欧盟人工智能大模型的知识产权保护路径及中国方案*

邵永乐

摘　　要：大模型的智力成果属性与公共产品属性之间的张力，引发了大模型研发者的权益保护和技术共享之间的冲突。为促进模型开源和激励技术创新，欧盟学者主张大模型的投资保护应从行为规制模式转向赋权保护模式。基于权利客体不适格和保护力度不适配等方面的原因，欧盟的著作权保护路径无法适配于大模型。考虑到新兴技术的发展，欧洲专利局通过修改人工智能相关发明的专利审查标准，使大模型纳入专利权客体成为可能。不过，在专利权保护路径之下，大模型可受保护的范围只能局限于特定的应用场景，保护效果仍有不足。我国应当在吸取欧盟经验的基础上，结合大模型自身的技术特征构建保护方案。妥当的路径是在未来的《人工智能法》中增设模型研发者的权利配置规范，从而明确大模型研发者的权利内容和权利限制。

关 键 词：欧盟；　大模型；　开源；　知识产权；　以公开换保护

作者简介：南京大学　法学院　博士研究生　南京　210008

中图分类号：D913.4

文献标识码：A

文 章 编 号：1005－4871(2025)05－0101－23

一、问题的提出

生成式人工智能大模型（以下简称为“大模型”）的发展带来新一轮的知识革

* 本文系国家社科基金青年项目“请求权视角下个人数据权利行使研究”（项目编号：24CFX038）的阶段性成果。

命。在全球竞逐的科技浪潮中，我国大模型技术迅速崛起，当前已形成“百模争鸣”的繁荣局面。[①] 大模型的研发是人工智能价值链生成的核心环节，通用大模型的出现更加强化了人工智能产业上下游之间联系的紧密程度，人工智能立法如何为技术创新与模型开源赋能成为了亟需研究的课题。一方面，大模型的研发汇集了开发者大量的智力贡献和高昂的经济投入，为保护投资，研发者更倾向于采用商业秘密模式保护自己的技术，由此引发了学者对于技术垄断的担忧。[②] 为应对技术封锁和技术垄断对人工智能产业发展的阻碍，有观点主张通用大模型应当强制开放。[③] 然而，强制开放意味着研发者的经济和智力投入难以获得有效回报，若制度供给不能为技术创新与技术共享提供行为激励，则将阻碍人工智能产业链的进一步发展。另一方面，知识蒸馏技术的发展可以实现低成本的知识迁移和模型优化，未经“教师模型”研发者许可蒸馏训练出的“学生模型”是否构成侵权尚无定论。[④] OpenAI曾公开指控DeepSeek涉嫌“不当蒸馏”，侵犯其知识产权。[⑤] 尽管该指控并无任何实质证据，却进一步加剧了技术不公开和技术垄断的紧张局面。[⑥] 可见，为促进模型开源共享和深度参与国际治理，未来立法需要对知识蒸馏带来的大模型知识产权侵权风险提供解决方案，其中首要任务是明确大模型的知识产权保护路径与大模型研发者的权利配置。

新一轮科技革命和社会经济关系的变化需要法律寻求新的利益平衡机制，由此催生各国立法供给与理论研究的热潮。在立法配置方面，2024年5月，欧盟理事会正式批准《人工智能法》，为人工智能的发展和监管提供了规范依据。[⑦] 在理论研究方面，德国马克斯·普朗克创新与竞争研究所团队发表的《人工智能与知识产权法的立场声明》以技术为导向，总结出人工智能与知识产权法交叉领域中的三大理论议题：根据“开发人工智能系统所需的输入”“作为过程的人工智能”“人工智能应用输出”的阶段划分，理论研究集中于训练数据阶段的知识产权保护问题、人

① 王飞跃：《我国生成式人工智能的发展现状与趋势》，载《人民论坛》，2025年第2期，第21－26页，这里第22页。

② 王健、吴宗泽：《生成式人工智能反垄断论纲》，载《法治研究》，2024年第6期，第131－137页；雷浩然：《生成式人工智能领域的垄断风险及其治理路径》，载《中国流通经济》，2025年第3期，第13－24页。

③ 许丽：《必需模型反垄断法强制开放的理据与进路》，载《华东政法大学学报》，2024年第6期，第53－66页。

④ 郑志峰：《DeepSeek技术应用的侵权责任风险》，载《中国社会科学报》，2025年2月25日，第5版；林秀芹：《DeepSeek模型蒸馏的著作权法正当性重勘》，载《知识产权》，2025年第4期，第91－110页；邓建鹏、赵治松：《DeepSeek的破局与变局：论生成式人工智能的监管方向》，载《新疆师范大学学报(哲学社会科学版)》，2025年第4期，第68－77页。

⑤ 李迅典：《OpenAI上书美国政府赤裸裸攻击DeepSeek》，载《环球时报》，2025年3月15日，第3版。

⑥ 目前，国际主流的大模型(如ChatGPT、GROK等)对我国实施IP封锁。

⑦ Artificial Intelligence Act, Regulation [EU] 2024/1689.

工智能算法或者大模型的知识产权保护问题，以及人工智能系统生成内容的知识产权保护问题三个方面。[①] 其中，欧盟有关大模型知识产权保护的讨论已经较为丰富，[②]可为大模型研发者的权利配置提供充足的理论依据。

相较而言，中国人工智能领域的立法还在进一步研讨过程中，理论研究尚显不足。《中共中央关于进一步全面深化改革 推进中国式现代化的决定》提出要“完善生成式人工智能发展和管理机制”。[③] 在此背景下，我国的《人工智能法（学者建议稿）》（以下简称为《学者建议稿》）和《人工智能示范法（专家建议稿）3.0》（以下简称为《专家建议稿》）相继公布。尽管《学者建议稿》和《专家建议稿》都体现出激励大模型创新的价值取向，但有关大模型研发者的权利配置方案仍有待进一步探讨。

有鉴于此，本文首先对欧盟大模型知识产权保护模式的理论争议进行系统梳理，然后检视欧盟大模型的知识产权保护路径是否妥当，最后在批判性借鉴欧盟经验的基础上，构建出大模型知识产权保护的中国方案。

二、欧盟大模型知识产权保护模式的理论争议

欧洲学者曾就人工智能和知识产权法之间的互动关系展开了激烈争论，大模型作为无形财产究竟应当被纳入知识产权的保护客体还是应通过反不正当竞争法保护是争论的焦点问题之一。[④] 然而，以反不正当竞争法为代表的行为规制模式可能造成技术垄断等不利后果，在此背景下，大模型的保护模式逐渐由反不正当竞争法的行为规制模式转向了知识产权法的赋权保护模式。

（一）行为规制模式的证否

根据通说观点，大模型是在大量数据上训练的，用于普适性目标、可优化适配多种下游任务的深度神经网络模型。[⑤] 由此可见，基于神经网络，经由数据训练，完成深度学习且具有一定程度的通用性能是大模型的典型技术特征。海量的训练

---

① Josef Drexl/Reto M. Hilty/Luc Desaunettes-Barbero et al., “Artificial Intelligence and Intellectual Property Law — Position Statement of the Max Planck Institute for Innovation and Competition of 9 April 2021 on the Current Debate (April 9, 2021)”, Max Planck Institute for Innovation & Competition Research Paper No. 21－10, pp. 1－25.

② Reto M. Hilty/Jörg Hoffmann/Stefan Scheuerer, “Intellectual Property Justification for Artificial Intelligence”, Max Planck Institute for Innovation and Competition Research Paper No. 20－02, pp. 1－28; Begoña Glez. Otero, “Machine Learning Models under the copyright microscope: is EU Copyright fit for purpose?”, Max Planck Institute for Innovation and Competition Research Paper No. 21－02, pp. 1－29.

③ 《中共中央关于进一步全面深化改革 推进中国式现代化的决定》，载《人民日报》，2024年7月22日，第1版。

④ Mauritz Kop, “AI & Intellectual Property: Towards an Articulated Public Domain”, *Texas Intellectual Property Law Journal*, Vol. 28, No. 1, 2020, pp. 298－342, here pp. 315－319.

