HANKUN

汉坤法律评述

2026 年 10 月 27 日

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

AI 与算法创新的专利保护（下）：规则重塑下的保护与布局策略 — 从维权举证到攻防一体

作者：吴丽丽 | 俞琳 | 郑天禹 | 徐天一 | 周菁

上篇讨论了算法创新确权端的四个问题：客体适格性、创造性判断、申请文件披露与发明人认定；贯穿其中的主线，是“技术性”论证重心的前置化 — 技术性的论证应当在撰写阶段就完成结构性的布置。获得授权只是保护的前半程 — 权利能否在诉讼中兑现，算法资产应当如何在专利、商业秘密与开源之间配置，跨境布局又如何应对不同法域的口径差异，构成本篇讨论的三个问题。

一、确权与维权：更具操作性的司法规则

在确权端，司法对客体的判断逻辑与上篇介绍的审查标准已趋于一致。最高人民法院知识产权法庭在“容错算法区块链共识方法”发明专利授权案中明确：区块链本身虽是一种数据结构，但若权利要求限定的区块链算法针对具体应用场景，融合分布式网络、共识算法与密码等技术形成综合性解决方案，其算法步骤的执行能够直接体现利用自然规律解决技术问题的过程并获得技术效果，即可构成专利保护客体[1]。本案要旨的参照意义不限于区块链：算法类方案的客体认定，司法机关看的同样是技术关联的实质 — 算法特征与技术特征是否构成一个整体、该整体是否采用了利用自然规律的技术手段 — 主题名称的标签并不起决定作用。

在维权端，算法的“黑箱”曾长期构成侵权比对的实质障碍，而近年的裁判案例正在打开缺口。在涉“视觉识别领域人工智能及算法”技术秘密侵权案中，最高法明确，可以综合考虑被诉侵权人有无接触技术秘密的可能性、被诉侵权技术信息的研发形成过程、人工智能模型训练的基本原理、被诉侵权产品与权利人产品在相同场景下的反应比较以及日常生活经验法则等因素，判断技术秘密是否被使用。[2]更早的指导性案例中，数十名接触技术秘密的人员短期内集中离职、被诉方在明显短于独立研发合理周期的时间内实现产品量产，法院据此减轻权利人的证明负担，推定被诉方获取、使用了全部案涉技术秘密[3]。

[1] “容错算法区块链共识方法”发明专利授权案，(2024)最高法知行终 573 号，最高人民法院，裁判要旨载《最高人民法院知识产权法庭裁判要旨摘要（2025）》（2026 年 4 月 22 日发布）。

[2] 涉“视觉识别领域人工智能及算法”技术秘密侵权案，（2023）最高法知民终 1503 号，最高人民法院知识产权法庭，裁判要旨载《最高人民法院知识产权法庭裁判要旨摘要（2025）》。

[3] 最高人民法院指导性案例第 273 号（浙江吉某控股集团有限公司等诉威某汽车制造温州有限公司等侵害技术秘密纠纷案，“加大科技创新知识产权司法保护力度”专题指导性案例，2026 年 2 月 28 日发布）。

缺口能否被利用，取决于留痕的质量。回到贯穿确权与维权两端的那条线索：发明人认定要求留下“人类创造性贡献”的痕迹，维权举证要求留下“研发实质推进”的痕迹，两者是同一个问题的两端，即人类贡献的可证明性。证明负担移转的触发，高度依赖权利人自身研发记录的质量 — 如果权利人无法清晰呈现“从开源基础等现有技术到产品之间究竟做了什么”，移转的杠杆就缺少支点。还需指出的是，专利侵权与技术秘密侵权中的举证规则依据不同，前者涉及新产品制造方法专利举证责任倒置的特别规定，后者源于反不正当竞争法第三十二条第二款的移转规则；但两者的底层困境同源 — 被诉方案的内部实现不为外人所见，而证据规则正在各自的轨道上回应这同一个困境。

