

汉坤法律评述

2026 年 8 月 24 日

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

云上方圆（三）：当算力成为交易标的 — AI 算力市场的业务模式与合规边界

作者：权威 | 段志超 | 郑博 | 王雨婷

一、AI 算力如何成为一项独立交易

过去，企业讨论云服务，通常围绕云主机、云存储、数据库、中间件和 SaaS 系统展开。进入大模型时代后，交易对象发生了明显变化。越来越多的合同开始围绕 GPU 服务器、专属算力池、智算平台、模型训练环境、推理 API、MaaS 服务和 AI 应用平台展开，“算力租赁”“智算服务”和“模型服务”逐渐成为独立的商业品类。

AI 算力也不再只是少数大模型公司的内部资源。它正在成为一种可以标识、计量、调度、租用和对外提供的市场化资源。算力交易可能同时包括硬件资源、调度平台、训练环境、模型能力和运维服务，法律关系也因此更为复杂。本文将从市场中的主要交易结构入手，分析 AI 算力业务的准入、数据、知识产权和合同问题。

二、AI 算力市场的参与主体与交易形态

（一）参与主体

与传统云服务相比，AI 算力市场的参与主体更为多元，大致包括以下几类：



同一主体可能同时持有智算中心资产、运营算力服务并提供 MaaS 接口。角色叠加意味着，其可能同时受到多类监管规则约束。分析具体交易时，需要先明确目标主体实际提供哪些服务、控制哪些资源并承担哪些责任。

（二）典型交易形态

从客户购买的对象看，AI 算力交易大致可分为四类，不同交易形态对应的控制结构和责任边界并不相同，具体见下图。

AI算力市场的交易结构与合规边界

HAN KUN

业态类型	业态特征	核心内容	法律视角关注要点
GPU服务器租用、裸金属GPU、GPU云主机或专属算力池	偏资源层	客户获得一定时间内对特定算力资源的使用能力。服务提供方通常控制数据中心、网络、电力、服务器、GPU设备和资源调度系统，客户则在约定范围内使用相关资源进行训练、微调、推理或其他计算任务	法律关注要点接近IaaS，即底层资源由谁控制，算力可用性如何定义，资源无法交付或性能不足时如何承担责任
AI训练平台、智算平台、模型开发平台或机器学习平台	偏平台层	不仅提供GPU资源，还提供任务调度、镜像环境、框架支持、数据集管理、模型训练、模型评估、推理部署等能力。客户在使用过程中不再只是调用GPU资源，还会依赖平台提供的运行环境和技术路径	法律关注要点接近PaaS，即平台规则、调度策略、版本兼容、训练任务中断、数据集管理和模型产物导出，前述要素都会影响客户对服务的实际控制能力
MaaS、模型API、推理API或智能体服务	偏模型层	客户不一定直接接触GPU资源，也不一定自行搭建训练环境，而是通过接口调用模型能力，获取文本、图片、代码、语音、视频或决策辅助等输出。其核心已经从算力资源供给，进一步延展到模型能力供给	区分模型能力提供方、推理完成方，并同时关注提示词和输出的处理方式、日志留存方式、模型升级是否影响输出稳定性，以及面向公众提供服务时是否需要适用生成式人工智能相关规则
面向行业场景的AI应用或AI SaaS	通常为SaaS与MaaS的叠加	例如智能客服、智能办公、代码助手、风控模型、工业质检、医疗辅助、营销内容生成等。这类服务通常将底层算力、模型能力和软件功能进一步封装，客户看到的是一个可直接使用的业务功能	除云服务本身的资源和系统控制问题外，还会进一步涉及内容合规、个人信息保护、行业准入、模型备案和输出责任

- AI算力市场典型交易形态 -

算力调度或交易平台虽然未必直接提供算力，但可能参与供需撮合、统一结算和资源归集，其责任边界需要单独判断。本文第三部分将进一步讨论。

三、AI 算力市场参与方适用的准入资质判断逻辑

本系列第二篇已经梳理了云服务涉及的增值电信业务许可，并讨论内部自用与对外经营、一次性交付与持续服务、代理销售与实际经营三组边界。这一框架同样适用于 AI 算力业务。下文仅分析 AI 算力交易中的新增问题。

（一）GPU 租赁与智算平台：是否构成互联网资源协作服务

对于 GPU 服务器租赁、云上 GPU 实例、专属算力池和 AI 训练平台，准入判断的重点是其是否构成 B11 互联网数据中心业务项下的互联网资源协作服务。按照《电信业务分类目录（2015 年版）》的定义，可以从以下四项进行判断：

