TIANTAI LAW FIRM
天驰君泰（杭州）律师事务所

企业人工智能应用法律风险研究

人工智能诉讼白皮书

北京天驰君泰（杭州）律师事务所 网络与数字经济专业委员会

2026 年 11 月

出品信息

出品单位

北京天驰君泰（杭州）律师事务所 网络与数字经济专业委员会

编委会成员（按姓氏首字母排序）

范家达　邱煜完　张萌萌　廖倩　孙梦玥

审校排版

魏宏岩　邱煜完

内容基准日

2026 年 10 月 29 日

本书以生成式人工智能及其应用层经营场景为重点，裁判、规范与公开程序信息截至 2026 年 10 月 29 日。书中案例仅用于呈现裁判思路，不构成针对具体事项的法律意见。

目录

01	前言	4
02	阅读导引	5
03	一页风险总图	6
04	第一部分　合规篇	7
05	第一站　采购、委托开发与接入	11
06	第二站　喂数据：训练数据来源与授权	20
07	第三站　AI 生成的成果物归谁、能不能用	29
08	第四站　AI 生成内容发布、营销、带货	36
09	第五站　面对人和钱：人格权、会员、退费	44
10	第六站　证据、禁令、刑事红线	52
11	结语与专项核查	62
12	出品与联系	64

前言

人工智能进入业务流程之后，法律问题也随之而来：训练数据从哪里取得，生成内容归谁所有，营销文案由谁负责，发生争议时证据在哪里。这些问题不再只属于模型研发者，而是落在每一家使用人工智能的企业身上。

本白皮书按照企业应用人工智能的业务流程展开，先说明不同业务形态对应的强制性合规义务，再依次讨论采购接入、训练数据、AI 生产、内容经营、人格权与收费、争议应对六个环节，梳理相关诉讼和裁判规则。每一站配有典型案例卡片和企业自查清单，便于企业结合具体业务查找需要核查的事项。

本书以生成式人工智能及其应用层经营场景为重点，裁判、规范与公开程序信息截至 2026 年 10 月 29 日。书中案例仅用于呈现裁判思路，不构成针对具体事项的法律意见。

本白皮书由北京天驰君泰（杭州）律师事务所 网络与数字经济专业委员会出品。

阅读导引

人工智能进入业务流程之后，法律问题不再只属于模型研发者。采购模型服务、将历史数据用于微调、让员工使用生成工具完成设计、把 AI 素材投入营销、向用户收取会员费，都会带来具体的合规义务和争议风险。

2026 年 9 月，最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》（法发〔2026〕10 号），涉 AI 纠纷已有初步裁判指引，备案、登记与标识规则也已实施。企业需要据此明确具体业务对应的合规要求，并完成相应动作。

第一站	采购、委托开发与接入；
第二站	喂数据：训练数据来源与授权；
第三站	用 AI 生产：生成的东西归谁、能不能用；
第四站	拿内容做生意：发布、营销、带货；
第五站	面对人和钱：人格权、会员、退费；
第六站	证据、禁令、刑事红线。

每一站依次回答五个问题：

—— 这一站你在与谁打交道，即业务的上下游；

—— 主要风险集中在哪些业务环节；

—— 法院目前如何处理这类争议；

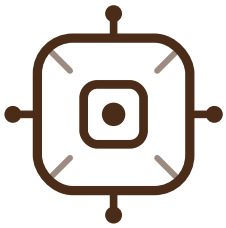
—— 企业内部应当立即检查哪些事实；

—— 域外动态与规则空白还可能带来哪些新问题。

本书以生成式人工智能及其应用层经营场景为重点，裁判、规范与公开程序信息截至 2026 年 10 月 29 日。书中案例仅用于呈现裁判思路；本书属于一般性研究资料，不构成针对任何特定主体或事项的法律意见。如某项业务与您的情况相近，建议就具体事实进一步核查或咨询。

一页风险总图

业务阶段	此刻需要回答的问题	主要相对方或外部主体	优先核查的风险
第一站　采购、委托开发与接入	自研、委托开发、开源微调还是 API 接入?	基座模型供应商、技术开发商、开源社区	成果权属、开源义务、上游许可与备案瑕疵、职务成果
第二站　喂数据：训练数据来源与授权	训练与微调数据来源，以及使用的权利基础是否清洁有效?	训练数据供应方、使用产品的B端/C端用户	抓取行为合规性、训练数据使用边界、个人信息处理合规、数据授权链条
第三站 用 AI 生产：生成的东西归谁、能不能用	生成结果归谁，能否作为资产使用和维权?	企业/企业员工、产品用户	智力成果及可版权性、模型技术与参数、职务与委托成果
第四站　拿内容做生意：发布、营销、带货	内容发布、营销与带货后，责任落在哪些环节?	用户、在先权利人、广告商	输出侵权、内容生态、标识、虚假宣传、再传播与再分发
第五站　面对人和钱：人格权、会员、退费	如何取得人的授权，如何处理用户费用与错误输出?	用户、名人、员工	肖像与声音、个人信息、AI 幻觉、会员预收款与退费
第六站　证据、禁令、刑事红线	争议发生后，如何固定事实并控制损失扩大?	相对方、法院、监管与司法机关	研发与电子证据、行为保全、批量维权应对、刑事红线



第一部分　合规篇

业务形态与持续义务

上马 AI：当下业务形态对应的强制性合规义务

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

企业应用 AI，应先确认业务形态及相应的强制性义务。本部分按业务形态列出对照，企业可先确定所属情形，再逐项核查资质、备案与合同安排。

一、定位产品属于哪种业务形态

不同业务形态对应的合规动作不同，可先按以下情形定位：

情形一：自行训练模型，或基于开源模型微调，并面向公众/其他B端提供服务。

定位：完整意义上的生成式人工智能服务提供者，合规义务最全。

情形二：不自研模型，调用已备案大模型的 API，在外层做应用功能。

定位：适用相对简化的登记程序，但内容安全与标识义务并不免除。

情形三：委托第三方开发模型或应用。

定位：风险集中在合同，成果归谁、数据是否被挪作他用、备案由谁办理。

情形四：仅在研发企业内部使用，不面向公众/其他B端机构。

定位：准入负担最轻，但数据与输出内容的基本义务仍然适用。

定位时需要区分两条界线：一是是否“面向公众提供服务”；二是是否具有“舆论属性或社会动员能力”。直接或间接面向一定规模公众或不特定 B 端企业的，应审慎评估。

二、资质、备案与登记

（一）基础资质

通过互联网向公众提供信息服务，无论是否收费，均须完成 ICP 相关手续：经营性的取得许可，非经营性的完成备案。嵌入互动或收费功能的，还需结合业态判断是否构成增值电信业务。

（二）备案与登记的三条线

自研或微调模型并对外提供服务的（情形一），通常需要同步完成三项动作：

—— 安全评估（具有舆论属性或社会动员能力的服务）；

—— 算法备案（生成合成类算法，线上办理）；

—— 大模型备案（向属地网信部门申报，取得备案编号并在显著位置公示）。

仅调用已备案模型做应用层的（情形二），办理上线登记、取得并展示上线编号即可，审查重点在应用侧风控与所调用基座模型的合规情况。

（三）行业专项许可

同一条技术路线落到不同行业，资质要求不同。常见场景对照如下：

应用场景	涉及的资质或审批
医疗辅助诊断	构成医疗器械的，需办理医疗器械注册
智能投顾	涉及证券投资咨询业务的，需取得相应业务资格
个人征信与信贷风控	涉及个人征信业务的，须经批准；从事信贷业务的，须取得相应金融资质
自动驾驶	道路测试与示范应用须经批准
AI 视频生成、数字人直播	可能涉及网络文化经营许可、网络视听节目服务许可
互联网新闻信息（AI 资讯生成与聚合）	须取得《互联网新闻信息服务许可证》
网络游戏与网络出版	游戏上网出版须经审批并取得版号；网络出版服务须取得许可
在线教育（AI 教学与答疑）	面向中小学生的线上学科类培训须经审批
智能外呼与客服中心	经营呼叫中心业务须取得增值电信业务经营许可

（四）外资主体

外商投资生成式人工智能服务，须符合外商投资准入负面清单；从实务观察，外资主体备案与登记的开放程度有限，宜在架构设计阶段就与属地网信部门前置沟通。

三、研发与采购环节合同要写清的几件事

（一）委托开发

委托开发合同应关注成果范围（代码、模型权重、训练数据、标注成果、技术文档，逐层定权属）、使用与转授权范围、二次开发与改进成果分配、受托方不得将委托方数据用于其他项目或优化自有模型、备案主体与备案服务范围等内容。

（二）数据

不同数据来源的操作方式有差异：自有数据，核对用户协议与授权是否覆盖训练用途；公开抓取，留存取得方式记录、不绕开平台技术措施；对外采购，要求供应商提供完整授权链条，并写入权利瑕疵担保与赔偿责任。

（三）算力

出租裸算力与在算力之上叠加模型调用能力后对外提供服务，两种模式的法律定性和义务分配不同，合同中应先予明确。资源可用率不等于训练任务完成，训练中断损失的责任也应分别约定。

（四）芯片与电力

采购境外先进芯片的，合同中应加入出口管制合规陈述与保证，并约定管制政策变化导致交付不能时的处理机制；转向国产芯片的，注意安全可靠测评已成为党政机关及关键行业采购的前置条件。智算中心用电量达到各省门槛的，需按电力市场化交易规则入市，偏差考核成本应在项目测算中提前体现。

（五）开源组件与开源模型

建立两份清单一一对应：开源组件清单（SBOM）与许可证清单。GPL、AGPL 等强约束型许可证的引入边界在立项时划定；模型权重的社区许可条款（用户规模门槛、不得用于训练其他模型、输出使用限制）与代码许可证分开审查。

四、上线后：需要持续运行的七项义务

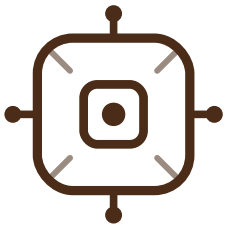
上线后仍需持续履行以下义务，建议逐项明确责任人：

1. 内容安全：对输入数据与生成结果建立审核、特征库与日志留存机制；
2. 标识义务：按《人工智能生成合成内容标识办法》与强制性国家标准 GB 45438—2025 完成显式与隐式标识；
3. 知识产权：训练数据不得侵权，高风险输出建立审核机制；
4. 个人信息：告知同意、敏感个人信息单独同意、事前影响评估与个人权利响应通道；
5. 竞争秩序：数据抓取边界，以及 AI 生成内容用于宣传的真实性；
6. 商业秘密：提示词模板、标注规则、评测集等也可能构成商业秘密，应纳入保密管理；
7. 人格权：提供人脸、人声编辑功能的，应提示使用者取得被编辑个人的单独同意。

五、立项阶段建议同步完成的四件事

合规工作的起点宜前移至立项阶段，与商业模式、技术路线、资金安排同步确定：一是完成监管适用性判断，明确需要备案还是登记；二是梳理数据与技术来源，形成可核查的授权链条与组件清单；三是就采购、委托开发与外协订立书面条款，写清权属、数据隔离与责任分配；四是确定合规责任人与报告通道。

以上为一般性梳理。具体到每个项目，仍需结合业务形态、数据来源、部署方式与属地监管口径逐项核查。我们可就上述事项提供针对性的核查与合规支持。



第二部分　诉讼篇

第一站

采购、委托开发与接入

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

一、场景导入：这一站你在跟谁做生意

企业开展 AI 业务，常见路径有三种：直接采购，即调用已备案大模型的接口，在外层开发智能体和工作流；委托开发，即由开发商定制模型或应用；自建，即基于开源模型微调并搭建服务。三条路径分别对应模型方、开发商和开源社区。与大多数采购不同，这一阶段的合同除交付和付款外，还会影响产品能否持续提供服务、代码和权重能否按预期使用，以及上游瑕疵由谁承担。

三类相对方的交易特征不同。模型方通常提供格式化的 API 服务合同，价格、用量和可用性较为明确，但训练数据来源、备案状态变化的责任分配通常未作约定；开发商按约定交付成果，签约时难以核验交付内容，发生争议后，委托方往往需要就已付款、约定成果与实际交付之间的差距举证；开源社区不在传统采购合同体系内，其“合同”是一份许可证，接受方式是把代码或权重下载下来，未签字不影响其约束力。

监管方面，需要区分以下要求：具有舆论属性或者社会动员能力的生成式人工智能服务，应按照国家有关规定开展安全评估，并履行大模型备案手续；直接调用已备案模型能力的应用或功能，还需按照属地监管实务核对登记及上线编号要求。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》（2025年11月1日起实施，以下简称《要求》）是推荐性国家标准，可作为安全能力建设与评估的参照。备案、登记并非所有 AI 应用整齐划一的上线前行政许可。本章重点讨论《要求》在交易对手违约、成果权属争议和监管核查中的合同与运营影响。

