AI 落地月度观察

第 001 期 · 深度版 —— agent 成为第一大落地形态：从「内容合规」到「行为合规」

法律服务：**合作法律服务机构提供**（含上海锦天城（重庆）律师事务所，持续增加中）　　主笔：**李章虎律师团队**

发布日期：**2026-10-24**　　期号：**001**

卷首语 · 为什么是「可核验」的月度观察

市面上不缺 AI 资讯，缺的是**敢给出编号、给出口径、敢被逐条核对**的观察。合规立场平台采取「双引擎」分工：**本平台「AI 智能解决方案库」专注 AI 应用落地**——3,528 条落地案例与 1,112 条律师简评回答「AI 正在被怎样使用」；**姊妹平台「涉 AI 案例地图」专注监管执法与司法案例**——中国库 294 条＋世界库 292 条回答「AI 用错了会怎样」；另有覆盖 33 法域的法源库（204 件）提供规则底座。每一条案例都有平台编号（如 `xz-135`、`sol-98873`），每一项统计都注明口径与统计时点。

因此本报告以「**应用落地」为主线**——落地数据、技术形态、行业跃迁是主战场；监管执法与司法动态作为「**落地的一体两面**」从案例地图引入，与落地数据互为镜像：落地跑到哪里，合规边界就跟到哪里。

我们不做预测，只做**有证据链的记录与解读**。读者可以在 ais.hegui66.com 逐条检索到本报告引用的原文出处；本期所有数据统计截止 2026-10-24，凡本报告无法核证的信息一律不作呈现。这是我们的方法论，也是我们的差异化。

—— 李章虎律师团队

本期要点

三个值得记住的判断，正文均有数据支撑

1 **增量已经换挡：Agent 成为第一大落地形态。**10 月新增落地案例中 Agent 类占 42%（28/67），而存量占比仅 16.6%（585/3528）——近三倍的浓度差，意味着 AI 应用正在从「会写、会看」转向「会做、会替你执行」。

2 **执法画像呈「一主两翼」。**10 月中国库新增执法类 17 条，其中 AI 谣言治理 11 条占 64.7% 为主线，未成年人保护与运营合规义务为两翼；未做安全评估即上线生成式 AI 功能被责令下线（`xz-136`）说明**备案与评估义务已进入执行层**。

3 **法律行业的 AI 落地出现跃迁。**10 月新增案例中法律行业 15 条居各行业之首（占 22.4%），累计排名第 4（149 条）；执法、司法与专业服务的「上游行业」正在成为 AI 落地的活跃地带。

平台数据资产带

双引擎分工：落地库与简评库属本平台（应用落地侧），中国库/世界库属姊妹平台「涉 AI 案例地图」（监管司法侧）

3,528	294	292	204
AI 落地案例库	涉 AI 监管执法与司法案例（中国库）	全球涉 AI 判例（世界库 / 12 法域）	法源库（33 法域 · 8 层级）

1,112

律师简评（覆盖 31.5% 落地条目）

注：双引擎分工——**落地案例库与律师简评库属本平台**（ai.hegui66.com / ais.hegui66.com，应用落地侧）；**中国库与世界库属姊妹平台「涉 AI 案例地图」**（hegui66.com/ai-case-map/，监管司法侧）；法源库为两线共用的规则底座。各库互相独立、各有权威源与核验流程；数字为 2026-10-24 实测值，均可在线逐条检索。

律师简评库是本报告的「第二引擎」

落地案例库的 3,528 条中，已有 1,112 条附有律师团队简评（覆盖 31.5% 且持续增长）。简评不是摘要，而是从**义务识别、风险定级、动作建议**三个维度对案例的专业注解——本期「合规动作」栏目与特稿的分析方法，正来自这批简评沉淀的办案经验。

