HANKUN

汉坤法律评述

2026 年 9 月 28 日

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

人工智能大模型开源软件的侵权责任与企业合规：评《最高人民法院关于依法审理涉人工智能纠纷案件的意见》第十三条

作者：吴丽丽 | 闻馨 | 况雨艳

2026 年 9 月 7 日，最高人民法院发布《关于依法审理涉人工智能纠纷案件的意见》（法发〔2026〕10 号，以下简称“《**意见**》”），就涉人工智能纠纷案件的审理作出系统性裁判规则指引。其中，《意见》第十三条专门规定涉人工智能开源软件相关方的法律责任，通过“综合考量、适当豁免”的规则设计，为开源人工智能生态中各参与主体的责任划分提供了司法指引。本文以《意见》第十三条为中心，在梳理既有开源软件司法实践与产业现实的基础上，综合分析该条所确立的责任认定框架及其具体适用条件，为人工智能技术革命浪潮中各相关企业的开源实践提出相应合规建议，以期为开源人工智能生态的开发者、提供者及其他相关主体提供参考。

一、《意见》第十三条进一步回应了开源软件责任认定问题

要理解《意见》第十三条的制度创新，有必要首先回顾我国涉开源软件的既有司法实践及制度留白。

在《意见》出台之前，我国司法实践已经开始涉及和逐步回应开源许可协议的法律性质、开源义务与著作权侵权责任之间的关系。例如，在（2019）粤 73 知民初 207 号案中，广州知识产权法院对开源许可协议的性质进行了分析，明确开源许可协议具有合同性质，系关于软件著作权许可的附解除条件的格式合同文本：“GPL V3 协议具有合同性质，是授权方和用户订立的格式化著作权协议”、“GPL V3 协议属于附解除条件的著作权合同”。该案所涉及的核心问题之一，即是开源许可协议的违约责任与被许可人著作权侵权责任之间的关系。又如，（2021）最高法知民终 51 号案中，最高人民法院裁判要旨明确：“被诉侵权人仅以涉案软件开发者并未依据开源许可协议开源为由，抗辩其不侵害涉案软件著作权的，人民法院一般不予支持。”换言之，软件开发者是否履行开源义务，与其是否基于独创性贡献享有涉案软件著作权，并不必然相关。

可以看到，上述裁判已经从不同维度为处理涉开源软件纠纷提供了重要的司法基础。但从责任配置的角度看，仍有一个值得进一步讨论的问题：当开源软件开发者、提供者并非直接实施侵权行为，而只是将代码模块免费提供给后续开发者使用时，其是否以及在何种条件下可以因开源行为本身获得侵权责任上的适当豁免？

这一追问源于开源人工智能产业的现实需求：

一方面，正如《〈最高人民法院关于依法审理涉人工智能纠纷案件的意见〉的理解与适用》（以下简称“**《理解与适用》**”）指出的，“当前，生成式人工智能模型的研发高度依赖开源软件生态”，而“开源人工智能大模型的研发链条长、参与主体多”。在这一研发模式下，开源软件一旦被广泛集成和二次开发，其潜在的知识产权风险可能沿着研发、修改、集成和再分发链条持续传导，并最终体现在后续开发的软件产品之中。如果将此类风险过度归于上游开源软件的开发者、提供者，可能增加其参与开源活动的法律风险与合规成本，并对开源创新的积极性产生一定影响。

另一方面，开源许可证有时会设置“不担保”、“免责”等条款，以降低开源软件开发者、提供者因下游使用行为承担责任的风险。比较法上，德国法兰克福地方法院在 Harald Welte 诉 D-Link 案[1]中将开源许可协议 GPL 认定为一般交易条款，并对其中包括无担保声明在内的许可条件进行了审查，认为相关条款未不适当地损害软件使用人的利益，因而具有法律效力。但与此相比，我国现有开源软件司法实践虽然已经确认开源许可协议具有合同及格式条款属性，但对于“不担保”、“免责”或者责任限制条款是否符合我国《民法典》第 497 条[2]规定的格式条款效力规则，还未进行明确的正面确认。因此，仅依据现有司法实践，尚不能认为开源软件开发者、提供者在许可证中设置一般性的免责声明或责任限制条款，就可当然可以排除其在特定情形下可能承担的法律责任。其具体效力仍有待结合《民法典》关于格式条款的相关规定以及具体条款内容、适用情形等因素予以判断。

