

智能时代科技期刊知识传播的数据安全风险与应对策略

何好婕, 杜辉, 李俊, 周翌城, 孙莹, 杨红[†]

上海市农业科学院, 201403, 上海

摘要 在智能时代知识传播的进程中,科技期刊在革新传播路径的同时,面临着复杂的数据安全风险。本研究聚焦科技期刊在传播中应用的智能技术,从数据内容安全和数据使用安全角度切入,探讨智能时代知识传播面临的数据伪造、数据投毒、数据泄漏、数据滥用及版权争议等风险,探索了依托技术、平台、法规构建完善的科技期刊智能传播数据安全协同治理体系的可行性。

关键词 科技期刊;知识传播;数据安全;风险防范

Data security risks and response strategies for knowledge dissemination in technology journals in the era of intelligence/HE Yujie, DU Hui, LI Jun, ZHOU Yicheng, SUN Ying, YANG Hong

近年来,在信息与通信技术(information and communications technology, ICT)的深度赋能下,以区块链、人工智能、大数据等为代表的智能技术被广泛应用于人们生活和学习的各个领域。在智能技术浪潮的推动下,人类社会迈入了智能时代,这也为科技期刊的知识传播带来了新的机遇与挑战。依托智能技术,科技期刊能够实现更加高效、精准的知识传播,从而有利于提升传播效果和学术影响力。但是,随之而来的数据安全风险问题也成为社会各界关注的热点。

传统的数据安全范式聚焦数据保密性(confidentiality)、完整性(integrity)与可用性(availability)的CIA三元组^[1]。但在智能时代科技期刊知识传播的过程中,数据则被赋予了信息载体与生产要素的双重属性^[2],其安全内涵已突破传统边界。作为信息载体,需严防科研成果泄露、学术数据篡改等内容安全;作为生产要素,则需应对数据垄断、算法偏见等新型要素安全的挑战。数据承载着个人隐私、学术成果、行业动态等关键信息,一旦出现安全风险,不仅会削弱期刊的学术公信力,还可能干扰正常的社会秩序。

近几年,学术界关于期刊的智能化发展已进行了较多研究。陈鸿等^[3]深入探讨了人工智能在选题策划、编辑加工、排版校对等环节中的应用策略与风险;代妮等^[4]从正反两方面探讨了人工智能对科技期刊出版的影响;周濛^[5]、闫立娟等^[6]从学术发展角度出发,揭示了科技期刊数据的风险边界和安全隐患。综合来

看,现有的研究多聚焦于智能技术在科技期刊编校、传播中的功能应用,而对智能技术在科技期刊知识传播中的数据安全风险问题则缺乏系统性研究。为此,笔者对科技期刊智能传播的形态与特征进行剖析,探讨其背后数据安全风险的类型与成因。在此基础上,从技术、平台、法规等方面出发,提出构建完善的科技期刊数据安全协同治理体系,从而为保障科技期刊高效、广泛、智能、安全地传播提供一定的理论支持。

1 科技期刊智能传播的形态与特征

媒介融合的初级阶段是传统媒体与新媒体的融合,而更高级的媒介融合是重构原有的知识传播模式。智能传播实现了从单一纸媒向全媒体矩阵的发展,形成了多平台、跨终端、多渠道融合的传播格局^[7]。

1.1 智能推送提供个性服务

智能推送是智能时代提升阅读效率、拓展科研视角的重要技术之一。对于用户而言,智能推送能基于用户的阅读数据,对用户的搜索记录、浏览时长、留言评论等行为进行分析,以此了解该用户的阅读倾向。同时,还以年龄、性别、职业、学历、阅读兴趣、学科领域等标签为基础,搜集用户的多源数据,以此构建用户画像,提取用户特征。对于读者而言,智能推送会深入分析读者的个体差异与阅读需求,通过深度算法对海量的学术资源进行智能筛选,以学术关键词、学术热词等为线索发现目标用户,从而提供更有效、精准、全面的服务。如表1所示,近年来各期刊和学术平台逐步推出智能推送服务。中国知网的“全球学术快报”、中国科学院的Pub Scholar公益学术平台、清华的AMiner团队等学术平台多采用平台本身实现个性化推送,而《计算机工程》《核动力工程》《应用生态学报》等期刊多使用邮件的形式进行精准推送^[8-11]。

