文章类型：论文 | 刊号（ISSN）：2630-4686 /（中图刊号）：380GL020

人工智能时代下高校师生安全素养提升路径研究

杨千千 沈乒松 姚伶
温州医科大学
DOI:10.32629/er.v9i3.6899

[摘　要] 在人工智能迅猛发展的时代背景下，高校师生的安全素养面临着新的挑战与机遇。当前高校师生在安全认知、安全技能、安全意识与行为等方面存在不同程度的不足。人工智能技术既为提升高校师生安全素养提供了创新手段与丰富资源，也带来了一定的消极影响，如信息过载、虚假信息干扰等。本文旨在探索人工智能时代高校师生安全素养提升的有效路径，以期为高校师生安全素养的提升提供理论支撑与实践指导，进而推动高校安全教育工作的创新发展，保障校园的安全稳定与师生的身心健康。
[关键词] 人工智能时代；高校师生；安全素养；提升路径
中图分类号：G645.5 文献标识码：A

Research on the Path to Improving the Safety Literacy of College Teachers and Students in the Era of Artificial Intelligence

Qianqian Yang, Pingsong Shen, Ling Yao
Wenzhou Medical University

Abstract: Against the backdrop of rapid advancements in artificial intelligence, the safety literacy of university faculty and students faces new challenges and opportunities. Currently, there are varying degrees of deficiencies in their safety cognition, skills, awareness, and behaviors. While AI technology provides innovative approaches and abundant resources to enhance safety literacy, it also introduces certain negative effects, such as information overload and misinformation interference. This paper aims to explore effective pathways for improving the safety literacy of university faculty and students in the AI era, offering theoretical support and practical guidance to foster the innovative development of campus safety education. Ultimately, this will contribute to safeguarding campus security, stability, and the physical and mental well-being of faculty and students.
Keywords: The era of artificial intelligence; university faculty and students; safety literacy; enhancement pathways

引言

在科技飞速发展的当下，人工智能已渗透到社会生活的各个领域，深刻改变着人们的生产生活方式。高校作为人才培养的重要基地，师生群体在享受人工智能带来便利的同时，其安全素养也面临着前所未有的挑战与考验。安全素养作为保障师生身心健康、维护校园安全稳定的关键因素，在人工智能时代被赋予了新的内涵与要求。因此，深入探讨人工智能时代下高校师生安全素养提升路径，不仅具有重要的理论价值，更具有迫切的现实意义。

1 当前高校师生安全素养的现状

1.1 安全认知层面

当前高校师生对传统安全领域如人身安全、财产安全、消防安全等具有较高的认知度和警惕性，这得益于长期以来高校常规安全教育的持续开展。然而，在人工智能时代背景下，师生对于新兴安全风险的认知呈现出明显的不足。一方面，对于数据安全的认知较为模糊，多数师生虽能意识到个人信息的重要性，但对数据泄露的具体途径（如 AI 驱动的钓鱼攻击、恶意爬虫技术窃取个人数据）、潜在危害（如身份盗用、精准诈骗）以及防护措施（如数据加密、隐私设置调整）缺乏清晰和系统的理解。另一方面，算法安全与伦理安全的认知更为薄弱，师生普遍对算法偏见可能导致的不公平待遇（如招聘、学术评价中的歧视）、算法滥用带来的信息茧房效应以及 AI 技术应用中的伦理边界（如深度伪造技术的恶意使用）等问题缺乏足够的关注和深入的思考，尚未形成完整的风险防范意识[1]。

1.2 安全技能层面

在传统安全技能方面，高校师生通过应急演练、安全培训等方式，基本掌握了灭火器使用、火灾逃生、基本急救等技能。但在人工智能相关的安全技能方面，师生的能力储备严重不足。其一，智能设备安全操作技能欠缺，许多师生在

使用智能教学系统、AI 助手、联网智能设备时，未能充分了解其安全设置选项，如弱密码问题普遍存在，对设备固件更新、应用权限管理等维护设备安全的基本操作重视不够。其二，信息甄别与批判性思维能力有待提升，面对 AI 生成的海量信息（如深度伪造的音视频、AI 撰写的新闻评论），师生往往难以快速准确地辨别其真伪，缺乏对信息来源的审慎验证和对内容逻辑性、客观性的深度剖析能力，容易受到误导。其三，数据保护与隐私维护技能不足，多数师生不熟悉常用的加密工具、隐私保护软件的使用方法，对于如何在网络活动中保护个人敏感数据（如在社交媒体分享信息时的隐私设置，在公共 Wi-Fi 环境下的数据传输安全）缺乏实际操作经验。