正是在这一背景下，《意见》第十三条对开源软件开发者、提供者的责任豁免作出了制度回应。与此前的司法实践相比，第十三条进一步将关注点延伸至开源行为整个链条的侵权责任之间的关系，并尝试通过注意义务、风险披露与责任豁免之间的衔接，对开源生态中的风险进行合理分配。

二、“综合考量 — 适当豁免”以及“免费开源 — 可以免责”

《意见》第十三条规定：“审理涉开源软件案件，认定开源软件开发者、提供者以及后续开发者、提供者的侵权责任，应当综合考量开源许可协议类型、权利限制的具体内容、安全合规举措和信息披露程度等因素，依法给予开源软件开发者、提供者适当的责任豁免。开源软件开发者、提供者以免费开源的方式提供涉人工智能软件研发所需要的部分代码模块，并公开说明其功能和安全风险，他人使用该代码模块导致侵权的，人民法院可以认定开源软件开发者、提供者不承担侵权责任。”从规范结构看，该条实际包含两个层次：第一层次是一般性的综合考量规则；第二层次是针对特定免费开源场景设置的更明确规则。

（一）一般规则：综合考量 — 适当豁免但不是“只要开源即可免责”

《意见》第十三条的核心并不是“只要开源即可免责”，而是要求人民法院结合开源行为的具体方式、风险控制能力以及信息披露情况，对不同主体的责任进行个案判断。从文义解释来看，具体包括如下四项考量因素。

1. 考量因素一：开源许可协议类型

开源许可协议是确定开源软件使用边界和后续义务的重要依据。其是一种具有法律效力的格式合

[1] 案件编号：LG Frankfurt, Urteil vom 06.09.2006, Az.2-06 O 224/06。

[2] 《民法典》第四百九十七条：“有下列情形之一的，该格式条款无效：（一）具有本法第一编第六章第三节和本法第五百零六条规定的无效情形；（二）提供格式条款一方不合理地免除或者减轻其责任、加重对方责任、限制对方主要权利；（三）提供格式条款一方排除对方主要权利。”

同，定义用户自由使用、修改、复制或分发开源许可作品的权利和义务。[3]不同开源许可协议在衍生作品、修改、再分发、署名、通知以及专利许可等方面的要求存在显著差异。因此，在认定开源软件相关主体责任时，首先需要确定涉案软件所适用的许可协议及其具体版本，进而明确其对下游使用者所设定的权利和义务。

以“著佐权”（Copyleft）[4]的典型代表 GPL[5]类开源许可协议为例，对于构成 GPL 意义上的衍生作品并进行再分发的情形，相关许可条件可能要求衍生作品继续按照 GPL 许可。相比之下，Apache 2.0、MIT、BSD 等开源许可协议则较为宽松，通常对修改、再分发及商业利用设置的限制较少。

2. 考量因素二：权利限制的具体内容

在确定开源许可协议类型后，还需进一步审查该协议所约定的权利限制具体内容，考察具体条款如何配置权利与义务。若开源许可协议中已对后续开发者、下游使用者享有的权利作出明确限制，下游主体是否遵守相关许可条件，可能成为法院判断各方责任的重要事实。

例如，开源许可协议已明确禁止将模型用于违法内容生成、歧视性决策、虚假信息传播、大规模监控、医疗、军事用途等特定场景，并要求下游在再分发时传递相同的使用限制。若下游违反该限制，将模型用于开源许可协议明确禁止的用途并导致侵权，则上游开源软件开发者、提供者通常可能获得适当豁免。

又如，开源许可协议明确约定，不得将开源软件与其他部分结合后构成对第三方专利的侵权。而下游使用者擅自将代码模块整合且构成专利侵权，则上游开源软件开发者、提供者通常可能获得适当豁免。

3. 考量因素三：安全合规举措

除协议约定外，开源软件开发者、提供者是否采取了相应的安全合规举措，也是《意见》第十三条明确要求法院考量的因素。这里的安全合规举措，可以理解为开源软件开发者、提供者对开源软件采取的安全管理措施，包括但不限于安全审计、漏洞检测、安全公告、合规审查以及其他合理的安全管理措施等。

这一因素体现出《意见》第十三条并非单纯根据“是否开源”分配责任，而是进一步关注开源软件开发者、提供者是否尽到与其技术能力、风险认知相符的注意义务。若开源软件开发者、提供者明知代码存在重大安全缺陷或侵权风险，却未采取任何提示、修复或披露措施，或者在收到明确安全风险反馈后仍长期不予处理，则即使其系免费提供，也可能因未尽安全合规义务而被认定存在过错，从而无法获得责任豁免。

