汉坤法律评述
2023 年 8 月 17 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

创新不离守正 — 生成式人工智能对基金管理公司的影响探析

作者：毛慧 | 解石坡 | 唐晓诚[1]

一、导言

自 2022 年 11 月 ChatGPT 横空出世，采用大语言模型的生成式人工智能源源不断地进入大众视野。本质上，ChatGPT 通过大量的文本材料习得自然语言，并对输入语言即时回应，以实现交互对话。除人工智能研发公司竞相发布、更新同类产品外，国内外各行各业也都关注着其应用场景及行业适配度。着眼公募基金行业，作为传统的强监管行业，人工智能将会被其拒之门外还是为其赋能，以及人工智能技术对基金管理公司的日常运营及合规管理将会产生何种影响，这些都是值得我们深入研究的问题。

本文将从业务开展和公司管理的视角出发，针对在本轮技术浪潮中基金管理公司的应对策略进行深入探讨，以期抛砖引玉，为行业更深入的思考提供抓手。

二、基金管理公司具体应用场景

（一）投资决策支持

生成式人工智能作为基金管理公司在投资决策中的重要辅助工具，其应用主要体现在投资策略优化和量化投资两方面。

- 投资策略优化：在投资策略决策中，生成式人工智能通过对大量的历史投资数据进行深度学习，从而识别并学习历史投资行为，生成更为精准的预测模型。基金管理公司可以应用生成式人工智能进行模型训练，利用历史数据学习证券价格的波动规律，预测未来的市场走势，为投资决策提供科学依据。不同于人类投资者的有限理性，生成式人工智能在面对市场的复杂性和不确定性时，能够在各种潜在的投资策略中选择最优解，增强收益预测的准确性。

- 量化投资：在量化投资方面，生成式人工智能可以利用其强大的数据处理和分析能力，对大量金融市场数据进行高速、准确的处理和分析，辅助投资人员制定出更为科学的投资策略。通过自然语言处理、情感分析等技术，生成式人工智能能够从各类新闻、报告、社交媒体信息等非结构化数据中提取有价值的信息，为量化投资提供更丰富的维度，从而提升投资决策的全面性和精准性。

  生成式人工智能在资产管理领域进步显著，行业内已展开独立 AI 基金经理、AI 交易员等应用场景

[1] 张一明、左昭阳对本文的写作亦有贡献。

的探索。目前，国内已有基金管理公司与某研究院跨界联合、将 AI 和投资相结合的实例。然而，就独立 AI 基金经理而言，当前其仍处于探索阶段，尚无法完全实现落地应用。今年 5 月，一家英国个人理财网站 Finder 发布题为《由 ChatGPT 创建的投资基金击败了英国十大最受欢迎的基金》的文章。文章称，Finder 网站此前选取了英国排名靠前的前十只基金，并要求 ChatGPT 从这些基金投资的股票中选取超过三十只股票建立一只模拟基金。ChatGPT 最终选出了 38 只股票并由此组建成立一只 AI 推荐基金，Finder 网站根据 ChatGPT 提供的投资组合跟踪这只 AI 推荐基金，并将其与十只英国领先基金进行比较。截至 4 月 28 日，该只模拟基金的收益率高于排名前十的基金的平均水平。此外，在 6 月 1 日，国内某私募基金公司公告称，其拟安排一个基于人工智能的机器人管理基金，并由一名员工监督。上述事件一时引发行业热议，对 AI 基金经理的探索也引发了一系列问题。其中，最直接的问题是，AI 是否能够取代基金经理？除 AI 基金经理的人格化问题之外，我们就 AI 基金经理实际落地的可操作性还评估得出如下问题，这些问题导致 AI 基金经理目前仍仅是一种设想。

首先，黑箱算法存在不可知性。生成式人工智能通过智能算法生成投资建议，但由于其“自动性”和“智能性”，我们暂时难以获取其生成结果的算法过程和依据，这对投资建议的合法性和可靠性提出了质疑。此外，投资决策过程的留痕问题仍是目前 AI 基金经理落地实施有待解决的问题。

