汉坤法律评述
2023 年 7 月 6 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡

生成式人工智能 — 开源的力量和挑战（一）：AI 模型

作者：段志超 | 鲁学振 | 迟嘉宁 | 梁杰

序言

生成式人工智能的诞生、发展和应用和开源密不可分。开源打破了技术壁垒，促进了分散资源和算力的整合，为 AIGC 的发展提供了助力。没有开源的力量，生成式人工智能不会以如此迅猛的速度发展到现在的高度。

另一方面，许多人工智能公司采用闭源而非开源的方式来运营产品（如 AI 模型），这也给习惯于使用开源组件的开发者们带来了一定的挑战。本文将以基于 LLaMA 模型开发 AI 产品为例，聚焦于 AI 产品开发过程中最为核心的模型代码及参数，以期为模型开发者和使用者提供相关指引。

目次

一、行业背景：AI 开发过程简介

生成式人工智能（Generative AI）是一种基于机器学习的人工智能技术，它可以根据输入数据生成新的、符合逻辑的输出数据。生成式人工智能的开发过程主要包括：模型选择、数据准备、模型训练、模型评估、模型优化、部署应用、模型更新等[1]。

[1] 参见 WBOLT — 大型语言模型训练浅析，https://www.wbolt.com/large-language-model-training.html。

下图简要说明了中间层及应用层[2]AI 产品的开发过程。首先，开发者选择适于自身需求的公开模型（如 LLaMA、ChatGLM，下图中表示为“**语言模型**”），获得了模型代码（Model Source Code）和模型参数（Model Parameter）之后，需要根据具体应用场景调整模型参数，以使其能生成适当的回答。参数的初始值一般来源于公开模型的开发者，中间层及应用层的参数调整在此基础上进行，调整参数的过程需要使用大量的训练数据集（DataSet）进行输入，并在多次重复训练中将模型参数调试到最佳状态。

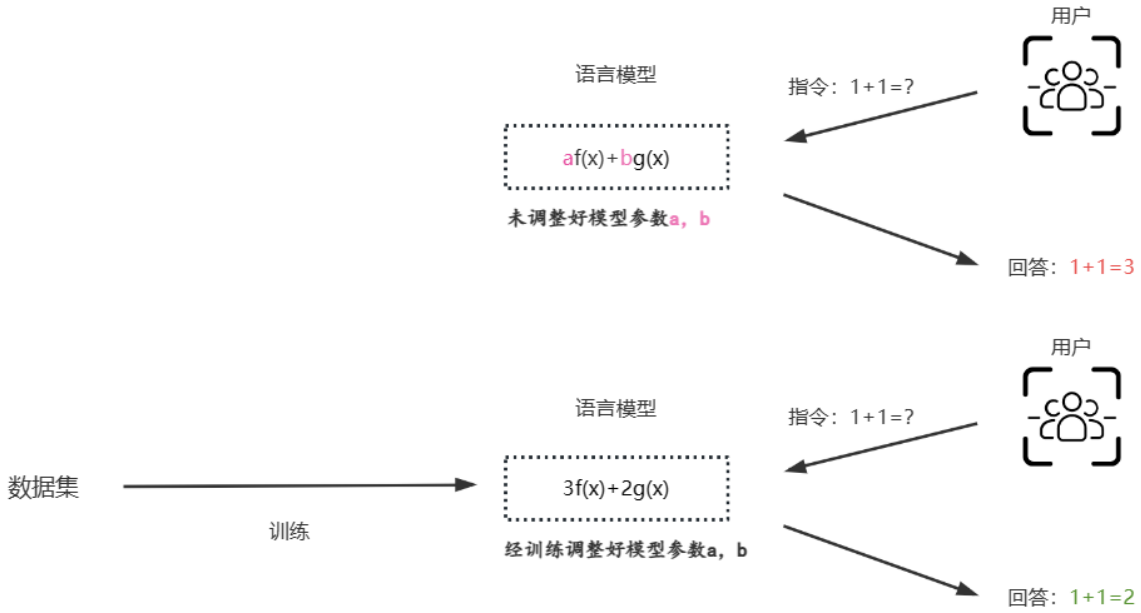

图 1 对 AIGC 模型开发的极简理解

上述过程中，**数据集**即用以给模型学习的人类的表达，可能是文字、图片等的集合。**模型代码和模型参数**组成了模型本身，模型代码实质上与其他软件程序一样，是由代码语言撰写的一系列命令组成。模型参数可以被视为模型代码中的变量，在训练中这些变量的值会不断地被调整和优化，以最大化模型的性能和准确性[3]。例如，在语言生成领域，模型参数可以控制生成文本的语法、词汇和语义等方面。

