财经法学 No. 2，2026
pp. 36 - 52

论作为独立财产保护的人工智能模型参数
——以“AI模型保护第一案”为切入点

廖慧姣*

内容提要：参数为模型开发企业投入大量资源、利用机器训练而形成的“机器知识载体”，因其“价值性”“可支配性”“非物质性”“知识载体性”以及“非人类符号性”构成了一类新型的知识财产对象。开发者所投入的培育劳动为参数的价值之源，为防止市场失灵应当为参数配置财产保护的激励机制，从而于制度层面实现公共安全与私人利益的平衡。现有保护框架无法妥当安置参数，亟待独立的财产保护路径。通过借鉴知识财产模块的制度设计，可为参数配置一套排他权保护规则。参数的排他权应归属于对“机器知识”增量价值做出决定性贡献的开发者，保护边界仅限于以参数为直接对象的知识迁移行为，包括获取与使用行为。为平衡创新、安全等多元公共利益，参数排他权应以10年保护期为限，并允许“科研、评价与安全评估目的”的反向工程。

关键词：模型参数　机器知识载体　新型知识财产对象　排他权保护　人工智能

在当前的人工智能（artificial intelligence，下文简称AI）浪潮中，模型参数（parameters），无疑是模型开发企业的核心资产。若将由代码所运行的模型结构视为一个大脑框架，那么参数则相当于这个大脑用以思考的“知识”载体。这些耗费大量算力进行数据训练所得出的“最终黄金”，不仅被业界视为最高价值资产，〔1〕也已进入各国政府的国家安全视野。〔2〕近日我国AI模型

* 廖慧姣，同济大学法学院博士研究生。

本文为国家社会科学基金重大项目“完善网络反不正当竞争法律规则研究”（25BFX178）的阶段性成果。

〔1〕 Anthropic的首席信息安全官杰森·克林顿（Jason Clinton）在访谈中表示：“我可能花了将近一半的时间来考虑保护模型的权重文件，这是公司中最受关注和优先考虑的事情，也是我们投入最多安全资源的地方。”See Sharon Goldman, *Why Anthropic and OpenAI Are Obsessed with Securing LLM Model Weights*, VentureBeat (15 December 2023), https://venturebeat.com/ai/why-anthropic-and-openai-are-obsessed-with-securing-llm-model-weights/, visited on 7 January 2026.

〔2〕 兰德国家安全研究部发布了一项主题为《保护人工智能模型权重》的报告，旨在深入关切模型参数的保护议题。See Sella Nevo et al., *Securing Artificial Intelligence Model Weights: Preventing Theft and Misuse of Frontier Models*, Rand (30 May 2024), https://www.rand.org/pubs/research_reports/RRA2849-1.html, visited on 7 January 2026.

保护第一案〔3〕的判决，从实践层面证实，法律亟须回应参数保护的现实需求。该案涉及抖音公司旗下一款部署于用户端的变身漫画成像模型，法院最终以《反不正当竞争法》第2条（以下简称“兜底条款”）为参数提供保护，认定原被告存在直接竞争关系，原告进行大量投入且获得引流效果的参数构成受保护的竞争优势，被告未经许可直接使用原告经数据训练而来的模型参数，有违AI领域的商业道德，扰乱竞争秩序，且因替代和分流作用，导致原告合法权益受到损害。

虽然判决从结果层面维护了原告利益，却在法律逻辑和保护范围上存在三大疑问，为未来的司法实践埋下隐患：其一，参数保护的正当性基础不明。故而，法院并未实质性回应被告的“开源来源”以及“非法训练”抗辩，〔4〕仅以举证不足为由驳回。学界就后者存在“保护前提说”〔5〕与“独立评价说”〔6〕两种观点。其二，参数保护的路径选择存疑。该案未充分论证参数适用知识产权专门法和反法专门条款保护的可能性。因而，有反对者提出，专门法的沉默即意味着法律的否定，不应轻易动用兜底条款打开“法外保护”的缺口。〔7〕其三，参数的兜底条款保护难以合理地划定保护边界。一方面，“竞争关系”和“合理利益损害”等要件无法适配参数的多元利用场景，如跨领域迁移学习（transfer learning）、〔8〕非商业性泄露或使用〔9〕等实践。另一方面，判决确立的“未经许可使用即违反商业道德”标准，实际为参数提供了近乎绝对权的保护，却未配置任何限制机制。依据该案的专家意见，被告可能通过技术手段从抖音软件中提取模型参数。由于提取对象为合法获取的客户端软件，该行为在性质上属于反向工程。因而，在软件版权领域视为正当的反向工程行为，在该案中被定性为不正当，缺乏充分的法理依据。

上述疑问的共同根源在于，法院在未明确参数法律性质的前提下，直接适用兜底条款提供“临时保护”。其虽实现了结果正义，却导致保护的正当性基础、适用范围和限制机制均不明晰甚至存在矛盾。现有研究多聚焦于兜底条款的适用争议，对于参数究竟是什么性质的财产对象讨论不足。财产对象的形态决定了财产对象的利用方式，进而影响主体间的法律关系。〔10〕参数的保护问题，仍需叩问参数的本质特性。参数为企业投入大量资源获得的“机器知识载体”，与传统知识财产对象存在亲缘关系（均承载知识），但又显现出特殊的“非人类符号性”（仅以机器可读

〔3〕 参见北京知识产权法院（2023）京73民终3802号民事判决书。

〔4〕 二审判决在回应被告抗辩时，以“未证明训练合法性与参数设计相关”为由回避实质审查，但在商业道德判断中，又强调参数系“经数据训练而来”，实际承认了训练行为对参数价值的决定性作用。

〔5〕 该观点认为，只有训练行为合法，参数才属于受保护的竞争利益。参见环球律师事务所：《环球科技法前沿系列 | 模型方法论在解决AI侵权纠纷中的作用——评首例AI模型结构和参数保护案》，载微信公众号“环球律师事务所”2025年4月29日。

〔6〕 该观点主张，训练行为的合法性与参数是否受保护系两个独立评价的问题。参见姚志伟、方梓楠：《数据训练行为合法性对模型开发者法益的影响研究》，载微信公众号“垦丁学社”2025年7月23日。

〔7〕 参见宋建宝：《人工智能模型结构与参数的知识产权保护》，载微信公众号“知产观察家”2025年10月30日。

〔8〕 迁移学习是将在特定领域（领域A）和任务（任务A）上训练好的模型参数（权重），应用到另一个完全不同领域（领域B）或任务（任务B）的模型中，以加速训练或提高性能。例如，将本案所涉及的变身漫画成像模型参数迁移至医学图像模型上。See Sinno Jialin Pan & Qiang Yang, *A Survey on Transfer Learning*, 22 IEEE Transactions on Knowledge and Data Engineering 1345 (2009).

