V&T LAW FIRM
万商天勤律师事务所

杭州上城·全球服务商中心
HANGZHOU SHANGCHENG·GLOBAL SERVICE CENTER

具身智能产业法律合规与风险防控白皮书

(2026)

立足杭州 · 辐射全国 · 链接全球

杭州上城·全球服务商中心

万商天勤律师事务所 数据合规与人工智能专业委员会

2026 年 8 月

目　录

卷首语 3

第一章 产业发展现状与法治环境 4

第二章 国内外监管政策趋势 6

第三章 全链条法律风险图谱 10

第四章 企业合规落地框架 18

第五章 常态化避险体系 20

第六章 专项法律服务方案公示 21

附录一：核心法规与标准清单 24

附录二：企业合规自查清单 26

附录三：典型案例速查表 29

附录四：编制机构说明 32

卷首语

2025 年被称为具身智能的“破圈元年”，2026 年则是它从技术展示迈向商业应用的重要节点。[1]随着人形机器人登上春晚舞台、参加马拉松赛事，具身智能正在从实验室走向大众生活。与此同时，伴随着应用场景不断拓展，一系列法律问题也逐渐显现：机器人采的海量数据归谁管？撞了人谁来赔？训练数据的边界在哪里？出海要面对什么样的监管？

杭州作为数字经济发展的重要城市，率先探索具身智能产业的法治保障路径。《杭州市促进具身智能机器人产业发展条例》于 2026 年 5 月 1 日起正式施行，是全国首部聚焦具身智能机器人领域的地方性法规，为产业创新、应用落地和规范治理提供了制度支撑。[2]

随着具身智能产业加速迈入商业化和资本化阶段，头部企业纷纷启动资本市场布局：宇树科技于 8 月 10 日启动科创板申购，智元创新推进赴港上市进程，乐聚智能、云深处科技亦分别获创业板、科创板受理。资本市场的持续关注，既体现了行业发展的巨大潜力，也对具身智能企业在技术研发、数据治理、知识产权、算法合规及公司治理等方面提出了更高要求。

在产业发展与制度建设交汇的时间节点，万商天勤律师事务所数据合规与人工智能委员会与杭州上城·全球服务商中心联合发布这本白皮书，旨在立足具身智能产业发展实践，从法律与合规视角系统梳理具身智能产业发展中面临的重要法律问题与合规风险，为企业创新应用和风险防控提供参考。本白皮书**立足杭州**（依托具身智能产业发展实践与地方立法探索），**面向全国**（适配各地企业的差异化监管环境），**链接全球**（为企业的出海之路提供多法域支撑）。

我们对这本白皮书的定位很朴素：给企业一份**看得懂、用得上、查得到**的实务指引。

- **看得懂**——不堆法条、不拽名词，而是围绕实际业务场景，从风险点、典型案例和应对措施三个维度展开分析；

- **用得上**——围绕具身智能企业从研发、知识产权，到生产、营销、运营、出海、融资等不同发展阶段的实际需求，提供可操作的合规建议；
- **查得到**——汇编国内外典型案例，并在附录中进行归纳，便于企业在面对具体问题时快速检索相关实践经验。

需要说明的是，本白皮书系基于现行法律法规、司法实践及行业发展情况形成的研究性成果，不构成针对具体事项的法律意见。企业在开展具体业务或作出相关决策时，建议结合自身情况咨询专业律师。

第一章 产业发展现状与法治环境

一、全球与中国产业概览

中国信息通信研究院《人形机器人产业发展研究报告（2024 年）》预计，2035 年中国人形机器人整机市场规模将达到 500 亿元，2045 年可达 10 万亿元级别，机器人数量超过 1 亿台，可用于工厂装配、养老护理、医疗辅助、特种作业等场景；工业和信息化部的数据显示，2025 年我国人形机器人整机企业已超过 140 家，发布产品超过 330 款。[3]

2025 年 3 月，“具身智能”首次写入国务院政府工作报告，和生物制造、量子科技、6G 一起被列为未来产业[3]；2026 年 3 月，“十五五”规划纲要把它正式纳入未来产业范畴。2025 年 11 月，国务院办公厅印发《关于加快场景培育和开放推动新场景大规模应用的实施意见》；2025 年 12 月，工信部等八部门联合印发《“人工智能+制造”专项行动实施意见》[4]。

全国主要产业高地呈现多极竞逐格局：北京主攻“大脑”关键技术，提出万台落地、千亿集群，配套总规模 1000 亿元政府投资基金[5]；上海以“模塑申城”方案建设世界级 AI 产业生态[6]；深圳依托 1200 家集群企业冲刺千亿规模，还配了知识产权“一站式”协同保护平台[7]；杭州则依托“立法先行 + 制造集群”形成独特的制度与产业先发优势 [21]。

二、杭州：从“六小龙”到千亿集群的法治样本

杭州已集聚宇树科技、云深处科技等机器人相关企业 700 余家，从核心算法、控制系统到整机制造，链条完整。2025 年，杭州具身智能产业集群产值 **1068 亿元**——四足机器人、人形机器人的国内市场份额分别超过 **80%**和 **50%**，运动控制算法等核心技术领跑全国 [2 1]。

在空间布局与支撑体系方面，杭州已建成以滨江物联网小镇、萧山机器人小镇、余杭人工智能小镇及之江机器人母港为核心的“三镇一港”产业格局。国家唯一面向具身智能领域的**国家级应用中试基地落户**滨江，要打通从国产芯片、国产模型到国产本体的全栈技术；钱塘区与西湖区分别建有省具身智能机器人质量检验检测中心、国家机器人检测与评定中心浙江检测中心，实现了本地企业“研发-测试-量产”全流程协同保障 [1]。

2024 年 12 月《杭州市人形机器人产业发展规划（2024—2029 年）》定下 2029 年整机年产 2 万台、核心产业规模 200 亿元的目标[8]；2026 年初“强链补链”行动方案提出 2027 年产值超 500 亿元 [1]；2026 年 5 月 1 日，**《杭州市促进具身智能机器人产业发展条例》正式施行**，作为全国首部具身智能领域地方性法规，在立法过程中直接吸纳了宇树科技、中控技术等企业的一线意见 [2]。

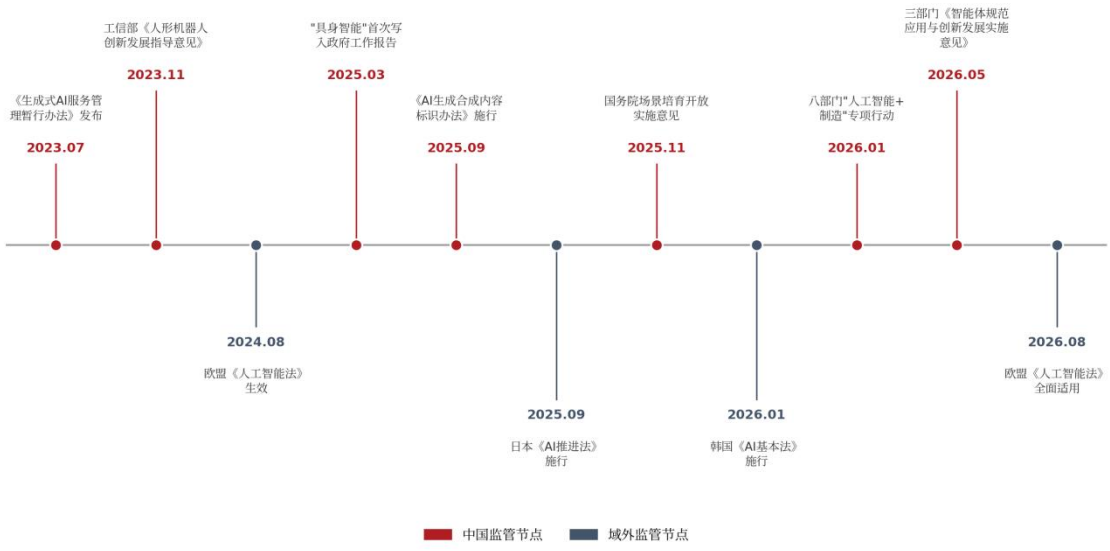
杭州互联网法院审理的“奥特曼 LoRA 模型案”（一审案号：（2024）浙 0192 民初 1587 号、二审案号：（2024）浙 01 民终 10332 号），是全国首例生成式 AI 平台著作权侵权认定案[9]；杭州中院审理的“AI 种草文案案”（案号：（2025）浙 01 民终 3998 号），明确了 AI 服务提供者的注意义务认定规则[10]（两案详情见第三章）。对企业来说，在杭州经营具身智能，裁判规则可预期，这本身就是法治红利。