二、问题的提出：LLaMa 模型能不能自由使用？

2023 年 2 月 24 日，Meta（或“**Facebook**”）在其官网发布了 LLaMA 语言模型（参数分为 7B、13B、33B 和 65B）[4]，其宣称 LLaMA-13B 尽管规模仅为 GPT-3（175B）的十分之一，但性能却优于 OpenAI 的 GPT-3 模型[5]。这意味着开发者能够耗费较少资源对 LLaMA 进行进一步开发训练，甚至在单个消费级显卡

[2] 可以将 AIGC 产业生态分为基础层、中间层和应用层。基础层主要指由预训练模型为基础搭建的 AIGC 技术基础设施层。如 Stability.AI 的开源模型 Stable Diffusion。中间层即基于预训练模型，面向个性化、场景化的模型和工具。如基于 AI 模型开发的家居装饰工具 HomeDesigns AI。应用层即面向消费者的服务。如聊天客服机器人。受限于芯片等问题，国内开发主要集中于中间层及应用层，因此本文也主要聚焦于中间层和应用层的开发。

[3] 参见机器学习填坑：你知道模型参数和超参数之间的区别吗？https://cloud.tencent.com/developer/article/1005660。

[4] Meta: Introducing LLaMA: A foundational, 65-billion-parameter large language model，https://ai.facebook.com/blog/large-language-model-llama-meta-ai/。

[5] 知乎专栏：Meta 开放小模型 LLaMA，性能超过 GPT-3，https://zhuanlan.zhihu.com/p/610482395。

上进行部署[6]。这对于受限于芯片短缺的我国开发者而言非常具有吸引力。

起初，Meta 在 LLaMA 的发布首页表示，其依请求对申请者提供模型代码和参数。而在 Meta 发布 LLaMA 后不久，LLaMA 的代码和参数便被以可下载的磁力链形式泄露[7]。此后，便有不少开发者基于 LLaMA 进行开发，目前，已经有多个基于该模型开发的产品问世。然而，LLaMA 模型能不能自由使用，是一个需要仔细讨论的法律问题。

三、归本溯源：LLaMa 并非可自由使用的开源项目

与传统的开源软件不同，LLaMA 并非就整体适用单一协议。根据 LLaMA 语言模型的相关资讯以及 LLaMA 项目在 Github 社区中的问答、讨论，初步可以判定 LLaMA 应分为三个部分，其中 LLaMA Inference Code[8]（注：Inference 即推理，是模型开发的一个步骤）适用的协议是 GPL v3，而 LLaMA 的权重（Weight）参数以及 LLaMA 模型代码适用 LLaMA LICENSE AGREEMENT 不允许用于商业。**因此，LLaMA 最核心的模型代码和参数并不是面向公众、允许所有主体自由使用的开源项目。**

（一）Inference Code 适用 GPL v3 协议

LLaMA 语言模型发布页给出了指向 Github 的 LLaMA Inference Code 的开源链接，Inference Code 项目的贡献者 Stella Athena[9]在该项目的 Pull requests 栏目发布了 Conversation[10]，对 Inference Code 的协议作出了澄清：“*许多用户对‘开放科学’（Open Science）和‘开放源码’（Open Source）之间的区别感到困惑，以及**本资源库[11]的许可**与**使用模型本身的条款**之间的关系。为了帮助减轻这种困惑，我增加了一个新的文件 LICENSE_WEIGHTS，它包含了管理**模型权重**本身的许可信息，并在 README 中指出了这种区别[12]。*”

