

银行业AI安全开发应用指导意见出炉

AI竞速

随着大模型技术加速演进, AI正在重构全球产业格局, 银行业的转型浪潮亦奔涌而至。如今, “AI+”不再是银行的可选加分项, 而是成为决定其业务增长、行业位次的关键变量, 各大机构纷纷加速布局, 掀起一场覆盖产品、算力、生态的全方位竞速。

从产品层面来看, AI已跨越后台辅助, 直抵一线业务场景。近日, 招商银行面向AI及科技从业者推出运通工程师信用卡, 为满足该人群对于Token等AI资源的需求痛点, 首创将Token纳入新户礼, 成为国内首张搭载Token权益的信用卡。据了解, 新户达标后, 最高可享受每月18亿Token M3用量, 可直接用于文档、图像、音视频等多模态模型调用, 以及MaxClaw龙虾部署等AI高频场景。

在业务应用层面, 中国银行上海市分行近期探索推出基于大语言模型的“惠Chat”数字化普惠平台, 聚焦小微融资“最后一公里”堵点, 将AI能力嵌入信贷流程, 构建“政策大脑—企业画像—智能匹配”服务体系, 为一线客户经理减负增效。

事实上, 从战略层面来看, 2025年以来, 多家银行已将AI置于公司发展的核心位置。工商银行首次提出“数智工行”, 启动实施了“领航AI+”行动; 邮储银行面向各分行开放十大项24个通用AI能力, 形成“对外全域触达+对内全员提效”的邮储银行“AI 2 ALL”数字生态; 招商银行则提出“AI First”理念, 将AI置于“优先、领先、率先”地位; 浦发银行亦将AI能力建设提升至战略核心地位, 推动“懂数智、用数智”成为全行共识。

全面铺开的AI布局, 也着实为银行带来了实实在在的降本增效成果。以工商银行为例, 2025年其创新实施“领航AI+”行动, 在30余个业务领域落地超500个AI应用, AI数字员工承担工作量5.5万人年; 建设银行人工智能大模型技术已规模化赋能集团398个场景应用, AI助手覆盖率已经达到99.42%, 日均访问量已经超过10万人次; 招商银行落地183个领域专精模型和856个大模型应用场景, 累计替代人工时长超1556万小时, 约等于节省超8000名全职员工工作量。

人工智能(以下简称“AI”)正从银行业的“技术选项”变为“生存刚需”。从各大银行高管频频布局AI战略、行业AI招标持续加码, 再到接连推出AI创新产品——AI早已跨越工具属性, 成为驱动业务增长、重塑组织模式、改写行业格局的关键变量。

在行业高速发展的同时, 金融监管总局发布银行业保险业首份AI安全开发应用指导意见, 从治理架构、开发应用、数据治理等多个维度为金融机构AI发展拧紧“安全阀”。

展望未来, 或许正如兴业银行董事长吕家进所言, “AI时代下, 硅基生命将大量替代碳基生命的工作, 今后客户经理将不再区分公司、零售、同业等类型”。

苏商银行特约研究员武泽伟表示, 行业竞速AI背后折射三大转型趋势: 一是AI定位从辅助工具升级为核心生产要素, 全面渗透客户服务、风险管控、运营管理等全业务链条; 二是行业竞争逻辑从渠道比拼转向技术能力比拼, 技术代差正在拉大不同银行的经营差距; 三是AI应用从后台降本向前台创收延伸, 产品创新与场景拓展速度持续加快, 逐步形成技术驱动的增长新范式。

同步拧紧

回溯来看, 2024年, 开展“人工智能+”行动首次被写入政府工作报告, 随后AI在各领域加速落地。2025年3月, 政府工作报告提出持续推进“人工智能+”行动。在2026年政府工作报告中, 相关部署进一步升级, 要求深化拓展“人工智能+”, 提出“促进新一代智能终端和智能体加快推广, 推动重点行业领域人工智能商业化规模化应用”, 并同步强调要“完善人工智能治理”。

三年三提, 从布局到深化, 政策信号逐级加码。在此背景下, 金融监管总局于6月18日发布《关于银行业保险业人工智能安全开发

应用的指导意见》(以下简称《指导意见》), 从治理架构、开发应用、数据治理、算力建设、风险管理、能力提升、保障与监督等方面提出了32项指导性意见。这也是金融业首份系统性AI安全开发应用监管文件。