救济力度也在同步加强。对于生效裁判认定侵权后继续实施相同或类似行为的侵权主体，人民法院已在多起案件中支持惩罚性赔偿，技术类案件的判赔水平整体呈上升趋势[4]。这些信号共同指向一个朴素的结论：权利要求撰写阶段就应预演取证路径 — 能够被外部观察或检测到的特征，才是诉讼中真正有价值的特征。

以上讨论多站在权利人一侧；视角切换到被诉方，信号同样清晰。2026 年 7 月，田纳西大学研究基金会（UTRF）在美国特拉华联邦地区法院起诉 Anthropic，主张其 Claude 系列产品侵犯两项神经网络基础专利 — 两项专利均于 2018 年授权，技术方案源自高校研究组更早年份开展的类脑计算研究，一件覆盖人工神经网络组件的构建与复用方法，另一件覆盖动态自适应神经网络阵列的构建[5]。该案被认为是 Anthropic 面临的首起专利侵权诉讼。它标示的方向是：人工智能领域的知识产权争端，正从训练数据与人工智能生成内容的版权，拓展至模型底层架构的专利。与著作权纠纷不同，专利侵权不以接触或复制为前提，独立研发不能构成抗辩 — “黑箱”的困境在此呈现镜像形态：被诉产品的内部实现对外部观察者同样不可见，风险排查的难度并不亚于权利人的举证。高校与科研机构在早期布局的基础专利，开始成为针对大模型企业的诉讼标的。

二、保护路径的组合：专利、商业秘密与开源

算法类创新中，核心算法信息与外围技术方案在可专利性、保护的有效性与公开后果上差异很大，单一依赖专利往往不是最优解。“核心算法以商业秘密保护、外围技术方案以专利覆盖”的复合模式，正在成为越来越多人工智能企业的实际选择。

分层的逻辑大致如下：算法与硬件或具体技术场景结合形成的、可被外部观察和检测的技术方案，可以以专利作为主要保护方式，以公开换取排他性权利；核心模型权重参数、超参数配置、数据清洗规则等不易被反向工程的部分，则留在“技术黑箱”之内，以访问控制、保密协议与竞业等安排构建商业秘密防线。一个简明的判断框架是：可观察性高、生命周期长且不易被规避设计的创新优先专利；反之倾向商业秘密。而连接两边的，正是上篇讨论的披露边界控制 — 说明书写到哪一层，商业秘密的防线就退到哪一层。

开源是当下极具讨论价值的一条路线。对人工智能企业而言，开源并不意味着放弃对算法资产的保护，其商业价值在于以部分公开换取生态位与标准话语权。我们观察到，以开源模型为生态入口的头部厂商，已有较为成熟的做法：在前述专利与商业秘密分层的基础上，将部分版本或部分规模的基础模型权重开源，工具链与评测框架整体开放，同时以商业授权协议约束高级功能的使用[6]。三者之间的衔接最终要落到具体的

[4] 参见涉“信号处理”发明专利侵权案，(2023)最高法知民终 3114 号，最高人民法院，裁判要旨载《最高人民法院知识产权法庭裁判要旨摘要（2025）》。

[5] University of Tennessee Research Foundation v. Anthropic PBC, No. 1:26-cv-00887 (D. Del., filed July 20, 2026)；涉案专利为 US 10,019,470（2018 年 7 月授权）与 US 10,095,718（2018 年 10 月授权）。

[6] 例如，DeepSeek-R1 的模型权重以 MIT 许可证发布，允许自由商用与蒸馏；阿里通义千问 Qwen 系列多数模型采用 Apache 2.0 许可证，部分版本的许可条款约定月活跃用户超过 1 亿的商用主体须另行取得授权；Meta Llama 系列采用社区许可证，月活跃用户超过 7 亿的主体须单独申请许可，且衍生模型名称须以“Llama”开头。

条款设计上：开源层以许可证约束下游使用，闭源层以 API 条款与保密协议控制访问，专利层则覆盖可被外部观察的推理优化特征 — 专利恰好落在开源与闭源之间的可观察地带。

