

# 隐私保护与开放共享:人工智能时代的教育数据治理变革

田贤鹏

(江南大学 田家炳教育科学学院, 江苏 无锡 214122)

**[摘要]** 如何推进基于隐私保护和开放共享的教育数据治理成为深化人工智能应用过程中需要迫切回应的两难议题。以此为语境,文章从隐私保护与开放共享的矛盾关系视角分析考察人工智能时代教育数据治理的迫切挑战、现实境遇和变革路径。研究发现:(1)教育数据的开放共享要求不断提升,但隐私空间却可能被严重压缩;教育大数据的开放应用场景将不断丰富,但隐私保障难度却空前提升;(2)隐私保护制度缺失导致的教育数据泄漏风险、开放共享支持不足造成的教育应用场景受限等正在成为教育数据治理面临的严峻考验;(3)促进教育数据治理变革需重构教育数据治理的制度伦理空间,强化教育主体的安全保障意识和能力、拓展基于技术升级的开放应用可能。

**[关键词]** 人工智能; 数据治理; 教育; 隐私保护; 开放共享

**[中图分类号]** G434

**[文献标志码]** A

**[作者简介]** 田贤鹏(1990—),男,河南商城人。副教授,博士,主要从事教育政策与管理研究。E-mail: xianpengtian@163.com。

## 一、引言

人工智能不仅是一场技术革命和产业革命,更是一场数据革命。无论接受与否,数据正在像空气和水一样成为不可或缺的基本生存资源,每一个虚拟或者实体的存在都将成为基于数据的信息综合体<sup>[1]</sup>。在教育领域,学校、教师和学生等相关主体都已被卷入这场声势浩大的数据革命之中,基于数据分析的电子书包、智能教室、智慧校园等相关应用正在渗透到教育教学改革的全过程之中,并且全方位地重塑教育治理的理念、方法和路径。随着智能应用场景的不断丰富和深化以及商业资本的推波助澜,数据革命对于学校、教师和学生的这种影响还将持续地走向深化。如何通过教育数据治理变革来科学处理数据产生、存储、使用和管理过程中的隐私保护和开放获取的关系,无疑会成为一个迫切的新时代议题。正如控制论

创始人维纳(Norbert Wiener)所言:“技术的发展,对善和恶都带来了无限的可能性。”<sup>[2]</sup>人们正在一方面享受着数据应用带来的各种便捷和福利,另一方面却遭受着个人隐私空间被不断压缩的烦恼和弊端。由于教育数据治理的失范,学生和教师数据信息被公开叫卖、侵犯学生和教师数据隐私等现象频繁发生,数据垄断、授权应用场景受限等诸多问题也在不断出现。推动教育数据的隐私保护和开放获取成为教育治理变革亟待破解的当务之急,但已有研究对此问题的关注却严重不足。

## 二、人工智能时代教育数据治理面临的迫切挑战

在卢西亚诺(Luciano Floridi)看来,“人工智能使得数据痕迹可以被记录、监控、处理,并被广泛应用于社会、政治或商业等各种目的。”<sup>[3]</sup>怎样使用数据并使

基金项目:江苏省高校哲学社会科学研究重大项目“人工智能背景下教育的技术逻辑研究”(项目编号:2019SJZDA072);中央高校基本科研业务费专项资金资助项目“高校学科专业结构布局与调整研究”(项目编号:JUSRP12076)

得数据价值得到合理发挥是教育数据治理迫切需要回答的问题。从治理诉求看,隐私保护与开放共享是人工智能时代教育数据治理的核心内容。

### (一)教育数据开放共享诉求日趋强烈,但隐私空间却被严重压缩

无论从教育应用还是商业应用的角度看,数据自身并没有特别的价值,其价值是在使用过程中实现的,开放共享是发挥和提升数据应用价值的前提基础。对于应用决策而言,数据只有经过系统整合、形成相互支持的应用价值链,才能在教育教学改革过程中发挥有效的价值。但由于开放共享准则与机制不完善,数据在不同部门和学校之间无法实现互通共享,信息孤岛、数据垄断等造成的共享壁垒严重阻碍了数据应用价值的最大程度发挥。推动开放共享成为人工智能时代教育数据治理需要回应的迫切诉求,且随着人工智能应用场景的深化和扩展,这种诉求也会愈来愈强烈。美国教育统计中心早在2009年就专门组织专业力量进行了“通用教育数据标准(CEDS)”的研发,以简化不同教育机构和学校之间的数据交换和比较过程,促进数据在横向和纵向层面的共享<sup>[9]</sup>。纽约大学、加州大学伯克利分校、华盛顿大学等则联合共建大数据生态系统(Ecosystem for Big Data),以期充分利用日益增加的共享数据进行教育管理和学生分析。

