人工智能体产品开发与上市的法律风险扫描

作者：杨迅 | 张莹

在当今数字化浪潮下，人工智能产品，尤其是智能体，正以前所未有的速度涌入市场，成为科技领域的焦点。从智能客服到智能写作助手，从智能家居设备到智能医疗系统，这些智能体产品不仅改变了我们的生活方式，也为企业带来了新的商业机遇。

然而，随着这些产品的广泛应用，其法律风险也日益凸显。这些风险并非局限于单一的知识产权或数据合规问题，而是涵盖了知识产权、数据安全、许可牌照、监管合规等多个法律领域的综合考量。

笔者结合近期处理的一些相关案件经验，与大家分享这些法律风险的识别与应对策略，以期为人工智能产品的健康、合规发展提供一些有益的参考。

一. 人工智能体产品纵览

人工智能产业正以一种前所未有的速度发展。技术的发展带来产业的进步，不仅涌现出一批专业开发人工智能的企业，大量传统企业也推出了人工智能应用产品，极大丰富了人工智能产业生态。

1. 人工智能产品的类别

人工智能产业，从其技术层次看，可以分为: (1)大模型，(2)智能体，和(3)智能设备三大层次。

请联系:

Publication@llinkslaw.com

大模型是人工智能体的基础，它们通过海量的数据训练，获得生成和理解各种语言内容的能力。这些模型通常由专业的科研团队或大型科技公司开发，其强大的语言处理能力为智能体提供了核心支持。例如，OpenAI 的 GPT 系列模型，以其庞大的参数量和卓越的性能，成为了智能体开发的重要基础。大模型的开发不仅需要巨大的计算资源，还需要严格的数据管理和伦理考量，以确保模型的可靠性和安全性。

人工智能大模型固然是人工智能发展的基础和保障，但丰富的人工智能应用产品则在更大程度上丰富了人工智能业务生态。智能体是基于大模型开发的应用程序或服务，它们能够与用户进行交互，提供个性化的服务。智能体通过调用大模型的接口，结合自身的业务逻辑和数据，为用户提供各种功能。例如，智能客服机器人可以自动回答用户的问题，智能写作助手能够帮助用户创作文本内容。智能体的设计需要充分考虑用户体验，确保交互的自然性和高效性。

智能设备则是集成了人工智能技术的硬件产品，比如智能音箱、智能机器人等。这些设备通过内置的智能体或直接调用大模型，给用户提供语言交互、图像识别、智能推荐等功能。可以说智能设备是利用人工智能技术赋能硬件产品，是软件和硬件的结合。

本文主要探讨智能体的法律风险问题。

2. 智能体的基本模块和基本架构

一个典型的智能体架构由输入模块、处理模块、输出模块、控制模块和数据管理模块构成，各模块协同工作以实现高效用户交互和服务提供。输入模块接收语音、文本、图像等多种形式的用户输入，并将其转换为适合处理的格式，如将语音指令转为文本，确保输入信息准确完整。处理模块作为核心，调用大模型进行语言处理和逻辑推理，深度分析输入文本并生成回应或执行操作，还需根据应用场景定制逻辑以满足业务需求。输出模块将处理结果以文本、语音、图像等形式反馈给用户，注重用户体验，保证输出内容清晰易懂。控制模块负责内容合法性和安全性，通过关键词过滤和输出过滤防止生成违规内容，确保符合业务和用户期望。数据管理模块则负责收集、存储和管理用户数据，采用加密和匿名化等技术保障数据安全和隐私。

智能体一般需要和大模型交互，利用大模型的能力。从与大模型的交互关系看，智能体部署模式主要有以下四种:

(1) 本地化部署

在本地化部署模式下，智能体和大模型都部署在本地服务器上。这种部署方式的优点是数据处理速度快，安全性高，适合对数据安全和处理速度要求较高的应用场景。然而，本地化部署需要较高的硬件成本和维护成本。

