扎紧智能风控“篱笆” 筑牢金融安全“防火墙”

唯有将生成式AI内容、智能体权限治理与金融市场行为监管有机衔接，方能激活金融科创活力，守护信息秩序、投资者权益与金融稳定。

图片由AI生成

□闫佳昕

当前，人工智能（AI）正加速嵌入金融业务全链条，技术形态快速迭代，风险形态也在相应变化。5月8日，国家网信办、国家发展改革委、工业和信息化部联合印发《智能体规范应用与创新发展实施意见》，将智能体界定为具备自主感知、记忆、决策、交互与执行能力的智能系统，并明确提出在金融服务场景中研发金融风控智能体。这一政策动向表明，金融领域的AI治理不能仅停留在效率层面，更需要回答风险是否可控、责任是否可追溯的问题。

金融AI应用风险形态分化

当前金融领域的AI应用，并非一个笼统的概念，而应作相应的分层审视。生成式AI和金融智能体虽同属人工智能范畴，但在金融业务链条中的位置、功能及其所伴生的风险形态，存在显著差异。

生成式AI主要作用于金融信息的生产环节。它可以依据提示词或指令，规模化生成宏观分析、行业研判与投资观点。这类系统并不直接执行金融交易，而是改变信息生产的速度、成本与仿真程度。其风险在于，一旦低成本、大批量、高度拟真的AI生成内容涌入金融信息环境，信息的质量、来源可追溯性和责任主体都可能被弱化。投资者面对的可能不再是可追溯至特定分析师或机构的有责信息，而是来源模糊、真假难辨、相互引用的“信息云雾”。

相较之下，金融智能体则更可能介入金融行为的执行层面。智能体不仅是内容的生成者，更是任务的执行者。它能够根据既定目标自主拆解任务、调用工具、与外部系统交互并完成操作。在金融场景中，金融智能体可用于信贷审批、智能投顾等环节，其风险重心已经移向权限是否清晰、执行是否可控、责任是否可穿透等方面。

这种分层意味着，金融AI的规范治理必须走出“一刀切”：对生成式AI，治理重点应放在内容真实性、来源留痕和标识披露上，防止不真实、不准确、具有误导性的信息污染金融信息环境；对金融智能体，治理重点则应转向决策权限、行为边界和责任穿透，防止不可解释、不可干预、不可追责的操作侵入关键金融决策。

当前金融智能应用亟待破解的问题

尽管AI为金融业带来效率革命，但若干风险隐患必须引起高度重视。

首先是金融信息污染问题。金融市场是高度依赖信息秩序的制度化市场，信息披露、投资者适当性、证券交易秩序和金融稳定监管，都以信息真实、准确、完整、及时为前提。生成式AI介入后，金融信息失范不再只是某一主体发布某一条虚假消息，而可能表现为错误、失真、误导或者被操纵的信息低成本、大规模进入金融信息环境，并被市场系统再次吸收。金融稳定理事会（FSB）2024年发布的《人工智能对金融稳定的影响》报告也警示，AI可能通过多种途径加剧系统性风险，包括对第三方服务提供商的依赖、与金融市场的关联性、网络安全风险、数据管理缺陷等，生成式AI还可能加剧金融欺诈和市场虚假信息传播风险。在投资者结构复杂、线上信息传播活跃的市场，此类污染信息极易放大追涨杀跌、主题炒作和情绪化交易，扭曲价格发现机制。因此，若大量金融机构采用相似的基础模型、相似的数据集和相似的投资策略逻辑，市场可能出现高度同步反应，放大金融市场的顺周期波动。

更值得警惕的是，随着智能体具备自动生成内容、抓取舆情、识别情绪并进一步执行操作的能力，传统虚假金融信息的多环节传导路径可能被压缩至同一自动化流程中。同一系统可能同时完成信息生成、社交平台扩散和交易执行等工作，风险传导时间大幅缩短，纠错窗口急剧收窄。这种一体化链条一旦形成，市场可能在短时间内出现高度同向反应，放大波动。

