金融场景下 AI 运用的若干问题研究

作者：吕红 | 陆奇 | 陶燕 | 陈雅秋

2025 年 2 月，一则关于十余家公募基金公司部署 DeepSeek 的新闻，在金融行业引发广泛关注。据相关报道披露，多家基金公司已顺利完成 DeepSeek 系列开源模型的私有化部署工作，并计划将其应用于投资研究、产品销售、风控合规、客户服务等金融机构核心业务场景之中。

实际上，当前已有众多机构正在积极评估大模型在应用层面的潜在可能性。这些探索广泛涵盖了多个领域，如在公司 APP 中部署 AI 对客，以提高客服工作质效；借助 AI 技术制作宣传推广材料，提升宣推效果；利用 AI 辅助制作定期报告、研究报告，提高报告生成效率与质量；组合运用 AI 和数据爬虫技术降低量化建模成本并提升量化策略有效性等。

在 AI 技术与金融行业深度融合的进程中，我们注意到行业在实践中遇到了一些值得共同思考的新课题。例如：金融机构在引入 AI 技术时，是否必须将 AI 部署于本公司内部系统，能否部署于其他机构的系统；若 AI 输出内容出现违规情况，责任应如何界定与承担；以及 AI 输出内容是否存在侵犯他人民事权利的潜在风险等。随着大模型技术的快速迭代，金融行业在探索出更多创新模式的同时，这些新问题也需要我们以更开放的心态持续探索。

在与同业交流过程中，我们发现 AI 客服、AI 图文生成，以及 AI 与爬虫的组合运用等业务场景备受机构关注。基于此，我们尝试从实际应用出发，对这些业务场景中可能涉及的合规风险与侵权问题进行初步梳理，希望能为行业提供一些参考。本文分析旨在抛砖引玉，期待与行业一同持续学习、探讨这些前沿问题的解决路径。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

一. AI 客服、AI 图文生成存在的风险

(一) AI 客服可能面临的特别风险

AI 客服是指利用人工智能技术来实现客户服务功能的系统或平台，当下有部分公司正在考虑将 AI 部署到公司 APP 中，实现与客户的直接交互。

1. AI 客服场景下呈现的特征

相比一般的 AI 图文生成，AI 客服具有实时交互性、数据敏感性及服务连续性等特征。

实时交互性方面，AI 客服需在用户发起咨询的极短时间内生成回复，形成实时对话。如果 AI 客服生成了违规内容，回复一旦发出，可能立即引发相应的后果。

数据敏感性方面，AI 客服在交互中，可能会收集、储存、处理用户提供的个人信息，例如用户的个人基本信息、用户的持仓信息和交易信息等，机构因此面临数据过度采集、储存或处理不当的风险。

服务连续性方面，AI 客服可能会被设置成 7*24 小时无间断运行，而 AI 存在数据漂移问题，即 AI 投入应用后传入的观察数据与模型训练数据之间的偏差，这一偏差会随着时间推移逐渐增大[1]，进而对 AI 客服服务的稳定性和质量产生影响。

2. AI 客服模型开发、内容生成阶段可能面临的风险

数据采集、处理、保存不当的风险。一方面，AI 客服模型开发阶段需要海量数据，在投入运用后与客户交互过程中也可能收集大量个人信息，在广泛收集处理数据时，可能存在侵犯个人信息权益的风险。例如，公司在收集投资者信息时，并未明确征得投资者关于使用其个人信息用于模型训练开发的同意。另一方面，搭载 AI 模型的系统也存在被攻击、系统数据被泄露、偷窃或者滥用的风险。

AI 生成内容违法违规的风险。AI 生成的内容可能存在如下违法违规情形：(1)违反宣推合规要求，如承诺保本保收益；(2)生成内容涵盖投资组合未公开信息、其他投资人/用户个人信息；(3)非法推荐股票、预测股市趋势；(4)生成内容不实(所谓 AI 幻觉)；(5)生成内容存在暴力、歧视语言等有害内容；(6)生成内容存在侵犯他人著作权、肖像权的情形等。

