

汉坤法律评述

2026 年 9 月 9 日

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

首个涉 AI 司法文件落地：最高人民法院《关于依法审理涉人工智能纠纷案件的意见》评述

作者：王焱 | 俞琳 | 钟奕 | 赵子璠

2026 年 9 月 7 日，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，以下简称《意见》），即日施行。次日，最高人民法院研究室主任周加海等五位起草人撰写了《〈最高人民法院关于依法审理涉人工智能纠纷案件的意见〉的理解与适用》（以下简称《理解与适用》），对起草背景、起草原则和重点条文的形成过程作了详细说明。规则文本与起草说明相互印证，使这份仅二十四条的文件呈现出远超其篇幅的信息量。

近几年，我们在处理人工智能相关诉讼和合规咨询时，反复遇到同一个问题：现行法律能否回答新技术提出的争议。《意见》给出的方法是“用足用好现有法律规定”——在专门人工智能立法尚未启动的现阶段，以民法典、个人信息保护法、著作权法、反不正当竞争法、产品质量法等既有规范为基础，整合适用于人工智能场景。这也意味着，《意见》不是一份宣示性的政策文件，而是一套可以直接在法庭上引用的裁判规则。以下按照实务中最常被问及的几个问题，谈谈我们的理解。

一、归责原则与平台责任：过错责任为基线，避风港落定、红旗未落

归责原则是《意见》的“题眼”。理论界曾存在观点认为由于人工智能具有高度自主性和不可解释性，应当适用高度危险责任等无过错责任。如今《意见》第 3 条给出明确的答案：“利用人工智能侵害民事权益产生的法律责任，应当依照民法典第一千一百六十五条第一款规定的过错责任原则认定行为人是否承担侵权责任。”《理解与适用》进一步专门解释了生成式 AI 不应适用无过错责任的理由：无过错责任多以高度危险为前提，而生成式 AI 仅向人类提供信息，一般不直接危及人身、财产安全，因而与无过错责任体系不具有相似性。《意见》同时结合 AI 自身特点给出了六个过错考量因素，即①应用场景②自主化程度③技术与信息透明度④潜在风险及影响范围⑤相关主体为预防和减少人工智能侵权所采取的措施及技术上的可能性⑥使用者对损害的预见能力与控制能力，换言之，是否采取与现有技术水平和风险程度相匹配的防范措施，将成为是否存在过错的重要判断因素。企业的风险提示、功能说明、防控记录，日后可能就是法庭上直接的无过错抗辩的证据。例如全国首例“AI 幻觉”侵权案中¹，法院认为“服务提供者已履行服务功能的显著提示说明义务、功能可靠性的基本保障义务和服务协议约定的注意义务等应尽注意义务的，可以认定其不具有过错。”

¹ （2025）浙 0192 民初 18143 号。

平台责任方面，第7条确立生成式AI服务提供者参照适用避风港规则：经权利人通知后生成式AI服务提供者未及时采取停止生成侵权内容等必要措施的，方承担责任。考虑到生成式AI的技术特征，两处调适尤具实务意义：一是对权利人“通知”的认定门槛实质降低，由于人工智能往往是“点对点”生成私密内容，权利人难以获得或者提供侵权内容的公开网络链接，因此权利人以模拟输入提示词、技术测试等方式合理证明侵权内容生成即构成有效通知；二是“必要措施”从“清除既存侵权”变为“防范继续生成”，核心是停止生成侵权内容、屏蔽相关生成指令。这意味着生成式AI平台的避风港义务不再局限于事后删除，而是进一步延伸至对侵权内容持续生成风险的技术控制。

值得注意的是《意见》未对“红旗规则”的适用作出规定。所谓“红旗规则”是指网络服务提供者知道或者应当知道网络用户利用其网络服务侵害他人民事权益而未采取必要措施，则与实施侵权行为的网络用户承担连带责任。《意见》征求意见稿曾写入“知道或者应当知道”具体判断标准，最终因产业界认为可能对AI服务提供者施加过重注意义务而删除，但《理解与适用》同时强调未规定不等于排除适用，如有确有证据证明平台对AI侵权内容进行编辑、筛选、推荐的，仍可能被追责。