其次，智能体自动执行边界模糊，形式授权难以替代审慎义务。《智能体规范应用与创新发展实施意见》已要求智能体执行操作不得超出用户授权范围。但在金融场景中，授权本身并不自动等同于“适当”。金融消费者往往并不真正理解智能体如何调用数据、判断风险、触发交易或调整授信额度。若金融机构仅以用户点击授权作为合规依据，就可能在事实上将法定的适当性义务、风险提示义务和审慎经营义务技术化外包，最终损害金融消费者权益。拒贷、降额、自动调仓、自动交易、账户冻结等直接影响客户权益或市场秩序的操作，绝不能仅依赖形式授权，而必须设置更严格的人工复核、操作留痕和申诉救济机制。

最后，责任穿透难题对现有监管框架带来挑战。当AI生成错误投资建议、智能体误判授信风险、模型误触发交易行为时，责任究竟由金融机构、模型服务商、数据供应商还是用户承担？在现行监管逻辑下，对外提供金融业务的持牌机构通常不能因使用模型、数据或外部技术服务而免除其主体责任，但AI应用链条拉长后，责任极易被拆解为技术问题、数据问题和用户授权问题，从而弱化监管问责的力度。若责任不能有效穿透，AI就可能异化为规避金融监管义务的技术工具。

守住金融创新与金融安全双重底线

推动金融AI健康发展，必须坚持发展与安全并重。对于深圳而言，金融智能治理具有一定制度试验价值。深圳金融业务场景密度高、种类全，作为国内重要的金融中心城市，深圳的银行、证券、基金、保险等市场主体高度集聚，金融活动与科技产业、先进制造深度交织。这意味着，AI在深圳金融领域的应用不是零星的、边缘的，而是广泛的、深层的。

基于此，深圳可在三个方面率先探索，构建分层次、全链条的金融AI治理体系。

其一，建立按场景分层的权限管理制度。对于信息检索等辅助性应用，应重在内容核验、生成标识和来源管理；对于投资建议、授信评估等判断性应用，须强化模型验证、人工复核和适当性审查；对于拒贷、降额、自动交易等执行性应用，必须设置更高等级的授权、留痕、复核和申诉机制。

其二，完善金融信息污染穿透式治理机制。深圳金融市场活跃，线上信息传播和投资者互动频繁，更需要防止AI生成内容污染金融信息环境。对于面向公众发布的AI生成财经内容，应强化来源管理、生成标识和责任落实；对于可能影响证券期货价格、金融产品销售和投资者决策的信息，应纳入异常信息识别和异常交易监测体系，构建从信息端到交易端的穿透式观察与干预能力，严防信息污染向交易行为传导。

其三，从金融稳定视角加强模型与外部服务风险监测。针对深圳金融科技创新活跃、模型应用场景多等特点，可率先建立金融机构AI应用信息库，动态掌握模型类型、应用场景、数据来源、服务商依赖和异常处置机制。对系统重要性金融机构、关键金融基础设施和大型平台型机构，应常态化开展AI压力测试，专门评估模型失效、网络攻击等情形下的风险传导路径，防止技术风险、数据风险和市场风险交叉叠加，守住不发生系统性金融风险的底线。

从发展前景看，金融智能应用仍是深圳提升金融服务实体经济能力的重要方向。智能风控、反洗钱等监管科技，都有望借助AI实现效率和覆盖面的大幅提升。但越是在创新活跃的前沿地带，越要清醒认识并牢牢守住金融安全底线。只有将生成式AI的内容治理、智能体的权限治理与金融市场的行为监管有机衔接起来，才能在激发金融科技创新活力的同时，有效维护金融信息秩序、投资者保护和金融稳定，为深圳建设具有国际影响力的金融科技中心城市提供坚实制度保障。

时评

中国科技“踢”满世界杯全场

□佘惠敏

2026年美加墨世界杯激战正酣，全球数十亿观众的目光聚焦绿茵场。场上虽然没有中国球员的身影，但赛场内外，一支由AI系统、芯片足球、新能源客车和超高清显示设备组成的中国科技队，正以前所未有的深度和广度参与这场全球盛宴。

