汉坤法律评述
2026 年 4 月 13 日

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

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

AI 企业出海（三）：全球出口管制合规与应对策略

作者：刘夏艺 | 蒋睿馨 | 时悦 | 赵晨辰

一、引言

进入 2026 年，AI 已由单纯的技术竞争焦点，演变为国际贸易摩擦与出口管制政策调整的重要领域。围绕先进算力、模型训练、核心算法以及相关技术的跨境流动，各主要法域监管持续收紧，AI 企业的全球化布局正面临前所未有的合规挑战。在 AI 企业出海的征途中，出口管制已不再局限于交易落地前的附属性审查，而逐步成为影响企业研发分工、算力布局、交易结构和全球化路径的重要制度变量。美国围绕先进计算形成的监管框架，正持续向模型训练活动、云算力调用和供应链反规避等环节延伸；中国则在既有技术进出口管理与出口管制制度基础上，对技术跨境流动实施更为审慎的监管。从整体趋势看，监管重心正由单一物项管制，转向算力、模型、技术和交付链条的整体审视，AI 企业的跨境研发、部署与交易安排，正在被纳入更严格的合规约束之中。

本文作为 AI 企业出海系列文章的第三篇，将承接前文关于股权架构与尽职调查的讨论，深入剖析 2025 – 2026年全球 AI 出口管制的最新动态，重点分析中国与美国在 AI 领域的出口管制规则及其演进趋势，并就企业如何构建系统化合规体系提出实务建议。

二、中国技术出口管制：从“限制目录”到“实质性出境”

中国对 AI 技术跨境转移的监管，主要涉及两套并行但并不完全重合的规范体系：一是《对外贸易法》《技术进出口管理条例》及《中国禁止出口限制出口技术目录》（简称“**《目录》**”）项下的限制出口技术许可管理；二是《出口管制法》及其配套制度项下，对特定两用物项、技术及相关服务的出口管制制度。2025 年以来，监管机构对 AI 核心技术的穿透式审查趋势愈发显著，不仅关注所有权的变更，更关注技术能力的实质性外移。

（一）限制出口技术的核心范畴

根据 2023 年底修订并持续施行的《目录》，多项与生成式 AI 密切相关的技术被列为“限制出口”类别。这意味着企业在向境外提供相关限制出口的技术或服务时，必须事先取得省级商务主管部门的许可。

限制出口的技术领域	目录编号	关键管控内容
信息处理技术	086501X	基于数据分析的个性化信息推送服务技术

限制出口的技术领域	目录编号	关键管控内容
计算机网络技术	086302X	巨型计算机（运算次数≥97 万亿次）网络系统、并行处理技术
计算机通用软件编制技术	086502X	巨型计算机（运算次数≥97 万亿次）软件技术； 并行计算机的微内核和多线程的实现技术，程序并行性识别技术及并行优化编译源程序

（二）“实质性出境”的认定困境

在 AI 企业出海实践中，最令创始人困惑的往往是：如果不涉及源代码的物理移交，仅仅是境外授权或团队外迁，是否构成“技术出口”？

根据我们的实务观察，监管机关在判断相关安排是否构成技术出口时，已逐步从单纯关注技术载体的物理出境，转向更加关注技术能力是否发生实质性跨境转移，监管重点在于是否发生了受规制的“技术转移”。以下三种典型场景极易触发合规红线：

- **核心团队整体外迁：**如境内研发团队整体迁往境外，并在迁移过程中伴随境内形成的核心算法、训练框架或相关技术资料被境外主体实际取得、持续使用或控制，则相关安排存在被认定构成技术跨境转移或技术出口的风险。
- **跨境授权与模型部署：**将境内训练的基础模型权重、算法模块、训练框架或其他相关技术资料授权或提供给境外主体使用，或在境外服务器上部署涉及限制出口技术的推理引擎，且在该等部署过程中向境外主体提供模型权重、算法模块、接口能力或其他技术资料，从而使境外主体能够实际获取或利用相关技术能力。
- **穿透式并购审查：**在涉及境外主体收购境内 AI 企业、研发团队或核心技术资产的交易中，如交易安排实质导致限制类技术向境外买方或其控制下主体转移，相关监管机构可能结合交易结构、交割安排及后续控制关系，对交易是否涉及限制类技术的变相出口进行实质性评估。

三、美国 EAR 新规：从先进芯片管制，转向模型训练与供应链执法强化

（一）先进计算规则仍是美国 AI 管制主干

美国当前针对 AI 和算力的出口管制，核心框架仍是 2022 年 10 月与 2023 年 10 月两轮先进计算规则。这两轮规则通过对满足阈值的高性能芯片及其整机、相关软件与技术实施许可管制，并结合最低减让标准（de minimis）与外国直接产品规则、最终用户/最终用途管制及清单工具，构成了美国当前限制中国获得先进 AI 算力的核心制度框架。对 AI 企业而言，美国规则的核心已不再是对个别芯片型号的零散限制，而是围绕先进算力能力建立起覆盖芯片、服务器、软件技术及相关交易链条的综合管制框架。具体解读请见我们之前发布的《*汉坤 • 观点 | AI 管制前沿 — 美国出口管制政策观察*》。