2026 年 4 月，群核科技登陆港交所，成为“杭州六小龙”第一家上市公司；宇树科技科创板 IPO 于 2026 年 3 月 20 日获受理，拟募资 42 亿元，有望拿下 A 股“人形机器人第一股”；云深处科技科创板申请 2026 年 5 月获受理，拟募资 25 亿元 [143]。有个细节特别值得企业家注意：云深处的招股书，把“主要法律法规及产业政策”“行业面临的机遇与风险”写成了专门章节 [7]，足以可见，**合规披露的质量，已经成了上市审核和投资者判断的显性要素**。

三、产业发展与合规导向

1. 具身智能已经从政策概念，进入“立法＋IPO”双检验阶段，合规不再是花钱的成本项，而是融资、上市、拿单的**准入项**；
2. 杭州的“立法先行＋中试基地＋检测认证＋标杆司法”，给了在杭企业全国最完整的合规基础设施[21]；
3. 跨区域经营的企业需注意北京、上海、深圳政策的差异化（比如深圳的知识产权协同保护平台[10]），建立差异化合规防控机制。

第二章 国内外监管政策趋势



中外人工智能与具身智能监管大事记（2023—2026）

一、国家层面：从“鼓励发展”走向“发展与规范并重”

时间	规范/政策	跟企业有什么关系
2023.08	《生成式人工智能服务管理暂行办法》	提供者要担“网络信息内容生产者责任”；训练数据须合法来源；违法内容须处置
2023.11	工信部《人形机器人创新发展指导意见》	人形机器人上升为国家战略赛道
2025.07	《人工智能全球治理行动计划》	中国方案走向国际，出海企业需关注
2025.09	《人工智能生成合成内容标识办法》	生成合成内容要加显式 + 隐式双标识
2025.11	国务院场景培育开放实施意见	场景开放政策，企业可争取场景资源
2025.11	GB/T 45654-2025 等 AI 安全国标实施	训练数据、数据标注、服务安全有了国家标准
2025.12	八部门“人工智能+制造”专项行动	人形机器人中试基地、训练场、标杆产线
2026.03	“十五五”规划纲要	具身智能纳入未来产业
2026.05	三部门《智能体规范应用与创新发展实施意见》	智能体界定；决策权限三级划分；注册平台“数字身份证”；用户叫停权
推进中	《人工智能法》草案	连续多年列入国务院立法工作计划预备审议项目，预计设责任专章

此外，网信部门的执法，已经从输出端管控（如生成内容标识、内容风控）延伸至**训练与数据端**。对于人脸、声纹等敏感个人信息，若在采集、清洗、训练及调用全流程中缺失单独同意、影响评估或安全保护措施，将面临数据安全与个人信息保护执法的叠加处罚。[11]。

二、地方层面：四城模式对比

城市	核心文件	目标与特色
杭州	《杭州市促进具身智能机器人产业发展条例》	法定定义 + 编码管理 + 电子围栏 + 全生命周期追溯
北京	《北京具身智能科技创新与产业培育行动计划（2025—2027 年）》	百余项关键技术、万台落地、千亿集群；1000 亿元政府投资基金
上海	《关于人工智能“模塑申城”的实施方案》《上海市具身智能产业发展实施方案》	模型驱动、应用示范、群链协同、开源生态
深圳	《深圳市具身智能机器人技术创新与产业发展行动计划（2025—2027 年）（修订版）》	1200 家集群企业、千亿关联规模；知识产权“一站式”协同保护平台

《杭州市促进具身智能机器人产业发展条例》的制度内核：

1. **法定定义**（第三条）：具身智能机器人，指具备物理形态，通过融合人工智能技术实现感知、认知、决策和行动一体化自主能力，可与真实环境实时交互、完成多种复杂任务的智能机器人。
2. **编码管理制度**：每台机器人一个唯一编码，相当于机器人的“身份证”，识别、追踪、定责全靠它[12]；
3. **电子围栏**：给机器人的活动范围划出电子边界；
4. **全生命周期追溯机制**：从研发、生产到退役，数据全程留痕 [20]；
5. **场景开放与包容审慎**：鼓励创新和守住底线，两手都要硬 [2]。

三、域外监管：出海企业的必修课

欧盟——全球监管标杆，也是出海欧洲的第一道门槛：

- **《人工智能法》（AI Act，2024 年 8 月生效，2026 年 8 月 2 日起全面适用）**：按风险分四级管理。搭载 AI 系统的机器人，大概率落入“高风险”类别——风险管理、数据治理、技术文档、透明度、人类监督、网络安全，义务一个不少；违法的代价最高是 3500 万欧元或全球营业额 7%[13]；
- **修订后《产品责任指令》（(EU) 2024/2853，2024 年 12 月 8 日生效）：软件被明确写进“产品”定义**（云端 SaaS 也算），适用无过错责任；还引入缺陷推定和因果关系推定——制造商拒不披露文件，直接推定有缺陷；产品卖出后还在控制更新的（OTA 升级、模型迭代），更新出的缺陷依然追责制造商[14] [15]；
- 《AI 责任指令》已于 2025 年 10 月正式撤回，民事责任回归各成员国国内法[16] [17]。司法层面，2025 年 11 月德国慕尼黑第一地方法院在 GEMA 诉 OpenAI 案中一审判决：未经授权使用歌词训练模型并可经简单提示词输出，构成对复制权和向公众传播权的直接侵犯[18]——欧盟成员国法院对训练数据的态度比想象中严厉。

美国——虽未设立统一联邦立法，但面临严峻的产品责任诉讼（设计缺陷、警示缺陷）、过失责任、代理理论（*Mobley v. Workday* 确立了 AI 供应商可以作为雇主的“代理人”被独立追责[19]）；版权集体诉讼已成建制出现，Anthropic 以 15 亿美元与作家集体达成和解[20]。各州立法呈碎片化趋势（科罗拉多 AI 法案、犹他披露义务、田纳西自动驾驶产品责任条款[21]）。

日韩——韩国《AI 基本法》2026 年 1 月 22 日施行，设“高影响 AI”风险管理义务、生成内容标识义务，**有罚则、有域外效力**；日本《AI 推进法》2025 年 9 月施行，无罚则、软规制，机器人致害纳入产品责任法处理[22] [23]。