从“赞助商”到“技术合伙人”，中国企业在世界杯舞台上的角色之变，折射出中国科技竞争力的结构性跃迁。这不仅仅是品牌曝光层面的升级，更是从“卖产品”到“卖能力”、从“跟跑”到“并跑”甚至“领跑”的深层质变，标志着中国创新开始真正嵌入全球顶级赛事的核心命脉。

回望往届世界杯，中国元素的呈现多停留在卖货层面，可替代性强。而2026年的绿茵场上，中国科技完成了从外围配套到内核嵌入的质变。中国企业不再是单纯的供应商和赞助商，而是赛事基础设施的提供者、技术标准的参与制定者。

联想集团深度嵌入2026年美加墨世界杯赛事运营、判罚支持、观赛体验等核心流程，足球AI超级智能体、3D数字人可视化方案及裁判视角AI视频增强系统等全方位为赛事保驾护航。官方比赛用球“三重浪”在中国生产制造，搭载500Hz芯片的智能球胆出自顶碁运动公司，每秒可记录500次触球数据。海信、利亚德、洲明科技、艾比森等中国企业在超高清显示设备领域深度参与，覆盖核心判罚系统、国际转播中心及赛场大屏等多个关键环节。

交通出行方面，由中国中车研发制造的轻轨列车已在墨西哥3座承办城市投入运营，墨西哥城专为世界杯组建的新能源接驳车队中95%以上为中国品牌客车。

世界杯是一面镜子，照出了中国科技企业的实力，也照出了未来的方向。这场科技盛宴，为体育产业智能化升级勾勒出清晰前景。

体育产业兼具高频率、标准化、强互动等特征，是AI技术落地的绝佳场景。2026年美加墨世界杯被誉为“首届AI世界杯”，完成了顶级赛事的极限验证，相关AI能力正通过模块化设计，从塔尖向塔身、塔基等方面扩散。职业俱乐部可复用赛事级战术分析系统，社区足球、校园体育能借助轻量化AI工具提升训练科学性，弱资源国家也能通过标准化智能系统缩小竞技差距。AI技术底座具备资产属性，将推动体育与文旅、消费深度融合，形成“顶级赛事验证—基层场景普惠”的可推广模式。

对中国企业而言，世界杯既是展示窗口，更是战略机遇。当全球最严苛的赛场成为技术“试金石”，中国科技企业收获的不仅是掌声，更是打开全球高端市场大门的金钥匙。

一方面，赛事为相关技术提供了全球最高容错标准下的资质背书，顶级赛事的认证远比赛场广告更具长期商业价值，能撬动全球体育场馆、广电市场的订单；另一方面，赛事倒逼企业突破核心技术，在AI推理、边缘计算、智能传感等领域实现迭代，推动中国技术向中国标准跃升。

未来，以世界杯为新起点，中国科技企业可在三方面持续发力。

从赛事营销到生态深耕，将赛事经验转化为可持续的行业解决方案；从单兵作战到集群出海，链主企业可联合专精特新中小企业组建产业联合体，形成系统交付能力，避免单打独斗；从技术输出到规则共建，中国企业应积极参与国际体育科技标准制定，争取话语权，同时警惕地缘政治风险，以可信赖的技术伙伴形象赢得长期信任，在技术合作中注重数据安全与合规运营。

绿茵赛场总有终点，产业赛场永不落幕。对中国科技企业而言，真正的决赛不在美加墨的球场上，而在全球产业智能化升级的广阔天地中。唯有持续创新、深耕场景、共建生态，才能在这场没有终场的竞赛中，踢出属于中国科技的“世界波”。

本海报部分素材由AI生成

主管主办单位:陕西新华出版传媒集团有限责任公司 出版单位:陕西出版传媒集团报刊有限责任公司 本报地址:西安市高新区锦业一路10号中投国际大厦A座18楼 邮编:710065 联系电话:(029)89668717 89668179 81168500
全年订价:298.8元 广告许可证:陕工商广字01-013 制版:本报照排中心 印刷单位:西安蓝星新技术开发有限责任公司 地址:西安市新城区咸宁东路东方厂北门 电话:(029)82466577