(2) API 调用

在 API 调用模式下，智能体通过 API 接口调用远端的大模型。这种模式的优点是开发和部署简单，适合快速迭代和更新。API 调用模式需要确保 API 的安全性和稳定性，同时要处理好数据传输过程中的安全问题。

(3) 云部署

在云部署模式下，智能体和大模型都部署在云端服务器上。云部署的优点是成本较低，易于扩展，适合中小型企业或个人开发者。不过，云部署需要依赖网络连接，数据传输的安全性需要特别关注。

(4) 混合部署

混合部署结合了本地化部署和云部署的优点，部分数据和模型部署在本地，部分部署在云端。这种模式可以根据具体需求灵活调整资源分配，既保证了数据处理的高效性，又兼顾了数据的安全性。

3. 智能体的应用场景和市场

智能体的主要应用场景涵盖了教育、医疗、金融、客服等多个领域。在教育领域，智能教育助手可以为学生提供个性化的学习方案，解答学习疑问；在医疗领域，智能医疗助手能够协助医生进行病历记录、诊断建议等；在金融领域，智能金融顾问可以为用户提供投资建议、风险评估等服务；在客服领域，智能客服机器人能够自动回答用户问题，提高客服效率。这些应用场景不仅提高了工作效率，还改善了用户体验。

智能体的市场主要分为 2B 市场和 2C 市场，这两个市场各有其特点和关注点。

在 2B 市场，智能体通常作为组件或服务嵌入到其他企业的系统或设备中。企业客户更关注智能体的性能、稳定性和与现有系统的兼容性。例如，智能体可能集成到车载系统中，实现语音识别、智能推荐等功能，从而提升车载系统的自动化能力和用户体验。就 2B 市场而言，智能体运营者必须考虑定制开发部分的知识产权归属和客户数据控制权等问题。

在 2C 市场，智能体直接面向消费者，提供各种在线服务。消费者更关注产品的易用性、功能丰富性和隐私保护。例如，智能写作助手可以直接为用户提供文本创作服务，满足个人用户的需求。2C 市场的消费者权益保护尤为重要，企业需要确保产品的用户界面友好，操作简便，同时提供丰富的功能来吸引用户。隐私保护是 2C 市场的一个重要考量因素，企业必须确保用户数据的安全，遵守相关的隐私法规，以赢得消费者的信任。通过关注这些不同的市场特点和需求，智能体运营者可以更好地定位产品，满足不同客户群体的需求，从而在竞争激烈的市场中脱颖而出。

二. 主要法律风险一览

随着人工智能体产品的快速发展，其面临的法律风险也日益复杂。这些风险不仅涉及知识产权保护，还包括数据安全、许可牌照和监管等多个方面。

1. 知识产权风险

智能体产品的开发和运营涉及多个层面的知识产权问题，这些风险不仅可能影响产品的合法性，还可能引发法律纠纷，给开发者带来不必要的损失。

第一，模型的知识产权保护。模型通常由算法和数据构成，表现为一定的计算机程序，受著作权法的保护。根据《中华人民共和国著作权法》和《计算机软件保护条例》，软件开发者对其开发的软件享有著作权，包括源代码、目标代码、文档等。因此，智能体运营者需要确保其开发的模型不侵犯他人的知识产权。如果需要利用第三方模型，必须明确模型的开源或闭源性质。对于开源模型，智能体运营者需要确认其是否符合开源许可证的要求，确保使用方式在许可范围内。例如，某些开源许可证可能禁止将模型用于商业目的，或者要求在使用时必须公开源代码。对于闭源模型，智能体运营者则需要获得相应的商业许可，以合法使用模型。

第二，训练数据合法性。训练数据的合法性是智能体开发中另一个重要的知识产权问题。根据《生成式人工智能服务管理暂行办法》第七条第(二)项规定:“涉及知识产权的，不得侵害他人依法享有的知识产权”。这意味着智能体运营者必须确保其使用的训练数据来源合法。在实际操作中，各国对于训练数据能否构成合理使用的标准尚有争议。例如，某些国家可能允许在特定条件下使用受版权保护的数据进行训练，而另一些国家则可能对此持更严格的态度。