金融监管总局有关司局负责人在答记者问时表示, 《指导意见》旨在规范银行业保险业金融机构对人工智能的开发应用, 有效防控人工智能技术应用可能带来的风险, 推动数字金融高质量发展, 有序推进人工智能科技创新与金融业务深度融合, 引导金融领域人工智能应用朝着有益、安全、公平方向健康有序发展。

同时, 《指导意见》明确了四大原则: 一是坚持谁使用谁负责, 压实金融机构作为金融服务提供方、人工智能技术使用方的主体责任, 强化金融机构内部各环节工作责任落实, 明确人工智能开发应用各方分工和权责义务; 二是坚持自主可控, 持续提升人工智能相关技术、设备自主可控水平, 提高对业务经营发展有重大影响的关键平台、关键软硬件的自主研发能力, 加强信息技术应用创新适配; 三是坚持务实高效, 以提升业务价值为导向, 科学规划人工智能开发应用投入, 有效平衡成本与效益, 摒弃“为新而新、为用而用”的倾向, 推动人工智能切实服务经济高质量发展和金融业务高效运转; 四是坚持安全发展, 严格落实国家网络安全和信息化工作要求, 遵



守网络安全、数据安全各项法律法规制度, 强化技术安全和应用安全保障, 全面提升安全防护和应急处置能力。

在武泽伟看来, 首份AI安全开发应用指导意见, 恰逢行业AI应用加速普及的关键节点, 具有重要的规范与引导意义。《指导意见》填补了金融领域AI系统性监管的空白, 构建了覆盖全流程的监管框架, 标志着金融AI正式步入有规可依的规范化发展阶段。

“对于银行创新而言, 短期将提升合规门槛, 倒逼机构完善治理体系与风险防控机制, 遏制技术滥用与无序竞争。从行业生态看, 统一的监管标准有助于营造公平竞争环境, 保护金融消费者合法权益, 为AI技术的长期规模化应用筑牢安全底线, 推动行业从粗放式创新转向高质量可持续发展。”武泽伟补充表示。

如何合规布局AI

如果说《指导意见》划定了金融AI发展的“安全边界”, 那么具体到操作层面, 银行如何将合规要求转化为落地方案, 仍是待解的课题。

从文件本身来看, 《指导意见》对模型开发、数据治理及算力建设三大要素提出了系统性要求。在模型开发方面, 金融机构应定期开展对模型效能的测评分析, 构建数据闭环

反馈机制, 形成“数据—模型—应用”的迭代优化; 在数据治理方面, 要求金融机构要推动数据运营机制建设, 建立覆盖数据全生命周期的管理流程, 提升数据服务能力; 在智能算力建设方面, 金融机构应充分依托已有算力资源基础, 按照国家相关政策要求, 按需布局智能算力资源建设, 应用绿色低碳技术, 建设自主可控、安全高效的算力底座, 助力高水平科技自立自强。同时, 要加强对人工智能应用的运行监测, 实现对应用、模型、算力、网络的一体化管理, 保障人工智能应用安全可靠运行。

除三大核心要素外, 外包合作风险也被纳入重点监管范畴。《指导意见》明确, 使用外部人工智能技术时, 金融机构应在外包策略、数据安全、集中度管理等方面建立管理机制, 通过合同协议明确安全管理方面的权责义务, 确保金融机构能够有效管控相关风险。与外部企业开展合作时, 应建立有效的风险隔离“防火墙”, 防范风险跨业传递。对外包合作机构实行名单制管理, 对引入的外部模型建立严格的内部评估框架, 有效评价模型的优缺点和适配性。

对于上述要求, 中国企业资本联盟副理事长柏文喜表示, 《指导意见》对算力、数据体系等提出高标准约束, 行业分化趋势或将进一步凸显, 头部银行资源优势持续放大, 中小银行转型压力增加, 同时合规门槛也倒逼金融科技服务商升级产品安全标准。他建议, 银行需搭建专属AI数据质量规范, 破解数据孤岛、无效数据堆积难题, 全程严守客户隐私与数据安全红线; 在人才层面要兼顾算法技术团队与通晓金融业务、合规伦理的复合型人才培养, 实现技术研发与风险管控能力同步升级。