但对谁开放共享数据、如何开放共享数据则具有高度复杂性和系统性,关涉各方面利益主体的相关利益及其隐私保护。也就是说,教育数据的开放共享是有限度的,其不仅与教育部门 and 学校的治理权限和能力有关,还与学生和教师的隐私权利保障有关。一方面,扩大教育数据的开放共享空间虽然有利于提升数据的应用价值、形成相互支持的应用价值链,从而更好地服务于教育教学改革,但却有可能侵犯到教师和学生等相关主体的隐私空间;另一方面,限制教育数据的开放共享空间虽然有利于保护教师和学生等相关主体的隐私空间,但却有可能束缚教育数据应用价值的发挥,导致教育教学改革无法享受人工智能发展带来的数据应用红利。从人工智能的不可逆态势看,推动教育数据开放共享是必然要求,促进教师和学生数据隐私保护也是必然要求。

### (二)基于教育大数据的开放应用场景不断丰富,但隐私保障难度却空前提升

为了最大化地挖掘数据的教育应用价值和商业应用价值,人工智能在教育教学改革中的应用场景将必然得到进一步深化和拓展,但由此带来的隐私保障难度也将不断提升。如何避免成为“裸奔的透明人”成

为人工智能时代教育数据治理面临的突出挑战。伊恩·艾瑞斯(Ian Ayres)就曾担忧地指出:“大数据分析减少了我们的有效隐私空间,我们生活在了一个越来越无法隐藏我们是谁、我们做了什么以及我们会做什么的世界里。”<sup>[10]</sup>基于教育大数据的分析应用已经广泛进入课堂、教室和校园,而且这种应用正在随着人工智能技术的提升而愈加深化和多元。但与传统信息环境不同,人工智能不仅破坏了一种基于匿名的隐私平衡,而且能在增加或减少信息摩擦上给信息智能体授权,其全方位场景应用在一定程度上架空了用户的选择权,迫使用户不得不做出某些被动的选择<sup>[9]</sup>。

通过对教师和学生的日常行为习惯和学习行为特征数据进行深度的挖掘分析,可以为教育教学和校园综合治理提供决策支撑,但这也在无形中将教师和学生的隐私暴露在了第三方空间之中,严重削弱了教师和学生对于自身隐私控制的实际能力。从价值角度看,数据是被动的客观存在,其到底是发挥积极功能还是消极功能则取决于使用主体。在教师和学生眼里,数据是其个人隐私,应当得到必要尊重和保护;在学校管理者眼里,数据是推进改进教育教学的支撑,应当得到有效的记录和保存;在商业开发者眼里,数据是拓展商业利益的工具,通过数据分析可以展开有针对性的商业营销。但随着教育应用场景的拓展,数据产生的来源将愈来愈广、过程将愈来愈复杂、规模将愈来愈庞大、使用目的也将愈来愈多元,而这显然会提升数据隐私保障的难度系数。

## 三、人工智能时代教育数据治理的现实境遇

从来源看,随着人机交互的不断深化,组织层面的学校、个体层面的教师和学生都将成为海量隐私数据的生产者和携带者,但却很难成为这些隐私数据的掌控者。事实上,大量的教育应用数据正在被第三方机构所掌控,学校、教师和学生往往成为被动的数据提供者,而由此带来的教育数据治理问题也将空前严峻。

### (一)隐私保护制度缺失导致教育数据泄漏风险加大

人工智能时代的万物互联、人机共存使得任何主体行为的发生都将被不可避免地记录在数据网络系统之中,无处不在的监控无论对于教师还是学生都将是—种恐怖的存在<sup>[6]</sup>。人的信息存在方式赋予了人权的数字属性,使得教师和学生由“自然人”转向“信息人”。

一方面,作为一项技术,人工智能是在不断发展

和突破的,而这也意味着基于现有技术的人工智能应用可能存在各种各样的漏洞。事实上,诸如“3D”人脸识别系统、指纹识别系统以及其他相关应用管理系统的安全保障问题已经引起了社会的广泛关注,“黑客”入侵数据系统的各类困扰也在频繁发生。教育领域中,智能头环、“刷脸”报道、“刷脸”签到等相关应用更是引发了人们对于数据安全问题的深度担忧。尽管万物互联、人机共存给个性化教育实施提供更多可能,但当每一种存在都成为数据的生产者和携带者时,数据泄露的渠道和路径就会增多,相关风险无疑就会越来越高。

