人工智能时代教育数据隐私保护：技术框架与伦理规范构建

严亮，陈冉阳*，黄诗佳
湖北文理学院理工学院，湖北 襄阳 441025
DOI:10.61369/EIR.2026040004

摘　　要： 在人工智能广泛应用到教育教学领域的背景下，教育数据量激增以及智能应用既给我们带来了前所未有的因材施教和精准施教的机遇，也给教育数据安全带来巨大挑战。本文聚焦人工智能时代下教育数据安全的重要命题。并且分别在技术和伦理层面深入探讨。文中对教育数据类型、属性及风险进行剖析后提出一套包括脱敏、联邦学习、链上存储、权限控制以及差分隐私计算在内的全方位保障教育教学数据采集—保存—使用—共享过程的技术架构方案。

关 键 词： 人工智能；教育数据；隐私保护；技术框架；伦理规范

Education Data Privacy Protection in the Age of Artificial Intelligence: Construction of Technical Framework and Ethical Guidelines

Yan Liang, Chen Ranyang*, Huang Shijia
School of Science and Technology, Hubei University of Arts and Science, Xiangyang, Hubei 441025

Abstract: Against the backdrop of the widespread application of artificial intelligence in the field of education and teaching, the surge in educational data volume and intelligent applications has not only brought unprecedented opportunities for personalized and precise teaching but also posed significant challenges to the security of educational data. This paper focuses on the crucial proposition of educational data security in the era of artificial intelligence, exploring it in depth from both technical and ethical perspectives. After analyzing the types, attributes, and risks of educational data, the paper proposes a comprehensive technical framework solution that includes desensitization, federated learning, on-chain storage, access control, and differential privacy computing to safeguard the entire process of educational data collection, storage, utilization, and sharing.

Keywords: artificial intelligence; educational data; privacy protection; technical framework; ethical guidelines

引言

目前，人工智能深度应用于教育领域的方方面面，如智能教室、在线学习系统、智能测评等，新的教育教学模式层出不穷，带来海量教育数据的增长。同时，我们也要思考如何保证在利用人工智能提升教育效能的同时保障教育数据的安全性与隐私性。这是推进教育数字化转型进程中必须重视的问题。为此，本文从这一角度出发，对人工智能时代下教育数据隐私保护的技术路径与伦理规范展开研究，希望为形成稳定有效的教育数据管理机制贡献一份力量。

一、人工智能时代教育数据隐私保护技术框架

（一）匿名化技术

匿名化是人工智能时代的技术基础，即对个人信息进行加工而避免其被直接或间接识别出个体信息的一种方式，用以保护学生的信息隐私安全。常见的方法包括删除、模糊及干扰等，如去除数据中的个人信息，例如姓名、身份证号或学校编码等。

然而，虽然这种方式简单直接，但是会导致数据信息的丢失，影响数据利用；第二种技术称为“泛化”，即以更加宽泛的类别来取代具体的个人信息，例如将学生的具体年龄替换为一个具体的年龄段，或者用所在城市来替代家庭住址等等。该方法既能够保障数据隐私又可以实现数据可用性，在过度泛化过程中也

作者简介：
严亮（1995.10—），男，汉族，湖北孝感人，研究生学历，助教，主要从事计算机方面教学工作，研究方向：目标检测，人工智能。
黄诗佳（1999.07—），女，汉族，湖北襄阳人，研究生学历，主要从事数据结构、文献检索、程序设计基础、Python程序设计、计算机基础等教学工作，研究方向：计算机视觉，目标检测。
通讯作者：陈冉阳（1996.01—），男，汉族，湖北襄阳人，硕士学历，助教，主要从事数据库原理及应用，面向对象程序设计，网页设计基础，移动应用开发，大数据处理与分析等课程的教学工作。

可能会降低数据精确度。扰动法是指通过对数据中加入随机噪声或微调等方式掩盖数据的真实值同时又能够确保统计数据特性不变的方法。例如在学生考试成绩上增加一定的微小不确定性既不影响我们对于全部学生学习情况研究，还可以防止用这些分数来准确地定位某一个学生。

（二）联邦学习

联邦学习是一种新型分布式智能技术，在不暴露原始隐私的前提下实现多方安全协同建模，其核心是将原本集中式的机器学习训练过程拆分成多个参与方协同完成的过程。该场景下，每个大学或学院都可以作为单独角色加入到这种协作式学习社区中并保留自己的教学材料。分布式协同进化算法中每个个体对自身的数据执行特征提取并更新自身模型参数，并将参数传输至主节点集中处理，主节点负责接收各个体传来的参数，将其整合后下发给各个体。他们可以利用这个新参数来进一步在自己的设备上进行训练。

例如，联邦学习能够使得各个学校共同训练出准确的学生学业评价模型而不需要共享学生的学业成绩或者个人信息。此外，根据参与者的地理位置，联邦学习还可以细分为横向联邦学习、纵向联邦学习以及联邦转移三种方法，指导中心可以根据自身数据特征和合作需求选择合适的联邦学习方法。