1.3 安全意识与行为层面

尽管高校不断强调安全的重要性，但部分师生仍存在安全意识淡薄、侥幸心理的情况。在日常行为中，表现为对安全规范的执行不够严格，例如，为了方便记忆而使用过于简单的密码，随意点击不明链接或下载来源不明的文件，在公共场合随意连接不安全的 Wi-Fi 并进行敏感操作等。在人工智能应用场景下，这种不良行为习惯带来的风险被进一步放大。例如，随意授权 AI 应用获取过多的个人权限，将个人生物特征信息轻易提供给非正规的 AI 服务提供商，或是在缺乏警惕的情况下参与可能涉及数据伦理问题的 AI 项目中。此外，部分师生在遭遇 AI 相关安全事件（如个人信息疑似泄露、遭遇 AI 诈骗）后，由于缺乏清晰的应对流程认知和主动报告意识，可能导致事件未能得到及时有效的处理，造成损失扩大或风险蔓延[2]。

2 人工智能技术对高校师生安全素养的影响

2.1 积极影响

人工智能技术为高校师生安全素养的提升带来了前所未有的机遇，主要体现在以下几个方面：

首先，AI 赋能安全教育模式创新。人工智能技术能够根据不同师生的专业背景、认知水平和学习需求，提供个性化、精准化的安全教育内容和学习路径。例如，通过智能学习分析系统，追踪师生的学习行为和知识掌握情况，自动推送与其薄弱环节相关的 AI 安全案例、知识点和练习题，实现“因材施教”。虚拟现实（VR/AR）结合 AI 技术，可以构建高度仿真的 AI 安全风险场景（如模拟遭遇 AI 钓鱼攻击、深度伪造信息识别训练），让师生在沉浸式体验中学习应对方法，显著提升安全教育的互动性和实效性。其次，AI 提升安全管理与预警能力。智能安防系统（如基于 AI 的视频监控、行为识别系统）能够实时监测校园环境，及时发现异常行为和安全隐患，并向管理人员发出预警，为师生创造更安全的物理和网络环境。AI 驱动的网络安全态势感知平台可以实时分析校园网络流量，识别潜在的网络攻击（如针对校园服务器的 AI 自动化渗透攻击），提前预警并辅助进行防御部署，保护师生的网络活动安全。这些技术的应用，在客观上为师生营造了一个更具安全感的环境，也间接促使师生更加关注和重视安全问题。

2.2 消极影响

人工智能技术在带来便利的同时，也对高校师生安全素养提出了严峻挑战，主要体现在以下几个方面：其一，安全风险的隐蔽性与复杂性增强。AI 技术的应用使得安全威胁更加隐蔽和难以察觉。例如，AI 驱动的钓鱼攻击能够通过分析目标的社交媒体信息、邮件历史等数据，生成高度个性化、极具迷惑性的钓鱼内容，传统的基于关键词匹配的检测方法难以奏效。深度伪造技术可以制作出几乎以假乱真的音视频，用于身份冒充、名誉诋毁等恶意行为，增加了信息甄别的难度。此外，AI 算法本身可能存在漏洞或被恶意利用，如投毒攻击、后门攻击等，其攻击手段复杂，对防御技术和人员的专业素养要求极高，使得师生面临的安全环境更为复杂。其二，信息过载与辨别难度加大。人工智能技术极大地提升了信息生产和传播的效率，师生每天都要接触到由 AI 生成或推荐的海量信息。这些信息良莠不齐，其中夹杂着虚假信息、误导性内容等恶意信息。AI 推荐算法在提供个性化信息服务的同时，也容易形成“信息茧房”，使得师生视野受限，更难接触到多元化的观点，从而削弱其独立思考和辨别信息真伪的能力，增加了受到不良信息影响的风险。

3 人工智能时代高校师生安全素养提升体系构建

3.1 完善高校安全教育内容体系

高校应构建动态更新的、涵盖人工智能时代特征的安全教育内容体系。首先，要将 AI 安全知识全面融入现有课程体系，开设专门的人工智能安全与伦理课程或在相关课程（如计算机基础、信息安全、思想政治教育、专业导论）中增设 AI 安全模块。内容应包括：AI 技术基本原理及发展趋势、常见的 AI 安全风险类型（如数据泄露、算法歧视、深度伪造、智能设备攻击等）、AI 伦理规范与法律法规（如《网络安全法》《个人信息保护法》以及国际通用的 AI 伦理准则）、AI 信息的甄别方法与批判性思维培养、数据隐私保护策略与技能、智能系统安全操作规范等[3]。其次，针对不同群体（如新生、毕业生、科研人员、行政管理人员）的特点和需求，设计差异化的教育内容。例如，对科研人员重点加强 AI 项目数据安全管理、科研伦理审查等内容的教育；对新生则侧重基础的 AI 安全认知和个人信息保护意识培养。再次，要注重案例教学，收集和整理国内外发生的 AI 安全典型案例（如高校数据泄露事件、AI 诈骗案例、算法歧视事件等），通过案例分析加深师生对风险的理解和提升应对能力。

3.2 创新安全教育教学方法与手段

利用人工智能技术本身赋能安全教育，创新教学方法与手段，提升教育效果。一是推广沉浸式与互动式教学，运用 VR/AR 技术构建模拟 AI 安全场景（如模拟遭遇深度伪造视