〔9〕 这是指泄露者或使用者与原模型参数所有者不存在竞争关系，且其行为本身不以直接获取金钱或商业利益为目的。例如，某开发者在开源平台上分享通过反向工程所提取的变身漫画成像模型参数。

〔10〕 参见李琛：《论知识产权法的体系化》，北京大学出版社2005年版，第38页。

的形式呈现）。这种特殊定性使得参数的知识迁移〔11〕行为呈现出独特的成本非对称性，导致参数既难以被现有知识产权专门法所涵摄，但又不能简单地排除在财产保护体系之外。据此，本文旨在从模型参数的法律定性这一原点出发，系统评价对其保护的正当性与必要性，进而确定适配的保护路径，最终构建一套既能保障模型开发者核心利益，又能促进产业健康发展的可行方案。

一、参数的新型知识财产对象定性

如果说人脑知识承载于神经元突触之中，那么，参数便为机器大脑中承载模型全部知识、驱动其智能涌现的“机器知识载体”。鉴于参数与知识财产对象具有一致的内在属性，但形态不同，应将其视为一种新型的知识财产对象。

（一）参数的本质特征：机器知识的载体

从逻辑范式（符号主义，symbolism）到生物范式（连接主义，connectionism），AI 大脑的知识载体由最初基于人类预定义符号的逻辑规则，转变为神经网络连接中的参数，这些参数通过数据驱动的端到端学习自主生成。〔12〕本文讨论的参数，为连接主义范式下承载机器所习得知识的载体，代表神经网络中一个节点对另一个节点的影响大小，〔13〕用以调节输出与所需输出之间误差的实数，〔14〕包括权重（weights）与偏置（bias）。若将一个神经元简化理解为线性函数“$Y=wX+b$”，其中 w、b 分别为权重和偏置，通过输入数据“X”以及真实结果“Y'”反复调整 w 和 b 的数值，从而使得预测结果“Y”和真实结果“Y'”之间的误差最小。在大模型中，这个函数则更为复杂，是一个包含数以万亿计参数的巨大非线性函数网络，共同决定着模型对输入的回应。从这个意义上而言，AI 模型保护第一案中，法院所列举的参数内容“如卷积层的输入数据的通道数、输出数据的通道数、卷积核的大小、卷积运算时的步长、是否使用偏置以及对图片的填充”是对参数概念的扩大解释，因其仅为规划训练步骤和方向的超参数，并非从数据中学习到最终知识的参数。

从上述技术原理来看，参数是模型开发企业通过投入大量资源，利用机器训练而形成的一种特殊财产对象形态——“机器知识载体”。其具备以下几个核心特征：其一，衍生性，即参数由原始数据衍生而来。参数并非人类直接设置或调控的结果，而是通过机器对大量原始数据进行训练而衍生的产物。这些原始数据的来源广泛，既可能包含受知识产权保护的对象，如该案涉及的漫画作品，也可能囊括各类机器数据（如教师模型的原参数、中间层特征表示等非人类可读数据）。〔15〕

---

〔11〕 知识迁移是指知识从一个主体转移至另一个主体的过程。在传统人类社会中，知识迁移主要通过外部符号系统（如书籍、论文、教学）实现。

〔12〕 See Hubert L. Dreyfus & Stuart E. Dreyfus, *Making a Mind Versus Modeling the Brain: Artificial Intelligence Back at a Branchpoint*, 117 Daedalus 15 (1988).

〔13〕 参见邱锡鹏：《神经网络与深度学习》，机械工业出版社 2020 年版，第 14 页。

〔14〕 同上注，第 12 页。

〔15〕 技术领域也有观点推测，该案被告是通过模型蒸馏（并非提取参数）而获得的最终模型。参见一川 Law：《闲话 AI | 第 23 期：AI 模型结构、参数侵权首案疑云》，载微信公众号“一川 Law”2025 年 6 月 3 日。

其二，实质投入性，强调企业需进行大量的资源投入以训练参数。模型参数的训练绝非简单的数据复制或机械转换过程，其需投入海量的、经过精心清洗和标注的数据作为“教材”，精巧设计的模型架构作为“骨架”，以及极其昂贵的算力与电力资源作为驱动训练的“能源”。正如AI模型保护第一案中法院所查明的事实，变身漫画特效模型参数的生成过程要历经“风格设定”“风格化量产”“模型训练”“模型再调整”四个需要大量资金和算力投入的过程。

其三，增益价值性，参数具有促使模型思考的知识增益价值。对于作品、个人信息等原始数据，其价值实现依赖于人类对其内容的理解和使用，而参数的价值体现在技术功能层面而非信息内容层面：参数通过控制神经网络中的连接强度，操控模型进行有价值的输出。如本案所争议的变身漫画特效模型参数，其价值并非体现在人类能够从中读取什么信息，而是在于其被加载到模型后，能够控制模型将“用户实时拍摄的照片视频”输出为符合预期的“漫画风格”图像。

其四，形态的特殊性。参数不是一种外部的“人类符号”，而是知识在“机器大脑”中的内部直接呈现。因此，参数仅以机器可读的数值编码形式存在，无法为人类直接感知和理解。即便获取了AI模型保护第一案中的参数文件，人类也无法直接从数值中理解其含义，必须将其加载到相应的模型结构中才能发挥作用。

（二）参数的法律定性：一种新型知识财产对象

财产意味着人们对某些事物控制权的争夺，这些事物是人们所需要的，或者所渴求的，有时还是个人或集团赖以维持生存的基础。〔16〕AI模型参数为机器通过海量数据学习形成的、催动机器运行的机器知识载体，已经构成人们所需要或渴求的事物。从法律定性而言，模型参数是一种具备财产属性的对象，而且与传统的“知识财产对象”属性一致，仅是形态不同，因而应当定性为一类新型的知识财产对象。

财产对象的成立需要满足两个核心前提：价值性与可支配性。价值性是产生财产关系的物质基础，无价值之物上并不产生法律争议，也无需法律加以调整。可支配性则是财产权利实现的现实条件，价值连城却无法支配之物，就如同海市蜃楼一般遥不可及，无法在社会关系的范畴内占据一席之地。模型参数显然具备价值性。基于OpenAI的Scaling理论〔17〕以及迁移学习的应用拓展，〔18〕参数的数量及优劣程度将直接决定AI模型的最终性能，及被移植至多任务或多模型的潜在价值。正如世界AI教父辛顿（Hinton）所指出的，机器的知识迁移速度远大于人类，因为相同架构的模型能够非常容易通过分享权重而迁移它们所学到的知识。〔19〕由此可见，模型参数不仅具备有益于人类生活享用的使用价值，〔20〕亦存在可交换的他用价值。〔21〕模型参数同样满

〔16〕 参见〔澳〕彼得·德霍斯：《知识财产法哲学》，周林译，商务印书馆2017年版，第17页。

〔17〕 See Jared Kaplan et al., *Scaling Laws for Neural Language Models*, ArXiv (23 January 2020), https://doi.org/10.48550/arXiv.2001.08361, visited on 7 January 2026.

〔18〕 See Santisudha Panigrahi, Anuja Nanda & Tripti Swarnkar, *A Survey on Transfer Learning*, 1 Intelligent and Cloud Computing: Proceedings of ICICC 781 (2020).

〔19〕 参见深智联融媒：《诺奖得主辛顿教授WAIC 2025重磅演讲：数字智能是否会取代生物智能?》，载微信公众号“深智联融媒”2025年9月13日。

〔20〕 参见〔英〕约翰·洛克：《论降低利息和提高货币价值的后果》，徐式谷译，商务印书馆2017年版，第40页。

〔21〕 参见〔德〕马克思：《资本论》（第一卷），中共中央马克思恩格斯列宁斯大林著作编译局译，人民出版社2004年版，第49页。

足可支配性要求。在人类世界中，我们之所以从未将人脑中的神经元和突触视为事实意义上的财产，在于它们虽然具有潜在价值，却无法被独立支配。〔22〕然而，当知识载体从“人脑神经元突触”转向“机器参数”时，其物理形态发生了根本转变。参数以可序列化的数值文件形式存在，在技术上具备独立存储、复制、转移与交易的能力，〔23〕使其从机器的“内在状态”转变为可被外部控制的“法律物”，从而在事实层面满足了法律所要求的“可支配性”要件。