⑤ 《生成式人工智能服务安全基本要求》第3.5条。

数据和数以千亿的参数设置决定了其研发过程需要大量资金和技术能力支撑，在欧盟法上，已经经过训练的大模型可以纳入商业秘密和反不正当竞争法的保护范围。

1. 商业秘密保护模式的弊端

根据欧盟《商业秘密指令》第2条的规定，商业秘密指的是任何“不为公众所知”、因保密而具有商业价值并已采取合理措施的信息，其序言第14条更是明确将有价值的专有技术、商业信息和技术信息纳入商业秘密的范围，只要存在保持其保密性的合法利益及维持该保密性的合理预期。[①] 由此可见，欧盟《商业秘密指令》对商业秘密的定义非常广泛，它可能涵盖任何数据，包括用户数据、算法以及由欧洲商业实体处理的新生成数据。[②] 在此立法模式下，未公开的大模型的核心技术方案和具体参数设置可以通过商业秘密获得保护，未经大模型研发者的同意，他人不得非法获取、使用或披露大模型的技术方案和具体参数，否则相关行为会被认定为侵权。我国对于商业秘密的界定和保护方式与欧盟类似。根据《最高人民法院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》第1条，商业秘密所保护的商业数据范围包括“与技术有关的数据”和“与经营活动有关的数据”。这使得将大模型纳入商业秘密的保护范围成为可能，但此种保护模式既可能造成保护不足，又可能造成保护过度。

首先，商业秘密的认定需要满足秘密性、价值性和保密性三要件。从人工智能产业链的发展现状来看，为提高市场影响力和市场竞争力，大多数新型模型在部署之初会采用开源方式。例如，OpenAI公司研发的GPT系列模型的前两代产品都是开源的，从GPT-3开始才转为闭源。[③] 尽管不同模型的开源程度有差异，但是研发者往往会主动披露模型源代码、训练算法、训练数据集、参数和超参数等部分或全部技术信息。由于这些技术信息通过主动披露而被公众熟知，无法满足秘密性的要件，故无法获得商业秘密的相关立法保护。

其次，即便对于闭源模型而言，采用商业秘密的保护模式亦不能有效防止反向工程。根据欧盟《商业秘密指令》的规定，对合法获取的产品实施反向工程是被允许的，除非合同另有约定。[④] 实践中，大模型的用户服务协议往往会对用户实施反

① Trade Secrets Directive, Directive (EU) 2016/943, Preface Article 14.

② Sandra Wachter/Brent Mittelstadt, “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI”, *Columbia Business Law Review*. Vol. 2019, No. 2, 2019, pp. 1 - 130, here p. 116.

③ Braeden Cullen, “OpenAI: Was the Shift to Closed Source Justified?”, 2021 - 02 - 03, https://sites.imsa.edu/hadron/2021/02/03/openai-was-the-shift-to-closed-source-justified/, 访问日期：2025 - 08 - 31。

④ 同注①, Preface Article 16。

向工程行为进行限制。例如，OpenAI 公司的服务协议规定用户不得试图或协助任何人对其服务的源代码或底层组件进行反向工程、反编译或发现，包括模型、算法或系统（除非适用法律禁止此限制）。[①] 尽管欧盟《商业秘密指令》对于反向工程行为规制的立法空白可以通过合同排除反向工程来弥补，但此类合同可能会阻碍技术创新和信息传播，从而受到反垄断法等相关法规的规制。对已经完成训练的“教师模型”进行知识蒸馏，从而生成新的“学生模型”是当前常见的模型侵权方式。如果采取商业秘密保护路径，只要他人获取大模型产品应用的方式是合法的，进而实施反向工程获得相应的技术数据，则该行为应被视为获取信息的合法手段。可见，商业秘密的保护路径并不能对大模型研发者的权利提供全面保护。

最后，商业秘密保护模式意味着企业要尽可能地维持大模型技术数据的保密状态，数据享有者对此拥有完全排他的控制权，这种保护力度已经远远超过了部分弱排他性的权利。这不仅不符合数字经济互联共享的发展规律，也无法满足企业间的交易需求，从而造成保护过度，形成垄断。因此，大模型的商业秘密保护路径具有一系列的负面影响，不利于人工智能领域的技术创新与人工智能产业链的发展。

2. 反不正当竞争法的保护模式

尽管欧洲整个学术界似乎都在讨论知识产权对人工智能及其输出的适用问题，但在相关学说尚未发展为成熟的知识产权立法之前，反不正当竞争法提供的保护机制可以作为大模型知识产权保护的替代方案。[②] 反对赋权保护路径的学者的核心理由在于，知识产权只是通过建立人为排他权来补救公共市场失灵的一种手段，在可以通过其他方式来保护大模型领域的投资范围内，缺乏知识财产权保护不会损害整体福利，其中反不正当竞争法就是可供选择的方式之一。[③] 值得注意的是，欧盟并没有统一的反不正当竞争法，但是欧盟对不正当竞争行为的监管呈现扩张趋势。针对企业对消费者施加的不公平商业行为，欧盟已经出台了《不正当商业行为指令》，[④]而针对企业之间的不正当竞争行为的监管措施尚未统一。尽管欧盟层面的统一立法尚未出台，学理上认为没有统一立法对于人工智能企业间的监管

① Open AI, “Europe Terms of Use”, 2025 - 04 - 29, https://openai.com/policies/eu-terms-of-use, 访问日期：2025 - 08 - 31。

② Stefan Scheuerer, “Artificial intelligence and unfair competition-Unveiling an underestimated building block of the AI regulation landscape”, Max Planck Institute for Innovation and Competition Research Paper No. 20 - 21, pp. 1 - 27, here pp. 18 - 21.

③ Josef Drexl/Reto M. Hilty/Luc Desaunettes-Barbero et al., “Artificial Intelligence and Intellectual Property Law — Position Statement of the Max Planck Institute for Innovation and Competition of 9 April 2021 on the Current Debate (April 9, 2021)”, p. 17.

④ Unfair Commercial Practices Directive, Directive 2005/29/EC, Article 3.

恰恰应被视为机遇而非阻碍，反不正当竞争法的灵活性特征恰好契合人工智能领域的动态特征，能够作为应对新型不可预见竞争风险的兜底机制发挥实效。①

在我国的大模型“抄袭”第一案中，法官正是通过《反不正当竞争法》的一般条款予以处理。审理法官认为，人工智能模型结构及参数构成开发者的竞争利益，从事人工智能模型研发经营的企业未经许可不得直接使用他人通过数据训练改进而来的模型结构和参数，此为人工智能模型领域公认的商业道德。被告未经允许直接使用他人通过数据训练改进而来的模型结构和参数，违反了人工智能模型领域公认的商业道德，导致市场激励机制失灵，扰乱了人工智能模型经营活动和健康有序的竞争秩序，故构成不正当竞争行为。② 本案将大模型的结构和参数纳入“竞争性权益”的保护范围，确立了人工智能模型保护的“竞争法路径”，是我国司法实践对人工智能大模型保护模式的创新发展。

诚然，在新型排他性权利或绝对主观权利创设之前，反不正当竞争法提供的保护方案是有特殊意义的，其一般条款在新型主观权利形成中具有“先导功能”，例如，在《著作权法》引入邻接权前，反不正当竞争法可以为音乐会主办方提供保护；③在数据领域的排他权创设之前，反不正当竞争法可以对数据库创建者提供保护。④ 此种机制常将初始仅通过个别防御权保护的法定地位，逐步发展为排他性权利。⑤

不过，反不正当竞争法提供的保护方案只能是过渡性和补充性的。⑥ 一方面，不正当竞争行为的认定更多依靠的是法官的自由裁量权，因而具有很大程度的不确定性。从司法实践现状来看，法官多以经营者利益、消费者利益和竞争秩序利益三重利益为依据展开分析，但是三重利益评价标准存在模糊性，造成裁判结果难以统一。例如，在“北京微梦创科网络技术有限公司与北京字节跳动科技有限公司不正当竞争纠纷案”中，一审和二审法院同样都是运用的三重利益评估方法，但是得出的结论完全相反。⑦ 正因如此，即便我国的《反不正当竞争法》第12条已对非法访问和利用他人数据的不正当竞争行为予以规制，学者仍主张应当设立“数据保护专门条款”，构建一种既赋予一定排他权，又兼顾数据流通的商业数据弱权利保护

① Stefan Scheuerer, “Artificial intelligence and unfair competition-Unveiling an underestimated building block of the AI regulation landscape”, p. 3.

