)数据泄密风险。柳厅文等[4]认为大数据时代公开数据中可能存在着极大的泄密隐患;马天一[5]分析了科学数据出版引发的泄密风险;秦晓雪[6]、唐迪等[7]、李品[8]分别分析了科技期刊、科技文献的泄密风险。3)泄密原因。秦晓雪[6]认为期刊泄密的原因有窃密技术发展、保密管理制度不全、责任主体保密意识淡薄等;唐迪等[7]从作者投稿、作者单位审查、编辑部处理稿件等环节分析了论文泄密原因。4)泄密应对举措。秦晓雪[6]提出应加强网络安全,健全并落实期刊保密管理制度,加强保密教育;代妮[9]提出科技期刊应强化保密意识,落实保密责任,加强技术监管。

上述研究从科技论文出版信息安全、数据泄密风险、泄密原因、泄密应对举措等多角度进行阐释,是本文重要的研究基础,除张晶晶等[2]指出的农业领域论文发表中的信息安全关键点之外,其研究着力点均集中在科技论文内容的外围,且提出的举措基本是对数据泄密风险的事后响应,缺少对科技论文数据泄露风险的事前研判,即未能深入研判论文内容本身。众所周知,科技论文数据泄露风险源头在于内容本身,如果能从源头上阻断风险数据,则可取得事半功倍之效。鉴于此,本文拟按照"原因分析—双向研判—规避阻断"的逻辑理路,以弥补上述研究缺口的尝试。首先结合大数据时代特点,陈述并分析科技论文数据泄露风险防范的必要性及原因和风险防范难点,再根据既有关于国外情报产品引用源的研究成果,反向推理出科技论文数据泄露风险关键点,最后从科技期刊出版角度提出数据泄露风险阻断路径,希望能为期刊出版相关人员提供些许警示。

1 科技论文数据泄露风险及其防范的必要性

1.1 理论基础

本研究有以下几组概念需要说明。1)科技论文数据。科技论文数据因科学研究特点不同可分为基础研究数据和应用研究数据。科技论文内容除了包含科技专业领域研究数据外,还可能包含国家政治、经济、军事、历史、文化等其他领域数据。科技论文因内容不同其数据泄露风险发生率也不相同,如反映国家尖端技术和科技前沿、具有明确领域范畴和内容指向的数据具有较高泄露风险。2)风险。Renn[10]认为风险的一种取向是概率(possibility),是行为主体通过理性预期和历史经验对事件、行为负面可能性作出的主观推断。既然风险是一种概率、测度,那么可以肯定的一点是,任何风险都具有不确定性,这种不确定性包括表现形式的不确定、发生与否的不确定、发生时间的不确定和导致结果的不确定。科技论文数据泄露风险也具有上述不确定性特点。3)泄露和泄密。泄密指泄露机密,因此,泄露风险与泄密风险属于包含与被包含的关系,泄露不一定泄密,而泄密则必先泄露。以往研究单纯针对泄密研究,在研究广度上可能会有所遗漏,因此,本文将视角放至科技论文数据泄露风险,包含了泄密风险。

1.2 科技论文数据泄露风险防范的必要性

1.2.1 科技论文数据泄露案例

案例1:恶意主动泄露行为。2020年,国内某广播电视台经相关部门授权报道了一起境外窃取能源领域国家秘密案。嫌疑人刘某供职于国内一家能源企业,因其具有博士学位的专业优势,同时被遴选为国内几家军事期刊的审稿人。刘某利用其审稿人的身份便利,将涉及国家能源建设方面的内部刊物及军事类杂志刊登的论文数据资料主动提供给境外谍报人员,以获取高额非法报酬。刘某作为期刊相关从业人员,其职业道德严重缺失,竟有意出卖国家战略资源数据以牟私利,给国家造成了经济损失和安全威胁[11]。

案例2:无意识泄露重大科研成果的研发细节。文献[12]披露:由于我国学术刊物不断地、无保留地刊载"青蒿素"和杂交水稻这2项国家重大科研成果的科研细节,先后发表了18篇有关抗疟新药"青蒿素"的文章和50多篇有关籼型杂交水稻的文章,使其中的关键性技术问题全部被暴露,所以外国人无偿获得了全部资料,致使我国在有偿转让这2项技术时失去谈判资本,严重削弱了我国医药技术和水稻杂交技术在国际市场上的竞争优势,其经济损失的重大教训极为深刻。

