中国经营报/2023 年/8 月/21 日/第 B01 版
金融

银行试水生成式 AI　数据合规治理迎考

本报记者　郝亚娟　张荣旺

自 ChatGPT 问世以来，银行纷纷加大生成式人工智能（以下简称“ 生成式 AI ”）的布局，并将其视为转型的突破口。

近日，波士顿咨询公司发布《银行业生成式 AI 应用报告(2023)》（以下简称《报告》）指出，生成式 AI 将为银行业带来巨大变革。目前，银行业具备由点及面推进生成式 AI 应用的三大条件，即扎实的数字化基础、完备的技术能力和多元丰富的数据。

值得一提的是，自今年 8 月 15 日起，《生成式人工智能服务管理暂行办法》（以下简称《办法》）施行，对于加强银行业使用生成式 AI 的监管起到重要作用。

分析人士指出，金融业作为数据密集型行业，数据安全保护将直接关系到投资者的个人隐私和财产安全。因此，银行在积极应用生成式 AI 的过程中，数据安全与隐私保护、数据质量控制、应用合规将成为银行必须解决的课题。

贯穿银行前中后台

超个性化内容、更具吸引力的客户体验、更好的洞察力……目前，已有多家银行将生成式 AI 应用到智能投研、智能理财场景中。

《报告》指出，生成式 AI 在银行业的应用场景可贯穿前中后台各个环节，包括市场和销售、渠道和运营、产品开发、投顾服务、客户服务以及风险合规等方面。银行的每条业务线、每个职能，都有可能找到生成式 AI 的应用场景。

《报告》显示，生成式 AI 在银行业的应用，从价值创造逻辑上可分为两大类：一是替代人工。生成式 AI 可以开展大量重复性较高、简单基础的任务，如处理文本的要素提取、处理进件、识别异常项、生成基础数据分析、生成标准化内容等，从而释放运营类人力资源，实现降本增效。二是赋能人工。利用生成式 AI 的“ 对话 ”和“ 创造 ”能力，可让 AI 成为助手，有效放大关键节点的“ 人 ”的产能，尤其是客户经理、财富顾问、产品经理、投研经理、信审经理、市场营销人员、编程开发人员等角色，赋能不仅体现在专业内容的形成上，还可能体现在基础管理环节。

交通银行党委委员、副行长钱斌在 2023 世界人工智能大会上指出，近些年，生成式 AI 在智能客服、智慧营销、智能风控等领域都取得了不错成绩，有助于解决包括金融发展不平衡、不充分的结构性问题，数据要素向数据资产转化的问题、金融科技人才短缺的问题，以及客户体验、运营效率和风险防控等经营效能提升。目前，包括交通银行在内的部分大型金融机构已在积极布局，推动实现商业价值。

钱斌举例指出，生成式 AI 将变革人机交互方式，赋能差异化的产品和服务创新，促进实现从人性化、个性化到感性化的体验升级。比如，在精准营销方面，借助生成式大模型，在灌注专业领域知识后，一方面提升行业洞察能力；另一方面将更为精准地解读个体个性化需求，帮助实现从理解“ 客群 ”到理解“ 客户 ”的跨越，提升客户服务精准度和满意度。在智能客服方面，生成式 AI 在准确理解人类意图，进行流畅、自然、高质量的对话方面具有优势，甚至能够体现出一定的共情能力，结合文档理解分析和生成能力，人机交互的体验和效率将有望出现质的飞跃。

冰鉴科技研究院研究员王诗强在接受《中国经营报》记者采访时表示，目前银行存在大量沉睡客户，主要是银行对这类客户知之甚少，即使通过电话、短信等与客户进行过沟通，但相关的沟通信息未经过深度分析，导致客户转化率较低。银行应该加大人工客服人员和数据标准人员招聘，并通过生成式 AI 对了解到的客户信息进行重新标注、分类、整理，以便向客户提供高质量