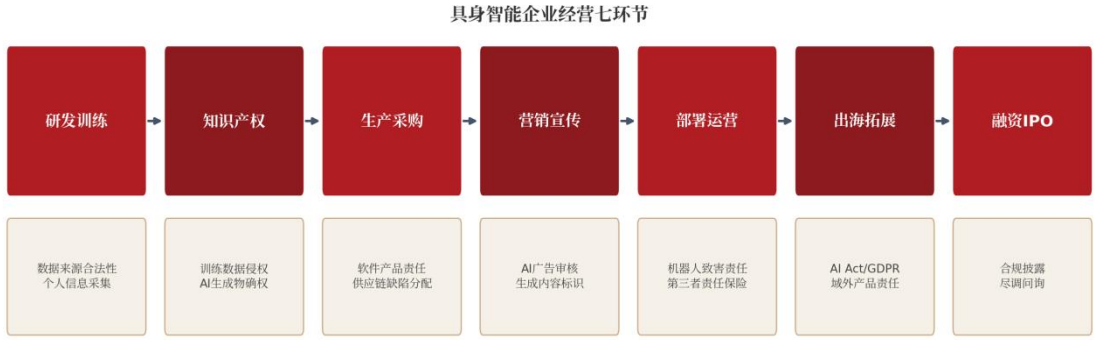
新加坡——2024 年 5 月发布《生成式人工智能模型治理框架》，从问责、数据、内容溯源等九个维度提出治理要求，虽非强制立法，但已成为东南亚监管参照系[24] [25]；2026 年 1 月又发布全球首个《智能体 AI 模型治理框架》，对自主智能体提出安全边界、人类接管、全量日志等专门要求[26]——布局东南亚市场的具身智能企业应当对标。

国际层面：欧洲委员会《人工智能与人权、民主和法治框架公约》（2024 年 9 月开放签署）是全球第一个 AI 国际条约；联合国大会 AI 决议（2024）、OECD AI 原则构成软法基线[27]。

四、六大趋势信号

1. **从“管行为”走向“建底座”**：机器人编码、智能体注册、内容标识、强制日志——“顺着机器找到人”的制度底座正在成型，企业的日志与留痕能力会变成法定能力[15 20]；
2. **执法从“输出端”扩展到“训练数据端”**：数据来源合法性、生物识别信息的采集训练，已进执法样本[17]；
3. **“双推定”全球扩散**：欧盟新 PLD 的缺陷推定、因果推定，极可能被中国未来《人工智能法》借鉴——企业“自证无缺陷”的文档能力，就是诉讼胜负手[22 28]；
4. **保险成为标配**：人保财险、平安产险、太保产险都已推出具身智能专属保险（保机器人本体损失、第三者责任）[5]；
5. **IPO 审核合规前置**：招股书专章披露法律风险成了常态，合规尽调从“上市前补课”变成了“融资轮即介入”[7 29]；
6. **域外监管“长臂”化**：欧盟 AI Act、韩国 AI 基本法都有域外效力——出海即受管辖[21 30]。

第三章 全链条法律风险图谱



具身智能企业全链条法律风险图谱

按企业经营链条，七个环节逐一拆解。

一、研发训练环节：数据来源合法性是“地基”

风险点：训练数据未经授权（可能存在著作权侵权与不正当竞争风险）；违法采集人脸、声纹等生物识别信息未经单独同意；网络爬虫抓取数据触碰三重授权红线。

典型案例参考：

1. **大众点评诉百度案**（案号：（2016）沪 73 民终 242 号）：百度地图抓取大众点评用户评价信息，法院认定点评数据的收集整理凝结了企业投入、构成竞争性权益，判百度立即停止并赔偿 300 万元及合理费用 23 万元[30] [31]；

2. **新浪微博诉脉脉案**（案号：（2016）京 73 民终 588 号）：脉脉通过授权登录获取微博用户信息后超范围使用，法院确立“用户授权 + 平台授权 + 用户授权”的**三重授权原则**[32]；

3. Thomson Reuters v. Ross Intelligence（美国特拉华联邦地区法院，2025 年 2 月即决判决；2026 年 6 月第三巡回上诉法院口头辩论）：ROSS 用 Westlaw 判例摘要训练 AI 法律检索引擎，法院认定侵犯其中 2243 条摘要的版权，训练性使用**不构成合理使用**[33]；

4. Bartz v. Anthropic（美国加州北区联邦地区法院）：Alsup 法官 2025 年 6 月裁定“切割式”规则——用**合法购买并扫描**的书籍训练属合理使用，但从盗版“影子图书馆”**下载并留存**书籍建库本身构成侵权；Anthropic 最终以 15 亿美元与作家集体和解（约 50 万部作品、每部约 3000 美元），2026 年 7 月获法院最终批准，并被要求销毁全部盗版文件 [28]；

5. GEMA 诉 OpenAI 案（德国慕尼黑第一地方法院，2025 年 11 月一审判决）：未经授权使用 9 首歌词训练 ChatGPT 且可经简单提示词输出完整歌词，法院认定构成对复制权和向公众传播权的**直接侵权**，驳回被告“仅是中立中介”的抗辩[26]。

合规措施：建立训练数据来源审查与留痕机制（来源、授权链条、使用范围、采购与许可凭证）[28]；经第三方采购的数据，核验授权链完整性；个人信息保护影响评估

（PIA）常态化；生物识别信息“单独同意＋影响评估＋安全措施”三件套 [17]；避免训练数据构成对原作品市场的替代 [41]。

二、知识产权环节：纠纷最密集、判例最丰富

1. 输入端——训练数据与输入内容侵权

全国首例生成式 AI 平台著作权侵权案（“奥特曼 LoRA 模型案”，一审案号：（2024）浙 0192 民初 1587 号、二审案号：（2024）浙 01 民终 10332 号）：用户上传奥特曼图片训练 LoRA 模型并分享，平台被判**帮助侵权**，赔偿 3 万元。法院认定平台属“兼具技术服务与内容供给双重属性的新型网络服务提供者”，并首创“**分类施策、宽进严出**”规则：输入、训练端相对包容，输出端从严——12 张被诉图片与奥特曼形象构成实质性相似，平台不仅须删除侵权图片，还须删除能稳定输出侵权形象的 LoRA 模型本身 [12 26]。平台是否担责看六个因素：服务性质、作品知名度、侵权事实可感知程度、侵权后果、营利模式、预防措施的可行性及履行情况 [12]。

广州互联网法院“奥特曼案”（案号：（2024）粤 0192 民初 113 号）则是另一种责任形态：被告 Tab 网站通过 API 接入第三方 AI 绘画服务，向充值会员提供文生图服务，**会员输入“奥特曼”提示词，平台直接生成实质性相似图片**——平台就是侵权内容的直接生产者。法院认定被告属生成式 AI 服务提供者，构成**直接侵权**，侵害复制权和改编权，判赔 1 万元；其过错在于欠缺投诉举报机制、未以协议提示用户不得侵权、未对生成物作显著标识 [12 26]。两案合看，规则很清晰：**用户投喂、平台只提供技术的，平台尽义务可免责或仅担帮助侵权责任；平台自己直接生成侵权内容的，按直接侵权论处。**

合规措施：禁止拿版权图库直接训练商业模型；建投诉举报机制并快速处置；模型分享社区设版权审核岗；输出端上线关键词过滤与相似度检测，阻断训练端风险向生成端传导 [26]。

2. 输出端——AI 生成物能不能拿到版权保护？

中外司法实践均坚持“作品必须是‘人的智力成果’”这一基本原则，具体司法案例如下：

案例一：美国版权局 2023 年《含 AI 生成内容作品的登记指南》和 2025 年 1 月《可版权性报告》：纯 AI 生成内容不予登记；含 AI 成分的作品要做“逐案、分解式”审查——只有人类有独创性的那部分才受保护[34] [35]；