参数具有知识财产对象的典型特征，即非物质的形式特征与知识载体的内在属性。与有体物不同，参数本质是一系列表征模型知识的数字编码，不具有物理意义上的物质形态。因此，参数的利用方式也表现出典型的非物质性，其既无法以物理形式进行占有或控制，且可无限次、快速而低成本地进行使用，〔24〕其与知识财产对象都存在盗用成本极低、传播迅速、使用不具有消耗性，且具有极高的隐蔽性等保护困境。〔25〕从内在属性来看，传统知识产权理论中的“知识说”将知识产权对象定义为以“形式、结果、符号系统”等为存在方式的知识。〔26〕受限于早期的技术发展，知识曾被狭隘地限定为人类文明成果的集合。〔27〕但随着 AI 时代的来临，法律语境下的“知识”应回归其更为本质的功能性定义，即知识预先决定了行为主体在特定条件下的行为方式。〔28〕在此视角下，参数与传统知识产权对象均是对“行为主体如何行为”这一知识的固化载体，参数承载着机器在特定输入条件下如何进行有效输出的知识，正如商标承载着消费者快速识别、建立信赖并作出购买决策的知识。

财产体系的建构规律正是以财产形态为依据，通过“财产形态—行为方式—规范设计”进行具有法律意义的归类。〔29〕如果参数仅仅具备上述知识财产对象的属性，将其纳入现有知识财产类型（如作品、专利、商业秘密）即可。〔30〕然而，参数体现出根本区别于传统知识产权对象的独特形态——非人类符号性，从而引发了行为方式的转换，使得既有知识财产规则无法有效调整相关法律关系。既有的知识财产对象体系，无不内嵌着一种“人类符号”中心主义，即人为创设的、具有指代功能的信号。然而，参数并非对知识的外部“符号化表达”（如源代码之于算法思想），而是经过大量学习后形成的知识最终载体本身，其更接近于人类大脑中经过学习后形成的“神经元突触”。这一特性导致了知识迁移行为的变迁。人类受制于碳基生命的物理局限，无法直接复制大脑中的知识载体（如通过复制爱因斯坦的神经元突触获得其全部知识），知识的代际传

〔22〕 随着脑机接口等技术的提升，其可支配性或将不再成为障碍。

〔23〕 参见极客教程：《正确提取学习的参数》，载极客教程，https://geek-docs.com/pytorch/pytorch-questions/255_pytorch_pytorch_extract_learned_weights_correctly.html，2026 年 1 月 7 日访问。

〔24〕 参见来小鹏、贺文奕：《数据财产权益知识产权法保护的难题与对策》，载《中国市场监管研究》2022 年第 7 期，第 41－45 页。

〔25〕 See Nicholas Carlini et al., *Stealing Part of a Production Language Model*, arXiv (23 January 2020), https://doi.org/10.48550/arXiv.2001.08361, visited on 7 January 2026.

〔26〕 参见刘春田主编：《知识产权法》（第 5 版），高等教育出版社 2015 年版，第 9 页。

〔27〕 参见刘春田：《知识财产权解析》，载《中国社会科学》2003 年第 4 期，第 109－121、206 页。

〔28〕 参见〔英〕马克斯·H. 博伊索特：《知识资产：在信息经济中赢得竞争优势》，张群群、陈北译，上海人民出版社 2005 年版，第 14 页。

〔29〕 参见李琛：《论知识产权法的体系化》，北京大学出版社 2005 年版，第 123、126 页。

〔30〕 参见许娟：《企业衍生数据的法律保护路径》，载《法学家》2022 年第 3 期，第 72－87、193 页；陶乾、李衍泽：《论衍生数据的知识产权保护模式》，载《大连理工大学学报（社会科学版）》2023 年第 4 期，第 94－101 页。

承只能依赖于外部符号这一缓慢且有损的媒介。但在机器世界中，模型的知识载体参数，却可以被近乎零成本、无损耗地直接复制和迁移，使一个“机器大脑”的全部“知识”以较低成本和时间移转至另一个“机器大脑”。

二、参数独立财产保护的正当性与必要性

参数这类特殊的“机器知识载体”，其独特的法律定性与现有财产体系子项并不具备同一性，可以展望其独立保护意蕴，并为日后类似特质的新型机器知识载体提供参考。

（一）参数独立财产保护的正当性

财产权的有效性依然有赖于道德支撑，但需借助一系列权威规则，解决社会整体共同追求财产时所产生的矛盾和冲突，而这些规则是由有效的权威机构基于社会利益而制定的。〔31〕

1. 劳动理论：财产确立的价值来源

劳动理论所持的“劳动成果理应受到保护”的观点，符合普遍的伦理直觉，因而往往作为司法实践的裁判理由。〔32〕劳动理论为参数保护提供了最基础的道德正当性。有学者质疑，在无形的知识产品世界中，从来就不存在也不可能存在洛克意义上的“自然共有状态”。〔33〕但“共有知识”实际上是客观存在的，与站在“巨人的肩膀上看世界”一样，参数的生成依赖于海量的优质训练数据，通常为凝结人类知识的作品、技术方案等。这些前人知识构建起了抽象的“共有知识”，在人们（现延伸至机器）的互动过程中具有重要的作用。〔34〕

即便承认知识的共有属性，劳动的模糊性使得“如果将番茄汁倒入大海，整片海域是否归我所有”〔35〕等诘问始终存在。参数的生成过程并非人类简单的劳动混合，而是一种“因果支配下的培育劳动”。如同“植物新品种”的育种者通过选种、杂交、环境控制等培育劳动，实现对育种结果的支配一样，AI 开发者（如 AI 模型保护第一案中的原告）对数据处理与模型训练等方面所付出的培育劳动，促成了参数的“涌现”，构成了权利主张的正当性基础。

因“侵占公共领域”而违背“留有足够多且同样好的东西给其他人所共有”消极要件的担忧，〔36〕在参数这一对象上并不成立。法律保护的是凝结在参数中的增值劳动，而非原始数据本身。通过调控保护范围，完全可以做到在保护参数的同时，不限制他人利用原始数据去生成新的模型参数。再者言，参数是功能性的“机器知识载体”，其内部机理常为“黑箱”，本身就不是为了向人类直接传递信息，保护参数也不会限制人类思想的自由流通。

---

〔31〕 参见黎华献：《知识财产利益权利化路径之反思》，载《现代法学》2020 年第 3 期，第 85 页。

〔32〕 参见崔国斌：《知识产权法官造法批判》，载《中国法学》2006 年第 1 期，第 144－164 页。如本案中，二审法院认为模型风格设定、收集训练数据以及模型训练等过程证明抖音公司为研发该特效模型投入了大量经营资源，因而模型参数属于受到保护的竞争利益。

〔33〕 参见李扬：《再评洛克财产权劳动理论——兼与易继明博士商榷》，载《现代法学》2004 年第 1 期，第 171－177 页。

〔34〕 参见〔澳〕彼得·德霍斯：《知识财产法哲学》，周林译，商务印书馆 2017 年版，第 86 页。

〔35〕〔美〕罗伯特·诺奇克：《无政府、国家与乌托邦》，姚大志译，中国社会科学出版社 2008 年版，第 388 页。

〔36〕 参见郑金涛：《数据产品确权的体系批判》，载《知识产权》2024 年第 6 期，第 111－126 页。

2. 功利主义：基于劳动的激励机制

虽然劳动理论为参数保护提供了价值来源，但其通常难以回应“提供何种程度的保护是合适的”。功利主义以社会总福利的最大化为评判标准，回答“为何必须通过法律介入来保护参数”。当劳动者难以获得足够的市场领先时间以收回实质性投入，而导致市场失灵出现时，法律这只“看得见的手”必须介入。AI 模型参数的非物质性使得其容易因他人的低成本复制而导致市场失灵。〔37〕参数开发与参数窃取之间存在巨大的成本差异，据估算 OpenAI 的 GPT-3.5 训练成本为 851 万美元，〔38〕且不论所耗费的人力和时间成本，不到 2000 美元的成本就可以盗取完整的 GPT-3.5-turbo 模型参数矩阵。〔39〕若无相应的财产保护，理性的市场主体可预见，任何巨额的前期投入都可能为他人作嫁衣，从而丧失投入资金进行前沿模型参数开发的动力。明确的财产边界可使开发者能够预期合理的投资回报、有效减少后续流通的交易成本，形成正向的劳动激励，从而愿意承担高风险、高投入的参数研发。这正是功利主义视角下法律干预的核心理由，通过产权配置纠正市场失灵，实现社会总福利的最大化。