4. 考量因素四：信息披露程度

开源软件具有开放传播、参与主体多、使用场景复杂等特点。对于下游使用者而言，能否及时、充

[3] 国家标准《信息技术 开源 开源许可证框架》（GB/T 44272-2024），参见：https://openstd.samr.gov.cn/bzgk/std/showGb?type=online&hcno=48875862F65D66457449A1964058C8B1&request_locale=zh。

[4] 著佐权（Copyleft）：允许创作衍生作品，但要求衍生作品采用与原作品相同的许可协议。例如，假设编写了某款软件，并依据 GPL 许可协议发布；之后他人修改了该软件并分发其修改版本，那么该修改版本也必须依据 GPL 许可协议授权。参见 Open Source Initiative: Frequently Answered Questions, https://opensource.org/faq/#what-is-copyleft-is-it-the-same-as-open-source。

[5] GNU 通用公共许可证（GNU General Public License，即 GPL）：强著佐权开源许可协议，由自由软件基金会发布。

分地了解代码的功能、适用范围及已知风险，将直接影响其对使用风险的识别和控制。

我们理解，充分的信息披露通常应包括：说明代码模块的功能、适用场景、固有局限、已知安全风险、不适宜用途，以及与第三方权利可能发生冲突情形的说明等。在实践中，披露形式既可以通过开源软件代码仓库中的自述文件（README）[6]，也可以通过安全策略文件（SECURITY）[7]、模型卡片（MODEL CARD）[8]、开源许可协议（LICENSE）等载体进行。合规关键并不在于披露载体的名称，而在于下游使用者能否通过合理渠道获取相关信息，以及该等信息是否充分、明确、及时，从而通过相关披露信息预见、防范开源软件风险。

（二）特别规则：免费开源 — 可以免责

如果说第一层次确立了开源软件侵权责任认定的一般考量框架，那么第二层次则设定了免费开源情形下更为明确的责任豁免要件。该等豁免并非“一刀切”地全部豁免，而是采用“可以认定”的方式，由人民法院结合个案具体情况判断是否予以豁免。该规则适用要件至少包含以下几个方面。

1. 要件一：主体为开源软件开发者、提供者

该规则限定了责任豁免的适格主体：即有权主张《意见》第十三条责任豁免的，仅限于开源软件开发者、开源软件提供者两类主体。在具体案件中，通常将结合开源软件的提交记录、发布公告、著作权署名信息等事实，判断相关主体与涉案开源软件之间的开发、维护或提供关系，综合认定被诉主体是否属于适格主体。

2. 要件二：以免费开源方式提供

“免费开源”是适用责任豁免的核心前提之一，《理解与适用》亦指出“以商业化方式提供开源代码的相关主体不能适用该豁免规定”。然而，“免费开源”要件是否意味着只要开发者、提供者通过代码获得任何收益均不能豁免？

结合我们实践经验来看，“免费”重在强调代码模块本身的许可不收取直接对价，但通过技术支持、订阅制云服务、定制开发等方式获得的收入，仍存在免责空间。这与开放源代码促进会（Open Source Initiative）官方关于“如果任何人都能卖我的代码，我该怎么赚钱？”的回答亦相契合：“你可以基于代码来卖服务（也就是卖自己的时间）、卖质保和其他保证、承接定制和维护工作、授权商标使用，等等。唯一与开源不兼容的盈利策略，是基于垄断的销售，也就是所谓的‘版税’[9]。”如果开发者、提供者对代码模块本身收取直接许可费对价，则难以被认定为“免费开源”。反之，开发者、提供者通过技术支持、订阅制云服务、定制开发等方式获得收入的，则不能仅因存在商业收入，就当然否定其“免费开源”的性质。

---

[6] 自述文件（README）：是开源软件基础的信息披露文档，通常告诉其他人开源软件为什么有用，能用开源软件做些什么，以及如何使用。参见：https://docs.github.com/zh/repositories/managing-your-repositorys-settings-and-features/customizing-your-repository/about-readmes。

[7] 安全策略文件（SECURITY）:是用于说明安全漏洞报告策略的文档。参见：https://docs.github.com/zh/code-security/how-tos/report-and-fix-vulnerabilities/configure-vulnerability-reporting/add-security-policy。

