人工智能与大数据协同发展中的数据依赖性风险与缓解策略

刘亚乾
内蒙古自治区大数据中心　内蒙古　呼和浩特　010010

摘　要：人工智能（AI）与大数据作为驱动第四次工业革命的核心引擎，其协同效应已深刻重塑了社会生产方式、商业模式乃至人类认知范式。然而，在二者深度融合的过程中，一种日益凸显且被广泛忽视的结构性矛盾——“数据依赖性风险”正逐步成为制约其健康、可持续发展的关键瓶颈。本文旨在系统剖析这一风险的多维内涵、生成机理及其潜在危害，并在此基础上，围绕技术、治理、伦理与法律等多个层面提出一套综合性、前瞻性的缓解策略。经研究，过度的数据依赖不仅可能导致模型性能脆弱、算法偏见固化、创新路径锁定等技术性问题，更会引发隐私侵蚀、市场垄断、社会不公乃至国家安全等深层次的社会性危机。通过构建“以人为本、多元共治、技术向善”的协同发展新范式，才能有效驾驭数据依赖性风险，释放人工智能与大数据融合的最大潜能，确保其发展真正服务于人类福祉。

关键词：人工智能；大数据；数据依赖性；算法偏见；数据治理；可信赖AI

引言

当下是数据定义的时代，海量大数据为人工智能（下文简称“AI”）尤其是深度学习模型提供“燃料”与“训练场”，AI 的强大能力又提升数据价值与应用广度，二者协同成为推动社会进步的核心动力。然而，强大能力同时往往伴随着相应风险，AI 与大数据协同背后潜藏根本悖论：AI 智能水平高度依赖数据质量、规模与多样性，这使 AI 生态异常脆弱。海量数据背后的隐性缺陷、偏差或恶意操控等有意或无意的风险，伴随AI训练的过程中会不断放大成为问题，产生系统性危害，此即“数据依赖性风险”。目前，学术和产业界对 AI 伦理等问题探讨多，但对数据依赖性这一根源问题系统研究不足，多停留在现象描述。为此，本文将填补空白，深入探究其生成逻辑、表现及连锁反应，提出立体化缓解策略，为构建稳健、公平、可信的AI 未来提供支撑与指引。

1 数据依赖性的生成机理与核心维度

1.1 技术范式的驱动：从符号主义到连接主义的转向

早期的AI模型（如专家系统）主要基于符号主义，依赖人工编码的知识规则进行推理。其局限性在于知识获取的“瓶颈”和规则的僵化。而以深度神经网络为代表的连接主义范式，则通过从大量数据中自动学习复杂的模式和特征表示，实现了对高维、非结构化信息（如图像、语音、文本）的有效处理。这一范式的成功，本质上是“数据驱动”而非“知识驱动”的胜利。模型的“智能”不再源于程序员的显式指令，而是内生于数据本身的统计规律之中。因此，数据的质量直接决定了模型所能学到的“知识”的上限。

1.2 核心维度解析

数据依赖性风险可以从以下四个相互关联的维度进行解构：

质量依赖性：AI模型的性能高度敏感于输入数据的准确性、完整性与时效性。噪声数据、缺失值、过时信息都会导致模型学习到错误的模式，从而在推理阶段产生谬误。例如，在金融风控模型中，若历史信贷数据存在大量未被发现的欺诈行为，模型可能会将这些欺诈模式误认为是正常行为，从而降低其检测能力。

规模依赖性：许多先进的AI模型，尤其是大型语言模型（LLMs）和计算机视觉模型，其性能随训练数据量的增加而显著提升，呈现出明显的“规模定律”（Scaling Laws）。这导致了一种“数据军备竞赛”，企业竞相收集更大规模的数据集以维持竞争优势。然而，这种对规模的盲目追求，往往忽略了数据的边际效益递减和潜在的负面外部性。

分布依赖性：AI模型是在特定数据分布（即训练数据所代表的世界）下进行优化的。当模型部署到现实世界，而现实世界的分布（测试分布）与训练分布存在差异时（即“分布外泛化”问题），模型的性能会急剧下降。这种依赖性使得AI系统在面对未曾见过的新场景、新群体或突发事件时显得尤为脆弱。