博通咨询首席分析师王蓬博建议, 银行应尽快建立覆盖董事会、高管层到业务条线的AI治理架构, 把风险管理嵌入开发全流程。在推动AI规模化应用时, 不能只看效率提升或成本下降, 更要评估可解释性、公平性和应急回退机制。从金融业历史发展来看, 安全与创新并非对立, 关键在于通过制度设计明确责任边界、技术标准和审计路径, 使AI真正成为可管、可控、可用的核心生产要素。

北京商报记者 孟凡霞 周义力

西街观察 Xijie observation

北京硬核创新的秘密

陶凤

以人形机器人、人工智能、医药健康三大硬核产业快速崛起为代表, 科创北京的名片越来越亮。在近期的“活力中国调研行”主题采访中, 以三大产业为主线, 大量创新案例组成典型坐标, 揭示了北京硬核创新的秘密。

三大产业共享了四大创新密码: 顶尖科研底座提供了最强大脑、头部企业带动构成了核心躯干、专业平台赋能意味着充沛的血液、真实场景落地则贡献了广阔的市场, 人才、企业、政策、市场循环耦合, 最终汇集成环环相扣的产业链条, 让北京的新质生产力加速从实验室走向产业化。

首先, 人形机器人与具身智能, 不仅是北京也是当下中国最具爆发力的赛道。北京的“机器人”不是单打独斗, 而是已经形成整机、算法、零部件、数据训练完整链条, 一批本土创新企业脱颖而出。

零售领域的熟练工种银河通用的Galbot G1, 已经在一些便利店常态化上岗。在工业与出海赛道上, 星岛纪元海外业务占据半壁江山。医疗“特种兵”罗森博特的骨折复位机器人, 凭借微创精准操作, 让具身智能真正助力医疗救治。配套企业同样技能出众, 无界动力专注机器人通用大脑与决策算法, 光轮智能搭建全流程仿真与数据采集平台。

一众企业快速迭代, 两大平台功不可没: 北京人形机器人创新中心, 专攻核心零部件中试、整机性能测试、关键技术攻关; 具身智能机器人数据与训练基地, 持续积累海量场景数据, 为整个人形机器人行业提供公共训练底座, 真正实现产学研用闭环提速。

人形机器人产业大爆发, 更离不开北京人工智能第一城深度孵化。AI时代, 北京不仅跑出了“大模型第一股”智谱, 还创生了新型研究机构智源研究院, 去做

那些“企业不愿做, 高校做不了”的事。明星企业、科研机构之外, 大量垂直类AI公司在行业内崭露头角。

智谱从清华园走向港交所, 实现了AI在资本市场的价值兑现, 智源研究院努力让世界模型走进真实物理状态。生数科技让几秒钟生成高清视频成为可能, 成为影视行业大规模落地的先锋。

在北京, 人工智能既有“高原”又有“高峰”, 更有完整的生态。产业原点之一就在中关村AI原点社区, 社区把校区、园区、街区深度融合, 集聚数百家人工智能科创企业。

不同于实验室里的技术演示, 北京用商业场景先行的打法, 让AI从代码中走出去, 落地成可触摸的服务与产品, 变成创造商业价值的“硅基打工仔”。在全球人工智能大浪淘沙的激烈筛选中, 凭借“人工智能第一城”的速度和执行力, 让真正有生命力的技术与企业沉淀下来, 也让AI真正沉下来。

北京的另一个产业高地来自医药健康。原始创新依旧来自顶级科研机构: 北京生命科学研究所、北京脑科学与类脑研究所, 持续产出世界级生命科学基础研究成果。

在产业转化端, 以昌平国际医疗器械城为代表, 向全社会搭建了一条完整的孵化、审批、量产、上市服务链条, 集聚大量创新器械企业, 形成从基础研究、前沿探索到临床应用、产业落地的完整生态, 持续领跑全国生物医药创新。

从人形机器人敢为人先, 到人工智能领跑全国, 再到“接住”医药健康原始创新, 北京的硬核创新不是单点突破, 也不是偶然爆发, 而是科研筑基、平台托举、企业争先、场景验证的系统性胜利, 是教育、人才、企业、政策合力的厚积薄发。

巨灾保险增厚灾害防御“安全垫”

巨灾保险作为现代应急管理体系的重要组成部分, 在完善社会灾害风险管理体系、服务国家防灾减灾战略、保障社会经济稳定发展方面发挥着越来越重要的作用。6月21日, 北京商报记者注意到, 近期多地完成了巨灾保险赔付。