落地数据 · 10 月新增与累计对照

口径：按信息发布日期（pub_date 完整日期）统计当月；排除测试条目；统计时点 2026-10-24

1. 当月新增 67 条：区域与行业分布

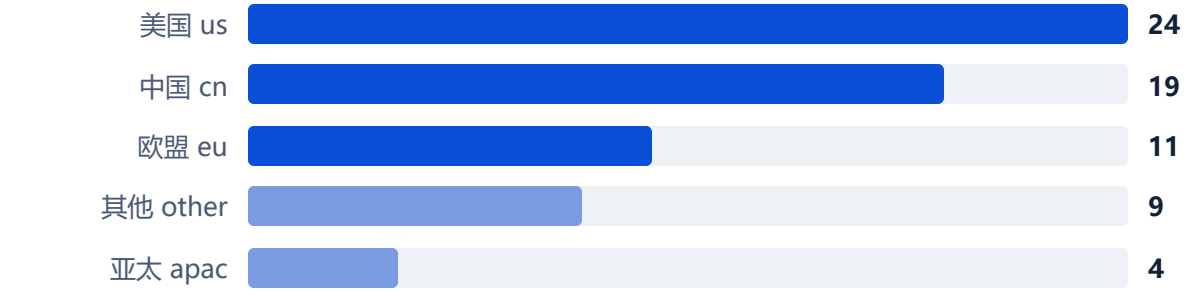


图 1 · 当月新增落地案例区域分布（n=67）

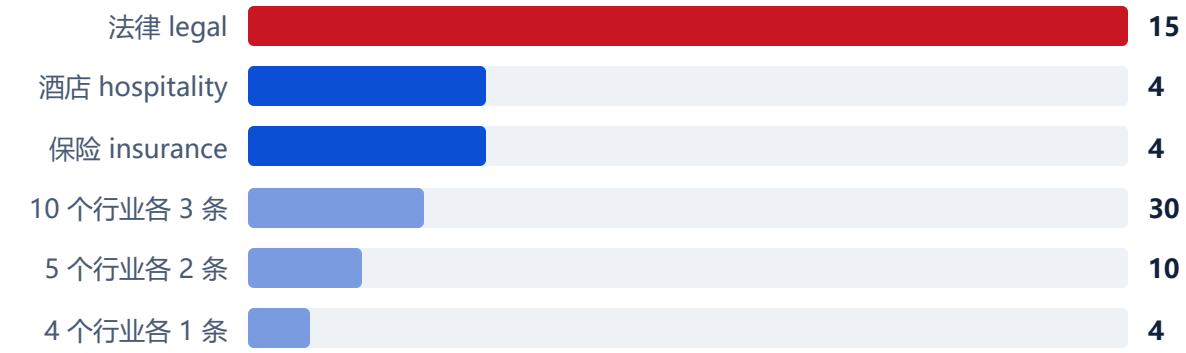


图 2 · 当月新增落地案例行业分布（n=67，仅列头部与汇总）

2. 当月新增 67 条：技术形态分布

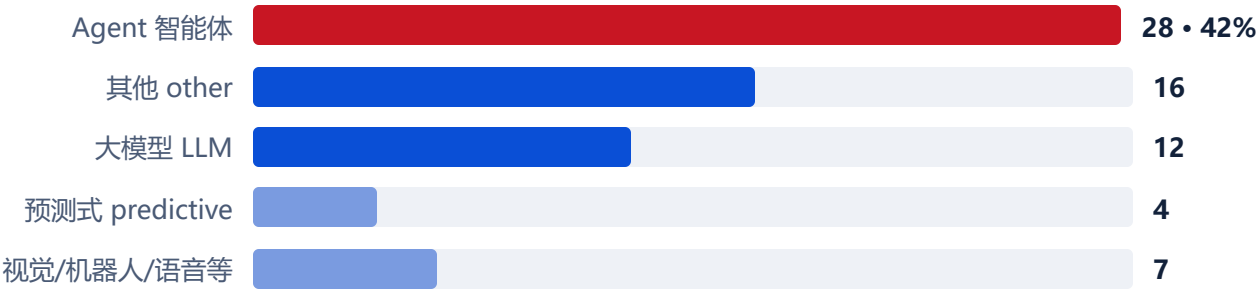


图 3 · 当月新增落地案例技术形态分布（n=67；rag 1 条计入其他）

3. 信息可信度结构：官方级来源占 43%

当月 67 条中，监管机构/法院等**已核证（verified）19 条、官方发布（official）10 条**，合计官方级来源 29 条（43%）；媒体渠道 24 条、厂商渠道 14 条。三级口径与编号溯源机制保证：官方级条目可回溯到监管原文，其余条目均有出处标注并按平台规则持续复核。