3. 工具主义：利益平衡的实现

工具主义认为，财产虽以前述“道德价值”为前提，但本质为实现特定社会目标、服务于道德价值而被设计出来的制度工具，其核心功能在于追问一项财产的设定能否有效平衡冲突的利益。〔40〕工具主义所进一步回答的“如何通过财产制度设计实现多元利益的动态平衡”，为参数保护提供了制度功能层面的正当性。参数的财产确认是在“公共安全”与“私人利益”之间寻找关键平衡点的必然选择。出于对安全风险和“黑箱”决策的深切忧虑，社会公众和监管机构要求模型透明的呼声高涨，希望通过审查模型参数来窥探 AI 的“心智”，确保其行为符合人类的伦理和安全底线。然而，模型参数是开发者投入巨额资本、算力和智力劳动凝结而成的核心资产，存在一批企业希望以商业秘密形式维持技术的“护城河”。〔41〕这种“公共监管的审查需求”与“核心资产的保密需求”之间的冲突，使得模型参数的财产地位确认变得异常紧迫。若完全倾向于公共审查而忽视其财产价值，则将严重打击创新投入的积极性；若认可参数主体的“保密”需求，又难以满足社会对透明度的安全诉求。将参数明确为财产对象，并非单纯地为了保护私有利益，而是构建一个法律框架，用以衡量、调和并平衡这对核心冲突。它承认私有利益的价值，同时为公共利益的介入（如强制披露、安全审查）提供了合法依据和程序保障，这与医药领域的专利公开与链接制度在逻辑上异曲同工，都是通过财产设计来实现利益平衡的制度典范。

当然，亦有观点从利益平衡的另一端提出警示，认为赋予参数财产保护将加剧市场垄断，特

〔37〕 参见刘维：《论数据产品的权利配置》，载《中外法学》2023 年第 6 期，第 1581－1599 页。

〔38〕 See Nestor Maslej et al., *Artificial Intelligence Index Report 2025*, Stanford Institute for Human-Centered Artificial Intelligence (April 2025), https://hai.stanford.edu/ai-index/2025-ai-index-report, visited on 7 January 2026.

〔39〕 See Nicholas Carlini et al., *Stealing Part of a Production Language Model*, arXiv (23 January 2020), https://doi.org/10.48550/arXiv.2001.08361, visited on 7 January 2026.

〔40〕 参见〔澳〕彼得·德霍斯：《知识财产法哲学》，周林译，商务印书馆 2017 年版，第 294 页。

〔41〕 See Dylan Patel & Afzal Ahmad, *Google 'We Have No Moat, And Neither Does OpenAI'*, Semianalysis (4 May 2023), https://semianalysis.com/2023/05/04/google-we-have-no-moat-and-neither/, visited on 7 January 2026.

别是享有数据和算力优势的科技巨头，最终损害社会整体福利。〔42〕这种担忧可能低估了当前 AI 生态的内在平衡机制。首先，与依赖封闭个人数据的传统产品不同，当前大模型的训练已转向作品等开放性语料，其价值创造模式削弱了“数据垄断”的基础，保护参数并不妨碍他人利用同样的数据集进行训练。其次，合成数据的兴起，〔43〕允许开发者通过现有模型生成训练数据，从源头上削弱了数据壁垒。最后，成熟的开源生态已极大降低了知识迁移的成本，中小开发者可通过在开源模型上微调来参与竞争，这本身就构成了对巨头垄断的强大制衡。〔44〕因此，对模型参数给予财产保护，并非必然导致垄断。相反，它是在承认其财产属性的基础上，将“公共审查”与“私有激励”从零和博弈的困境中解放出来，为复杂的利益冲突提供了一个可调节、可平衡的制度平台，从而实现技术创新与社会安全的动态平衡。

（二）参数独立财产保护的必要性

前文从劳动理论、功利主义和工具主义三个维度，对参数是否应当受到保护展开了论证。在此基础上，仍需从必要性视角，剖析参数应如何进行保护。通过梳理既有保护框架的局限性可知，参数亟须获得独立的法律保护，而非仅依靠兜底条款进行个案化裁量。

1. 算法和原始数据保护的激励失效

传统数据加工始终在人类可理解的信息形式中运作，遵循线性、可预见的处理逻辑，而 AI 模型参数的生成是一次信息形式的“跨物种”转换，故而参数训练被业内类比为高成本、高风险与不可控的“炼丹”过程。〔45〕同样的数据和算法可能因训练过程的随机性催生出性能迥异的参数配置。因此，参数的价值核心在于训练过程中“涌现”的知识，这一知识无法从数据或算法的保护中自然推导获得，对原始数据和算法的保护，难以激励参数的创新。

2. 技术措施的封闭化风险

在模型领域，技术措施的过度依赖将演化为“丛林规则”下的消耗战，〔46〕严重损害社会长远发展的总福利。况且，技术措施的保密将显著降低参数的流动性，巨头公司会倾向于选择封闭的模式控制模型参数的“接触”。〔47〕这种趋势有违 AI 商业实践中所广泛流行的开源参数生态。〔48〕若产权缺位，开源将成为无源之水，开发者会倾向于采取更严格的技术保密措施，反而会阻碍已经形成的知识共享生态，提升整个社会的创新成本。

3. 合同机制的相对性与无效风险

在参数领域，因合同的相对性效力以及无效可能性，合同的配套形式亦将面临困难。截至目

〔42〕 参见胡开忠：《数据知识产权赋权理论之质疑》，载《法学》2025 年第 10 期，第 114－131 页。

〔43〕 参见程学旗、陈薇：《人工智能合成数据》，载《中国科学基金》2022 年第 3 期，第 442－446 页。

〔44〕 See Creative Commons, *Supporting Open Source and Open Science in the EU AI Act*, Creativecommons (26 July 2023), https://creativecommons.org/2023/07/26/supporting-open-source-and-open-science-in-the-eu-ai-act/, visited on 7 January 2026.

〔45〕 参见格物智：《训练模型为什么叫“炼丹”?》，载微信公众号“上海浦东新区格物科创金融研究院”2024 年 7 月 11 日。

〔46〕 参见崔国斌：《网络反爬虫措施的法律定性》，载《中国法律评论》2023 年第 6 期，第 157－174 页。

〔47〕 参见参胡凌：《商业模式视角下的“信息/数据”产权》，载《上海大学学报（社会科学版）》2017 年第 6 期，第 12 页。

〔48〕 2023 年全球共计发布了 149 个基础模型，更是有 65.7%是以开源形式开放，这些开源模型都至少开放了模型参数。See Nestor Maslej et al., *Artificial Intelligence Index Report 2024*, Stanford Institute for Human-Centered Artificial Intelligence (April 2024), https://hai.stanford.edu/ai-index/2024-ai-index-report, visited on 7 January 2026.