1.2.2 科技论文数据已成为国外情报机构收集情报的开源信息源

在大国竞争中,科技越来越成为影响国家竞争力和战略安全的关键要素,对维护相关领域安全的作用日益凸显。以美国为代表的竞争对手国家的智库和情报机构长期对我国科技领域进行监测和数据分析。有学者分析了美国典型智库研究科技问题的信息源,其中对中国期刊论文的引用率占13.87%[13]。以下列举美国典型智库和情报部门对我国论文数据的引用情况。

1)美国忧思科学家联盟(The Union of Concerned Scientists,UCS)于2009年发布一份名为"Anti-Satellite (ASAT) Technology in Chinese Open-Source Publications"的报告,该报告分析了1971—2007年中国328个科研机构的957名研究人员发表在292种中国期刊上的1 486篇关于ASAT武器和技术方面的学术文献。该报告认为中国会在学术资源数据库中发表一些相关的技术和非技术报告,给美国对中国ASAT技术的情报分析提供了丰富的信息来源[4]。

2)美国新型高端智库——新美国安全中心专注于国家安全研究,明确提出了"把翻译、分析和传播中国关于科技前沿技术的出版物作为优先事项"[14]。新美国安全中心搜集和引用的中国期刊主要是专业性较强的期刊,如《电子对抗》《火力与指挥控制》《宇航学报》《战术导弹技术》《现代防御技术》《国防科技》等,说明中国学术期刊在无意间为美方提供了大量涉华防务的学术信息。

3)美中经济与安全评估委员会(U. S. - China

Economic and Security Review Commission,USCC)在每年向美国国会提交的年度报告中关于科技竞争的章节引用的公开情报源包括中国重要出版物、科技期刊发布的文章。如引用了《今日纳米》中的“董海燕等,中国与美国之间的纳米技术竞赛,今日纳米,2016(11)”“李丹丹,这名中国教授填补了国内的碳纤维空白,航空制造技术,2018 年 7 月 11 日。翻译”等[15]。

4)2000—2013 年兰德公司关于中国军情分析的 17 篇报告中,我国期刊中被引次数大于等于 1 的引用源共列举了 39 种[16]。

通过以上实例分析和定量统计发现,科技论文确已成为国外情报机构收集情报的开源信息源。随着我国科技论文总体产出持续增长、开放科学的发展以及世界百年未有之大变局的交织叠加,看似正常的科技论文出版已经或可能给国家科技安全带来更多风险挑战,这理应引起包括科技期刊在内的风险相关方的重视,其应重新审视科技论文数据泄露问题。

2　大数据时代科技论文数据泄露风险原因分析

关于科技论文数据泄密原因已有很多文献进行了讨论,主要包括:主动泄密行为;数据保护意识淡薄;科研细节过度披露;论文发表同行评议要求;情报机构的恶意攻击与信息收集;技术防范措施不到位等。对此,本文不再重述,但强调一点,除主动恶意泄露行为之外,科技论文数据泄露均属于间接泄露和无意识泄露,这是科技论文泄露风险发生的多数情况,具有高隐秘性、难识别性特点。造成这一现象的主要原因应归结于大数据特点,间接泄露风险和无意识泄露风险隐藏于海量论文数据及其知识关联中,这也是科技论文数据泄露风险防范的难点。

2.1　大数据时代数据泄露与否的难以确定性

随着人类社会、信息空间、物理世界三元深度融合,数据规模呈爆炸式增长,且数据异构多源、动态演变、真伪混杂、界限模糊,不应简单和孤立地以二分法(泄密和非泄密)去静态评估数据泄密风险隐患。传统意义上认为安全的数据,在大数据时代也仅是相对意义上的安全,保密将不得不关注更多的非密信息[17]。进一步从竞争情报视角来看,科技论文数据泄露具有不确定性特点,即科技论文数据是否存在泄露风险对于竞争对手而言并不具有稳定性,其会随着竞争双方科技实力对比变化而可能产生不同维度或不同程度的泄露风险,也会随着竞争对手认知变化而变化。例如,基础研究本身发生泄密风险事件的概率极小,而基础研究一旦发展得较为成熟并基于此开展应用研究时,其泄密风险可能会大幅提升。此外,某些预研性信息(如概念性、探索性、前瞻性等前期研究成果,或从事尖端和前沿研究的关键科技工作者的思想观点和经验总结等)也会因研究的不断深入而增强泄密的风险[8]。因此,结合具体场景动态评估和预测海量论文数据泄露风险显得尤为重要。