其次，以 ChatGPT 的使用政策为例，其明确提到，在缺少具有资质的相关人员审核信息的情况下，不得使用模型提供定制财务建议。类似的限制在其他生成式人工智能的使用政策中亦有体现。显然，对基金管理公司而言，这一条款至少意味着在合同约定的层面限制了生成文字的用途，使用者不得将此类生成式人工智能输出的文字用作独立的资产管理建议。

（二）运营管理

基金管理公司还可能将生成式人工智能融入公司的日常运营，尤其是在数据处理、客户服务与投资者教育以及交易执行等方面。

- 数据处理：基金管理公司在日常运营中会产生海量的数据，包括但不限于投资数据、市场数据、客户数据等。生成式人工智能通过利用深度学习等技术，可以提高数据处理的效率和准确性，并将这些数据转化为对基金管理公司有价值的信息。例如，通过生成式人工智能处理投资数据，基金管理公司能够实时了解基金的收益情况、风险水平等关键信息，为管理决策提供数据支持。同时，大语言模型能够有效应用于重复性、机械性工作。此前，此类工作往往由公司员工或自动化软件进行，而这两种处理方式各有利弊。由公司员工处理的方式面临效率不高、准确性不高的问题，自动化软件处理则面临机动性与智能化不足的问题。而大语言模型的出现恰恰能弥合上述两方面缺陷，一方面能有效解决因人为操作导致的误差问题；另一方面，基于智能学习和深度学习算法，其又能弥补自动化软件机动性和智能化不足的缺陷。

- 客户服务与投资者教育：在客户服务方面，生成式人工智能可以通过聊天机器人等应用提供 24 小时的客户服务，极大提升客户的体验感和满意度。目前，一些基金管理公司已经开始使用基于生成式人工智能的客服机器人，解答投资者的各类问题，提供个性化的服务，以提高客户满意度。与此同时，大语言模型的优点之一在于可以通过与使用者的互动以及使用者提供的信息和数据，形成针对用户自身的模型，并根据用户的个人需求和偏好提供个性化的服务。若能够确保初始训练数据的准确性与适当性，基金管理公司则能够将大语言模型运用于投资者教育板块，与现有的投资者教育渠道相辅相成。

- 交易执行：在交易执行阶段，AI 交易员的角色也不容忽视。作为 AI 技术的一个重要应用，AI 交

易员能够利用 AI 技术，通过识别和提取关键要素以及理解上下文逻辑，实时把握深层次的意图，快速获取对手方意图并主动发问。同时，AI 交易员能够通过智能化的方式进行询价和议价，完成询价需求的采集，并将询价状态实时反馈，获取并反馈最终匹配交易结果，进而与对手方确认后完成交易。此外，AI 交易员还能根据与对手方交流获得的信息，进行个性化布局，实现相应的风险控制策略。这种先进的交易方式大大提升了交易效率，进一步推动了基金管理公司在交易执行领域的创新。近期，国内已有基金管理公司将人工智能技术应用于资金交易领域，这标志着公募基金行业迎来了“AI 交易员”的新里程碑。

AI 技术与交易场景的结合，一定程度上替代了大量的重复劳动，极大提升了工作效率，降低了操作风险。但由于基金交易的复杂性与高风险性，基金管理公司在布局 AI 交易员的过程中目前仍面临如下重点问题：

第一，使用大语言模型面临一系列风险，如训练数据的合规性、输入信息的泄密风险、生成内容的数据合规风险等。这体现在交易场景则更加明显。一方面，在基金交易场景，交易员需要进行大量的信息交换与共享，如何保障输入信息的安全性是亟须考虑的问题。另一方面，监管部门对于特定交易场景下 AI 技术应用的态度有待确认，或需进行个案判断。

第二，由于基金交易的高风险性与复杂性，AI 交易员的应用还面临投资者交易观念的阻碍。根据某基金管理公司展示的“资金回购聊天场景截图”，我们将 AI 交易员与对手方的交易流程概括为：AI 交易员通过询价议价，完成对手方的询价需求采集，将询价状态实时反馈给人工交易员，并获取最终匹配交易反馈至人工交易员，和对手方确认后完成交易。上述交易流程的问题在于：一方面，即使可以通过 AI 交易员完成询价议价过程，但整个交易过程仍需要人工交易员的介入，AI 交易场景的效率有待论证。另一方面，由于基金交易涉及用户账户、财产、个人隐私等私密、重要的信息，并且受自身交易习惯与传统交易观念影响，投资者极易对 AI 交易员的安全性产生质疑，进而更加倾向于传统的交易模式。