近期, 四川省阿坝藏族羌族自治州若尔盖县举行城乡居民多灾因住宅巨灾保险现场赔付仪式。作为中国城乡居民地震巨灾保险共同体首席承保人, 人保财险阿坝州分公司代表共保体将总计296万元保险赔款全额支付给在“1·26”甘肃迭部5.5级地震中房屋受损的147户若尔盖县铁布镇农户。

黄山市也在近期举行了一场特别的赔付仪式, 因为前段时间连续强降雨, 人保财险黄山市分公司作为首席承保人, 把417.92万元的巨灾保险赔款交给了黄山市财政局。此外, 5月24日, 浙江省淳安县发布杭州今年首个暴雨红色预警。预警发布后仅数小时, 90万元巨灾保险赔款直达应急管理部门。

一笔笔直达基层的赔款, 成为灾后重建的“及时雨”。作为国家防灾减灾体系的市场化抓手之一, 各地巨灾保险试点正加速扩容, 持续增厚全社会灾害风险抵御的“安全垫”。

事实上, 经过多年试点, 我国巨灾保险发展已迈入加速提质的全新阶段。自2014年宁波、深圳率先开启巨灾保险试点以来, 我国巨灾保险保障体系初步搭建并持续完善, 保障范围从最初单一的地震灾害, 逐步拓展至台风、洪水、滑坡等多类常见自然灾害, 全方位提升了全社会整体抗风险能力。行业数据显示, 截至目前, 我国巨灾保险试点项目已覆盖20多个省市, 2025年, 累计为全国7489万户次居民提供33.71万亿元巨灾风险保障。

在苏商银行特约研究员付一夫看来, 巨灾保险在政府应急救灾中发挥了重要的缓冲作用。付一夫指出, 一方面, 它能快速提供灾后补偿资金, 如阿坝州案例中及时赔付农户房屋损失, 减轻受灾群众经济负担; 另一方面, 它

分担了政府的财政压力, 使救灾资源可以更高效地配置, 同时通过市场化机制促进全社会风险意识提升。

经过十余年试点深耕, 我国巨灾保险体系逐步成型, 有效提升了全社会防灾抗灾的整体能力。但是其作为自然灾害补偿机制中的重要途径, 当前的渗透率和覆盖率不高, 经济损失承担比例远低于全球平均水平。

北京商报记者了解到, 欧美地区巨灾保险赔付比例可达40%—60%, 亚洲地区平均约为27%, 我国平均不到10%, 灾害补偿以政府财政兜底为主, 巨灾保险的保障缺口依然较大, 发展中仍有诸多不足之处。

对于行业现存瓶颈, 付一夫表示, 一方面, 产品设计单一, 覆盖场景和触发条件有限, 财政支持与激励机制尚不完善, 部分地区保费补贴不足; 另一方面, 巨灾风险分散渠道有限, 再保险市场及巨灾债券等工具运用仍处于起步阶段。

业内普遍认为, 巨灾保险与重大灾害和防灾减灾工作有着天然联系, 应逐步推动巨灾保险制度与国家灾害治理体系的融合发展, 引导商业保险公司参与国家灾害治理体系。从顶层设计层面, 付一夫建议, 我国应逐步构建“政府+市场+社会”的巨灾保险体系, 强化风险分担机制和公众教育。完善顶层立法, 明确巨灾保险的法定地位和强制参保范围; 建立国家巨灾风险数据库, 为定价和产品创新提供支撑; 推广“多灾因”综合保险模式, 扩大覆盖范围。

在产品精细化创新层面, 业内专家提到, 可推广实施差异化保费设计, 按区域风险等级(如洪水重现期、地震烈度)划分费率, 可参考德国洪水险1—4级风险定价机制, 高风险区(如珠江三角洲、强地震带等)采用“高保费+高保障”, 低风险区灵活调整; 此外, 可推广参数化巨灾保险, 沿海地区或洪涝灾害易发地区, 可以参考广东试点的“台风指数保险”(以风速、降雨量为赔付依据), 在农业、旅游业等领域开发“旱灾指数险”“滑坡指数险”等保险产品, 实现“灾害发生即赔付”, 缩短理赔周期, 为灾后重建、复工复产提供效率支撑。

北京商报记者 李秀梅