2.2　大数据关联分析增加了数据泄露风险发生概率

大数据从字面意思看仅仅是指拥有大量的数据,而大数据的真正价值是对一组数据进行挖掘分析,能得出新的更有深度的数据。现在更是能借助大语言模型的超高运算效率,收集在互联网上发布的海量信息,通过数据挖掘手段对这些信息进行深入分析,由此给传统的信息保密工作带来了全新挑战[17]。

只关注论文本身研究内容的数据利用是以科学交流和共享为目的,而以竞争为目的的数据利用则不满足于对原始数据的分析,而是会在已获取的数据基础上,再关联论文之外的其他知识推理出作者不愿意公开的信息。特别是如果竞争对手采用更加专业的技术手段,针对重点领域开展主动性长期追踪,对同组文献进行关联分析,那么极易导致“规模致敏”和“汇集致密”[8]。一篇文献不足以造成泄密,但是一组文献经专业情报人员分析就很容易被探查出国家关键数据、领域尖端科技和战略性信息,从而引发安全隐患[8]。在网络信息技术的加持下,除了我国保密法规定的保密信息外,更多公开或者含有密点的碎片“敏感信息”,被专业情报人员拼图聚类成具有高价值、强威胁的保密信息,具体表现为:因基于数据关联还原“关键事实”而泄密、因提供可对“关键事实”证实或证伪的数据而泄密、因提供互补性数据以提高信息的完整度而泄密[18]。

因此,仅做好涉密数据的保护和防范已无法满足大数据环境下的保密需求,如何把握好非密数据的传播,避免非密数据成为失泄密的源头,将是一个崭新而严峻的课题。反观编辑工作实践,绝大部分科技论文作者或编辑更多的体会是对论文数据泄露风险隐患的研判缺少可依据的抓手,以致造成间接泄露或无意识泄露。马克思主义矛盾论认为,内因是决定性因素。应对大数据时代高速度、大范围数据共享和复制带来的科技论文数据泄露风险挑战,不应仅是对风险防范的事后响应,而应将着力点放在事前对风险的研判和规避上,或可在一定程度上阻断科技论文数据泄露风险。

3　科技论文数据泄露风险研判和规避关键点

3.1　科技论文数据泄露风险研判

对科技论文数据泄露风险关键点的研判,可以借助情报研究领域“知己知彼”方略来分析。

一是对外。采用文献计量、引文文本分析、语义分析等研究方法,持续关注竞争对手国家出台的各类战略报告、政策简报、国会证词、咨询文本等,如美国《国家安全战略》、美国国会年度报告等。一方面分析其引用源情况,重点是其中对中国科技文献的引用行为特点,包括发表途径、文献类别、数据来源、研究主题、引用内容以及基于此形成的认知理念等,以此明确竞争对手国家重点关注的我国科技领域研究内容,预估、研判其以此为参考准备采取的反制措施。另一方面结合其正文内容,了解其重点关注的科技主题,识别和预判这些国家的战略发展趋势和科技领域技术需求。通过对文本的解读和分析进而反向推理出具有高泄露风险的研究关键点。关于这方面的研究成果广泛分布于情报研究领域,出版界可共享借鉴。

二是对内。知悉国家战略需求在竞争双方博弈过程中的变化调整,跟踪调研我国重点科技领域的发展和推进情况,掌握科学技术前沿领域与发展动态,熟知科学技术新名称和科技领域敏感主题。遵照执行有关部门颁布的数据安全、保密涉密相关法律法规条例,明确国家需要保护的科技领域数据范围和内容,以此框定科技论文数据泄露风险关键点,在科技论文出版前注意审查、规避此类选题和内容。

3.2 科技论文数据泄露风险规避关键点

运用上述研判方法,结合既有文献中提到的竞争对手国家监测我国科技发展情况的侧重点以及编辑出版实践,科技论文数据泄露风险规避关键点梳理如下:

1)国家战略性信息(政府战略规划、重点行业发展报告、计划类政策文件)。为调整竞争策略,竞争对手国家会持续监测我国科技、经济领域的发展态势,并全面评估我国前沿技术的探索能力及科技政策支持走向等。既有研究[13,15]表明,竞争对手国家长期监测我国的公开情报源包括:党和国家领导人的讲话信息,中共中央、国务院召开的会议及发布的官方文件,国家各部委发布的文件信息,军口主要媒体发布的信息,我国地方政府部门发布的中长期战略发展规划、产业发展规划等,中国本土高科技龙头企业信息,中国投资机构相关信息,中国重要科技战略研究咨询机构发布的研究报告(具有详实数据,以说明行业技术发展态势、产业链供给、关键技术产品、国际合作与援助等),中国重要科研机构和重要单位发布的信息等。美国参议员汤姆·科顿办公室研究人员从相关文件中获得了中国在半导体、生物医药等领域的战略目标信息,并提交了《Beat China: Targeted Decoupling and the Economic Long War》的研究报告,该报告对目标信息展开了详细分析及预测,由此成为美国脱钩策略确定的依据之一[13]。