（三）风险控制与合规管理

在风险与合规管理方面，生成式人工智能能够辅助基金管理公司精准识别市场风险，建立风险预警机制，提升风险管理效率，同时也能够提高合规检查的效率。

- 风险管理：基于风险管理系统，生成式人工智能可以快速识别并预警潜在风险，帮助基金管理公司及时采取风险防范措施。例如，通过对大量市场数据进行深度学习，生成式人工智能可以预测市场可能出现的异常波动，提前预警投资风险。

- 合规检查：生成式人工智能可以通过自然语言处理技术，实现对各类合规文件的快速分类、解析和审核，大大提高合规检查的效率。例如，生成式人工智能可以自动识别和标记合规文件中的关键信息，辅助合规人员进行审核，提升合规工作的效率和质量。

（四）公关与市场推广

在公关与市场推广方面，生成式人工智能可以帮助基金管理公司提升客户体验和市场影响力。

- 社交媒体管理：生成式人工智能可以根据用户行为和喜好针对性地产出优质内容，在生产设计、内容生成、名称拟定以及实时个性化等各个环节为基金管理公司高效提供创新灵感。此外，生成式人工智能也能高效管理各类社交媒体账号，实现各类社交媒体运营风格的一致性。并且，应用生成式人工智能技术，基金管理公司能够与受众实时在线互动从而提升粘合度，提高公司社交媒体的影响力。

- 市场推广：生成式人工智能可以分析市场趋势，定制个性化的市场推广策略，提高市场推广的效果和效率。例如，通过对市场数据的分析，生成式人工智能可以精准识别市场需求，为基金管理公司制定出更符合市场需求的推广策略。

三、从业人员日常使用之合规性分析

公募基金的各项运作关系广大投资者的切身利益，因此监管机构历来对公募基金的从业人员提出更高的行为规范要求。尽管目前未有监管规则对从业人员使用生成式人工智能作出单独规定，但结合生成式人工智能使用方法及技术逻辑的特殊性，有必要强化使用过程中的法律风险及相应行为规范，对此我们总结得出以下要点：

（一）使用行为的风险分析

生成式人工智能主要有两种使用方式，第一是由使用者输入命令，进而使人工智能系统直接生成一篇关于一般主题的简短文章或内容；第二是输入特定的数据、内容或文本后命令系统对输入的内容进行处理或生成新内容。目前，员工使用生成式人工智能的法律风险集中于第二种情形，即使用生成式人工智能进行信息输入。对此，我们就该使用行为所涉风险梳理如下：

1. 输入信息的泄密风险及应对

使用端的基金管理公司及有关从业人员在投资交易过程中需要收集、流转和处理大量敏感、隐私的个人信息数据和其他敏感数据，因此我们再次强调基金管理公司需对投资者的个人信息、产品的投资信息等承担保密职责，尤其是在涉及到信息安全的领域。根据目前了解到的 ChatGPT 的服务条款和使用条款，提供商有权处理、使用用户提供的信息以维护、开发和升级其技术。若员工向 ChatGPT 输入的内容涉及相关保密数据和信息，如投资者的个人信息、产品的投资信息(包括持仓和交易等重大非公开投资信息)、商业秘密以及公司其他的保密文件、数据等，该内容将会被提供商获得，并可能应用于 ChatGPT 的训练数据或标准化模板，进而作为回答内容提供给其他用户，这存在极大的泄密风险。事实上，生成式人工智能的提供商同样存在避免风险的需求，例如国内某 AI 创作平台用户协议就从要求使用者承诺输入内容不侵犯他人权利的角度作出规定[2]，以避免信息安全与个人隐私问题。