前，仅我国通义千问开源模型全球下载量便突破 6 亿次，衍生模型超 17 万个。〔49〕面对数量如此巨大的参数使用和微调用户，合同的相对性所发挥的监督效力较差，难以直接控制第三人。况且，这些协议的效力也可能因知识产权的公共政策而陷入无效。〔50〕总而言之，明确的财产定位是市场交易的前提。基于此，围绕参数的许可、转让、联合开发等商业模式得以建立，从而形成健康的 AI 技术交易市场。

4. 既有知识产权的逻辑错配

参数的“非人类符号性”难以满足著作权的作者和表达要求。由于参数并非人类符号，人类不知其编译逻辑，故模型的内部工作机制也以“黑匣子”著称。〔51〕对这类非人类符号，其既不属于作品意义上的表达，人类也无法存在作者意义上的独创空间。或许有人会辩称，开发者或使用者对于数据的选择、标注输入以及监控干预等行为或许可以算得上作者的创作行为。但这些行为可等同于为了获得苹果丢入红色蜡笔，虽从方向来看是必要的，但参数的具体生成仍然不可控，难以认定为创作行为。

也有观点提出，专利法或可为包含这些参数的技术方案提供一定保护。〔52〕然而，参数因其非技术方案以及非技术手段的特征，无论作为独立还是技术方案的组成诉诸专利保护都面临诸多阻碍。参数仅仅是负责调节不同神经元作用程度的函数，既不能独立解决技术问题，也不涉及自然规律的应用，更不产生符合自然规律的技术效果。因而独立的参数无法获得专利法的保护。至于作为组成部分，参数为训练后获得的“后见之明”，而非“利用自然规律的技术手段”，无法作为技术特征进行保护，若仅作为算法设计方案的示例存在，则独立保护范围相当有限。

尽管在实践中，许多闭源模型的开发者暂时依赖商业秘密来保护其模型参数，但参数与其以“保密占有利益”为核心的逻辑〔53〕存在冲突。商业秘密所要求的保密要件实际扮演着守门人的角色，要么保密，要么公开换取保护。〔54〕既确保通过赋予法律权利的保障〔55〕来鼓励信息传播，又引导容易被公众通过产品获知的发明〔56〕进入专利或著作权体系。但 AI 模型所催生的以“开源”为核心的全新商业生态模式，以及社会对模型透明度的监管需求，与商业秘密的“保密性”前提相悖，而专利、著作权制度又因适格性障碍无法介入。传统“守门人”提供的路径，在此都走不通。此外，商业秘密制度预留的“反向工程”豁免窗口，是“人类符号”时代下的平衡机

〔49〕 参见阿里云：《今天，世界互联网大会给我们颁了一个奖！》，载微信公众号“阿里云”2025 年 11 月 6 日。

〔50〕 See Peter Henderson & Mark A. Lemley, *The Mirage of Artificial Intelligence Terms of Use Restrictions*, arXiv (10 December 2024), https://doi.org/10.48550/arXiv.2412.07066, visited on 7 January 2026.

〔51〕 See Zachary C. Lipton, *The Mythos of Model Interpretability*, 61 Communications of the ACM 36 (2018).

〔52〕 See Peter R. Slowinski, *Rethinking Software Protection*, in Jyh-An Lee, Reto Hilty & Kung-Chung Liu eds., Artificial Intelligence and Intellectual Property, Oxford, 2021, pp. 341 - 362.

〔53〕 参见黄武双：《商业秘密保护的合理边界研究》，法律出版社 2018 年版，第 13 页。

〔54〕 See Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 Stanford Law Review 311, 338 (2008).

〔55〕 法律保护可以弥补排他性天生不足的困境，从而减少企业对于保密措施的投入，进而鼓励公开；另一方面，也可以在交易时提供公开的保护环境。

〔56〕 主要包括自我披露型发明以及可以通过反向工程破解的发明。

制。但模型参数的反向工程技术成本极低，且自动化程度高，这使得豁免规则所预设的“付出相当努力”前提不复存在。在AI模型保护第一案中，原告的模型参数“随抖音APP发放至用户终端在本地运行”便面临商业秘密救济不能的困境，一方面，其可能因直接部署于用户终端而难以满足保密性要求。另一方面，即使其落入商业秘密保护范围，被告“通过技术手段提取模型本身并进行解密”的行为也很可能落入“通过技术手段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息”的反向工程豁免范畴。

5.“互联网专条”的场景局限与目的错位

《反不正当竞争法》第12条“互联网专条”常被用于数据相关权益的保护，但参数的应用场景却并不限于互联网环境，还包括各类离线的AI系统。AI模型保护第一案中所涉及的漫画特效模型，便是部署在用户端侧提供服务的离线模型。另一方面，该条款的核心规制目的与参数的保护诉求并不符合，该条款旨在维护互联网的竞争秩序，而模型参数的保护诉求在于保障其流通价值。因此，互联网专条亦难以为参数提供全面、有效的法律保护。

6. 兜底条款保护的权宜性与不足

当专门财产体系无法为新型财产对象提供有效保护，司法实践总会诉诸兜底条款，但这并非长久之策：其一，裁判标准的高度不确定。这种个案化的裁判模式，依赖法官对“不正当性”的临时裁量，可能导致保护标准高度不确定。〔57〕这种不确定不仅体现为保护得不充分，还可能表现为保护得过度。如该案判决便体现出“竞争优势利益”存在即推导“行为不正当”的倾向，论证往往显得草率而循环。其既未充分论证为何未经授权使用他人参数即违反商业道德，亦未对模型参数与原始数据的关系进行充分论证。更为重要的是，被告是否窃取参数这一事实问题仍存在疑问，曾有技术观点指出，被告可能是通过模型输出进行知识蒸馏，才实现模型效果的“抄袭”。〔58〕真若如此，法院对于兜底条款的适用便已超越了参数的保护边界。

其二，构成要件的证明困难。兜底条款的适用须遵循“竞争优势利益存在、行为不正当性、损害合法权益以及存在竞争关系”的论证路径，但对于参数的多样市场行为，“损害合法权益”以及“竞争关系”的证明存在困难。如果行为人只是复制了部分参数，并在自己的大模型中进行了微调，或者将其应用于一个完全不相关的领域，这是否还构成“实质性替代”的损害后果？若行为主体与参数所有人之间不存在直接竞争关系，学术研究机构出于非商业目的的复制与公开、技术媒体的意外泄露、黑客的纯粹破解炫技行为是否可获得该条款的保护？以Meta开源模型参数的泄露事件为例，Meta原本仅针对非营利机构的“学术申请”有限开放参数，〔59〕但这个“受控发布”的计划在不到一周内就因匿名技术人员泄露参数而宣告失效。〔60〕

其三，反不正当竞争法难以为参数这类机器知识载体配置相应的保护限制规则。传统知识产权法在赋予权利的同时，都精心设计了相应的保护限制规则，以平衡私人激励与社会公共利益，

〔57〕 See Richard A. Posner, *Misappropriation: A Dirge*, 40 Houston Law Review 638 (2003).

〔58〕 参见一川Law：《闲话AI丨第23期：AI模型结构、参数侵权首案疑云》，载微信公众号“一川Law”2025年6月3日。

〔59〕 这种有限开放的开源形式，因开放对象不特定，难以符合商业秘密的秘密性和保密性要求。可参见类似的开源数据案例，例如北京知识产权法院（2024）京73民终546号民事判决书。

〔60〕 SeeTheodore McKenzie, *Meta's AI Language Model LLaMA Gets Leaked*, 80LV (6 March 2023), https://80.lv/articles/meta-s-ai-language-model-llama-gets-leaked/, visited on 7 January 2026.

