

# 联邦学习：兼顾数据价值释放与隐私权利保护

□ 金玲飞

习近平总书记在中央政治局第二十次集体学习时强调，人工智能带来前所未有的发展机遇，也带来前所未有的风险挑战。其中，数据泄露风险就是风险挑战之一。随着人工智能在医疗、金融、交通、教育等领域的不断深入应用，人工智能的安全治理与个人信息隐私保护的交叉融合已成为不可回避的关键议题。当前主流的人工智能系统大多依赖于机器学习算法，而数据作为其核心驱动力，既支撑着模型的性能，也带来了数据泄露和隐私侵犯的隐忧。因此，如何在保障数据安全利用和用户隐私的前提下有效释放数据价值，成为人工智能发展的重大课题。

近年来，隐私计算技术不断取得进展，如安全多方计算、同态加密、可信执行环境等，在一定程度上提升了数据在隔离状态下的计算能力。然而，由于人工智能应用场景复杂多样、需求多变，现有技术仍难以全面覆盖所有场景，存在效率瓶颈和落地难题。以智慧医疗为例，假设甲、乙两家医院希望联合训练一个疾病预测模型，以提高诊断的准确性和泛化能力。但受数据监管政策和隐私合规要求的限制，原始医疗数据无法直接共享。若两家医院各自单独建模，训练数据的代表性和规模难以保证，会影响模型性能。因此，在数据物理隔离和隐私保护的前提下，实现

“数据可用不可见”的联合建模需求，就需要一种新的训练范式——联邦学习。

联邦学习（Federated Learning）正是为解决这一难题而生。该概念最早于2016年由谷歌提出，2017年谷歌研究团队推出了初步的系统性解决方案。其核心思想是，在不共享原始数据的前提下，多个数据持有方通过协同参与模型训练，实现模型优化与数据保护的双重目标。在联邦学习框架中，算法训练从传统的中心化模式转变为分布式模式：中心服务器将模型参数分发给各参与方，各参与方在本地使用私有数据进行模型更新，随后将加权参数上传，由中心服务器聚合，形成新的全局模型。整个过程中，数据始终保留在本地，有效解决了数据孤岛与隐私泄露的双重难题。同时，分布式训练还可缓解中心计算资源压力，提升系统可扩展性。

根据参与方数据在样本空间和特征空间的重叠情况，联邦学习可分为三种主要类型：横向联邦学习、纵向联邦学习和联邦迁移学习。横向联邦学习（Horizontal FL）适用于参与各方拥有相同的特征空间但不同的用户群体，比如多家银行之间合作建模。纵向联邦学习（Vertical FL）适用于参与各方拥有相同的用户但不同的特征空间，例如银行和电商平台之间的合作。当参与各方

用户和特征都较少重合时，可借助联邦迁移学习（Federated Transfer Learning）进行跨域建模。

尽管联邦学习在数据隐私保护方面展现出独特优势，但其本身并非“绝对安全”，仍面临多种潜在威胁。例如，模型反演攻击试图通过模型的预测结果反推出训练数据；梯度反演攻击则借助模型参数在传输过程中的梯度信息，还原本地数据的敏感特征。这些攻击手段虽具有一定技术挑战性，但已在多个研究中得到验证，对参与方隐私构成实际威胁。

为应对上述安全挑战，联邦学习通常与差分隐私（Differential Privacy）相结合，进一步增强系统的抗攻击能力。差分隐私通过在模型参数或输出结果中添加随机噪声，使攻击者即使掌握了模型信息，也难以准确推断出单个用户的数据。在联邦学习场景中，噪声可被添加至每轮上传的本地参数中，提升整体隐私保护水平。该策略已在医疗、金融、社交网络等多个敏感数据领域获得应用验证。

不过，差分隐私的引入也带来了新的平衡问题：噪声越多，隐私性越强，但模型性能可能越差。因此，需要根据应用需求精细设计噪声机制，常见方式包括在中心服务器端加入噪声，实现中心化差分隐私；或在本地客户端加入噪

声，实现本地差分隐私。不同策略适用于不同场景，需权衡安全性、精度和效率。除了隐私性，联邦学习的通信成本也是实践中面临的重要挑战。每轮模型训练涉及大量参数传输，可能引发通信延迟和带宽压力。为此，研究人员提出了如参数压缩、稀疏更新、异步通信等技术优化方案，力求在降低通信开销的同时保障模型训练效率。