（二）监管重点进一步延伸

在此基础上，美国监管重点近两年明显进一步前移。2025 年 1 月，美国工业和安全局（简称“**BIS**”）在《人工智能扩散框架》中曾将监管范围从先进计算芯片延伸至 AI 模型训练和模型成果本身，其中新增 ECCN 4E091，拟将特定先进闭源 AI 模型权重纳入管制，主要针对训练计算量达到 10^26 次运算及

以上的模型权重[1]。虽然该规则已于 2025 年 5 月被撤销，但 BIS 同期又发布了围绕 AI 模型训练、先进计算芯片反转用以及一般禁令十（GP10）适用的多份政策文件[2]，进一步表明美国对 AI 的管制重点，正在从单纯的物项控制，延伸至模型训练活动、云算力/IaaS 场景、供应链来源以及第三方规避风险。

（三）2026 年新动态

2026 年 1 月，BIS 发布最终规则《关于先进计算商品许可审查政策的修订》，对 H200 等特定芯片对华出口许可审查政策作出有限调整，在特定条件下由“推定拒绝”调整为“逐案审核”。但该调整仅属有限放宽，且附带严格条件，包括确保美国供应优先、禁止用于军事最终用户等。对企业而言，美国出口管制规则仍保持高压态势，仅在个别商用品类上保留了有限的政策弹性。

2026 年 1 月，美国众议院通过《远程访问安全法案》，旨在填补此前通过云服务绕开硬件管制的“法律漏洞”。该法案拟通过修订《出口管制改革法》（ECRA），将特定“远程访问”场景更明确地纳入出口管制法授权范围，以填补通过云服务远程获取受控算力的监管缺口。截至本文成稿日，该法案仍处于立法程序中，尚未成为生效法律。

四、实务建议：构建多维度合规体系

面对日益严峻的出口管制环境，AI 企业不能心存侥幸，必须建立一套动态、敏捷的合规管理体系。结合当前监管重点，建议重点把握以下几方面：

（一）明确境内外主体分工及技术边界

企业在规划出海布局时，需尽早明确境内外主体各自承担的研发、训练、部署及运营职能，重点厘清哪些环节涉及境内研发形成的核心算法、训练框架、模型能力及其他关键技术成果。对于可能落入中国技术出口或出口管制范围的内容，需重点评估其是否会通过授权许可、技术支持、联合开发、境外部署等方式，向境外实现实质转移；针对境外主体，应要求其在所在法域的合规框架内，独立开展应用开发、本地化运营及相关交付工作，避免因境内技术介入或技术能力跨境转移，引发中国技术出口与境外出口管制的叠加监管风险。

（二）重点核查算力来源、训练活动和技术流转安排

AI 企业出海的核心合规风险，往往集中在底层算力获取与技术流转路径上。其中：

- 就算力层面而言，需提前核查 GPU、服务器及云算力的来源渠道、交易路径、服务商背景及相关限制条件，避免在算力来源不明、交易路径不清或合规条件未明确的情况下推进相关合作。
- 就模型训练活动而言，需结合具体业务场景，判断是否涉及敏感最终用途、特殊客户背景及其他监管关注场景，不可仅从硬件采购角度简单理解出口管制风险。
- 就技术流转而言，若境内形成的算法、模型参数、训练方法、技术文档及相关支持服务，需由境外主体持续使用，需同步评估中国技术出口、数据跨境流动及相关知识产权的合规风险，提前做好应对安排。

[1] https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion。

[2] https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens。

（三）加强最终用户及第三方合作管理

企业应关注最终用户、实际控制方、总部所在地以及底层服务提供方等因素。建议建立动态筛查机制，定期核查美国外国资产控制办公室（OFAC）制裁名单、BIS 实体清单（Entity List）等相关限制名单，并结合具体交易背景持续更新客户和合作方风险画像。对于客户身份不清、用途说明模糊、交易路径异常，或存在第三方代采、代持、代用等迹象的情形，应提高尽职调查及合规审查等级，并在必要时审慎评估是否暂缓或终止相关交易安排。尤其在境外云算力、第三方服务商或合作伙伴参与的安排中，交易链条越长，越有必要进一步核查服务商身份、总部所在地、底层算力来源、用途说明、再转让限制及终止机制；对于涉及技术合作、数据共享或模型部署的合作安排，也建议在合同中明确出口管制、数据合规和用途限制条款，并结合项目情况设置必要的通知、暂停和终止机制。

（四）将合规要求嵌入项目设计和交易文件

对 AI 企业而言，更高效的合规路径，往往不是事后整改补救，而是在项目启动阶段，同步评估相关安排是否可能触发中国技术出口管理、美国先进计算管制、数据跨境流动规则及第三方供应链合规风险。与此对应，算力采购、模型训练、技术授权、境外部署及联合开发等各项安排，均应在交易结构设计和合同文本中，嵌入必要的出口管制、数据合规及用途限制等合规管控条款，从源头降低后续调整成本与执行风险，确保项目合规推进。

五、结论

在 2026 年的全球 AI 竞争中，合规能力已成为企业的核心竞争力之一。出口管制不再仅仅是法务部门的日常工作，而是需要企业在战略决策层面予以高度重视的顶层设计。先行一步的合规规划，不仅能为企业赢得宝贵的时间窗口，更能避免因违规而导致的断供风险或巨额罚单。在全球监管环境持续收紧的背景下，只有提前建立系统化合规机制并持续动态调整的企业，方能在全球 AI 竞争中保持稳健发展。

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

蒋睿馨

电话： +86 10 8524 5808
Email： ruixin.jiang@hankunlaw.com