如时间期限的限制、合理使用的豁免等。《反不正当竞争法》兜底条款作为一般性条款，缺乏这种保护限制机制的设计空间，反而可能会为参数提供“无限期”“无限制”的超额保护，而忽视科研创新、市场竞争、公众讨论以及安全审查等公共利益的需要。

其四，频繁动用兜底条款往往将引发实证主义法律观的质疑。受制于财产体系已然建成的横向关系，常有观点认为，新型对象如果因不满足专门法的保护要件而无法获得保护，就不应通过兜底条款获得保护。这不仅符合立法者有意为知识财产设置的微妙平衡格局，〔61〕亦是“禁止冗余规则”、〔62〕维护法律体系内在和谐、防止一般法架空专门法的重要体现。〔63〕通过上文分析可知，以“人类符号”为核心的专门法从未意图“吸收”或“评价”参数这一“机器知识载体”，因此其“沉默”并非“有意拒绝”，而是“立法空白”。

综上，法院暂时依赖兜底条款提供保护仅是权宜之计。〔64〕从长远角度来看，正视模型参数作为一种高度类型化的新型知识财产对象的客观现实，以特殊立法为代表的知识财产独立保护应为更合理的选择。

三、参数独立财产保护的排他权路径

当财产体系面对技术变革所催生的新型对象时，如何以自然、严谨且平和的方式将其纳入法治框架，始终是立法者与司法者共同面临的难题。〔65〕在确定参数这类新型对象具备财产保护正当性，以及独立保护的必要性后，如何设置其独立保护路径将成为重中之重。财产对象的定性可为财产权益的设置起到模块化的作用，从而节约信息成本。〔66〕作为一种新型的知识财产对象，参数的保护路径探索可借鉴知识财产的模块设计，以特殊立法为代表进行独立保护。

（一）参数的排他权配置

财产是一个人所拥有的经济价值意义上的利益与权利的总称，只要它们具有货币上的价值。〔67〕讨论参数这类新型对象的财产保护问题，不可避免地会涉及“权利”与“利益”路径的选择。但随着财产权理论的演进，以“排他”为核心的知识财产保护使得权利与利益保护的效果差异愈发模糊。由于有形物具有对象边界清晰以及稀缺性的天然特征，正面利益的归属效能与排他效能之间的对应关系十分直观，是以所有权立法中法律不必规定苹果的所有权人可将苹果吃掉、做苹果饼或榨成果汁，〔68〕而与参数性质类似的知识产权却往往需要列举具体行为以框定权利的保护范围。因此，于这类无形财产而言，财产权利或利益的设置，其最终目的和实现方

〔61〕 参见何炼红：《知识产权的重叠保护问题》，载《法学研究》2007 年第 3 期，第 64－67 页。

〔62〕 参见宋建宝：《人工智能模型结构与参数的知识产权保护》，载微信公众号“知产观察家”2025 年 10 月 30 日。

〔63〕 参见于飞：《〈民法典〉公序良俗概括条款司法适用的谦抑性》，载《中国法律评论》2022 年第 4 期，第 52－61 页。

〔64〕 See Annette Kur, *What to Protect, and How? Unfair Competition, Intellectual Property, or Protection Sui Generis*, in Nari Lee et al. eds., Intellectual Property, Unfair Competition and Publicity: Convergences and Development, Edward Elgar, 2014, pp. 11－32.

〔65〕 参见黎华献：《知识财产利益权利化路径之反思》，载《现代法学》2020 年第 3 期，第 85 页。

〔66〕 See Henry E. Smith, *Property as the Law of Things*, 125 Harvard Law Review 1691 (2012).

〔67〕 参见〔德〕卡尔·拉伦茨：《德国民法通论》（下册），王晓晔等译，法律出版社 2003 年版，第 1006 页。

〔68〕 参见李琛：《论知识产权法的体系化》，北京大学出版社 2005 版，第 74 页。

式，都是对他人行为的规制。目前参数的保护困境也体现为诸如开源等参数开放或交易的流通过程中无法获得足够的排他保护，以及缺乏合理的利益平衡机制。基于上述认识，本文主张超越“权利”与“利益”的机械划分，将参数直接作为一种新型财产对象予以承认，并为其配置一套弹性的、模块化的排他权保护规则，以行为规制为中心来构建其排他权的归属、保护范围和限制。

本文主张采取“单独立法＋民法典衔接”的模式进行制度设计。具体而言，类似集成电路布图设计、植物新品种等特殊知识财产对象，为参数等机器知识载体制定专门的单独立法，并与《民法典》第123条知识产权条款（即“法律规定的其他客体”）相衔接。首先，诸如参数这类机器知识载体将成为不断扩展的对象类别，随着AI代理、空间智能〔69〕的发展，机器之间的知识迁移载体会越来越多，除模型参数外，还包括模型的内部输出（如中间层特征表示〔70〕）、外部输出（如含思维链〔71〕的生成内容、合成数据）等。其次，参数等机器知识载体具有不同于传统知识产权客体的特殊性——它们是非“人类符号”，其生成、传播、使用和目的都具有独特性。单独立法可以有针对性地设计权利归属规则、保护范围、限制与例外等，避免削足适履地套用现有制度。最后，通过《民法典》“其他客体”条款衔接，既保持了知识产权体系的开放性，又维护了既有知识产权以“人类符号”为中心的内部稳定性。

（二）参数排他权的归属

参数的生成过程涉及多方主体的贡献，主要包括训练数据提供者（参数生成所使用数据集的权利人或提供者）、算法提供者（训练算法或参数迁移方法的设计者或权利人）、模型本身（训练过程中自主学习数据特征、调整参数配置的人工智能系统）以及参数开发者（实际组织和执行参数训练、迁移过程的主体）。本文认为，应当首先排除机器本身的主体资格，其次基于“参数知识价值的决定性贡献”原则，确立参数开发者为权利归属主体。

1. 参数开发者应当成为参数排他权的归属主体

首先应当明确的一点是，机器本身不应也不能成为参数排他权的归属主体。其一，法律本身就是调节人与人之间关系的规范体系。参数这类新型财产所引发的，仍是人类之间就这些具有价值的机器知识载体的控制权争夺。机器作为法律主体、成为争夺知识载体利益方的时代尚未到来。其二，参数作为财产对象的价值之源，在于人类投入的劳动成本，所要配置的激励机制以及实现的利益平衡，亦发生于人类关系之间。机器在此过程中仅是工具，而非劳动的付出者或利益的享有者。明确参数排他权归属，本质在于理清符合正当性论述的利益由谁起到决定力，以及对谁的劳动进行激励和利益平衡。参数的价值在于驱动模型在特定情况下作出决策的知识能力，其来源于开发者所投入的数据清洗、模型训练等算力和人力成本，因此对参数的知识能力价值做出决定性贡献的开发者应当成为参数排他权的归属主体。

对于训练数据提供者而言，原始数据虽是参数生成的“原材料”，但参数的价值源于训练过

〔69〕 See Fei-Fei Li, *From Words to Worlds: Spatial Intelligence is AI's Next Frontier*, Substack (10 November 2025), https://drfeifei.substack.com/p/from-words-to-worlds-spatial-intelligence, visited on 7 January 2026.

〔70〕 中间层特征表示是指神经网络隐藏层在处理输入数据时生成的中间状态，编码了从低级特征到高级语义的层次化知识。

〔71〕 思维链（chain-of-thought，CoT）是大语言模型输出用以展示逐步推理过程的表达。

程对数据中隐含知识的提炼、抽象与重构，数据提供者不应享有参数权利。在以人类数据（如文本、图像等）为蓝本的训练或微调过程中，参数既不“复制”原始数据的表达，〔72〕也不进行“汇编”，仅从海量数据中学习、抽象并归纳出语义关联和模式特征，最终以非人类符号的形式呈现，具有独立于原始数据的功能价值。对于算法提供者而言，算法设计者虽然设计了模型架构和训练方法，但其劳动成果已经通过专利权或商业秘密得到充分保护。特别是，算法虽影响参数的生成质量，但并非参数增量价值的决定性因素。参数的生成是多重因素下的加工产物，需要耗费大量的人力、算力和资金，并非算法与数据的线性结果。即使使用同一套算法和数据，其训练的参数也可能因训练策略、初始化方式、训练轮次等因素而存在显著差异。

综上，参数的增量价值主要源于开发者的实质性劳动，包括数据的筛选、清洗与预处理，训练策略的设计与优化，算力资源的投入等。这些劳动使参数从“可能性”转化为“现实性”，从原材料和工具转化为具有独立功能价值的知识财产对象。因此，参数开发者应当成为参数排他权的归属主体。

