VOICE OF AMAC

（2022 年第 1 期，总第 168 期）

中国证券投资基金业协会　　2022 年 1 月 9 日

市场中介机构和资产管理机构使用人工智能和机器学习技术情况、潜在风险、应对措施及监管建议

【编者按】随着人工智能（Artificial Intelligence，以下简称 AI）和机器学习（Machine Learning，以下简称 ML）技术的发展，金融行业越来越多的市场中介机构（Market Intermediaries）和资产管理机构（Asset Managers）（两类机构以下统称公司）开始应用这些技术降低运行成本、提升利润率以及为投资者提供更高效的服务。然而，使用这些技术也可能创造或放大某些风险，并对整个金融市场的效率产生影响，最终损害投资者利益，因此如何在金融市场中应用 AI 和 ML 技术已成为全球监管机构的关注焦点。2021 年 9 月，国际证监会组织（IOSCO）发布了《市场中介机构和资产管理机构使用人工智能和机器学习技术情况》的最终报告，对公司使用 AI 和 ML 情况、潜在风险、公司面对潜在风险的应对措施进行调研，并向各辖区监管机构提出建议。

一、市场中介机构和资产管理机构使用 AI 和 ML 情况

（一）AI 和 ML 的定义

AI 由数据科学家约翰·麦卡锡（John McCarthy）于 1956 年提出，定义为“制造智能机器的科学和工程”，通过使计算机模仿人类的学习、推理、规划、感知和语言理解能力，从而做出决策、解决问题。目前 AI 在金融服务行业的应用仍处于早期阶段。

ML 可以看做是 AI 的子项和具体应用，指通过计算机程序的开发，使机器无需再有明确的程序就可以通过既往经验进行自主学习，根据人为干预程度的不同，分为监督学习[1]（Supervised Learning）、非监督学习[2]（Unsupervised Learning）和强化学习[3]（Reinforcement Learning）三类。

（二）AI 和 ML 的应用场景

1、市场中介机构应用场景。一是提供咨询和客户服务。机器人投顾服务或自动化投顾服务是其代表，通常使用演绎推理算法，某些服务还开始使用预测性的算法。在使用技术提供咨询服务时，通常仍设有人工干预流程。如果投资顾问认为技术生成的建议较为恰当且符合客户需求时，就会推荐该建议。**二是进行风险管理。**AI 和 ML 技术在风险管理方面的应用主要是使用数据对风险敞口进行定价和管理，包括信贷风险、市场风险、运营风险和流动性风险。市场中介机构利用基于技术的风险管理系统进行风险监控、识别和评估。

---

[1] 监督学习（Supervised Learning）：指向算法提供一组被标记分类的初始数据，基于这组初始数据集进行训练，算法可以学会分类规则并对数据集里其他的数据进行预测分类。

[2] 非监督学习（Unsupervised Learning）：指算法通过观察找出具有相似特征的数据组并判断其形态特征，使算法独立地找出数据的结构特征。

[3] 强化学习（Reinforcement Learning）：指向算法提供一组未被标记分类的初始数据，然后命令算法去识别并分组具有相似特性的数据。当算法对具体的数据做出选择时，它会收到相关反馈以帮助它学习。

三是客户识别及监测。AI 和 ML 技术使得市场中介机构可以将对客户登录、欺诈识别、洗钱和网络攻击各环节的监控自动化，如在客户登录时进行了解客户（Know Your Customer）的例行检查。此外，AI 和 ML 技术还可以根据制裁清单对客户和交易进行筛选和监控，察觉潜在的洗钱、恐怖主义融资和其他金融犯罪证据。**四是选择交易算法。**市场中介机构通过为客户提供软件解决方案对历史交易情况和产品表现进行分类，预测不同交易策略的表现并提出具体的交易建议，从而使工作人员专注于更为复杂的研究工作。