（三）区块链存储

区块链分布式存储和不可篡改性以及全流程可追溯等特点能够有效保障信息的真实性和个体隐私，在智慧校园中信息安全越来越成为影响个人信息隐私的重要方面，传统中心化存储存在单点失效导致信息丢失的问题。基于区块链存储教育数据，在整个网络中分散存储，每个节点都有一个完整副本，可以防止因单一节点故障造成的资料丢失。每条在链上的数据都有一个时间戳，是不可篡改的真实数据流记录，不论是谁想要对这条数据进行修改都会被全网识别出来，并追溯源头来保证数据的真实性及可追溯性。将学生的学习成绩、毕业证书、知识经历等作为教育领域应用中存储于区块链里的数据。

例如，学生的学位证书可以存储到区块链上，并以数字形式存在，因此用人单位可以快速地验证它们的有效性以及真实性，而不用再依赖于纸质文件或者第三方机构进行验证了。同时，学生将拥有自己个人信息数据的所有权，除非学生允许的情况下，如果否，则任何人都不能访问上述信息以保证个人信息的安全性和隐私性。将区块链应用到教育领域的数据存储中时，我们需要根据需求选择合适的区块链平台以及存储方案或者结合其他存储方法弥补区块链在存储方面的不足。

（四）访问控制机制

为保证教育信息的安全性和私密性，我们需要使用访问控制来确保只有合格的人才能访问特定的学习信息，并防止未授权的数据盗用和滥用。由于 AI 的发展，学习信息被越来越多的不同类型的人所接收，比如：学生、教师、家长、学校的管理人员、研究人员以及商业合作伙伴等等。而他们对这些信息的需求及权利又不尽相同。为确保系统安全可靠运行，需构建合理的权限管控机制，并依据人员职能、岗位属性、业务需求、信息安全等级进行定制化资源授权操作。现阶段，较为普遍的权限管控方式主要有三种类型，分别为用户自主式权限管控 (DAC)、系统强制性权限管控 (MAC) 和职位导向式权限管控 (RBAC)。其中，自主型模型由数据所有者来决定谁可以获取相关数据信息，虽然方便但存在安全风险；而基于约束模型则事先制定好安全评估机制，并由系统管理方依据数据敏感性和用户的可信度设定可访问的数据范围，这么做固然能起到监督作用，但缺乏一定的灵活性。

（五）隐私增强计算

隐私增强计算是指可以保证信息保密的前提下，在数据上进行一些计算或者分析的一组方法和技术。因此，如何利用隐私增强技术来处理人工智能时代下的教学数据就显得非常重要。但在教育领域使用人工智能模型往往需要较多的学习样本数据，如果直接以原始形式的数据来进行计算，则存在个人隐私泄露风险。但加入差分隐私技术可以实现不公开原始数据进行数据运算分析的目的。安全多方计算、同态加密及差分隐私是目前比较常见的隐私增强计算技术，允许多个参与方在不共享各自私有数据的前提下协同完成一个计算任务，并保证所有参与方的计算结果为公开可验证，但各参与方原始输入数据均处于保密状态。

例如，安全多方计算可以让各学校共同分析学生学习情况，并比较各自的教学效果而不暴露个人隐私信息；而同态加密是一种特殊的加密技术，允许在不揭示原始数据的情况下对其加密进行操作，最终的结果和对原始数据的操作结果相同。这也就意味着对于教学资料的数据处理环节中，首先要将这些教学资料进行加密处理，在此基础上再进行智能算法学习分析，最后才可以对计算结果进行解密处理，以此来保护个人隐私信息；差异化保密技术就是针对数据库搜索的结果产生一定噪声，以避免黑客使用该方法获得单个个体的信息。

二、人工智能时代教育数据隐私保护伦理规范构建

（一）确立核心伦理原则

在智能教育时代确立教育数据保密性的伦理准则，首先要明确主要的伦理规范，对教育数据的收集、使用及共享等环节进行基本的伦理约束，并贯穿于教育数据处理全过程之中，以此指导学校的决策者、人工智能技术提供方、教师以及家长等多元主体的行为。

其一，尊重原则。该原则主要是针对学生的个性发展和自主性的保障，同时也应该尊重其个人意愿和需求，在收集教育数据时，应该取得学生及其父母明确同意，并告知所收集数据的目的、用途、存储方式及相关风险；学生拥有决定哪些个人信息可以被收集的权利，而且随时可以撤回授权。

其二，最小必要原则。在实现预定目的的前提下，对获取、使用的信息进行严格控制，并限定为能够满足实现上述目的所需要的最低限度，不应超出合理必要的限度而获取、使用相关信息，比如只须知晓学生的学习进程，就无须获取其经济状况等个人信息。对于信息来说，在进行处理过程中，应当尽量减少其中涉及学生私密的信息数量，只留下直接对教学工作产生影响的

数据。

其三，公平透明原则。教育数据使用的公平性和公正性保障。避免因教育数据应用过程中产生的歧视及不公等问题。例如，在学生评价、升学推荐等方面需注意评估及推荐过程中的公正性，以避免数据歧视造成学生发展权的丧失。