1. 是否利用架设在数据中心之上的设备和资源：智算中心内的 GPU 集群、高速网络和存储系统通常满足该要件；
2. 是否通过互联网或其他网络提供服务：通过专线、VPN 或 API 向客户开放算力资源亦在其列；
3. 是否以随时获取、按需使用、随时扩展、协作共享等方式提供：按卡时计费、弹性扩缩容、任务排

队调度均属典型形态；

4. 所提供的是否为数据存储、互联网应用开发环境、互联网应用部署和运行管理等服务：模型训练环境、镜像管理、任务编排和推理部署与该等表述具有较高的结构相似性。

如果上述要素均具备，相关业务原则上应在取得 B11 互联网资源协作服务许可后开展，具体仍需结合实际服务形态判断。

反之，以下两类场景通常不构成 B11 业务：一是企业自购 GPU 服务器用于内部模型训练，属于内部资源使用；二是系统集成商一次性交付 GPU 集群或私有化训练环境，并将系统控制权移交客户，属于项目制交付。

值得提示的是，在算力场景中，“内部自用”与“对外经营”之间还存在一类边界形态：集团算力共享平台向参股公司、生态伙伴或外部研发合作方有偿开放。一旦使用方超出集团合并范围且存在对价安排，相关服务则存在被认定为对外经营的可能，需要结合主体关系、计费方式和服务承诺具体评估，必要时可以调整交易结构。

（二）算力转售、代采与白标平台：是否实质参与经营

在 GPU 资源阶段性紧缺的背景下，市场上出现了大量“算力代采”“算力包转售”“白标智算平台”安排。判断此类主体是否实质参与经营，可以重点核查：算力销售方和合同签署方；可用率、交付时间和排队规则的承诺方；账号开通、资源分配和调度策略的控制方；服务费收取方和发票开具方；故障和安全事件的响应方。如前述重点事项均由同一主体承担对应责任，则该主体即使不持有任何 GPU 设备，也存在被认定为实际经营互联网资源协作服务的风险，需要对业务模式进行进一步分析。

（三）算力调度与交易平台：区分撮合与转售

算力调度和交易平台是近年出现的新角色。近年来，多地政府推动建设区域算力调度平台并配套发放“算力券”等补贴工具；《算力互联互通行动计划》进一步提出建设国家、区域、行业三级算力互联互通平台，开放算力标识检索、状态感知、供需匹配等调度能力。“算力供需对接”本身正在成为一种业务形态。

在服务定性层面，如果平台仅提供算力资源信息发布、标识检索、供需匹配和撮合服务，由算力供给方与需求方直接缔约、直接结算，平台更接近信息服务或居间服务：视其功能形态，可能涉及 B25 信息服务业务；提供在线交易处理能力的，还可能涉及 B21 在线数据处理与交易处理业务。如果平台以自己名义向需求方销售算力、统一定价、统一结算，并对算力可用性承担责任，则其实质已经转向算力转售或互联网资源协作服务经营，应回到前述（二）的框架判断。对于入驻政府算力平台、承接算力券结算的企业而言，还需要关注地方政策对入驻服务商资质条件、结算路径和价格机制的具体要求。

四、MaaS 与模型 API 的合规要求

与 GPU 租赁和智算平台相比，MaaS 和模型 API 的法律结构更为复杂。客户购买的不是可见的硬件资源，也不一定直接使用训练环境，更多情况下其需要的服务是持续调用某一模型能力，即客户输入提示词、业务数据或任务指令，服务提供方通过模型推理生成输出并返回结果。整个过程中，底层算力、模型参数、推理调度、内容安全和日志记录通常均由服务提供方或其上游技术方控制。

（一）应先区分服务场景和主体角色

判断适用规则前，需要先回答两个问题。

1. 服务对象：面向境内公众还是仅供企业内部使用

《生成式人工智能服务管理暂行办法》适用于利用生成式人工智能技术向中华人民共和国境内公众提供生成文本、图片、音频、视频等服务；行业组织、企业、教育和科研机构等研发、应用生成式人工智能技术，未向境内公众提供生成式人工智能服务的，不适用该办法。据此，企业内部调用模型 API 进行代码生成、知识库问答、客服辅助或文档处理，与面向境内公众开放生成式 AI 产品，在规则适用上存在实质差异：前者更接近企业内部工具或 B 端能力调用，重点在数据安全、个人信息保护、保密和知识产权问题；后者则需要落实生成式 AI 服务提供者的全套义务，包括训练数据来源管理、生成内容安全、个人信息保护、内容标识和投诉处理机制等。