在该 README 中，StellaAthena 写明[13]，“*有关该资源库的许可信息，请参见[LICENSE]文件。LLaMA 模型上的权重可以根据研究人员的要求在**不同的许可**下提供，你可以在[LICENSE_WEIGHTS]文件中找到。*”

因此，Inference Code 的协议即存在于该项目的 LICENSE 文件中，该 LICENSE 文件载明其适用 GPL v3 协议。关于 GPL 协议的风险及降低风险的缓释措施，我们在之前的开源文章已有论及，可参阅[*汉坤 • 观点 | 没有无义务的权利：从开源软件侵权谈 GPL 开源合规*]。

---

6 康奈尔大学发布可以在一张消费级显卡上微调 650 亿参数规模大模型的框架：LLMTune，https://www.datalearner.com/blog/1051684078977779。

7 https://www.theverge.com/2023/3/8/23629362/meta-ai-language-model-llama-leak-online-misuse。

8 https://github.com/facebookresearch/llama。

9 在 Github 社区，代码项目可能由创建者之外的众多贡献者共同完成。Inference Code 项目要求贡献者签订 CLA（Contribution License Agreement）赋予项目所有者以使用或授权该项目的权利。在 StellaAthena 发布的 Conversation 中，StellaAthena 带有 CLA 已签署的标签，可证明其属于该项目的开发者/贡献者之一，因此其发言带有较强真实性、权威性。

10 https://github.com/facebookresearch/llama/pull/234。

11 即 Inference Code。

12 原文为“Many users are confused about the distinction between ‘open science’ and ‘open source’ and how the license in this repository relates to the terms under which one can use the model itself. To help alleviate some of this confusion, I have added a new file LICENSE_WEIGHTS which contains the licensing information that governs the model weights themselves and noted this distinction in the README.”

13 https://github.com/facebookresearch/llama/pull/234/commits/3f23e93b476cef85f2cabc7d8221a66adc4e6dfe。

（二）模型代码和模型 Weight 参数适用 LLaMA LICENSE AGREEMENT 不允许商用

LLaMA 模型代码适用 LLaMA LICENSE AGREEMENT 不允许用于商业。Meta 在 LLaMA 语言模型的发布页明确指出[14]，“*为了保持完整性和防止滥用，我们在非商业许可下发布了我们的模型，重点是研究用例。*”该页面随附一份获取模型（Access to Models）的申请表[15]，填写申请表需要同意 LLaMA LICENSE AGREEMENT，该 AGREEMENT 并非通用的开源协议，其载明不允许商业使用。

LLaMA 的 Weight 同样适用 LLaMA LICENSE AGREEMENT，不允许用于商业。前述 Stella Athena 给出的适用于 Model Weight 的 LICENSE_WEIGHTS 文件中的文本即为 LLaMA LICENSE AGREEMENT。

综上所述，可以得出，LLaMA 的 Weight 参数以及 LLaMA 模型代码适用定制的 LLaMA LICENSE AGREEMENT 协议不能用于商业，且使用需向 Meta 申请；而 Github 上的 LLaMA Inference Code 适用 GPL v3 协议。若开发者使用 Inference Code 触犯了开源风险但并未履行开源义务，则可能由于授权终止构成著作权侵权；若未另经许可将模型代码或 Weight 参数商用，则有可能构成违约，暴露在侵权风险之下。下文就未经授权使用 LLaMA 模型代码及参数的侵权风险进一步进行释明。

四、实务探讨：违反协议使用 LLaMa 模型的多维度风险

（一）使用 LLaMA 模型的著作权侵权风险

- **LLaMA 模型代码**

模型代码与其他代码实质相同，均可以作为计算机软件作品得到保护。中间层及应用层的 AI 产品往往基于现有的公开模型开发，因此对于模型代码的风险识别和合规使用可以参照开源软件风险识别，企业未经授权在开发的产品中使用他人的模型代码**可能构成著作权侵权或对使用协议的违约**。

就 LLaMA 模型代码而言，由于其系 Meta 的研究成果，很大概率包含了具有独创性的表达，因此可以认为其作为计算机软件作品得到保护，Meta 对其拥有著作权。虽然一些非官方渠道发布了 LLaMA 的模型代码，使其处于公开状态，也确实有不少开发者在基于 LLaMA 的模型代码进行开发（如 RedPajama）。但由于 Meta 在发布页中明确表示该模型仅能用于研究使用，并依据请求提供代码[16]，这表明 Meta 并未放弃 LLaMA 的著作权，LLaMA 仍然受到著作权法的保护。

