

汉坤法律评述

2026 年 8 月 13 日

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

人工智能（AI）创新的商业秘密保护：三起典型案例的观察

作者：吴丽丽 | 郑天禹

随着人工智能（AI）和大模型技术的快速发展，底层算法逻辑、核心训练代码、海量数据集等关键技术要素已成为 AI 创新企业的核心无形资产。面对这些新兴技术要素，用何种方式的知识产权进行保护成为业界思考和讨论的热点。

纵览各国知识产权保护制度，传统的专利和著作权保护路径存在一定的局限性：专利难以直接覆盖数据集或纯粹的底层算法本身，而著作权仅保护代码或数据的表达形式，无法覆盖其背后的算法思想与数据内容本身。

在此背景下，商业秘密（“技术秘密”）凭借客体范围广、自动产生、无需公开等优势，正成为企业保护 AI 核心资产的重要路径。但在实务中，由于 AI 技术通常由多种要素叠加而成而天然具有“黑盒”属性，其商业秘密的保护边界并不清晰。究竟哪些 AI 创新要素能够切实通过商业秘密途径获得司法保护，已成为当下 AI 企业尤为关注的焦点问题。

近年来，最高人民法院及各地法院陆续审结了多起涉 AI 创新的商业秘密典型案例。本文选取其中三起具有代表性的案例，试图结合最新司法实践对上述焦点问题作出总结与思考。

一、案例一：采用已有模型的算法可以得到商业秘密保护

2025 年初，最高人民法院在将本案作为“人民法院保护科技创新典型案例”[(2021)粤 03 民初 3843 号]，由此可见该案在保护 AI 创新方面的代表性。

（一）案情回顾

原告智某公司是一家互联网高科技企业，其核心产品“天某”APP 和 AI 写作机器人采用自主开发的大数据追踪系统，具备智能跟踪、个性化推荐、智能摘要等功能。原告请求保护的涉案技术秘密本质是一种推荐算法。

被告光某公司（其研发团队成员与原告存在重合）采用了与原告实质相同的推荐算法，用于融资及推出竞品应用程序。

庭审中，被告抗辩称，从所采用的模型来看，涉案算法采用的是已经公开的模型，因此不构成商业秘密。

（二）裁判要旨

深圳市中级人民法院经审理认为，涉案算法的核心为模型特定顺序的选择优化，即使搜索算法或推荐算法所采用的技术均为公开模型，但具体模型选择及权重排序，是权利人通过大数据的收集、处理和测试后，构成最优选择，该最优选择属于权利人付出劳动的成果，不为公众所知悉，并能为权利人带来商业利益和可保持竞争优势，应当作为商业秘密予以保护[深圳法院发布 2022 年数字经济知识产权司法保护典型案例，参见 <https://www.ciplawyer.cn/articles/150545.html>]。

（三）实务观察

本案系全国首例将算法作为商业秘密进行保护的案件，为 AI 创新企业提供了双层指引：

1. 确立算法本身可以作为商业秘密的法定保护客体

在过去相当长一段时间内，算法常因被视为抽象的数学规则或思想而面临知识产权保护的困境。2020 年，最高人民法院出台了司法解释《关于审理侵犯商业秘密民事案件适用法律若干问题的规定》，将“算法、数据、计算机程序”明确列入技术信息的范畴，从而在制度层面初步解决了算法作为商业秘密客体的适格性问题。

在司法层面，本案首次确认了这一客体适格性。2025 年初，最高人民法院在将本案作为“人民法院保护科技创新典型案例”发布时进一步指出，“**算法作为推动人工智能发展的关键基础，是开发者耗费大量的人力、物力和时间通过大数据不断地测试获得的劳动成果，其研发成果具有一定的商业价值，构成反不正当竞争法上的商业秘密** [人民法院保护科技创新典型案例，参见 <https://www.court.gov.cn/zixun/xiangqing/452031.html>]”。此外，已于 2026 年 6 月 1 日起实施的《商业秘密保护规定》第五条吸收了上述司法解释对“算法、数据、计算机程序”的列举，并进一步将“代码”明确列入技术信息范畴。