2. 主体角色：服务提供者还是技术支持者

在算法推荐、深度合成和生成式人工智能规则体系下，“服务提供者”与“技术支持者”承担的义务并不相同。MaaS 服务商如果只向下游企业输出模型能力，由下游企业组装为面向公众的产品，其更接近技术支持者角色，面向公众的内容安全、标识和投诉处理等义务原则上由作为服务提供者的下游企业承担。但是，如果 MaaS 服务商直接面向公众开放对话或生成入口，其自身即构成服务提供者。实践中，同一模型能力往往沿“模型厂商—MaaS 平台—应用开发者—最终用户”的链条逐层传递，每一层主体都需要单独判断自身角色和义务，也同时需要承接其他层主体带来的责任和义务转嫁，我们建议在对应的合同中应当预留该等责任分配的条款。

（二）常见合规义务及实操建议

1. 备案与登记：“双轨制”适用

根据《生成式人工智能服务管理暂行办法》第 17 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。

从国家网信办历次公告及备案实践看，相关程序已形成“备案”与“登记”双轨：使用自研或经过微调训练的模型、面向公众提供服务的，需通过属地网信部门履行生成式人工智能服务备案（实践中常称“大模型备案”），提交上线备案申请表、安全自评估报告、模型服务协议、语料标注规则、关键词拦截列表、评估测试题集等材料；直接调用已备案模型能力、未对模型本身进行再训练或微调的服务（典型如基于已备案大模型 API 开发的应用），则适用相对简化的登记程序。国家网信办在生成式人工智能服务已备案信息公告当中也同时强调，已上线的生成式人工智能应用或功能，应在显著位置或产品详情页面公示所使用已备案生成式人工智能服务情况，注明模型名称及备案号。

实操建议：上游模型已经完成备案且备案持续有效，是下游应用方适用登记程序的前提。因此，MaaS 合同中的陈述保证与持续配合事项里应当纳入上游模型的备案状态、备案号及其维持义务；模型升级或更换底层模型可能触发备案变更或重新登记，亦应纳入合同的变更通知与协助机制。

2. 内容标识义务

《人工智能生成合成内容标识办法》已于 2025 年 9 月 1 日起施行，配套强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》（GB 45438—2025）同步实施。按照该办法，人工智能生成

合成内容需要添加显式标识和隐式标识，服务提供者、提供网络信息内容传播服务的平台和应用程序分发平台分别承担相应义务。

实操建议：对 MaaS 相关交易项下各参与主体而言，标识义务同样存在逐层传导问题：模型层是否在输出中嵌入符合标准的隐式标识（如元数据标识）、应用层是否按要求添加显式标识、标识被删除或篡改时责任如何划分，都需要在技术方案和合同条款中预先安排。

3. 与算法推荐、深度合成规则的交叉

MaaS 还可能与算法推荐、深度合成等规则发生交叉。《互联网信息服务算法推荐管理规定》适用于在中国境内应用算法推荐技术提供互联网信息服务的活动，并将生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类算法纳入算法推荐技术范围；具有舆论属性或者社会动员能力的算法推荐服务提供者，需按规定履行备案手续。涉及深度合成（如换脸、拟声、数字人等）的服务，还需对照《互联网信息服务深度合成管理规定》判断服务提供者与技术支持者的各自义务。

实操建议：建议进一步排查服务与应用场景，区分适用具体监管规则，并在合同条款中进行对应体现。

综上，MaaS 和模型 API 的合规判断应当参考下列路径：先确定自身在服务链条中的角色（服务提供者还是技术支持者），再区分服务面向对象（境内公众还是企业内部），再判断输出内容类型与功能形态（是否涉及生成合成、深度合成、算法推荐），最后对应识别安全评估、备案或登记、内容标识、行业监管及数据出境等具体要求。

五、AI 算力交易中的数据、知识产权和保密风险

与传统云服务相比，AI 算力服务项下的客户输入数据、训练数据、模型产物和输出内容之间的关系更加复杂。在普通云主机场景中，服务提供方通常只提供基础资源；在 AI 训练和 MaaS 场景中，客户数据可能进入数据清洗、标注、向量化、训练、微调、推理、日志分析和安全过滤等多个环节，服务提供方对数据与日志的接触能力明显增强。因此在这一层面，建议重点关注以下四个维度：