第三，输出结果的合法性。智能体的输出结果虽然由用户控制，但智能体的提供者仍可能构成著作权侵权。例如，智能体可能由于生成与他人受版权保护的作品相似的内容，或者未经授权使用他人的作品作为生成内容的基础，而被指控侵犯著作权。比如我国两起“奥特曼”案件((2024)粤0192 民初 113 号和(2024)浙 01 民终 10332 号)即是如此。因此，智能体运营者需要在智能体的设计和运行中采取措施，防止生成内容侵犯他人的著作权。这可以通过设置内容过滤机制、关键词过滤等方式实现，确保生成内容的合法性和安全性。

2. 数据安全风险

智能体的运行以数据处理为核心，因此数据安全风险不仅可能影响产品的合法性和安全性，还可能引发法律纠纷和用户信任危机。

第一，个人信息保护。个人信息保护是数据安全的核心问题之一。智能体在运行过程中会收集和处理大量的用户个人信息，这些信息可能包括用户的姓名、联系方式、位置信息、偏好设置等敏感数据。因此，智能体运营者必须确保在使用这些个人信息进行模型训练和推理时，已经获得

了用户的明确授权，并且严格遵守法律法规的要求。例如，医疗智能体如果使用未脱敏的患者病历进行训练，可能违反《个人信息保护法》。此外，智能体在向远端大模型提供个人信息时，也需要确保该对外提供行为符合用户的授权范围，避免未经授权的二次使用。

第二，隐私风险。隐私风险是智能体产品面临的另一个重要问题，尤其是在智能体辅助人肉搜索和披露个人详细信息方面。智能体可能会无意中记住训练数据中的敏感细节，并在与用户的交互过程中泄露这些信息。例如，智能体可能通过用户的输入识别出特定个人的详细信息，并在回答中无意披露这些信息，从而侵犯个人隐私。智能体运营者需要在智能体的设计中加入隐私保护机制，如关键词过滤和输出过滤，以防止生成内容中包含敏感信息。

第三，数据泄露风险。数据泄露风险是智能体产品面临的最严重的数据安全问题之一。例如，企业员工在使用智能体进行代码优化或提取会议纪要时，可能会将公司的机密信息提供给智能体，从而导致泄密风险。如果智能体运营者将这些机密信息作为模型的训练数据，将会导致二次泄密风险。此外，智能体的训练数据可能被攻击者通过技术手段反向提取出来。因此，智能体运营者需要采取技术措施，如数据加密、访问权限控制和日志溯源，来防止数据泄露。同时，需要在法律层面明确数据的权属和使用范围，确保数据的合法使用和保护。

3. 许可牌照风险

在智能体产品的开发与运营过程中，许可牌照风险是企业必须面对的重要法律问题之一。在开展智能体业务过程中，常见的许可证要求如下:

第一, ICP 许可。ICP(Internet Content Provider)许可是提供互联网信息服务的企业必须取得的许可。根据《互联网信息服务管理办法》第七条第一款规定:“从事经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门申请办理互联网信息服务增值电信业务经营许可证。”如果智能体产品通过互联网向用户提供收费服务，如付费咨询、会员制服务等，企业必须取得 ICP 许可。

第二，文化产品许可和音视频经营许可。通过智能体提供文化产品或音视频服务的，需要取得文化产品许可或音视频经营许可。通常以下智能体运营者需要获得该等许可: (1)教育智能体运营者，比如提供智能课程辅导、生成绘本故事等; (2)影音智能体运营者，比如提供音视频语音点播和智能搜索等; 以及(3)音乐智能体运营者，比如提供智能音乐创作等。

第三, EDI 许可。EDI(Electronic Data Interchange)许可主要适用于在线交易结算类业务，包括电子商务、支付结算等。通过智能体提供商品交易撮合和结算的，需要 EDI 许可。