2. 两种典型参数生成范式下的权利归属

在确立“开发者享有参数排他权”的基本原则后，需要进一步明确两种主流参数生成范式下，如何具体界定“开发者”及其权利范围。两种范式包括通过训练将人类符号形式数据转化为高维度的、非人类可读的内部机器知识载体，以及基于已有的模型参数，通过迁移学习等技术，将既有的机器知识扩展至新的领域或任务。在第一种范式中，由于仅存在唯一的以原始数据训练模型的开发者，参数的排他权完整地归属于开发者。这也能解释，为何 AI 模型保护第一案中被告所提出的“训练合法性”抗辩无法成立。参数的价值源于开发者的训练投入，而非数据本身的价值延伸。即使训练数据的使用存在合法性瑕疵（如未经授权使用他人数据），这也仅导致开发者可能就其训练行为承担侵权责任，但不影响参数本身作为独立知识财产对象的可保护性，也不影响开发者对参数享有的排他权。

在第二种范式中，虽然新参数系从既有模型参数调整而来，但若新开发者运用复杂的技术手段对原参数进行了实质性的调整、重组与优化（如参数微调、〔73〕参数剪枝〔74〕等），新开发者应享有增量部分的排他权。此时的权利归属类似于著作权法中“原作品”与“演绎作品”之间的关系。AI 模型保护第一案同样涉及类似争议，“原告模型源于开源模型”的抗辩核心并不在于开源模型采用何种著作权许可，而是，即使原告的参数源于开源模型，只要原告通过微调、迁移等技术手段为参数赋予了新的、可验证的知识能力，这部分增量价值就应当获得法律保护，并归属于原告。在该案中，原告的变身漫画特效模型与最早的开源模型存在较大差异，其在“漫画特效”

〔72〕 美国版权局曾在报告中提出一个激进观点，即模型的“权重”本身可能构成对原始作品的侵权复制，因某些数字文件虽然以数学方式编码或压缩内容，肉眼无法直接感知其中信息，但其本质上仍是对原始内容的复制。See United States Copyright Office, *Copyright and Artificial Intelligence*, *Part 3: Generative AI Training Pre-Publication Version*, United States Copyright Office (May 2025), https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf, visited on 7 January 2026. 不过，这一认知有违技术原理，权重并非按照某一可逆的“数据重编码”进行，而是从海量数据中学习、抽象并归纳出语义关联和数据特征，并以非人类符号呈现。因此，模型权重是训练投入所产生的、具有独立功能价值的“机器知识产品”，而非训练数据的“副本”。

〔73〕 参数微调（fine-tuning）指在既有参数的基础上，使用新的数据集进行继续训练，调整部分或全部参数值。

〔74〕 参数剪枝（pruning）指删除冗余参数，压缩模型规模。

这一垂直领域所表现的优越性足以证明其产生了增量价值。因此，开源来源不构成否定参数可保护性的理由，新开发者对其创造的增量价值享有独立的排他权。

（三）参数排他权的内容

1. 排他权边界的厘清：参数的知识迁移行为

排他权应仅限于对参数的知识迁移行为，而不应扩展至其他机器知识载体的知识迁移行为。形象而言，机器之间的知识迁移可简单分为两类。第一类为对参数的复制和迁移，可类比理解为直接复制爱因斯坦的大脑。第二类为通过模型的内外部输出进行知识迁移，也即最近引发广大争议的“知识蒸馏”技术，如同通过脑机接口读取电流信号、阅读知识浓度很高的外部符号，以理解和学习方式来吸收知识。这两种知识迁移行为针对的并非同一“物”，相互间具有本质的独立性区别。参数排他权应当仅涉及第一类行为，即对参数这一机器知识载体本身的直接获取和使用。以 AI 模型保护第一案为例，若所涉行为并非“从软件中破解提取、复制参数”，而是“大量收集该模型的输出用以训练己方模型”，则该行为不应纳入参数排他权的保护范围，其属于第二类知识迁移行为，应在其他类型机器知识载体的保护范畴下予以判定。

2. 排他权的核心：参数的获取与使用行为

人类符号下知识的迁移遵循“编码－传播－解码”的三段论：抽象的知识需以信息形式被编码为外部符号，这些符号传播，最终，接收者通过解码过程，将外部符号内化为大脑中的知识。由于这些过程需要成本，且出于“促进全人类的知识福祉”等公共利益，知识产权往往仅精细调控“外部符号”的传播行为，实现激励知识“编码”（创新）与保障知识“解码”（公共利益）之间的微妙平衡。因此，既有的知识财产体系多围绕“人类符号”的传播行为展开。然而，一旦获取了模型参数，行为人便可以完全跳过解码过程，通过部署类似框架模型直接获得与原模型相同或相近的知识能力。这种“获取即使用”的特性，使得对获取行为本身的控制成为保护参数价值的关键。法律调控的对象不再是外部符号的传播行为，而是对大脑内知识载体本身的获取和使用行为。此外，参数的使用往往发生在“黑箱”之中，并且大部分盗用者会对模型参数进行微调或继续预训练后再应用于下游场景，这使得即使存在盗用行为，通常很难通过参数对比来识别相似性进而确认是否存在盗用行为。〔75〕因此，如果法律不对获取行为本身进行规制，仅依靠对使用行为的事后追责，将使参数排他权形同虚设。

具体而言，参数的排他权内容应包括两方面：一为未经权利人许可，通过任何技术手段获取他人模型参数的行为。包括技术措施破坏或避开型，即通过破坏或规避技术保护措施获取模型参数的行为；协议违约型，即超出授权范围获取模型参数的行为，如内部人员的泄露、超出商用目的限制等情形；反向提取型，通过对模型的合法访问，采用技术手段从模型的输出中反向推导、提取或重构模型参数的行为。如 API 攻击、向量攻击等。二是未经权利人许可，使用他人模型参数的行为。包括直接使用型，即行为人未经授权或超出授权范围，直接调用、访问他人参数，将其应用于自身的模型训练、推理或其他商业用途；加工使用型，即行为人在获取他人机器知识载

〔75〕 See Boyi Zeng et al., *Huref: Human-readable fingerprint for large language models*, 37 Advances in Neural Information Processing Systems 126332 (2024).

体后，未经许可对其进行二次开发、微调、迁移或其他技术处理，形成衍生产品并加以使用，例如，对他人的预训练模型参数进行微调后作为自有产品推出，或通过迁移技术将他人模型参数用于轻量化模型的开发；让他人使用型，即行为人将不正当获取的机器知识载体提供给第三方使用，包括转售、分发、开源或以 API 接口等形式供他人使用，例如，将盗取的模型参数上传至开源平台供公众下载，或让他人付费使用未经授权的模型参数。

3. 参数排他权的限制：时间限制与有限目的的反向工程限制

（1）以 10 年作为保护期限

知识产权保护的目标并非让权利人获取其创造的全部社会价值，而是提供“足够的激励”以覆盖其平均固定成本，包括固定成本和合理利润。〔76〕其中，美国为集成电路布图设计设定的 10 年保护期，正是基于该原则的经典实践。与集成电路布图设计类似，虽然 AI 参数的迭代周期非常短，往往仅为数月至数年（如 GPT-3 到 GPT-4、DeepSeek-V2 到 V3）。但产业应用中，企业通常不会频繁更换模型，因为模型切换涉及重新训练、测试、部署等高昂的迁移成本，旧有模型参数预计仍将会获得长达 3～7 年的稳定使用。以 GPT-3.5 为例，尽管已经发布三年，但仍是 OpenAI API 服务中使用量最大的模型之一。〔77〕在我国 AI 模型保护第一案中，涉案的变身漫画特效模型自 2020 年 6 月发布至今，仍在应用端持续使用。即使某一参数在其原始应用场景中被新版本替代，但仍可能以新版本模型的养料、轻量化部署或开源社区利用等形式继续产生商业价值。综合上述分析，参数的实际商业生命周期可划分为两个阶段：具有最高的商业价值和竞争优势的高价值期（0～3 年），以及垂直领域和特定场景中应用的稳定应用期（3～7 年）。因此，10 年的保护期限既能覆盖参数在产业应用中的完整生命周期，充分保护权利人在高价值期和稳定应用期的投资回报，实现“充分激励”的目标，又不会因过度保护而阻碍技术进步。

