

生成式人工智能赋能大型仪器设备 开放共享工作的思考

曹莹方 艾 菲

当前,生成式 AI 技术发展迅速,从美国的 ChatGPT 到我国自主研发的 DeepSeek,模型的精细化程度不断提升,版本迭代周期不断缩短,文本生成和推理能力显著提高,在高校教学科研及管理服务领域的应用已从工具性辅助层面迈向系统性变革新阶段。生成式 AI 的应用推广给高校仪器设备开放共享工作也带来了机遇与挑战:一方面,生成式 AI 为仪器设备开放共享管理服务模式创新注入了新的活力;另一方面,其潜在的数据风险与技术偏差可能影响设备的高效安全使用。在充分利用生成式 AI 的技术优势服务仪器设备开放共享工作创新发展的同时,必须坚持底线思维,构建完善的风险防控与治理体系。

一、生成式 AI 激发仪器设备开放共享活力

生成式 AI 打破了传统仪器设备开放共享的诸多局限,在资源精细化管理、用户个性化服务、实验技术开放创

新等方面为仪器设备开放共享工作的内涵式发展提供了新的选择,重塑着仪器设备共享的工作格局。

1. 重构设备资源管理模式

生成式 AI 依托学校仪器设备购置、运行、管理、服务和绩效评价全周期产生的大数据知识库进行模型训练和内容生成,可在仪器设备资源配置,共享时段优化调度、收费标准动态调整等方面快速产出贴合设备实际管理需求的方案建议,能够提升设备资源管理的效率、精度和智能化水平。例如,实验室管理处依托腾讯元宝大语言模型建设的“仪器设备共享助手”,可以与用户通过自然语言交互,生成与仪器设备功能关联的使用指南,推荐用户感兴趣的仪器设备,提升设备使用的规范性和便利性。

2. 优化精准服务实现路径

生成式 AI 可以通过分析设备共享数据、用户交互数据等为设备和用户“画像”,精准识别使用需求、精准供给服务内容、精准评估共享效果,优化仪

器设备开放共享的服务路径。能够支持建立设备使用诊断引擎,通过数据分析识别设备的潜在故障,实时推送维护建议,甚至可以识别潜在的安全隐患并实时推送干预措施。通过对用户使用仪器设备的行为分析,动态监测用户操作习惯,对违规操作、过度使用等进行预警,根据用户的实际情况提供个性化的使用指导。构建自适应的服务路径,根据用户学科、行业、实验需求差异,为校内外不同用户群体设计个性化的设备使用培训方案,也可以帮助不同用户

制订或推送个性化的设备预约计划。实验室管理处通过生成式AI辅助自主开发的仪器设备共享数据监控与知识挖掘系统对上述路径进行了深度探索(见图1)。

3. 拓展共享服务时空边界

生成式AI与虚拟现实(VR)、增强现实(AR)技术的融合,可突破传统设备共享的时空局限,拓展服务场景的边界。构建“虚拟仪器设备”交互系统,可实现与用户的智能交互,让用户在虚拟环境中进行操作演练,加深对设备原理



图1 仪器设备共享数据知识挖掘系统

和操作的理 解。打造“虚拟实验室”等数字场景,激活用户在虚拟现实中的操作体验,强化实践能力。进行设备使用模拟实验,构建虚拟的实验环境和设备故障场景,设定实验条件、故障类型、初始状态等,让用户在模拟挑战中提升设备操作和故障处理能力。

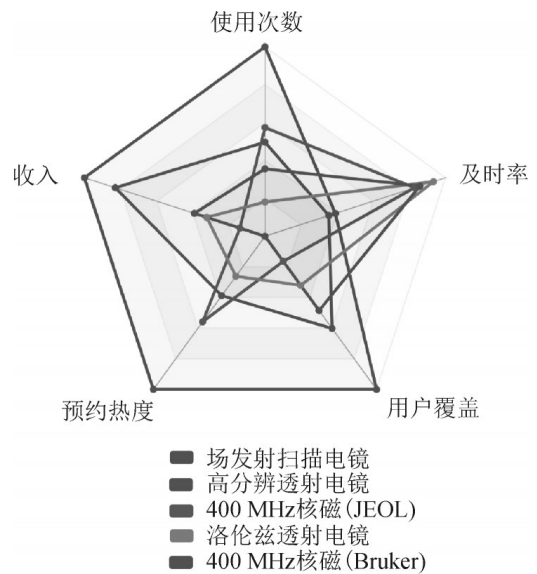


图2 效率雷达对比

二、生成式 AI 对高校仪器设备开放共享工作的挑战

(一)形成数据安全治理隐患

生成式 AI 在设备数据采集和处理过程中,可能会突破边界采集到教学科研、管理服务或用户个人的敏感数据,形成数据安全隐患。一方面,学校仪器设备开放共享涉及大量的设备运行数据、教学科研数据、人事财务数据和用户操作记录等敏感信息,若数据采集、存储或使用不当,或集中存储在云端的设备数据遭遇黑客攻击,极有可能引发数据泄露风险。另一方面,用户在共享仪器设备过程中普遍对数据风险认知不足,缺乏对设备使用数据的保护意