对此，我们建议基金管理公司应对 ChatGPT 的使用记录进行系统留痕，并对其处理的所有信息进行分类，为每一类信息制定相应的保护措施。对于最敏感的信息，应采取最高级别的保护措施，包括加密存储、限制访问和复制等。同时，公司还应明确规定禁止输入人工智能系统的信息类别，以及在输入人工智能系统前需进行去标识化和匿名化处理的信息类别，如投资者的个人信息、产品的投资信息等，并设置敏感文字、数据、文件等进行实时筛查。

2. 使用生成内容的风险及应对

ChatGPT 大型语言生成系统的本质使得其生成内容的准确性无法保证。对于知识性内容或可能出现事实错误，引发政治、法律或舆论等风险。因此，从业人员需要结合其他工具对生成内容进行综合判

[2] 该用户协议规定："我们尊重并保护用户及他人的知识产权、名誉权、姓名权、隐私权等合法权益。您保证，在使用服务时上传以及输入的内容不侵犯任何第三方的知识产权、名誉权、姓名权、隐私权等权利及合法权益。同时您同意并承诺，您使用本服务所提供、使用的文本内容已获得了充分、必要且有效的合法许可及授权。否则，我们有权在收到权利方或者相关方通知的情况下移除该涉嫌侵权内容。针对第三方提出的全部权利主张，您应自行处理并承担全部可能由此引起的法律责任；如因您的侵权行为导致公司及其关联公司遭受损失的(包括经济、商誉等损失)，您还应足额赔偿我们及其关联公司遭受的全部损失。"

断。

除内容本身的合法性以外，使用人对生成内容的使用也可能引发知识产权侵权风险。我们在查阅国内部分知名语言模型软件的用户协议后发现，这些语言模型软件的用户协议往往规定，语言模型软件生成内容的知识产权归软件所属主体所有，这也就导致用户对于通过输入信息、数据得到的内容无法享有知识产权，因此也难以对外商业使用，否则将面临侵犯语言模型软件所属公司知识产权的问题，而这在无形中也阻碍了语言模型软件的广泛使用。此外，如果生成的内容包含他人的知识产权，公司亦将面临侵权诉讼的风险。

对此，基金管理公司应深入理解并遵守相关的知识产权法律法规，并建立相关的内部合规制度。在使用生成式人工智能生成内容前，公司应做好全面的合规核查工作，以确保其使用行为符合知识产权相关规定，避免在没有明确获得许可的情况下使用人工智能生成的内容。

此外，公司应在使用生成式人工智能时对其生成的内容进行严格的审查，以确保内容的准确性并避免误导投资者。虽然生成式人工智能可以提供有价值的分析和见解，但其并不能替代专业的投资建议。因此，公司应确保在发布任何基于生成式人工智能的内容之前进行适当的校验、核实、评估及确认。

3. 是否符合国家监管要求的风险及应对

由国家互联网信息办公室等七部门联合公布的针对生成式人工智能的专门管理规定《生成式人工智能服务管理暂行办法》（“**《生成式人工智能办法》**”）自 2023 年 8 月 15 日起正式施行，其对生成式人工智能服务实行包容审慎和分类分级监管，并明确了提供和使用生成式人工智能服务的总体要求、安全评估与备案手续要求等。此前，监管机构也已根据《互联网信息服务算法推荐管理规定》《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》《互联网新闻信息服务新技术新应用安全评估管理规定》《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》等规定对生成式人工智能进行监管，要求其在符合一定条件时进行安全评估和备案，未履行相关程序将引起合规风险。

对此，我们建议基金管理公司在使用人工智能时，应注意所依据的大语言模型是否已经按照规定履行了安全评估以及备案手续等程序，以避免合规风险。

4. 生成式人工智能自身的数据合规风险及应对

从运行过程来看，人工智能生成内容的过程以及结果均面临数据合规的风险，具体体现在数据的收集、处理、流转、存储以及数据跨境的各个阶段。我们参考 ChatGPT 的隐私政策，就生成内容的各个阶段所涉及的数据合规问题进行检视，识别出以下数据合规风险：