② 参见北京知识产权法院(2023)京73民终3802号民事判决书。

③ BGH, Urt. v. 24.5.1963-Ib ZR 62/62, BGHZ 39, 352 (354 ff).

④ BGH, Urt. v. 10.12.1987-I ZR 221/85, NJW-RR 1988, 809 (810).

⑤ Vgl. Herbert Zech, *Information als Schutzgegenstand*, Tübingen: Mohr Siebeck, 2012, S. 161 - 162.

⑥ 杨明：《试论反不正当竞争法对知识产权的兜底保护》，载《法商研究》，2003年第3期，第119 - 128页，这里第120页。

⑦ 一审法院判决书参见北京市知识产权法院(2017)京73民初2020号民事判决书；二审法院判决书参见北京市高级人民法院(2021)京民终281号民事判决书。

机制。[①]

另一方面，反不正当竞争法只能提供被动的防御性机制，且保护范围极为有限。在保护方式上，反不正当竞争法只能为权利主体提供事后救济，无法满足数字经济时代大模型流通交易的需求。在保护范围上，该法仅能对具有竞争关系的主体之间的商业行为提供规制，对于非竞争关系主体的模型蒸馏等侵权行为则无能为力。正因如此，即便是支持反不正当竞争法保护路径的欧盟学者也认为，该方案只能是在新型知识产权创设前的补充方案。[②]

（二）赋权保护模式的证成

传统理论认为，知识产权授予的正当性是基于道义论推理和经济学推理两方面证成的，前者认为人类创造者的努力和人格应当得到尊重，后者则认为需要建立无形商品的排他权以激励投资创新。[③] “劳动赋权理论”和“创新激励理论”能够为大模型的强化保护提供理论支撑。不过，在单一的强化保护理论下，模型研发者可能选择商业秘密或者闭源方式保护大模型，这种倾向与全球范围内共同提倡的大模型开放共享的理念相违背，[④]“促进开源共享”理论由此提出。于是，“劳动赋权理论”“创新激励理论”和“开源共享理论”共同构成了大模型赋权保护的理论基础。

“劳动赋权理论”认为，无形财产赋权的正当性在于个人的智力创造。[⑤] 在智力成果的生成过程中，行为人需要以现有知识资源为基础进行加工、创造等智力劳动，从而实现知识资源的生产，该智力成果因融入了智力劳动而得以成为权利客体。[⑥] 大模型的训练过程需要分为几个阶段：首先，对模型架构进行编程；其次，设计训练算法；再次，整理训练数据集，根据训练过程建立模型；最后，利用新数据对完成初步训练的模型进行检验，以产生特定输出。大模型的整个训练和研发过程凝聚了研发者的智力劳动，因此对其劳动成果赋权保护具有理论上的正当性。

“创新激励理论”认为，知识产权引发的创新激励会带来福利增长，可以为更多

---

① 孔祥俊：《论反不正当竞争法“商业数据专条”的建构》，载《东方法学》，2022 年第 5 期，第 15－29 页，这里第 15 页。

② Stefan Scheuerer, “Artificial intelligence and unfair competition-Unveiling an underestimated building block of the AI regulation landscape”, p. 19.

③ Reto M. Hilty/Jörg Hoffmann/Stefan Scheuerer, “Intellectual Property Justification for Artificial Intelligence”, pp. 4－23.

④ Global Partnership on AI, “Fostering Contractual Pathways for Responsible AI Data and Model Sharing for Generative AI and Other AI Applications”, Report, November 2023, pp. 1－44.

⑤ Vgl. Karl-Heinz Fezer, „Digitales Dateneigentum — ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft“, in Stiftung Datenschutz (Hrsg.), *Dateneigentum und Datenhandel*, Berlin: Erich Schmidt Verlag, 2019, S. 101－160, hier S. 133.

⑥ 冯晓青：《大数据时代企业数据的财产权保护与制度构建》，载《当代法学》，2022 年第 6 期，第 104－120 页，这里第 107 页。

创新和创造的出现提供制度激励，由此可实现社会财富的最大化。[①] 从功利主义的角度观察，持久的创新发展需要财产权制度作为保障。只有在财产权能够充分保障创新成果的地方，科学技术才能获得创新内在驱动力和可持续发展。[②] 以“创新激励理论”证成大模型知识产权保护的正当性取决于两个前提：一是创新过程周期较长，需要高额投资；二是模仿与盗用的可能性较高，若缺乏知识产权保护将导致定价低于研发者的边际成本。如前所述，大模型的研发训练需要高额投资，可以满足前提一。在大模型开源的背景下，模型蒸馏等侵权复制行为日益普遍化，前提二也可以得到满足。在当前激烈的国际科技竞赛的背景下，大模型作为战略资产，其研发需要政策支持和知识产权保护，以抵御外部掠夺性使用。故有必要在法律层面为模型研发者配置相关的知识产权以保护研发者的投资回报，为大模型的持续创新提供激励。

更为重要的是，赋权保护模式有利于促进大模型的开源共享。计算机软件技术的发展催生了开源理念。上世纪末开始，世界范围内兴起了“自由软件运动”和“开源软件运动”，“开源”一词就此广为传播。[③] 不过，开源软件运动在一开始就带有很强的理想主义色彩，由于缺乏经济激励且对开源软件研发者的权利保障不足，即使在软件领域，开源方式也并未成为主流。[④] 大模型开源是软件开源运动的延续，与计算机软件相比，大模型的研发成本更高，开源的内容也更广。根据开放源代码促进会（Open Source Initiative）的定义，开源软件的核心是提供并允许他人使用源代码。[⑤] 但是大模型的技术特征决定了代码并非影响其功能的关键因素，仅仅公布源代码对于模型复制利用的作用甚微。尽管目前大模型的开源实践的做法不一，但总体上看，大模型的开源除代码外，还包括模型架构、训练数据集合、模型参数、算法实现细节、模型训练步骤等多方面内容。[⑥] 可以预见，前述影响软件开源的障碍在大模型领域将表现得更为突出。

---

① Tom G. Palmer, “Intellectual Property: A Non-Posnerian Law and Economics Approach”, *Hamline Law Review*, Vol. 12, No. 2, 1989, pp. 261－304, here p. 262.

② 曲三强：《论人工智能与知识产权》，载《知识产权》，2023年第8期，第30－52页，这里第34页。

③ 苏宇、郭雨婷：《人工智能开源生态的法律治理》，载《宁夏社会科学》，2024年第5期，第119－130页，这里第120页。

④ 在我国司法实践中，开源软件与派生软件之间的侵权纠纷存在支持“开源抗辩”和“不支持开源抗辩”两种不同观点。支持开源抗辩的案例可参见江苏省南京市中级人民法院（2021）苏01民初3229号民事判决书，江苏省无锡市中级人民法院（2023）苏02民初482号民事判决书。反对开源抗辩的案例可参见最高人民法院（2019）最高法知民终663号民事判决书，北京市高级人民法院（2018）京民终471号民事判决书。

⑤ Open source initiative, “The open source definition”, 2024－02－16, https://opensource.org/osd, 访问日期：2025－08－31。

⑥ 周辉：《开源人工智能模型的法律治理》，载《上海交通大学学报（哲学社会科学版）》，2024年第8期，第18－33页，这里第20页。

尽管大模型开源可能会因造成技术扩散并引发安全负外部效应而遭受批评，尤其是开源大模型可能会被复制、修改而用于危险活动，[①]但各国仍在鼓励和促进大模型朝着开源的方向发展。例如，欧盟《人工智能法》序言第89条指出，应鼓励免费和开源工具、服务、流程或人工智能组件；[②]第102条指出，根据自由和开源许可证发布的软件和数据（包括模型），允许公开共享，并且用户可以自由访问、使用、修改和再分发这些软件和数据或其修改版本，这有助于市场上的研究和创新，并可为联盟经济提供重要的增长机会。[③] 我国一直鼓励、支持和引导人工智能技术的开放共享，《专家建议稿》第18条规定，国家支持开源开发平台、开源社区和开源项目运营，第21条规定开源大模型利用他人作品开展模型训练构成合理使用。[④] 可见，开源共享应是大模型未来的发展趋势。