2)国家重大科研项目信息。国家投入巨额资金资助的重大科研项目是政府重点扶持的科学研究活动,这些项目反映科技战略布局和重大科技基础设施等国家战略科技力量,涉及重大经济利益,事关国防和国家安全,对科技和经济发展将会产生深远影响。国家重大科研项目在科技论文中应规避的数据包括:重大项目清单,项目招投标信息和创新平台清单,主流媒体或者建设方公布的项目研究进展、所获成果以及社会各方对其的解读和反响等。在论文中不能直接标注涉密项目名称,不能引用涉密科研项目中的文件资料和图表参数,更不能将涉密科研项目的成果原封不动地发表。

3)关键技术数据。关键技术领域聚焦时代进程,瞄准科技前沿,对未来产业基础发挥奠基作用。其应规避的关键点主要包括:限制公开的新材料制作配方、具体制作方法和流程;保密技术的技术背景、技术指标、开发程序和实验方法以及实验获得的有关数据;保密技术实验设备的具体型号或具体参数;未经公布的我国特有资源和尚未公开的传统工艺;我国独有的新发明、新工艺、重大科技成果和专利;医疗秘方、疫情发病率和死亡率等类似数据。

4)作者署名数据。中国人才培养相关信息也是竞争对手国家监测信息的侧重点[13],主要从人才相关数据中挖掘我国科技创新的范围、规模和对产业的重视程度。除了科技论文中明确述及的科技人才相关数据要规避外,作者署名中披露的数据也应引起高度重视。作者署名虽然从一定程度上体现知识贡献、身份地位与荣誉归属,但署名规范没有统一强制性著录标准,各刊对作者署名的著录范围、内容和格式大多不同,一般较侧重著录姓名、ORCID、出生年、性别、籍贯、学历、职称、研究方向、单位名称、单位详细地址、邮编、电子邮箱等信息。海量作者署名数据在互联网上公开发布,有可能会被竞争对手国家窃取用来做数据关联分析,极易形成“规模致敏”。其中,创建于2010年,由在美国注册的一个号称全球性的非营利性组织ORCID Inc.负责运营的ORCID拥有注册学者的学术经历、科研成果等敏感数据,据此可轻易判断不同科研领域的投资情况、科研水平和科技人才培养状况,存在安全隐患和风险[19]。此外,作者单位名称如果是部队番号,甚至著录驻地具体地址,也具有引发国外情报部门重点关注的风险隐患,如果此类数据搜集量足够多,那么完全有可能会被关联估测我国军事部署情况[20]。

5)社会热点事件数据。社会关注的热点问题关系经济发展和社会稳定,描述和引用社会热点事件应

以官方正式公布的数据为准,在查证事实的基础上还要注意社会影响。以笔者所在期刊开设的“舆情研究”栏目为例,该栏目研究论文多有涉及社会热点事件的介绍,在此类论文中则应淡化对舆情事件过程、细节的描述和披露,防止国外敌对势力以此作为污名化中国的所谓“证据”。

4　科技论文数据泄露风险阻断路径

通过上述对科技论文数据泄露风险规避关键点的梳理,为有效识别和阻断泄露风险提供了抓手和依据。为避免大数据关联推理,溯源性阻断应是科技论文数据泄露风险最理想的阻断模式。科技期刊,特别是部分战略领域处于泄露高风险区的期刊,是科技论文得以面世的最重要的渠道之一,也是阻断数据泄露风险的最后关口之一,应主动作为,一方面注重发挥学术界和出版界联动效应,另一方面建立审查机制,对内容数据进行有效把握和审查。