首先，在数据收集阶段，根据《中华人民共和国个人信息保护法》，处理个人信息应当与处理目的直接相关，采取对个人权益影响最小的方式，即“最小必要”原则。而在当前隐私政策下，虽然 ChatGPT 已保证收集个人信息满足“最小必要”原则，但由于未将收集与用途一一对应，因此我们无法直接判断所收集的信息是否均满足“最小必要”原则，数据收集阶段的合规性有待进一步论证。此外，处理个人信息应当以“告知 — 同意”为基本前提，由于 ChatGPT 收集个人信息的范围广泛且一定程度上不完全可控，因此，其处理的个人信息是否已全部满足“告知 — 同意”要求也存在不确定性。

其次，在数据处理阶段，虽然 ChatGPT 的隐私政策承诺对所收集的个人信息进行“去标识化”。但是，在将所收集的个人信息与第三方平台进行共享的情况下，仅仅“去标识化”是不够的，其仍然面临着通过多种信息结合而被识别出信息主体的风险。因此，在数据处理过程中，对用户隐私权的保护仍需要采取进一步的措施，如对收集的个人信息进行匿名化处理等。

再次，在数据流转阶段，ChatGPT 的隐私政策表明用户的个人信息将在关联方之间共享，但对于信息将在何种情形、哪些“关联方”中得以共享，隐私政策并未说明，其亦未说明在关联方之间共享的必要性和合理性。

最后，在数据存储和跨境阶段，ChatGPT 表明，所收集的个人信息将存储于美国，对于涉及跨境传输的场景，ChatGPT 将依法采取适当的数据转移机制来确保跨境传输安全。但我们理解，ChatGPT 对于个人信息的存储期限并未进行明确告知，同时对于“匿名化或去标识化的个人信息将永久存储”这一条款，其合规性仍然有待商榷。此外，对于数据的跨境流动，在各国数据跨境规范、标准差异极大的情况下，其可操作性仍需进一步探讨。例如，对于数据跨境的评估要求，是否按照中国法律的要求进行安全评估或签署标准合同，或者按照其他数据来源国的规定履行相关程序。

对此，我们建议当前阶段将人工智能的应用限制在公开数据的搜集以及数据处理的初级阶段，并对上传的数据、个人信息采取去标识化或匿名化处理，以应对在当前阶段生成式人工智能的数据合规问题。

（二）接入方式的法律风险

若使用以 ChatGPT 为代表的境外开发的软件，则还需要解决接入方式的问题。根据《中华人民共和国计算机信息网络国际联网管理暂行规定》，“计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网。”如违反上述规定，由公安机关责令停止联网，给予警告，可以并处 15,000 元以下的罚款；有违法所得的，没收违法所得。因此，通过邮电部国家公用电信网以外的信道进行国际联网并使用 ChatGPT 的行为属于违法行为。目前国内也已发生多起因建立、使用非法定信道进行国际联网而受到行政处罚的案件，这对基金管理公司利用 ChatGPT 产生了一定限制。

四、生成式人工智能法规剖析

我们注意到，国内多家基金管理公司已着手开发自己的生成式或其他类型的人工智能系统。针对生成式人工智能，《生成式人工智能办法》在其征求意见稿发布后的短短三个月后，于 2023 年 7 月 13 日正式对外公布，并已自 2023 年 8 月 15 日起施行。结合此前监管机构就互联网信息服务与算法做出的监管规定，我们理解该领域法律法规的具体适用仍有待厘清，若基金管理公司有自行开发有关技术的意向，则应当持续关注相关领域的立法动态，遵循法定流程。

作为中国首份生成式人工智能监管文件，《生成式人工智能办法》的发布对基金管理公司开发、使用生成式人工智能产生重大影响。对此，我们就该文件的重点内容及具体影响作出以下解读：

关注要点	重点内容	法律建议
适用范围	根据《生成式人工智能办法》，向中华人民共和国境内公众提供生成式人工智能服务的，无论直接或间接，都将受限于《生成式人工智能办法》的相关规定。	我们建议，基金管理公司在选择服务提供商时，应确保该服务提供商已经履行了安全评估和备案等流程，得到适当授权，并遵守网络安全、数据和个人信息保护等相关法律法规。与此同时，基金管理公司应研究并了解其数据处理流程，以避免数据跨境问题。
分级监管	虽然《生成式人工智能办法》没有详细	由于缺乏具体规则的指引，我们对此建议基金