4. 累计 3,528 条：与增量对比的三组信号

技术形态 存量 vs 当月增量

- LLM：990（28.1%）存量第一 → 增量仅 18%
- 视觉：782（22.2%）→ 增量仅 3%
- **Agent：585（16.6%）→ 增量 42%，近三倍浓度**

行业 Top5 累计口径

- 制造 544 / 采矿 156 / 物流 152
- **法律 149（第 4 位，10 月跃升）**
- 政府 123

区域 累计口径

- 中国 2,245（63.6%）/ 美国 430 / 欧盟 425
- 亚太 361 / 其他 67

可信度 累计口径

- 媒体 2,252（63.8%）/ 厂商 595
- 已核证 503 / 官方发布 178
- 官方级合计 681（19.3%）

5.「法律行业跃迁」意味着什么

当法律行业的 AI 落地从累计第 4 走到当月增量第 1，说明两件事：一是**法律服务的交付方式正在被重构**——检索、尽调、合同审查、类案分析等环节的 Agent 化速度超过其他专业服务；二是**规则供给端与需求端在同时数字化**，监管执法数据的可获得性提升，使「合规决策计算」从理念变为可执行的产品形态。对法律人而言，这不是替代叙事，而是分工重构：机器承担事实整理与初步筛查，律师聚焦价值判断与责任承担。

监管执法 · 「一主两翼」画像（姊妹平台信号）

来源：姊妹平台「涉 AI 案例地图」中国库（hegui66.com/ai-case-map/，2026-10 月新增 25 条 = 执法 17 + 司法 8）——本节是「应用落地」主线的合规边界镜像

10 月中国库新增执法类 17 条，结构清晰地呈现「一主两翼」：



图 4 · 当月执法类案例结构（n=17；谣言类占比与《AI 执法处罚月度数据报告》9 月号口径一致，系跨月延续性特征）

「主翼」之外，三条标志性案件

编号	案件	执法要点	信号

xz-135	宁波某公司生成 AI 谣言案	结合未成年人保护情节处罚款 10 万元	谣言治理与特殊主体保护叠加
xz-136	西安某公司未安全评估即上线生成式功能	责令下线整改	安全评估与备案义务进入执行层
xz-138	湖南监管部门集中约谈 4 家大模型企业	约谈整改，列明整改事项	监管从个案处罚转向规模化约谈

运营合规义务矩阵：企业对照自查

从当月执法案例反推，生成式 AI 运营者的核心义务集中在以下四组。这不是理论清单，而是**从 17 条执法事实中提炼的「被罚点」**：

义务组	典型被罚情形	对应动作
上线前评估	未开展安全评估即向公众提供生成式服务（xz-136）	上线前完成安全评估并留存报告；涉算法推荐的完成算法备案
内容标识	AI 生成内容未添加显式/隐式标识流入传播链	按《人工智能生成合成内容标识办法》落实双重标识
信息内容管理	平台内 AI 谣言未被识别处置（当月 11 条的主因）	建立谣言识别、辟谣与处置留痕机制
特殊主体保护	涉未成年人有害内容（xz-105 等）	未成年人模式、内容分级与投诉响应

> 「企业最容易低估的不是技术风险，而是『上线即合规』的时间差——很多处罚案例的共同点是：功能先上线，评估在路上。安全评估报告不是合规装饰品，是发生事件时企业免责抗辩的第一证据。」
>
> 「谣言类执法占比连续两月过半，说明监管的注意力已经从『AI 生成内容是否存在』转向『平台有没有管住传播链』——识别、处置、留痕三件事缺一件，就可能成为下一个案例编号。」
>
> —— 摘自合规立场律师简评库（lawyer-notes）对当月执法条目的团队简评

司法动态 · 三条规则信号（姊妹平台信号）

案例地图中国库当月新增司法类 8 条，以下三条对企业管理最具直接参考价值

编号	案件	争议焦点	规则信号	状态

ms-61	北京朝阳：员工拒用 AI 办公软件被解雇案	企业是否有权强制员工使用 AI 工具并据此解雇	法院认定解除违法——**AI 工具使用管理需经民主程序与合理告知**	已判决
ms-62	赛力斯诉名誉侵权索赔 100 万元	AI 生成不实内容涉企业商誉损害的责任承担	**AI 内容的发布者与传播平台责任边界正在划清**	在审
ms-64	AI 生成图片著作权系列案	提示词贡献能否构成独创性	裁判尺度趋同：**人的实质性智力投入是关键变量**	多案在审