二、风险地图

争议点	裁判活跃度	后果量级	一句话说明
委托／合作开发成果权属（专利、技术秘密、软件、模型权重）	★★★	高	合同没写清的，按法定缺省规则处理，结果往往与企业预期相反
开源许可证义务传导（GPL／AGPL 传染性，Llama 类社区许可）	★★☆	高	组件引入容易剥离难；违反 GPL 等许可证的授权条件，可能导致授权终止并引发侵权责任
上游模型备案、许可瑕疵对下游的传导	★☆☆	中高	上游服务状态变化或备案信息与实际服务不一致，可能引发下游停服与合同争议
受托方数据混用、模型污染	★☆☆	中高	数据被拿去优化竞对模型，公开裁判通常以数据权属争议/不正当竞争为呈现方式
职务成果归属（员工基于开源模型微调、用公司资源开发）	★☆☆	中	需结合工作任务、物质技术条件与合同约定分别判断，不能仅凭开发时间或设备归属下结论
备案代办、合规服务等 AI 采购合同的履行与付款	★☆☆	低中	按普通合同规则处理，已有判例
算力与模型 API 服务合同（可用率、中断损失、服务者定性）	★☆☆	中	“算力租赁”与“模型服务”定性不同，义务分配随之不同

三、法院现在怎么判

（一）GPL 类许可证具有合同效力，违反授权条件可能导致授权终止

现有裁判已将 GPL 类开源许可证作为合同进行审查：许可条款构成授权条件，违反授权条件可能导致授权终止，继续使用则可能丧失权利来源并构成侵权。

案例卡片｜罗盒 GPL 开源侵权案

案号：

（2019）粤73知民初207号

法院与裁判日期：

广州知识产权法院，2021年9月29日

事实与争点：

被告在其收费软件中使用原告以 GPL V3 发布的开源代码，未按协议公开源代码，并收取会员费；争点为违反开源协议的责任性质。

裁判要旨：

GPL V3 属附解除条件的著作权合同；违反开源义务未公开源代码的，授权自动终止，继续使用构成侵权。衍生部分应遵循 GPL 发布；收取会员费不违反 GPL V3。判令停止侵权并赔偿50万元。

规则意义：

该案首次明确认定开源协议的合同性质，确认许可条款构成授权条件；同时确认 GPL 的传染性及于衍生部分，收取会员费用于运营维护并不违反 GPL V3。

案例卡片｜最高法开源软件维权主体案

案号：

（2021）最高法知民终2063号

法院与裁判日期：

最高人民法院，2023年5月5日

事实与争点：

开源软件项目管理者起诉使用方违反 GPL3.0，争点为项目管理者是否具有原告资格，以及未开源是否导致授权终止。

裁判要旨：

结合该案项目治理与贡献事实，项目管理者对源代码形成具有决定性作用，贡献者参与可视为默示同意其起诉。GPL3.0 属附解除条件的许可，未开放源代码则授权自动终止，被诉使用行为构成侵权。

规则意义：

最高人民法院确认，项目管理者对源代码形成具有决定性作用、贡献者参与可视为默示同意其起诉的，具备维权主体资格；并在最高审判层级重申，附解除条件的许可在条件成就时授权自动终止，被诉使用行为构成侵权。

规则提炼：开源许可证不是参考文本而是授权条件：许可条款构成授权条件，违反授权条件可能导致授权终止，继续使用则可能丧失权利来源并构成侵权；维权一侧，项目管理者的原告资格可结合项目治理与贡献事实认定。

（二）二次开发的独创性成果受保护，权利与义务“两分”

违反开源协议的嫌疑，不当然剥夺二次开发者的著作权；但维权成立，也不等于免除其对上游的违约或侵权责任。另需注意，GPL 与 AGPL 的触发场景不同：以 SaaS 或 API 形态对外提供服务时，AGPL 组件即使不发布软件亦须开放源代码。模型权重多采用厂商自定的社区许可，审查要点与代码许可证不同，两份清单应分别建立、分别审查。

案例卡片｜网经 OpenWRT 二次开发案

案号：

（2021）最高法知民终51号

法院与裁判日期：

最高人民法院，2023年10月12日

事实与争点：

原告基于 OpenWRT 系统软件（适用 GPLv2）二次开发形成涉案软件并取得著作权登记，其前员工入职被告公司后复制、修改该软件并销售同类产品；被告以“原告未按 GPLv2 开源、故不享有著作权”提出抗辩。

裁判要旨：

开发者自身是否违反 GPLv2 与是否享有软件著作权是相对独立的两个问题；不免除开发者潜在违约或侵权责任，也不剥夺其基于独创性贡献享有的著作权。不侵权抗辩不成立，判令停止侵权、共同赔偿50万元。

规则意义：

确认权利与义务“两分”：二次开发的独创性成果受著作权保护，自身涉嫌违反开源协议不剥夺其基于独创性贡献享有的著作权；但维权成立，也不等于免除其对上游的潜在违约或侵权责任。

规则提炼：对二次开发企业，这是一组双向提示：既要留存独创性贡献的形成证据以支撑维权，也要单独核查上游开源义务的履行情况，避免“能维权”与“被追偿”同时发生。

（三）委托开发：合同没写清的，按法定缺省规则处理

公开裁判中尚无成型的 AI 委托开发案例，争议发生后将回到《民法典》技术开发合同的一般规则：合同未约定时，委托开发完成的发明创造，申请专利的权利属于研究开发人，委托人取得的只是实施权；技术秘密成果未约定的，各方均有使用和转让的权利。大模型项目的“成果”至少包括代码、模型权重、训练数据与语料、标注成果、技术文档五个层次，合同应逐层写明权属与使用范围，并明确禁止受托方将委托方数据用于其他项目或优化其自有模型。

（四）备案主体错位与准入判断

备案针对特定主体、特定服务作出。委托开发中“A 公司备案、B 公司运营”的结构并非当然违法，但备案信息与实际服务主体、服务范围不一致的，可能在监管核查与融资并购尽调中被要求解释或整改。备案瑕疵对下游的传导尚无公开裁判，但备案相关服务合同已进入诉讼，法院按普通合同规则处理。

案例卡片｜大模型备案代办合同案

案号：

（2025）粤0607民初12853号

法院与裁判日期：

佛山市三水区人民法院，2026年3月5日

事实与争点：

受托方按协议约定完成大语言模型上线备案代办后，委托方拖欠尾款；争点为备案服务合同效力与付款义务。

裁判要旨：

备案代办服务协议合法有效，受托方按约完成备案的，委托方应支付服务费余款64000元及逾期违约金；约定违约金过高部分，酌按 LPR 上浮50%计。

规则意义：

备案安排可以成为合同标的，备案相关服务合同已进入诉讼，法院按普通合同规则处理：受托方按约完成备案的，委托方的付款义务不免除。

规则提炼：备案瑕疵向下游传导尚无公开裁判，损失分配只能事先写进合同；备案代办等服务采购的付款节点，应与可验证的交付成果（备案编号）挂钩。

（五）职务成果：客体、归属与秘密性分别判断

员工完成的模型微调、提示词工程、数据标注方案归谁，应分别回到专利、著作权、技术成果与商业秘密的规则判断，不能仅凭“工作时间完成”或“使用公司设备”概括。劳动合同、保密与知识产权协议及离职交接清单的作用，是让上述判断有清晰的事实与约定基础。

（六）算力与模型 API 采购：定性与指标是两组问题

出租裸算力不构成生成式人工智能服务提供者；在算力之上叠加模型调用能力并对外提供的，落入提供者定义。这一定性决定合同应表述为“算力租赁”还是“模型服务”，也决定义务如何分配。可用率达标与训练成功是两件事，资源可用性指标与任务完成类的责任、救济应分别约定。

四、自查清单

A. 相对方与上游合规

- ☐ 拟采购的模型服务，其提供方是否在国家网信办已公告的备案清单内，备案编号能否对应到实际调用的模型版本
- ☐ 上游备案主体与合同签约主体、实际运营主体不一致时，是否核对了服务安排、备案信息及合同责任分配
- ☐ 上游模型所用开源组件与模型许可证清单能否提供，许可证类型是否逐一列明
- ☐ 外资背景主体的增值电信、新闻信息服务等负面清单业态，是否影响备案或登记的可行性

B. 委托／合作开发合同

- ☐ 合同是否将“成果”拆分为代码、模型权重、训练数据与语料、标注成果、技术文档五层，并逐层写明权属
- ☐ 未约定事项落入法定缺省规则时（专利归研究开发人、技术秘密各方均有使用权），是否与商业预期冲突
- ☐ 是否约定受托方不得将委托方数据用于其他项目或优化其自有模型
- ☐ 是否约定交付时的数据与模型权属声明、开源合规保证及违反时的责任
- ☐ 改进成果（后续微调、迭代版本）的归属与使用范围是否写明
- ☐ 备案由谁办理、备案服务范围与实际功能是否一致，是否写入合同

C. 开源与第三方组件

- ☐ 是否建立开源组件清单（SBOM）与许可证清单，二者能否一一对应
- ☐ 是否根据商业化模式识别 GPL、AGPL 等强约束型许可证的引入边界，且在立项时形成清单
- ☐ 模型侧是否单独审查社区许可条款（如月活跃用户规模的另行授权门槛、不得用于训练其他模型、输出使用限制）
- ☐ 对已引入的强约束组件，是否有等效宽松型替代方案
- ☐ 开源合规检查是否覆盖开发中途节点，而非上线前一次性排查

D. 数据与模型隔离

- ☐ 多租户训练平台或受托开发环境下，数据隔离措施是否写入合同并可验证
- ☐ 甲方提供的数据、乙方标注的成果、双方共有的语料，各自的权利边界是否明确
- ☐ 模型权重开源的项目，是否核实了训练数据的授权范围（权重开源不等于数据可再分发）

E. 备案、登记与合同衔接

- ☐ 是否结合服务属性、功能及属地口径核对安全评估、算法备案与登记要求，并留存判断依据
- ☐ 仅在已备案模型基础上做应用层的，是否核对并完成适用的登记及上线编号展示要求
- ☐ 上游备案状态变化（被注销、被下架、政策调整）时，合同是否约定了通知、替代、解除与费用分担机制
- ☐ 备案代办等服务采购的付款节点是否与可验证的交付成果（备案编号）挂钩

F. 职务成果与人员

- ☐ 员工利用公司设备、数据或在其本职范围内完成的微调、开发与创作，是否按职务成果管理
- ☐ 员工基于开源模型的个人项目与公司业务的边界，是否在劳动合同、保密与知识产权协议中写明
- ☐ 离职员工带走的提示词体系、评测集、标注规则等成果，权属是否有约定
- ☐ 主要利用公司物质技术条件创作并由公司承担责任的计算机软件，是否登记在公司名下

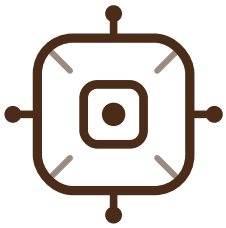
五、域外风向：上游训练争点与下游用户的波及

美国人工智能版权诉讼的程序阶段各不相同。以下仅陈述截至本书基准日的程序阶段与争点，不对在审案件结果作预测。

《纽约时报》诉 OpenAI、微软案（纽约南区联邦法院）中，2025年4月法官就驳回动议作出裁定：核心版权侵权请求继续推进，普通法不正当挪用请求被驳回。2026年9月，美国司法部发表利益声明，支持 OpenAI 的转换性使用抗辩；同月，双方提交简易判决交叉动议。截至基准日，相关动议尚无裁判结果。本案对下游的意义在于：训练阶段的版权风险如何在模型方、API 用户与被授权方之间分配，仍需结合后续裁判与具体许可文本观察。

Bartz 诉 Anthropic 案提供了另一组区分。法院2025年6月作出简易判决：合法获取的书籍用于训练构成合理使用，但下载并保留盗版副本构成独立侵权；双方其后达成集体和解，法院于2026年7月20日最终批准。Thomson Reuters 诉 Ross Intelligence 案中，第三巡回上诉法院于2026年9月29日维持训练不构成合理使用的结论，同时明确该裁判不解决生成式 AI 的训练问题。两案的事实与裁判层级不同，不能拼成统一的“美国规则”，但共同提示采购方分别核查训练素材的获取方式、训练用途及输出对权利作品市场的影响。

这些域外争点可用于国内上游尽调，但不能替代中国法审查。模型已经商用、供应商规模较大或许可费已经支付，均不能替代对训练数据来源、开源义务和下游赔偿安排的核查。



第二部分　诉讼篇

第二站

喂数据：训练数据来源与授权

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

一、场景导入

企业开展 AI 项目，需要取得训练语料、微调样本、标注图库、评测集等数据。数据来源、权利人授权、形成的资产与权益归属，以及企业能否使用相关数据，是主要争议和合规审查重点。

从取得方式看，训练数据大体有四个来源。第一类是自有数据，即企业经营中沉淀的数据，包括但不限于：交易与订单记录、客服与日志数据，基于用户协议收集的账户信息、行为数据与用户生成内容，以及研发过程中形成的标注数据、人工反馈数据和评测集。第二类是公开渠道采集的数据，包括但不限于：网页与平台内容抓取、开放数据集、开放接口返回的数据。第三类是采购与授权取得的数据，包括但不限于：语料库采购、数据集授权、业务合作中的数据交换。第四类是协作与人员流动带入的数据，包括但不限于：合作方共享的数据、新入职员工使用或携带的原雇主数据。