服务。

生成式 AI 如何更安全？

生成式 AI 加速发展，在不断催生新场景、新业态、新模式和新市场的同时，也暴露出一定的安全风险。

钱斌也指出，数据少、质量差和处理能力弱，限制了人工智能的应用场景，降低了人工智能大模型的“智商”。前期，金融业虽然已经积累了大量数据和数据处理经验，但相对于大模型需要的数据量、知识密度和处理质量来说，还远远不够。目前，互联网中文数据相比英文数据还非常少，开源语料库有限，数据质量参差不齐，细分到金融领域的专业数据和公共数据更加不足。同时，由于金融制度的差异，无法完全照搬国外的金融语料、金融知识，而金融服务的专业性、精准性又对人工智能技术的效果和可信度提出了非常高的要求。因此，相关应用在丰富数据种类、强化数据治理、提升数据质量、保障数据安全、完善数据共享机制等方面仍任重道远。

德勤中国金融服务业风险咨询合伙人蔡帼娅在接受记者采访时指出，数据安全与隐私保护、数据质量控制、应用合规、以及新的风险管理是银行应用生成式 AI 面临的挑战。

在数据安全和隐私方面，银行业涉及大量的客户敏感信息，如客户的个人信息、交易记录等。银行数据的安全等级分类标签及应用范围需要足够清晰，确保生成式 AI 在学习和生成过程中，数据的安全和用户的隐私得到充分保护。如果不慎泄露，可能会导致重大的经济损失和声誉损害。

在数据质量控制方面，生成式 AI 的效果和准确性在很大程度上依赖于数据质量。在德勤全球研究中已经提出，“人工智能系统的好坏最终取决于它们所获得的数据，不完整或不具代表性的数据集可能会限制人工智能的客观性。”银行需要对关键数据进行必要的检核，并持续落地数据质量闭环监控，提高数据的准确性和完整性。当然，这个过程也可使用 AI 技术促进数据质量的自我修复。

在应用合规方面，银行业属于强监管的行业，过去银行每一个新产品、新服务都有人工审查的成分确保合规性。而在生成式 AI 中，因为缺少及时的人工审查和纠偏，训练环节产生任何偏见都有可能会使后续生成式 AI 将偏见循环持续下去。例如 AI 生成的贷款决策、投资建议，都有可能倾向于特定群体，这可能会触及不正当竞争法、消费者权益保护法等。银行可能会面临潜在的罚款、诉讼甚至吊销执照等严重后果。银行可以考虑应用模型解释和可视化工具，对生成式 AI 的决策过程进行解释和可视化，提高模型的透明度和解释性。同时，需要建立内部审核和监督机制，确保模型的公平性和合规性。

针对生成式 AI 可能存在的风险，《办法》通过完善监管框架，规范银行应用人工智能技术，加强对银行业使用生成式 AI 的监管，确保其符合相关法律法规和行业标准，保障金融市场的稳定和安全，促进其健康发展。

与此同时，监管部门也尤其重视数据安全管理。今年 7 月 24 日，中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》，包括数据分类分级、数据安全保护总体要求、数据安全保护管理措施、数据安全保护技术措施、风险监测评估审计与事件处置措施、法律责任等内容。

“在合规数据治理方面，银行等金融机构首先应该参考国家发改委、教育部、科技部等七部门联合发布的《办法》。其次，监管部门发布的《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等重要法律法规也值得重点参考。”王诗强指出。

蔡帼娅建议，银行业为提升生成式 AI 技术应用的合法合规性，完善合规数据治理，可以采取以下措施：一是建立合规数据治理框架，制定明确的合规数据治理政策和流程，包括数据收集、存储、使用和共享的规范和控制要求，并建立数据管理团队，负责数据隐私保护和合规性的监督和管理；加强数据安全和隐私保护：二是加强数据安全和隐私保护措施，包括数据加密、访问控制、数据脱敏等技术手段的应用；三是提高数据质量，建立数据质量管理机制，定期对数据进行清理和校验，以保证数据的准确性和完整性；四是建立模型风险管理机制，包括模型的开发和验

证、模型的监测和更新等环节，并建立模型风险管理团队，负责对生成式 AI 模型的风险评估和监测，及时发现和应对模型的风险和漏洞；五是加强合规培训，定期对员工进行数据合规的培训，以确保员工了解并遵守所有的数据合规要求，全面提高员工的合规意识和能力。