二、开源软件：首个责任豁免规则

《意见》第13条首次在司法规则层面明确了AI开源软件相关方可能承担的法律风险，并从以下四个因素出发，为个案中适当认定开源软件相关方的注意义务及责任豁免提供了判断依据：①开源许可协议类型②权利限制的具体内容③安全合规措施④信息披露程度。上述因素实际上体现了“开源并不当然免责，责任应与风险控制能力相匹配”的基本思路。其中，信息披露义务尤其值得关注。《意见》进一步明确指出，如果以“免费开源方式”提供代码模块并“公开说明其功能和安全风险”的，他人使用该代码导致侵权的，可以认定其不承担责任。换言之，对于开源软件相关方而言，充分、明确的风险披露不仅是开源治理的重要合规措施，也可能直接影响其在具体侵权纠纷中的责任认定。同时，《理解和适用》还披露，条文最初对豁免规定得较为绝对，征求意见后改为“可以认定”，其表明满足相关条件并不意味着开源软件相关方可以当然、绝对地免除责任，法院仍需结合具体案件进行判断，从而为个案裁量留了空间。从企业合规角度看，AI开源项目的运营者、代码贡献者及平台方未来应更加重视开源过程中的风险留痕和信息披露。例如，应当明确开源许可的具体范围及限制条件，对已知功能和安全风险进行充分说明，并根据项目特点采取必要的安全测试、漏洞管理及合规措施。相关措施不仅有助于降低实际侵权风险，也可以在发生争议时形成证明自身已尽合理注意义务的重要证据。

三、专利与数据权益：AI创新活动的两颗“定心丸”

专利方面，《意见》第14条明确了涉AI发明创造的专利保护边界，为涉AI的创新活动给出稳定的法律预期。根据该条，采用遵循自然规律的技术手段，解决了技术问题、实现了符合自然规律的技术效果的涉人工智能发明创造，属于专利法保护的客体。对于自然人使用人工智能完成的发明创造，只要该自然人对实质性特点作出创造性贡献，即应当认定其为发明人，这延续了“人工智能是工具而非主体”的基本立场。可以预见，“是否对实质性特点作出创造性贡献”将成为涉AI专利确权与权属争议的核心争点。相应地，企业在AI辅助研发过程中，应更加重视研发过程的留痕和证据保存，包括研发过程记录、实验数据、提示词及输出结果、技术方案迭代记录以及设计文档等，以证明自然人在技术方案形成过程中所发挥的实质性、创造性作用。换言之，AI参与研发越深入，对研发过程证据化、可追溯性的要求就越高。

数据权益方面，第16条构造了较为清晰的涉AI数据使用的四种保护路径：①合法获取的数据权益受保护；②构成汇编作品的依著作权法；③构成商业秘密的依反不正当竞争法商业秘密条款；④对于不构成商业秘密的数据，由反不正当竞争法第十三条关于数据权益保护的规定予以兜底。此外，虚构干扰数据、恶

意标注、对抗样本攻击等损害 AI 运行安全的行为，被明确列为违法行为。经营者利用数据、算法等技术手段构成垄断的，应承担相应责任。这一分层保护思路也对企业的资产管理提出了更明确的证据要求：选择著作权保护路径的，应重点留存数据或数据集的独创性证据；主张商业秘密保护的，应重点落实并留存相应的保密措施证据；适用反不正当竞争法数据保护路径的，则应重点证明企业在数据获取、整理、加工、维护等方面的实质性投入。因此，企业未来的数据权益保护不能仅停留在“数据归谁所有”的层面，而应根据不同数据类型提前确定保护路径，并同步建立与相应法律要件相匹配的证据体系。

四、著作权侵权：责任分配的逻辑与举证天平的校正

关于 AI 生成内容侵害著作权的责任认定，《意见》第 12 条确立了“责任承担与控制能力相匹配”的基本原则，从①人工服务类型②行业特点③训练数据来源④各方参与度、采取的必要措施和⑥获利情况等六个维度，对不同主体的责任认定进行综合考量。《意见》将相关责任落实至两类主体：生成式人工智能服务使用者系生成、选择和传播的直接行为人，其在知道或应当知道在先作品存在而利用人工智能生成实质相似内容时，不能仅以内容系 AI 生成为由免责；对人工智能服务开发者及提供者而言，其在知道或应当知道使用者侵权而未采取必要措施时，同样需要承担连带责任。

