汉坤法律评述
2026 年 3 月 31 日

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

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约 | 硅谷

AI 企业出海（二）：法律尽职调查关键风险合规自查指南

作者：刘夏艺 | 段志超 | 姜泽骏 | 赵晨辰

引言

近年来，中国人工智能产业正经历前所未有之资本热潮。数据显示，2024 年中国人工智能行业一级市场融资总额达 1,052.51 亿元，融资事件 696 起，近十年行业融资规模已从2015 年的 300.7 亿元扩张逾 3.5 倍[1]；进入 2025 年，这一趋势更趋强劲——截至 2025 年 11 月，仅具身智能产业，全年融资事件超 305 起，总额超过 380 亿元，参与投资机构数量逾 600 家[2]。从月之暗面、智谱 AI 等头部大模型企业单轮数十亿元级融资，到自动驾驶、具身智能、AI 基础设施等细分赛道的持续吸金，资本正以前所未有的密度涌入这一领域。

值得注意的是，融资热潮的背后，是投资人日趋审慎的尽职调查态度。随着 AI 企业出海进程加速、监管框架日趋完善（如算法备案、大模型备案、数据跨境传输等合规要求的落地），以及开源合规风险等新型法律问题的涌现，法律尽职调查在投融资交易中的地位愈发重要。对于创始人及管理团队而言，融资不仅是资金层面的对接，更是企业合规体系接受全面检验的过程，任何一处系统性疏漏都可能成为交易推进的障碍，甚至影响企业后续的资本化路径。

本文作为 AI 企业出海系列文章的第二篇，将承接前文关于股权架构的探讨，梳理在融资法律尽职调查中针对 AI 企业特殊属性的合规自查核心要点，涵盖业务资质、数据安全、知识产权以及股权架构四大维度，以期为 AI 企业提供一份实用的合规自查指南，助力 AI 企业在资本化道路上行稳致远。

一、业务资质：业务发展之准入门槛

AI 企业的业务模式往往涉及复杂的互联网信息服务、算法推荐及生成式人工智能服务，这使得相关资质许可成为法律尽职调查的首要关注领域。以下就大模型备案、算法备案及 ICP 许可/备案三项核心资质展开分析。

（一）大模型备案：生成式 AI 服务的“身份证”

根据《生成式人工智能服务管理暂行办法》（2023 年 8 月 15 日施行，以下简称“**《暂行办法》**”）第十七条，“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，应当按照国家有关规定开展

[1] 2024 年人工智能行业融资超 1000 亿元，有一半 AI 公司成立三年内获投，IT 桔子，2025 年 02 月 25 日。

[2] 36 氪研究院 |2026 年具身智能产业发展研究报告，36 氪研究院，2026 年 1 月 30 日。

安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案和变更、注销备案手续”。国家互联网信息办公室（“**国家网信办**”）于 2024 年 3 月发布的《生成式人工智能服务已备案信息》公告进一步明确，大模型备案采取“上线一批、备案一批”的滚动机制。截至 2026 年 2 月，已有将近 800 款大模型完成备案并对外公布[3]。

对于 AI 企业而言，大模型备案的触发条件具有广泛适用性。只要企业提供的生成式 AI 服务具备“舆论属性”或“社会动员能力”（例如面向公众提供文本生成、图像生成、代码生成、音视频合成等服务）即落入备案范围[4]。

根据我们的项目经验以及相关法律法规的要求，大模型备案实行“属地初审、中央终审”的两级审核机制。主管部门为企业注册地所在的省级互联网信息办公室[5]，由其负责材料初审与技术安全评测，初审通过后，上报国家网信办进行最终复核并统一公示。

（二）算法备案：算法推荐服务的“准入证”

根据《互联网信息服务算法推荐管理规定》（2022 年 3 月 1 日施行，以下简称“**《算法规定》**”）第二十四条要求，“具有舆论属性或者社会动员能力的算法推荐服务提供者应当在提供服务之日起十个工作日内通过互联网信息服务算法备案系统填报服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息，履行备案手续”。根据《算法规定》第二条，算法推荐技术包括“利用生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术向用户提供信息”。

AI 企业往往是算法技术的重度使用者，其业务形态与算法备案的关联度极高。以下为需完成算法备案的常见的算法技术种类及算法功能[6]，其中，生成合成类算法系提供大模型相关 AI 服务的 AI 企业所主要涉及的算法备案类型：