识,为获得更精准的人工智能服务,他们可能在交互中透露实验内容、操作习惯、科研数据等敏感信息,进行数据过度披露,埋下安全隐患。

(二)存在资源分配失衡风险

生成式 AI 本身是一种不具备价值判断力的算法模型,各类设备使用需求和数据都有可能成为数据库海量参数和训练数据的一部分,学校仪器设备开放共享工作也要警惕生成式 AI 融入后可能引发的资源调度分配失衡的风险。生成式 AI 基于历史使用数据优化设备预约与调度时,若训练数据存在偏差(如某学科设备使用记录占比过高),可能导致算法倾向于优先分配资源给特定学科或团队,加剧跨学科资源分配的不均。

(三)加剧人机关系异化趋势

人机关系异化就是在人与机器的互动中,技术逐渐脱离人的控制、反客为主,导致人类在认知、情感、社会关系等方面出现疏离或扭曲的现象。生成式 AI 融入高校仪器设备开放共享重构了传统的人机关系,正在改变设备管理人员和用户的认知习惯与互动模式,可能会削弱师生的主体地位。师生如果过度依赖人工智能生成的设备操作指南和故障处理方案,放弃对复杂问题的辩证思考,便会逐渐丧失独立操作能力,影响自身科研创新能力的提升。人机关系异化还表现为师生与设备管理人员的情感联结弱化,虚拟助手、数字客服等技术的普及,可能会削弱传统服务中的面对面交流、手把手指导等情感传递;用户也许可以拥有 24 小时在线的“人工智能设备管家”,但少了真实可感的沟通和反馈,程式化的回应也会让用户产生服务疏离感。

三、风险防控与治理体系的构建

为实现趋利避害,在有效防范风险的同时充分释放技术潜能推动工作创新,以底线思维建立风险防控与治理体系。

1. 建立“红蓝对抗”审核机制

“红蓝对抗”机制是通过模拟真实攻击与防御场景,评估和提升组织安全能力的一种系统性方法。在防范设备资源分配偏差和数据安全风险过程中,高校可将生成式 AI 的风险抵御能力从被动响应升级为主动防御,在技术应用中筑牢设备共享安全底线。要做好设备使用内容安全审核,使用我国高校设备管理的先进理念训练判别模型,对人工智能生成的资源分配方案进行安全性审查,并由人工协同纠偏,对高风险设备使用申请设置人工复审机制,建立“人工智能初筛+专家终审”的混合审核流程。还要实现算法透明化,要求模型展示资源分配的推理逻辑,检验其决策是否符合高校设备共享的实际需求;着眼于本土化模型的开发与应用设计“设备共享逻辑层”,将仪器设备开放共享的相关理念、目标等,通过一定的逻辑架构和算法设计融入人工智能系统中,促进人工智能在与人的交互中主动进行资源合理分配。

2. 完善数据治理制度

构建“技术可控、风险可溯、责任可究”的数据治理体系是风险防控的关键环节。一方面,强化设备数据分级管

理,建立智能数据中台,根据数据敏感度与使用场景,针对公开数据、内部数据、敏感数据等分级制定管理标准,并结合设备使用动态调整分级标签;从采集、存储各个环节进行设备数据的全生命周期管控,必要情况下要设定自动删除规则。另一方面,组建专门的数据治理与风险防控专家工作组,成员应包括法学领域的专家、数据安全保障的工程师、设备管理一线的教师、来自不同学科和年级的学生代表,共同对设备共享智能推荐系统的算法逻辑进行审查,明确设备数据使用的边界与责任。

3. 提升用户数字素养

风险防范最终依靠人的素养,依靠教育主体,要双管齐下促进师生数字素养的提升。促进设备管理人员从人工智能工具应用能力到管理能力的提升,推动管理模式创新,避免陷入技术依赖;强化管理人员的技术伦理意识,明确工具使用边界。培养师生批判性思维,开设相关通识课揭示人工智能生成内容的随机性与偏见来源,帮助师生技术祛魅;在设备使用培训中引入“人机辩论”模式,引导师生在对抗性思辨中强化自主思考和操作的意识。

作者

曹莹方 西安交通大学实验室管理处
科级干部

艾 菲 西安交通大学实验室管理处
职员