HANKUN

汉坤法律评述

2026 年 9 月 3 日

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

汉坤具身智能数据合规与治理系列（五）：生态治理

作者：陈文昊 | 原舒仪 | 李诗

摘要

一台具身智能设备通常由机器人厂商、模型公司、云平台、芯片和传感器供应商等共同提供，并经系统集成商、经销商或运营商进入客户场所，客户还可能允许设备或 Agent 访问内部数据和业务系统。本文所称“客户”，是采购、部署或运营产品或服务的主体；“用户”是实际操作、使用设备或接受服务的人员。因此，同一产品往往同时涉及数据处理、模型调用、设备控制和多主体责任。

企业即使已经开展数据来源审查、场景化评测并设置 Agent 权限和人工控制，相关措施仍可能因第三方接口、模型更新、经销部署或客户配置而失效。生态治理的核心，因而是查明各方实际掌握的决定权和控制能力，并据此配置责任。

基于这一思路，本文依次讨论参与主体与责任、接口和第三方治理、数据与模型权益以及全球部署。尽管出口管制和境内外制裁虽不属于数据治理，但会直接影响技术提供、供应商选择、远程更新和跨境交付，本文亦作必要提示。

一、多主体协作如何改变具身智能的合规边界

传统第三方数据合规管理主要关注供应商是否接触个人信息、是否具备安全能力，以及合同是否约定保密和事件处置义务。具身智能还需进一步查明：谁选择模型和决定数据用途，谁配置工具及设备动作权限，谁能够远程更新或停止系统，以及谁掌握还原模型判断、接口调用和设备执行过程所需的证据。要回答这些问题，首先需要理解多主体协作对系统运行方式的影响。

（一）硬件、模型、云服务和现场部署由不同主体负责

具身智能产品通常由多方共同完成：制造商设计本体，上游供应商提供传感器和芯片，模型公司提供基础模型，云平台承载推理，语音、地图和视觉能力通过 SDK 接入，Agent 再借助插件访问客户系统，最后由集成商完成现场部署。由此，各方通常只掌握部分能力和信息，未必存在完整了解系统运行过程的单一主体。

这种分工提高了开发和交付效率，也使责任和证据分散。模型公司可能不了解设备动作，制造商未必能够解释模型更新，部署方和客户又可能改变权限或运行环境。事件发生后，如版本、权限和日志记录不能相互对应，合同中的抽象分工便不足以支持事实还原和责任判断。

（二）接口使数据处理、模型调用和设备控制相互关联

数据的“提供”或“共享”不仅包括数据库导出和文件传输，还可能通过 API 查询、SDK 回传、远程访问、模型输入、RAG 检索、插件调用、参数更新或机器人云平台同步完成。供应商即使“不存储客户数据”，仍可能实时接触图像、提示词、设备状态或工具返回结果。

因此，仅绘制数据流图不足以说明系统如何运行。企业还应记录谁发出指令，指令经过哪些模型、规则和接口，谁可以覆盖安全限制，以及执行结果向谁反馈。只有把数据访问与模型调用、设备动作对应起来，才可能准确识别风险和责任。

（三）同一主体的法律角色可能随活动变化

系统进入具体场景后，各主体的数据处理作用还会进一步变化。例如，工厂、医院、仓库、商场或家庭可能向设备开放场景数据、账户、门禁、订单、生产系统和其他接口，并自行配置知识库、插件、动作范围或更新节奏。此时，客户不仅采购或使用产品，也可能决定部分数据处理目的、接口权限和设备行为。客户决定员工数据的采集目的，制造商基于产品安全处理故障日志，模型公司将输入用于自身模型改进，三者所承担的责任并不相同。因此，企业应按具体场景和处理活动，结合实际决定权与控制能力逐项判断。

二、主体角色与责任：实质大于形式

在明确多主体协作的事实结构后，下一步是分配法律角色和责任。其目的不是指定一个主体承担全部责任，而是确定每项活动由谁作出关键决定、谁能够预防或停止风险、谁保存相应证据。个人信息保护、数据安全、AI 治理和产品责任可以基于相同事实，但各自的法律规则和责任要件不能相互替代。

（一）个人信息处理角色应按具体活动分别判断

个人信息处理角色应当首先按活动区分。依据《个人信息保护法》，企业需判断相关主体是独立决定处理目的和方式、共同决定，还是仅受托处理。判断应以实际处理行为为基础，合同称谓、收费模式、服务器位置或谁先取得数据均不能单独决定结论。