案例二：北京互联网法院菲林诉百度案（一审案号：（2018）京 0491 民初 239 号、二审案号：（2019）京 73 民终 2030 号）：威科先行数据库自动生成的分析报告，不构成著作权法意义上的作品[36] [26]；

案例三：深圳南山法院腾讯 Dreamwriter 案（案号：（2019）粤 0305 民初 14010 号）：AI 写作机器人生成的财经报道，因创作过程体现原告团队的个性化安排与选择，被认定构成法人作品——全国首例认定 AI 生成内容构成作品的判决[37]；

案例四：北京互联网法院 2023 年“AI 文生图第一案”（案号：（2023）京 0491 民初 11279 号）：用户用 Stable Diffusion 输入提示词、反复调整参数生成图片，**构成美术作品，版权归用户**[38]；

案例五：美国 Thaler 案（D.C. Cir. 2025）：DABUS 系统自主生成的作品不予登记——“作者”必须是自然人[39] [40] [41]。

对企业的直接启示：AI 生成的图纸、外观方案、营销素材，**版权保护是不确定的**——独创性要由“人的实质性智力投入”来支撑。常熟法院（2024）苏 0581 民初 6697 号、武汉东湖高新区法院（2024）鄂 0192 知民初 968 号都认可了保护，但前提是能拿出提示词迭代、参数调整、人工选择的完整创作记录 [46]。反之，张家港法院审理的 Midjourney“幻之翼透明艺术椅”案中，设计师丰某某仅凭提示词一键生成蝴蝶椅效果图并据此主张著作权，因无法提供创作过程的原始记录、也无法复现生成过程与结果，被法院认定不符合作品构成要件，全部诉请被驳回[42] [43]。

合规措施：关键设计坚持“AI 辅助 + 人工深度介入”；创作过程全流程留痕（提示词历史、参数记录、版本迭代、设计手稿）；核心素材辅之以商业秘密和外观专利双重保护；生成物对外使用前，先做侵权相似度扫描。

3. 智能体输出端——AI 说的错话，算谁的？

“AI 种草文案案”（案号：（2025）浙 01 民终 3998 号）中，**原告是行某信息科技（上海）有限公司，即“小某书”社交电商平台的经营者**；被告乙、丙两公司通过一款 AI 写作工具，提供明确指向该平台的“种草文案”“笔记标题”自动生成服务，被告丁公司提供该工具下载。平台起诉的理由是：被告的定向生成服务助长“虚

假种草”，损害平台基于真实内容生态获得的竞争优势和商业利益，构成不正当竞争并侵害著作权。杭州中院二审认定：乙、丙公司在 AI 工具中设置针对特定平台的功能，违反《反不正当竞争法》第二条，构成侵权，判令停止侵权、连带赔偿 10 万元[13]。法院的说理分四层：被诉服务属生成式 AI 服务，“技术中立”不能成为挡箭牌；服务以特定平台场景为应用层，指向性明显，且违背平台明示规则；服务带有明确指向性和诱导性，让“虚假种草”效率更高、成本更低；服务以会员收费营利，提供者应负更高注意义务[13]。

还有一起案子的被告是 **AI 的使用者（案号：**（2024）浙 0108 民初 10311 号），自媒体博主李某某用文心一言生成一篇含针对某集团公司不实信息的文章，未作任何审核直接发布。法院认定：AI 本质上是辅助工具，“AI 幻觉”在当前技术条件下难以完全避免，**使用者对生成内容负有合理审核义务**，判决其发布声明消除影响、赔偿 3 万元[26]。

合规措施：营销类 AI 工具不得设置指向特定平台的“场景化”生成功能[13]；内置广告合规词库和强制人工复核节点；生成内容发布前由人审核真实性——AI 幻觉不是免责理由[26]；生成的种草、测评内容必须显著标识“AI 生成”。

4. 商业秘密与专利

在具身智能及高阶智能驾驶领域，商业秘密侵权是研发人员流动过程中高发的法律风险。研发人员携带核心代码、模型参数或训练配方跳槽，极易将招聘企业与离职员工个人同时置于侵权被告席。具体案例如下：

案例一：Waymo 诉 Uber 案（美国加州北区联邦地区法院）：谷歌自动驾驶项目核心工程师 Levandowski 离职前下载超过 14000 份机密文件（激光雷达设计图、测试数据、制造文件），随后创办 Otto 并被 Uber 以约 6.8 亿美元收购。Waymo 起诉后，Uber 在庭审第四天即以 **2.45 亿美元股权**达成和解并承诺不使用相关商业秘密；Levandowski 本人 2020 年被判处 18 个月监禁[44] [45]；

案例二：特斯拉诉曹光植案（美国加州北区联邦地区法院，2019 年起诉、2021 年 4 月和解）：特斯拉起诉前工程师曹光植，指其在入职小鹏汽车前将 Autopilot 源代码副本上传至个人 iCloud 账户。案件最终以和解告终[53]。

合规措施：针对核心技术，企业可实行“专利与商业秘密双轨分层”保护策略：易被反向工程的技术方案优先申请专利，难以反向工程的算法模型、训练配方及数据

集则纳入商业秘密管理；企业在制度层面落实“保密与竞业协议、分级访问授权及操作日志留痕”的四位一体防护；新员工入职前要做好背调、离职时必须进行合规审计。

对于具身智能研发过程中使用的开源代码、开源模型及第三方算法工具，还应关注相应开源许可证的授权范围及合规义务。特别是具有传染性要求的 Copyleft 类许可证，可能对衍生代码的再许可、源代码开放及商业化使用产生影响。企业应建立开源组件登记、许可证识别、使用审批及发布前合规审查机制，实现开源软件的来源可追溯、使用可核验、责任可倒查。

三、生产与采购环节

欧盟新 PLD 已明确将软件纳入“产品”范围，适用无过错责任。AI 模型作为组件嵌入机器人的，整机制造商与软件供应商**连带担责**；远程更新（OTA）引入的缺陷照样算数 [22] [23]。反观中国现行《产品质量法》第 41-43 条，已针对因产品缺陷造成损害确立了生产者无过错责任制度，但该制度主要围绕传统实体产品展开。对于软件更新、算法缺陷等新型风险，目前更多通过合同责任与侵权责任路径进行调整。随着人工智能技术在机器人、智能设备等领域的深入应用，未来人工智能相关立法预计将进一步完善软件、算法与实体产品之间的责任衔接机制，并逐步向国际规则趋同。

在机器人硬件安全方面，应重点关注现行强制性安全标准要求。例如，GB 11291.1-2023《工业机器人安全要求 第 1 部分：整机》已对工业机器人的设计、制造、集成及验收等环节提出安全要求，是企业开展产品合规管理的重要依据。

此外，具身智能产业链高度依赖芯片、传感器、控制器、精密零部件及其他关键软硬件，企业除关注供应商资质、产品质量及交付能力外，还应关注出口管制、经济制裁及贸易限制对供应链稳定性的影响。对于涉及受管制技术、产品或特定国家和地区的交易，应在供应商准入、采购及销售环节开展合规筛查，避免因交易对象、最终用户或最终用途触发出口管制或制裁风险。

合规措施：供应链合同要明确缺陷责任分配、召回费用分担、数据共享义务；供应商准入增加“模型安全评估报告”硬门槛；OTA 更新做灰度发布和回滚预案，更新日志完整留存；整机出厂对标 GB 11291.1-2023 等强制性安全标准 [54]；对于生产过程中涉及的电池、电子元器件、稀土材料及其他特殊材料，还应关注生产、流通、回收及退役处置过程中的环境合规要求。