关注要点	重点内容	法律建议
	说明分级监管的具体规则，但国务院已将《人工智能法》列入 2023 年度立法工作计划，我们预计，生成式人工智能的分级监管将在即将出台的《人工智能法》中得到明确。	管理公司应适时预测和提前准备。具体而言，基金管理公司可从欧盟的《人工智能法案》中借鉴相关指导原则，尤其是对风险的划分。我们预测，生成式人工智能的监管法规可能会对不同级别风险的 AI 系统采取不同管理措施。因此，基金管理公司应该根据这些原则，提前做好风险评估和等级划分，以便根据自身等级对应的监管要求，提前做好准备。
服务提供者的义务和责任	《生成式人工智能办法》要求服务提供者采取有效措施提高训练数据质量，并强调与用户签订服务协议时应明确双方权利义务，对用户违法活动的监督增加了“警示”、“限制功能”以及“保存记录”和“报告”的义务。	对于基金管理公司而言，首要任务就是提升数据质量，这不仅是为了满足监管要求，更是为了提供更优质的服务。因此，为了明晰与用户的权利义务关系，公司应组建专门的法律团队起草服务协议，明确约定双方权利义务，尤其是对于用户违法行为的处理方式。
知识产权与数据保护	《生成式人工智能办法》要求服务提供者开展预训练、优化训练等训练数据处理活动，并使用具有合法来源的数据和基础模型；涉及知识产权的，不得侵害他人依法享有的知识产权；涉及个人信息的，应当取得个人同意或者符合法律法规要求。此外，提供者对使用者的输入信息和使用记录应当依法履行保护义务，不得收集非必要个人信息，不得非法留存、提供个人信息。	基金管理公司应做好知识产权和数据合规的核查工作，建立健全的知识产权与数据管理体系，包括数据收集、处理、存储和使用的规范化流程，以及知识产权侵权的核查机制。同时，应对数据收集做好必要的告知、说明工作，做好收集对应信息的必要性说明，并及时清理所存储的非必要信息。
安全评估和算法备案	《生成式人工智能办法》要求“提供具有舆论属性或者社会动员能力的生成式人工智能服务”的服务提供者履行安全评估和算法备案手续。	如果基金管理公司自研的生成式人工智能被应用于向广泛的公众客户提供服务，则其很可能需要对自身算法进行安全评估和备案。为此，公司需要组建专门团队以配合监管机构开展安全评估和算法备案工作，以确保算法的透明性、安全性与公正性。
境外服务服务提供者和外商投资	《生成式人工智能办法》要求来源于中华人民共和国境外的服务提供者应符合法律、行政法规和监管文件的规定，如若境外服务提供者存在违反相关法律法规要求的，国家网信部门应当通知有关机构采取技术措施和其他必要措施予以处置。	对此，我们建议如果基金管理公司拟引入外资共同开发生成式人工智能服务，或者使用境外服务提供者的服务，公司需仔细审查境外服务或其提供者的合规性。公司应要求外商投资者或服务提供者提供其合规性证明，以确保其遵守中国的法律法规和监管要求。

最后，基金管理公司若不自行开发生成式人工智能技术，而是通过采购外部服务开发新技术，也应在相关技术服务协议文件中明确技术提供方满足上述法律法规的要求，确保自身的合规性。更进一步，在进行业务运营和规划时，基金管理公司不仅要保持对生成式人工智能监管法规的敏感性，而且要积极参与到法规的讨论和制定中来，以便及时反馈自身的需求和痛点。

五、结语

生成式人工智能的出现为基金管理公司提供了新的机遇，抓住技术变革的契机实现飞跃自然是美好愿景，但创新不离守正，在乱花渐欲迷人眼的人工智能爆发时代，基金管理公司及相关从业人员唯有坚持从业规范及合规管理的基本要点，才能在这场变革中稳步前行。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

毛慧

电话： +86 21 6080 0506
Email： ellen.mao@hankunlaw.com

解石坡

电话： +86 10 8524 5866
Email： angus.xie@hankunlaw.com