据此，云平台如仅按客户指示提供存储和计算，通常属于受托处理；模型公司如将客户输入用于训练自身通用模型，可能就该训练活动独立承担责任；制造商与客户共同设计员工行为分析功能的，则可能构成共同处理。同一主体在不同活动中可以承担不同角色。

角色确定后，还需将合规义务落实到接口和流程。由谁履行告知、取得必要同意、响应删除请求、决定保存期限、管理跨境访问并通报事件，应与各方实际掌握的数据和系统权限一致。否则，合同上的角色划分难以转化为可执行的合规措施。

（二）AI 与产品责任应结合实际决定权和控制能力分配

除个人信息处理角色外，AI 和产品责任还取决于各方对系统的实际控制。基础模型提供方、Agent 开发者、设备制造商、系统集成商、部署方和运营方之间如何分工，应结合谁选择模型、配置工具和动作权限、决定部署场景、更新或停止系统，以及谁向客户和用户作出性能承诺判断。

在具身场景中，同一事故往往由多个环节共同造成。例如，模型更新改变识别能力、集成商取消安全阈值、客户扩大作业区域或远程运维人员绕过审批，均可能导致危险动作。合同可以约定协作、赔偿和追偿，但不能排除各方依法承担的产品质量、侵权、网络安全、数据安全和监管责任。

因此，责任条款应与实际控制能力相互校验。不具备模型更新能力的一方不宜单独承担底层模型修复义务；不掌握必要记录的一方难以独立完成调查；能够远程控制设备或覆盖安全限制的一方，则应承担相应的审批、记录和事件处置义务。

（三）证据保存应与各方实际控制的环节相对应

责任分配要能够落地，还需要相应证据。数据来源证明、模型和组件版本、权限配置、更新记录、访问日志、设备日志、人工确认和现场记录，可能分别由不同主体掌握。企业应在合作开始前明确证据种类、保存主体、记录格式、调取条件和保存期限，避免事后无法拼合事实。

但日志并非越多越好。记录范围仍应遵守最小必要、商业秘密保护和保存期限要求；同时，关键记录必须足以还原事发时的版本、授权和工具调用情况。二者之间应当通过风险分级取得平衡。

在此基础上，跨主体协查还应预设触发条件和时限，明确谁先保全记录、谁通知其他参与方、谁对接客户和监管部门，以及谁有权暂停模型服务或设备运行。证据保存、权限控制和事件响应相互衔接，合同分工才具有执行基础。

三、接口与第三方治理：将授权边界落实为系统控制

责任边界明确后，还需将其转化为系统控制，而接口正是主要落点。API、SDK、插件、云平台和远程运维通道不仅传输数据，也可能改变模型上下文、长期记忆、设备参数和实际动作。因此，接口治理必须同时考虑数据风险和设备行为后果。

（一）接口应按照数据、模型和设备动作风险分级

企业可以先将接口区分为数据读取、数据写入、模型推理、工具调用和设备控制等类型。只读接口并不必然属于低风险，读取家庭视频、工业参数、重要数据或商业秘密需要严守数据生命周期的合规要求，并防范可能的数据泄露；写入和控制接口可能直接改变模型记忆、设备参数或动作，通样需要更严格控制。

完成类型划分后，还应结合数据敏感性、形成重要数据的可能性、动作可逆性、影响范围、调用频率和外部暴露程度评定风险。高风险接口可采用独立账户、短期凭证、设备或网络绑定、参数允许清单、双重确认、调用限额和异常阻断，避免通用令牌同时覆盖多类高风险能力。

同时，授权应具体到必要字段和功能。例如，故障诊断通常只需设备型号、错误代码和时间戳，导航插件可能只需经模糊化处理的位置。合同中的目的限制应进一步转化为对字段、频次、期限和返回结果的技术限制。

（二）SDK、插件和机器人云平台需要持续治理

接口并非一次授权后即可长期不变。SDK 和插件更新可能增加数据采集、远程通信或工具权限，企业应维护版本和依赖清单，审查代码来源、网络行为、权限变化、许可证、维护状态和安全响应能力，并禁止未经验证的组件接入高权限 Agent 或设备控制器。

对于 Agent，还需防范提示注入经工具和接口扩散。网页、文档或工具返回值可能夹带指令，诱导 Agent 读取其他数据或调用无关接口。企业应区分业务数据与系统指令，结构化处理输入输出，并通过权限网关、规则引擎或隔离环境限制调用范围。

对于云端推理、远程诊断和模型更新，则应采取租户隔离、对外传输数据过滤、更新签名、分批发布和回滚等措施。模型、插件或控制参数发生实质变化时，还应重新评估数据用途、接口权限和设备动作风险，不能以“技术上可用”替代场景验证。