四、营销环节

AI 生成的营销文案、测评视频、数字人口播等内容，如具有推销商品或服务的商业目的，原则上应纳入广告监管范围。对于相关广告活动，广告主（即推广企业）仍承担主体责任。与此同时，向同行业经营者提供具有特定平台导向的 AI 营销工具，若被用于扰乱市场竞争秩序，也可能涉及不正当竞争风险。对于经营者直接使用 AI 生成内容进行宣传，若未履行必要审核义务，导致内容包含虚假或误导性信息并造成损害的，使用者仍需依法承担相应责任。根据《人工智能生成合成内容标识办法》等相关规定，AI 生成合成内容应依法履行显式标识和隐式标识义务。企业如未按要求进行标识，可能面临网信等主管部门的监管处罚。

合规措施：企业应将 AI 营销内容纳入现有广告审核体系，在发布前重点审查极限用语、功效宣传以及医疗、金融等特殊领域广告合规要求；同时，在与 AI 服务供应商合作时，应通过合同明确生成内容审核、标识义务和责任承担机制。

五、运营环节：交付前是“产品”，交付后是“使用者责任”

机器人交付之后，传统责任框架是否仍然适用？从以下案例可以看出：

1. 加拿大航空聊天机器人退款承诺案（*Moffatt v. Air Canada*, 2024）：客服机器人向消费者提供了错误的退票政策信息，加拿大法院最终认定航空公司不能以“错误信息由机器人生成”为由免责，仍应承担相应责任。[46] [47]；

2. *Mata v. Avianca*（S.D.N.Y. 2023）：律师使用 ChatGPT 生成虚假案例并提交法院，最终受到司法制裁。[4849]；

3. Uber 自动驾驶致死案（2018，亚利桑那）：自动驾驶测试车辆发生致死事故后，安全员被追究刑事责任。Uber 与家属达成和解[50] [51]；

4. *Garcia v. Character Technologies*（M.D. Fla. 2025）：对聊天机器人与未成年人互动并造成严重后果的案件，法院未采纳平台关于“言论自由”的抗辩。

综合上述案例可以看出，目前司法实践中尚未认可“人工智能独立承担责任”。

合规措施：企业在部署机器人前应进行场景风险评估；根据业务风险配置相应责任保险；在用户协议、操作规范中明确使用边界、禁止行为以及事故报告义务；完全运行日志留存制度，确保关键操作、系统状态和决策过程可追溯。

六、出海环节：不止欧盟

欧盟市场主要面临三方面合规要求：**AI Act 高风险合规**（技术文档、CE 合格评定、人类监督机制）、**新 PLD 产品责任**（无过错 + 双推定，败诉风险明显高于国内）、**GDPR 数据合规**（机器人采的声画数据十有八九是“个人数据”[52]）。还要盯住成员国司法动态——德国法院已经在训练数据版权问题上作出不利 AI 企业的判决[26]。

美国的核心风险不是监管罚款，而是**诉讼**：版权集体诉讼（Anthropic 15 亿美元和解[28]）、产品责任与代理理论（*Mobley v. Workday*[27]）、各州碎片化立法（科罗拉多、犹他、田纳西各有要求[29]），法定赔偿单部作品最高 15 万美元的制度设计让版权风险呈几何级放大[28]。

日韩监管路径存在一定差异：韩国《AI 基本法》有罚则、有域外效力，“高影响 AI”要建风险管理机制；日本软规制，但机器人致害按产品责任法处理[30][31]。

东南亚对标新加坡：生成式 AI 治理九维框架虽非强制，但已是区域监管参照系[32]；2026 年 1 月的智能体治理框架全球首创，对自主智能体的安全边界、人类接管、日志审计提了专门要求[34]——具身智能产品进入东南亚市场，建议按此自查。

合规措施：企业在产品出海前 12—18 个月启动合规差距分析；根据目标市场展展开“监管地图”，避免简单复制单一市场合规方案；在研发阶段同步完善技术文档，按照欧盟 AI Act 等法规要求建立产品合规材料，而非临近上市后再进行补充；针对美国市场，加强版权风险审查，并通过责任保险等方式分散潜在诉讼风险。[28]。

七、融资与 IPO 环节

宇树科技拟募 42 亿、云深处拟募 25 亿[3][4]，云深处招股书把“主要法律法规”写成专章[7]。投资方尽调越来越细。对具身智能企业开展融资、并购或 IPO 尽职调查时，除传统的数据、知识产权、产品责任等事项外，还应重点核查重大劳动争议、重大安全事故及刑事风险、开源许可证合规情况、出口管制及经济制裁风险，以及境外市场环境准入义务。上述事项一旦涉及重大诉讼、行政处罚、供应链中断或持续经营风险，均可能进一步影响企业估值及资本市场信息披露。

合规措施：企业在融资前先自查合规（数据来源、诉讼、处罚、保险）；股权激励和退出条款考虑 IPO 锁定要求；重大合规事项建“留痕档案”，应对问询。

第四章 企业合规落地框架



企业合规落地三层框架

一、事前：建制度（合规体系搭建）

数据合规底座：数据分类分级；训练数据来源合法性审查规程；PIA 常态化；生物识别信息单独同意机制 [17] [62]；

知识产权策略：专利布局（结构/控制算法/感知系统）、版权登记（人工深度介入的创作留痕）、商业秘密管理（模型参数、训练配方分级管控）、开源协议审查 [42] [43]；

产品合规设计：安全标准前置（GB 11291.1-2023 等机器人安全国标 [54]、GB/T 45654-2025 等 AI 安全国标 [14]）、编码管理对接（杭州条例）、电子围栏功能预留、日志系统内建 [20]；

合同体系：供应商责任分配条款、用户协议免责与警示条款。

二、事中：控流程（运营合规管理）

1. 内容审核：建立 AI 生成内容审核流程，对涉及广告宣传、商业推广等内容进行合规审查，重点关注《广告法》《反不正当竞争法》等相关要求。同时，明确人工审核责任，避免未经核验直接发布 AI 生成内容所引发的法律风险。[26]；

2. 算法与模型管理：完善人工智能模型全生命周期管理机制，建立生成内容标识流程，做好模型迭代、参数调整及功能更新前的风险评估。对于涉及系统能力变化的 OTA 更新，应设置审批程序，[55]；

3. 安全运营：建立人工智能系统运行监测机制，持续关注机器人运行状态和异常行为，完善安全事件报告和处置流程，并通过定期安全检测、漏洞排查等方式提升系统安全保障能力。；

4. 员工管理：加强员工人工智能使用规范管理，明确禁止通过公共 AI 工具处理未经授权的商业秘密或敏感信息；通过合同及内部制度明确 AI 辅助创作成果的权属安排。同时，完善员工入职审查、权限管理和离职审计机制，[52]。

三、事后：能兜底（争议应对与保险）

1. 保险组合：结合具身智能产品可能涉及的人身损害、财产损失及网络安全风险，合理配置产品责任险、第三者责任险以及网络安全保险等商业保险工具；
2. 证据管理：日志留存不少于 3 年；事故“黑匣子”数据封存流程；同时，做好人工智能生成内容创作过程记录与训练数据来源台账的归档；
3. 争议预案：在合同中合理约定争议管辖条款；针对海外业务，应结合目标市场诉讼规则制定专项应对方案，重点关注欧盟集体诉讼等制度带来的风险。同时，建立舆情应对和监管沟通机制，确保发生重大事件时能够及时响应、妥善处理。