1.2 智能检索深度数据赋能

相较于传统的检索模式,智能检索不再局限机械化的关键词匹配,而是通过智能算法深入理解用户搜索的语义内涵与潜在需求,以此过滤冗余信息,确保检索结果与研究主题的高度契合,从而提升检索的精确度。此外,智能检索还能依托知识图谱与可视化分析等技术,实现数据之间的深度关联。其原理是通过抽取整合相关数据,以此在海量数据库中关联相应文章,

[†] 通信作者

表1 智能推送应用案例

智能推送方式	期刊或学术平台	智能推送特征
邮件	《中国科学:物理学力学天文学(英文版)》	推送单篇文章、专题或虚拟专题
邮件	《中华内分泌外科杂志》	以学科专业组建读者和作者群进行推送
邮件	《中华医学杂志》	构建读者画像,实现精准推送
邮件	《计算机工程》	将“读者—文章—标准关键词”进行匹配
邮件	《核动力工程》	构建用户画像,并在推送时建立反馈平台
邮件	《应用生态学报》	构建单篇论文推送客体指标体系
微博、微信、邮件	《计算机研究与发展》	构建多渠道精准传播体系
平台	Springer Link	基于用户行为、画像提供服务
邮件、应用	Elsevier	基于用户行为、画像提供服务
平台	UNSILO	基于内容智能分类提供服务
平台	全球学术快报	基于用户行为、画像提供服务
平台	Pub Scholar	基于用户行为、画像提供服务
微信、邮件、平台	AMiner	基于用户行为、画像、关键词提供服务

并构建同类信息知识网络,对用户搜索的相关内容推送,从而实现检索的全面性。超星科技的“域出版”功能,打破了传统的数据库的界限,支持读者进行跨数据库阅读,实现了联合检索和文内搜索^[12]。Semantic Scholar平台对学术论文进行深度解析,并提取文献等关键信息。Yewno工具则借助语义算法将出版物分解为独立的信息单元,建立概念关联,形成可视化知识结构和知识网络。

1.3 智能生成创新内容生产

AIGC(artificial intelligence generated content,人工智能生成内容)技术在科技期刊出版领域的应用正不断拓展,编辑人员通过智能化的内容转化机制有效弥合专业鸿沟,以其高效的内容生产能力和多元的呈现形态,为读者构建起沉浸式的知识获取体验。同时,编辑人员还能通过该技术辅助期刊出版,突破传统纸媒在内容呈现形式上的局限性,推动知识传播向更加生动、形象的方向发展。目前,《智慧农业(中英文)》《农业图书情报学报》《石油钻探技术》《创伤与急诊电子杂志》等期刊通过应用AR、VR和DVH(virtual digital human,虚拟数字人)等AIGC技术,合成了音频、短视频、海报等内容,使前沿科研成果突破学术圈层限制,实现更广泛的社会化传播^[13-14]。

2 科技期刊智能传播的数据安全风险与成因

在智能化的知识传播体系中,数据作为核心要素,是所有技术应用的基础。数据的内容安全和使用安全直接关系到用户信息的安全性与保障性,也影响学术信息的真实性与可靠性。科技期刊数据安全的包含范围较广,从个人隐私到学术创新,在数据收集、存储和使用过程中的每一个环节都面临潜在风险。

2.1 数据内容安全风险

2.1.1 虚假数据伪造风险

随着AIGC技术在期刊出版领域的渗透,学术质量管控迎来了新的挑战,数据伪造风险尤为突出。AIGC的运行依赖海量数据训练,而获取数据这一环节存在着一定的隐患。其原因是网络爬取的数据无法保证其来源的真实性,这就导致未经核实的数据进入数据库。并且,算法的不可解释性可能使生成的内容具有不确定性和虚构性,这就进一步模糊了信息真实性的边界。因此,利用AIGC所生产的虚假数据风险较大。从科研层面来看,虚假数据可能会对科研工作者的研究方向产生一定误导,干扰学术研究的正常秩序,甚至直接破坏学术诚信和科研道德。从社会层面来看,虚假数据会削弱公众对科学技术的信任基础,从而对科技发展产生负面影响。