3. AI 客服风险控制的重点和难点

机构对 AI 生成内容导致的违规后果承担责任，该等责任不因搭载了 AI 模型或委托 AI 服务供应商开发模型而免除。AI 客服风险管控的难点在于，如何在 AI 实时对话机制下实施有效的合规审查，以确保生成内容的合法合规。可以考虑的控制措施包括：在模型训练阶段，对于内容生成规则进行规范；事中设置敏感词库拦截机制以及熔断机制，禁止输出包含敏感

[1] 陈思琳：《人工智能生成内容技术信息安全风险分析》，载于《保密科学技术》(2024 年.09 期)。

词汇的内容，并在客户输出敏感词汇时及时熔断 AI 客服转人工服务；事后进行 AI 客服对话回检，如发现问题的，及时予以修正。

在数据安全方面，机构需全面检视现有制度、机制及相关协议，确保 AI 客服涉及的所有数据处理场景已被涵盖。在用户协议及隐私政策方面，需要明确取得投资人或用户授权同意，并告知相应的处理规则。机构需要将 AI 客服系统纳入数据安全应急处理机制，定期进行应急预案演练。另外需要提示注意，如 AI 训练数据涵盖公司保密信息、投资组合未公开信息、投资者个人信息的，相关 AI 模型不应搭载在其他机构的系统中，避免泄露公司保密信息或违反法定保密义务。

具体还需要与技术团队通力协作，在技术可实现的基础上作详细论证评估。

(二) AI 图文生成可能面临的特别风险

AI 在显著提升材料、报告等的制作效率的同时，也引发了更多有关著作权侵权及数据安全方面的隐忧。

1. AI 图文生成面临特有著作权侵权风险

2024 年 2 月，广州互联网法院对全球第一例人工智能平台侵害著作权案作出判决[2]。该案中，法院认为被告某人工智能公司在进行人工智能模型训练时未经许可使用了享有著作权的美术作品“奥特曼”，并认定通过该平台用户获得的图片和原告主张著作权保护实质相似，进而认定被告侵害了原告作品的复制权和改编权。这表明，AI 图文创作带来的著作权侵权问题已经成为了司法及公众关注的问题，尽管 AI 技术具有创新性，但无论是 AI 训练过程，还是运用 AI 生成的图文内容，均无法超脱著作权相关法律法规的约束范畴。

造成 AI 生成内容特有著作权侵权风险的技术根源主要有两方面。其一，部分 AI 工具在模型训练阶段，纳入了未经授权的内容，例如盗版书籍、付费论文等，这些侵权素材被用于训练，使得 AI 生成的内容可能携带侵权隐患。其二，部分 AI 模型缺乏有效的溯源机制，未能精准标记内容来源，这导致一旦出现侵权纠纷，难以清晰追溯 AI 生成内容的原始出处，进一步提高了侵权风险。

2. AI 图文生成面临的数据安全风险及违反法定保密义务的风险

有媒体报道，某知名外国公司在引入 ChatGPT 后不到 20 天，即发生了 3 起机密数据泄露事件。该公司员工因三个动作导致了泄密，上传产品计量数据库源代码、上传设备产量和产品良率相关代码、将会议记录输入 ChatGPT，以上信息在上传的瞬间即成为了 ChatGPT 的学习资料，被发送到了公司外部服务器储存，且公司无法再收回。[3]

从以上案例可以总结出向 AI 上传信息可能面临的数据泄露、数据滥用风险。AI 需要将用户上传的数据传输至服务器处理，这将使得数据脱离公司的安全管理范围；公司无法控制 AI

[2] 上海新创华文化发展有限公司诉某 AI 公司侵害其他著作财产权纠纷一审判决书((2024)粤 0192 民初 113 号)。
[3] 《三星引入 ChatGPT 不到 20 天，被曝发生 3 次芯片机密泄露》，https://www.36kr.com/p/2199588798164105。