算法技术种类	算法功能[7]
生成合成类算法	利用深度学习、虚拟现实等生成合成类算法制作文本、图像、音频、视频、虚拟场景等网络信息（大模型企业的文本生成、图像生成、语音合成等核心功能）。
个性化推送类算法	基于用户画像的内容推荐（如广告推送、信息内容推送）。
排序精选类	根据特定算法规则对信息进行排序展示，突出或屏蔽特定内容（如搜索引擎结果排序、热搜榜单、电商平台店铺/商品排序）。
检索过滤类算法	基于用户需求或法律要求对信息进行检索和过滤（如 AI 搜索、AI 问答等）。
调度决策类	自动或辅助生成供需匹配、资源配置、路径规划等调度决策结果（如车辆调度分配）。

值得特别注意的是，实践中，算法备案与大模型备案存在交叉但各有侧重。前者关注算法机制本身的透明度与安全性，后者聚焦生成式服务的整体合规。对于同时涉及两类服务的 AI 企业，需确保“双

[3] 796 款生成式人工智能服务完成备案，新华社，2026 年 03 月 17 日。

[4] 《生成式人工智能服务管理暂行办法》，国家互联网信息办公室，2023 年 07 月 10 日。

[5] 国家互联网信息办公室关于发布生成式人工智能服务已备案信息的公告，中国网信网，2024 年 04 月 02 日。

[6] 《互联网信息服务算法推荐管理规定》，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局令第 9 号，2022 年 03 月 01 日起施行。

[7] 《App 推荐算法用户权益保护技术要求及测评规范》，电信终端产业协会，2022 年 11 月 25 日。

备案”齐备，避免遗漏。

（三）ICP 许可与备案：互联网经营的“资格证”

ICP（Internet Content Provider）许可与备案制度由《互联网信息服务管理办法》（国务院令第 292 号）确立。根据该办法，互联网信息服务分为经营性与非经营性两类：经营性服务实行许可制度（即 ICP 许可证）以及非经营性服务实行备案制度（即 ICP 备案）。

AI 企业并非必然落入 ICP 许可与备案制度的监管范围。根据我们的项目经验，若企业仅从事模型研发、训练，通过私有化部署向企业客户交付模型能力（不涉及互联网信息服务），或仅作为技术提供商向其他企业授权模型使用权而不直接面向终端用户，则可能无需办理 ICP 许可或备案。然而，如果 AI 企业通过互联网（网站、APP、小程序等）向上网用户直接提供信息服务，无论该服务是免费还是收费，均需履行相应 ICP 手续（ICP 许可或 ICP 备案）。

ICP 许可与备案制度本身系由来已久的监管框架，针对该类监管的具体要求不再做具体阐述。但值得注意的是，鉴于中国互联网信息服务领域对外资实行准入限制（根据《外商投资准入特别管理措施（负面清单）》及《外商投资电信企业管理规定》，除少数例外，互联网信息服务仍属外资限制类业务，经营增值电信业务（互联网信息服务（ICP）属于增值电信业务第二类）[8]的外商投资电信企业的外方投资者在企业中的出资比例，最终不得超过 50%），在 AI 企业采用红筹架构进行出海布局的情况下，AI 企业需视是否要取得 ICP 等增值电信业务资质以及结合后续上市进展和监管要求，统筹规划其股权架构安排。

二、数据安全：业务发展之根本保障

AI 企业的数据合规风险贯穿 AI 企业的全生命周期，数据合规风险集中于两个核心场景：一是模型训练阶段的语料数据合规，二是面向客户提供服务时的数据合规。

（一）训练阶段数据合规：语料训练的“源头治理”

《暂行办法》第七条明确要求，服务提供者开展预训练、优化训练等训练数据处理活动，应当“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、行政法规规定的其他情形”。

通过公开渠道查询审核问询函可见，证监会在 AI 企业上市审核中对此问题高度关注。以旷视科技（科创板 IPO）为例[9]，证监会要求其说明“数据收集方式及其合法合规性”；对智谱华章、硅基智能等企业，证监会问询问题均涉及“训练数据的收集规模及来源合法性”。由此可见，AI 企业的训练数据来源合法性是 AI 企业无法规避的数据合规问题，语料数据来源合规已成为 AI 企业上市的实质性审核要点，在法律尽职调查中亦会受到重点核查，值得 AI 企业核心重点关注并合规自查。