数据来源不同，审查重点也不同。自有数据应核查用户同意是否覆盖训练用途、公开内容能否直接入集、敏感个人信息是否取得单独同意等；外来数据应核查来源是否清洁、授权链条是否完整、取得过程能否经受潜在诉讼检验。公开采集的数据体量较大，争议主要集中在是否绕过技术保护措施、后续商业用途是否合法，以及是否不正当地侵害他人在先商业利益。采购与授权虽有合同外观，但合同本身不能担保数据来源清洁。人员流动带入的数据，权利状态往往不透明，却可能在项目推进后集中暴露；例如，新员工使用原雇主数据开展项目，可能使企业卷入商业秘密纠纷。

二、风险地图

争议点	相对方	裁判活跃度	后果量级
爬取的合法性边界（Robots协议、技术措施、实质性替代）	数据持有平台	★★★	高：停止侵权、消除影响与赔偿，并存在行为保全风险
数据集合的竞争性权益	竞争者	★★★	高：指导性案例已确立保护框架，已有500万元判赔样本
数据知识产权登记证书效力	同业数据商	★★☆	中：登记证书仅作初步证据，权利基础仍须实质审查
训练作品的著作权边界	著作权人	★★☆	高：针对开发者单纯训练行为的公开裁判有限，输出端已有多案
个人信息与生物识别信息	用户、检察机关	★★★	高：民事侵权与公益诉讼并行，已有生效公益诉讼判决
数据采购与标注合同	数据供应商	☆☆☆	中高：公开裁判有限，风险集中在合同与供应链管理
协作与人员流动中的数据	原雇主、合作方、离职员工	★★☆	高：可能涉及商业秘密责任与行为保全
数据来源的刑事升级	侦查、检察机关	★★☆	极高：须独立审查犯罪构成与情节，不由民事违法自动推导

注：裁判活跃度仅表示本书检索样本内的相对密度，不代表全国案件数量统计。

三、司法实践

（一）爬取边界：Robots协议不是免责条款，手段与用途分别评价

爬取类案件的判断沿三条线索展开：手段是否正当（是否绕开登录验证、风控等技术措施），是否实质性替代源平台的产品或服务，后续用途是否构成替代性利用。已有裁判否定“技术中立”“用户承诺免责”抗辩；绕过风控抓取、并以“AI 生成视频”等功能对数据作二次利用的，与抓取行为作整体评价。单案存在数百万元的较高判赔。

案例卡片｜短视频数据搬运案（指导性案例262号）

案号：

（2021）京73民终1011号

法院与裁判日期：

北京知识产权法院，2023年3月16日

事实与争点：

被诉应用抓取搬运权利平台 50392 条短视频及用户昵称、头像、评论，并在自己应用中对外展示传播；争点为平台对用户上传内容形成的数据集合能否主张权益。

裁判要旨：

平台经营者对数据集合形成的经营性利益受法律保护。未经许可获取并向公众提供相关数据，实质性替代平台产品或者服务，扰乱市场竞争秩序、损害平台经营者合法权益的，可以适用反不正当竞争法认定构成不正当竞争。

规则意义：

该案已入选指导性案例 262 号，确立了平台经营者对数据集合的竞争性权益框架与“实质性替代”的评价标尺。

案例卡片｜电商数据爬取ToB服务案

案号：

（2024）浙02民初562号

法院与裁判日期：

浙江省宁波市中级人民法院，2025年6月4日（一审判决已生效）

事实与争点：

被告通过比价插件截取用户 Cookie、突破多种反爬保护措施获取电商平台商品数据，有偿提供“价格监测”“市场分析”“定制 API”等ToB服务。

裁判要旨：

数据不正当竞争案件应区分数据获取手段的正当性与使用场景的合理性，按公开数据、附条件公开数据、不公开数据分层划界；本案绕开风控机制大规模爬取并对外有偿提供数据服务，获取与使用行为构成不正当竞争。

规则意义：

一审判决已生效，并入选最高人民法院 2025 年人民法院知识产权典型案例，判赔 500 万元并消除影响；确认了获取手段正当性与使用场景合理性分别评价、按数据公开程度分层划界的保护框架。

规则提炼：爬取合规的自查顺序与法院的评价顺序一致：先看手段是否正当（是否绕开登录验证、风控等技术措施），再看是否实质性替代源平台的产品或服务，最后看后续用途是否构成替代性利用。

（二）数据集合的权益层次与登记证书的效力

企业积累的数据被整体搬运时，可以主张的是一种受反不正当竞争法保护的竞争性权益，而不是新的绝对财产权——民法典第一百二十七条是引致规范，不能据此主张著作权法上的权项。《数据知识产权登记证》可作为享有财产性利益与收集行为合法的初步证据，但不能替代对数据来源的实质审查。

案例卡片｜AI语料数据案

案号：

（2024）京73民终546号

法院与裁判日期：

北京知识产权法院，2024年6月28日

事实与争点：

数据科技公司经收集、加工、标注形成的语音训练语料数据集（已获数据知识产权登记）被同业公司抓取用于AI训练；该数据集合能否依民法典第127条、汇编作品或商业秘密路径获得保护。

裁判要旨：

数据集具有数据财产权益，但民法典第一百二十七条系引致规范与宣示条款，不得径自使用该条类推绝对财产权请求保护；涉案数据集不构成汇编作品、不构成商业秘密，应使用反不正当竞争法路径；数据知识产权登记证可作为享有财产性利益与收集行为合法的初步证据；违反开源协议非商业使用规则获取、展示数据获取流量的，构成不正当竞争。

规则意义：

该案被称为“AI 语料数据第一案”，考察了数据权益的真正法律渊源。讨论了著作权、商业秘密、不正当竞争在数据集场景下的适用空间。

规则提炼：登记证书固定的是投入与合法外观，开源协议的许可条件划定使用边界：违反开源协议非商业使用规则获取、展示数据获取流量的，构成不正当竞争。

（三）训练语料中的作品：训练行为本身尚无定论

截至目前，针对模型开发者单纯训练行为直接主张侵权的案件，尚无公开终局裁判；较明确的说理主要来自输出端案件与使用者上传物料训练的案件。《意见》第十二条虽文义关于生成端，但在训练段有适用空间。即，法院可能按照以下举证规则进行分配：开发者提出不侵权抗辩的，应当提供训练数据来源、训练过程记录、模型运行模式等予以佐证。

案例卡片｜杭州奥特曼案

案号：

（2024）浙0192民初1587号（一审）；（2024）浙01民终10332号（二审）

法院与裁判日期：

杭州互联网法院，2024年9月25日；浙江省杭州市中级人民法院，2024年12月30日

事实与争点：

用户上传奥特曼图片训练 LoRA 模型并生成近似形象，权利人主张平台删除相关物料与数据并承担侵权责任；争点为平台的训练、生成、发布行为如何定性与归责。

裁判要旨：

训练图片由用户上传、生成指令由用户下达的，平台不构成直接侵权，但对明显可识别形象怠于采取必要措施的构成帮助侵权；平台对用户投喂数据的注意义务应与其身份及信息管理能力相适应，开发者自有数据库应具有合法来源。

规则意义：

该案划定了平台注意义务的动态边界：训练图片由用户上传、生成指令由用户下达的，平台不构成直接侵权；但对明显可识别形象怠于采取过滤等必要措施的构成帮助侵权，注意义务应与平台身份及信息管理能力相适应。

规则提炼：训练行为本身尚无终局裁判，但举证规则已经先行：《意见》第十二条要求提出不侵权抗辩的开发者提供训练数据来源、训练过程记录、模型运行模式等佐证，训练过程留痕不是可选项。

（四）个人信息与生物识别信息：“已公开”不构成豁免

为模型训练在合理范围内处理个人已合法公开的个人信息，且个人未明确拒绝的，一般不认定为侵害个人信息权益；“合理范围”须结合处理目的、信息类型与敏感程度、个人公开时的场景及可合理预期的使用范围综合判断。人脸、声纹等敏感个人信息须取得单独同意。

（五）采购、标注与人员流动：以合同和流程管理控制风险

数据采购与标注外包的公开裁判有限，应通过合同与流程管理控制风险：采购合同应写入权属瑕疵担保、授权范围、赔偿与审计条款；标注外包应约定成果归属、保密义务与转委托限制；标注记录、训练日志、数据版本应全程留痕；员工带入原雇主数据或将自有数据随离职外流的，按商业秘密规则处理，行为保全往往先于实体判决启动。

（六）数据来源的刑事红线

绕开技术措施抓取数据、非法获取或出售公民个人信息的，可能分别触及非法获取计算机信息系统数据罪与侵犯公民个人信息罪；但是否入罪须独立证明行为方式、主观方面与法定情节，不能由使用爬虫或民事侵权直接推导。

四、自查清单

按数据“获取—使用—流转”的顺序，对照检查：

来源盘点

- ☐ 训练、微调数据集是否逐批登记来源（自采、采购、公开收集、用户回流、第三方授权），并留存取得方式与时间的证据？
- ☐ 是否绘制数据流图，明确每一类数据的来源、处理主体、所入模型及对应功能？
- ☐ 自有业务回流数据，是否核对了用户协议中个人信息处理与用户内容授权条款的覆盖范围？

采集行为边界

- ☐ 抓取是否遵守目标平台的Robots协议？是否绕过登录、验证码、风控等任何技术措施？
- ☐ 抓取频率与方式是否可能妨碍源平台正常运行？
- ☐ 采集与后续使用是否实质性替代源平台的产品或服务？是否对外商业化（数据接口、比价工具、AI功能变现）？
- ☐ 所使用的开源数据集许可条款（CC协议、研究用途限制、权利保留声明）是否逐份审查并留档？

个人信息与生物识别信息

- ☐ 训练集中是否含人脸、声纹等敏感个人信息？如有，是否取得单独同意或具备其他合法基础？
- ☐ 使用已公开个人信息是否完成“合理范围”三因素评估并留档？对个人权益有重大影响的，是否另行取得同意？
- ☐ 医疗、心理、未成年人等高敏感场景的训练项目，是否在启动前完成个人信息保护影响评估？
- ☐ 涉及境外主体个人信息的，是否核查数据出境路径的合规性？

作品与第三方权利

- ☐ 训练语料中作品类内容的占比与权利状态是否盘点、分级（清洁／待查／高风险）？
- ☐ 训练数据来源清单与训练过程记录是否留存，足以应对《意见》第十二条的举证要求？
- ☐ 是否设置权利人通知的受理与响应渠道？接到通知后能否定位并处置对应训练物料与生成功能？

供应链与留痕

- [ ] 数据采购合同是否具备权属瑕疵担保、转授权范围、赔偿与审计条款？供应商自身数据来源是否经过尽调？
- [ ] 数据标注外包的成果权属、保密义务与转委托限制是否书面固定？
- [ ] 研发过程（代码托管日志、训练数据版本记录）是否全程留痕，足以在诉讼中证明数据与成果的合法形成时间？
- [ ] 离职员工的账号权限、数据访问与外带风险，是否有离职审计与协议约束？

五、域外风向

训练数据是全球 AI 诉讼的重要争点。域外法院同样需要判断训练是否构成复制、已公开内容能否直接使用、技术例外如何划定，但各法域尚未形成统一答案。现有裁判逐渐区分数据集构建、模型训练与输出复现，并分别审查获取和使用行为。以下在审案件仅记录程序阶段与争点，不预测结果。

Kneschke v. LAION（德国）（案号：310 O 227/23；5 U 104/24；I ZR 281/25）。摄影师诉非营利组织LAION，主张其照片被用于构建开放训练数据集。汉堡高等法院2025年12月10日二审判决维持一审结论：认为构建训练数据集落入UrhG第60条d款（实施《单一数字市场版权指令》（《DSM指令》）第3条）“科学研究例外”。关于是否构成UrhG第44条b款（实施《DSM指令》第4条）“一般文本和数据挖掘例外”，汉堡高等法院认为权利人的使用保留须以机器可读方式作出，自然语言声明不构成有效保留，举证责任在权利人一侧。该案再审申请已获受理，且据报道法院正考虑将欧盟版权指令的例外条款解释问题提交欧盟法院。截至本书基准日，该案仍在再审程序中。

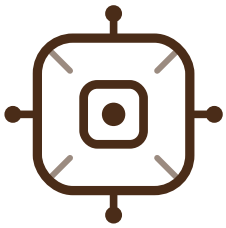
Andersen v. Stability AI（美国）（案号：N.D.Cal. 3:23-cv-00201-WHO）。艺术家集体诉Stability AI图像模型训练案，目前案件仍处于审前程序。