如何使用上传的数据，相关数据可能被用于训练模型、商业分析，甚至 AI 系统本身也可能因被攻击而泄露相关数据。

从金融机构的角度，向外部系统传输客户信息、投资组合未公开信息等公司负有法定保密义务的信息，本身即构成违规。

3. AI 图文生成内容直接对客使用面临的风险

AI 输出内容是模型基于自然语言理解能力对搜索来源中的信息的整合，AI 本身并不具备分辨真实与虚构的能力，因此其输出内容可能存在不准确之处，或可能存在对原文内容的不当改写。如将使用 AI 制作的宣推材料、定期报告或其他报告直接向客户发布，将可能因为披露内容不准确、不真实而面临宣推、信息披露等方面的合规问题。

4. 相关建议

为尽量降低使用 AI 进行图文创作带来的额外合规风险及侵权隐患，建议采取以下防范措施:

一是审慎选用合规的 AI 工具。在选择和使用 AI 工具前，应审慎甄别其合法性，详细研读相关用户协议，特别是关于训练数据来源的条款。明确确认协议中是否包含对训练数据合法性的说明和保证。避免使用可能因训练数据来源不合法而构成潜在侵权风险的 AI 工具。

二是强化人工审查。原则上，所有 AI 生成内容均应当进行人工审查确认。机构需详细记录 AI 所标识的数据来源，重点排查是否存在疑似未被 AI 标识来源的他人独创性内容。若需引用他人作品，务必依法提前获取授权，杜绝未经授权使用他人知识产权的情况。另一方面，为避免对客资料披露不准确、不真实的问题，应当加强对 AI 生成图文与基金法律文件一致性以及表述准确性等方面的内容审查。

三是特别注意禁止上传未公开信息。在引入 AI 前应当做好对员工的必要培训，提高其合规意识，严禁将投资组合未公开信息、投资者/用户信息、公司经营管理信息等保密信息上传至 AI。

二. AI 与数据爬虫技术组合运用存在的风险

数据爬虫是一种通过编程技术自动化地访问网页，并系统性地提取指定数据的行为，可用于研究分析、市场跟踪以及优化投资策略等。伴随 AI 技术的迅猛发展以及大数据分析需求的与日俱增，部分机构，特别是资产管理机构，开始采用 AI 技术来强化和优化数据爬虫策略。通过 AI 算法，能够更精准地从海量数据里挖掘出有价值的信息，大幅提升量化模型有效性验证的效率，AI 及爬虫技术的组合运用已然成为这些机构提升研究效率的重要手段。然而，AI 技术催生的数据爬虫需求急剧增长，也使得与之相关的问题愈发突出。

根据我们观察，目前区分不同场景，面临的责任风险不一:

(一) 在内部研究用途中使用爬虫技术的法律风险

1. 违约风险

数据爬虫在技术层面需要与目标网站建立访问连接，而目标网站通常会在服务条款中明确禁止非授权性爬虫行为。例如，不少网站通过弹窗或者勾选服务协议的形式，将“禁止非搜索引擎的爬虫抓取”作为条款之一，并对相关内容进行加粗提示或其他显著标识。基于《中华人民共和国民法典》及相关司法解释，网站如果能够有效证明其在电子合同模式下充分履行了提示和告知义务，则服务条款里的相关禁止性约定对用户可能具有一定法律约束力。

因此，对于机构而言，在使用爬虫技术进行数据抓取前，必须仔细研读目标网站的服务条款，以避免触发违约责任。

2. 侵权风险

(1) 扰乱网络服务的风险

根据《网络数据安全管理条例》的相关规定，通过自动化工具实施数据抓取，应当评估对目标网站带来的影响，不得非法侵入他人网络，不得干扰网络服务正常运行。例如，绕过目标网站的技术保护措施、频繁访问导致服务宕机等行为，均可能构成违法。因此，机构在使用爬虫系统时，应审慎评估目标网站的网络运行状况，合理设置爬取频率与策略，以免引发网络安全问题。

(2) 侵犯个人信息权益风险

针对含有个人信息的公开数据，爬取、加工甚至存储此类数据可能被认定为侵犯个人信息权益。根据《民法典》及《刑法》相关规定，非法获取或处置公民个人信息的行为可能构成侵权甚至犯罪行为。《网络数据安全管理条例》也明确规定，因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，网络数据处理者应当删除个人信息或者进行匿名化处理。为此，在涉及个人信息的数据爬取场景中，需采取必要的脱敏和隐私保护措施，严格遵守相关法律法规。