另一方面,数据是一种可供生产实践应用的资源和工具,为了追求应用价值的最大化,相关主体可能在违背教育伦理的情况下滥用数据以谋取非正当性利益。不同于传统的外显化侵权,人工智能时代的“算法黑箱”<sup>[7]</sup>会形成自动化的歧视和侵权“决策”,一旦存在算法歧视、信息控制、侵犯隐私等问题,就会成为连续性的常规动作,产生系统化和机制化的侵权后果。人工智能场景中,教师和学生的数据信息不仅有巨大的教育应用价值,而且其商业开发价值也同样可观。垄断性的数据平台能够借助各类教师和学生数据进行非教育目的的营利性行为。

## (二) 开放获取支持不够造成教育数据应用场景受限

不同教育应用场景的数据系统具有相对的自我封闭性,呈现出松散的碎片化特征,难以构成支撑教育决策的完整应用价值链。从教育数据治理的角度看,实现基于开放共享的数据整合是充分挖掘教育数据应用价值的前提保障,开放获取支持不够会限制和束缚人工智能在教育场域中的应用空间范围。人工智能应用的巨大优势在于基于海量数据的精准分析和预测,但其发挥的基础在于不同系统之间的数据整合和共享。

首先,不同教育数据系统的异质性增加了开放共享的难度。数据产生于行为,在不同的系统,基于学生和教师行为产生的数据记录方式和内容有所不同。高校信息管理系统建设主要以实现业务功能为导向,在底层数据结构设计方面并没有构建起统一的数据存储标准和管理准则,导致大量数据在不同高校信息管理系统之间的存储形式不一,由此形成了一数多源的“数据孤岛”<sup>[8]</sup>。而且,教育应用市场上的管理信息系统开发主体相对多元,彼此之间并没有形成基于开放共享的数据基础架构,导致不同高校管理信息系统之间的相互兼容性严重不足。

其次,数据的机构性垄断造成了教育应用共享的排他性。超级机构平台可以通过数据生态系统的构建来采集和存储海量数据,以达到特定的数据控制目的。从性质上讲,数据一旦生成就能够被无限制地复制和应用,但从应用角度讲,对谁开放、怎样开放却涉及复杂的权利和利益问题。具有垄断性能力的超级平台机构为了维护自身的权利和利益往往会拒绝向第三方提供数据共享服务。2019年5月,由中国人民大学发布的国内首份有关数据垄断的研究报告《互联网平台新型垄断行为的法律规制研究》显示,数据管理平台呈现出“赢者通吃,一家独大”的特点。在美国,诸如 Coursera 等超级学习平台已经占有超高的市场份额,并且正在利用自身的数据闭环系统来限制用户转移以排斥其他平台进入,从而达成数据控制的目的。

最后,学校对于技术的不信任阻碍了数据开放共享的进程。由于教育对于技术应用的反应相对迟钝,导致大数据在教育领域中的应用场景非常有限。从深层原因看,这种反应的相对迟钝可能源自于学校对于技术的不信任。与国外相比,人工智能在我国商业应用领域发展较快,企业相关机构的技术接受能力较强,但在教育领域,由于基于技术的数据素养教育缺失,教育管理者、教师和学生的技术接受能力相对较弱,其数据素养提升速度远远落后于人工智能的应用发展速度。

## (三) 教育数据治理中隐私保护与开放共享的关系矛盾难以化解

如何获取数据涉及隐私保护和开放共享之间的关系平衡和处理。隐私保护要求充分尊重教师和学生的知情权,保障教师和学生的相关隐私不受侵犯;开放共享则要求扩大教师和学生的数据信息整合力度,以便最大化地挖掘数据的应用价值。从根本上看,隐私保护和开放共享之间存在着严重的矛盾冲突性。对此,学术界也呈现出了两种不同声音:一是从公共视角出发,将教育数据视为一种公共资源,主张强化底层数据架构的顶层设计,推动数据在不同应用主体之间的互通共享;二是从个体视角出发,将教育数据视为一种个人隐私,主张完善数据隐私保护的法律法规,将学生和教师的数据隐私权作为一项基本权利纳入隐私权的保障范围。随着人工智能在教育场景应用的范围和深度不断拓展,两种声音此起彼伏。但教育数据治理不可能离开隐私保护而探讨开放共享,也不可能为促进开放共享而不顾隐私保护。事实上,人工智能构筑了一个包含无数教育应用场景的、基于数据分析的虚拟空间。只有进入这个空间,才能享受到全