Thomson Reuters v. Ross Intelligence（美国）（一审案号：D. Del. No. 1:20-cv-00613；上诉于第三巡回法庭No. 25-2153）。2026年9月29日，美国联邦第三巡回法院作出判决，维持原判：被告未经许可复制Westlaw法律检索平台的编辑性批注，用于训练与之直接竞争的法律AI工具，不构成合理使用。判决同时明示，被告并非生成式AI系统，本案结论不解决生成式AI训练问题。训练用途与权利人自身市场形成竞争的场景中，合理使用抗辩未获支持，这一点可与境内“实质性替代”的裁判方法对照观察，但两套规则不能直接互替。目前该案仍在中间上诉程序中。

Bartz v. Anthropic（美国）（案号：3:24-cv-5417）。该案简易判决已区分“获取与使用”：合法取得的书籍用于训练被认定构成合理使用，但下载并保留盗版副本构成独立侵权。双方其后达成集体和解，2026年7月20日获法院最终批准。

GEMA v. OpenAI（德国）。慕尼黑第一地区法院2025年11月一审判决：ChatGPT将德语流行歌词“记忆化”于模型参数、经提示可近乎逐字复现，构成未经许可的复制，文本与数据挖掘例外不适用，判令禁令与损害赔偿；后续上诉情况截至本书基准日未见公开报道。

总体而言，各法域均未形成“训练当然合法”或“训练当然侵权”的统一规则。数据集构建与模型训练逐渐被分开评价，opt-out 的技术有效性、输出端可复现性成为重要争点。对境内企业而言，即使未来训练行为获得更大空间，数据集构建环节的权利清洁审查仍不能省略。这是现有域外裁判与境内举证规则共同提示的风险。



第二部分　诉讼篇

第三站

AI生成的成果物归谁、能不能用

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

一、场景导入：这一站你的相对方是模型方与员工

企业把 AI 接入生产流程后，成果的形成方式随之改变：市场人员用文生图工具制作海报，设计人员用图生图完成方案，研发人员用开源模型微调行业模型，文案团队让大模型生成脚本，再由人工筛选、修改并交付。过去能够从草稿、源文件和邮件中看清的创作过程，现在则压缩为一次对话、一组参数和若干次自动生成记录。

由此产生三个问题。第一，生成结果是否属于法律意义上的作品，企业能否阻止他人搬运；第二，即便能够受到保护，权利属于实际操作者、用人单位、委托方，还是受模型服务条款约束；第三，生成结果如果与他人作品、模型或商业标识相近，谁应当承担责任。三个问题分别涉及权利有无、权利归属和使用边界，不能相互替代。作品登记证书不能回答使用是否侵权，平台标注“可商用”也不能替代在先权利审查。

这一阶段的主要相对方包括提供模型、工具和许可条款的模型方，以及参与成果形成的员工、顾问和外包团队。成果发布后，还可能涉及竞争者与在先权利人。企业需要管理从任务分配、工具调用、人工加工到对外交付的完整生产过程，而非只保存最终生成结果。

二、风险地图：权利形成与侵权风险要分开判断

争议点	典型业务场景	裁判活跃度	后果量级
AIGC 可版权性与权属	AI 海报、插图、文案、设计方案被搬运或许可他人使用	★★★	中：无法确权、维权受限，或错误处分他人权利
创作过程举证	员工离职、外包交付、批量内容维权	★★★	高：证据不足可能直接导致权利主张失败
模型结构与参数竞争利益	微调模型、行业模型被复制或替代	★★☆	高：核心模型资产流失、竞争优势被削弱
职务成果与委托成果	员工使用企业账号生产，外部团队交付 AI 成果	★☆☆	中高：权属链断裂、交付后无法持续使用
生成结果侵害在先权利	以参考图、角色名称或提示词生成近似内容	★★★	高：停止生成与传播、赔偿、商业项目下架
署名与生成合成标识	内容发布、广告交付、平台分发	★☆☆	中高：整改、平台处置，并可能影响民事过错判断

注：裁判活跃度仅表示本书检索样本内的相对密度，不代表全国案件数量统计。职务成果和标识义务不因公开民事样本较少而降低审查必要性。

三、法院现在怎么判

（一）AIGC 可版权性：审查人的表达性贡献

已有案件体现了三种审查路径：使用者对最终表达作出可识别的个性化投入时，肯定作品属性；法院要求还原提示词、参数、选择与修改对最终表达的实际影响时，严格审查；最终表达主要由机器随机形成、使用者无法证明实质智力投入时，不予保护。法发〔2026〕10号对可版权性问题暂作留白，个案事实仍是决定性变量。

案例卡片｜文生图第一案

案号：

（2023）京0491民初11279号

法院与裁判日期：

北京互联网法院，2023年11月27日（一审判决，双方未上诉）

事实与争点：

原告使用 Stable Diffusion，经提示词设计、参数设置和反复调整生成图片，被告去除署名水印后作为文章配图发布；争点为图片是否构成作品、使用者是否为作者。

裁判要旨：

涉案图片体现使用者的独创性智力投入和个性化表达，构成美术作品；AI模型不能成为作者，实际设置并选定图片的使用者为作者；去除水印侵害署名权。

规则意义：

AIGC 可版权性肯定路径的起点案件，判令赔礼道歉并赔偿 500 元；其价值在举证方法——提示词设计、参数设置与反复调整的过程记录，而非“使用 AI 即享有版权”的结论。

案例卡片｜伴心案

案号：

（2024）苏0581民初6697号

法院与裁判日期：

江苏省常熟市人民法院，2024年10月18日（一审判决）

事实与争点：

创作者使用 Midjourney 生成、迭代，并以 Photoshop 修改完成《伴心》图，被告将该图用于商业宣传并搭建类似的立体气模装置。

裁判要旨：

涉案图片的场景、色彩、光影、角度及排列组合体现独创性，构成美术作品；保护范围限于登记附件所载平面作品，不及于抽象创意与简单元素，立体装置不构成复制；判赔1万元。

规则意义：

人机协作边界的样本：以 Photoshop 进行人工后期加工，是认定表达性贡献的关键事实；保护范围限于登记附件所载平面作品，不及于抽象创意与简单元素。

案例卡片｜提示词主题概念案

案号：

（2025）浙0192民初17573号

法院与裁判日期：

杭州互联网法院，2025年12月9日（小额诉讼终审判决）

事实与争点：

权利受让人主张 AI 文生图片构成美术作品，但仅能提交主题性提示词，未能展示其他生成创作过程。

裁判要旨：

提示词仅提供主题概念，未具体设计物品形态、色彩、空间布局、光影等视觉元素；在案证据不能证明使用者作出实质性、可识别的创造性判断、选择或编排，图片不构成作品，驳回诉请。

规则意义：

否定路径的代表：仅有主题概念提示词、拿不出创作过程证据的，权利基础不成立，全部诉请被驳回。

规则提炼：三案构成“肯定—审查—否定”的完整光谱：分界不在工具或法院，而在能否证明人的表达性贡献——提示词、参数、迭代记录与人工修改文件等过程证据，决定权利是否成立。

（二）“我微调的模型归谁”：先区分客体，再选择保护路径

源代码、模型结构、权重参数、训练数据、评测集、技术文档可能分别落入著作权、商业秘密、反不正当竞争一般条款或合同的保护范围，不能一概按“版权”处理。企业应保存基座模型来源、许可证版本、微调过程与独立研发记录，避免相似性争议中无法说明技术来源。

案例卡片｜变身漫画特效案

案号：

一审（2023）京0105民初71391号；二审（2023）京73民终3802号

法院与裁判日期：

北京市朝阳区人民法院、北京知识产权法院；2025年3月31日二审判决（终审）

事实与争点：

权利人聘请十余名手绘师绘制五万余张漫画训练数据，经多轮训练、调校形成漫画特效模型；被告后上线的特效与其成像高度近似；争点为被诉方能否直接使用他人 AI 模型结构和参数。

裁判要旨：

经数据训练和调校形成的模型结构与参数可构成反不正当竞争法保护的竞争利益；结合接触可能、模型结构参数高度相似及自研证据不足，认定直接使用成立，二审维持构成不正当竞争的认定。

规则意义：

该案入选最高人民法院 2025 年反不正当竞争典型案例，确认经数据训练和调校形成的模型结构与参数可构成受保护的竞争利益，而非绝对权；认定依赖三组事实：接触可能性、模型参数高度相似（36 个卷积层中 33 个数据一致）、被告自研证据不足。

规则提炼：模型结构与参数经由反不正当竞争法获得保护，认定关键在接触可能、参数相似度与自研证据三组事实；独立研发抗辩能否成立，取决于可回溯的研发记录，而非口头说明。

（三）员工与外包团队参与生产：AIGC 不当然等于企业资产

先识别成果类型，再适用相应权属规则；平台授予的输出使用权、员工或外包方的成果交付、成果本身构成作品，是三层不同依据，可能同时存在，也可能只有一层。把平台账号注册在企业名下，不等于其中每项输出都构成企业享有著作权的作品。

（四）“能不能用”是独立审查：可版权不等于不侵权

即便生成内容构成作品，也可能同时包含他人在先作品的表达，商用前必须另行审查接触可能、实质性相似与合理使用。《意见》第十二条按服务类型、各方参与度、采取的必要措施与获利情况分配开发者、提供者、使用者的责任。应用层企业不能把所有责任推给模型方。

（五）署名与标识：作者署名、平台水印和 AI 标识不是一回事

署名表明创作身份，生成合成标识服务公众知情，二者不能相互替代。《人工智能生成合成内容标识办法》与强制性国家标准 GB 45438—2025 已确立显式与隐式标识并行规则；《意见》第十九条还将删除、篡改标识取得虚假证据列为妨害司法秩序的行为。标识解决透明度，不解决权利许可。

四、自查清单：只查关键事实，不用证书代替审查

（一）创作与权属

- ☐ 是否按项目记录实际操作者、任务来源、使用工具、模型版本和形成时间？
- ☐ 是否保存原始提示词、参数、输入素材、迭代记录、输出历史和人工修改文件，而非只保留最终成品？
- ☐ 是否能够指出最终成果中由人完成的具体表达，而不是笼统主张“投入很多”？
- ☐ 是否区分保护具体表达与保护风格、创意、功能，避免权利主张过宽？
- ☐ 员工、顾问和外包合同是否按成果类型明确权属、许可范围、署名和后续修改权限？

（二）模型与上游许可

- ☐ 基座模型、微调模型、代码、权重、数据集和技术文档是否分别建档？
- ☐ 是否保存所用模型及数据集的许可证文本、版本、取得时间和商用限制？
- ☐ 模型服务条款是否分别覆盖输出使用、再许可、微调、商用和输入用于训练等事项？
- ☐ 是否保存独立研发、模型训练、调校、权限管理与保密措施记录？
- ☐ 与第三方合作时，是否明确模型及中间成果的交付范围和退出后的使用权限？

（三）发布前使用审查

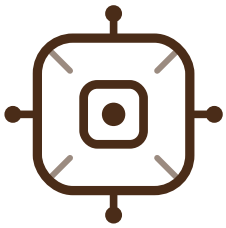
- ☐ 是否检查输入的参考图、文本、音频和其他素材具有合法来源与相应授权？
- ☐ 是否避免以特定在先作品为对象进行刻意仿写、逼近或规避检测？
- ☐ 是否对最终成果开展在先作品、角色形象和商业标识的实质相似审查？
- ☐ 是否能够提供人工筛选、修改和审核记录，以说明企业在生成与使用环节的参与情况？
- ☐ 作者署名、平台来源信息和 AI 生成合成标识是否分别核对，导出与转码后是否仍然保留？

五、域外风向：美国把“人的作者贡献”放在登记审查中心

美国版权局 2025年1月29日发布的《版权与人工智能》第二部分（可版权性）报告，核心结论不是“使用 AI 即不受保护”，而是区分 AI 辅助创作与 AI 替代人的作者贡献：纯粹由 AI 生成的材料，以及人对表达元素控制不足的部分，不受版权保护；人类作者可被感知的既有表达、对 AI 材料的创造性选择、编排和修改，仍可获得保护。基于当时普遍可用的技术，版权局认为提示词本身通常不足以使使用者成为输出的作者。

Thaler 诉美国版权局案处理的是更极端的情形：申请人把机器列为唯一作者。哥伦比亚特区联邦巡回上诉法院 2025年判决维持“作者须为自然人”的要求，美国联邦最高法院于 2026年3月2日拒绝调卷审查，该判决因此发生终局效力。但须注意，拒绝调卷不等于实体认可，该案也未为所有“人机协作”划出统一的提示词数量或修改比例，不能被误读为美国最高法院对 AI 辅助创作作出了全面实体判决。

跨境经营企业需要注意，同一成果在不同法域的保护范围可能不同。在中国个案中被认定构成作品，不代表其在美国登记或诉讼中会获得同样评价；中国法院对提示词、参数和筛选作用的重视，也不能替代美国版权局对表达控制力的审查。据此可作一项有限研判：未来企业的 AIGC 资产管理将从“保存最终文件”转向“保存可分解的人类贡献”，跨境项目尤其需要单独留存人工输入、修改和编排记录。这是基于现有规则差异提出的风险判断，不是对任何在审案件结果的预测。