2.1.2 恶意数据投毒风险

数据投毒是指在数据训练过程中,集中添加污染数据(如错误样本或恶意样本),导致生产的数据模型在决策时发生偏差,从而影响模型的有效性或可用性^[15]。相较于虚假数据伪造风险,数据投毒多发生在模型训练阶段,以污染现有数据为目的,且具有一定的隐蔽性和破坏性。另外,当数据库被插入异常数据,还会导致算法学习出现错误模式,从而污染整体的信息环境。

2.2 数据应用安全风险

2.2.1 用户隐私泄露风险

隐私泄露风险是互联网时代面临的重大挑战之一。在数据收集、存储和使用的过程中,数据背后所承载的用户信息均面临泄露的风险,如表2所示。在数据收集环节,授权机制的模糊极易发生过度收集信息,从而导致侵犯公民的身份信息、健康信息等隐私权。

在数据存储环节,主动泄露或被动攻击都会导致信息泄露,例如,内部管理不善与操作失误,数据访问权限控制不严,工作人员违规导出数据等。值得注意的是,

数据服务器存在的安全漏洞更是会成为不法分子的突破口,一旦防护措施薄弱,就会存在被攻击的风险,导致用户信息被不法窃取。

表2 常见隐私数据泄漏原因

数据泄漏层面	数据收集环节	数据存储环节	数据使用环节
管理层面	过度收集隐私数据	员工滥用权限	违规传输数据
	超出范围收集数据	第三方非法导出	第三方窃取数据
	未告知用户使用范围	未定期清理数据	恶意出售数据
技术层面	采集系统存在漏洞	存储技术加密漏洞	数据去标识化不彻底
	恶意攻击窃取数据	存储设备物理漏洞	推断隐私数据

2.2.2 版权归属争议风险

由于AIGC在创作的过程中缺乏人类的实质性参与,并且其创作基础来源广泛,需要大量使用第三人作品作为训练数据,这就使AIGC生成的作品难以直接适用传统的版权法律进行判定。目前,我国现有的法律尚未对AIGC技术生成的作品版权归属做出明确规定,AIGC技术也不适用于《中华人民共和国著作权法》规定的法定许可范围。在2024年度新时代推动法治进程十大提名案件中,虽然已对AIGC生成的作品归属问题进行了有效探索,但是不同国家和地区对于AIGC版权归属的规定存在差异。部分学者否认人工智能的主体性,其原因是他们认为人工智能本质上是由人类编写的算法和程序驱动的,它缺乏自主意识、情感和道德判断能力;而部分学者则肯定其贡献,他们认为虽然人工智能没有主观意识,但它的“创作”成果是人类智慧与机器算力相结合的产物,为文化、科技等领域带来了新的创作形式和内容。因此,这种认识的差异性加剧了版权认定的复杂性,也导致科技期刊在使用AIGC内容时,极易引发版权侵权风险。

2.2.3 数据无序滥用风险

数据滥用是指在数据收集、存储、使用、共享等环节中,违反法律法规、伦理规范或用户授权,以不当方式处理数据,导致个人权益受损、社会公共利益被破坏。近几年,在学术出版领域,数据滥用现象引起了越来越多的关注。随着通用人工智能的运用推广,其公共属性愈发凸显,不同数据或是主动或是被动地输入模型,人们无法完全预知与了解模型的训练数据及其中间业态,从而导致数据滥用频发^[16]。更为严重的是,部分科研人员甚至违反学术伦理,滥用未公开的个人私密信息,或引入与研究问题无关的数据。这样不仅会误导学术研究方向,还会损害学术质量与可信度。