司法信号与执法画像形成呼应：执法管住「上线前」，司法正在划定「使用中」的边界——用人单位义务、平台责任、著作权归属三块拼图在本月均有新进展。

本月合规动作 · 按主体分三张卡

每张卡均为三步清单，可直接转为内部流程

① 内容发布防线

适用：内容平台、自媒体运营者、企业新媒体团队

风险锚点：当月 11 条谣言类执法（占执法类 64.7%）

1. **识别前置**：AI 辅助生成的内容发布前过一遍事实核查清单，标注生成来源；
2. **标识合规**：显式标识（用户可见）+ 隐式标识（元数据）双轨落实；
3. **处置留痕**：谣言类内容的发现-处置-举报记录留存不少于法定期限，形成「管理动作证据链」。

② AI 服务运营者底线

适用：向公众提供生成式 AI 功能的产品与研发团队

风险锚点：xz-136 未安全评估被责令下线；xz-138 规模化约谈

1. **评估先行**：新功能上线前完成安全评估，报告归档并与版本号绑定；
2. **备案同步**：核对算法备案与生成式服务备案范围是否覆盖当前功能形态；
3. **投诉与未成年人机制**：投诉入口、处置时限、未成年人模式三项逐一验活。

③ 法务部门的两份清单

适用：企业法务、合规负责人

风险锚点：ms-61 违法解雇判决；Agent 应用扩张带来的行为合规缺口

1. **员工 AI 使用制度**：对照 ms-61，检查制度是否经民主程序、告知是否充分、处罚是否有据；
2. **Agent 应用台账**：盘点本企业已上线/试点中的 Agent 类应用，按「动作分级」分类（见本期特稿）；
3. **数据出域审查**：确认 Agent 调用外部工具/第三方 API 时的数据出域路径与合同约束。

本期特稿

当 Agent 成为第一大落地形态：从「内容合规」到「行为合规」

李章虎律师团队 · 基于 3,528 条落地案例与当月增量的对比分析

一、数据说明问题

存量 3,528 条落地案例中，大模型（LLM）类以 990 条（28.1%）居首、视觉类 782 条（22.2%）次之，Agent 类 585 条（16.6%）仅列第三。但当月新增 67 条中，Agent 类 28 条占 42%，是存量浓度的近三倍。这不是统计噪声——Agent 的本质是「让模型替你执行动作」：调工具、查数据、下单、发函、写代码。**当 AI 从「生成内容」变成「执行行为」，合规的对象就从「说的是不是真话」变成「做的是不是被授权的事」**。

二、三张表：把行为合规拆成可执行的框架

我们基于律师简评库的方法论，把 Agent 合规拆解为三张表。**第一张：动作分级表**——按行为后果把 Agent 动作分为四级，级别越高，人的介入必须越深：

级别	动作类型	示例	人的介入要求
L1 只读	检索、汇总、摘要	查库出报告	抽查即可
L2 起草	生成文书/邮件草稿	拟合同初稿	人工审定后发出
L3 对外表达	代表企业对外表态	客服应答、对外报价	授权范围书面化 + 抽检话术
L4 处分行为	交易、支付、删除、发函	自动下单、自动退款	金额/对象阈值 + 双人确认

第二张：数据出域表——Agent 每调用一次外部工具，就可能发生一次数据出域。企业需要盘点的是「哪个 Agent、带什么数据、去哪个域、基于什么合同约束」，而非笼统的「我们用了 AI」。

第三张：审计留痕表——Agent 的每个自主动作都应可回答四个问题：谁授权的、依据什么规则、动作前看到了什么数据、动作后留下了什么记录。四问缺一，事后举证就会陷入「系统说了算」的困境。

三、给决策者的三句话

第一，**不要用内容合规的旧地图找行为合规的新大陆**——内容审核团队管不住 Agent 的下单权限。第二，**分级是成本最低的合规抓手**——大多数企业 80% 的 Agent 应用停在 L1/L2，真正需要重兵把守的是 L3/L4 的白名单与阈值。第三，**留痕不是负担，是资产**——完整的行为审计链既是监管检查的通行证，也是发生纠纷时企业自证清白的核心证据。