4. 监管要求

除前述法律风险外，监管风险是人工智能体产品面临的另一个重要问题。比如，《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》等规范下的算法备案、安全评估等要求；《互联网用户账号信息管理规定》下的实名认证要求，《人工智能生成合成内容标识办法》下的标识要求；以及《未成年人网络保护条例》下的防沉迷要求等。这些规定都在各个方面对智能体的设计和运营提出要求。

三. 法律风险控制流程

为了有效应对人工智能体产品开发与上市过程中面临的法律风险，智能体运营者必须采取全面且系统的法律风险控制方法。一方面，Compliance by Design(合规设计)是一种关键策略，它要求在产品设计的早期阶段就将合规要求融入其中，而非等到产品完成后才进行法律审查。例如，通过在智能体设计中加入关键词过滤和输出过滤功能，可以确保生成内容的合法性，从而预防潜在的法律问题。此外，合规设计还涉及数据管理、用户隐私保护和知识产权保护等多个方面，确保产品从一开始就符合法律法规的要求，而不是简单地写一写“隐私政策”。另一方面，法律风险控制应贯穿产品的整个生命周期，而不仅仅是上市前的合规审查。这意味着智能体运营者需要在产品的开发、设计、商业化和运行阶段持续进行法律风险评估和控制。全生命周期的风险管控有助于及时发现和解决潜在的法律问题，确保产品在各个阶段都符合法律法规的要求。

同时，智能体的法律风险管控也不仅仅是数据合规或知识产权的单方面问题，而是需要综合考虑多个法律领域的综合思考。智能体运营者需要综合考虑数据合规、用户隐私保护、内容合法性、市场推广合规性等多个法律问题，采取全面的法律风险控制措施，确保产品的合法性和安全性。

智能体开发、上市、运行各阶段关注要点如下:

1. 开发阶段

智能体开发阶段主要关注以下法律风险问题:

(1) 模型知识产权

在人工智能体的开发过程中，智能体运营者必须确保其开发的模型不侵犯他人的知识产权。这包括确保所有使用的基座模型都有合法的来源和必要的授权。如果智能体运营者选择使用第三方模型，必须明确该模型是开源还是闭源，并严格遵守相应的许可协议。例如，对于开源模型，智能体运营者需要确认其使用方式是否符合开源许可证的要求，如是否需要公开源代码或是否可以用于商业目的。对于闭源模型，则需要获得相应的商业许可，以确保合法使用。

(2) 数据来源的合法性

数据是人工智能体开发的关键要素。智能体运营者需要建立严格的数据来源审核机制，以确保所有数据可溯源，以及数据处理符合法律法规的要求。对于敏感数据，智能体运营者需要采取额外的保护措施，如匿名化处理，以保护用户隐私。例如，在使用用户数据进行模型训练时，智能体运营者必须确保已经获得了数据使用的授权，或者数据的使用符合法律规定的合理使用范围。

(3) 部署方式的选择

选择合适的部署方式是开发阶段的另一个关键法律风险控制要点。智能体运营者需要根据产品的具体需求和安全要求，选择本地化部署、云部署或混合部署等部署方式。不同的部署方式决定了不同的数据安全和合规要求。例如，在本地化部署中，智能体运营者需要确保本地服务器的安全性，防止数据泄露和未授权访问。在云部署中，智能体运营者需要与云服务提供商签订数据安全协议，明确双方在数据保护方面的责任和义务。在混合部署中，智能体运营者需要确保本地和云端的数据传输安全，采用加密技术保护数据的传输过程。

2. 产品设计阶段

产品设计阶段主要考察以下方面:

(1) 控制模块

在产品设计阶段，控制模块的设置是确保生成内容合法性和安全性的关键措施。智能体运营者需要在智能体中设置关键词过滤和输出过滤功能，以防止生成违反法律法规或道德规范的内容。这些过滤功能可以自动检测和过滤掉可能存在问题的内容，如暴力、色情、歧视等。此外，智能体运营者还需要定期更新过滤规则，以应对新的法律要求和潜在风险。