新的价值体验,但进入这个空间也就意味着留下数据,而留下数据在一定程度上就是对自身隐私权的转让抑或对自身数据信息的共享。在技术力量的强大驱动下,愈来愈多的教师和学生正在或主动或被动地进入这个空间,一方面意味着愈来愈多的数据隐私侵权问题将有可能发生,另一方面则意味着愈来愈多的数据共享价值将会得到更大程度的挖掘。如何在保障教师和学生隐私信息的同时推进数据开放共享,是人工智能时代的教育数据治理必然面临的两难选择。

#### 四、人工智能时代教育数据治理的路径选择

人工智能时代,数据权利逐渐成为公民的一项基本权利,推动人工智能时代的教育数据治理变革需充分关照组织层面和个体层面相关主体的矛盾复杂性以及隐私保护与开放共享的内在冲突性。一方面,要将学生和教师的隐私权益置于价值秩序的优先序列,确保教师和学生的合法权益不受侵害;另一方面,要借助人工智能来推动教育教学变革,从而更好地为促进学生健康成长和教师专业发展服务。在此背景下,如何在保障学生和教师隐私不受侵犯的基础上最大程度地发挥教育大数据的应用价值是人工智能时代教育数据治理不懈的目标追求。

##### (一)优化教育数据隐私安全保护机制,重构数据治理的制度伦理规范

为了保障数据隐私安全,欧盟早在20世纪90年代中期就制定出台了《数据保护指令(简称DPD)》,确立了“数据主体在收集数据时应给予通知”“未经数据主体同意,不得披露同意数据”等七条促进个人数据保护的基础原则和制度伦理规范。随着人工智能开启的大数据革命的到来,其在《数据保护指令》的基础上于2018年修订出台了《通用数据保护条例(简称GDPR)》,进一步赋予数据主体以“删除权、限制处理权、反对权和自动化个人决策相关权利”,同时在2019年制定出台了《欧盟人工智能伦理准则(简称EGAI)》。此外,针对教师和数据隐私和安全,美国曾先后制定实施了《家庭教育权利与隐私法案(FERPA)》《保护学生权利修正案(简称PPRA)》《儿童在线隐私保护法(简称COPPA)》《学生数字隐私和家长权利法案(简称SDPPRC)》等相关法规,联邦教育部则专门建立了首席数据隐私官(简称CPO)制度。

与此同时,国内学者也在不断呼吁建立立体化、多层次的教育数据安全机制,例如制定《教育大

数据权利法》《个人教育数据保护法》《教育大数据行业公约》等。但从实际的政策行动看,相关的呼吁并没有得到足够的重视和响应,泄露教师和学生数据隐私的问题仍然频繁发生<sup>[10]</sup>。重构基于教育数据安全保护的制度伦理规范将会愈来愈迫切。

具体而言,可主要从四方面推进:一是在数据收集和使用过程中,要保障教师和学生的知情权,必须经过教师和学生同意后方可进行收集和使用;二是学校不得将教师和数据用于商业营利目的,未经授权不得随意向任何第三方机构或者个人转让;三是要确保学生和教师数据的有效性,严格禁止任何捏造、篡改教师和学生数据行为的发生;四是建立教育数据安全管理的问责机制,任何泄露教师和学生数据隐私的行为以及违反数据安全保护原则的举动都应受到相应的严格惩戒。

##### (二)提升教育决策主体的数据治理能力,强化教师和学生数据安全保护意识

从相对发展看,人工智能在教育场景中的应用更新速度远超教育数据治理体系重构的速度,而相关主体的数据治理能力的落后则是其关键所在。就现实状况而言,人工智能带来的突破变革及其对教育发展的渗透影响程度是社会各界所始料未及的,变化之快、力度之大远超正常想象,但数据准确性不高、一致性不强、标准性不足等问题<sup>[11]</sup>却在严重制约着其具体应用价值的发挥。如何通过数据治理能力提升来最大限度地挖掘其正向价值、避免负向应用价值,是教育相关主体需要着力回应和解决的迫切议题。对此,有学者认为,应通过设置教育数据治理的组织机构、制定和完善数据通用标准<sup>[12]</sup>等来促进相关治理体系的完善;也有学者指出,要通过一站式服务中心、数据中心和认证建设,在平台服务层实现业务流程整合、数据统一规划治理和管理服务应用标准化<sup>[13]</sup>等。从深层次看,这些举措的核心在于提升与人工智能发展速度相适应的现代化数据治理能力。