3 构建科技期刊智能传播数据安全协同治理体系

科技期刊智能化转型的核心在于数据资源的合理

有效利用^[17]。数据安全风险的复杂性决定了单一的治理手段难以实现有效防控,需构建多维度、多层次的协同治理体系,将技术防护、管理规范与法律约束深度融合。

3.1 升级数据安全防线

3.1.1 升级数据使用技术

在运用智能化的传播媒介时,平台应首先优化基础设施设备,升级相关技术,构建覆盖数据采集、存储、处理的传播全周期保障体系。其次,要使用数据加密、隐私保护技术,在数据的存储、传输和处理过程中引入对称或非对称加密,将明文信息转化为代码,并仅向授权者公开解密密钥,有效地抵御未经授权的访问和数据泄露风险^[18]。在数据加密的前提下,还要采用数据融合技术,对数据进行清算和处理,保证数据的全面、准确。最后,对于所采集的用户数据,平台应当依据数据类型进行分级、分模块的存储,并利用云存储、区块链等技术保证数据的不可篡改与安全性,提升数据的可靠性与容灾能力,做好数据的备份与归档。平台可引入用星际文件系统(inter-planetary FileSystem, IPFS),实现网络去中心化。同时,使用去中心化存储项目Filecoin帮助IPFS节点存储、备份和提供内容,解决平台运行过程中面临的数据存储和隐私安全问题^[19]。图1是升级数据使用技术提升数据安全的方法和效果。

3.1.2 更新配套监管措施

防范数据安全风险既要凭借人工智能技术的迭代升级,又要依托实时安全检查与风险预警机制的强化。平台可利用SIEM(安全信息和事件管理系统)和人工智能监管沙盒等配套工具对人工智能技术进行监管,实现数据安全的全流程管理。平台可利用SIEM系统收集、分析工作中的数据,识别并监测潜在的安全风险。也可利用人工智能监管沙盒模拟真实使用场景和风险控制规则,验证风险控制规则的有效性。人工智能监管沙盒作为金融科技监管机制的延伸^[20],能够连接创新者和监管机构,并为他们提供合作受控环境^[21],

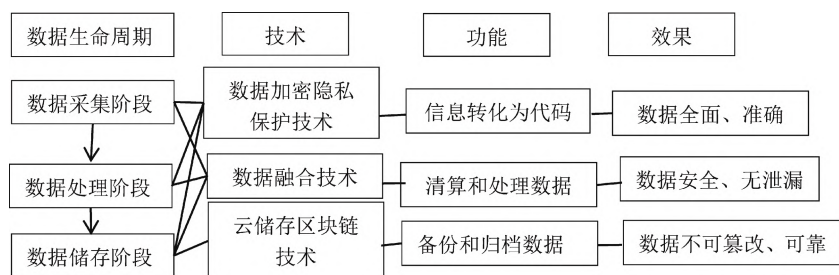


图1 升级数据使用技术提升数据安全

并对人工智能所生成的内容进行安全测试。

3.2 明确平台治理责任

3.2.1 完善平台管理制度

平台应当建立健全的数据安全管理制度,明确数据处理全环节的操作规范。在收集环节,需严格遵守法律法规底线,仅收集与核心服务相关的用户信息。收集过程中,应以书面形式告知用户数据收集的目的、方式和范围,在获得用户授权后方能进行信息采集。在数据使用与共享环节,平台应对员工的数据使用权限进行分级,并建立严格的审批流程,明确数据使用与共享的条件和范围,确保数据使用与共享合法合规。若发现数据访问异常,需及时记录和审查,有效避免数据的恶意泄露。此外,平台应当定期自查,对数据的管理制度进行评估和动态更新,确保制度的有效性和适应性。

3.2.2 加强内容动态审核

动态审核机制是一种实时、持续的审核方式,能够对科技期刊平台上的数据进行全方位、多层次的监测和审查。基于期刊发展的需要,可设置专门的宣传推广部,明确传播内容的制作和审核人员。在内容发布前,对论文和二次生成的宣传产品进行严格审查。在内容发布后,持续关注可能存在的数据安全问题。一旦发现问题,立即采取措施,如撤回内容、发布更正声明、对违规作者进行处罚等。同时,科技期刊可以利用AI辅助审核工具与人工审核相结合的方式,加强对平台内容的动态审核。AI辅助审核工具可通过图像识别、文本查重、逻辑校验等技术,对投稿论文和生成内容进行实时检测,自动识别虚假数据、抄袭内容、侵权行为等问题。