因此，若开发者在未经许可的情形下，下载使用 LLaMA 模型代码进行开发，则不免将 LLaMA 的代码复制、部署于开发者的本地端，由于该行为复制了一份 LLaMA 的代码，因而可能侵犯复制权[17]。若开发者未经许可将含有 LLaMA 代码的模型部署应用，向公众传播，则可能构成对信息网络传播权的侵犯[18]。

---

[14] “To maintain integrity and prevent misuse, we are releasing our model under a noncommercial license focused on research use cases.”

[15] https://docs.google.com/forms/d/e/1FAIpQLSfqNECQnMkycAp2jP4Z9TFX0cGR4uf7b_fBxjY_OjhJILlKGA/viewform。

[16] “To maintain integrity and prevent misuse, we are releasing our model under a noncommercial license focused on research use cases. Access to the model will be granted on a case-by-case basis to academic researchers; those affiliated with organizations in government, civil society, and academia; and industry research laboratories around the world. People interested in applying for access can find the link to the application in our research paper.”，see Meta: Introducing LLaMA: A foundational, 65-billion-parameter large language model，https://ai.facebook.com/blog/large-language-model-llama-meta-ai/。

[17] 《计算机软件保护条例》第八条……（四）复制权，即将软件制作一份或者多份的权利。

[18] 参见广州知识产权法院（2022）粤 73 民终 805 号，“尚游公司作为《西游女儿国》游戏的开发者、原始著作权人，在未经合法授权的情况下使用了《梦幻西游》游戏中的美术作品、文字作品，并授权游族公司在运营过程中通过信息网络向公众提供上述作品，尚游公司、游族公司的行为侵害了网易雷火公司就涉案作品享有的复制权和信息网络传播权，依法应当承

■ **LLaMA 模型参数**

模型参数虽然可以被视为是模型的一部分，但一方面，参数实际是大量的数值，可能并不存在一般意义上人类可读的表达。另一方面，参数作为模型的变量，是通过将给定数据拟合到模型来估计[19]，是在不断的重复训练过程中被选择出来而非由开发者主观创造出来的[20]，可能无法体现人类的独创性。从这个方面看，其也可以被理解成为另一种形式的 AI 生成物，其能否和模型代码一样被作为作品保护亦存在一定的疑问。

对 AI 生成物是否能受到著作权保护存在不同观点。2023 年 2 月，美国版权局就 AI 生成图片是否享有版权作出回复，认为根据美国版权局实践纲要，任何非人类创作的作品都将被拒绝受到版权保护[21]。但我国司法实践存在并不截然排斥 AI 生成物著作权的案例，在被实务界广泛讨论所谓“认可 AI 生成文章著作权”的 DreamWriter 案中，法院认为基于开发者对于写作软件的生成过程的选择和安排认可了软件生成文章的可作品性[22]。

然而模型参数的生成方式却不同，在机器学习中，模型参数是用于定义模型的可调整变量，这些变量可以被优化，以使模型能够更好地拟合训练数据，并在新数据上表现更好。相关参数是基于大量训练数据集的输入，调整模型的原始参数值，以保证得到最佳输出而得出的。参数的得出是一个不断寻找最优解的过程，**输出的参数值并不能体现开发者的安排和选择**。因此，在这一角度，模型参数是否能被认定为体现人类独创性的表达，也有待进一步探讨。

这一问题的讨论也体现在 LLaMA 参数的使用中。在 LLaMA 被以可下载的磁力链形式泄露后[23]，开发者 Shawwn 通过链接下载了 LLaMA 模型的 Weight 参数置于 Github 平台的 LLaMa-dl 项目中，Meta 在 Github 上发布了通知，指控 Shawwn 侵犯了 Meta 版权，要求 Github 下架该项目[24]。