人工智能环境下,教师和学生不仅要有与人沟通交流的能力,在奥恩(Joseph E Aoun)看来,科技素养、数据素养和人文素养将会成为人们充分利用数字世界所必备的基本素养<sup>[14]</sup>。如何在教育数据治理能力提升的基础上培养教师和数据素养,强化其数据安全保护意识,也是传统教育内容体系需要进一步突破和创新的内在要求。首先是提升数据素养在整个教育教学内容体系中的地位,推动数据素养教育进教材和课堂,培养适应人工智能发展的新时代公民,以弥补传统教育教学中的数据安全意识教育缺失

问题;其次是优化数据素养教育的过程保障机制,明确应用主体在数据使用过程中的权利和义务边界,为教师和数据素养能力提升提供立体化、全方位的支持;最后是大力推动教师和学生数据隐私安全保障的政策与法规的制定和落实,并据此完善合法权益保障的相应救济规则,依法惩戒侵犯教师和学生数据安全的行为。

### (三)促进基于区块链的安全保障技术应用,拓展教育数据获取的开放应用可能

区块链是一种分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式<sup>[15]</sup>,因其具有去中心化、可靠性和可追溯性等特征而被认为是确保数据安全的重要技术突破。目前区块链已经广泛应用于信用背书、信息加密、智能合约等诸多领域,并且在教育领域也显现出巨大的潜力<sup>[16]</sup>。从趋势特征看,区块链构成了联结教育数据治理中隐私保护和开放共享的技术载体,为实现数字教育资源共建、共享提供了新的工具和方向。对于教育数据治理而言,首先要从价值层面突出关注数据存储、挖掘和获取过程中的应用伦理构建,以确保避免数据使用过程的非法行为发生;其次要从事实层面重点关注技术自身的创新突破,以技术进步弥补传统工具手段的不足。显然,区块链技术在教育领域中的应用属于后者,需要以新技术的进步和创新来回应原有技术的缺陷和漏洞。促进基于区块链技术的教育应用需要从两方面进行努力。

一方面,深化以区块链技术研究为基础的教育数据安全保障系统优化,提升技术自身的抗风险性和安全性。正如联合国教科文组织2019年报告《教育中的人工智能:可持续发展的挑战和机遇》中所指出的那样,“构建开放、高质量和包容性强的教育数据系统是人工智能教育可持续发展的重要前提”<sup>[17]</sup>,而基于区块链技术的研究深化则是构建开放、高质量和包容性强的教育数据系统的技术保障基础。现阶段,包括安全保障技术在内的人工智能正处在一个飞速发展的关键节点,尽管各种新技术手段和应用层出不穷,但基于基础研究的底层数据安全架构却并不完善,数据泄露或者被盗用导致的各种风险仍然广泛存在。从原理上看,区块链技术的研究深化将在很大程度上缓解教育数据治理过程中隐私保护和开放获取关系矛盾难以调和的困境。其不仅可以通过去中心化消除教育

数据共享过程中的隐私保护问题,而且能够借助分布式数据系统存储拓展教育数据的开放共享空间,从而在确保教师和学生数据隐私保障安全的基础上,促进人工智能在教育中的应用场景的深化。

另一方面,加强区块链技术在教育数据治理领域的安全应用和推广,推动去中心化的教育数据共享新机制构建。从技术成熟度来看,区块链还处在一个快速变革创新的初始阶段,有关区块链的技术应用仍然有待进一步的实践探索和检验。事实上,从基础研究开发到技术成熟应用有一个相对漫长的周期。就教育领域而言,决策者要保持对区块链技术进步的敏感性,以便及时将成熟的技术应用在相对合适的教育场景,但又不能冒进、盲目的信赖技术。从未来趋势看,加强区块链技术的安全应用和推广为教育数据治理的应有之义和重要内容。目前理论界和实践界已经达成的一个基本共识是:“区块链技术能够在一定程度上解决当前开放教育资源建设面临的运营成本高、版权保护弱、资源共享难和资源质量低等现实问题。”<sup>[18]</sup>构建基于区块链技术的教育数据开放共享新机制有着巨大的应用和推广前景,是推动教育数据治理中隐私保护和开放共享关系矛盾化解的重要手段和路径方向。