（三）第三方管理应覆盖准入、变更和退出

确定接口和组件风险后，第三方管理才能有明确重点。分级不能只看其是否接触个人信息，还应考虑其能否改变模型、调用工具或控制设备，以及服务中断是否影响生产或人身安全。例如，传感器供应商的固件漏洞可能影响控制，远程运维商则可能同时接触数据并修改设备参数，均可能属于高风险第三方。

在准入阶段，企业应要求与风险相匹配的证据。对高风险供应商，可核验数据处理流程、系统架构、访问角色、分包商、模型版本、训练数据来源、日志能力、漏洞管理、跨境安排和删除机制。集团层面的通用认证只有覆盖具体服务、版本和部署方式，才具有相应证明作用。

合作期间，应通过重大变更通知、定期复评、漏洞和监管通报监测、日志抽查及整改追踪持续管理；合作退出时，则应撤销密钥、远程账户和设备证书，迁移或删除必要数据，并处理缓存、备份、长期记忆和微调成果，确保原供应商不能继续更新或控制设备。

（四）合同约定应覆盖模型、权限和服务功能变化

上述技术控制还需获得合同支持。合同应要求供应商就模型、数据用途、分包商、存储地点、接口权限、安全措施或服务功能的重大变化提前通知，并赋予客户重新评估、限制功能、暂停使用或退出的权利，并且自动更新不得绕过高风险功能审批。

除变更机制外，训练、微调、RAG 和服务改进权限应与履行服务所需的一般数据处理分开约定，数据访问、工具调用和设备动作权限也应分别限定。对关键服务，还可根据业务连续性风险约定替代方案、数据和配置迁移，以及必要的技术资料托管。

事件发生时，条款应进一步明确触发条件、通知时限、证据格式、调查分工、监管和客户协作、漏洞修复、模型回退、设备停用或召回。只有让义务与各方的系统能力和证据掌握情况相匹配，事件安排才具有可执行性。

四、数据与模型权益：训练许可应当单独、具体约定

接口治理解决“如何使用”的问题，数据与模型权益则要回答“是否有权使用”。合同常以“数据归甲方所有”或“项目成果共有”概括全部权利，但相关数据和模型还可能涉及个人信息权益、隐私、商业秘密、知识产权及合同安排。单一所有权表述不足以界定各方能够实施的具体行为。

（一）同一数据可能涉及多类主体和多项权益

同一数据可能同时涉及多类主体。客户拥有设备或场所，不当然可以处分画面中自然人的个人信息；制造商投入算法和硬件，也不当然取得客户运行数据的训练权。合同应分别约定数据的持有、访问、使用、加工、训练、对外提供、经营和删除等具体权限。

关于数据权属的约定，政策文件可以提供合同设计参考。例如，“数据二十条”提出数据产权结构性分置，国家数据局也对数据持有权、使用权和经营权作出解释，但这些概念不能替代个人信息、重要数据、知识产权、商业秘密和合同效力审查。

（二）提供设备服务不等于允许训练通用模型

提供设备或排障服务不等于取得通用模型训练许可。训练条款应明确数据来源和授权主体、数据范围、训练或微调用途、地域和期限，是否允许与其他客户数据混合、形成衍生数据和模型参数、商业化或再许可。不同处理目的不宜由一项概括授权覆盖。

训练许可还应覆盖退出安排，包括数据进入训练集后能否定位和删除、微调参数能否分离、模型输出是否可能复现客户内容，以及个人权利请求或第三方侵权主张由谁处理。这些问题应在合作开始时约定，而非留待终止后协商。

如涉及联合研发，还应分别界定基础模型、微调参数、数据集、标注和评测成果、提示词、开发工具及改进成果。笼统约定“项目成果共有”，通常无法回答由谁部署、许可、开源、向第三方提供或在退出后继续使用。

（三）开源许可和数据资产化不能替代来源审查

开源许可不能替代来源审查。代码或模型许可证通常仅界定相应许可范围，并不证明训练数据来源合法，也不保证输出不涉及第三方权利。企业应分别审查代码、模型、数据集和权重的许可条件，并关注署名、同源开放、用途限制、再分发和商业化要求。

同理，数据资源的会计确认或披露也不等于企业取得不受限制的法律权利。企业推进数据资产化前，仍需审查数据来源和权利基础，以及个人信息、重要数据、知识产权、合同限制、数据质量和删除义务。

可信数据空间、隐私计算或“可用不可见”等技术可以降低原始数据暴露，但不会自动补足法律依据和授权。技术措施仍应与参与方角色、处理目的、使用边界、审计、退出和责任安排结合。