展望未来，联邦学习仍有巨大的发展潜力。随着算法优化、系统设计和隐私机制的不断进步，其适用范围将进一步拓展。例如，在智能制造、智慧交通、车联网、智能家居等新兴领域，如何在数据边缘安全高效地实现协同智能，将成为下一阶段的研究热点。同时，随着公众对个人数据保护意识的增强，全社会对可信人工智能系统的需求也愈加迫切。政府、产业界与学术界应携手推进隐私计算标准化建设，完善法律法规与技术手段，共同打造一个兼顾数据价值释放与隐私权利保护的人工智能新生态。



（上接1版头条）要创新治理模式机制，推进“光伏+治沙”，现阶段落实好“发电”为主转向“治沙”为主的要求，强化光伏治沙规划管控，合理划定好适建区和禁止区，严禁在已治理或已绿化土地上发展光伏；推进以路治沙，将穿沙公路纳入农村公路建设，有序建设成防沙路、防火路、致富路；推进产业治沙，利用沙区独特资源，适度发展中药材、优质牧草、经济林果、沙漠旅游产业，实现治沙又致富。要创新央企参与机制，充分利用央企技术、资金、管理优势，进一步完善央企参与“三北”工程建设的政策措施，强化要素保障，加大绿色金融支持力度，支持央企更好履行高标准社会责任。

注重统筹协调，在凝聚合力上下功夫。习近平总书记强调，“实施‘三北’工程是国家重大战略，要全面加强组织领导，坚持中央统筹、省负总责、市县抓落实的工作机制，完善政策机制，强化协调配合，统筹指导、协调推进相关工作”。持续打好“三北”工程攻坚战，必须按照“1+N+X”工作方案，统筹抓好一盘棋格局，突出重点治理，调动各方面积极性。中央层面要发挥国务院“三北”工程协调机制作用，统筹抓好重大问题研究解决、重要规划布局、重点项目和用地、用水、用钱等政策要素保障，通过林长制层层压实地方责任。各部门要发挥各自优势，加大支持力

度。省级层面要切实担负起总体责任，统筹研究解决区域性重大问题，抓好目标任务落实，加强全过程指导管理。市县层面要结合本地实际强化具体执行，统筹抓好任务落地、资金使用、物资保障。

弘扬“三北精神”，在讲好中国防沙治沙故事上下功夫。习近平总书记强调，“抓生态文明建设，既要靠物质，也要靠精神”。战天斗地、改造山河的英雄气概，甘于奉献、造福子孙的家国情怀，持之以恒、代代相传的历史担当，尊重群众、依靠群众的求实作风，铸就伟大的“三北精神”，深刻影响激励着一代又一代治沙人，赢得了国际社会广泛赞誉。持续打好

“三北”工程攻坚战，要继续用好用足“三北”这座富矿，持续选树典型经验和先进人物，让“三北精神”不断赓续发扬，化为推动“三北”工程攻坚战的巨大精神力量。要用好用足国际组织和平台，广泛宣传习近平生态文明思想，主动展示美丽中国建设成果，生动讲好中国防沙治沙故事，积极引领全球生态治理。

坚决打好“三北”工程攻坚战是重大政治任务，林草系统将牢记嘱托、感恩奋进，以高度的政治自觉和强烈的责任担当，不断推动“三北”工程标志性战役取得重要成果，以优异成绩向党和人民交上合格答卷。

（上接1版二条）完善信贷支持机制，健全科技型企业授信容错纠错机制，着力营造创新驱动、包容审慎的良好金融服务环境。特别是在科技要素集聚区，根据需要发展科创金融特色机构，有效提升科技型企业融资可得性和便利度。更好发挥资本市场关键枢纽作用。资本市场具有独特的风险共担、利益共享的激励相容机制，能够提供全链条、接力式融资服务，可以满足不同阶段企业需求。支持科技型企业上市挂牌融资和科技型上市公司高质量发展，持续规范“后备库”，打造上市“预科班”，分层分类提供培育服务，推动解决卡点堵点问题。强化区域性股权市场服务能力，推动专精特新专板做大做强，设立瞪羚、独角兽专板，促进企业股权和可转债融资。加快落实债券市场“科技板”政策，摸排企业需求，创新服务模式，积极支持债券发行。