2、资产管理机构应用场景。资产管理机构对于 AI 和 ML 技术的应用正处于萌芽阶段，主要用于辅助人工决策。**一是提升内部研究能力。**为了取得竞争优势，某些在传统上注重基础研究能力的主动管理型资产管理机构开始通过利用多样化的数据来扩展其量化分析方式，如利用对社交媒体数据、地理空间数据的分析提升内部研究能力。**二是优化投资组合管理。**某些资产管理机构开始应用 AI 和 ML 技术进行资产分配和定价，例如通过发现数据之间的相互关系来创造新的交易想法（被称为“阿尔法信号”，Alpha Signals），或根据历史价格和当前的趋势来预测未来资产价格。**三是将技术应用于合规性检查、交易代理服务和客户服务。**如某些资管机构通过风险管理和合规审查流程的自动化，跟踪个别投资组合经理的行为，自动生成交易执行质量报告和评估市场流动性风险。

二、应用 AI 和 ML 技术的潜在风险

（一）公司内部治理和监督审查问题

IOSCO 调研显示，许多已应用 AI 和 ML 技术的公司并未将其视为与传统方式有根本区别的技术。大多数公司仍然依靠现有的内部治理及监督审查流程来批准、开发和使用，只有少数公司认为需要引入新的风控程序或是修订现有的风控程序专门管理 AI 和 ML 技术的使用风险。同时，风控和合规管理部门的参与往往集中在 AI 和 ML 技术的开发和测试阶段，而不是应用该技术的整个生命周期。技术一旦投入使用，部分公司主要依靠技术的使用部门进行监控。此外，行业对承担最终责任的公司高级管理层以及负责风险管理和监督的专业人员是否必须具备相关技术专长尚未达成共识，大多数公司表示尚未聘请具备技术背景的合规人员。

（二）技术的开发、测试和长期监控问题

目前大多数公司都没有专门针对 AI 和 ML 技术的整体开发和测试框架。在开发过程中，如果有过多的“噪声”数据（Noisy Data），可能会导致算法失灵。稳健的开发和测试控制对于区分有统计意义的数据与“噪声”数据非常必要。因此在 AI 和 ML 技术应用的整个周期中都应进行持续监控，确保不会由于运行条件的微小变化或噪声数据而影响技术表现水平。

（三）数据质量和数据偏见问题

AI 和 ML 技术的表现水平根本上取决于建模时输入的数据质量，公司能否获取足够大的数据集来训练应用程序（特别是与投资决策相关的数据）以及如何保证数据质量都是关

键风险。另一个风险是数据本身的有限性。如当技术模型基于年轻客户群体非常有限的投资交易记录展开行为分析，分析结果可能出现偏差。此外，在应用 AI 和 ML 技术前对数据进行清理可以降低“噪声”并提升技术表现水平，但由于数据清理本身涉及主观判断，可能会在无意中引入其他偏见成分。

（四）技术的可解释性和透明度问题

一方面，公司要想有效地应用 AI 和 ML 技术，就必须保证其算法不仅准确，而且能够被公司内部一线业务人员及合规人员、市场交易对手、投资者以及监管机构所理解。如公司应用了难以理解的算法技术来改善交易策略，可能使公司面临巨大法律风险和监管风险。但技术模型的可解释性或可理解性是一个极具挑战的问题，一些 ML 模型以“黑箱”（Black Box）方式运作，模型背后的逻辑清晰度有限，如在“无监督深度学习”（Deep Unsupervised Learning）的算法中，由模型做出的决策就有可能导致缺乏相关技术知识的普通人无法理解。另一方面，虽然公司可以通过对于技术模型的详细解释提升透明度，从而增强利益相关方对技术的理解和信心，但对于披露内容尚未达成共识，如披露需涵盖公司应用 AI 和 ML 技术的全流程还是侧重于与投资决策有关的流程？对监管机构、交易对手以及不同的客户类型（机构客户和零售客户）的披露内容是否应有所不同？此外，部分公司还担心过多的透明度可能给个人非法利用或操纵该技术创造机会。

（五）过度依赖第三方服务商的问题

由于 AI 和 ML 技术依赖于大型的数据集及计算资源，第三方服务商有可能提供更便宜、更全面的技术解决方案，已有越来越多的公司利用第三方服务商提供的服务，特别是规模较小的公司更倾向于寻求外部技术解决方案。同时，许多公司不仅使用供应商提供的服务，还会使用其提供的数据库和云计算技术。这种趋势不仅会引发业务过度集中于某些服务商的风险，而且当公司并不具备足够的专业技能对服务提供商进行有效的尽职调查评估时还可能产生数据隐私泄露、网络安全和运营风险。

