# 2024中关村论坛——数据安全治理与发展论坛精彩观点

近日，2024中关村论坛——数据安全治理与发展论坛在中关村国际创新中心成功举办。会上，国内外科研院所专家学者交流前沿理念、分享研究成果。

数据安全治理与发展论坛现场。中关村论坛供图

精彩观点碰撞

柳俊泓

新加坡资讯通信媒体发展局局长

数据虽然看不见摸不着，但它推动着数字经济的发展。如何在数据安全保护和创新发展之间取得平衡？大多数国家和地区都有着相似的处理方式。首先，获得用户授权同意，是使用个人数据非常重要的环节；第二，数据机制需要明确数据不可用的领域；第三，顶层设计要审慎，数据可用的领域应占大多数；第四，要建立协调机制，通过标准合同条款进行协调，有助于实现一定程度的全球一致性。

数据是人工智能的核心，一些新服务、新解决方案由传统人工智能和生成式人工智能创造出来。我们需要对数据和人工智能建立信任，要真正聚焦共性的人工智能测试方法，促进人与人之间的交流。人工智能发展凸显出数据的重要性，同时也在创造一个全球性的治理框架，其中建立互信是最重要的因素。

沈昌祥

中国工程院院士

大数据具有多源异构、非结构化、低价值度、快速处理等特点。随着信息技术发展和海量数据爆发，安全成为支撑大数据健康发展的关键。我们要打造数据治理安全可信的新生态，构建数字经济主动免疫保障体系，实现“六不”防护效果，使数据安全治理达到有效的目标：一是“进不去”，即攻击者进不去；二是“拿不到”，即非授权者重要信息拿不到；三是“看不懂”，即窃取保密信息看不懂；四是“改不了”，即系统和信息改不了；五是“瘫不成”，即系统工作瘫不成；六是“赖不掉”，即攻击行为赖不掉。

郭毅可

香港科技大学首席副校长

在人工智能和大语言模型为各行业带来变革的时代，数据安全治理显得尤为重要。为防止未经授权访问和数据泄露，要采取严格的安全措施，通过数据匿名化技术、用户同意和隐私设计原则以及实施数据分类、访问控制和加密方法等，保护知识产权和防止未经授权的披露。除了制定明确的政策和框架，以及有效的数据分类和归类以外，访问控制和权限管理也是确保数据安全的关键因素。

此外，我们需要在保护数据隐私和敏感信息的同时，建立国际机构框架和制定法规来确保数据安全。通过建立健全法规，应用先进技术，加强国际合作，推动人工智能规范发展，确保数据安全治理有效实施。

孙茂松

清华大学人工智能研究院常务副院长

生成式人工智能带来很多挑战。我们发现，机器翻译产生的双语质量并不高，用这些数据训练机器翻译系统，反而会造成损害。随着其生成能力的增强，如果放任不管，机器生成的内容很快就会超过人类创作的内容，而且其中很多内容可能与事实不符，用这些内容来训练大模型，可能会带来隐患。因此，这一领域确实面临着许多挑战，需要全球各国政府和学者共同努力，从技术上解决这些问题。同时，生成式人工智能也为数据治理提供了非常重要的正面推动作用。我们可以通过为大模型增加某些条件，如特定提示词（Prompt）或标签（Tag），让它生成尚未遇到过的情景数据，从而帮助我们进行预判。

七大成果发布

北京市数据跨境便利化实践

继全国首个数据出境安全评估项目、首个通过订立标准合同实现个人信息合规出境案例“两个全国第一”在北京落地后，北京市政产学研联合打造数据出境“绿色通道”机制，覆盖汽车、医药、民航、零售、人工智能五大行业百余家企业，通过政策咨询、宣讲解读、靠前指导、材料预审等一系列便利化举措服务企业主体超4000家；设立数据跨境服务中心，搭建全国首个数据托管服务平台、数据安全与治理公共服务平台，数据跨境高质量社会化服务能力大幅提升。近一年，北京市数据出境安全评估通过企业增长650%，个人信息出境标准合同备案通过企业实现破百，出境数据多样性和通过率稳居全国前列，为加快发展新质生产力、推动数字经济高质量发展提供有力保障。