目前，促使大模型研发者开源的动力更多的是一种对技术平等和技术民主的理想主义追求，模型研发者可自由选择是否将模型开源。[⑤] 为促进大模型的开源共享，全球人工智能合作伙伴关系（GPAI）项目小组提出，应当通过建立“标准化合同条款”来实现法律不确定情况下的权利分配，以此实现人工智能大模型和数据共享。[⑥] 这种方式仍然致力于完善大模型的开源生态，本质是希望通过合同创设权益换取大模型的技术共享。不过，单纯依靠商业行为准则和行业自律的方式解决前述问题依旧带有很强的理想主义色彩，“市场激励”方式能够带来的正向价值十分有限。国内有学者认为，为鼓励大模型开源，应当从三个方面提供支持：其一是政府提供财政和公共采购服务支持，其二是制定税收抵免等优惠政策，其三是引入“开源抗辩”，赋予法律责任豁免特权。[⑦] 前两项措施是通过提供经济激励的手段缓解大模型研发的经济压力，由于财政、税收等措施涉及公共利益，实际落地的难度较大。相较而言，引入“开源抗辩”是通过责任豁免的方式来促进技术发展，带来

① Edd Gent, “Protesters Decry Meta’s Irreversible Proliferation of AI But others say open source is the only way to make AI trustworthy”, Ieee spectrum, 2023-10-06, https://spectrum.ieee.org/meta-ai, 访问日期：2025-08-31；Elizabeth Seger/Noemi Dreksler/Richard Moulange et al., “Open-Sourcing Highly Capable Foundation Models: An evaluation of risks, benefits, and alternative methods for pursuing open-source objectives”, Centre for the Governance of AI, 2023-09-29, https://arxiv.org/abs/2311.09227, 访问日期：2025-08-31。

② Artificial Intelligence Act, Regulation [EU] 2024/1689, Preface Article 89.

③ 同上，Preface Article 102。

④ 参见《人工智能示范法（专家建议稿）3.0》第18条和第21条。

⑤ 高奇琦、张皓淼：《技术扩散基础上的整体性对齐：大模型的开源与闭源之争》，载《上海大学学报（社会科学版）》，2024年第5期，第84-97页，这里第86页。

⑥ Global Partnership on AI, “Fostering Contractual Pathways for Responsible AI Data and Model Sharing for Generative AI and Other AI Applications”, p. 4.

⑦ 周辉：《开源人工智能模型的法律治理》，第20页；李学尧：《人工智能立法的动态演化框架与制度设计》，载《法律科学（西北政法大学学报）》，2025年第3期，第32-44页，这里第43页。

的激励效果可能更为直接。不过,责任豁免并没有解决大模型作为智力产品的知识产权保护问题,对于技术公开的激励作用仍然有限。

法律不能无条件强制大模型研发者开放自己的技术和知识,而是需要提供相应的对价,这种对价就是为模型研发者配置无形财产权,对模型研发者赋权可以在私法层面实现创新激励和技术共享的价值目标,即所谓的"以公开换保护"的对价衡平机制。① 在我国,专利权制度是典型的"以公开换保护"的制度设计,②在此模式下,公开和权利呈现的是镜像关系。一方面,大模型开源是赋权保护的前提,但开源并不意味着模型的使用是免费的,③研发者仍然可以向商业应用的下游企业主张经济回报。另一方面,基于开源大模型所创造出的新模型需要继续开源,否则原权利人可以主张侵权救济,由此可以保证大模型的开放使用不会导致原权利人的利益受损,并且可以促进新型大模型不断开源。这种"以公开换保护"的对价机制能够真正解决创新激励不足和权益救济难题。

三、欧盟大模型知识产权的保护路径

既然要对大模型采用赋权保护路径,首先应当考虑的是既有的无形财产权体系能否适用于大模型。人工智能从产生之日起,就与知识产权有着天然的亲缘关系。如果说作为科学技术的人工智能是一种必然,那么作为法律机制的知识产权就是一种应然。④ 从知识产权类型学的角度观察,大模型作为一种新型的智力劳动成果,与著作权和专利权的客体具有一定的相似性,在欧盟现行知识产权框架下,大模型可以适用著作权或者专利权的保护路径。⑤

(一)欧盟大模型的著作权保护路径

欧洲议会与欧盟理事会联合发布的《计算机程序保护指令》并未明确计算机程序的概念,仅限定"计算机程序"应包括嵌入硬件的程序及其预备性设计材料。该指令提供的保护适用于计算机程序以任何形式呈现的表达,但不延伸至程序(包括其接口)背后的思想、原理、逻辑、算法或编程语言。⑥ 尽管《计算机程序保护指令》

① 徐瑄:《知识产权的正当性——论知识产权法中的对价与衡平》,载《中国社会科学》,2003年第4期,第144-154页,这里第149页。

② 梁志文:《论专利公开》,北京:知识产权出版社,2012年版,第41页。

③ 郑志峰:《人工智能产品责任的立法更新》,《法律科学(西北政法大学学报)》,2024年第4期,第3-17页,这里第17页。

④ 曲三强:《论人工智能与知识产权》,第39页。

⑤ Peter Georg Picht/Valerie Brunner/Rena Schmid, "Artificial Intelligence and Intellectual Property Law: From Diagnosis to Action", Max Planck Institute for Innovation and Competition Research Paper No. 22-08, pp. 1-41, here p. 7.

⑥ DIRECTIVE 2009/24/EC, Article 1.

并未明确计算机程序的概念，但是欧盟法院通过案例的形式确认，计算机程序是“以编程语言编写、可被计算机执行以完成任务”的指令集。[①] 基于该指令，计算机程序被视为《伯尔尼公约》中的文学作品，从而受到欧洲版权法的保护。不过，大模型与计算机程序在技术特征方面存在巨大差异，大模型能否像计算机程序一样受到欧洲版权法的保护尚需检视。

根据《计算机程序保护指令》第 1 条第 3 款，计算机程序受到版权保护的前提是具有独创性，即属于作者自身的智力创造成果。[②] 欧盟立法并未直接规定独创性的判断标准，但自 Infopaq 案始，欧盟法院通过判决形式确立了作品独创性的判断标准：作品必须体现作者“自由且富有创造性的选择”，能够反映出作者基于其个性的智力创造。[③] 与之相反，若作品的表达方式由技术或功能规则决定，此时作品并非通过作者独创性的方式表达，无法体现出作者的个性特征，因而无法认定满足创造性要件的要求。[④] 换言之，仅遵循技术功能要求而创作出的作品无法体现作者的智力创造。由于大模型具有自主学习的特征，即便研发者在算法架构的选择、参数设置和训练数据的整理方面有独创性的贡献，但研发者无法决定上述初始贡献能够对最终完成训练的模型产生怎样的影响，即研发者并未定义和完全控制大模型研发的具体过程，因而大模型的研发并不能体现作品创作的完全自主性。[⑤] 因此，大模型能否像计算机程序一样成为版权法的保护对象尚存疑问。

此外，基于思想和表达二分法，欧盟的《计算机程序保护指令》只保护表达而不保护思想。大模型的核心是数学函数，属于不受保护的思想范畴，大模型的功能与表达的弱关联性导致版权法无法为其提供有效保护。[⑥] 即使认为大模型构成版权法意义上的作品，版权保护模式仍存在三点弊端。

其一，版权保护模式只能将保护范围限于大模型包含的算法表述或特定排列，

① Bezpečnostní softwarová asociace-Svaz softwarové ochrany v Ministerstvo kultury, Case C-393/09, Judgment of the Court (Third Chamber) of 22 December 2010, ECR 2010 I－13971, ECLI:EU:C:2010:816.

② DIRECTIVE 2009/24/EC, Article 1.3.

③ Case C-5/08 Infopaq International A/S v Danske Dagblades Forening [2009] ECLI:EU:C:2009:465; Case C-145/10 Painer [2011] ECLI:EU:C:2011:798.

④ Case C-393/09 Bezpečnostní softwarová asociace [2010] ECLI:EU:C:2010:816.

⑤ Begoña Glez. Otero, “Machine Learning Models under the copyright microscope: is EU Copyright fit for purpose?”, p. 27.

⑥ Josef Drexl/Reto M. Hilty/Luc Desaunettes-Barbero et al., “Artificial Intelligence and Intellectual Property Law — Position Statement of the Max Planck Institute for Innovation and Competition of 9 April 2021 on the Current Debate (April 9, 2021)”, p. 18.