四、组织保障：合规不是法务一个部门的事



合规组织三层架构

- **决策层**：董事会下设 AI 治理委员会；
- **管理层**：首席合规官/数据合规负责人统筹，法务、技术、业务三线联动；条件成熟的企业可对标 ISO/IEC 42001 建立人工智能管理体系并通过认证[53]；
- **执行层**：研发设“合规接口人”，重大项目合规一票前置。

第五章 常态化避险体系

企业合规建设不能停留在一次性制度搭建阶段。真正有用的是**常态化机制**：

1. **法规监测**：每月更新监管动态（订阅网信办、工信部、欧盟委员会官方渠道；关注《人工智能法》草案进展[16]）；

2. **年度合规体检**：结合企业业务变化和监管要求，对照风险清单开展定期检查；

3. **合同模板年度修订**：人工智能监管规则和商业模式不断变化，企业应根据最新法律要求和业务实践，定期更新供应商合同、用户协议、数据处理协议等核心文件；

4. **红队演练**：每年至少一次模拟“机器人伤人/数据泄露/知产诉讼”应急演练；

5. **保险动态调整**：随业务规模和出海市场调整保额与险种；

6. **诉讼案例跟踪**：建立人工智能相关案例跟踪机制，关注国内外裁判规则变化，定期更新企业案例库。

第六章 专项法律服务方案公示

万商天勤律师事务所数据合规与人工智能委员会，依托全国 20 家办公室及国际网络，面向具身智能与人工智能企业推出“全链条、模块化、可落地”的专项法律服务。企业可按经营环节单点采购，也可按年度整体委托。

一、服务模块

服务模块	服务内容	交付成果
训练数据合规专项	训练数据来源合法性审查与授权链核验；爬虫与第三方数据采购合规评估；PIA 个人信息保护影响评估；生物识别信息专项合规；数据出境安全评估与标准合同备案	数据合规评估报告 + 数据来源台账模板 + 整改方案
知识产权护城河专项	专利布局规划（结构/控制算法/感知系统）；AI 生成物确权策略与创作留痕体系设计；商业秘密分级保护体系（保密协议、竞业限制、权限与日志制度）；开源协议合规审查；商标与外观专利组合申请	IP 布局方案 + 权属与留痕文件体系 + 商业秘密制度
平台责任与内容合规专项	生成式 AI 服务备案与登记；投诉举报机制、用户协议与平台规则设计；生成内容标识体系；营销内容广告法审核机制	平台合规手册 + 协议模板库 + 内容审核 SOP
智能体治理专项	智能体注册与“数字身份证”对接；决策权限三级配置方案；用户叫停权与日志留痕体系；智能体出海对标新加坡智能体治理框架	智能体治理手册 + 技术对接清单
产品责任与质量合规专项	机器人安全国标（GB 11291.1-2023 等）符合性审查；供应链缺陷责任分配与召回条款设计；OTA 更新合规流程；产品责任险与第三者责任险方案比选	产品合规审查报告 + 合同条款包 + 保险配置建议
出海合规专项	欧盟 AI Act/新 PLD/GDPR 差距分析；美国版权诉讼与产品责任风险评估；日韩、东南亚（新加坡框架）准入咨询；出海监管地图定制	出海监管地图 + 分法域合规差距报告
融资 IPO 合规专项	合规尽调自查与整改；招股书法律风险章节支持；历史数据与版权瑕疵清理；问询答复支持	合规尽调报告 + 披露文件支持 + 问询预案

争议解决专项	著作权、商业秘密、不正当竞争诉讼代理；产品责任与人身损害事故应对；域外诉讼协同（依托国际网络）	诉讼策略方案 + 证据固定清单
常年合规顾问	法规月报与案例速递；年度合规体检；合同模板库维护；高管合规培训；24 小时应急响应	年度合规报告 + 模板库 + 培训记录

二、服务方式

1. **主办律师负责制**：每个项目由合伙人牵头、主办律师负责，配备熟悉 AI 技术与知识产权、数据合规的复合团队；
2. **双周例会与专线响应**：项目期内双周例会通报进展，重大监管动态 48 小时内专项解读；
3. **“意见书 + 工具包”双交付**：所有方案以“可落地、可检查、可举证”为标准——企业拿到的不只是法律意见，还有能直接执行的清单、模板和流程；
4. **跨办公室协同**：涉多地经营的企业，由杭州办公室统筹、相关城市办公室落地执行；涉外事项联动国际网络成员所。

附录一：核心法规与标准清单

一、中国法律、法规与政策

名称	要点	施行/状态
《民法典》	过错责任、共同侵权、网络侵权、产品责任、声音权益	现行有效
《产品质量法》	缺陷产品无过错责任	现行有效
《反不正当竞争法》	不正当获取、使用他人数据构成不正当竞争	2025 年修订
《生成式人工智能服务管理暂行办法》	训练数据合法来源；内容生产者责任；标识义务	2023.08.15 施行
《人工智能生成合成内容标识办法》	显式 + 隐式双标识	2025.09.01 施行
《杭州市促进具身智能机器人产业发展条例》	全国首部；编码管理、电子围栏、全生命周期追溯	2026.05.01 施行
《智能体规范应用与创新发展实施意见》	智能体界定、决策权限分级、数字身份证	2026.05 发布

二、重要国家标准与国际标准

标准号	名称	要点	状态
GB/T 45654-2025	《网络安全技术 生成式人工智能服务安全基本要求》	训练数据安全、模型安全、安全措施	2025.11.01 实施
GB/T 45652-2025	《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》	训练数据来源与安全要求	2025.11.01 实施
GB/T 45674-2025	《网络安全技术 生成式人工智能数据标注安全规范》	数据标注安全	2025.11.01 实施
GB 11291.1-2023	《工业机器人安全要求 第 1 部分：整机》	设计、制造、集成、验收全生命周期强制	现行有效

		性安全要求	
ISO/IEC 42001:2023	《信息技术 人工智能 管理体系》	AI 管理体系（AIMS）建设与认证	现行有效

三、域外主要法规

法域	名称	要点	状态
欧盟	《人工智能法》（AI Act）	风险四级管理；最高罚全球营业额 7%	2026.08.02 全面适用
欧盟	《产品责任指令》(EU) 2024/2853	软件=产品；无过错责任；缺陷与因果双推定	2024.12.08 生效
韩国	《AI 基本法》	高影响 AI 义务；有罚则、有域外效力	2026.01.22 施行
日本	《AI 推进法》	软规制；机器人致害按产品责任法处理	2025.09 施行
新加坡	《生成式人工智能模型治理框架》《智能体 AI 模型治理框架》	九维治理；全球首个智能体治理框架	非强制性框架
欧洲委员会	《人工智能与人权、民主和法治框架公约》	全球首个 AI 国际条约	2024.09 开放签署

附录二：企业合规自查清单

按八个模块对照自查，任一答“否”即为风险点，建议列入整改清单。

模块一：数据与训练合规

序号	自查项	是/否
1	训练数据来源是否全量建档（来源、授权链、采购/许可凭证）？	
2	第三方采购数据是否核验授权链完整（对齐三重授权原则）？	
3	是否存在爬虫获取数据？是否评估过不正当竞争风险？	
4	人脸、声纹等生物识别信息采集是否取得单独同意并完成 PIA？	
5	训练数据是否含他人作品？是否评估过市场替代风险与合理使用空间？	
6	数据出境是否完成安全评估/标准合同备案？	

模块二：知识产权

序号	自查项	是/否
1	核心 AI 辅助创作是否有过程记录（提示词迭代/参数/版本/手稿）？	
2	生成物商用前是否做过侵权相似度扫描？	
3	模型参数、训练配方是否按商业秘密分级管控？	
4	员工保密协议、竞业限制、权限分级、操作日志是否齐备？	
5	新员工是否做“带密入职”背景调查？离职是否做拷贝审计？	
6	开源组件是否完成协议审查（Copyleft 传染风险）？	

模块三：平台与内容

序号	自查项	是/否
1	是否设置便捷的侵权投诉举报机制并公示？	
2	用户协议是否明示禁止侵权、权利归属与责任分配？	
3	AI 生成内容是否按《标识办法》加显式 + 隐式双标识？	

4	输出端是否上线关键词过滤与相似度检测?	
5	AI 营销工具是否避免设置指向特定平台的“场景化”功能?	