五、全球部署：分别审查数据、出口管制和制裁规则

完成境内合作安排后，产品进入全球市场还会面对不同法域的规则。企业可以建立统一的安全、隐私和 AI 治理基线，再根据市场、用途、主体角色和服务方式增加当地控制；但数据出境合规并不能回答设备、软件、技术或服务能否向特定主体提供，还需考察相关出口管制和制裁规则。

（一）合规审查需结合当地法律和具体场景

尽管涉及不同法域，作为合规工作的方法论，全球部署合规应当覆盖数据最小化、加密、访问控制、供应商管理、模型评测、人类监督、漏洞管理和事件响应。在中国境内部署时，还需结合业务判断个人信息处理基础、重要数据识别和出境路径，以及算法、生成式人工智能服务、内容标识、网络安全等级保护和事件报告等要求。但需要强调的是，进入其他市场后，则应根据用途和主体角色识别当地义务。例如，欧盟《人工智能法案》区分高风险 AI 系统、通用人工智能模型和特定透明度场景；美国等法域还可能适用州隐私法、消费者保护、产品安全和行业规则。

另外，在数据架构上，全球训练也不必以集中全部原始数据为前提。企业可以采用本地清洗、边缘处理、区域训练、联邦学习、参数传输和匿名化统计降低跨境风险；境外访问仍应遵守最小权限、审批和日志要求，并与数据出境结论保持一致。

（二）出口管制审查不限于设备出境

完成数据合规判断后，还需单独审查出口管制。依据中国《出口管制法》和《两用物项出口管制条例》，从境内向境外转移受控物项（包括货物、技术、服务及相关技术资料等数据），或者中国公民、法人和非法人组织向外国组织、个人提供受控物项，均可能构成受管制的出口活动。

具体判断仍应回到管制条目和技术参数。具身智能产品并不因“使用 AI”当然受控，但芯片、传感器、激光器、导航定位、信息安全、无人系统部件及配套软件和技术可能受到管制。样机、备件、境外展览或维修，以及源代码、算法、模型权重、技术文档和远程调试，也不能仅按有形货物审查。

在物项识别和归类基础上，还应核对目的国家或地区、最终用户、最终用途、交易和运输路径及规避风险。需要许可的，合同、技术说明及最终用户和用途文件应与真实交付一致；物项、用户、用途或目的地变化时，应重新判断。

（三）境外出口管制和经济制裁应根据具体连接因素判断

如果供应链含有境外来源的芯片、软件、源代码、云服务或技术，还需判断相关外国规则是否适用于出口、再出口、境内转移、技术访问或人员支持。以美国《出口管理条例》（Export Administration Regulations, EAR）为例，应先判断物项是否受其管辖，再结合归类、目的地、最终用户和最终用途确定是否需要授权。交易方未被列名并不当然意味着无需许可。

制裁审查则不能只搜索客户名称。美国 OFAC 制裁、欧盟限制性措施等是否适用，取决于主体、物项、资金流、服务方式、交易地域和具体项目。企业还应识别所有权和控制关系、实际最终用户、收付款银行、经销和维修主体、云服务租户及服务发生地，并按相关法域的具体标准判断。

由于交易主体、股权结构、最终用途和管制清单均可能变化，筛查应覆盖准入、签约、发货、云服务开通、远程更新、续约和退出。发现疑似名单匹配或其他异常时，应先暂停相关交易或服务，再由有权限的人员复核并决定后续措施。

（四）中国反制和阻断规则要求单独评估法律冲突

境外制裁规则在中国境内执行时，还需考察中国反制裁法律的适用。《反外国制裁法》及其实施规定、《不可靠实体清单规定》等规定了反制措施和相关限制，可能涉及交易、合作、进出口、投资以及数据或个人信息提供。企业进行境外制裁筛查时，应同步核对中国发布的名单和具体公告。

《反外国不当域外管辖条例》（国务院令第 835 号）进一步建立了外国不当域外管辖措施的识别、恶意实体清单、禁执令和救济机制。相关措施经主管部门识别并公告后，组织和个人不得执行或协助执行；特殊情况下确需执行的，应依法申请同意。由此产生的法律冲突不能由境外总部规则单方面解决。

因此，跨国企业不宜将境外总部的制裁规则直接配置为中国业务的自动拒绝条件。境外规则要求停止交易，而中国法可能禁止或限制执行相关措施时，应启动法律评估及适用的报告、豁免或批准程序，不应由业务人员或自动化系统自行决定。

相应地，合同也应保留适用法律和冲突处理空间。笼统要求一方遵守“任何国家的全部制裁”，可能导致合同无法履行或产生中国法风险。条款宜限定在相关法律具有约束力的范围内，并约定冲突时的通知、协商、暂停范围、许可或豁免协作、数据提供边界和退出机制。