全球视野 · 世界库动态

全球涉 AI 判例库 292 件 · 覆盖 12 法域（2026-10-24 实测）

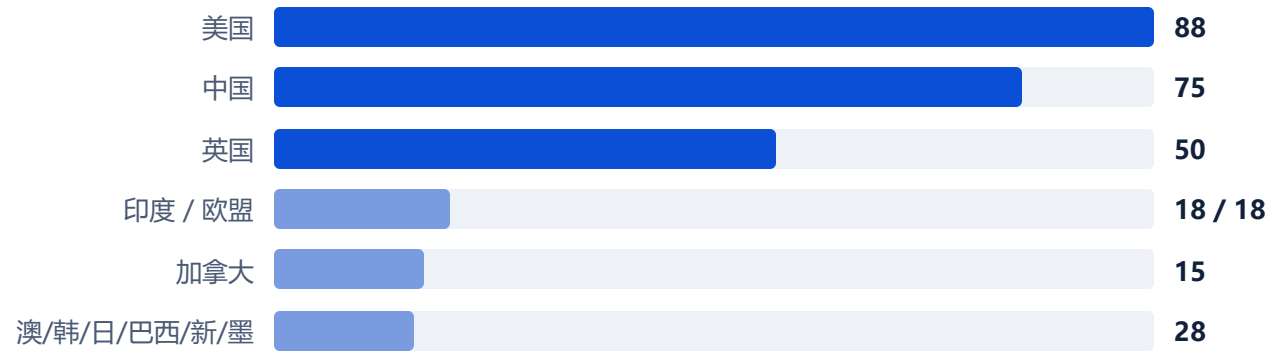


图 5 · 世界库法域分布（n=292；末行 6 法域合计）

说明：世界库「裁判日期」字段格式与当月统计口径尚未统一，本月匹配 0 件，**我们选择如实呈现而不硬凑数据**；字段标准化已列入世界库迭代计划。本期全球视野以结构画像为主，判例精读自第 002 期起按法域轮换推出。

法源库速览

合规立场法源库现有 **204 件** AI 相关法律法规与监管文件，覆盖 33 个法域、8 个效力层级，全部经四重核验（文件完整性＋页数＋首页正文＋文件尾标）入库。经逐件核对，**2026 年 10 月无新生效的国家层级法律法规**——本期不设「新规速递」栏目，不凑数。监管动态以执法与司法渠道呈现（见前文），法源维度保持「宁缺毋滥」。

数据附录与口径声明

1. **统计时点**：2026-10-24；当月口径=信息发布日期（pub_date）在 2026-10 的条目，采用完整日期 10 位口径，不使用入库时间戳（避免历史回补污染）。
2. **落地案例库**：n=67（当月）/ 3,528（累计）；已排除平台测试条目（canary 段编号）。
3. **中国库**：294 条（监管执法 184 + 司法 110），当月新增 25 条（执法 17 + 司法 8）。

4. **世界库**：292 件 / 12 法域；裁判日期字段格式未统一，当月匹配 0 件，如实呈现。
5. **法源库**：204 件 / 33 法域 / 8 层级；本月无新生效国家层级法规，不设凑数栏目。
6. **律师简评库**：1,112 键，覆盖落地条目 31.5%；当月 67 条中 66 条已有简评。
7. **编号溯源**：文中 xz-/ms-/xs- 编号均可在 hegui66.com/ai-case-map/ 检索原文；落地案例编号可在 ai.hegui66.com 检索。
8. **更正机制**：如发现数据错误，我们将在下一期显著位置更正并保留更正记录；本报告存档含 SHA256 校验值，发布台账见专栏。
9. **独立性声明**：本报告数据不依赖任何厂商提供，来源以监管机构、法院、官方发布原文为最高口径。

扫码直达本报告专栏

ais.hegui66.com/report/ —— 全部历史期次在线阅读、PDF 下载与数据溯源入口（免费开放，欢迎转载请注明出处）

合规立场旗下「点策AI智库」

法律服务：合作法律服务机构提供（含上海锦天城（重庆）律师事务所，持续增加中）

主笔：李章虎律师团队 | 专栏：ais.hegui66.com/report/ | 期号：001（创刊号 · 深度版）

本报告仅供一般性信息参考，不构成针对具体事项的法律意见；引用数据以平台在线版本为准。

存档校验：SHA256 见发布台账 _archive_ledger.md