3.2.3 落实人员专题培训

期刊从业者的数据安全素养,直接决定科技期刊数据安全的维护成效。因此,构建完善的数据安全素养培养体系至关重要。科技期刊编辑部可通过定期开展专题培训,采用线上线下相结合的形式,邀请法律、技术等领域的专家授课,帮助编辑人员定期学习数据安全基础知识、数据安全管理等内容。

3.3 规范行业法规标准

3.3.1 细化落实安全法规

当前,我国数据安全法规体系已初步构建。《中华人民共和国国家安全法》《中华人民共和国民法典》《中华人民共和国网络安全法》(下文简称《网络安全法》)《中华人民共和国数据安全法》(下文简称《数据安全法》)等,为数据安全提供了基础性的法律框架。但对期刊出版发行领域,智能传播场景下的数据安全风险呈现复杂性,仍需具体的细则和适应性修订,以有效应对各类风险。

在数据内容安全方面,现有法规对于AIGC技术导致的数据伪造、数据投毒等新型风险缺乏明确的界定和规范。《网络安全法》第十条提出“维护网络数据的完整性、保密性和可用性”的总体要求,并在第三章明确了网络运行者在运行各流程中的权责,禁止非法侵入、干扰、窃取网络数据等行为^[22]。但在数据的使用环节,涉及多元主体,应当明确不同主体的责任,强化全链条监管。《数据安全法》提出了国家建立数据分类分级保护制度、数据安全应急处置机制、数据安全审查等制度^[23],为数据安全的防范提供了有效指导。虽然该法律明确了数据处理者的主体责任,加强了数据内容的安全保障,但对于AIGC生成数据的责任主体认定、伪造数据的法律后果等具体问题,仍未给出清晰的规定。

在数据使用安全方面,《网络安全法》第四十二条第二款仅规定个人信息泄露的通知义务,且缺乏程序细则^[24]。然而,对于信息推送平台在收集、存储和使用用户数据过程中的权利和义务规定不够细化,难以有效约束平台的行为,保护用户的隐私权益。针对数据归属权,近几年出台的《互联网平台分级分类指南》《互联网平台落实主体责任指南》等文件尝试弥补不足,但仍处于征求意见阶段。欧盟将责任主体细分为数据控制者与数据处理者,并对多个数据控制者如何进行责任分配进行了详细规定,这些做法都值得借鉴^[25]。

3.3.2 制定完善行业标准

不同的技术应用、不同的传播环节可能存在不同的数据安全风险,因此,期刊从业者需制定统一的学术

传播行业标准,为科技期刊提供明确的数据安全管理指引,降低数据安全风险。中国科学技术信息研究所牵头联合施普林格·自然(Springer Nature)等3家国际出版集团共同编制的《学术出版中AIGC使用边界指南》,以及我国多个部委联合发布的《生成式人工智能服务管理暂行办法》^[26]等文件,均为编辑人员提供了学习借鉴的依据。

在期刊的出版发行工作中,应建立行业数据类型分类标准,对期刊知识传播中涉及的学术数据、用户数据、内部数据、公开数据和敏感数据进行分类,以此实现数据的分级、分类存储。同时,对于数据的采集范围和授权标准制定合理的规定,明确禁止采集的数据范围和方式。在数据的存储传输过程中,针对存储和传输方法制定相应的标准。对AI生成内容的使用规则、场景进行规范,推动构建安全、开放、创新的学术传播生态。

4 结束语

在智能传播技术兴起的当下,科技期刊面临着新的挑战。本研究聚焦智能时代科技期刊在知识传播过程中的主要数据安全风险,并从技术防护、平台治理、法规建设这3个维度提出应对措施,重新审视科技期刊在新时代的传播路径。

科技期刊应当充分发挥时代优势,运用智能推送、智能搜索、智能生成等技术,促进知识传播。同时,编辑人员也需主动审视随之衍生的数据内容安全风险和数据使用安全风险,通过区块链、云储存等技术,强化安全防护技术水平,构建传播全周期运行保障体系;依托智能监测沙盒、SIEM等工具实施有效监管,规避风险。在平台层面,需建设完善的管理制度,对员工数据使用进行合理分级与实时监控,并加强数据安全培训。此外,需完善并遵守数据安全的法律法规,编辑人员也需针对数据安全类型、数据采集范围、数据采集手段等方面制定行业标准,为数据安全提供制度保障。