第二部分　诉讼篇

第四站

AI生成内容物发布、营销、带货

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

一、场景导入：内容发布后的商业化使用

第三站讨论生产环节的权利形成，本站讨论成果离开企业后的商业化使用。用 AI 批量生成商品图并上架、用数字人直播带货、用 AI 配音投放信息流广告、用智能客服机器人接入第三方会议、将热门 AI 产品名称注册为企业名称、用 AI 种草笔记填充内容生态，都属于这一环节。此时内容已经面向公众，经营者从中直接获利，争议重点也从权利归属转为商业化使用是否合法。

发布、营销和带货同时受三层规则约束：著作权和标识规则决定生成内容能否使用、如何标注；反不正当竞争规则处理仿冒产品名称、干扰内容生态、搭便车式营销等行为；消费者权益保护规则判断 AI 修饰的商品展示是否构成欺诈。平台也不再只是中立通道，可能因提供生成、存储、分发工具而承担与其控制能力相匹配的注意义务。

与生产环节相比，经营环节有三项特点。其一，除是否构成作品外，还要审查是否造成市场混淆、生态干扰或消费者误认。其二，责任主体可能包括开发者、提供者、平台、MCN、广告代理商，各环节分别评价。其三，法律后果除停止侵权、赔偿损失外，还可能包括符合法定条件时的惩罚性赔偿、股东连带责任和伪证制裁。企业需要管理从生成、投放到售后反馈的完整内容流程。

需要先行说明：本部分所涉不正当竞争案件均裁判于 2025年修订的反不正当竞争法施行（2025年10月15日）之前，法院适用的是当时施行的 2019年修正文本。修订后文本的条文序号与表述有所调整，企业对照生效判决设计合规动作时，应以现行文本核对具体要件，不宜直接照搬旧条号。

二、风险地图：四类主体、四种责任逻辑

争议点	典型业务场景	裁判活跃度	后果量级
输出端著作权侵权与平台注意义务	AI 成片工具提供影视切条、平台分发侵权内容	★★★	高：停止侵权、高额赔偿、产品功能下架
AI 种草与内容生态不正当竞争	批量生成种草笔记、仿冒平台内容生态引流	★★☆	中高：停止侵权、赔偿，连带责任按实际参与划分
产品名称与语音指令仿冒	抢注热点 AI 产品名称注册企业、设置近似唤醒词	★★☆	中：改名、赔偿，特定情形下另有股东责任与伪证制裁
生成合成标识缺失	广告、直播、商品图未作显式或隐式标识	★☆☆	中：整改与平台处置，并可能影响过错判断
再传播与 AI 假图消费欺诈	AI 美化商品图、合成效果图误导购买	★★☆	高：退货退款、符合法定条件时的惩罚性赔偿
工具化接入后的数据再分发	AI 会议机器人、数据分析工具超范围使用数据	★☆☆	高：停止利用、赔偿、刊登声明

三、法院现在怎么判

（一）输出端著作权：根据服务内容与控制能力判断责任

将侵权内容切分、重排或经 AI 再包装，不影响侵权责任的认定；平台是否担责，取决于其服务类型、对生成过程的控制能力和接到通知后的处置措施，而非单纯的技术形态。

案例卡片｜度加《庆余年》案

案号：

一审（2024）湘0105民初3790号；二审（2024）湘01民终18114号

法院与裁判日期：

长沙市开福区人民法院、长沙市中级人民法院；2024年12月30日二审判决（终审）

事实与争点：

被告运营的“度加剪辑”将《庆余年》剧集切分为 3 至 7 秒片段存储于自家服务器，供用户通过“AI 成片”功能一键生成解说视频，并设积分奖励机制；争点为平台对切条存储、推荐分发应负何种责任。

裁判要旨：

切条存储供生成使用，直接侵害信息网络传播权；投诉渠道单一、无拒答策略、未及时下架构成明显过错；积分奖励不构成教唆；竞争损害已被著作权法覆盖，不再适用反法第二条；判赔80万元，二审维持。

规则意义：

确立两层审查框架：将作品切条存储并向用户提供的行为直接侵害信息网络传播权，不因切条较短、由 AI 重新拼接而改变定性；平台过错看投诉渠道、拒答策略与处置速度三项事实的叠加；积分奖励缺乏针对特定侵权内容的教唆故意，不构成教唆侵权；竞争损害已被著作权法覆盖的，不再适用反法第二条重复评价。

> 规则提炼：平台过错的认定落在运营机制上：投诉渠道是否畅通、是否设置拒答策略、接到通知后是否及时下架——这些是日常运营要建设的机制，不是诉讼发生后的补救动作。

（二）AI 种草与伪原创：功能设计与内容生态的竞争法评价

平台投入形成的真实内容生态构成受反不正当竞争法保护的竞争利益；批量生成、定向投放、以营利为目的的伪原创内容，即使单条难以指认受害者，也可整体评价为不正当竞争；连带责任应根据各方对侵权行为的实际参与程度确定，而非简单按“上下游”关系划分。

案例卡片｜小红书 AI 种草案

案号：

一审（2024）浙0192民初3396号；二审（2025）浙01民终3998号

法院与裁判日期：

杭州互联网法院、杭州市中级人民法院；2025年8月7日二审判决（终审）

事实与争点：

被告通过“单乎”网站向商家出售一键生成种草笔记的服务，笔记模仿平台真实用户的体验表达，批量投放于平台；争点为平台内容生态是否受反法保护。

裁判要旨：

真实种草内容生态构成受保护竞争利益；法院结合生成式AI利用、特定场景、指向诱导与营利性认定构成不正当竞争；二审改判赔偿10万元，工具运营方不承担连带责任。

规则意义：

该案入选浙江省高级人民法院 2025 年度知识产权典型案例，确立了以四组因素评价功能设计与商业生态的框架：是否利用生成式 AI、是否属于面向特定场景的应用层产品、是否具有明确指向性和诱导性、是否以营利为目的。

规则提炼：连带责任按各方对侵权行为的实际参与程度切割，而非简单的“上下游”关系：工具提供方未直接参与生成和投放的，不当然为投放方的行为买单。

（三）产品名称与语音指令：反不正当竞争法与注册商标保护

AI 产品名称与语音唤醒词可经“有一定影响”获得反不正当竞争法保护，不以注册商标为前提；已注册商标可叠加驰名商标保护。企业名称、字号、域名、网站备案应作为一组统一检索、统一管理。

案例卡片｜“文心一言”产品名称案

案号：

（2024）渝0192民初4813号

法院与裁判日期：

重庆自由贸易试验区人民法院；2024年10月14日（一审判决，双方均未上诉）

事实与争点：

被告在百度发布“文心一言”当日申请注册含“文心一言”字样的企业名称，其后又备案 16 个含“文心”字样的网站；争点为是否构成混淆。

裁判要旨：

结合发布当日密集报道等事实，“文心一言”构成有一定影响的商品名称；在企业字号中使用构成混淆；判赔3万元，股东因简易注销承诺不实承担连带责任；伪造证据者另被罚款5000元。

规则意义：

发布当日的密集报道及后续实际运营，即可支撑“有一定影响”的认定，名称保护不以注册商标为前提；股东因简易注销承诺不实承担连带责任、伪造证据者被另行罚款 5000 元，提示程序行为本身也有责任。另在“小爱同学”案中，被告在电动晾衣架产品上使用与“小爱同学”近似的“xiaoaixiaoai”语音指令，被认定构成不正当竞争，“小米”注册商标被认定为驰名商标并获跨类保护（四川省成都市中级人民法院一审，案号：（2022）川01民初6589号）。

规则提炼：企业名称、字号、域名、网站备案与语音唤醒词应作为一组统一检索、统一管理，并与热点 AI 产品名称保持必要距离。

（四）标识义务：生成、导出、转载和投放各环节均应保留标识

显式标识与隐式标识并行，义务沿“生成—传播—使用”链条分层。多数经营者的实际风险在自己掌控的环节：模型输出带隐式标识，经剪辑导出、转码压缩、多平台分发后元数据可能丢失；广告代理商二次制作时可能移除显式标识。标识解决透明度，不解决权利许可；应标未标也可能成为民事过错判断的事实。

（五）再传播与 AI 假图：宣传内容的实质审查

经营者对 AI 生成宣传内容负有与人工制作内容同等的真实性和审查义务，不能以技术中立替代审查；明知或应知内容系 AI 合成且失实仍转发、投放的，可能被评价为共同参与虚假宣传。

案例卡片｜AI 假图消费欺诈案

案号：

一审（2025）粤0192民初17104号；二审（2025）粤01民终27243号

法院与裁判日期：

广州互联网法院、广州市中级人民法院；2026年3月10日二审判决（终审）

事实与争点：

经营者在商品详情页使用 AI 合成图片，展示效果与实物严重不符，并声称系真人实物拍摄，消费者购买后主张欺诈。

裁判要旨：

AI合成失实商品图叠加“真人实拍”虚假陈述构成消费者权益保护法第五十五条欺诈，改判三倍惩罚性赔偿1233元；经营者不能以技术中立替代对宣传内容的审查。

规则意义：

一审曾以技术中立为由未认定欺诈，二审改判认定：合成失实图像叠加“真人实拍”虚假陈述的复合行为足以使消费者陷入错误认识——使用 AI 工具不改变欺诈的构成，技术中立不能替代对宣传内容的审查义务。

规则提炼：一审的“技术中立”说理已被二审否定：宣传内容的实质审查义务不因内容系 AI 生成而降低，三倍惩罚性赔偿同样适用于 AI 生成的虚假展示。

（六）AI 工具化使用的数据边界：合法接入不等于可以任意再分发

许可范围之内的收集与提供是正当经营，越过许可范围的复制与公开则可能构成不正当竞争。上海浦东法院在“会议机器人案”中认定，会议机器人经许可参会本身正当，但将会议数据向超越白名单范围的不特定公众提供，实质性替代了会议主办方对数据的控制与经营利益，构成反不正当竞争法第二条规制的不正当竞争，判赔 400 万元。采购 AI 工具时，应明确数据归属、改进使用范围与退出删除义务，并防范员工将经营数据接入未经批准工具的“影子 AI”风险。

四、自查清单

（一）内容与著作权

- ☐ 提供给模型或工具的素材（影视切条、图片、文本）是否逐一核对授权链条?
- ☐ “AI 成片”“一键生成”类产品功能是否评估过输入来源的合法性?
- ☐ 平台是否建立与侵权线索积累相匹配的关键词过滤、拒答和下架机制?
- ☐ 收到权利人通知后，处置记录（时间、措施、范围）是否完整留存?
- ☐ 平台奖励、积分等激励机制是否可能被解读为针对侵权内容的诱导?

（二）营销与竞争

- ☐ 商品名称、企业字号、域名、网站备案是否与热点 AI 产品名称保持必要距离?
- ☐ 新产品发布前是否完成名称、字号、域名、备案的四项统一检索?
- ☐ 语音唤醒词、指令集是否检索过他人有一定影响的语音标识?
- ☐ 种草、测评、口碑类内容是否区分“真实用户体验”与“批量生成内容”?
- ☐ 对外宣传中“真人实拍”“实测”等表述是否有相应证据支撑?

（三）标识与消费者权益

- ☐ AI 生成内容在导出、剪辑、转码、多平台分发后，显式与隐式标识是否仍可核查?
- ☐ 广告代理商、MCN 等合作方是否被纳入标识义务的传递条款?
- ☐ 商品展示图与实物的差异是否超出合理美化范围，是否保留原始拍摄素材备查?
- ☐ 消费者投诉中涉及“图片与实物不符”的，处置流程是否有完整记录?
- ☐ 明知或应知系 AI 生成且失实的内容，转载投放前是否有独立审核?

（四）工具化数据使用

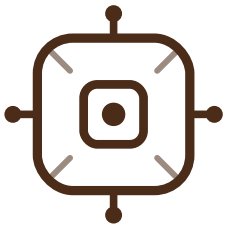
- ☐ AI 工具接入第三方会议、群聊、店铺后台时，许可范围是否书面明确?
- ☐ 工具输出的数据存储位置、使用场景、再分发对象是否登记在册?
- ☐ 与工具供应商的合同是否覆盖数据归属、改进使用、退出删除等事项?
- ☐ 供应商侧是否保留审计权利，以核查数据实际使用范围?