频诈骗、智能实验室安全事故处置等），让师生在虚拟环境中进行体验式学习和应急处置演练，增强教学的直观性和参与感。二是开发智能化学习平台与工具，利用 AI 技术开发个性化学习系统，根据师生的学习进度、知识掌握情况和兴趣点，自动推送学习资源、习题和案例，实现“千人千面”的精准教学。同时，开发 AI 安全知识问答机器人、虚拟安全导师等，为师生提供即时的学习辅导和咨询服务。三是引入游戏化学习元素，设计 AI 安全主题的知识竞赛、攻防演练、解谜游戏等，将枯燥的安全知识转化为有趣的游戏任务，激发师生的学习积极性和主动性，在轻松的氛围中提升安全技能。四是开展跨学科融合教学，邀请计算机科学、法学、伦理学、教育学等不同领域的专家共同参与安全教育课程设计与教学，从多角度解读 AI 安全问题，培养师生的综合素养[4]。

3.3 构建多层次安全技能培训与实践平台

为师生提供常态化、多样化的安全技能培训和实践机会，提升其实际操作能力。首先，建立 AI 安全实验室或创客空间，配备必要的硬件设备和软件工具，为师生提供开展 AI 安全技术研究、漏洞挖掘、攻防演练、数据安全防护实验等实践活动的场所。其次，定期组织 AI 安全技能培训班和工作坊，邀请网络安全专家、AI 技术开发者、法律实务工作者等进行授课和现场指导，内容涵盖智能设备安全配置、数据加密技术应用、恶意代码分析、AI 生成内容识别工具使用等实用技能。再次，积极组织和参与各类 AI 安全竞赛与演练活动，如高校 AI 安全攻防大赛、数据隐私保护创新大赛、AI 伦理辩论赛等，通过以赛促学、以赛促练的方式，检验和提升师生的安全技能水平和团队协作能力。

3.4 强化校园安全文化建设与氛围营造

营造全员参与、人人重视的校园安全文化氛围，是提升师生安全素养的重要保障。一是加强安全宣传与引导，利用校园网、公众号、宣传栏、电子屏、校报等多种渠道，常态化宣传 AI 安全知识、最新的安全动态、典型案例警示以及学校的安全管理制度，提高安全信息的覆盖面和知晓率。二是树立安全榜样，表彰在 AI 安全实践中表现突出的师生个人和集体，宣传其先进事迹和经验做法，发挥示范引领作用，激发师生提升安全素养的内生动力。三是开展形式多样的安全主题活动，如“AI 安全文化节”“数据隐私保护周”等，组织安全讲座、主题班会、知识展览、情景剧表演等，寓教于乐，使安全理念深入人心，内化为师生的自觉行为。

3.5 健全安全素养评价与激励机制

建立科学合理的安全素养评价体系和有效的激励机制，引导和推动师生主动提升安全素养。一是制定高校师生 AI 安全素养评价指标体系，从安全认知、安全技能、安全意识、安全行为、安全知识等多个维度进行全面评估，明确不同层级（如基础级、进阶级、专业级）的素养要求。二是将安全素养评价结果纳入相关考核体系，例如，作为学生综合素质评价、评奖评优、毕业资格审查的参考依据之一；作为教师年度考核、职称评聘、评优评先的考量因素之一，增强师生对安全素养提升的重视程度。三是建立多元化的激励机制，对在安全素养评价中表现优秀的师生、积极参与安全培训和实践活动并取得良好成绩的师生、在安全事件处置中发挥重要作用或提出创新性安全建议的师生，给予精神奖励（如荣誉称号、通报表扬）和物质奖励（如奖学金、学习用品、培训机会等），激发师生提升安全素养的积极性和主动性[5]。

4 结语

综上所述，人工智能技术为高校师生安全素养的提升带来了新的契机与挑战。通过积极应对人工智能带来的影响，构建完善的高校师生安全素养提升体系，包括丰富安全教育内容、创新教学方法、搭建实践平台、营造安全文化氛围以及健全评价激励机制等措施，能够切实有效地提高高校师生的安全素养水平，保障校园的安全稳定，为高校的教育教学活动的顺利开展以及师生的健康成长创造良好的环境。

[参考文献]

[1]毕红棋,王小辉.人工智能时代高校网络安全体系构建研究[J].教师博览,2024(33):15-17.

[2]张瑞,宋兆函.总体国家安全观视域下地方高校平安校园建设研究[J].湖北职业技术学院学报,2024,27(03):17-21.

[3]朱燕.直播课背景下高校师生网络安全素养的提升研究[J].山西青年,2024(11):13-15.

[4]宋金玻.新时代高校文化安全的现状及对策研究[D].沈阳建筑大学,2024.

[5]魏顺平,侯文婷,程罡.大学生科学数据素养现状调查与提升策略研究[J].河北开放大学学报,2024,29(01):71-76.

作者简介：

杨千千（1988-），女，汉族，浙江温州人，硕士研究生，研究方向：安全教育。

基金项目：

2025 年度浙江省高等教育学会高校保卫工作分会重点研究课题：人工智能时代下高校师生安全素养提升路径研究（2025GBZDKT003）。