等待监管划“红线”

金融行业新一轮没有硝烟的战争，落在了大模型上。

从“百模大战”到“千模大战”，大模型在2023年如雨后春笋般冒出，又在经历市场探索后从通用大模型涌向了面向垂直领域的产业大模型。期间，金融行业成为了大模型落地的主战场。

而金融行业所独有的行业属性和监管要求，也让大模型在应用的前置环节迎来了约束。从隐私数据到科技伦理，监管划出的红线让大模型在合规审慎的框架内有序发展。与此同时，政策准入打消了从业机构在场景布局方面的顾虑，也让从业机构主动将风险防控与合规写入大模型的发展脉络，大模型的潜力与价值在金融领域得到了更为具体的展现。

监管框架正成型 >>>

近年来科技创新快速发展，科技创新在各类新业态应用后爆发的安全风险受到各国监管部门的关注。过去五年间，我国与科技创新相关的监管框架不断完善，科技伦理治理成为重要一环。

2022年3月，中共中央办公厅、国务院办公厅印发《关于加强科技伦理治理的意见》，提出强化科技伦理审查和监管。随后，人民银行于同年10月正式发布并实施《金融领域科技伦理指引》（以下简称《指引》）。

《指引》明确提出金融科技的定义为“技术驱动的金融创新”，强调金融科技的本质是金融，杜绝以“科技创新”的名义模糊业务边界、交叉嵌套关系、实施无证经营或超范围经营等行为。

另一方面，进入2023年后，大模型概念愈演愈烈，聚焦在人工智能本身的监管体系开始明确。7月13日，《生成式人工智能服务管理暂行办法》正式发布，同时明确了网络安全、数据安全、个人信息保护等法律文件作为上位法，对生成式人工智能提出包容审慎和分类分级监管原则，并在内容标识、安全评估手续等方面进行了更完善的补充管理。

10月8日，科技部联合十部门印发《科技伦理审查办法(试行)》，成为科技伦理风险防控与创新风险治理的准则。同期有市场消息指出，人民银行正在指导制定一项关于金融领域人工智能应用风险治理的推荐性行业标准。根据介绍，该标准将为金融行业人工智能系统应用的风险识别与防控，以及系统升级、实现、验证、测试、管理提供依据。

复旦大学金融科技研究院院长柴洪峰认为，金融数据和垂直领域大模型密切相关，存在数据安全、大模型安全可信和伦理等问题。同时金融领域也涉及敏感信息和决策，对于金融大模型的监管必不可少。

安全合规是发展前提 >>>

大模型的价值绝不在于纸上谈兵，最终还是要落在具体的场景应用中。大模型适用的场景中，市场纷纷将目光投向了金融领域。一方面金融行业本身具备丰富的业务场景，对于人工智能应用要求高、需求高；另一方面大模型应用离不开数据、算法的支撑，金融行业复杂而专业的知识体系也为金融大模型的应用提供了沃土。

在蚂蚁集团财富保险事业群架构师赖永兴看来，金融是一个专业性高、逻辑严谨、重风险，合规性和可靠性要求高的行业，在金融业务中，严格的合规要求和法律法规的遵守至关重要。同时需要全面考虑市场、信用、操作等各种风险因素，并制定有效的风险管理策略。基于前述特点，大模型落地金融产业是一项复杂的系统工程。

思则生变，从大模型领域参与主体的视角出发，各类参与机构已开始关注大模型的合规发展。与大模型相关的讨论中，“合规”是高频出现的词汇之一。度小满CTO许冬亮曾提到，金融是强监管行业，安全合规是大模型落地的前提条件和重要保障。金融大模型安全合规既需要监管政策的约束，更需要大模型企业自身的主动作为。

马上消费金融CTO蒋宁也曾提出，当前金融大模型在应用规范方面缺少100%符合监管要求的客观标准和评价体系，希望与协会、监管单位共同努力，推进金融大模型在落地过程中所需要的一些客观能力的评价和标准。

透过受访企业提供的信息不难发现，大模型已然成为竞争的新赛道，互联网公司、科技公司、金融机构等市场主体均已“起跑”。而安全监管与运维是相关机构发力大模型的重要环节，例如奇富科技通过数据脱敏处理和隐私计算，在保障安全使用数据的同时最大程度挖掘数据价值。

加强审查和风险评估 >>>

于大模型而言，金融行业是机会，也是挑战。当尚未完全成熟的大模型遇上强监管的金融行业，金融大模型作为金融创新应用展现形式，不可避免地在安全隐私等方面受到考验。

对于大模型在金融领域的应用，有大模型行业从业人员向北京商报记者表示，大模型还处于发展早期阶段，随着后续技术的不断升级迭代，大模型应用场景将更为丰富，对应的合规要求必然也会更为细化。

经济学家余丰慧直言，金融是强监管行业，安全合规是大模型落地的前提条件和重要保障。如何通过大模型技术强化金融机构的风险管理和内控体系建设，确保交易场景的可控和稳健经营是当前金融行业面临的重要问题。

“金融机构在应用大模型技术时，需要充分考虑数据的质量和可靠性，建立完善的数据管理和治理机制，确保模型的准确性和稳定性。同时，金融机构还需要加强对大模型技术的监管和审计，建立健全的内部控制体系，确保大模型技术的应用符合监管要求和合规标准。”余丰慧补充道。

围绕金融大模型监管，柴洪峰建议，建立监管框架与标准，确保大模型在金融领域的应用符合法规与道德要求，通过政产学研的合作制定相关的政策和指南。对于金融大模型的部署与使用，需要协同共治，提升透明度，保证数据质量和可解释性的机制。这可以帮助用户与监管机构理解模型的决策依据，并确保其不带有偏见或歧视性。同时，监管机构还应加强对金融大模型的审查和风险评估，对于关键人物和系统，应建立审查和测试的机制，确保其性能和安全性。