LLaMa-dl 提交了反通知，认为 Weight 所体现的事实并没有足够的独创性，因此无法获得版权。它们是通过死记硬背的自动程序从用于训练模型的作品中复制出来的，并不反映任何人工选择或安排。Meta 对这些 Weight 没有版权利益，因此 LLaMA-dl 不会诱发对任何可版权利益的侵犯[25]。

若按照 LLaMa-dl 的观点，LLaMA 参数无法成为作品受到著作权保护，因此使用 LLaMA 参数不会构成著作权侵权。但由于目前法律对此尚无明确回应，在法律和司法实践作出回应前对参数的未经授权使用应持谨慎态度。

（二） 使用 LLaMA 模型的侵犯商业秘密风险

模型参数/模型代码作为商业秘密进行保护需要满足非公知性、价值性和采取保密措施的要件。模

担停止侵权、赔偿损失的侵权责任。”

19 参见极客教程 — 模型参数与超参数的区别，https://geek-docs.com/machine-learning/ml-ask-answer/the-difference-between-model-parameters-and-hyperparameters.html。

20 参见机器学习模型调参指南（附代码），https://cloud.tencent.com/developer/article/1701823。

21 AI-created images lose U.S. copyrights in test for new technology | Reuters。

22 （2019）粤 0305 民初 14010 号判决书。

23 See The Verge — *Meta's powerful AI language model has leaked online — what happens now?* https://www.theverge.com/2023/3/8/23629362/meta-ai-language-model-llama-leak-online-misuse。

24 Github – DMCA, https://github.com/github/dmca/blob/master/2023/03/2023-03-21-meta.md。

25 Github – DMCA, https://github.com/github/dmca/blob/c1aca5130c2e9f798cf58881ed0fc1966f8f05be/2023/04/2023-04-27-meta-counternotice.md。

型代码作为需要耗费大量精力研究且具有一定应用于市场产生商业价值的产物，参数作为需要耗费大量算力和时间得出的对于模型表现有重要意义的数值，可以认为两者均满足价值性的要件。因此，若模型开发者对于新开发出的模型参数/模型代码采取了必要的保密措施，则模型参数可以作为商业秘密得到保护。

就 LLaMA 模型来看，其代码和参数已经被泄露，且被广泛使用。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》第三条：“*权利人请求保护的信息在**被诉侵权行为发生时**不为所属领域的相关人员普遍知悉和容易获得的，人民法院应当认定为反不正当竞争法第九条第四款所称的不为公众所知悉。*”对于模型参数的泄露者而言，其相关行为可能为《反不正当竞争法》第 9 条第 1 款前 3 项所禁止[26]。若其相关行为发生的时间早于公开前，也就是说，在侵权行为发生时，LLaMA 的模型代码、参数还可能处在不为公众所知悉的状态，具有非公知性，泄露者可能承担相应的侵犯商业秘密的责任。

而对于使用泄露的 LLaMA 模型代码及参数进行开发的主体而言，其行为模式可能落入《反不正当竞争法》第 9 条第 3 款的规制范围 — “*第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条第一款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密*”。但由于其使用的是他人泄露的 LLaMA 模型代码及参数，在开发时，LLaMA 模型代码及参数可能已处于公知状态，开发者可以尝试主张上述模型代码及参数不具有非公知性，不能作为商业秘密受到保护。

五、结语：谨慎中前行

AIGC 产品作为科技革命的最新产物，法律对其的回应和规制难免稍显落后和局促。从开发者的角度，若严格适用既有的法律制度，则不免对开发者要求过苛，不利于 AI 产业的发展和技术的进步；但从社会的角度，对 AIGC 产品进行一定的规制以避免侵权和隐私泄露又是必要之举。

对于开发者来说，对模型的选用应保持相对谨慎的态度，尤其是大型互联网企业，在考虑产业需求的同时，还需要对模型本身的可能带来的法律风险进行全面细致地分析，避免未经授权使用带来的侵权风险。后续 Meta 对 LLaMA 模型的未授权使用的态度和相关权利行使行动的进展尤其将对生成式人工智能的模型使用边界起到举足轻重的影响。

[26] 第九条 — 经营者不得实施下列侵犯商业秘密的行为：（一）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；（三）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。

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：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com