模块四：产品质量与安全

序号	自查项	是/否
1	整机是否对标 GB 11291.1-2023 等强制性安全标准?	
2	供应链合同是否明确缺陷责任分配与召回费用分担?	
3	OTA 更新是否有审批、灰度、回滚机制并全程留痕?	
4	机器人是否完成编码登记（杭州）并设置电子围栏?	

模块五：部署与运营

序号	自查项	是/否
1	部署前是否完成场景风险评估（公共场所/老人儿童接触场景上调等级）?	
2	用户协议是否写明正确使用边界、禁止行为与事故报告义务?	
3	运行日志是否全量留存且不少于 3 年?	
4	AI 生成内容对外发布前是否经人工审核（AI 幻觉防线）?	

模块六：出海合规

序号	自查项	是/否
1	目标市场的 AI Act/GDPR/新 PLD 差距分析是否完成?	
2	美国市场是否完成版权诉讼风险与法定赔偿暴露评估?	
3	技术文档是否按欧盟 AI Act 附录 IV 标准建立?	
4	东南亚业务是否对标新加坡生成式 AI/智能体治理框架?	

模块七：保险与争议

序号	自查项	是/否
1	是否投保产品责任险与第三者责任险？保额是否随业务规模调整？	
2	是否建立事故“黑匣子”数据封存与证据固定流程？	
3	是否有海外诉讼（含欧盟集体诉讼）应对预案？	

模块八：组织与机制

序号	自查项	是/否
1	是否设立 AI 治理委员会或明确合规负责人？	
2	是否建立法规月报、年度体检、红队演练等常态化机制？	
3	是否考虑对标 ISO/IEC 42001 建立 AI 管理体系？	

附录三：典型案例速查表（26 案）

一、数据与训练环节

案件	管辖/法院	裁判要点	企业启示
大众点评诉百度案（（2016）沪 73 民终 242 号）	上海知识产权法院	爬取平台评价数据构成不正当竞争，	爬来的数据不能直接做训练语料
新浪微博诉脉脉案（（2016）京 73 民终 588 号）	北京知识产权法院	确立“用户＋平台＋用户”三重授权原则	第三方数据须核验授权链
Thomson Reuters v. Ross（2025—）	美国特拉华地区法院/第三巡回法院	Westlaw 摘要训练 AI 不构成合理使用，2243 条侵权	市场替代是合理使用抗辩的命门
Bartz v. Anthropic (2024—2026)	美国加州北区法院	合法购书训练属合理使用；盗版建库侵权，15 亿美元和解	获取方式与使用方式分开审查
GEMA v. OpenAI (2025)	德国慕尼黑第一地方法院	歌词训练＋可输出，构成复制权、传播权直接侵权	欧盟成员国对训练数据态度趋严

二、知识产权——输入端（平台责任）

案件	管辖/法院	裁判要点	企业启示
奥特曼 LoRA 模型案（（2024）浙 0192 民初 1587 号；（2024）浙 01 民终 10332 号）	杭州互联网法院/杭州中院	“分类施策、宽进严出”；平台帮助侵权赔 3 万元；六因素定注意义务	建投诉机制、删模型断源头
广州奥特曼案（（2024）粤 0192 民初 113 号）	广州互联网法院	平台直接生成侵权图片，构成直接侵权（复制权、改编权）	平台直接生成=直接责任
美杜莎案（2025）	上海市金山	用户训练发布侵权 LoRA	尽到义务的平

	区人民法院	赔 5 万元；平台尽告知、审核、下架义务，不侵权	台可免责

三、知识产权——输出端（确权）

案件	管辖/法院	裁判要点	企业启示
菲林诉百度案（（2018）京 0491 民初 239 号；（2019）京 73 民终 2030 号）	北京互联网法院/北京知产法院	纯机器自动生成内容不是作品	AI 输出需人工加持方可确权
腾讯 Dreamwriter 案（（2019）粤 0305 民初 14010 号）	深圳南山法院	体现团队个性化安排的 AI 生成报道构成法人作品	创作组织过程决定权利归属
AI 文生图案（（2023）京 0491 民初 11279 号）	北京互联网法院	人工深度介入的 AI 生成图构成美术作品	创作过程全留痕
常熟 AI 设计师案（（2024）苏 0581 民初 6697 号）、武汉 AI 图案案（（2024）鄂 0192 知民初 968 号）	江苏常熟/湖北武汉	凭完整创作记录获得保护	提示词迭代记录是确权证据
Midjourney 蝴蝶椅案（2024）	张家港法院	一键生成、无创作记录、无法复现，不构成作品	无记录 = 无权利
Thaler v. Perlmutter（D.C. Cir. 2025）	美国华盛顿特区巡回法院	AI 自主生成作品不予登记 [48]	“AI 是作者”全球都行不通

四、知识产权——商业秘密与智能体输出

案件	管辖/法院	裁判要点	企业启示
Waymo v. Uber（2017—2018）	美国加州北区法院	工程师带走 14000 份机密文件，Uber 以 2.45 亿美元和解	保密体系与入职背景调查

特斯拉诉曹光植案（2019—2021）	美国加州北区法院	Autopilot 源代码传个人 iCloud 后跳槽，和解结案	离职审计盯住代码与参数
AI 种草文案案（（2025）浙 01 民终 3998 号）	杭州中院	平台诉 AI 工具商；指向特定平台的生成服务构成不正当竞争，赔 10 万元	AI 营销工具不得定向“寄生”平台
文心一言不实信息案（（2024）浙 0108 民初 10311 号）	杭州滨江区法院	使用者未审核 AI 生成不实内容直接发布，赔 3 万元	AI 幻觉不是免责理由

五、运营、产品与责任

案件	管辖/法院	裁判要点	企业启示
Moffatt v. Air Canada（2024）	加拿大民航局	聊天机器人错误承诺，航司必须兑现	AI 客服输出纳入话术管理
Mata v. Avianca（2023）	美国纽约南区法院	ChatGPT 虚构案例，提交律师被制裁	人对 AI 输出真实性负责
Mobley v. Workday（2024—）	美国加州北区法院	AI 招聘工具供应商可作雇主“代理人”担责	B 端 AI 供应商直面终端索赔
Uber 自动驾驶致死案（2018）	美国亚利桑那	安全员被追刑责，企业与家属和解	安全员制度不是免责金牌
Riad v. Tesla（2026）	美国加州最高法院	免责声明不能对抗欺诈与产品责任请求	营销宣传与免责条款一致性审查
Garcia v. Character Tech（2025—）	美国佛州中区法院	聊天机器人涉未成年人自杀，言论自由抗辩被驳	C 端情感陪伴类 AI 风险极高
Ayinde v. Haringey（2025）	英国高等法院	AI 虚构判例，律师被移交监管	专业场景 AI 输出须人工核验