而大模型最有价值的部分，即此类排列的功能性将不受保护，并保留在公共领域。[①] 大模型的典型功能性特征是能够根据特定输入生成特定输出结果，其主要应用于三类场景：第一类是图像检测、视频检索，如人脸识别；第二类是智能决策，如能与人下围棋的阿尔法狗；第三类是自然语言处理。[②] 从现有的侵权方式来看，利用知识蒸馏或者模型蒸馏等技术进行知识迁移，训练出与原模型功能相同的新模型是典型的侵权方式，例如竞争者可以通过模型微调、剪枝、蒸馏的方式，根据已知网络的输入输出训练一个替代模型，从而侵犯原模型研发者的权利。[③] 从大模型研发者的权利诉求来看，其想要获得保护的并非模型代码，而是防止他人通过窃取自己研发成果和技术的方式开发出功能相同的替代模型。一方面，即使是按照相同的代码，数据训练不同，最终呈现的大模型的功能差异亦很大。另一方面，即使是代码不同，功能仍然可能是相似的。例如，在斯坦福大学学生剽窃中国人工智能大模型案件中，两个模型尽管在表达方式方面具有一定的不同，但是在提供的答案内容甚至答案的错误方面具有高度相似性。[④] 如果仅对大模型代码的文字表达形式进行保护，则此类侵权行为就无法得到有效制止。

其二，著作权自作品创作完成时的自动取得，以及著作权登记的形式审查等制度设计与大模型的保护并不适配。大模型的训练过程会诱发著作权和个人信息权益等领域的侵权风险。[⑤] 正因如此，国内学者多从风险治理的角度展开相应讨论，主张通过强化法定义务的方式化解大模型训练阶段的侵权风险。[⑥] 大模型训练的高侵权风险要求监管部门提高监管和审查门槛，不满足合法性要件的大模型不仅无法获得法律保护，研发者还需承担相应的法律责任。因此，训练过程的合法合规

---

① Begoña Glez. Otero, "Machine Learning Models under the copyright microscope: is EU Copyright fit for purpose?", p. 25.

② 曲三强：《论人工智能与知识产权》，第47－48页。

③ 王馨雅、华光、江昊等：《深度学习模型的版权保护研究综述》，载《网络与信息安全学报》，2022年第2期，第1－14页。

④ Hu Yuwei, "China runs to be one of top global players in AI model R&D, says ModelBest co-founder", *Global Times*, 2024－06－20, https://www.globaltimes.cn/page/202406/1314470.shtml, 访问日期：2025－08－31。

⑤ Philipp Hacker, "A Legal Framework for AI Training Data — From First Principles to the Artificial Intelligence Act", *Law, Innovation and Technology*, Vol. 13 No. 2, 2021, pp. 257－301, here p. 261; Sandra Wachter/Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, Vol. 2019, No. 1, 2019, pp. 494－620, here p. 497.

⑥ 黄锫：《人工智能大模型训练数据的风险类型与法律规制》，载《政法论丛》，2025年第1期，第23－37页；陈禹衡：《生成式人工智能中个人信息保护的全流程合规体系构建》，载《华东政法大学学报》，2024年第2期，第37－51页；张涛：《生成式人工智能训练数据集的法律风险与包容审慎规制》，载《比较法研究》，2024年第4期，第86－103页。

是赋权保护的前提，未经合法性审核的大模型无法满足设权要求，著作权的自动取得模式不能适用于大模型。

其三，著作权的保护期限是50年，如此长的权利保护期限容易对技术创新造成过度限制，不利于生成式人工智能的产业更新。以OpenAI为例，其研发的GPT系列模型几乎以每年一更新的速度从GPT-1提升到GPT-5，更新换代的速度非常快。对大模型设置过长保护期明显与创新激励的制度目标相违背。综上可见，著作权保护路径面临权利客体不适格和保护力度不适配两方面的困境，无法满足人工智能技术迭代背景下模型研发者的权利保护需求。综上可见，欧洲版权法框架下的保护模式难以适配大模型的技术特征与研发者的权益诉求。

（二）欧盟大模型的专利权保护路径

由于版权保护模式存在弊端，欧盟开始寻求专利权的保护模式。专利权是典型的“以公开换保护”的对价平衡机制，发明人必须公开技术方案才能获得专利权保护。[①] 其制度构造与大模型开源保护的价值取向相契合，因此通过专利权路径保护研发者的权利更为适合。随着计算机软件技术和生成式人工智能的迅速发展，现代各国专利立法和授权实践的总体趋势是将“可专利主题”的范围不断扩大。[②] 为适应人工智能时代技术发展的需要，欧洲专利局（EPO）更新了人工智能发明的审查标准，以期为人工智能的专利保护扫清障碍。

根据《欧洲专利公约》的规定，一项发明被授予专利权的条件是具备技术特征并解决技术问题，具有新颖性和创造性，且能够进行工业应用，科学发现和数学方法被排除在专利的保护范围之外。[③] 故与其他发明一样，通过计算机实现的发明（CII）和人工智能相关的发明必须满足新颖性、创造性、工业实用性和技术特征等基本法律要求才能获得专利。由于新颖性和工业实用性要件的满足并不困难，通过计算机实现的发明能否被授予专利权主要取决于其是否满足技术特征要件和创造性要件的要求。从人工智能发展史来看，人工智能整体经历了从基于规则符号的人工智能转向基于数据的连结人工智能的演进脉络。相较于传统人工智能，深度学习模型并非按照预先设定的规则执行演算，而是从数据中学习和生成自己的规则。[④] 由于深度学习模型最终呈现为数学函数，其本身属于智力活动的规则和方法，因而长期被排除在专利权保护的客体范围之外。

---

① 吴欣望：《对价视角下的专利制度》，载《知识产权》，2021年第3期，第69－83页，这里第69页。

② 吴汉东：《人工智能生成发明的专利法之问》，载《当代法学》，2019年第4期，第24－38页，这里第27页。

③ European Patent Convention, Article 52.

④ Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law*, Cambridge: Cambridge University Press, 2020, pp. 28－30.

但是，随着基于实用主义的“伦理化最小化”思想在专利法律实践中的运用，各国专利保护的客体范围限制正逐渐放宽，介于科学发现与发明创造中间形态的智力成果逐步被专利法所接纳。[①] 尽管生成式人工智能模型（作为数学函数）本身不能作为专利权的客体，但是只要其嵌入具有技术效果的具体应用场景便可被纳入专利权的保护范围。[②]

作为《欧洲专利公约》缔约国授权的专利授予机构，欧洲专利局一直致力于根据最新技术发展动态更新审查实践，用于评估通过计算机程序实现的发明的可专利权，具体包括对数学方法、人工智能及计算机实现的模拟、设计或建模的可专利性提供进一步指导。[③] 通过计算机实施的发明和人工智能相关专利申请量的激增，促使欧洲专利局开始认真审视决定其可专利性所需的标准。欧洲专利局上诉委员会作为该组织的司法机关，有权对《欧洲专利公约》进行解释，在过去的几十年间，其处理了逾千起通过计算机实施发明的案件。在此过程中，上诉委员会通过多项裁决对《欧洲专利公约》中关于“发明”定义的条款进行阐释，由此建立了一套成熟的判例体系，为此类发明的可专利性标准提供了明确指引。[④] 其主要的贡献在于明确了技术特征要件和创造性要件的审查标准。

对于技术特征要件的审查，欧洲专利局认为，若权利要求仅限定抽象客体（如数学方法），则属于排除范畴。例如，仅限定“使用机器学习的分类方法”的权利要求被视为抽象方案（即非技术性方案）而予以排除。同理，“深度学习”和“人工神经网络”等术语若直接作为权利要求主题，均属于《欧洲专利公约》第52条第（2）款（a）项的排除对象。然而，若权利要求包含技术手段，则不被归入排除客体。因此，与算法有关的发明，其权利要求至少需包含一项技术组件才具备可专利资格。例如，只要提及物理系统（如“在计算机上实施的方法”）即可为权利要求提供通过资格测试的充分技术基础。类似地，权利要求中引用特定物理信号也可使其具备技术性——该方法常被称为“任意硬件法”。[⑤] 由于计算机实施发明仅需体现或利用

① 刘鑫：《人工智能时代科技伦理的专利法回应》，载《法商研究》，2025年第2期，第187－200页，这里第191页。

② Josef Drexl/Reto M. Hilty/Luc Desaunettes-Barbero et al., “Artificial Intelligence and Intellectual Property Law — Position Statement of the Max Planck Institute for Innovation and Competition of 9 April 2021 on the Current Debate (April 9, 2021)”, p. 16.