5 参考文献

- [1] 刘金瑞. 数据安全范式革新及其立法展开[J]. 环球法律评论, 2021, 43(1): 5
- [2] 时建中. 数据概念的解构与数据法律制度的构建 兼论数据法学的学科内涵与体系[J]. 中外法学, 2023, 35(1): 23
- [3] 陈鸿, 刘育猛, 裴孟. 人工智能与期刊发展融合的机遇、挑战和实践路径研究[J]. 中国科技期刊研究, 2019, 30(3): 217
- [4] 代妮, 步召德. 人工智能对科技期刊出版的影响[J]. 出版广角, 2021, (11): 46
- [5] 周濛. 大数据时代学术期刊出版的数据风险及防范策略[J]. 中国科技期刊研究, 2023, 34(8): 982
- [6] 闫立娟, 张改侠, 孙晓红, 等. 人工智能在期刊出版中的应用及带来的挑战[J]. 编辑学报, 2024, 36(增刊2): 91
- [7] 刘庆振. 媒介融合新业态: 智能媒体时代的媒介产业重构[J]. 编辑之友, 2017(2): 70
- [8] 潘雪, 王维朗, 果磊. 人工智能时代科技期刊增强新质传播力之应对策略[J]. 编辑学报, 2024, 36(4): 360
- [9] 李保朋, 刘斌. 基于精准传播方式的科技期刊传播体系构建[J]. 传播与版权, 2024(2): 69
- [10] 潘雪, 张海生, 果磊. 科技期刊智能出版的发展前景、现实困境与推进策略[J]. 编辑学报, 2022, 34(4): 378
- [11] 邱彦, 周茂, 黄可东, 等. 科技期刊智能传播体系架构与应用探索[J]. 编辑学报, 2024, 36(4): 425
- [12] 唐冰寒, 肖茹予. 基于智能算法的学术期刊传播平台构建[J]. 当代传播, 2018(4): 109
- [13] 陈研, 何炳蔚, 刘宇清, 等. 献礼人民卫生出版社建社65周年: 虚拟现实和增强现实技术在医学科技期刊创新及医学同质化教学中的应用实践: 《创伤与急诊电子杂志》应用虚拟现实和增强现实技术办刊初探[J]. 创伤与急诊电子杂志, 2018, 6(1): 1
- [14] 薛春璐, 王元杰, 刘继芳, 等. 基于智能新技术的科技期刊智慧出版与传播模式优化[J]. 编辑学报, 2023, 35(增刊1): 117
- [15] 林伟. 人工智能数据安全风险及应对[J]. 情报杂志, 2022, 41(10): 105
- [16] 马治国, 张楠. 通用人工智能的数据风险及法治应对路径[J]. 北京工业大学学报(社会科学版), 2024, 24(5): 131
- [17] 秦小燕, 王珏, 任娇菡, 等. 人工智能对科技期刊传播的影响机制与对策建议[J]. 中国科技期刊研究, 2025, 36(4): 428
- [18] 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
- [19] 李媛. 人工智能时代的学术期刊数字化传播[J]. 中国科技期刊研究, 2019, 30(11): 1183
- [20] 张欣. 生成式人工智能的数据风险与治理路径[J]. 法律科学(西北政法大学学报), 2023, 41(5): 42
- [21] 雷挺, 吴义熔. 他山之石: 欧盟人工智能监管的经验与启示[J]. 科技管理研究, 2023, 43(24): 43
- [22] 中华人民共和国网络安全法[J]. 中华人民共和国最高人民检察院公报, 2017(2): 1
- [23] 中华人民共和国数据安全法[J]. 中华人民共和国全国人民代表大会常务委员会公报, 2021(5): 951
- [24] 许可. 数据安全法: 定位、立场与制度构造[J]. 经贸法律评论, 2019(3): 52
- [25] 张晓君. 数据主权规则建设的模式与借鉴: 兼论中国数据主权的规则构建[J]. 现代法学, 2020, 42(6): 136
- [26] 生成式人工智能服务管理暂行办法[J]. 中华人民共和国国务院公报, 2023(24): 39

(2025-06-14收稿; 2025-10-20修回)