五、域外风向：C-250/25 的版权责任四问

欧盟法院大法庭审理的 C-250/25（Like Company 诉 Google Ireland 案）围绕 Gemini 输出与训练提出四组问题：聊天机器人回答中显示与新闻出版者网页内容部分相同、且长度已达到《数字单一市场版权指令》第15条保护范围的文本，是否构成该指令第15条第1款与《信息社会指令》第3条第2款意义上的向公众传播，“下一词预测”的技术过程对该定性是否有影响；训练大语言模型的过程是否构成复制；若构成复制，对合法可获取作品的训练是否适用《数字单一市场版权指令》第4条文本与数据挖掘例外及权利人选择退出机制；用户输入与新闻出版内容相同或指向该内容的指令后，聊天机器人输出部分或全部相关内容，是否构成服务提供者的复制。大法庭已于2026年3月10日开庭审理。截至本书基准日，佐审官意见与判决均未检索到公开发布，本案任何实体结论均属未知。

四组问题各有对应的境内参照。输出内容向公众传播的定性问题，可与境内“度加案”对平台直接侵权的认定对照观察；训练过程是否构成复制的问题与训练端定性相关，境内法院目前亦未形成统一口径；文本与数据挖掘例外及选择退出机制在境内尚无对应制度安排，权利人主要通过个案侵权诉讼救济；输出复制与服务提供者责任的认定则与境内信网权规则功能相近。境内“度加案”“奥特曼案”已经从平台控制能力与动态注意义务角度搭建输出端责任框架，而 C-250/25 提供了观察欧盟指令如何处理输出传播、训练复制、文本与数据挖掘例外及服务提供者责任的样本。不同法域的请求权基础与免责结构并不相同，不能作机械映射。

后续值得观察的是，欧盟法院是否会围绕服务类型、控制能力、训练与输出阶段分别设定责任条件，以及这些条件与《意见》第十二条的多因素框架有何异同。在佐审官意见和判决发布前，本书不对裁判方向或结果作预测。



第二部分　诉讼篇

第五站

面对人和钱，人格权、会员、退费

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

一、场景导入：这一站你在跟谁做生意

前四站讨论模型、数据、生成成果及其商业化使用，本站讨论人格权益和费用争议。相关权利义务主要体现在用户协议、授权书和员工劳动合同中，而非采购合同和开发协议。

出事的场景通常是这样：一位国风博主发现自己的仿妆视频成了你平台上明码标价的换脸模板；一位配音演员在别人家的图书带货视频里听见了自己的声音，而一位做过“虚拟艺人”的年轻人，在公司数字角色的配音里听见自己的声音；一位考生拿着 AI 编造的校区名称和“内容有误赔偿十万元”的聊天截图，要你为模型自己说出的话负责；一位已故老人的子女，发现老人在一条图书推荐视频里“开口”荐书；一位数字人客户因为平台封号，拿着合同要求退还全部服务费。

本站涉及的人格权益相对方包括三类：用户既提供素材，也可能受到错误输出影响，或者诱导生成侵权内容；名人的肖像和声音可能被复刻，相关维权路径较为成熟，批量诉讼活跃；员工的录音、出镜和配音可能在履职过程中完成，但劳动合同中的职务成果归属条款并不覆盖其人格权益。费用争议也涉及三类主体：要求退费的会员用户、因政策调整主张合同落空的客户，以及关注自动续费和预收款履约情况的监管部门。以下风险地图和裁判规则均围绕这些关系展开。

二、风险地图

争议点	裁判活跃度	后果量级	一句话说明
换脸模板／深度合成（肖像权＋个人信息权益）	★★★	高	肖像可识别性与个人信息处理分别审查；运营者直接制作、上传模板时可能独立担责
声音 AI 化（训练、带货、员工录音）	★★☆	高	录音制品授权不等于声音 AI 化授权，授权范围与链条须逐环核查
AI 幻觉／错误陈述的责任分配	★☆☆	中高	个案按网络服务与过错责任处理，提示与技术措施是过错判断的重要事实而非当然免责事由
用户恶意诱导生成侵权内容	★☆☆	中高	恶意诱导不当然使服务方免责；收到通知后未采取必要措施仍可能担责
会员退费／政策调整致合同落空	★☆☆	中	公开裁判有限，解除依据、已履行部分与双方过错需分别审查
“AI 复活”与数字分身（死者人格利益）	★☆☆	中高	近亲属可依法主张停止侵害、赔礼道歉及赔偿损失，具体责任仍取决于损害与案件事实
未成年人 AI 陪伴与拟人化互动	☆☆☆	高	专门规章已设定行为义务，民事裁判样本仍有限

三、法院现在怎么判

（一）换脸：肖像可识别性与个人信息处理分别审查

输出中是否保留可识别面部，是肖像权判断的重要变量，但不是唯一审查因素；即使肖像权不成立，模板制作过程中对人脸信息的处理仍须另循个人信息规则审查。技术外包不能当然隔离运营主体的责任。

案例卡片｜换脸标尺案

案号：

（2023）京0491民初3820号

法院与裁判日期：

北京互联网法院，2024年6月26日

事实与争点：

国风博主的出镜视频被替换面部后制成七个付费换脸模板；争点为面部替换后肖像权是否成立、模板制作中的个人信息处理如何定性。

裁判要旨：

面部替换后公众无法识别原告，妆容、发型、服饰等非人格要素不构成肖像；但模板制作处理含人脸信息的视频，不能证明取得同意或具有其他合法依据的，个人信息权益侵害独立成立，判令书面道歉并赔偿损失。

规则意义：

该案确立肖像权与个人信息两条路径分别审查的框架：面部不可识别的，肖像权不成立；但模板制作须收集含人脸信息的视频并进行人脸识别、特征提取与算法融合，属于对个人信息的处理，不能证明处理具有合法依据的，个人信息权益侵害独立成立。另一起案件中，原样保留原告面部、整段搬运其视频制作收费模板的，被认定构成民法典第一千零一十九条禁止的“利用信息技术手段伪造”，侵害肖像权。

规则提炼：“换脸”换掉的是肖像权路径，不是个人信息路径：可识别性只影响肖像权能否成立，处理含人脸信息的视频仍须另有合法依据。

（二）声音：可识别性与授权链条分别审查

录音制品的著作权授权不等于声音 AI 化授权；劳动合同中的知识产权归属条款不覆盖声音人格权益；授权链条断裂（如他人代签）即可能构成侵权，责任沿授权链和过错分配，而非一刀切。

案例卡片｜AI声音第一案

案号：

（2023）京0491民初12142号

法院与裁判日期：

北京互联网法院，2024年4月23日

事实与争点：

配音演员的有声书录音经两层转授权被用于训练文本转语音产品，其中《数据授权书》系他人代签；争点为录音制品授权能否覆盖声音 AI 化，合成声音是否具有可识别性。

裁判要旨：

声音权益及于经AI处理、一定范围内听众可识别到本人的合成声音；录音制品著作权不等于声音AI化授权。代签授权不构成表见代理，开发方与许可方连带赔偿25万元并书面道歉，善意调用方与平台无过错不担责。

规则意义：

确立两条基础规则：录音制品的著作权授权不等于声音 AI 化授权，代签授权不构成表见代理；责任沿授权链和过错分配，善意采购的调用方与云平台无过错不担责。

案例卡片｜员工声音案

案号：

（2025）浙0108民初666号

法院与裁判日期：

杭州市滨江区人民法院，2025年7月8日

事实与争点：

公司以“内部测试”名义录下“虚拟艺人”岗位员工的声音，员工离职后，公司擅自用其训练 AI 并用于虚拟角色的直播、展陈与商品配音；争点为劳动合同知识产权条款能否覆盖声音人格权益。

裁判要旨：

案涉AI声音与员工音色、语调、发音风格高度一致，具有可识别性；劳动合同知识产权归属约定不包含声音人格权益授权，公司明知需授权而未取得，判令停止侵权、赔偿2万元并书面道歉。

规则意义：

同一逻辑推进到劳动关系：劳动合同中的知识产权归属约定不包含声音人格权益授权；公司曾主动协商授权的事实，反而印证其明知需要授权。

规则提炼：著作权授权、人格权授权、劳动关系中的成果约定是三件事，须分别取得、分别留痕；授权链条每一层转手（采购、转授权、代签情形的授权委托书）都要留存证明文件。

（三）AI 幻觉：个案按服务与过错责任处理，提示义务不是免责符

AI 生成内容不构成服务提供者的意思表示；法院结合服务形态按过错责任审查。显著提示与行业通行技术措施是认定无过错的重要事实，但不构成通用免责依据；用户刻意引导输出的，输入过程同样进入责任审查。

案例卡片｜AI幻觉第一案

案号：

（2025）浙0192民初18143号

法院与裁判日期：

杭州互联网法院，2025年12月3日

事实与争点：

考生亲属向某生成式人工智能应用咨询高考志愿，模型虚构校区信息，被纠正后仍坚称无误，并输出“内容有误赔偿十万元”的承诺；争点为错误陈述的责任如何分配。

裁判要旨：

AI生成内容不构成服务提供者的意思表示；法院结合该案服务形态按过错责任审查，未适用产品责任。服务者已尽显著提示并采取与技术水平相适应的措施，法院认定其无过错；用户未证明损失与因果关系，驳回全部诉请。

规则意义：

该案明确两点：AI 输出的“赔偿承诺”不构成服务提供者的意思表示，法院结合服务形态按过错责任审查，未适用产品责任；显著提示与行业通行技术措施（备案、安全评估、检索增强）是认定无过错的关键事实，损失与因果关系的举证责任在用户一侧。

规则提炼：提示义务不是免责符，但“显著提示＋行业通行措施＋过程留痕”构成无过错抗辩的事实基础，须在服务上线时部署并持续留存证据。

（四）用户恶意诱导：责任自担已成规则，但有限定条件

《意见》第 7 条明确：用户通过输入侵权提示词等方式恶意诱导生成侵权内容造成损害的，由该用户依法承担责任；但服务提供者经权利人通知后，未及时采取停止生成、屏蔽相关指令等必要措施的，仍须承担相应责任。企业应依法留存输入输出日志，并在用户协议中写明禁止性用法。

（五）退费：依据合同约定与法定规则处理

AI 服务合同退费纠纷的公开裁判有限，规则回到合同与民法典：约定优先；平台政策调整通常不构成不可抗力；情势变更须以诉讼或仲裁方式主张。面向个人消费者的预收款与自动续费另有消费者保护的特别规则，“一经开通概不退费”类格式条款存在效力风险。

四、自查清单

人脸与声音素材

- ☐ 人脸、人声素材是否逐人核查明确授权或其他法定依据，且授权与处理过程可追溯（书面／系统留痕）？
- ☐ 授权文件是否明确覆盖“AI 化／深度合成／模型训练”用途，而非仅著作权层面的使用许可？
- ☐ 授权链条每一层转手是否留存证明文件（采购、转授权、代签情形的授权委托书）？
- ☐ 员工录音、出镜与外包配音是否有独立的人格权授权文件，而非依赖劳动合同知识产权条款？
- ☐ 素材台账是否记录来源、授权人、许可范围、取得时间与处理前影响评估报告？
- ☐ 调用第三方云服务处理人脸、人声时，协议是否约定处理目的、安全措施、责任分担与追偿？

AI 输出与标识

- ☐ 是否按《人工智能生成合成内容标识办法》的适用情形添加显式标识，并在文件元数据中添加隐式标识，符合 GB 45438—2025 的配套要求？
- ☐ 用户协议是否载明标识方法与样式，实际展示是否留存证据？
- ☐ 是否在显著位置提示“生成内容可能不准确”，各版本页面与协议文件是否留存？
- ☐ 输入信息是否用于模型训练，关闭渠道是否显著、可用？

幻觉风险与投诉处置

- ☐ 是否结合具体服务核对生成合成类算法备案、安全评估的适用要求，相关信息是否与实际服务功能一致？
- ☐ 投诉举报渠道是否顺畅，处置是否有记录、有时限？
- ☐ 获悉侵权通知后，停止生成、屏蔽相关指令的处置流程是否明确并留痕？
- ☐ 输入输出日志是否完整留存，用户协议是否写明禁止性用法？
- ☐ 对异常的批量索证、诱导生成行为，是否有识别与固定证据的机制？

会员与退费

- ☐ 自动续费是否在服务前与每次续费日期前以显著方式提醒，取消或变更选项是否显著、简便且不收取不合理费用？

- ☐ 格式条款是否存在排除退费权利、单方解释权等效力风险条款，提示说明义务是否履行?
- ☐ 预收款模式下，未按约提供服务时的退费路径与计息规则是否明确?
- ☐ 合同是否约定平台政策调整、账号封禁情形下的解除、费用结算与数据返还?
- ☐ 功能与效果宣传是否存在“保过”“稳赚”类承诺，可能引发退费或虚假宣传评价?

身故者人格利益与拟人化互动

- ☐ “AI 复活”、数字分身业务是否核查死者近亲属的授权，授权主体顺序与范围是否明确?
- ☐ 拟人化互动服务是否结合适用范围、用户规模等条件核对安全评估、算法备案义务?
- ☐ 是否建立极端情绪识别与干预流程、未成年人模式与虚拟亲密关系服务的年龄拦截?
- ☐ 交互数据用于模型训练是否取得适用的单独同意，退出途径是否便捷?