③ Jean-Marc Deltorn/Andrew Thean/Markus Volkmer, “The examination of computer implemented inventions and artificial intelligence inventions at the European Patent Office”, 4iP Council (Jan. 2019), pp. 1－6, here p. 1.

④ William Chandler, “Patentability of computer- implemented inventions (CⅡs): state of play and developments”, Official Journal EPO, Supplementary publication 5, 2015, p. 73.

⑤ 同注③，p. 5。

任何形式的技术手段即可通过《欧洲专利公约》第52条第(2)款和第(3)款的第一道可专利性门槛，这一资格门槛通常比较容易跨越。

对于兼具技术与非技术特征的混合型发明创造性要件的审查，欧洲专利局遵循判例确立的审查原则：在评估同时包含技术特征与非技术特征、整体具有技术性的发明的创造性时，应考虑所有解决技术问题的特征，而未作出此类贡献的特征不能作为支持创造性的依据。换言之，若一项特征未能通过产生技术效果而解决技术问题，则在创造性评估中不予考量；反之，所有对发明技术属性作出贡献的特征均应纳入创造性要件的判断考量。[①] 故关键问题在于判断非技术特征是否以及在何种条件下能够产生技术贡献。对于数学方法而言，若能证实该数学方法因应用于技术领域或适配于特定技术实施而产生技术效果，则在评估创造性时，应考虑各步骤在实现该既定技术效果时的计算效率，计算效率的提升可构成技术效果。例如，当算法专门适配计算机内部运行机制，如利用不同处理器单元(CPU与GPU)分阶段训练机器学习模型，即可视为对发明作出技术贡献。[②] 同理，服务于技术目的的数学算法也可增强计算机实施发明的技术属性。[③]

在此背景下，欧洲专利局总结了日益丰富的判例法的经验，并将其整合后修改了《欧洲专利局审查指南》(以下简称为《审查指南》)，以确保对人工智能相关发明审查标准的一致性。最新版《审查指南》扩充了关于“数学方法”的章节(G-Ⅱ部分第3.3节)，并新增专门针对“人工智能与机器学习”的子章节(G-Ⅱ部分第3.3.1节)。这些章节为计算机实施发明和人工智能领域相关发明的可专利性判断提供进一步指引。《审查指南》G-Ⅱ部分第3.3节列举了数学方法可实现的多类技术目的(非穷尽示例)，其中包括控制特定技术系统或工艺，数字音频、图像及视频领域的编码、压缩或分析等应用同样属于技术目的，但仅限定输入数据本身并不足以确保数学方法产生技术贡献——数学方法是否服务技术目的，主要取决于其所产生的结果是否具有直接技术关联性。[④]

由于大模型与算法本身具有抽象的数学性质，《审查指南》G-Ⅱ部分第3.3节关于数学方法的指引同样适用。《审查指南》明确指出，人工智能和机器学习基于计算模型与算法，例如人工神经网络、遗传算法、支持向量机、K均值算法、核回归以及判别分析，这类计算模型和算法本身具有抽象的数学性质，无论其能否通过训练数据进行“学习”。[⑤] 然而，若一项技术方案中包含数学函数，并不当然意味着其

① Case T 0641/00(Two identities/COMVIK)of 26 September 2002, OJ EPO 2003, 352.

② Case T 0258/03(Auction method/HITACHI)of 21 April 2004, OJ EPO 2004, 575.

③ Case T 1227/05(Circuit simulation I/Infineon Technologies)of 13 December 2006.

④ Guidelines for Examination in the European Patent Office, G-Ⅱ, 3.3.

⑤ 同上，G-Ⅱ，3.3.1。

不可获得专利权保护。例如，在心电监护设备中运用人工神经网络识别心律失常的模式被视为有技术贡献；对音频、图像及视频信号的分类亦属典型技术应用，上述发明因满足技术特征要件而可被授予专利权。但仅根据文本内容对文本文档进行分类属于语言学目的，而非技术目的。类似地，对抽象数据记录甚至“电信网络数据记录”进行分类，但并未指明该分类结果有任何技术用途，这本身也不构成技术目的。[①] 因此，在欧盟，无论是包含人工智能技术的应用还是基于注意力机制的大模型系统都有成功获得专利授权的案例，只要其能够转化为特定领域的技术应用或能够解决具体的技术问题。[②]

四、大模型知识产权保护路径的中国方案

中国的人工智能相关立法正处于广泛征集意见的阶段，《专家建议稿》和《学者建议稿》已经建立了相对完善的义务和责任体系，为促进人工智能技术向善和大模型风险防范提供制度支撑。[③] 相较而言，对于大模型研发者的权利配置规范则相对薄弱，尽管《专家建议稿》已通过专章的形式规定了支持大模型创新的措施，涵盖了基础模型训练利用作品法定许可和开源基础模型训练著作权合理使用的内容，但未进一步明确大模型研发者的权利配置方案。对此，可在借鉴欧盟经验的基础上，充分发挥后发优势，构造大模型知识产权保护的中国方案。

（一）欧盟大模型知识产权保护路径对我国的启示

通过前述对欧盟大模型保护路径的梳理可知，行为规制路径存在明显局限性，赋权保护模式更为可取。大模型赋权保护的理论基础不仅在于“强化保护”，而且在于“促进开源”，这就要求立法者在以下两方面取得平衡：一方面是通过知识产权权利可能提供的激励来促进创造与创新，另一方面则是要应对此类排他性权利可能产生的垄断固化和功能失调等风险，保证公众可以享受新兴技术发展的红利。[④]

为实现上述利益平衡，我国一方面需要从权利的弱排他性构造出发，另一方面需要强化对大模型的监管，尤其是强化开源模型的风险防范机制。就前者而言，首先，赋权保护以模型开源为前提，闭源模型被排除在权利客体之外，这与专利权“以

① Guidelines for Examination in the European Patent Office, G-Ⅱ, 3.3.1.

② Rebeca Ferrero Guillén/Altair Breckwoldt Jurado, “Vagueness in Artificial Intelligence: The‘Fuzzy Logic’of AI-Related Patent Claims”, *Digital Society* , Vol. 2, No. 3, 2023, pp. 1-25, here p. 11.

③ 《专家建议稿》和《学者建议稿》第四章都通过专章形式确立了人工智能研发者与提供者的义务性规定，内容涵盖安全性义务漏洞管理义务、审计义务、补救和通知义务、公开透明性义务、可解释性义务、人工智能伦理审查义务和备案义务等义务体系，可为人工智能的风险防范提供相对充足的制度支撑。

④ Reto M. Hilty/Jörg Hoffmann/Stefan Scheuerer, “Intellectual Property Justification for Artificial Intelligence”, p. 12.

公开换保护”的制度设计相契合。其次，知识产权赋权所要求的智力成果要件需要得到满足，不满足创造性要求的大模型不予赋权保护。最后，为避免对研发者权利的过度保护造成创新阻碍或垄断风险，需要对大模型研发者的权利进行适度限制。就后者而言，欧盟《人工智能法》确立了“基于风险”的治理路径，设计了禁止规则、合规规则和豁免规则三类人工智能监管规则，从而建立了一整套人工智能监管体系。[①] 值得注意的是，欧盟《人工智能法》过度强调风险防范，忽视了模型研发者的权利保护。根据比利时智库欧洲国际政治经济中心的预测，过高的监管成本会导致成百上千亿欧元的消费者福利损失。[②] 为避免欧盟立法模式带来的弊端，我国立法应当妥善平衡风险监管与知识产权保护的关系。

国务院印发的《新一代人工智能发展规划》指出，要建立人工智能技术标准和知识产权体系，加强人工智能领域的知识产权保护，健全人工智能领域技术创新、专利保护与标准化互动支撑机制，促进人工智能创新成果的知识产权化。[③] 可见，赋权保护模式契合中国人工智能发展的政策导向。为了满足专利权保护路径对技术特征、新颖性、创造性、工业实用性等要件的要求，欧盟修改了技术特征和创造性要件的认定标准，从而将大模型纳入专利权的保护范围之内。这意味着，大模型只有在下游应用端和特定应用程序结合在一起时才能作为“应用系统或装置的一部分”获得专利保护。