更好发挥创业投资生力军作用。创业投资是科技创新的重要资金来源，尤其在支持初创企业和早期项目方面发挥着不可替代的作用。优化投资基金设立条件，丰富创业投资种类，拓宽投资资金来源，积极争取国家级基金支持，广泛吸引银行保险资金和其他长期资本来辽投资。积极申请金融资产投资公司股权投资试点，畅通科技金融“资金—资本—资产”的有效循环。建立健全基金绩效管理和容错机制，鼓励投早、投小、投长期、投硬科技。

更好发挥保险“减震器”“稳定器”作用。科技保险具有风险补偿、资金杠杆作用，能够为科技创新提供风险分散和金融保障支持。实施“险资引入畅通工程”，是在拓展长期稳定资金供给方面的一项创新实践。通过搭建高效“险企”对接平台，高频组织“险资入辽”活动，引导长期资本、耐心资本深耕，一举打破东北地区3年来无险资引入困局。积极探索以共保体方式开展重点领域科技保险风险保障，开展重大技术攻关、中试、网络安全等风险分散试点。针对科技型企业技术研发、生产运营、市场推广、成果转化等环节的重点风险开发推广新型保险产品。鼓励保

险机构设立科技保险专营机构、部门、团队，探索投资科技金融资产支持计划等证券化产品，争取保险资金长期投资改革试点，促进保险资金参与实施国家重大科技任务。

更好发挥政府性融资担保和风险补偿增信作用。财政资金在科技创新中发挥重要的杠杆作用，通过融资担保、风险补偿等政策工具，可以撬动更多金融资源流向科技创新领域。增强政府性融资担保和风险补偿增信功能，建立科技创新类“白名单”信息共享机制，深入实施支持科技创新专项担保计划，通过给予风险补偿、担保费奖补、提供增信服务等政策扶持，进一步降低科技型企业融资成本。健全科技金融风险补偿制度，探索推广科技金融风险补偿资金池，进一步拓宽风险补偿范围，合理分摊金融机构风险成本。

## 在科技需求端协同发力,拓展深化科技金融应用场景

科技型企业作为科技金融的需求端，在获得金融机构提供优质产品和服务的同时，也需要修炼好自身内功，着力构建“科技出题、金融答题”的协同机制，实现供需适配、相互促进的良性循环，形成相向而行、双向奔赴的良好格局。

强化关键核心技术攻关。科技金融的功能定位和战略属性已经不局限于服务科技型企业融资，而是提高到支撑国家战略科技体系和能力建设的更高目标，向关键核心技术攻关和基础研发领域延伸。从源头看，发展科技金融，需要全面提升原始创新能力。坚持以国家战略需求为导向，加强基础研究和应用基础研究，实施科技重大专项，有针对性部署重大科研攻关任务，力争多出“从0到1”的原创性成果，打通产业发展过程中遇到的技术“断点”、创新“卡点”。强化企业科技创新主体地位，加强企业主导的产学研用深度融合，着

力发挥科技领军企业龙头作用，大力培育壮大科技型企业群体，促进产业链上下游企业、大中小企业协同创新，合力打好关键核心技术攻坚战。

加强知识产权保护利用。科技创新具有高投入、高风险、高回报的特点，其发展离不开金融的支持。但科技型企业普遍具有“轻资产、重知产”的属性，呈现“缺担保、多专利”的特征，难以满足金融机构传统业务模式和风险偏好，导致金融资源无法有效流向科技创新领域，亟须在盘活无形资产上下功夫，积极探索知识产权与金融资源融合的有效模式。大力实施知识产权高标准保护工程，稳妥推进国家知识产权保护示范区建设，充分发挥知识产权融资杠杆作用，最大限度挖掘知识产权经济价值，不断强化知识产权运用，积极争取知识产权金融生态综合试点，助力实现“知产变资产”的金融创新，有效破解轻资产科技型企业融资难题。