(2) 防沉迷机制

保护未成年人的合法权益是产品设计阶段的重要法律风险控制要点。智能体运营者需要设计符合防沉迷要求的机制，如限制使用时间、设置家长控制功能等。这些机制可以有效防止未成年人过度使用智能体产品。例如，智能体运营者可以在产品中设置每日使用时间限制，一旦超过设定时间，智能体将自动提示用户休息或暂停使用。此外，智能体运营者还可以提供家长控制功能，允许家长远程监控和管理未成年人的使用情况。

(3) 数据安全和隔离机制

保护用户数据的安全和隐私是产品设计阶段的核心法律风险控制要点。智能体运营者需要采用加密技术保护数据在传输和存储过程中的安全，防止数据泄露和未授权访问。同时，

智能体运营者还需要建立数据隔离机制，确保不同用户的数据不会相互泄露。例如，智能体运营者可以在产品中采用多租户架构，为每个用户提供独立的数据存储空间，确保用户数据的隔离和安全。此外，智能体运营者还可以采用访问控制技术，限制对敏感数据的访问权限，确保只有授权用户才能访问和使用数据。

(4) 数据共享管理机制

确保数据共享的合法性和安全性。智能体运营者需要明确智能体在运行过程中如何与远端大模型或其他数据处理第三方交互和共享数据。如果涉及数据共享的，应建立安全的共享渠道以及建立获得相关数据主体知情同意的机制。

(5) 人工智能内容标识

根据监管要求，智能体运营者需要在生成内容中加入明确的标识，告知用户内容是由人工智能生成的；该些标识应当清晰可识别，符合相关国标。此外，智能体运营者还可以提升内容来源的透明度，帮助用户判断内容的可信度。例如，可以在产品中提供内容生成的背景信息，如使用的数据来源和生成算法等。

3. 商业化阶段

在智能体产品准备投入市场的商业化阶段，需要重点考虑如下问题:

(1) 许可牌照

在商业化阶段，确保服务符合相关许可要求是重要的法律风险控制要点。智能体运营者需要根据产品提供的服务类型，申请并获得必要的许可牌照，如 ICP 许可、文化产品许可、音视频经营许可等。

(2) 知识产权分配

如果涉及到通过合作伙伴定制开发、系统集成的，需要注意平衡智能体运营者和合作伙伴的权益。在与合作伙伴的商业合同中，智能体运营者需要明确知识产权的归属和使用方式，尤其是，定制开发和集成开发部分的权利归属。

(3) 渠道管理

智能体的商业化需要建立和维持智能体产品的合法销售渠道。智能体运营者需要建立合法的销售渠道，防止未经授权的分发和使用。例如，智能体运营者可以在产品中设置防伪标识，确保产品的合法销售。此外，智能体运营者还需要定期检查销售渠道的合法性，确保产品的销售和使用符合法律法规要求。

4. 运行阶段

在智能体产品的运行阶段，重点关注以下问题:

(1) 避风港原则

在运行阶段，保护智能体运营者免受用户侵权行为的连带责任是重要的法律风险控制要点。智能体运营者需要在用户协议中明确避风港原则的适用，在实际操作中建立避风港机制，确保智能体运营者在用户侵权行为发生时能够免受连带责任。

(2) 投诉举报处理机制

及时处理用户的投诉和举报，保护用户的合法权益是智能体运营中的关键问题之一。智能体运营者需要建立有效的投诉举报处理机制，确保用户能够方便地提交投诉和举报。例如，智能体运营者可以在产品中设置投诉举报入口，方便用户提交问题。此外，智能体运营者还需要定期处理和回复用户的投诉举报，确保用户的问题得到及时解决。

(3) 数据保存和管理机制

智能体运营需要确保数据的安全和可用性。第一，智能体运营者需要建立数据保存和管理机制，确保数据的安全存储和备份。第二，智能体运营者还需要定期检查数据保存和管理机制的有效性，确保数据的安全性和可用性。第三，对于个人信息，智能体运营者应当按照法律要求和相关隐私政策的约定保管和删除个人信息，确保个人信息处理的安全与合规。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@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