[8] 模型卡片（MODEL CARD）：由 Margaret Mitchell 等人在论文“Model Cards for Model Reporting”中首次提出。主要内容包括模型的用途、模型描述、预期用途和限制、如何使用、局限性和偏见、训练数据、训练程序、评价结果。参见：https://huggingface.co/docs/course/zh-TW/chapter4/4。

[9] 开放源代码促进会（Open Source Initiative）官方 FAQ 中关于开源软件商业化的问答。参见：https://opensource.org/faq#%3A~%3Atext%3DAbsolutely.%2Cnot%20the%20same%20as%20proprietary。

3. 要件三：提供涉人工智能软件研发所需要的部分代码模块

《意见》第十三条并非对所有开源软件提供无差别的责任豁免，而是进一步限定其客体为“涉人工智能软件研发所需要的部分代码模块”。例如，为模型训练、推理、数据处理、计算加速、模型部署等人工智能研发环节提供基础功能的开源代码模块，通常更容易落入该规则所关注的范围。其他领域的开源软件若非为人工智能软件研发所需要的，则难以符合豁免的客体要件。

这一条件也意味着，企业在进行开源时，应当尽可能清晰说明代码模块的功能及应用场景，以便在发生争议时证明其与人工智能软件研发之间的实际关联。

4. 要件四：公开说明功能和安全风险

要件四与《意见》第十三条第一层次中的“信息披露程度”直接衔接。《理解与适用》也指出“这一规则引导开源软件开发者、提供者增强信息披露意识，形成‘贡献—披露—免责’的良性机制”[10]。

因此，如前所述，实践中开源软件开发者、提供者可借助 README、SECURITY、MODEL CARD、LICENSE 等文件，对代码模块的功能、适用范围、已知局限以及已知安全风险进行合理披露。对于人工智能软件而言，如果代码模块存在已经识别的安全漏洞、明显的适用限制或者特定技术风险，相关信息尤其值得明确记录和持续更新。

5. 要件五：他人使用该代码模块导致侵权

要件五要求侵权与“他人使用”之间存在因果关系，即，《意见》第十三条所豁免的，是开源软件开发者、提供者作为代码提供方，在他人利用其所提供代码实施侵权时可能承担的责任，而并非对其自身实施的侵权行为提供免责。

因此，如果侵权行为本身由下游使用者或者后续开发者实施，并且该侵权与使用涉案开源代码模块存在相应因果联系，则可以进一步考虑上游开发者、提供者是否符合《意见》第十三条的责任豁免条件。反之，若开源软件开发者、提供者自身直接利用该代码模块实施侵权行为，则原则上不能仅因其具有“开源软件开发者”身份而主张免责。

三、企业合规启示

《意见》第十三条为开源软件提供者、开发者提供了明确的抗辩路径。但更重要的是，它向开源软件开发者、提供者释放了较为明确的合规信号：从开源许可协议选择、文档撰写、信息披露到安全治理，都将共同影响责任认定。因此，企业不宜将第十三条理解为一种事后免责工具，而应及时将第十三条的豁免要件转化为可落地、可留痕的合规安排。

（一）审查 LICENSE、README 及其他配套文档

传统开源项目往往将 LICENSE 视为主要甚至唯一的合规文件。但从《意见》第十三条的规范结构看，仅有一份 LICENSE 文本可能不足以完整体现开发者已经采取的安全合规措施及信息披露措施。

以下表所列的部分国产人工智能开源模型为例，开源许可协议主要采用 MIT、在 MIT 基础上修改

[10] 周加海、司艳丽、秦元明、贾玉慧、张音：《〈最高人民法院关于依法审理涉人工智能纠纷案件的意见〉的理解与适用》，载《法律适用》2026 年第 11 期。参见：https://ipc.court.gov.cn/zh-cn/news/view-6039.html。

的 Modified MIT、Apache 2.0。

#	模型名称	开源许可协议	链接
1.	deepseek-v4-pro	MIT	https://huggingface.co/deepseek-ai/DeepSeek-V4-Pro/blob/main/LICENSE
2.	glm-5.1	MIT	https://huggingface.co/zai-org/GLM-5.1/blob/main/LICENSE
3.	kimi-k2.6	Modified MIT	https://huggingface.co/moonshotai/Kimi-K2.6/blob/main/LICENSE
4.	Qwen2.5-1.5B	Apache 2.0	https://huggingface.co/Qwen/Qwen2.5-1.5B/blob/main/LICENSE