偏见依赖性：数据并非客观中立的，它记录的是人类社会的历史、文化和权力结构，不可避免地携带着各种形式的偏见（如性别、种族、地域、社会经济地位

等）。AI模型在学习数据模式的同时，也会无意识地学习并固化甚至放大这些偏见。这种依赖性使得AI系统可能成为社会不公的自动化执行者。

2 数据依赖性风险的具体表现与深层危害

上述四个维度的依赖性，在实践中交织作用，催生出一系列复杂且深远的风险。

2.1 技术性能风险：脆弱性与不可靠性

数据依赖性首先在技术性能上展现出其脆弱性。由于模型对输入数据的微小扰动极度敏感，攻击者可以通过精心构造人眼无法察觉的“对抗样本”，诱使模型做出完全错误的判断，这便是对抗性攻击的典型体现。例如，在自动驾驶场景中，对交通标志牌贴上特定贴纸，就可能让车辆的视觉系统将其误识别为其他指令，造成致命后果。这暴露了数据驱动模型在鲁棒性上的根本缺陷[1]。此外，现实世界是动态变化的，数据背后的规律（概念）也会随之演变，这种现象被业界称为“概念漂移”。用户偏好、市场趋势、疾病传播模式都在不断变化，假使AI系统不能及时感知并适应这种漂移，其预测和决策将迅速过时，导致业务失败或公共政策失效，从而使其在真实世界中的可靠性大打折扣。

2.2 社会公平风险：偏见固化与数字鸿沟

数据依赖性在社会危害上的体现尤为深刻，集中表现在对社会公平的侵蚀。AI模型在学习历史数据时，会无意识地继承并放大其中蕴含的社会偏见，导致算法歧视。招聘AI可能因历史招聘数据中男性占优而倾向于筛选男性简历；信贷AI可能因历史数据中低收入群体违约率较高而系统性拒绝该居民群体的贷款申请；司法AI可能因地域性历史判例中的种族偏见而对特定族裔给出更重的量刑建议。这些自动化决策因其“客观”、“高效”的表象，反而更具隐蔽性和破坏力，加剧了社会不平等。与此同时，主流数据集往往过度代表了特定人群（如发达国家的年轻网民），而边缘群体（如老年人、残障人士、偏远地区居民）的数据则严重匮乏。这导致为大众设计的AI产品（如语音助手、人脸识别系统）在特定群体身上表现极差，形成新的“数字鸿沟”，剥夺了他们享受和适应技术红利的权利，在非主观因素上无意识的强化了特定社会结构的待遇不公平和不适应条件。

2.3 经济与市场风险：垄断与创新抑制

在经济层面，数据依赖性催生了严峻的市场失衡问题。拥有海量高质量数据的科技巨头凭借其数据优势，构筑了极高的竞争壁垒，形成了事实上的数据垄断。新进入者难以获取同等规模和质量的数据来训练有竞争力的模型，导致市场趋于寡头垄断。这种“赢者通吃”的局面不仅抑制了市场良性竞争，也扼杀了技术创新的多样性。更值得警惕的是，整个行业对现有大规模数据集的深度依赖，使得研发资源过度集中于已被验证的数据模型范式，而对需要全新数据类型或小样本学习等创新技术路径投入不足。这种路径依赖与创新锁定效应，可能导致整个AI领域陷入“内卷”，错失真正的突破性机遇，长远来看损害了整个行业的活力与潜力。

2.4 隐私与安全风险：监控资本主义与数据滥用

为了满足AI对数据规模和粒度的需求，个人数据正在通过刻意识或无意的广度和深度进行收集、聚合与分析，这在不经意间构成了对个人隐私的系统性侵蚀。“监控资本主义”模式将用户的行为数据商品化，用户在不知情或非自愿的情况下，成为了被分析和操纵的对象。即使数据经过匿名化处理，通过数据融合技术，依然可以重新识别个体身份，使得传统的隐私保护手段形同虚设[2]。在安全层面，数据依赖性也带来了新的攻击面。作为一种主动攻击手段，数据投毒通过向训练数据集中注入恶意样本，从源头上污染模型的学习过程，使其在特定任务上失效或产生后门。这对于依赖众包数据或开放数据源的AI系统构成了根本性的安全挑战，攻击者则利用这一弱点，可以低成本达到瘫痪或操控关键AI服务。

2.5 治理与主权风险：黑箱决策与国家安全隐患

数据依赖性还给现代治理体系带来了前所未有的挑战。当一个高度依赖复杂数据流的AI系统做出错误甚至有害的决策时（如自动驾驶致死事故、AI医疗误诊），责任链条将变得模糊。数据提供者、模型开发者、部署方乃至AI本身多方责任边界不清，形成了问责困境，现有的法律和伦理体系难以实现公正评判，给司法和道德评判施加了压力。从国家层面看，关键领域的AI系统（如国防、金融、能源、公共卫生）若过度依赖特定境外或不受控的数据源，将构成严重的国家安全风险。特定方可能通过操控数据流来干扰或瘫痪关键基础设施，或利用特定国家公民的敏感数据进行情报分析和战略预判，从而威胁国家的数据主权与整体安全。