（五）将跨境交易审查嵌入产品和交付流程

上述审查应嵌入报价、采购、研发协作、账户开通、设备交付、远程更新和售后服务，而非留到报关或交易末端。企业可以围绕物项归类、最终用户和最终用途、主体筛查、许可状态、交付地域和服务功能设置放行条件。

在系统侧，可将国家或地区、客户、租户、设备序列号、功能模块和更新包关联管理，限制未经批准的下载、远程访问或功能启用，并保留筛查版本、复核理由和放行记录。但技术工具只能执行控制，不能替代适用法律和交易事实分析。

在合同侧，应支持最终用户和最终用途核验，禁止未经授权转移物项或改变用途，并约定重大变化通知、记录与审计、许可协作、暂停交付和合规退出。可能同时适用境内外规则的事项，还应设置统一升级机制，避免不同地区团队作出冲突决定。

六、企业落地：建立六类基础台账并持续更新

为避免上述判断停留在法律意见和合同文本中，企业可以建立六类相互关联的基础台账，分别记录参与主体、数据处理、模型与组件、系统权限、跨境限制以及证据和事件响应，并在模型、供应商、用途、地区或名单状态变化时同步更新。

（一）第 1 类：主体与控制台账

列明制造商、模型公司、云平台、关键组件供应商、SDK 和插件提供者、OEM、ODM、系统集成商、经销商、运营商、客户和开发者，记录合同及分包关系，并说明谁决定数据用途、配置权限、更新系统和停止运行。

（二）第 2 类：数据处理与训练台账

记录各主体可以接触的数据类别、处理目的、法律角色、存储地点、保存期限、训练或改进用途、再提供和跨境情况，并覆盖 API 访问、远程运维、日志、模型输入输出、长期记忆和反馈数据。

（三）第 3 类：模型与组件台账

记录基础模型、世界模型、动作或策略模型、RAG、SDK、插件、控制器和关键硬件的供应商、版本、更新方式、许可证、已知限制和替代方案，使产品实际状态与评测结论、合同约定和对外承诺相对应。

（四）第 4 类：权限与设备控制台账

记录谁可以读写数据、调用工具、修改模型、向设备下发指令、覆盖安全限制、更新固件和实施紧急停止，并将实际权限与用户授权、合同责任和内部审批逐项比对。

（五）第 5 类：出口管制与制裁台账

将可能受控的硬件、软件、技术和服务与目的地、最终用户、最终用途、供应来源和许可状态关联，并记录境内外名单、所有权或控制关系、交易限制、潜在法律冲突及升级节点。

（六）第 6 类：证据保存与事件响应台账

明确数据来源证明、模型说明、筛查和许可记录、访问及设备日志、供应商报告和现场记录由谁保

存，并约定事件发生后证据保全、调查、通知、修复、版本回退、设备停用、召回和监管沟通的责任。

六类台账的价值在于相互关联。供应商更换可能同时改变组件版本、数据处理、系统权限和出口管制归类；客户扩大用途也可能改变个人信息处理角色、模型评测范围、最终用户和最终用途结论。企业应将这些变化设为重新审查的触发条件，经相应业务负责人确认后方可继续交付或运行。

结语：生态治理要求责任与实际控制能力相匹配

综上，具身智能将个人信息、重要数据、模型能力和设备行为置于同一产业协作关系中。隐私保护、重要数据和 AI 治理措施可能因第三方接口、模型更新、经销部署或客户配置而失效。生态治理的作用，就是把相关要求落实到参与方的合同义务、系统权限和操作流程。出口管制和境内外制裁虽然不属于数据治理，但同样依赖对产品、技术、交易主体、目的地、最终用途和服务控制能力的准确掌握。企业如能以一致的产品事实支撑数据治理、模型评测、第三方责任和跨境审查，既能提高事件处置和责任判断的确定性，也有助于提升产品可信度和全球商业化能力。

****

至此，《汉坤具身智能数据合规与治理系列文章》所讨论的四个治理维度形成一套合规方法论的闭环：隐私保护解决个人信息能否合法进入系统，重要数据治理解决关键数据能否汇聚、共享和出境，AI 治理解决模型和 Agent 能否实施安全、可信、可控的行为，生态治理则确保这些要求在各参与方之间持续落实。希望我们的分析能够为中国具身智能行业的数据合规与治理提供一些思路和参考，对行业发展有所裨益。

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：

陈文昊

电话： +86 21 6080 0359
Email： wenhao.chen@hankunlaw.com