我们认为，《意见》第 12 条中最具有实务意义的，是对 AI 侵权纠纷中的举证责任进行双向校正。一方面，权利人无需在诉讼初始阶段就证明人工智能模型内部的全部运行机制，原则上仅需就侵权内容系由相关人工智能生成、以及该内容与其权利作品构成实质性相似等基本事实承担初步举证责任。在针对 AI 使用者的侵权主张中，权利人只需举证证明行为人已经接触过在先作品，或者具有接触在先作品的可能性；在此基础上，可以推定行为人知道在先作品的存在，从而降低权利人面对复杂 AI 生成过程时的举证难度。另一方面，《意见》也没有将所有举证责任一概转移给开发者和提供者。如果 AI 开发者提出不侵权抗辩，则需要就模型的训练数据来源、训练过程记录、模型运行模式以及相关科学理论依据等进行举证和说明。这意味着，在传统技术侵权案件中长期存在的“算法黑箱”与信息不对称问题，将在一定程度上通过举证责任的合理配置得到缓解：对于掌握模型训练数据和技术资料的一方，其不能仅以技术复杂、商业秘密或内部信息为由作概括性抗辩，而需要在其主张不侵权时，对关键技术事实提供相应证据予以佐证。

结合《意见》第 17 条的证据妨碍及不利推定的相关规则，这一举证责任安排的实际影响可能更为显著。如果开发者、服务提供者掌握相关训练数据、训练过程记录等关键证据，却无正当理由拒不提供，相关证据缺失可能进一步影响法院对其抗辩及责任的判断。因此，从企业风险管理角度看，AI 企业未来在模型开发和迭代过程中，应当建立完整、可追溯的训练数据溯源机制，保存数据来源及授权情况、数据清洗和处理记录、训练过程记录、模型版本迭代记录以及风险测试和干预措施等材料。这样既有助于企业履行相应的注意义务，也能够在未来发生知识产权争议时，为不侵权抗辩及责任划分提供关键证据。

五、产品责任、自动驾驶与消费者保护

《意见》第 9 条以《产品质量法》为基础，进一步将“人工智能产品”限定为以实物为载体的产品（如具身智能机器人、自动驾驶汽车等），生成式 AI 服务则被排除在外，以免无过错责任泛化。人工智能产品的缺陷认定着重审查生产者、销售者是否就该产品的适用场景、固有局限和可预见风险作了真实说明与明确警示。在此背景下，是否履行充分的风险提示和信息披露义务，可能成为人工智能产品诉讼中相关责任认定的重要考量因素。

《意见》还围绕自动驾驶事故责任的认定这一业内高度关注问题构建了四层分析结构：第一，自动驾驶事故原则上仍适用现行交通事故责任认定规则；第二，随着自动驾驶系统对车辆控制权的提高，侵权责任将

逐渐由驾驶员过错责任过渡至产品责任；第三，在车辆缺陷与驾驶人过错共同导致损害的情况下，受害人可以同时向驾驶人以及生产者、销售者主张责任；第四，对于就自动驾驶等级、智能化程度等进行虚假或误导性宣传的行为，相关主体还可能承担相应民事责任。在举证责任方面，《意见》明确，人民法院可以要求相关车企提供真实、完整的自动驾驶事件记录数据，为事故责任认定提供依据，在一定程度上缓解受害人在技术信息不对称情况下的举证困难。

针对消费者权益保护，《意见》对“大数据杀熟”等差别待遇行为采取更为精细化的认定路径，强调需同时考察差别待遇行为及其不合理性，动态调价、新客优惠等具有合理商业目的或其他正当理由的差异化经营行为通常不属于规制范围。对于利用人工智能技术仿冒名人开展商业宣传并构成欺诈的行为，消费者可依法主张惩罚性赔偿。

六、人格权与个人信息：两条高频业务线的规则要点

人格权方面，《意见》第4条、第5条、第8条分别针对深度合成技术应用、网络“开盒”乱象和预防性救济机制作出回应。要点有四：其一，肖像可识别性的判断不要求人工智能生成内容与本人完全一致；即使AI换脸后与本人存在差异，或未直接呈现面部特征而使用整体外部形象，若公众仍能识别出特定自然人，同样可能构成对肖像权的侵害；此外，偶发性的“AI撞脸”也不能成为当然的免责事由；其二，对已故自然人虚拟数字形象的使用提供了合规路径；在死者生前已作出相关授权，且使用行为不违反公序良俗的情况下，被授权人可以依法使用相关虚拟数字形象；对于涉及数字人、虚拟形象等商业应用的企业而言，完善授权链条将成为业务开展的重要前提；其三，明确非法网络“开盒”与合法数据分析的关键界限在于是否以“刺探隐私为目的”；其四，人格权禁令可责令服务提供者停止提供有关服务，维权重心得以从“事后索赔”前移至“事前阻断”。