（2）以科研、评价和安全评估为目的的反向工程豁免

在传统技术领域，反向工程制度被法律所容许，建立在一个关键的利益平衡机制之上：高昂的“反向成本”使得反向工程者无法轻易廉价地剥夺创新者的竞争优势。对“人类符号”中知识的反向工程必然包含三个成本递进的环节：解构成本（通过拆解、测绘、分析等手段获取技术信息）、理解成本（人类专家对技术信息进行认知、消化和掌握）以及重构成本（基于理解重新设计、制造或实施）。正是这三重成本的叠加，使得反向工程的总成本通常与独立研发相当。〔78〕即便在软件领域，反编译技术使解构成本大幅降低，但著作权法和专利法的保护使得其理解和重构成本依然高昂。〔79〕这种成本结构确保了反向工程者仍需付出实质性投入，无法通过简单复制剥夺创新者的市场先机，从而维持了市场竞争的相对公平。

然而，当反向工程技术可以廉价、快速生成完全相同的复制品，以至于剥夺创新价值时，法

〔76〕 See Lemley M A, *Property, Intellectual Property, and Free Riding*, 83 Texas Law Review 1031 (2004).

〔77〕 See Sarah Wang et al., *How 100 Enterprise CIOs Are Building and Buying Gen AI in 2025*, Andreessen Horowitz (10 June 2025), https://a16z.com/ai-enterprise-2025/, visited on 7 January 2026.

〔78〕 参见崔国斌：《替代成本视角下商业秘密法的理论解构》，载《政治与法律》2025 年第 7 期，第 30 页。

〔79〕 参见张吉豫：《软件反向工程的合法性及立法建议》，载《中国法学》2013 年第 4 期，第 56 页。

律在一定期限内限制这种破坏市场的反向工程行为是具备经济合理性的，〔80〕如早期美国禁止通过船体注塑工艺进行反向工程。〔81〕在数据的商业秘密保护领域，也存在类似实践。近期，淘宝“生意参谋”不正当竞争案中，涉及一种“指数一键还原”的插件功能，通过对“生意参谋”数据产品的逆向推演，可以极低成本还原出接近真实的非公开经营数据。法院最终认定这种获取方式属于侵犯商业秘密的“不正当手段”。〔82〕其行为不正当的本质，在于此种反向工程〔83〕通过机器手段，以近乎零的成本实现了信息的反向，从而导致市场的破坏性后果。于模型参数而言，这种市场破坏性将更为严重。反向参数的目的不是为了让人类学习，而是为了让另一台机器“模仿其智能能力”，且反向的参数，本身就是最终的、可直接部署的“产品”。与此同时，专利和著作权法无法直接保护参数。因此，这种成本的降维打击，将导致参数的反向工程会对市场造成极大的破坏性后果。〔84〕如果允许对参数的自由反向工程，权利人将难以通过商业秘密保护回收训练成本，必然导致投资激励减损、技术封闭加剧、市场效率降低以及创新动力削弱。

据此，针对市场中出现的反向 AI 模型参数的行为，应采用“原则禁止，科研、评价与安全评估目的例外豁免”的原则。例外割免的价值在于：其一，符合科学研究和创新的需求。学术机构和研究人员需要通过对模型参数的深入分析，探索神经网络的表征学习、知识存储、泛化能力等基础科学问题。如果完全禁止对参数的反向工程，将严重阻碍 AI 基础研究的进展，不利于整个领域的长远发展。其二，保障模型性能评价的客观性。随着 AI 模型在各领域的广泛应用，独立的研究机构和评测组织需要通过对模型的深入分析（包括必要时的参数检查），验证模型的实际性能、适用范围和局限性，为用户选择和监管决策提供可靠依据。其三，契合安全评估的公共利益诉求。国际社会和各国监管机构日益强调 AI 系统的透明度和可解释性，为有效识别和消除 AI 模型所存在的风险，应允许监管机构、安全研究人员和公益组织对模型参数的深度测试和评估。

四、结　语

体系化的任何形式都是后来的产物。原始的“法”不知体系化为何物。〔85〕这些今天看来极为粗糙的体系化尝试，提醒着我们体系化的过程性。〔86〕每一次技术变革都在叩问知识财产既有

〔80〕 See Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale Law Journal 1575 (2001).

〔81〕 See Paul Heald, *Federal Intellectual Property Law and the Economics of Preemption*, 76 Iowa Law Review 959 (1990).

〔82〕 参见江苏省南京市中级人民法院（2023）苏 01 民初 4082 号民事判决书。

〔83〕 虽然该案未针对涉案行为是否构成反向工程进行深入讨论，但“指数一件还原”插件系针对合法来源下的“生意参谋”数据产品，进行反向破解和推演，从而还原出与原数据高度近似的“替代原数据”。综上，将涉案行为视为反向工程并无不妥。

〔84〕 See Carlini N. et al., *Stealing Part of a Production Language Model*, arXiv (23 January 2020), https://doi.org/10.48550/arXiv.2001.08361, visited on 7 January 2026.

〔85〕 参见〔德〕马克斯·韦伯：《经济与社会（下卷）》，林荣远译，商务印书馆 1998 年版，第 16 页。

〔86〕 参见李琛：《论知识产权法的体系化》，北京大学出版社 2005 年版，第 123、126 页。

体系的边界与容量，并在二者之间重新取得平衡。〔87〕新型对象的财产定位，关涉财产体系的进化能力。模型参数作为“机器知识载体”，以其“非人类符号性”对传统知识财产范式构成了深刻挑战。随着 AI 代理等自动化技术的发展，更多机器知识载体形式的复杂利益将不断涌入法律场域。参数独立保护，正是为承接这些新型利益关系而进行的示范性尝试。知识财产体系如何容纳这些复杂的利益形态，如何在激励创新与促进流通之间建立新的平衡机制，是摆在我们面前无法回避的时代命题。本文对于参数保护的探索仅是这一宏大命题的起点，财产体系能否保持开放性与进化能力，将决定知识财产法能否在技术变革的浪潮中继续发挥其应有功能。

Abstract：Parameters constitute a “machine knowledge carrier” formed by model development enterprises through substantial resource investment and machine training. Due to their characteristics of value, controllability, intangibility, knowledge carriers and non-human symbolic nature, they represent a new type of intellectual property object. The cultivation labor invested by developers serves as the source of parameters' value. To prevent market failure, an incentive mechanism of property protection should be allocated to parameters, thereby achieving institutional balance between public safety and private interests. Existing protection frameworks cannot adequately accommodate parameters, urgently requiring an independent property protection path. By drawing on the institutional design of intellectual property modules, a set of exclusive rights protection rules can be configured for parameters. The exclusive rights to parameters should be attributed to developers who make decisive contributions to the incremental value of “machine knowledge.” The protection boundary should be limited to knowledge transfer behaviors that directly target parameters as objects, including acquisition and use behaviors. To balance multiple public interests such as innovation and safety, parameter exclusive rights should be subject to a 10-year time limitation and exemption clauses for reverse engineering “for research, evaluation, and safety assessment purposes only”.

Key Words：model parameters, machine knowledge carrier, novel intellectual property objects, exclusive rights protection, artificial intelligence

（责任编辑：张金平）

〔87〕 参见乔磊、陈凡：《科技进步与知识产权变迁》，载《科学学研究》2011 年第 3 期，第 338－339 页。