这些协议本身主要解决的是软件或模型的授权、使用和责任限制问题。尽管它们大多设置了典型的免责条款 —“在任何情况下，作者或版权持有人均不对因本软件或本软件的使用或其他处置所引起或与之相关的任何索赔、损害或其他责任承担责任，无论该等责任基于合同、侵权还是其他事由。”但免责声明并不能当然替代《意见》第十三条要求的安全风险披露和功能说明等完整披露。

据此，企业在开源人工智能软件或模型时，可以将 LICENSE、README、SECURITY、MODEL CARD 等文件结合起来进行整体设计，至少确保以下信息能够被下游使用者合理获取：

- 代码或模型的主要功能及适用场景；
- 已知的技术局限；
- 已知安全风险及漏洞处理方式；
- 不适宜使用的场景；
- 下游使用者需要履行的许可条件；
- 必要的第三方权利及合规提示。

更有利于满足《意见》第十三条所体现的信息披露要求，以确保在潜在的开源软件纠纷中能够有效主张责任豁免。

（二）建立人工智能开源项目的全生命周期治理机制

《意见》第十三条所释放的导向，并非单纯关注开源发布这一时间点，而是将责任承担与注意义务相匹配，强调开发者、提供者在其能够控制的范围内所采取的合理措施。因此，企业不应仅仅依赖开源许可协议和说明文档进行被动抗辩，而应将合规要求嵌入人工智能开源项目的研发、审查、发布、运营、争议解决等环节的全生命周期，以积极、主动地契合《意见》的实质要求。

- 发布前，应重点审查开源许可协议的适配性，并同步完成代码来源、第三方开源组件、数据、专利、商标等基础审查；根据项目特点，编制 LICENSE、README、SECURITY、MODEL CARD 等文件，明确功能、局限、禁止用途和已知风险。
- 发布时，应确保最终发布版本与经过审查的版本一致，保存许可证、代码版本、提交记录、发布页

面及相关披露材料。

- 发布后，则应持续进行版本管理、漏洞响应、安全更新和供应链维护。对于已经发现的重要漏洞或其他重大风险，应根据实际情况及时采取修复、通知、更新等措施。

通过上述机制，企业便可以将《意见》第十三条所要求的考量维度转化为企业日常可执行的流程。

（三）留存合规证据，构建诉讼抗辩基础

由于《意见》第十三条责任豁免采取“可以认定”的表述，而非当然豁免。主张适用《意见》第十三条豁免的各方，需要举证证明其符合减轻或豁免的要件。若不能在潜在纠纷中有效举证，仍难以实现豁免。为此，开源软件开发者、提供者应当留存完整、可追溯、可验证的全套合规证据材料，至少包括：

- 开源及许可证据。包括开源许可协议文本、版本迭代记录、发布公示记录及发布时间等，用以证明涉案代码模块的来源、许可方式及具体版本。
- 信息披露证据。包括 README、MODEL CARD、SECURITY、风险提示、版本说明、更新日志等，用以证明已就代码模块的功能、适用场景、固有局限及已知安全风险等作出充分披露。
- 安全治理证据。包括安全审计记录、漏洞披露与修复记录、版本更新日志、风险公告等文件，用以证明企业已尽到与技术能力相匹配的安全合规注意义务。对于重要开源项目，还可以留存内部开源审批记录、法律审查意见、技术安全评估等材料，以证明企业在开源前已经进行了必要的风险识别和治理。

这些材料不仅可以服务于《意见》第十三条下的责任认定，也能够在发生开源许可争议、著作权侵权争议或者其他知识产权纠纷时，为企业还原项目开发及发布过程提供证据基础。

四、结语

开源软件依托共享协作的模式，整合全球智力、算力及数据资源推动软件技术持续迭代。对于人工智能产业而言，开源生态更是连接模型、代码、工具链和应用场景的重要基础设施。《意见》第十三条并非简单地为开源软件开发者、提供者提供一项当然免责规则，而是通过“综合考量 — 适当豁免”以及“免费开源——可以免责”的两层规则结构，在知识产权保护与开源创新之间建立更为明确的责任配置机制，有助于引导生成式人工智能模型的各类参与方更积极地融入开源生态。

对于参与人工智能开源生态的企业而言，《意见》第十三条所提供的制度空间，需要通过具体的合规措施加以承接。与其将责任豁免理解为发生纠纷后的事后抗辩，不如在事前即建立起完善的合规体系。因此，企业可以借《意见》发布的契机，使《意见》第十三条所关注的各项因素真正转化为企业可以执行、持续维护并在必要时予以证明的合规机制。

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

© 2026 Han Kun Law Offices. All Rights Reserved.