促进科技成果转化。科技创新中蕴含着巨大的价值，而科技成果的价值在于运用。科技金融的核心在于解决科技创新过程中的资金瓶颈问题，通过金融手段引导资本流向科技创新领域，推动科技成果转化成为现实生产力。进一步完善科技成果转化体系，提升孵化转化载体建设水平，加强重点领域、重点单位针对性布局和应用示范场景建设，为新技术新产品应用推广助力。加强科技成果转化服务，引进和培育专业化技术经理人、中介服务机构，支持鼓励高校院所建立专业化技术转移机构，推动专利链、产业链深度融合，持续释放“沉睡”技术潜力，推动更多创新成果从实验室走进车间、走向市场，为实体经济的创新发展注入不竭的动力与活力。

## 在体制机制上强化保障,着力营造科技金融良好生态

科技金融是一项复杂的系统工程。

推进科技金融体系建设既需要从供给侧和需求端同向发力，也需要创新体制机制、营造良好生态。

健全工作机制。高效有序的工作机制，是推动科技金融体系高效运行的重要保障。我们将持续强化系统观念，加强科技金融工作的部门协调、政策联动和信息共享，统筹研究制定科技金融重要政策、先行先试和组织实施等相关事项。注重政策宣传解读，努力让更多科技型企业应知尽知、应享尽享，切实提升政策触达率和兑现率。加强执行跟踪评估，将金融机构服务科技型企业评价结果作为科技金融示范机构评选的重要依据，稳步推进科技金融示范机构、示范点、示范项目建设。

鼓励创新实践。科技金融作为新领域、新业态，需要在实践中不断丰富发展路径和工具体系，加强间接融资和直接融资联动，强化政策性金融和商业性金融补充，优化权益类投资和债务性融资组合，通过业务融合、股债联动、产品互补等方式，增强科技金融整体服务合力。全面推广“创新积分制”，构建覆盖科技型企业创新能力的多维度评价指标体系，对科技型企业“精准画像”，搭建科技型企业创新积分综合服务平台，发布科技型企业“创新积分制白名单”，丰富积分应用场景。开展区域性创新实践，鼓励引导各地区和金融机构大胆探索各具特色的创新实践，形成一批可复制、可推广的经验。

加强能力建设。发展科技金融，归根结底需要依靠提升服务能力来实现。强化数字赋能，充分借力大数据、区块链和人工智能等科技手段，加强金融科技的应用和应用，加大金融机构数字化转型力度，以金融科技赋能科技金融发展。强化中介服务，进一步提高科技咨询、价值评估、风险评价等服务公信力，为科技金融业务开展提供参考。强化人才培养，不断完善内外培训、选拔激励、监督管理等全链条工作机制，提升科技金融从业人员专业水平，打造一批既懂金融又懂科技的复合型人才。（作者系辽宁省委常委、副省长）

人工智能是引领新一轮科技革命和产业变革的战略性技术，是赢得全球科技竞争主动权的重要抓手。党中央高度重视人工智能，习近平总书记在中央政治局第二十次集体学习中强调，全面推进人工智能科技创新、产业发展和赋能应用。当前，人工智能技术快速演进，以前所未有的深度和广度渗透到经济社会的各个领域，深刻改变人类生产生活方式。加快构建人工智能生态体系，是适应新形势下发展要求、抓住发展机遇的战略路径，也是推动经济高质量发展的必然选择。

人工智能生态体系是一个由基础层、技术层和应用层相互关联、协同运作所构成的复杂系统。基础层涵盖了算力基础设施和算法框架等要素，作为根基为技术层提供了必要的支撑；技术层聚焦模型训练和工具开发，构建了人工智能的核心技术，是链接基础层和应用层的桥梁；应用层则将技术层的模型和工具融合应用到具体场景中，使人工智能的价值最终落地实现。良好的生态体系下，技术进步驱动应用创新、应用创新反哺技术进步共同推动人工智能迭代优化。一方面，推动应用场景从单点突破迈向多元化拓展，不断深入细分行业，广泛赋能智能制造、智慧医疗、金融风险等领域，持续催生新质生产力。另一方面，下游应用提供了更加丰富的数据和反馈，促进人工智能的迭代升级，推动模型能力快速提升。