该路径的优点在于可回避模型本身专利性适格的判断难题，同时便于结合具体技术场景撰写明确的权利要求。但此时大模型的权利范围受限于特定应用装置或应用系统，难以覆盖大模型在其他场景中的通用性价值，从而无法体现模型自身的独立价值。如果不能将大模型本身的技术方案写进权利要求，则权利人无法对使用者的“分发”或“将参数更新再生产”等行为主张权利，[④]最终导致对研发者的权利保护不足。于是，在专利权的保护路径下，大模型可受保护的范围只能局限于特定的应用场景，其通用性能越强，获得专利权保护的可能性越小。这种结果与大模型的技术特征相悖，也与激励通用型大模型发展的价值取向相悖。

从大模型的研发过程可知，可训练的参数（权重）可以通过深度学习模型自主

① 刘子婧：《欧盟〈人工智能法〉：演进、规则与启示》，载《德国研究》，2024年第3期，第101－128页，这里第115页。

② 曾雄、梁正、张辉：《欧盟人工智能的规制路径及其对我国的启示——以〈人工智能法案〉为分析对象》，载《电子政务》，2022年第9期，第63－72页，这里第68页。

③ 《新一代人工智能发展规划》（国发〔2017〕35号），第5条。

④ 河野英仁：「AI技術の特許による保護——日本及び米中での特許による保護—」，パテント，73巻8号，2020，頁51－52。

学习并更新，正因如此，输入训练集合的不同会改变模型功能。这就意味着，只需要改变或者提升训练数据集合的内容，已完成训练的大模型就会被更好的数据训练的学习模型所替代。有学者指出，此类专利的保护范围将受到严重限制，侵权者只需对权利要求中的部分参数稍作修改，就能逃避法律制裁——这种修改并不会显著影响调整后模型的技术效果，故针对具体神经网络的专利实际上几乎无效。[①] 例如，新模型的研发者基于新获得的训练数据，在云服务器上对已分发的学习模型进行再训练，可以更新学习模型的参数。然后，新模型研发者可以通过云服务器向目标设备分发再训练后的参数，从而在不改变已分发的学习模型的超参数的情况下，仅更新模型的部分参数。在这种情况下，学习模型的功能会暂时丧失，但是通过使用新的参数，再次生成的模型可以完成功能升级，也就是说，超参数本身没有被改变，但通过参数的更新，新的学习模型得以再生。[②] 对于此类利用原模型技术方案开发新模型并应用于新领域的行为，原模型研发者难以主张权利，实质上构成了侵权豁免。

由此可见，专利权的保护路径仍然有一定程度的局限性。为实现大模型研发者权利的全面保护，我国应当在参照专利权保护路径的模式下，构造出符合大模型技术特征及其公益属性的新型知识产权保护方案。中国的人工智能立法正处于研讨阶段，与其改造专利法，不如直接在未来的《人工智能法》中增设模型开发者的权利保护规定，创设新的权利类型。权利客体、权利内容和权利限制是新兴权利构建的核心内容，因此我国需要从以上三个方面展开大模型研发者的权利构造。

（二）大模型知识产权保护的中国方案构造

1. 权利客体

由于大模型凝结的创造性智力劳动与专利权客体的相似性，以及专利制度“以公开换保护”的制度模式与大模型开源理念相匹配，专利权的构造模式可为大模型权利设计提供借鉴。“产品专利”与“方法专利”是一种公认的对专利客体类型的划分方式。同样，大模型知识产权的客体界定方式也可以考虑分为“算法模型的生成方法”和“完成深度学习的模型结果”两种。不过，前者界定方式存有明显弊端应予放弃，能够获得知识产权保护的客体只能是完成训练的模型本身，原因在于以下几个方面。

其一，在现有的技术条件下，“算法模型的生成方法”差别不大，模型训练过程在很多场景中已被视为常见操作，将模型训练方法作为知识产权客体明显无法满

① Thomas Watkin/Andrew Rau, “Intellectual property in artificial neural networks - In particular under the European patent convention”, *Ⅱ C-international Review of Industrial Property and Copyright Law*, Vol. 27, No. 4, 1996, pp. 447-469. here p. 464.

② 河野英仁：「AI技術の特許による保護——日本及び米中での特許による保護—」，頁52。

足创造性的要求。相反，训练完成的模型则可以在模型规模、应用能力、通用程度等多方面体现出功能区分。大模型的运算结果的准确率和精确度等功能的提升，可以反映研发者智力贡献的创造性程度，更符合知识产权客体需具备智力成果属性的要求。

其二，从社会整体效益来看，即使公开模型的研发过程和方法，在缺少高质量数据集合的情况下，大模型也难以被其他经营者或社会公众所再现，更无法研发出相同的产品。[①] 尤其是对于通用型大模型的研发来说，研发所需要投入的人力、财力和物力仅有少数企业才能做到，这种技术公开所带来的积极价值有限。与公开模型研发方法不同，公开已完成学习的算法模型并允许他人使用，可以直接为下游企业赋能，从而有助于形成完整的人工智能产业链并且为用户提供基础服务。大模型的通用性能越强，能够助力的产业和行业就越多，由此获得的利益就应当越多，高度契合“以公开换保护”的制度目标。

其三，“算法黑箱”和“技术黑盒”等难题仍未解决，即使是研发人员也无法解释算法模型最终能够呈现何种形态。[②] 此外，准确描述技术方案在可行性上也有所欠缺，基于同样的理由，第三方主体对于权利客体的审查亦有困难。相较而言，对于完成训练的模型本身进行描述和审查都更为清晰，这有助于合理地划定权利客体的边界范围。因此，大模型知识产权的客体只能是已完成训练的模型本身，而非其训练方法。

正因如此，欧盟《人工智能法》第 3 条关于通用人工智能的定义从技术特征和功能特征两方面加以界定，权利客体的实质性要件可考虑按此方式确定。首先，从技术特征来看，大模型是基于深度学习架构并在大量数据上训练而来的，表现为一定规模参数的算法模型。其次，从功能特征来看，大模型可以执行特定或多种任务，并有可适应性、可扩展性和可使用性，能够为下游应用提供基础。最后，大模型的训练和研发一定是合法的，满足合法性要件是大模型获得财产权保护的前提。作为数据驱动的技术成果，大模型训练的合法性要件主要体现在训练数据的收集和利用的合法性上。从欧盟的审查实践来看，大模型作为专利客体的精准描述需要从算法架构、权重、训练数据、技术性能等方面来限定。[③] 综合上述特征和欧盟

① 王德夫：《论人工智能算法的知识产权保护》，载《知识产权》，2021 年第 11 期，第 50－70 页，第 63 页。

② Cary Coglianese/David Lehr, “Transparency and Algorithmic Governance”, *Administrative Law Review*, Vol. 71, No. 1, 2019, pp. 1－56, here pp. 14－16.

③ Rebeca Ferrero Guillén/Altair Breckwoldt Jurado, “Vagueness in Artificial Intelligence: The‘Fuzzy Logic’ of AI-Related Patent Claims”, pp. 13－19.

标准，[①]大模型的创造性要件主要体现在模型的参数量、数据集合的质量或大小、训练模型所用的计算量、模型的输入和输出模式以及模型能力等方面，由此可以做到模型之间的区分。

2. 权利内容

基于“以公开换保护”的对价平衡机制，大模型研发者获得模型知识产权保护的前提是将模型开源，但是开源并不意味着模型研发者的权利不受保护。欧盟《人工智能法》第53条第2款规定，通用人工智能模型的开源许可包括允许他人获取、使用、修改和分发模型，其参数，包括权重、模型结构信息和模型使用信息，均向公众公开。[②] 由此可以反推，模型研发者应当享有使用权、修改权和分发权等权利。其中，使用权指向的是财产性权利，而修改权和分发权则与著作权的修改权和保护作品完整权相似，指向的是人身性权利。除修改权和保护作品完整权外，著作人身权还包括发表权和署名权。类比作品发表权一次用尽原则，[③]大模型一旦开源就不再享有发表权，但是研发者仍然应当享有署名权。因此，大模型知识产权的内容应当包括署名权、修改权、分发权和使用权。

署名权指的是大模型研发者有权在大模型上标明研发者身份，并且要求任何使用模型的下游企业标明该身份信息。署名权不仅是知识产权人格利益属性的体现，更是市场经济条件下为大模型开源提供正向激励的制度安排。一方面，“套壳”他人模型是实践中模型窃取的主要方式之一，即将他人研发、共享模型谎称是自行研发的模型，Llama3-V套壳MiniCPM-Llama3-V 2.5就是一个典型的例子。[④] 为干预和制裁此类权益侵犯行为，立法上需要设置署名权。开源大模型的研发者很难通过直接出售使用权的方式获取经济回报，但可以通过与开源大模型相关的扩展化与定制化服务来获得经济收入。[⑤] 大模型的免费开源可以被当作一种“价格战”手段，署名权的设立可以帮助模型研发者扩大企业的影响力和市场知名度，从而在市场竞争中占据优势地位。这是目前大模型研发者愿意开源的主要经济动力。因此，署名权是大模型研发者的一项重要权利。

修改权指的是研发者可以自己或者允许他人对大模型的架构、参数、数据、算

① Artificial Intelligence Act, Regulation [EU] 2024/1689, Annex XⅡI.