- 1. 训练数据和客户数据的边界。**客户上传的数据可能包含商业秘密、个人信息、重要数据、受版权保护内容或第三方数据。若服务提供方仅为客户提供封闭环境和计算资源，通常更接近受托处理或技术承载关系；若服务提供方拟将客户输入、提示词、标注结果、训练样本或反馈数据用于自身模型训练或服务优化，则需要取得明确、具体的合同授权，但考虑到格式条款本身具有效力瑕疵，我们建议这部分的约定可以使用更细的颗粒度。
- 2. 模型产物和权利归属。**客户可能通过平台训练形成微调模型、LoRA 权重、向量库、提示词模板、业务知识库或输出内容。相关权利由谁享有、客户是否可导出、导出的格式是否可在其他平台复用、服务提供方是否可复用相关产物、服务终止后是否删除及如何验证删除，均需要在合同中明确。否则，一旦客户迁移平台或发生商业争议，很容易出现模型资产和数据资产边界不清的问题。
- 3. 输出内容责任。**MaaS 或 AI SaaS 可能生成文本、图片、代码、音频、视频或决策建议。服务提供方通常希望将输出的使用责任交由客户承担；客户则希望服务提供方至少承担模型服务合规、基础安全过滤、明显违法内容防控和故障响应义务。双方责任如何分配，需要结合服务对象、功能形态、输出控制能力和合同约定综合判断。
- 4. 数据出境和境外技术支持。**部分 MaaS 或 AI 算力服务可能涉及境外模型、境外技术团队、境外日

志分析或跨境 API 调用。判断是否构成数据出境，既需要关注服务器所在地，也需要关注输入端、访问端是否形成跨境路径。这部分的合规义务可以结合此前《促进和规范数据跨境流动规定》及其相关规定中对于数据出境前置流程的豁免规定同步进行判断。

六、AI 算力交易的合同关注要点

AI 算力市场的商业风险，在当前 GPU 资源紧张、模型迭代快、任务调度复杂的背景下需要加以关注，并在合同中作出对应的风险防范安排。我们在下方列举了典型的交易场景及重点条款，但具体可谈空间仍需要回归市场情况进行判断：

- **GPU 租赁和专属算力池：**重点关注设备类型、显存规格、集群规模、网络带宽、存储能力、资源独占或共享属性、交付时间、排队规则、可用率、维护窗口和替代资源。如果涉及到高价值 GPU 设备，则需进一步关注物理设备相关风险并在合同层面进行风险管控，例如权属（含第三方权利）、出口管制等供应链因素等。
- **AI 训练平台：**重点关注训练环境、框架版本、镜像管理、任务调度、断点恢复、训练失败重跑、数据集隔离、模型产物归属、导出机制和平台兼容。考虑到训练任务通常耗时较长且失败成本较高，“任务是否成功完成”与“资源是否曾经可用”之间需要明确区分，可用率达标并不等于训练成功，建议对于二者对应的责任和救济分别约定。
- **MaaS 和模型 API：**重点关注调用量、并发数、响应时间、模型版本、版本升级通知、输出过滤、敏感内容处理、日志留存、输入数据是否用于训练、备案与登记状态的陈述保证、内容标识的技术配合，以及终止后的数据删除。模型能力的稳定性不能只用传统可用率衡量，输出一致性、版本透明度和接口兼容也应纳入合同治理。

七、结语

AI 算力市场是云服务在人工智能时代的延伸，也是数据中心、GPU 供应链、模型服务、数据治理和行业应用共同作用下形成的新型市场。尽管 GPU 租赁、智算平台、模型 API、MaaS 和 AI SaaS 在商业表达上各不相同，但其共同基础仍然是外部能力的持续供给，只是延伸到了不同的层级，例如资源层、平台层、模型层和应用层。随着业态的不断迭代与融合，单一主体参与此类交易时所适用的具体合规义务与权责事项也需要结合服务和能力边界进行个案分析。无论市场“冷”还是“热”，清晰的权责边界对于每一交易链条参与方而言都是管控风险、长期稳健发展的前提。

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：

权威

电话： +86 21 6080 0946

Email: wei.quan@hankunlaw.com

段志超

电话： +86 10 8516 4123

Email: kevin.duan@hankunlaw.com