开源策略的关键一环在于许可证的选择，它在很大程度上决定了下游可以在多大范围内使用、修改和商用开源成果。许可证与随附的说明文档不仅划定了下游的使用边界，也关系到开源方自身的责任认定。最高人民法院于 2026 年 9 月 7 日发布的《关于依法审理涉人工智能纠纷案件的意见》第十三条，对开源软件相关方责任采取“综合考量、适当豁免”思路，使开源方得以通过许可证与说明文档等事前安排，对自身责任形成相对稳定的预期 — 当然，“不承担侵权责任”的认定以免费开源、公开说明功能和安全风险等要件为前提，以商业授权方式提供的高级功能等闭源部分，并不因开源层的存在而自动获得豁免[7]。算法资产的保护配置，因此很难脱离商业模式单独设计。

除自有资产如何配置之外，还需关注他人专利的风险排查。底层架构专利多由高校、科研机构与专利运营机构在早期布局，技术方案成型早于大模型时代，权利人主张的覆盖范围往往要到诉讼中的权利要求解释阶段才真正接受检验。对模型层与应用层企业而言，与其将自由实施分析（FTO）视为产品出海前的合规手续，更应考虑将其前移至产品架构定型之前 — 推理优化、调度机制等通用底座技术环节的专利密度上升较快，排查越早，规避设计的代价则越低。



图 1 算法资产的保护分层：专利、商业秘密与开源

三、域外规则对照：三种口径，一个共同方向

对于有算法跨境布局需求的企业，同一套算法创新在不同法域面对的审查口径并不相同，差异值得在撰写阶段就纳入考量。

中国的路径已如上篇所述，此处不再重复；撰写阶段真正需要细分口径的，是美国与欧洲。美国的口径近期明显放宽，回顾其判例史：2010 年的 Bilski 案否定了“机器或转换”测试作为客体适格性的唯一标准，2014 年的 Alice 案确立两步审查法，并在相当程度上收紧了软件与算法类权利要求的适格空间[8]。Desjardins 案并未在 Alice 之外另起炉灶。它的位置在 Alice 框架的“实际应用”概念内部 — 为“对模型本身运行的

[7] 《最高人民法院关于依法审理涉人工智能纠纷案件的意见》（法发〔2026〕10 号）第 13 条。

[8] Bilski v. Kappos, 561 U.S. 593 (2010); Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208 (2014)。

改进”找到了一个可以站住的落脚点。该案确认，对机器学习模型本身功能的改进，例如在连续学习中防止“灾难性遗忘”、降低存储需求与系统复杂度，在 Alice 框架下构成实际应用，从而满足客体适格性；该案同时明确，界定保护范围的恰当工具是新颖性、非显而易见性与说明书条款，而非适格性条款 — 事实上，该案仅撤销客体驳回，针对权利要求的显而易见性驳回未被一并触动 — 适格性口径的放宽并未替代创造性的审查。此后，美国专利商标局进一步允许申请人依据 37 CFR 1.132 提交客体适格性声明（SMED），为边缘案件提供了一条补充举证的程序路径 — 这属于证据规则层面的调整，审查标准本身没有再次放宽[9][10]。这也是为什么美国本轮调整被概括为“放宽适格性口径、把战场移向其他条款”。Alice 框架本身并没有被推翻。值得留意的是，该案确认的“对模型本身运行的改进”，与中国规则中“算法与计算机系统内部结构形成特定技术关联”在判断结构上颇有可类比之处；但两地规则的生成方式不同，同一份说明书在撰写时，需要同时为两地不同的判断侧重预留论证空间。欧洲则延续 COMVIK 方法，区分技术与非技术特征，只有对技术问题的解决作出贡献的特征才计入创造性 — 申请人需要证明算法特征产生了技术效果；模型架构或预测质量的提升本身，不构成这种技术效果[11]。

三大法域在“纯抽象算法不可专利”上一致，分歧集中在“技术性”的认定口径与举证方式。对中国申请人而言，把算法写进具体技术语境是最基础的共同要求；但同一份说明书在三地之间的可移植空间有限，撰写时即应按目标法域的差异预留分层的实施例。在主要法域，撰写时只考虑授权而不预演证明与执行，可能已不再是最优策略。域外布局的差异，本质上是“预演”在不同程序结构中的具体形态差异。