综上，算法作为商业秘密保护客体的适格性，已在制度与司法两个维度得到充分确认。企业在主张算法构成商业秘密时，无需再就客体属性本身展开论证，而应将举证重心集中于密点的具体界定、对商业秘密法定要件的对应满足、侵权行为、损害赔偿等实体问题。

2. 由公开模型组合而得到的特定算法，模型的选择优化与权重排序可以构成商业秘密密点，并在未来的商业秘密纠纷中有效应对可能的公知性抗辩

在 AI 应用中，完全从零开始构建底层算法的情况相对罕见，多数企业采用公开模型进行组合或者基于开源框架进行二次开发的技术路线。本案在实务上的关键启示在于，针对由公开模型组合而得到的特定算法，模型的选择优化与权重排序可以构成商业秘密密点，成为公司的宝贵财富。

本案法院在判决中指出，虽然搜索算法的每个分部技术中采用的模型均为公开模型，但解决同一运算和逻辑问题存在各种不同算法。权利人通过对多达上万种算法的不断测试，耗费大量人力、物力和时间，最终选择使用的特定技术组合排除了模型间的相互妨碍并达到最佳效果。因此，在主张特定算法为商业秘密时，企业可以将密点明确界定为模型的选择优化与权重排序。此类密点的证明高度依赖过程性证据，即模型选择记录、参数迭代日志、测试数据等研发过程文档。这些过程性文档既是证明企业付出实质性劳动的直接依据，也是应当在纠纷发生前就着手留存的证据基础。反之，被诉侵权方若以技术公开或自主研发为由抗辩，同样需要以完整的研发记录证明其技术来源。

二、案例二：训练代码与标注数据库可以得到商业秘密保护

该案为最高人民法院于 2025 年 12 月 25 日审结的商业秘密上诉案件[（2023）最高法知民终 1503 号]。二审判决改判认定等五被诉侵权人实施了针对原告涉案技术秘密的共同侵权行为并需承担相应侵权责任。该案是最高人民法院知识产权法庭审结的首例涉视觉识别领域人工智能及算法技术秘密侵权纠纷案件，也清晰阐明了对已有模型进行训练的训练代码与标注数据库可以得到商业秘密保护。

（一）案情回顾

原告翎某公司研发了一款包含指尖识别及点读功能的产品，其主张作为商业秘密保护的技术信息包括指尖识别技术相关的训练代码及近百万张标注图像构成的数据库。翎某公司对上述信息采取了签订保密协议、使用 Gitlab 系统进行代码与数据权限管理等保密措施。

张某曾任翎某公司股东并担任 CTO，李某、王某、黄某系翎某公司核心研发员工。张某离职后设立被告纸某公司，李某、王某、黄某相继加入。纸某公司在成立不到两个月的时间内，向第三方学习平板产品提供了能够实现手指定位及识别功能的技术支持。翎某公司据此主张张某等人与纸某公司构成共同侵权。

庭审中，纸某公司抗辩称，被诉侵权技术的最初来源是从各种公开渠道收集的相关开源代码，属于自主研发，不构成侵犯商业秘密。

（二）裁判要旨

最高人民法院二审经审理认为，将不同渠道获取的开源代码整合形成初始模型，并通过后期大量数据训练形成性能完善的模型，是涉案人工智能技术研发的核心难点。翎某公司涉案技术的研发过程历时一年五个月，而纸某公司仅用不到两个月即从无到有推出了具备同等视觉识别与定位功能的产品，该研发周期有违日常经验法则。

最高法进一步指出，人工智能模型必须经过前期高频次、高强度的训练，模型的自我学习和泛化能力高度依赖海量数据的投喂。在翎某公司已提供初步证据表明其商业秘密被侵害，且纸某公司相关人员有渠道获取该商业秘密、被诉信息与商业秘密实质相同的情况下，举证责任依法发生转移。纸某公司主张自主研发，但未能充分举证证明其研发过程及训练数据的合法来源，故认定纸某公司及张某等人构成共同侵权，需承担连带赔偿责任及迟延履行金。