4.1　提高对作者告知义务履行的实效

科技期刊可通过网站首页、投稿须知或微信公众号平台等多渠道告知投稿作者论文中应规避的数据泄露风险点。根据编辑实践,作者更多关注的是其投稿进度和审稿结果,对期刊平台互动消息的关注度并不高,为此期刊可创新告知方式和消息形式,如将此互动消息设置为投稿的强制性浏览环节等。考虑到实际告知效果,期刊可将告知内容提炼为问答形式或图表形式(此处仅展示设计的样表,如表 1 所示),有条件的期刊还可采用多媒体(视频、动漫)形式,使作者知晓论文创作的“为”与“不为”。图表或多媒体展现形式因其内容简洁明快、赏心悦目,可激发作者的阅读观看兴趣,能起到较好的提醒作用,有助于将数据泄露风险阻断在源头阶段。

表 1　论文创作的“为”与“不为”清单

为	不为
介绍科学理论探索、科学规律发现以及新材料发明等基础研究情况	限制公开的应用研究技术细节
说明技术成果、技术发明的意义和作用	阐述具体的涉密技术过程,给出关键性数据
对敏感词句进行转换或模糊处理	使用和引用明显涉密信息和内部官方文件
客观表达专业领域研究观点和学术思想	主观评述社会热点敏感事件
采用笼统、泛指的项目名称	公开保密项目具体名称和编号
……	……

4.2　细化科技论文数据泄露风险审查

1)明确审查责任。科技论文出版过程中的保密审查责任主体主要由 2 方构成,即科技论文作者及其所属单位和科技期刊出版者,承担科技论文保密审查责任是双方的法定义务。因此,科技期刊应严审作者所在单位保密部门开具的审核证明的效力,避免流于形式,并妥善留档,便于审查责任落实。

2)做到审稿与审密分离。目前的稿件三审制主要是从技术角度审核论文的科学性和创新性,除此之外,期刊还应从涉密角度对稿件进行审核。在借鉴军事科技期刊“五级保密审查制度”(作者及其所在科研单位,责任编辑,审稿人,主编,期刊保密委员会)[21]的基础上,期刊应结合实际确定专门的定密专家团队或主办单位的相关部门负责论文审密。

3)把握好内容保密审查的灵活性。科技论文的内容各不相同,保密审查的侧重点、方法、程序也不相同。期刊应在实践中对科技论文数据分类分级,确定是否审密、审密内容、由谁审密、怎样审密。一般情况下,除军事类、涉密专业方向科技期刊外,大部分科技期刊涉密内容较少,编辑部可以自主研判是否需要作者提供保密审查证明。内容审查时,一看单位,如果是军事院校或国防科工委下属单位等,则需重点审查这类单位的保密审查证明是否为单位保密委员会出具,而如果涉及军口民口多个单位,则应要求所有署名单位均提交保密审查证明。二看研究方向,一般基础理论研究数据泄露的可能性低,而工程应用类研究数据泄露的可能性高。对于不易确定是否需要保密审查的内容,期刊应秉持怀疑精神,并按照规定请示相关上级部门审定和鉴定。

4)重视对图表数据的审查。图表是科技论文的重要组成部分,但却是内容审查时容易忽视的一项内容。实验数据更多会以图表来展示,反映的是研究核心数据。照片图中拍摄对象是否涉密,是否出现尺寸参照作用对象,设计图中是否标有详细设计尺寸,表格数据是否提供关键核心技术参数等,期刊都应重点关注。境外敌对势力能通过解析原始图片,获得拍摄日期和定位数据等关键数据,从而使某些国防装备部署位置、使用频率等重要数据暴露的风险加大。

5)创建动态泄露风险元数据。编辑应关注时事报道,了解动态新闻,收集工作中需要的行业关键信息,尤其是部分战略领域处于泄露高风险区的行业敏感信息,建立科技期刊所属学科领域的泄露风险元数据,并根据形势调整更新,以此作为科技论文数据泄露风险研判和识别的基础数据。

6)简化作者署名的著录内容。科技论文的学术价值通过其内容体现,作者署名中涉及的关于身份、地位、研究领域等信息与论文学术水平缺乏直接相关性,

作者署名的著录目的应回归于信息交流、促进科技传播。对于重点科技领域的作者,仅著录其姓名和单位即可,目前国内已有科技期刊采用这种著录格式;此外,可借鉴国外作者署名著录方式,即仅著录作者姓名、单位和通信作者联系方式。关于著录ORCID,虽然目前对此褒贬不一,但在当前科技竞争日趋激烈以及西方部分国家对我国进行科技战的大背景下,我们应强化国家科技安全意识,不盲目宣传推广甚至执行西方某些组织制定的所谓"国际规范",更不能不加限制地将相关信息向西方国家经营的ORCID之类的机构输出[19]495。