（二）完善监管体系

有效的制度保障是确保在人工智能背景下落实教育数据伦理原则的重要条件。应由相关部门负责主要的管理监督工作，并出台相关的政策法规以及技术指南来明确教育数据隐私权保护的具体措施及违法惩处机制。

一方面，健全相关法律制度体系，在当前已有的个人信息保护法框架内，针对教育特殊性设定更加具体的实施条款。具体而言，应当明确界定并区分教育信息的具体范围、类别及级别，以及采集、保存、传输过程规范，强化对教育信息的保护，二是健全问责机制，加大违法行为处罚力度。

另一方面，建立完备的监管机制。设置专门的数据管理机构监督学校的教育数据和人工智能教育企业的数据处理行为，并通过例行检查、专项调查、投诉举报等方式及时发现和纠正教育数据处理中的违法违规行为。

（三）明确主体责任

智慧教育中涉及的教育信息隐私保护涉及到多方主体：学校、人工智能提供方、教师、家长以及学生本人等，厘清各方的责任担当是制定道德规范的重要前提。从学校方面来说，由于其主要承担着收集和存储的角色，所以首要承担责任应该是学校。学校应建立内部信息管理系统，并配备相应信息化管理人员，明确职责任务；加强对教职工隐私保护意识宣传教育工作，提高法律意识；在引入人工智能产品厂商合作的过程中签订严格的保密协议，明确双方对学校数据使用过程中的权利义务关系，确保其按照规范的方法途径利用学校数据信息。

对 AI 技术供应商而言，则需将隐私保护理念融入到产品设计与开发阶段，在系统架构和技术方案上采用可信的安全技术和数据管理手段确保教育资源存储、传输与使用过程中的安全性，为教育机构提供整体化的教育信息安全管理服务。为了及时补救软件安全漏洞；教师作为教育信息的使用者，应遵守学校数据使用规范，合理使用学生学习数据，不可滥用学生学习数据用于非教务目的，也不得泄露学生个人隐私。家长以及儿童本人都应加强信息安全意识，了解自身的权利义务并积极参与到教育数据的安全保障中来。家长对子女学习资源的利用情况进行定期检查，在出现不正当收集运用个人信息的情形时及时进行质疑和反对；儿童掌握自身隐私保护方法，不随便向不可信的人或者网站暴露个人隐私信息。

（四）强化教育引导

加强全社会的教育数据隐私保护意识离不开教育引导，一是将数据隐私保护知识纳入学校教育体系，从小培养学生的数据隐私保护意识及素养，二是以专门课程的形式或讲座的方式或者实操等形式开展相关教育。从而使其具备必要的个人信息保护的知识、技能和伦理准则。

例如，教会学生正确使用网络的教学软件，保护自己的账号密码安全，分辨虚假的信息索取等问题，并对老师、家长以及学校的管理进行培训和教育，以讲座或者开会的形式普及个人信息保护的重要性和必要性在教育材料中的重要性。提升他们使用这类材料依法办事的习惯及能力。

此外，其次，可以通过各类媒体进行宣传教育数据安全知识，如拍摄公益宣传片或者专题报道等，宣传维护个人信息隐私的重要性。更为直接的是，在主流电视平台、报刊媒体及网络平台定期发布教育领域数据安全分析报告，具体分析产生问题的原因及影响并提出切实可行的隐私保护方式以增强公众抵抗能力。构建多渠道的宣传教育体系能让公众充分认识到教育数据私隐保护的重要性与紧迫性，达到全民防护的目的。

三、结束语

综上所述，人工智能时代下的教育数据隐私保护是巨大的系统工程，既需要技术体系支撑，也需要伦理规范引导。技术体系可以为教育数据隐私保护提供强有力的保障，在此过程中主要运用到的技术包括：数据脱敏技术、联邦学习技术、分布式存储技术（区块链）、身份认证技术和差分隐私技术。可有效防止发生在采集、存储、处理以及共享等各个环节中的教育数据隐私泄露风险。随着教育信息化深入发展，在不断探索如何将科学技术的应用与伦理规范相结合的同时，我们应该不断完善教育信息安全机制建设。运用合理的人工智能等先进技术，既要提升教书育人的效果，并促进教育公平，也应当重视保护学生个人信息安全。构建稳定可靠的教育信息安全保障体系，为我们的所有求学者营造出一个安全、可信的网络学习环境。

参考文献

[1] 戚万学，谢娟 . 教育大数据的伦理诉求及其实现 [J]. 教育研究，2019（7）：26-35.

[2] 杜静，黄荣怀，李政璇，等 . 智能教育时代下人工智能伦理的内涵与建构原则 [J]. 电化教育研究，2019（7）：21-29.

[3] 徐峰，吴旻瑜，徐萱，等 . 教育数据治理：问题、思考与对策 [J]. 开放教育研究，2018（2）：107-112.

[4] 李青，韩俊红 . 数据治理：提升教育数据质量的方法和途径 [J]. 中国远程教育，2018（8）：45-53.

[5] 宋苏轩，杨现民，宋子强，等 . 教育信息化 2.0 背景下新一代高校智慧校园基础平台建设研究 [J]. 现代教育技术，2019（8）：18-24.