3 数据依赖性风险的缓解策略：迈向多元共治

3.1 技术层面的创新：从被动依赖到主动塑造

在当前环境下应多角度发展和拓宽思路，积极探索小样本学习与自监督学习等前沿技术可行性，旨在减少对海量标注数据的依赖。小样本学习致力于让模型从极少的例子中快速学习新概念，而自监督学习则通过设计巧妙的预训练任务，从未标注数据中自动提取监督信号，有望打破“数据规模至上”的局面。同时，着力

提升模型的鲁棒性与可解释性，研发能抵御对抗性攻击、适应分布外数据的鲁棒模型，并大力发展可解释AI（XAI）技术，使模型的决策过程不再是“黑箱”，能够追溯其判断依据是否源于数据中的合理模式还是有害偏见，从而增强人类的监督与干预能力。此外，构建合成数据与联邦学习生态也是关键路径[3]。利用生成对抗网络（GANs）等技术创建高质量的合成数据，可以用于补充真实数据的不足或保护隐私；而推广联邦学习框架，则允许多个参与方在不共享原始数据的前提下协同训练模型，实现“数据不动模型动”的新规则，从根本上解决数据孤岛和隐私泄露问题，重塑数据协作的范式。

3.2 治理层面的完善：构建全生命周期的数据治理体系

应建立贯穿数据采集、存储、处理、使用的全生命周期数据治理体系，推行严格的数据质量标准与第三方审计机制，对用于训练关键AI系统的数据集进行偏见、准确性和代表性的评估，并强制披露审计报告。在数据收集的源头，必须严格实施“数据最小化”与“目的限定”原则，只收集实现特定、明确且合法目的所必需的最少数据，并禁止数据的二次滥用。尤为重要的是，应建立算法影响评估（AIA）制度，对于在公共领域或高风险领域部署的AI系统，强制要求进行事前的全面评估，重点审查其数据来源的合法性、潜在的偏见风险以及对弱势群体的影响，并将评估结果作为系统上线的前置条件，将风险防控关口前移。

3.3 伦理与法律层面的规制：确立以人为本的价值导向

在现有的、流于形式的“点击同意”模式上加以改变，强化和探索更有效的动态同意机制，强化用户的知情同意权，并赋予其随时撤回同意、访问、更正乃至删除其数据的完整权利（即“被遗忘权”），真正将数据控制权交还给个人。在法律层面，亟需立法明确AI开发者、部署者和使用者在不同场景下的责任边界，可以借鉴产品责任法，将高风险AI系统视为一种“产品”，其提供者需对其造成的损害承担严格责任，以此倒逼其在数据选择和模型设计阶段就充分考虑风险[4]。更进一步，应倡导“价值敏感设计”（Value Sensitive Design）理念，将公平、透明、问责、隐私等伦理价值内嵌到AI系统的整个开发生命周期中，而非事后补救，并鼓励开发团队吸纳伦理学家、社会科学家等多元背景成员，进行常态化的跨学科伦理反思，确保技术发展始终锚定在正确的价值引航方向上。

3.4 社会层面的赋能：促进公众参与与数字素养

通过教育体系和社会宣传，大力提升全民的数字素养与AI素养，普及数据和AI的基本知识，让公众理解数据依赖性风险的存在，学会批判性地看待AI输出的结果，并有能力参与到相关的公共讨论和政策制定中，形成自下而上的监督力量。

4 结语

人工智能与大数据协同发展如双刃剑，数据依赖性既是其力量源泉，也是脆弱性根源。本文尝试揭示该风险在技术、社会等多维度的表现与危害，本质是体现技术逻辑和社会价值的张力，从而化解风险。但并非否定数据价值或阻碍 AI 发展，而是尝试越过技术决定论，走审慎、包容、负责的发展路径。这需构建由技术创新、精细治理、伦理约束和公众参与共同组成“免疫系统”，探索发展高效且少依赖海量数据的 AI 技术，建立全生命周期数据治理体系，用法律伦理设定边界，赋能数据主体。未来竞争不仅面向算力和数据之争，更是治理、伦理与创新能力多角度间竞争，只有管理好数据依赖性风险，才能让 AI 与大数据驶向公正、安全、繁荣的未来。

参考文献

[1]周霞,谷莹,陈为东,等.政府数据协同治理影响因素及其驱动-依赖机制研究[J].情报科学,2025,43(02):67-75+148.

[2]朱新武,刘小丽.数据赋能与数据依赖：大数据技术嵌入社会治理的双重效应[J].宁夏党校学报,2022,24(05):86-95.

[3]杜传忠,李钰葳.人工智能与大数据深度融合驱动科技创新范式变革的机制与路径[J].社会科学研究,2026,(01):30-40+229.

[4]张雪.人工智能与大数据融合赋能中国式现代化研究[J].数字经济,2025,(12):102-104.