诉讼端也应纳入撰写深度的评估。同一份说明书在审查端过得了关，不等于其权利要求用语在诉讼端守得住界：以前述 Anthropic 案为例，双方对专利覆盖范围的争议，最终要经由权利要求解释程序逐项界定，撰写阶段留下的用语弹性，会在这一程序中被放大检验。跨境布局的撰写深度，因此同时面向审查与诉讼两种检验 — 这在三大法域是共同的约束，只是检验的程序形态不同。



图 2 三大法域的审查口径对照

[9] Ex parte Desjardins, Appeal No. 2024-000567 (PTAB Appeals Review Panel, Sept. 26, 2025)（2025 年 11 月 4 日被指定为先例裁决）。

[10] USPTO 局长备忘录《Subject Matter Eligibility Declarations》（2025 年 12 月 4 日），申请人可依 37 CFR 1.132 提交客体适格性声明（SMED）。

[11] EPO 上诉委员会 T 0641/00（COMVIK）及扩大上诉委员会 G 1/19。

结语

回到开篇提出的问题。算法创新能否成为专利保护的对象，取决于技术关联是否成立、合规要求是否已经内嵌到方案之中；授权前景则更多落在实质技术贡献上，场景包装本身很难支撑创造性。至于是否申请、以何种方式申请，需要在可观察性、生命周期与披露代价之间做权衡。而权利最终能否兑现，往往在撰写阶段就已经有了轮廓 — 审查与取证是否被预演，决定了后续还有多少调整空间。

对持有算法资产的企业而言，这一轮规则调整可以转化为四个具体动作：其一，在研发流程中建立贡献留痕机制，实验记录、版本迭代文档与人工智能使用痕迹的留存，同时服务于发明人认定与维权举证两端的需要；其二，按可观察性与生命周期对创新成果分层，在专利、商业秘密与开源之间作出与商业模式匹配的组合配置，并以自由实施分析排查底层架构环节的既有专利风险；其三，将合规审查与论证设计前置到撰写阶段，在说明书中充分铺垫技术问题、技术关联与效果机理，并审慎控制披露边界；其四，有跨境布局需求的企业，在撰写阶段即按目标法域的口径差异预留分层实施例，避免以同一份文本通行各局。

在数量维度上，中国创新主体的积累已经相当可观 — 全球约六成的人工智能专利为中国所拥有[12]，生成式人工智能专利族 2024—2025 两年合计的公布量，超过了此前十年的累计总量；但在这一最活跃的赛道上，国际专利族仅占公布总量的约 9%，绝大多数权利的法律效力止于国境之内[13]。这一轮规则调整的方向因此可以收束为一个判断：人工智能专利的竞争单位正在从“件数”变成“可执行性”。一件在撰写阶段就预演了审查、合规与取证全链条的专利，其战略价值持续上升；而大量以场景包装为特征的申请，在无效与维权环节面临的风险更高。这一轮调整的实际受益者，是那些在撰写阶段就把审查、合规与取证一并纳入考虑的创新主体。

[12] 国家数据局《数字中国发展报告（2025 年）》（2026 年 4 月 29 日于第九届数字中国建设峰会发布）：“我国已成为全球人工智能专利最大拥有国，占比达 60%。”

[13] 世界知识产权组织技术 SPARK 报告《生成式人工智能专利趋势更新》（2026 年 7 月）：2024—2025 两年合计公布的生成式人工智能专利族超过 56,000 件，超过 2014—2023 年的累计总量（其中 2023 年约 14,000 件，2025 年约 37,800 件）；国际专利族（在两个以上法域公布的专利族）2025 年占生成式人工智能专利族公布总量约 9%，报告指出部分原因在于中国申请人通常主要在国内提交申请。

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：

吴丽丽

电话： +86 10 8516 4266
Email： lili.wu@hankunlaw.com

俞琳

电话： +86 21 6016 9780
Email： lin.yu@hankunlaw.com

© 2026 Han Kun Law Offices. All Rights Reserved.