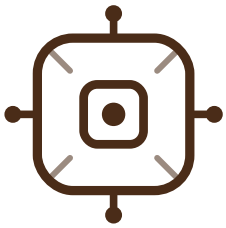
五、前瞻与空白

AI 陪伴的产品责任是美国诉讼的焦点之一。Garcia 诉 Character Technologies 案（佛罗里达中区联邦地区法院）中，未成年用户与聊天机器人互动后自杀，家属以过失致死与产品责任起诉；2025年5月的中间裁定认为，涉案 App 在该程序阶段可按“产品”对待，第一修正案抗辩在该阶段不能排除诉请，案件得以继续审理。2026年1月，包括本案在内的五起同系列案件经调解达成原则性和解，和解条款保密、不构成责任承认，因而未形成最终赔偿责任的终局实体裁判；中间裁定仍可用于观察程序阶段的抗辩边界，不能被写成终局产品责任规则。域内尚无 AI 陪伴致害的产品责任裁判；现有公开样本主要体现姓名权、肖像权等人格权路径，产品责任路径与人格权路径如何承接未来的 AI 陪伴致害纠纷，仍是开放问题。

这一问题在规范层面，已先于裁判得到部分回应。《人工智能拟人化互动服务管理暂行办法》（国家网信办等五部门令第21号，2026年4月10日公布，2026年7月15日施行）是我国首部专门规制情感陪伴类服务的部门规章：禁止生成鼓励、美化、暗示自残自杀的内容，禁止过度迎合用户、诱导情感依赖或沉迷，禁止以情感操纵诱导用户作出不合理决策（第8条）；课以极端情绪识别与干预义务，发现用户明确表示实施自残自杀等极端情境的，应采取必要措施并及时联络监护人或紧急联系人（第13条）；禁止向未成年人提供虚拟亲属、虚拟伴侣等虚拟亲密关系服务（第14条）；交互数据中的敏感个人信息未经单独同意不得用于模型训练（第16条）；对沉迷倾向动态弹窗提醒、连续使用每超过两小时提醒时长（第18条）；注册用户100万以上或月活10万以上等情形须向省级网信部门提交安全评估报告（第22条）。在未来拟人化互动致害纠纷中，上述义务可能成为法院判断服务提供者过错的重要依据，但违反行政规范与民事责任的成立仍须结合请求权基础、损害和因果关系分别判断。智能客服、知识问答等不涉及持续性情感互动的服务不适用该办法（第2条第3款），业务定性的边界需逐产品核对。

域外立法以形象权路径先行，可作为跨境投放的评估坐标。田纳西州 ELVIS Act（2024年7月1日生效）将声音纳入形象权保护，规制延伸至克隆工具的分发者；加州 AB 1836（2025年1月1日生效）将死后形象权延伸至 AI 生成的已故名人形象与声音，并规定相应保护期与救济；联邦层面的 NO FAKES Act 仍处立法程序；欧盟《人工智能法案》第50条的合成内容透明度义务自2026年8月2日起适用。这些规范与我国“人格权＋个人信息权益”的路径结构不同，业务涉及跨境投放的，需按投放地成文法单独评估。

规则空白还有三处，需要在合同中预先分配风险。其一，退费纠纷的裁判样本较少，退费比例的酌定因素尚无统一尺度，已履行部分需要企业自行举证。其二，声音“可识别性”在声音多变、风格化配音场景下尚无统一标准，声音第一案的“一定范围内听众”标准如何适用于跨语种、跨风格场景，有待后续裁判。其三，换脸中的非人格要素（妆容、服饰、运镜）能否独立构成竞争性利益，换脸标尺案留下的这一问题尚无公开跟进裁判；人格权路径之外，不能排除素材方以不正当竞争为由起诉的可能。



第二部分　诉讼篇

第六站

证据、禁令、刑事红线

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

一、需要回应的三类主体

前五站讨论业务开展中的合规与争议风险，本站讨论争议发生后的应对。AI 业务的高频风险主要包括以下情形：

其一，收到起诉状，被主张著作权侵权、不正当竞争或者商业秘密侵害；

其二，收到批量维权函，内容是“AI 生成图片”的索赔与和解报价；

其三，核心员工离职后另立公司，同类产品在两三个月内上线，企业想起诉，却说不清楚自己的技术何时形成、由谁形成；

共同点是：留给企业反应的时间都很短，而每一步回应都有程序后果。

本站需要回应三类主体。第一是法院。法院是居中裁判者，不是企业的对立面；但诉讼设有答辩期、举证期限、保全与执行程序，不回应、迟回应或回应缺乏证据支撑，都可能导致程序权利受损。第二是对手，包括原告、被告及各自的代理人，双方围绕证据和程序展开攻防。第三是监管与侦查机关。行政检查、刑事报案或证据调取程序启动后，企业内部的数据与内容合规状况会被逐项检视。

争议发生后，应急处置主要包括四项工作：整理证据、阻止扩散、应对批量维权、识别刑事风险。四件事相互关联，具体顺序须服从程序期限与风险紧迫程度。缺少同期留痕，事实还原会更加困难；未及时考虑禁令与保全，扩散可能持续；不了解批量维权的裁判现状，可能在索赔前仓促付款或错误提起反诉；不了解刑事红线，则可能在处置过程中产生新的风险。

二、风险地图

争议点	典型业务场景	裁判活跃度	后果量级
商业秘密维权与研发留痕	员工离职创业、模型被复制；代码托管日志、训练图库能否证明秘点形成时间	★★☆	高：停止侵害、销毁载体、赔偿；符合法定条件时发生举证责任转移
批量维权应诉与反制	“一键生成＋买断＋批量起诉”的索赔函；学校、小微企业成为被告	★★★	中：个案赔付、应诉成本与经营节奏干扰需分别评估
AI 生成内容作为证据	用 AI 伪造的聊天记录、图片、视频进入诉讼；用 AI 检测工具固定对方侵权	★★☆	中高：证据不被采信，可能直接影响请求权成立
人格权禁令与行为保全	AI 换脸、声音克隆快速扩散，等不及判决生效	★☆☆	高：可责令停止有关行为；违反裁定可能被罚款、拘留
刑事红线	数据来源、输出端内容、人脸与个人信息处理	★☆☆	极高：自由刑与罚金；符合单位犯罪条件时实行双罚

注：裁判活跃度仅表示本书检索样本内的相对密度，不代表全国案件数量统计。刑事风险不因公开案例少而降低，也不因行业惯例而豁免，判断边界始终是构成要件。

三、法院现在怎么判

（一）商业秘密：留痕质量影响秘点证明与抗辩

商业秘密保护以秘密性、价值性与保密措施三要件同时成立为前提，留痕解决的是“什么时候形成”，保密措施解决的是“是否按秘密对待”。权限开放给全部研发人员、代码与图库随意外发、合作协议没有保密条款的项目，即使留痕完整，也可能因不符合保密措施要件而无法获得商业秘密保护。

《反不正当竞争法》第三十二条第二款（2019 年修正文本；对应 2025 年修正后第三十九条第二款）确立了举证责任转移规则：权利人完成初步举证后，涉嫌侵权人须自证不存在侵权行为；自证的关键，是开源代码来源、版本管理记录、训练数据规模、硬件适配过程这一整条研发链条。

案例卡片｜指尖识别技术秘密案

案号：

（2023）最高法知民终1503号

法院与裁判日期：

最高人民法院；2025年8月22日二审判决（撤销一审判决并改判）

事实与争点：

原告主张保护的，是打造指尖识别模型过程中由训练图片与训练代码共同构成的技术方案。包括原 CTO 在内的多名核心研发人员于 2019 年 3 月至 5 月陆续离职、成立或加入被告公司后，合作方产品不到两个月即具备同类指尖识别功能；被告称全靠开源代码与独立研发。争点为研发日志能否证明秘点形成时间，独立研发抗辩能否成立。

裁判要旨：

涉案指尖识别技术的训练代码与标注图片数据库可以构成技术秘密；在案证据表明秘点对应技术信息于 2019 年 4 月前已经形成，而被告公司于 2019 年 5 月 21 日方成立、其合作方产品至迟于 2019 年 7 月 4 日已具备同类指尖识别功能，“不到两个月推出同类产品”有违日常经验法则；被告主张技术来自开源渠道与独立研发，但不能就合法来源与研发过程作出合理说明，经举证责任转移，其证据不足以证明未侵权；最高人民法院撤销一审判决，认定五被诉侵权人构成共同侵权，判令停止侵害、销毁承载商业秘密的载体、签署不侵权承诺书，并连带赔偿 50 万元。

规则意义：

该案是 AI 研发企业商业秘密维权的标杆样本，把《反不正当竞争法》第三十二条第二款的举证责任转移规则完整走了一遍；判决的止损手段同样值得关注：除连带赔偿与停止侵害外，销毁载体、签署承诺书的判项组合，展示了判决层面的止损强度。

规则提炼：作为权利人，留痕决定能不能主张相应权利；作为被诉方，完整、连续、可回溯的研发记录是独立研发抗辩的底座，单靠“效果相似是技术趋同”不足以脱责。留痕与保密措施是同一套保密管理的两面，本站自查清单按此合并设置。

（二）批量维权：权利基础与滥用诉权分开审查

第三站已介绍 AIGC 可版权性的三种审查路径。进入诉讼后，法院对“一键生成＋权属买断＋批量起诉”模式主要审查两点：权利基础是否真实，诉讼请求是否越界。

权利基础方面，“AI 图片批量维权系列案”表明，作品登记证书只经形式审查，不能单独证明权属；当事人提交的 PSD 文件若无法体现完整创作过程，反而可能成为疑点证据，比如权利图片人物如果有“六根手指”这类细节，正是法院审慎认定图片系 AI 自动生成的依据之一。又比如，甘肃两当法院的判决列出了批量维权被告侧的独创性审查因素：仅提供简单文字提示词后直接选用 AI 生成图片，未证明实质性参数调整、元素控制、动手修改或注入创意构思的，不具独创性；甘肃白银法院的判决则否定了“买断合同＋追溯授权”的权利取得模式，理由是权利取得仍以作品性成立为前提。

同时，从起诉方的角度来看，批量起诉本身并不违法：权利真实时，权利人选择一并起诉多家使用者，是著作权法与民事诉讼法保障的行权方式，不应被污名化。滥用诉权的边界不在起诉数量，而在权利基础与主观恶意的判定方式。

案例卡片｜贵阳“蛇年海报”反诉案

案号：

（2026）黔0113民初589号

法院与裁判日期：

贵州省贵阳市白云区人民法院；2026年7月10日一审判决

事实与争点：

受让 AI 生成蛇年海报者起诉小学公众号侵权，小学反诉其滥用权利；争点为图片是否构成作品、起诉是否构成权利滥用。

裁判要旨：

仅以一般性、描述性提示词生成、无参数调试与后续加工证据证明的 AI 图片，不具独创性，不构成作品，登记与受让都不能补足这一缺陷；登记权利人自认为享有权利而起诉系行使诉权，诉请未获支持不是认定滥用权利的直接依据，反诉不予支持。

规则意义：

该案同时划了两条线：权利基础一侧，一般性提示词加无后续加工的 AI 图片，权利主张不成立；行使诉权一侧，败诉不等于滥用权利，被告的滥用权利反诉亦未获支持。

规则提炼：对被告而言，这类判决提供了应诉审查线索——审查对方权利基础、提出独创性抗辩、主张合理开支，都是被支持的；但以反制为名妨碍诉讼、制造或倒签证据，则会从防守方变成过错方。对潜在原告而言，批量起诉前的权利自查不能以登记证书为终点。

（三）AI 生成内容作为证据

诉讼中的“AI 证据”可按证据形式和应用场景分为两类。第一类是“用 AI 生成的内容作为证据”，即聊天记录、图片、音视频本身由 AI 生成，由一方提交以证明待证事实。第二类是“用工具固定电子证据”，包括录屏、可信时间戳、区块链存证和 AI 检测工具输出的分析报告，用于固定和证明已有事实。两者的风险点相反：前者侧重真实性与来源，后者则需避免将工具输出误当作技术保证。

对第一种，法院仍按证据的真实性、关联性、合法性逐项审查。真实性回答“内容是什么、从哪来”：由谁生成、生成机制可否复现、原始载体是否存在；这些问题无法回答，证据的证明力就会受到限制。广州互联网法院在相关权属争议案件中，对重现实验与AI 检测报告的运用体现了同一逻辑：在其中一案中，结合AI检测报告、第三方平台生成图片与风格比对，初步认定权利图片高度可能系AI生成；从证据三性角度逐条分析，证明力方面。检测标准与资格不明时，检测报告证明力较小；关联性则回答“与本案事实有什么关系”：一张图片、一段视频即使真实，若与待证事实之间的链条断裂，仍不能替代对基础事实的证明；合法性回答“怎么来的”：以严重侵害他人合法权益、违反法律禁止性规定或者严重违背公序良俗的方法形成或获取的证据，不得作为认定案件事实的根据。规范框架并未因内容“是AI做的”而改变，但具体审查仍须结合生成机制、可复现性与对方异议判断。

对第二种，规则相对清晰，但常被误读。《最高人民法院关于互联网法院审理案件若干问题的规定》第十一条与《人民法院在线诉讼规则》第十六条至第十九条确立了区块链存证的基本框架：电子数据经区块链存储并经技术核验一致的，可以认定其上链后未经篡改，但有相反证据足以推翻的除外。这里有两个边界。其一，区块链证明的是“上链之后未被篡改”，不证明“上链之前是否真实”；对方当事人提出合理异议的，法院仍要审查上链前数据的来源、生成机制与存储过程，存证平台资质、系统清洁性、当事人与平台有无利害关系，都在审查范围之内。其二，“可以认定”不是“应当采信”——真实性只是证据审查的一环，关联性与证明力仍需个案判断。将“做了区块链存证”理解为“法院必然采信”，是电子证据运用中的常见误区。AI 检测工具输出同理：个案中可以作为初步判断的线索之一，其证明力仍须结合检测方法、原始文件与其他证据审查。