② 同上，Article 53(2)。

③ 李杨：《论发表权的“行使”——以发表权的权能构造为切入点》，载《法律科学（西北政法大学学报）》，2025年第6期，第133－143页，这里第137页。

④ 朱悦：《模型窃取攻防的技术与法律之维》，2024－06－15，https://mp.weixin.qq.com/s?__biz=MzI3MTYzODg0Mg==&mid=2247565729&idx=1&sn=0d9f83ed65b4acae96d13baf2c35e877&chksm=eaa61e415e9f578815056cb6403d542d400ad0939e1a0e19814e2717c4c3cf7a2dfd0a66c0f9&scene=27，访问日期：2025－08－31。

⑤ 高奇琦、张皓淼：《技术扩散基础上的整体性对齐：大模型的开源与闭源之争》，第87页。

法等因素进行调整和优化。尽管在开源社区内，大模型研发者应当允许其他研究者或开发者对原有模型进行修改或完善，但是与开源软件类似，修改完善后的大模型研发者只有在继续开源的情况下才可以主张“开源抗辩”，否则仍然构成侵权。[①]这种制度安排一方面可以促进大模型不断开源共享，另一方面可以阻止其他企业剽窃技术后选择闭源从而获得不正当竞争优势，消除大模型开源后权利不受保护的担忧。

分发权指的是研发者可以通过云端服务、本地部署等方式将大模型分发给他人使用。在互联网时代，掌握了分发权不仅意味着可以累积更多的用户、发挥规模效应，还能通过分发应用获取更多的训练数据和优化数据，从而促进模型性能不断改进和提升。这使其成为大模型研发者获得市场竞争的有效手段，也是大模型开源的动力之一。

使用权指的是研发者有权自己使用和允许他人使用大模型的权利。在开源模式下，用户或者其他研发者正常使用大模型无需经过原权利人的许可，但是除通用型大模型需要强制免费使用外，其他类型的大模型是否一律应当免费使用仍有探讨的空间。即使认为开源模型的合用途使用应当是免费的，但如果用户违法或者违规使用大模型仍然构成对使用权的侵犯，研发者仍然可以主张侵权救济。

3. 权利限制

精细化的产权结构设计与适度的强制许可制度，可防范对技术资源的过度保护，从而促进知识流通和市场竞争。[②] 在“以公开换保护”的对价平衡机制下，权利保护与权利限制是同步发生的。知识生产具有公共产品的性质，其创造过程本身离不开对社会资源的吸收与利用。大模型作为具有公共产品属性的技术产品，研发者的权利膨胀容易引发垄断危机，[③]因此必须对其权利范围进行合理限制。为促进技术创新和公开披露，人工智能系统应当开源，同时为了适应创新指数级增长的节奏，可以考虑参照未注册外观设计的超短保护期或者采用法律设定的付费许可制度。[④] 因此，大模型研发者的权利限制可以从模型开源、法定许可和保护期限三个方面展开。

首先，模型开源是规避垄断和避免“重复造轮子”的必然要求，亦是模型研发者获得权利保护的前提条件。为促进大模型的创新发展，大模型应当尽可能地全方面开源。目前，大模型开源的实践模式并不统一，我国应尽快加强开源社区的建

① 参见最高人民法院(2019)最高法知民终663号民事判决书。

② Rebecca Tushnet, “Economies of Desire: Fair Use and Marketplace Assumptions”, *William & Mary Law Review*, Vol. 51, No. 2, 2009, pp. 513－546, here p. 513.

③ 许丽：《必需模型反垄断法强制开放的理据与进路》，第54页。

④ Mauritz Kop, “AI & Intellectual Property: Towards an Articulated Public Domain”, pp. 314－315.

设，构建统一的大模型开源标准，避免实践中的无序和混乱状态。需要明确的是，在赋权保护模式下，对于影响模型功能的关键技术因素应当予以全面公开，包括模型架构、训练数据集合、模型参数、算法实现细节、模型训练步骤等多方面内容。此外，我国还应当加强开源模型的风险防范机制构造。在行业内部，我国可以通过开源许可证认证机制实现行业主体的自我约束。例如，可以通过在开源许可证中增设负责任使用条款或行为限制条款，为开源社区提供自我管理和自我监管的手段，促使人工智能系统的使用符合伦理和负责任的标准。国家有关部门应当为开源模型设置不同的风险管理义务和责任条款，将研发者的义务与责任控制在合理范围内，保证措施行之有效且不会造成规制过度。《专家建议稿》中的负面清单管理制度以及研发者的义务性规定可搭建起技术风险防范的基本框架。更为重要的是，开源生态的建立需要政府部门之间、政府和企业之间、国家和国际组织间建立起协同治理机制，防止技术误用和滥用。①

其次，法定许可制度的引入是平衡提供者和使用者权利的制度工具，由此可避免技术垄断和不正当竞争的发生。《专家建议稿》第20条规定了基础模型训练作品的法定许可制度和开源基础模型训练著作权的合理使用制度。同样，已完成训练的大模型作为知识产权的保护客体，仍然需要受到法定许可制度的制约，未来立法对此应予明确。网络用户或其他市场竞争主体使用大模型无需另行经过研发者同意，但其他市场竞争主体若基于商业目的使用大模型，则可以要求其支付一定的报酬或者分享部分利益。国家应当鼓励引导建立许可使用费用及相关行业标准，为技术普惠提供支持。

最后，我国应当设置合理的权利保护期限。基于大模型技术特征和更新换代的速度考量，权利保护期限的设置不宜过长。从GPT系列模型的生命周期来看，大模型更新迭代的周期一般不超过三年。因此，将权利保护期限设置为三年是较为合理的选择。

五、结　语

生成式人工智能的发展引发了技术监管与创新保护的双重需求，二者共同构成了人工智能时代规范配置的理论基础。如何实现技术安全和技术创新的价值平衡成为理论研究的重点课题。欧盟有关大模型保护路径的理论讨论和实践路径为我国立法提供了参考经验，我国应当寻求兼顾技术安全和技术创新的人工智能立法新范式。商业秘密和反不正当竞争法的保护路径容易造成技术垄断，且提供的保护力度并不适配，因此应当舍弃。单一的“强化保护理论”已无法满足数字经济

① 周辉：《开源人工智能模型的法律治理》，第31－32页。

发展的需要，“促进开源共享理论”可作为大模型赋权保护的理论基础，通过“以公开换保护”的对价衡平机制在私法层面实现技术创新激励和技术共享的双重价值目标。考虑到著作权保护路径在权利客体不适格和保护力度不适配等方面的局限性，欧盟倾向于通过专利权保护路径实现对大模型研发者的权利配置。不过，专利权保护路径需将大模型研发者的权利范围限定于特定应用装置或应用系统，难以覆盖大模型在其他场景中的通用价值，无法完全契合大模型自身的技术特性。考虑到欧盟方案的不足，我国应当在欧盟方案的基础上加以改造，通过在《人工智能法》中增设模型研发者权利保护规定的方式，实现研发者权利的全面保护，促进技术开放共享。具体而言，大模型研发者应享有署名权、修改权、分发权和使用权，但须受模型开源、法定许可和保护期限三方面的限制。

责任编辑：江语林