## 五、结 语

数据既具有个体意义上的隐私性,又具有组织层面的开放性。对于教育数据治理而言,隐私保护与开放共享是对立统一的矛盾综合体。一方面,隐私保护要求决策主体应当充分关照与教师、学生和高校数据有关的合法权益,构建基于个体隐私的数据开放边界,避免教育数据泄露或滥用带来的制度伦理风险;另一方面,开放共享却要求决策主体从打破教育数据垄断、促进教育智能应用深化出发,推动不同数据综合体之间的互动和联结,从而实现对教育数据价值最大程度的挖掘。从内在联系看,隐私保护是开放共享的前提和基础,是教育数据治理必须坚守的基础准则;开放共享则是充分挖掘教育数据价值的必然要求,是促进人工智能在教育领域应用深化和拓展的客观需要。深化人工智能时代的教育数据治理变革,需要动态平衡隐私保护与开放共享的对立统一关系,重构基于隐私保护和开放共享的制度伦理空间,在确保教师、学生和高校等相关主体的隐私得到合理保护的同时,致力于最大限度地挖掘和拓展教育数据的应用价值。

### [参考文献]

[1] 卢西亚诺·弗洛里迪.第四次革命:人工智能如何重塑人类实践[M].王文革,译.杭州:浙江人民出版社,2016.

- [2] 诺伯特·维纳.控制论[M].郝季仁,译.北京:科学出版社,2016.
- [3] Common education data standards. The CEDS Initiative[EB/OL].[2019-08-20].<https://ceds.ed.gov/whatIsCEDs.aspx>.
- [4] 伊恩·艾瑞斯.大数据思维与决策[M].宫相真,译.北京:人民邮电出版社,2016.
- [5] 侯浩翔.人工智能时代学生数据隐私保护的动因与策略[J].现代教育技术,2019(6):12-18.
- [6] 江山.校园拒绝摄像头[N].中国青年报,2019-09-11(007).
- [7] AUDET C, LE DIGABEL, SEBASTIEN, TRIBES C. Dynamic scaling in the mesh adaptive direct search algorithm for black-box optimization[J]. Optimization and engineering, 2016(2):333-358.
- [8] 董晓辉,郑小斌,彭义平.高校教育大数据治理的框架设计与实施[J].中国电化教育,2019(8):63-71.
- [9] 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.
- [10] 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.
- [11] 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.
- [12] 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.
- [13] 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.
- [14] 约瑟夫·E·奥恩.教育的未来:人工智能时代的教育变革[M].李海燕,王勤辉,译.北京:机械工业出版社,2019.
- [15] 任仲文.区块链领导干部读本[M].北京:人民日报出版社,2018.
- [16] 李青,张鑫.区块链:以技术推动教育的开放和公信[J].远程教育杂志,2017(1):36-44.
- [17] UNESCO. Artificial intelligence in education: challenges and opportunities for sustainable development [EB/OL].[2019-08-20].  
<https://unesdoc.unesco.org/ark:/48223/pf0000366994>.
- [18] 李新,杨现民.应用区块链技术构建开放教育资源新生态[J].中国远程教育,2018(6):58-67,80.

## Privacy Protection and Open Sharing: Reform of Education Data Governance in the Era of Artificial Intelligence

TIAN Xianpeng

(Tin Ka Ping College of Educational Science, Jiangnan University, Wuxi Jiangsu 214122)

**[Abstract]** How to promote the governance of education data based on privacy protection and open sharing has become a dilemma that needs urgent response for deepening the application of artificial intelligence. On this account, this paper analyzes the urgent challenges, realistic situations and reform paths of education data governance in the era of artificial intelligence from the perspective of contradictory relationship between privacy protection and open sharing. The study finds that (1) the requirements for open sharing of education data are increasing, but the privacy space is likely to be severely compressed; the open application scenarios based on education big data will be continually enriched, but privacy protection will be more difficult than ever. (2) The risk of education data leakage due to the absence of privacy protection systems and limited educational application scenarios due to inadequate open sharing support are becoming serious challenges for education data governance. (3) Promoting the reform of education data governance requires reconstructing the institutional ethical space for education data governance, strengthening the security awareness and capacity of educational subjects, and expanding the possibilities of open applications based on technology upgrading.

**[Keywords]** Artificial Intelligence; Data Governance; Education; Privacy Protection; Open Sharing