5 结束语

科技论文数据是国家科学知识储备能力和科技综合实力的重要表征之一,竞争对手国家通过开放平台获取相关数据并经专业分析,就可以很快锁定某国科技战略重点和领域核心人才,为打压其优势行业和领域提供战略情报,进而对其科技安全构成直接威胁。目前,虽然从表面上看,科技论文数据泄露风险大多还处于隐而未发状态,但风险事件一旦发生,即是可能涉及国家科技安全的大事件。本文基于情报视角紧扣科技论文内容本身,遵循数据风险"感知、探理、化解"的问题逻辑,采用定性和定量相结合的方法,分析了科技论文数据泄露风险发生的大数据方面的原因和风险防范难点,从对外对内两方面反向推理出科技论文数据泄露风险规避关键点,并从科技期刊角度探寻科技论文数据泄露风险阻断路径,力求启发和警示出版相关人员,提升其对论文数据泄露风险的识别力和研判力,使其对风险见之于未萌、化之于未发。囿于作者思想认知与知识结构,本研究不可避免存在一定主观性,下一步研究还需融入学科领域差异,提高研究针对性,在理论与实践的双向互动中实现科技论文数据泄露风险的消弭。

6 参考文献

[1] 王珏,任娇菡,杨恒,等. 开放科学环境下我国科技论文发表中的信息安全问题与管控[J]. 中国科技期刊研究,2022,33(12):1599

[2] 张晶晶,赵伶俐,李云霞,等. 农业科技期刊论文发表中的信息安全问题及应对策略[J]. 中国科技期刊研究,2022,33(12):1635

[3] 段尧清,郑卓闻,王蕊. 科学论文发表中的信息安全问题探讨与建议:基于作者、审稿人和编辑视角[J]. 中国科技期刊研究,2022,33(12):1613

[4] 柳厅文,李全刚,时金桥. 大数据时代公开数据的泄密风险[J]. 保密工作,2018(4):52

[5] 马天一. 科学数据出版面临的风险隐患及其治理对策[J]. 情报杂志,2023,42(12):168

[6] 秦晓雪. 科技期刊泄密风险及保密管理对策分析[J]. 出版与印刷,2021(2):67

[7] 唐迪,夏雪莲. 科技论文发表过程中存在的保密问题及对策[J]. 保密科学技术,2015(1):62

[8] 李品. 开放科学环境下科技文献泄密风险防控探析[J]. 情报理论与实践,2023,46(6):10

[9] 代妮. 科技期刊应加强保密工作[J]. 编辑学报,2022,34(3):244

[10] RENN O. Concepts of risk: a classification[C]//Sheldon Krimsky, Dominic Golding. Social Theories of Risk. New York:Praeger Publishers Inc,1992:53

[11] 重案公布! 境外组织策反博士高工,细节曝光[EB/OL]. [2023-12-26]. https://news.sina.cn/gn/2020-10-31/detail-iiznezxr9088144.d.html

[12] 李晓光. 我国科技期刊贯彻执行《保密法》工作亟待加强[J]. 中国科技期刊研究,2004,15(2):145

[13] 张秀妮,张薇,任佳妮. 美国典型智库研究科技问题的信息源分析[J]. 情报理论与实践, 2024, 47(1): 185

[14] 王君,李品. 科技情报泄密视角下国外智库涉华科技报告引文分析[J]. 情报理论与实践,2023,46(10):61

[15] 陈峰. 美中经济与安全评估委员会年度报告的公开情报源分析:以2016—2019年度报告的中美科技竞争部分为例[J]. 情报杂志,2021,40(2):7

[16] 齐欣,杨建林. 美国智库对华军事研究的信息源分析:以兰德公司2000—2013年报告的引文分析为例[J]. 图书与情报,2014(3):118

[17] 蒋云珑. 浅谈大数据时代保密安全隐患[J]. 保密科学技术,2019(6):27

[18] 唐超,钟灿涛. 数据汇集中的安全风险评估研究[J]. 保密科学技术,2019(6):10

[19] 代妮. 强化安全意识,守住科技安全底线:以科技期刊注册ORCID为例[J]. 编辑学报,2021,33(5):492

[20] 冯景,蒋恺,宋犀,等. 学术期刊编辑应注意的论文保密审查问题[G]//刘志强. 学报编辑论丛:2021. 上海:上海大学出版社,2021:290

[21] 朱大明,高永红,任飞. 试论军事科技期刊内容的"五级保密审查制"[J]. 中国编辑,2014(4):49

(2024-01-05收稿;2024-02-17修回)