根据我们的项目经验，目前 AI 企业的语料数据获取主要依赖四类渠道，基于不同渠道，AI 企业的合规自查关注要点亦存在区别，我们具体梳理如下：

[8] AI 企业主要可能涉及的经营增值电信业务系互联网信息服务，但不排除部分 AI 企业基于其自身业务形态可能需要取得其他的增值电信业务许可。

[9] 《关于旷视科技有限公司首次公开发行存托凭证并在科创板上市的发行注册环节反馈意见落实函之回复》，旷视科技有限公司，2021 年 5 月。

语料数据获取渠道	具体内容	合规自查要点
开源语料与公开数据收集	通过 GitHub 或学术数据集等获取	需确保所使用语料数据的开源许可协议的合规性，以及避免语料中混杂的受版权保护内容。
从网络爬取或抓取的数据	通过爬虫技术抓取公开网页数据	需避免在抓取过程绕过反爬虫机制，以及关注被爬取的数据的商业化可能相关的反不正当竞争风险。
商业采购与数据合作	向第三方数据服务商采购或与其他平台合作获取	■ 需确保授权链条的完整性； ■ 数据买受人对数据来源负有审慎注意义务，明知或应知数据涉及商业秘密仍予接收使用的，需与数据提供者承担共同侵权责任； ■ 通过 API 接口获取数据用于训练时，需确保相关服务协议明确允许此类使用，避免超出授权范围。
合成数据	通过算法生成构造训练数据	需关注生成数据本身是否基于原始数据训练而来，进而关注前述语料数据相关合规要点是否满足。

（二）服务阶段数据合规：运营中的动态风控

当 AI 企业向客户提供服务时，数据处理进入收集、存储、使用的管理周期，AI 企业的合规自查应当聚焦于如下方面：

数据处理环节	关注原则	合规自查要点
数据收集环节	合法性与最小必要原则	■ AI 企业在提供服务过程中收集的用户输入提示词、生成内容、用户画像等数据，需在产品界面显著位置告知用户收集范围、目的及使用方式，并取得用户同意； ■ 不得收集与服务无关的用户信息（如无关的通讯录、位置信息）等。
数据存储环节	境内外数据隔离原则	■ 境内用户数据原则上应在境内存储，确需向境外提供的应当通过安全评估或签订标准合同； ■ 采用地理隔离存储架构，将中国境内与境外用户数据物理隔离，规避数据跨境传输风险。
数据使用环节	目的限制原则	■ 向客户提供服务过程中收集的数据只能用于服务提供目的，不得超范围用于模型训练或商业化分析，除非重新取得用户同意； ■ 需建立数据分类分级保护制度，对可能构成重要数据（如特定行业训练数据、大规模个人信息集合）或核心数据的，履行重点保护义务； ■ 需注意在跨境业务开展过程中是否存在境外调用的情形，需严格遵守《个人信息保护法》项下关于向境外提供个人信息的相关规定。

三、知识产权：业务发展之核心资产

相较于传统企业，AI 企业既面临核心知识产权归属清晰等传统企业涉及的共性风险，也因其独特的业务业态，产生知识产权衍生成果归属、技术出境管制等新型风险。该等风险是法律尽职调查中需额外关注的重点，AI 企业亦需在合规自查过程中予以特别关注。

（一）衍生成果归属

AI 企业的知识产权保护需超越传统的专利、商标、著作权登记，深入业务场景中的衍生知识产权归属安排。当前 AI 企业向客户提供服务主要采用两种模式，衍生知识产权归属风险各异：

模式类型	具体内容	合规自查要点
私有化部署模式	企业向 B 端/G 端客户提供本地化模型部署服务，客户基于基础模型进行微调产生衍生模型	需在服务协议中明确： ■ 微调产生的模型权重、参数优化成果的归属方； ■ 客户是否获得衍生模型的完整所有权或仅享有使用权； ■ 企业是否有权将客户优化成果用于其他客户或基础模型迭代（若约定不明，企业可能丧失对核心技术演进路径的控制权，或面临客户主张衍生模型独立知识产权的纠纷）。
API 服务模式	企业通过接口向客户提供 AI 能力，客户基于 API 开发应用	需在服务协议中明确： ■ 输出内容的知识产权归属客户还是企业； ■ 企业对客户输入数据的合理使用范围； ■ 因客户输入数据侵权导致的企业免责条款。

（二）技术出口合规

根据《中国禁止出口限制出口技术目录》，“基于数据分析的个性化信息推送服务技术”、“智能语音交互技术”、“语音合成技术”等与大模型相关的技术已被明确列为限制出口技术。同时，《技术进出口管理条例》规定，限制类技术出口需经省级商务主管部门审批，取得《技术出口许可证》后方可对外转让。