各地因地制宜培育人工智能，有力推动了生态体系建设。北京市海淀区计划每年投入超10亿元，建设具有全球影响力的创新策源地，打造世界级人工智能产业集群；上海市徐汇区打造大模型“超级孵化器”，推动形成以“模速空间”为中心的高密度、全要素人工智能创新生态；浙江省杭州市从激励场景供需双方联合创新、奖励场景创新成果绩效两个维度支持“人工智能+”应用创新，加速智能产品在真实场景的首试首用和全面推广。在各地有力探索下，我国人工智能生态逐步建立。基础层蓬勃发展，算力规模和技术成果爆发式增长。

2024年，我国智能算力规模达725.3EFLOPS，同比增长74.1%，市场规模突破190亿美元，增速高达86.9%；截至2025年4月，我国人工智能专利申请量以38.58%的全球占比稳居世界首位。技术层迭代快速，关键技术不断取得重大进展，DeepSeek-R1仅用极少标注数据便极大提升了模型推理能力，性能对标OpenAI o1正式版；华为昇腾910C NPU在计算效率方面已超越英伟达H800 GPU。应用层百花齐放，百度阿波罗系统在自动驾驶系统、智能座舱、地图等方面构建了竞争优势；浙江大学智能创新药物研究院的靶点发现大模型和小分子药物设计大模型使药物靶点分子生成成功率翻倍，为AI驱动的药物研发提供全新高效解决方案。各地将人工智能作为产业创新的抓手，加速探究行业应用，从医疗诊断的精准辅助到具身智能的创新探索，以多元应用场景推动人工智能从概念走向现实，持续优化发展生态。

我国人工智能生态培育起步时间尚短，内外多重因素叠加下仍需解决几个关键问题。基础层，国产芯片算力与人工智能快速发展的需求相比仍有差距，个别西方国家对华芯片禁运加剧了国内算力供给紧张；全球数据生态中，中文公开数据规模与质量落后于英文数据，随着高质量数据需求从通用知识向专业知识转变，我国数据质量短板愈加凸显，制约了算法效能的发挥。技术层，人才缺口较大，云计算、深度学习等技术岗位人才供需比低至0.27，2030年人工智能熟练专业人员缺口或达400万人，技术人才储备成为关键掣肘。应用层，AI赋能中小企业过程中存在“藩篱”。目前，AI需求侧市场高度碎片化，大量中小企业个性化应用场景问题亟待解决，AI技术落地到千行百业真实场景的“最后一公里”尚未贯通。此外，基础层、技术层和应用层间融合不足也限制了人工智能生态的整体效能发挥，基础层芯片与技术层算法的高效对接、技术层创新成果在垂直行业中转化和微调等存在障碍。

# 加快构建我国人工智能生态体系

□ 杨超

习近平总书记强调，面对新一代人工智能技术快速演进的新形势，要充分发挥新型举国体制优势，坚持自立自强，突出应用导向，推动我国人工智能朝着有益、安全、公平方向健康有序发展。我国构建高质量人工智能发展生态，需从三方面着力。一是筑牢基础层底座，强化支撑体系建设。大力扶持国内算力芯片、数据中心等核心技术产品研发与产业化；优化算力基础设施布局，实现高效算力资源供给、调配和共享；面向重点领域及未来产业需求建设专业化高质量数据集，扩大数据供给、完善标准、加速可信数据空间构建，夯实数据基础；鼓励企业与科研机构开展数据服务创新，提供数据标注、清洗等专业服务，加快推动公共数据开放与企业间数据流通，推动数据生态体系构建。二是创新体制机制，激发各类主体创新活力，形成创新驱动、场景牵引、生态协同的全链条生态新格局。支持前沿理论探索，推动原始创新，加速共性技术研发；强化基础层、技术层、应用层协同，探索政策沙盘、新场景应用等机制建设，带动多领域场景全域开放；推动人工智能领域大中小企业优势互补、深度合作，加快标准推广与开源体系建设，打通人工智能向垂直行业应用“最后一公里”。三是保障安全可控，规范产业发展。为应对敏感信息泄露风险高、算法模型安全隐患规避难、虚假信息多等问题，加速相关法律法规或政策的制定，尽早出台针对人工智能重点领域的法规政策或行业规范，强化技术滥用的法律规制，为产业发展划定清晰的法治边界。健全分类分级监管机制，确保人工智能安全、可靠、可控，助力大模型应用落地和产业生态高质量发展，释放人工智能的巨大潜能，因地制宜发展新质生产力。