附录四：编制机构说明

万商天勤律师事务所是一家拥有全国 20 家办公室的大型综合性律师事务所，国际网络覆盖全球主要法域。杭州办公室深耕数字经济法律服务，数据合规与人工智能委员会由执行主任牵头，专注人工智能、具身智能、数据要素领域的合规、交易与争议解决法律服务。

杭州上城·全球服务商中心是杭州市上城区“全球服务商计划”的核心支点、服务枢纽和赋能平台，位于上城区钱江新城核心区。中心旨在为全省、全市有跨境发展、海外布局需求的企业提供“一窗受理、全域联动”的一站式出海服务，助力企业“扬帆出海”。

主编：彭晓燕（万商天勤律师事务所杭州办公室执行主任、数据合规与人工智能委员会主任）

联系方式：18626876096 | pengxiaoyan@vtlaw.cn

---

[1] 杭州网. https://hznews.hangzhou.com.cn/chengshi/content/2026-07/29/content_9266993_0.htm

[2] jfdaily.com. https://www.jfdaily.com/wx/detail.do?id=1106585

[3] 中国信息通信研究院《人形机器人产业发展研究报告》，2024 年 12 月

[4] 上海证券交易所. https://static.sse.com.cn/stock/disclosure/announcement/c/202605/002190_20260518_G44F.pdf

[5] 北京市人民政府网站. https://www.beijing.gov.cn/zhengce/zhengcefagui/202503/t20250304_4024579.html

[6] 微信公众平台. http://mp.weixin.qq.com/s?__biz=Mzl1MTQyMzl2MA==&mid=2247490240&idx=1&sn=843b3e3093a1e26a5e1e443958409ffe

[7] 深圳市科技创新委员会网站. https://stic.sz.gov.cn/xxgk/tzgg/content/post_12851036.html

[8] 财新网. https://www.caixin.com/2025-03-03/102294076.html?originReferrer=kimi

[9] ccpit-patent.com.cn. https://cn.ccpit-patent.com.cn/news/Intellectual/other/2026/0428/6464.html

[10] 北京金诚同达律师事务所. https://www.jtn.com/CN/booksdetail.aspx?type=06001&keyid=00000000000000009230&PageUrl=majorbook

[11] 安全内参. https://www.secrss.com/articles/86785

[12] 杭州网. https://hznews.hangzhou.com.cn/chengshi/content/2026-05/01/content_9215484.htm

[13] cliffordchance.com. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/01/the-eu-introduces-new-rules-on-ai-liability.pdf

[14] 微信公众号(法的社会视野). http://mp.weixin.qq.com/s?__biz=Mzg4MTI5MzE4Mw==&mid=2247503849&idx=3&sn=326a89fa2585bb1aa6fc1eade82b186e

[15] 微信公众号(蒋律师在线). http://mp.weixin.qq.com/s?__biz=MzA4ODQ3NDk3Ng==&mid=2651373560&idx=1&sn=024f025571178c220c7e19b002207c80

[16] EAPIL. https://eapil.org/2025/10/09/european-commission-withdraws-two-proposals-assignments-of-claims-regulation-and-ai-liability-directive/

[17] europa.eu. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive

[18] 君合. https://www.junhe.com/legal-updates/2887

[19] Quinn Emanuel Urquhart & Sullivan, LLP. https://www.quinnemanuel.com/the-firm/publications/emerging-ai-legal-risks-july-2026-update/

[20] getechlaw.com.cn. https://www.getechlaw.com.cn/blog/anthropic-1-5b-ai-copyright-settlement-final-approval

[21] hengtai-law.com. https://www.hengtai-law.com/insight/research/data_637.html

[22] AI INSIGHT. https://yojigen.llc/blog/posts/japan-korea-ai-law-2026-guide/

[23] faxin.cn. https://zk.faxin.cn/flqk/content.html?gid=F823256&libid=all

[24] 东方律师网. https://www.lawyers.org.cn/mobile/detail.jsp?id=613c2a623cae4c72815a52735001e8eb

[25] Morgan Lewis. https://www.morganlewis.com/pubs/2024/07/singapore-expands-its-ai-governance-approach-to-include-generative-ai

[26] Pertama Partners. https://www.pertamapartners.com/insights/singapore-model-ai-governance-framework-genai-agentic

[27] state.gov. https://2021-2025.state.gov/the-council-of-europes-framework-convention-on-artificial-intelligence-and-human-rights-democracy-and-the-rule-of-law/

[28] 微信公众平台. http://mp.weixin.qq.com/s?__biz=MzA4NjUwOTk4NA==&mid=2247493133&idx=1&sn=981d3f3b002e7192c4d57539aa9540f2

[29] 张逸瑞. https://www.kingandwood.com/cn/zh/insights/latest-thinking/investing-in-embodied-ai-enterprises-a-due-diligence-guide.html

[30] volcengine.com. https://developer.volcengine.com/articles/7433743560358232114

[31] 上海知识产权法院. https://www.shzcfy.gov.cn/detail.jhtml?id=10010536

[32] icourt.cc. https://www.icourt.cc/prac-document/159475.html

[33] getechlaw.com.cn. https://www.getechlaw.com.cn/blog/ai-training-fair-use-thomson-reuters-ross

[34] 微信公众平台. https://mp.weixin.qq.com/s?__biz=MzUyMzAxNTYxOA==&chksm=f8ad1a1b62aadf0a26de51c3f9def54e394f3261c322715850a68ebc7a2619f37b1343f0efbb&idx=1&mid=2247517067&scene=27&sn=87cef5ea67c04281f3d21bd05668e969

[35] 搜狐. https://www.sohu.com/a/814980552_470230

[36] 微信公众平台. https://mp.weixin.qq.com/s/M2iZm3v23MgQChQYV43s2g

[37] 中国知识产权律师网. https://www.ciplawyer.cn/articles/144915.html

[38] 搜狐. https://www.sohu.com/a/967706557_121124708

[39] The Supreme Court. https://www.supremecourt.uk/cases/uksc-2021-0201

[40] airights.net. https://airights.net/legacy/do-ai-have-rights

[41] Bird & Bird. https://www.twobirds.com/-/media/new-website-content/insights/pdfs/pat25_chapter-28-united-kingdom.pdf

[42] 最高人民法院知识产权法庭. https://ipc.court.gov.cn/zh-cn/news/view-4513.html

[43] 新华报业网. https://www.xhby.net/content/s69dc2761e4b0639de44f5bed.html

[44] Smart Patent. https://zhuanli66.com/blog/waymo-uber-trade-secret-case

[45] zenseegroup.com. http://www.zenseegroup.com/news/862878/

[46] mccarthy.ca. https://www.mccarthy.ca/en/insights/blogs/techlex/moffatt-v-air-canada-misrepresentation-ai-chatbot

[47] Pinsent Masons. https://www.pinsentmasons.com/out-law/news/air-canada-chatbot-case-highlights-ai-liability-risks

[48] Github. https://github.com/vectara/awesome-agent-failures/blob/main/docs/case-studies/chatgpt-lawyer-sanctions.md

[49] JD Supra. https://www.jdsupra.com/legalnews/federal-court-turns-up-the-heat-on-1849454/

[50] BreakingNews.ie. https://www.breakingnews.ie/world/back-up-driver-in-first-fully-autonomous-car-death-pleads-guilty-to-endangerment-1508601.html

[51] NPR. https://www.npr.org/2023/07/28/1190866476/autonomous-uber-backup-driver-pleads-guilty-death

[52] 中国知识产权律师网. https://www.ciplawyer.cn/articles/157537.html

[53] Microsoft Learn. https://learn.microsoft.com/zh-cn/compliance/regulatory/offering-iso-42001