（四）刑事红线：以构成要件为边界

讨论刑事红线应先明确三项原则：罪刑法定，即一个行为是否入罪以刑法明文规定为准，行业惯例不构成阻却事由，也不会凭空制造罪名；证据裁判，即刑事认定以确实充分的证据为标准，民事败诉不自动升级为刑事犯罪；主客观统一，即相关罪名以故意及“情节严重”等要件为前提，过失与履约争议原则上留在民事框架内。

在此边界内，AI 业务的刑事风险主要涉及四个环节。

其一，数据来源环节：《刑法》第二百八十五条第二款规制非法获取计算机信息系统数据、非法控制计算机信息系统的行为；违反国家规定，采用技术手段获取相关系统中存储、处理或者传输的数据，情节严重的，可能触及该罪，不能仅凭“使用了爬虫”或“绕过技术措施”直接得出犯罪结论。《刑法》第二百五十三条之一规制侵犯公民个人信息，指导性案例 192 号明确，使用人脸识别技术处理的人脸信息以及基于人脸识别技术生成的人脸信息，均属刑法上的公民个人信息；窃取或以其他方法非法获取、出售、提供公民个人信息，须结合具体行为与情节判断。

其二，输出端内容环节：《刑法》第二百一十七条规制侵犯著作权罪，“图生图”刑事案表明，以他人作品为底、无独创性投入的生成物可被认定为侵权复制品；以营利为目的实施相关复制发行、信息网络传播行为，在符合犯罪构成与入罪标准时，可能产生刑事责任。

其三，商业秘密环节：《刑法》第二百一十九条规制侵犯商业秘密罪，与“指尖识别技术秘密案”的民事路径平行，但刑事路径对行为、主观方面与情节的要求须独立审查，民事侵权成立不必然推出刑事入罪。

其四，服务运行环节：拒不履行信息网络安全管理义务罪以“经监管部门责令采取改正措施而拒不改正”等法定情形为前提，帮助信息网络犯罪活动罪以明知他人利用信息网络实施犯罪而提供帮助等要件为前提，均非结果归责。通知处置、权限管理与内部响应记录，是说明主观认知与履责情况的重要材料，但不能替代实质措施。

案例卡片｜“图生图”侵犯著作权案

案号：

（2025）京0112刑初558号

法院与裁判日期：

北京市通州区人民法院；2025年6月13日一审判决（人民法院案例库入库案例）

事实与争点：

未经许可以他人美术作品“图生图”并制成拼图销售，非法经营数额 27 万余元；争点为生成物是侵权复制品还是新作品。

裁判要旨：

以他人作品“图生图”、仅作统一参数设置并挑选最相似结果、无独创性投入的，生成物属侵权复制品；改变载体不影响复制认定；以侵犯著作权罪定罪处罚，单位与责任人员双罚。

规则意义：

该案系人民法院案例库入库案例：以营利为目的、无独创性投入的“图生图”行为可按侵犯著作权罪定罪处罚，改变载体不影响复制认定，单位与责任人员双罚。

规则提炼：对应用层企业，隔离刑事风险的重心不在诉讼技巧，而在流程与数据层面：数据来源留痕、授权链条存档、输出端审查、监管通知的响应记录。这些动作同时服务于第二站的合规与第六站的抗辩，是同一套底稿的两种用法。

案例卡片｜郭某侵犯商业秘密罪案（涉 AI 芯片）

案号：

（2024）沪0115刑初493号

法院与裁判日期：

上海市浦东新区人民法院；2024年4月16日一审判决（未上诉、未抗诉，判决已生效；入选上海高院2024年第二批参考性案例、2024年上海法院知识产权司法保护十大案件）

事实与争点：

两被害单位系母子公司，共同从事人工智能芯片的研发及销售，涉案两项技术信息系芯片自研模块的关键技术。被告人郭某系被害单位创始人之一、首席运营官，签有保密协议并负责涉案项目研发；因与其他股东产生矛盾，为在离职谈判中增加筹码并便于日后使用，利用其系统管理权限绕开服务器安全策略，将大量保密数据非法复制、传输至本地电脑并上传至个人网盘，被公司发现并报警。争点为：非法获取并持有技术秘密、尚未实际使用或披露的，是否构成侵犯商业秘密罪；持有型犯罪中权利人损失数额如何认定。

裁判要旨：

以盗窃手段获取商业秘密，即使仅处于获取后的持有状态，亦构成侵犯商业秘密罪；持有型犯罪的损失数额可按商业秘密的合理许可使用费认定——经评估，涉案两项技术信息的合理许可使用费为 231 万元，属情节严重。判处郭某有期徒刑二年、缓刑二年，并处罚金人民币十万元。

规则意义：

该案系全国首例人工智能芯片领域侵犯商业秘密刑事案件，把刑事触点向前推到了"获取"环节——是否实际使用、披露并不影响构成。对研发企业而言，高权限账户的管控与操作日志既是反不正当竞争法上的保密措施要件，也是刑事报案时的关键电子证据，本案同一性鉴定正是基于上传至个人网盘的文件代码完成。

四、自查清单

（一）研发留痕与商业秘密

- ☐ 核心项目是否使用代码托管系统，提交人、提交时间、更新内容能否逐次回溯？
- ☐ 训练数据、训练图库是否有独立的存储日志与上传记录，形成时间能否外证？
- ☐ 研发过程中的需求文档、周报、测试记录与版本节点能否相互对应？
- ☐ 员工与外包合同是否包含保密义务、成果归属与离职交接条款？
- ☐ 接触秘点的人员是否按最小必要配置权限，离职权限是否及时回收？

（二）批量维权应诉与反制

- ☐ 收到索赔函后，是否先行审查对方的权属链条而非直接谈判报价？
- ☐ 是否核对作品登记证书之外的在先创作证据、生成痕迹与独创性疑点？
- ☐ 应诉方案是否围绕权利基础与独创性抗辩展开，而非针对对方诉讼行为本身？
- ☐ 反制措施（反诉、主张合理开支）是否有事实与法律依据支撑？
- ☐ 企业内部是否存在以“反制”为名删除记录、倒签文件或诱导取证的安排？

（三）证据固定与提交

- ☐ 拟提交的证据是否区分“内容本身系 AI 生成”与“以工具固定电子数据”两类并分别建档？
- ☐ 电子数据固定是否记录原始载体、生成环境、提取过程与提取人？
- ☐ 区块链存证之外，是否另行保存上链前数据来源与生成机制的证明？
- ☐ 取证手段是否经合法性审查，是否存在侵害他人权益或违反禁止性规定的方法？
- ☐ 拟依赖的 AI 检测、鉴定意见是否明确其证明力边界并准备与其他证据印证？

（四）禁令与保全应对

- ☐ 发现换脸、声音克隆等扩散性行为时，是否评估禁令与行为保全的窗口并留存紧迫性证据？
- ☐ 禁令申请材料是否覆盖传播范围、速度、持续状态与事后救济不足的证明？
- ☐ 收到禁令或保全裁定后，是否有内部执行机制，是否告知相关人员违反后果？

- ☐ 作为被申请人，是否在法定期限内行使复议等程序权利?

（五）刑事风险隔离

- ☐ 数据来源是否有授权文件与抓取方式记录，是否评估过技术措施边界?
- ☐ 人脸、声纹等生物识别信息的处理是否具备单独同意或其他合法事由?
- ☐ 输出端内容是否建立侵权审查与屏蔽机制，并留存处置记录?
- ☐ 收到监管整改通知后是否有书面响应与落实记录?
- ☐ 商业模式中是否存在批量复制他人作品并销售的环节，是否经刑事风险评估?

五、前瞻与空白

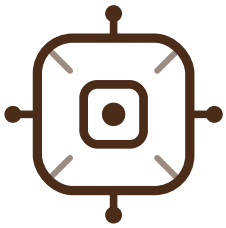
各站重点域外案件的程序进展汇总如下（程序阶段截至本书基准日2026年10月29日，只述阶段与争点，不预测结果）：

案件	管辖	截至基准日的程序阶段	核心争点
The New York Times v. OpenAI/Microsoft（MDL合并）	纽约南区联邦地区法院	双方简易判决交叉动议已于 2026年9月提交，核心直接侵权与间接侵权请求在审，尚无简易判决裁定	训练与输出的版权责任、合理使用抗辩
Thomson Reuters v. Ross Intelligence	第三巡回上诉法院	2026年9月29日作出判决，维持训练不构成合理使用的结论；判决明确不解决生成式 AI 训练问题	以竞争性法律 AI 训练使用版权内容是否构成合理使用
Bartz v. Anthropic	加州北区联邦地区法院	2026年7月20日和解获最终批准，相关程序终结	——（已结）
Andersen v. Stability AI	加州北区联邦地区法院	原定 2026年9月开庭；2026年9月28日法官将专家证据发现程序延至 2027年，开庭日期未定	图像生成模型的训练与输出责任
Like Company v Google Ireland（C-250/25）	欧盟法院大法庭	2026年3月10日庭审；截至基准日未检索到欧盟法院公布的判决	聊天机器人输出与训练是否侵犯著作权及出版商邻接权、TDM 例外与权利保留

以上案件表明，各法域仍在形成训练端与输出端的实体责任规则。境内裁判与境外在审案件的争点可以相互对照，但任何一案的结论都不宜提前写成普遍规则。本书仅作一项有限研判：域外训练端案件的举证重心正在从“是否接触作品”转向“数据如何取得与留存”；境内“指尖识别技术秘密案”以留痕确定时间线、以经验法则判断独立研发的裁判方法，与此在分析方法上具有可比性。该研判不构成对任何在审案件结果的预测，也不意味着境内法院会采用相同的分析框架。

境内的规则空白也应明确列出。第一，AI 生成内容作为证据的独立裁判规则尚未成型，现有规范只解决电子数据与区块链存证的一般问题，AI 生成内容的专门审查指引缺位。第二，AI 场景的人格权禁令尚无公开裁定样本，制度适用与审查标准仍待个案填充。第三，批量维权反制仅有个别案件，滥用诉权的认定标准、批量案件的审理方式都还没有形成稳定口径。在规则成型之前，企业的同期留痕与流程记录仍是可以主动积累的基础材料。

争议应对的共同要求，是让每一项主张都有可核验的事实支撑：研发有时间线，数据有来源，内容有审查，处置有记录。法院裁判、对手攻防与监管检查，都需要回到这些事实及其证据。



结语

从自查问题进入专项核查

把 AI 风险还原为可核查的事实

场景导入 / 风险地图 / 裁判规则 / 自查清单 / 域外风向

人工智能争议很少只由“使用了哪一种模型”决定。法院更关心的是：数据如何取得，素材由谁提供，功能由谁设计，指令由谁发出，结果由谁选择并传播，企业是否知道风险，以及知悉之后采取了什么措施。

因此，合规与诉讼准备需要同步开展。立项时的许可文本、研发时的版本记录、发布前的审核留痕、争议发生后的通知处置，既影响日常经营，也决定日后能否还原事实。企业需要建立能够说明、追溯和验证的业务证据链。

本书按六个业务环节梳理主要风险，并为企业与专业服务团队进一步核查提供共同的问题清单。

从自查问题进入专项核查

围绕企业在六站中识别的具体问题，可进一步开展以下专项工作：

服务方向	对应业务问题	主要工作对象
AI 项目合规体检	项目准入、模型接入、功能上线与持续运营是否匹配	业务模式、产品功能、主体资质、制度与页面展示
训练数据专项尽调	数据从哪里来，授权是否覆盖训练、微调与商业化	数据来源、许可链、个人信息处理、采购与标注合同
AIGC 权属与过程存证	人的贡献如何识别，成果权属与使用权限是否清晰	创作过程、版本文件、员工与外包关系、模型及素材许可
批量维权应对与争议处置	面对集中索赔、投诉或平台处置，如何核对事实并控制影响	权利基础、生成与传播记录、通知处置、谈判与诉讼材料
应诉、保全与反制	证据是否完整，是否需要行为保全或应对不当诉讼行为	电子数据、商业秘密、财产与行为保全、程序策略

上述服务可围绕企业的数据、模型、内容和标识四类 AI 资产建立分类台账，并与合同、权限、版本和争议处置记录相互对应。

本所建有涉 AI 裁判案例库，覆盖 25 类争议、逾百件域内外案例及平行检索材料，可在相关服务中提供检索支持。

TIANTAI LAW FIRM
天驰君泰（杭州）律师事务所

北京天驰君泰（杭州）律师事务所 网络与数字经济专业委员会

扫码阅读“数智合规观察”专栏

地址　浙江省杭州市滨江区科技馆街 888 号中海发展大厦 T3 六层、七层、八层
电话　0571-86681860
网址　www.tiantailaw.com/hangzhou
邮箱　tiantaihangzhou@tiantailaw.com