（三）实务观察

本案作为涉及深度学习模型的典型纠纷，为 AI 企业在技术秘密保护客体的确定以及侵权举证规则的适用上提供了明确的裁判指引：

1. 可以从最小单元到完整技术方案分层次确定和主张 AI 技术秘密的密点

在人工智能深度学习场景中，算法代码与训练数据深度耦合，企业的核心技术门槛更多体现为二者结合形成的整体技术方案。最高法在翎某案中明确，如何将从不同渠道获取的开源代码加以整合形成一个初始模型，并通过后期大量训练进一步形成性能完善的模型，既是研发中的关键环节，也是研发中的核心难点。该案原告主张的商业秘密亦同时包含了算法的训练代码及训练图片数据库[《涉人工智能及算法技术秘密侵权纠纷案件中举证责任转移的适用》，最高人民法院知识产权法庭，<https://ipc.court.gov.cn/zh-cn/news/view-5162.html>]。

在实务中，权利人可以采取分层界定与组合主张相结合的策略。所谓分层界定，是指逐项界定核心训练代码、特定标注数据库等技术信息的具体内容，明确所主张商业秘密的密点范围，并就其三性分别举证。在此基础上，权利人可以进一步主张上述要素整合形成的完整技术方案作为整体亦构成商业秘密。这种策略能够有效降低因客体范围模糊或单一要素存在公知瑕疵而产生的败诉风险。

2. AI 密点的同一性比对可以从传统的代码比对转向基于产品功能表现与行业研发规律的综合认定来确定

深度学习模型具有明显的“黑盒”属性，在侵权诉讼中直接采用传统的源代码比对方式不仅面临技术障碍，也极易使权利人陷入举证劣势。翎某案确立了以产品功能表现与行业研发规律辅助“实质相同”认定的裁判逻辑，从而破解这一困境。

具体而言，法院并未局限于底层代码的相同或者实质性相同比对，而是首先考察被诉侵权技术与涉案商业秘密在实现视觉感知、辨识、理解等流程动作上的高度一致性。在此基础上，法院引入深度学习高度依赖海量数据高频次训练的行业客观规律，认定被告在极短时间内从无到有推出同类功能产品的行为有违日常经验法则。上述功能表现的高度一致与研发周期的显著异常，构成了认定“实质相同”的重要初步证据。

3. AI 商业秘密权利人举证责任转移门槛降低被诉侵权人合法来源抗辩要求提高

在确立上述初步举证的基础上，本案进一步明确了涉 AI 商业秘密纠纷中的举证责任分配规则。在实务中，权利人在证明涉嫌侵权方具备接触条件的基础上，若能结合产品功能高度一致及被告研发周期异常等外部事实完成初步举证，即可触发举证责任的依法转移[参见《反不正当竞争法》（2019 年修正）第三十二条第二款，2025 年修订后为第三十九条第二款。]。此时，证明相关技术具有合法来源的举证责任转移至被告。涉嫌侵权方若主张自主研发，应当提交完整的研发过程记录及训练数据合法来源等实质性证据予以反驳，否则将承担举证不能的不利后果。

三、案例三：数据集的秘密性边界决定了可以通过商业秘密保护还是可以通过不正当竞争保护

近些年，各地法院陆续对于 AI 创新做出了一些探索性判决，试图从已有法律规定找到对 AI 创新的保护路径。本部分从商业秘密和不正当竞争方面进行介绍。

（一）案情回顾

数某公司经授权收集了 1505 小时中文普通话语音数据集，并取得了《数据知识产权登记证》。隐某公司未经许可，在其官方网站上提供该数据集中 200 小时子数据集（即本案诉争的涉案数据集）的免费下载服务，以此吸引用户注册。数某公司提起诉讼，主张隐某公司侵害其商业秘密及构成不正当竞争。

一审法院认定涉案数据集已采取合理保密措施，构成商业秘密，判决隐某公司侵权[(2021)京 0491 民初 45708 号]。二审法院查明，数某公司曾于被诉侵权行为发生前，在其官网面向不特定公众公开披露了该涉案数据集的下载渠道和训练方法。据此，二审法院改判涉案数据集因主动公开而丧失秘密性，不构成商业秘密。但二审法院同时认定，隐某公司的行为违反了反不正当竞争法第二条，构成不正当竞争[(2024)京 73 民终 546 号]。