个人信息部分，第6条给出训练数据合规迄今最明确的司法标准：为模型训练，在合理范围内处理已合法公开的个人信息且个人未明确拒绝的，一般不构成侵权；对个人权益有重大影响的，应取得同意。在“合理范围”的判断因素中，“公开时的场景以及合理预期”最值得平台注意——人工智能训练应符合用户对信息使用场景的合理期待。若平台已通过用户协议、公告等明确声明用户公开内容的具体用途，后续擅自将包含个人信息的内容用于未声明的AI训练，可能构成对用户合理预期的突破。

七、两处留白，以及我们的判断

《意见》最有深意的安排，也许在于它没有规定什么。人工智能生成内容的可版权性、未经许可使用他人作品训练大模型的定性——两个争议最大的问题均未作规定。《理解与适用》同样指出，目前理论界和实务界针对上述问题远未达成共识，全球立法亦无相关先例。

我们的判断是，留白不会持续太久。从产业发展情况看，人工智能生成内容的创作与商业化应用正在加速推进，市场上已出现以《后西游记》等AI影视剧集为代表的优质AIGC作品，进一步展现了人工智能生成内容的应用潜力与商业价值。从域外司法实践看，美国 *Bartz v. Anthropic* 案等代表性案例已开始通过个案裁判进一步厘清AI训练场景下合理使用的适用边界及相关侵权责任，相关司法规则正加速成型。从既往司法实践看，对于新技术发展所带来的法律适用问题，人民法院通常会通过个案裁判，并结合指导性案例、典型案例等方式逐步明确裁判规则。事实上，自2023年“人工智能文生图第一案”²以来，人民法院已开始围绕人工智能问题展开司法探索，而《意见》第22条的提级管辖机制则进一步为涉AI诉讼的统筹指导准备

² （2023）京0491民初11279号。

了程序通道。

这至少意味着两个方面的变化。其一，涉 AI 纠纷可能进入裁判规则加速形成的阶段。由于现阶段成文规则仍有较多留白，早期典型案件的裁判思路和规则提炼，可能对后续同类案件产生较强的示范和引导作用。因此，无论对于原告还是被告，早期案件都不宜仅作为孤立个案看待，其诉讼策略和裁判结果可能具有超出个案本身的影响。其二，企业 AI 合规也需要进一步强化诉讼视角。相较于备案、标识等行政合规要求，训练数据能否有效溯源、侵权通知与处置机制能否形成闭环、开源许可及相关权利链条是否清晰、对外宣传是否与产品实际能力及自动化程度相匹配等问题，都可能直接影响未来诉讼中的事实认定、举证责任和责任承担。换言之，AI 合规不仅需要满足监管要求，也需要经得起司法审查。而在规则尚未完全定型的领域，如何将抽象的法律原则转化为可执行的业务规则，并提前为潜在争议保留证据和抗辩空间，也正是专业服务价值密度最高的领域。

结语

《意见》的颁布，标志着我国涉人工智能纠纷的司法应对从个案探索进入体系化规则阶段。二十四条规则划定了当下的裁判框架，两处留白预留了未来的博弈空间。对产业界而言，关键问题已经不在于人工智能领域是否会形成司法规则，而是如何在现有规则框架与未来发展趋势之间，提前完善合规体系、优化业务安排，并有效管理潜在的法律风险。我们团队将持续跟踪人工智能领域的裁判动态，并围绕人工智能知识产权、数据权益保护、平台责任、合规体系建设及争议解决等重点议题开展系列研究，期待与各界就人工智能发展中的法律问题展开深入交流。

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：

王焱

电话： +86 21 6080 0200

Email: yan.wang@hankunlaw.com

俞琳

电话： +86 21 6016 9780

Email: lin.yu@hankunlaw.com