中文互联网语料库CCI 2.0

北京智源人工智能研究院发布中文互联网语料库CCI 2.0，规模约500G，是经过严格清洗过滤的中文数据集。CCI 2.0在1.0版本基础上，进一步扩充数据来源、完善数据处理流程、提升数据规模和质量，并通过数据集“共建-共享”合作运营机制，持续推动迭代更新，为大模型技术发展提供高质量、高可信的数据资源支撑。

数据认证实践和展望

由国家市场监管总局、国家网信办牵头，中国网络安全审查认证和市场监管大数据中心具体支撑的数据安全管理认证制度和个人信息保护认证制度最新实施进展发布，全国首个地市级数据认证联络工作站落地北京市海淀区。数据安全管理认证制度和个人信息保护认证制度贯彻落实国家法律要求，有力推动企业数据安全和个人信息保护意识与能力提升，有效促进数据要素合理利用和便捷流动。

北京人工智能数据训练基地监管沙盒

北京市经信局、北京市网信办组织相关单位建立北京人工智能数据训练基地监管沙盒机制，依托北京数据基础制度先行区、北京人工智能数据训练基地提供的可信空间和强大智算资源，形成多项人工智能训练数据应用创新机制，向大模型企业模型训练提供“强大算力+海量数据+监管合规”的完整训练要素，成为我国首个将监管沙盒机制应用于人工智能领域的案例。

北京市高级别自动驾驶示范区数据安全治理白皮书

北京市高级别自动驾驶示范区办公室发布《北京市高级别自动驾驶示范区数据安全治理白皮书》，基于示范区海量自动驾驶产业数据，以“保障示范区数据全过程安全合规，促进车路云一体化数据价值挖掘”为目标，率先开展数据分级分类、实时感知安全态势、定期进行风险评估、推动应用技术创新等专项工作，为解决产业数据安全治理共性需求打造标杆实践指南。

生成式人工智能安全风险测评平台及大赛

中科院信息工程研究所创新构建大模型安全技术测评体系，研究开发生成式人工智能安全风险测评平台，并依托该平台举办首届生成式人工智能安全大赛，设置安全攻击、安全检测、对齐防护三大赛道，构建“众研、众用、众创”的中文大模型安全评估模式，促进人工智能底层技术和基础底座的安全可控水平不断提升。

国家网络安全融合发展试验区（北京市海淀区）网络安全公共服务平台

北京市海淀区依托国家网络安全教育技术产业融合发展试验区建设，创新打造网络安全公共服务平台，立足“政府主导、企业经营、市场运作、社会参与”的工作思路，开通“网安120”24小时公共服务热线，汇集头部网络安全资源，面向社会公众、企业提供网络安全应急处置、溯源分析、整改加固等全栈服务。

数据安全治理与发展论坛现场。中关村论坛供图

此外，在圆桌论坛环节，来自清华大学、剑桥大学、香港科技大学、IBM、华为、奇安信的数据安全专家，聚焦生成式人工智能数据安全治理热点问题，从理论研究、技术应用、产业实践、国际合作等方面分享实践经验、研讨发展路径，推动人工智能技术赋能产业健康发展。

本次论坛由国家互联网信息办公室、北京市人民政府主办，国家互联网信息办公室网络数据管理局、北京市互联网信息办公室、北京市经济和信息化局、北京市政务服务和数据管理局、北京市商务局、海淀区人民政府、大兴国际机场临空经济区（大兴）管理委员会承办，清华大学人工智能国际治理研究院、国家互联网应急中心北京分中心协办。

澎湃新闻2024-5-9