（二）裁判要旨

本案裁判确立了如下规则：

数据集若不为公众所知悉并采取了合理保密措施，可适用商业秘密相关法律规定予以保护。数某公司取得的《数据知识产权登记证》，可作为证明其享有涉案数据集相关财产性利益及数据来源合法的初步证据。

数据集作为商业秘密保护的前提是维持其秘密性。权利人若在官网上主动公开数据下载渠道及训练方法，将导致该部分数据丧失不为公众所知悉的法定要件。

未能获得商业秘密保护的数据集，若系权利人投入大量技术、资金和劳动形成，且具有商业价值，仍受反不正当竞争法保护。同业竞争者无视开源协议规则，擅自提供下载服务以截取原告用户流量、损害原告获取数据改进建议的机会，违背商业道德，构成适用反不正当竞争法第二条一般条款的不正当竞争行为。

（三）实务观察

本案为 AI 企业在数据要素的确权、日常合规管理及维权路径选择上提供了指引：

1. 明确数据集的商业秘密客体适格性及数据登记的证据效力

本案一审法院承认了数据集可作为商业秘密保护客体。企业投入大量技术、资金和劳动，合法收集形成具有一定规模的数据集，若采取了保密措施且未对外公开，则可作为商业秘密受到保护。此外，本案还阐明了《数据知识产权登记证》的司法证据效力。在以往的诉讼实务中，企业证明海量数据的权属及来源合法性往往耗时费力。本案通过判例确立了《数据知识产权登记证》可作为权利主体和来源合法性的初步证据，大幅降低了企业在确权阶段的举证门槛。

2. 商业推广与秘密性维持的界限

涉案数据集未能获得商业秘密保护的直接原因在于权利人的主动公开行为。AI 企业在经营中常需要在商业推广、参与开源生态与核心资产保密之间寻找平衡。本案提示，秘密性一旦因主动公开而丧失，将产生不可逆的后果。企业在进行学术交流、论文发表或提供开源下载前，需建立严格的内部审查机制，明确区分用于引流的公开数据集与作为核心资产的保密数据集，避免因营销动作破坏核心资产的保护基础。

3. 核心 AI 资产的多维度保护路径展望

当 AI 数据集等核心要素因主动开源或未能采取有效保密措施而无法主张商业秘密保护时，企业仍可尝试其他维权路径。例如，若数据集在数据的选择或编排上体现出独创性，可尝试寻求著作权法的保护[本案二审法院认定，涉案数据集不符合汇编作品的构成要件。]；若他人获取和使用数据的行为违背诚实信用原则和商业道德，则可诉诸反不正当竞争法的一般条款（即本案二审法院最终适用的路径）。需要注意的是，相比于商业秘密保护，上述替代路径在独创性认定或竞争性权益的举证要求上往往面临更大的挑战。

四、结语

通过上述三起典型案例可以看出，司法实践正逐步厘清 AI 要素在商业秘密保护体系下的裁判规则。从

明确算法、训练代码与数据集的客体适格性，到适用举证责任转移规则破解技术比对难题，再到划定开源行为与秘密性维持的法律边界，法院为 AI 创新企业提供了一套具有可操作性的确权与维权指引。

面对复杂的竞争环境，AI 创新企业可以基于上述裁判规则，建立体系化的 AI 商业秘密合规机制。具体而言，企业需在研发阶段做好技术信息的分层分类与数据留存，在确权与维权阶段灵活运用组合主张策略及数据知识产权登记证等初步证据，并在商业推广阶段严格审查开源行为，避免核心资产因主动公开而丧失法定保护基础。

需要指出的是，商业秘密保护的前提在于维持技术信息的秘密性状态。当 AI 要素因业务需求必须对外公开，或因客观原因丧失秘密性时，商业秘密路径将不再适用。对于此类已公开的 AI 要素，企业能否通过著作权法主张基于独创性的保护，或者诉诸反不正当竞争法一般条款寻求兜底路径？关于这些维权路径的司法审查标准与实务策略，我们将在本系列的后续文章中进行深度解析。

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： +852 10 8516 4266

Email: lili.wu@hankunlaw.com