在 AI 企业业务开展过程中，AI 企业向海外提供与上述技术相关的服务可能构成“技术出口”的情形，具体体现在向海外子公司或合作伙伴授权使用基础模型；在境外部署服务器时传输模型架构、源代码或训练框架。这些行为若涉及限制出口目录内的技术，均需履行出口许可，否则可能面临行政处罚。

据此，如 AI 企业涉及前述情形，则应当将相关技术出口手续是否完成作为合规自查的一个核心重点。

四、股权架构：业务发展之核心基石

在上一篇文章*《AI 企业出海（一）：全球股权架构搭建策略》*中，我们已系统介绍了 AI 企业出海常见的股权架构模式。就 AI 企业出海过程中所搭建的股权架构亦是法律尽职调查中核心关注的内容之一。本节仅重点提示在红筹架构以及平行架构下所需关注的核心要点：

（一）红筹架构下的关注要点：37 号文登记与 ODI 手续

1. 37 号文登记

对于采用红筹架构的 AI 企业，37 号文登记是创始人及中国籍自然人股东必须完成的前置合规程序。

根据国家外汇管理局《关于境内居民通过特殊目的公司境外投融资及返程投资外汇管理有关问题的通知》（汇发〔2014〕37 号）（“**37 号文**”），境内居民个人以境内外合法资产或权益向特殊目的公司（BVI 公司）出资前，应向外汇管理局申请办理境外投资外汇登记手续。在实践中，37 号文的办理进度将直接决定红筹架构的搭建进度，进而对融资交割取得融资款的进度产生直接影响。

因此，对于初创并且计划采取红筹架构的 AI 企业而言，其应当在与投资人接触的初期尽快启动 37 号文已经对应红筹架构的搭建工作，以避免因此导致融资交割的延后。

2. ODI 手续

根据《企业境外投资管理办法》（发改委令第 11 号）及《境外投资管理办法》（商务部令 2014 年第 3 号）及《境内机构境外直接投资外汇管理规定》（汇发〔2009〕30 号），境外直接投资（“**ODI**”）手续实行发改委核准/备案、商务部核准/备案以及外汇登记的监管框架。

若采用红筹架构的 AI 企业存在境内机构投资者，且该等境内机构投资者无适当的境外关联方，则该等境内机构投资者需履行 ODI 手续，以实现其在 AI 企业红筹架构中的境外融资主体之上持股。若 AI 企业直接通过境外直接投资设立海外子公司的方式实现出海布局，则该等 AI 企业亦需履行 ODI 手续。

（二）平行架构下的关注要点

平行架构因其实现了境内外业务风险的物理隔离，在 AI 出海企业中具有特殊意义，但其也带来了如下特殊的法律尽职调查关注点：

- 融资范围的完整性确认：需首先确认该次融资的尽调范围，即以平行架构中境内外业务所涉的境内外两套架构为统一整体进行融资，覆盖境内外全部权益，还是境内外架构彼此独立、分别融资。尽调范围的认定将直接决定 AI 企业法律尽调合规审查的范围以及该次融资交易文件条款设计上的差异。
- 股东身份与关联关系核查：需穿透核查境内外两套架构的股东是否完全一致，是否存在非关联第三方仅持有境内或境外单一架构股权的情形。如果构成关联关系，则境内外两套架构之间的商业合作将构成关联交易，亦需考虑该等关联交易对 AI 企业未来上市的影响。
- 创始人的实际控制权确认：需确保创始人对平行架构框架下境内外两套架构的统一控制。

五、结论及建议

本文所梳理的业务资质、数据安全、知识产权保护与合规以及股权架构问题共同构成了 AI 企业在融资过程中法律尽职调查的主要核心关切。这些合规问题并非孤立存在的，而是相互交织、动态影响的，因此，AI 企业需在出海布局启动前完成系统性的合规论证，将法律尽职调查从被动应对的“检查清单”转化为主动自查的“战略工具”。

要强调的是，本文所提示的法律尽职调查重点关注问题仅为 AI 企业的共性核心法律风险。AI 行业日新月异，各个 AI 企业所处的细分赛道、融资阶段、目标市场及股东结构也不尽相同，因此各个 AI 企业所对应的法律风险以及法律尽职调查要点的优先级亦不相同。我们建议 AI 企业在合规自查过程中，结合企业自身业务实际与发展规划，在专业法律顾问的协助下量身定制切实可行的合规方案。

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：

刘夏艺

电话： +86 10 8516 4158
Email： xiayi.liu@hankunlaw.com

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com