（六）道德伦理问题

2008 年金融危机以来，市场参与者的道德约束力和诚信情况得到了越来越多的重视。在 AI 和 ML 技术领域，如果算法模型缺乏全面数据清理和数据匿名化过程，有可能演化出社会偏见，给出不良投资建议，引发道德伦理问题，尤其是与多样性和包容性相关的问题。如当市场参与者大量使用非传统数据集（如卫星数据或是社交媒体数据）来开发 AI 和 ML 算法模型，能否确保所开发的模型不会对某一类人群产生歧视，能否确保产生的决策是公平和无偏见的。目前 IOSCO 金融科技网络（Fintech Network）已将机器人顾问服务认定为一种具有潜在重大道德伦理影响的技术应用。

三、公司对潜在风险的应对措施及监管建议

（一）公司对潜在风险的应对措施

一是有限使用 AI 和 ML 技术。目前大多数司法辖区仅有针对公司整体制度和风控的监管要求，没有专门针对 AI

和 ML 技术的监管要求，且不是所有的技术都与现有监管要求相兼容。面对尚未完备的监管体系，一些公司表示在完全有能力遵守所在司法辖区的法律法规前不会使用或仅会有限使用 AI 和 ML 技术，以应对潜在的监管风险。

二是倡导公司文化。公司高层可以通过公司内部激励机制和行为管理来创造和形成良好的公司文化，以减少不当行为对投资者造成的损害，其中道德伦理是关键要素，如诚实、公平、勤勉尽责、关心和尊重他人。

三是建立问责制度。问责制旨在通过让从业者对其行为负责来减轻对投资者的损害并强化市场诚信。随着 AI 和 ML 技术的应用，问责对象从公司高级管理人员扩展到数据分析师、数据科学家和数据工程师等岗位。

四是选聘专业员工。很多公司已将技术知识和专业技能纳入招聘员工的考量范围，知识和技能也涵盖了良好的道德行为标准。

五是增强抗风险能力。许多公司在应用 AI 和 ML 技术时将公司运营中的抗风险能力列为首要关注的问题，对第三方服务商的尽职调查和监督审查是其控制风险的关键一环。

六是实施差异化信息披露。依据投资者类型和专业程度进行不同程度的信息披露，核心目的是使投资者感受到公司是基于投资者的最佳利益来开发和使用新技术的。

（二）监管建议

一是监管机构可考虑要求公司高级管理层对 AI 和 ML 技术的开发、测试、部署、监控和风控过程监督负责。具体包括制定内部治理框架、明确高级管理层的问责制度。公司

还应指定一名或一组具有相关专业技能和知识的高级管理人员负责该技术的初期部署和后期的实质性更新。

二是监管机构可考虑要求公司持续性地对 AI 和 ML 技术进行测试并监控以验证其结果。公司在部署 AI 和 ML 技术前应在一个与日常业务环境相隔离的环境下进行测试，以确保该技术在不同市场环境下的运行能力均能达到预期水平且符合监管要求。

三是监管机构可考虑要求公司相关员工具备足够的技能和专业知识。足够的技能和专业知识是开发、测试、部署、监控和监督审查公司使用 AI 和 ML 技术的基础，如合规部门和风险管理部门应能够理解和质疑技术生成的算法，并对第三方服务提供商开展尽职调查。

四是监管机构可考虑要求公司了解其对第三方服务提供商的依赖程度，有效地管理和审查与服务商的业务关系。为确保充分的追责能力，公司应与第三方服务商签订具备明确服务要求的协议，约定外包职能的范围和服务提供商应承担的责任。

五是监管机构可考虑要求公司对使用 AI 和 ML 技术进行有效的信息披露。例如向投资者披露公司在使用 AI 和 ML 技术时对客户利益产生的实质影响以及向监管机构披露是否符合监管要求。

六是监管机构可考虑要求公司建立适当的控制体系确保数据质量，使技术应用有稳健的数据基础。公司应建立适当的流程和控制体系，核查所使用的数据源的质量，确保所使用的数据集就目标人群而言有足够的代表性。

【本文摘译自国际证监会组织（IOSCO）于 2021 年 9 月发布的《市场中介机构和资产管理机构使用人工智能和机器学习技术情况》最终报告，由中国证券投资基金业协会王紫祺、张蔚然、胡刚伟审校译稿】