(3) 著作权侵权风险

不同类型的数据内容是否构成《著作权法》下的“作品”，需要满足独创性、属于智力成果等要件。例如，网络文章、论坛帖子等通常被认定为具有独创性和版权性质，而高度概括的短评(例如，“给力”等字词或字词的简单组合)或单纯事实消息一般不具备著作权保护。因此，机构在使用爬取到的内容前，应明确数据的属性及著作权归属，避免因未经授权使用受保护数据而承担侵权责任。

(二) 数据爬虫技术的外用风险(如数据转售或公开发布)

当数据爬虫技术被用于对外提供、出售或发布数据时，相关风险可能显著加剧。其主要表现如下:

1. 违约与侵权法律风险的升级

公开或出售未经授权爬取的数据，可能违反目标网站的服务条款，并构成侵权行为。特别是在涉及个人信息或享有著作权的数据内容时，未经许可即进行商业化利用，将容易导致较为严重的法律后果。

此外，公开或出售未经授权爬取的数据，显著增加了违约和侵权风险的暴露程度。相较于内部使用，对外披露或商业化利用更加容易被目标网站监测并采取法律行动。

2. 不正当竞争风险

在使用爬虫技术对外直接竞争的情形下，可能会构成不正当竞争行为。如爬取某平台付费或需要大量努力才能建立的独特数据资源，并将其用于直接竞争或替代性服务，则可能被认定为故意扰乱市场秩序。根据《反不正当竞争法》规定，不正当竞争行为不限于传统意义上的“直接竞争者”，而是将所有具有商业决策、经营活动的主体均纳入“经营者”范畴。

司法实践中，也广泛支持数据持有方对其合法数据权益的控制。例如，在天津自由贸易试验区人民法院审理的“上海某公司爬取新闻平台数据案”(案号: 2022 津 0319 民初 11108 号)中，法院认定未经授权的广泛爬取行为超出了合理使用数据的范围，构成不正当竞争。

3. 数据本身准确性风险

若将爬取得到的数据对外销售，由于销售方承担标的物的瑕疵担保责任，还应当进一步关注数据本身的准确性及完整性风险。数据的准确性直接影响到买卖合同的履行。如果出售的数据存在错误或不完整，可能导致买方无法实现预期的经济利益，从而引发合同纠纷。

(三) 相关建议

为防范上述法律风险，建议机构在应用爬虫技术时应采取以下合规措施:

1. 技术评估

在开展数据爬虫之前，应对目标网站的相关法律条款和技术构架进行全面的评估。包括研究目标网站的服务条款(如《用户协议》《隐私政策》等)，以确认其中是否明确禁止爬虫活动。此外，还应对目标网站的网络运行环境和数据权限进行细致分析，确认使用爬虫技术不会绕过权限限制或干扰网站正常运行。

2. 数据分类与敏感性控制

对爬虫所获得的数据进行分类，厘清公开信息与非公开信息的边界，遵守个人信息保护、著作权及商业秘密相关法律。对敏感数据采取脱敏、加密等技术处理措施。同时，制定严格的数据管理制度，防止泄露或滥用。

3. 限定使用目的与范围

在数据使用环节，应严格控制爬取数据的用途及应用范围。建议机构将爬取数据的用途限定于内部研究和分析用途，并明确禁止未经授权的进一步传播、加工或使用行为。例如，擅自将数据对外出售或在未获得授权的情况下公开披露，会加剧相关违约及侵权责任风险。

如您希望就相关问题进一步交流，请联系：

吕 红
+86 21 3135 8776
sandra.lu@llinkslaw.com

陆 奇
+86 21 3135 8695
qi.lu@llinkslaw.com

陶 燕
+86 21 3135 8755
yan.tao@llinkslaw.com

陈雅秋
+86 21 3135 8744
jane.chen@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野