汉坤法律评述
2022 年 11 月 8 日

HANKUN
汉坤律师事务所
Han Kun Law Offices

“开源合规”系列之二 — 企业应如何构建开源合规制度？

作者：段志超 | 鲁学振 | 高航[1]

作为汉坤开源系列文章的序言，在“*没有无义务的权利：从开源软件侵权谈 GPL 合规*”一文中，我们从“罗盒案”入手，探讨了 GPL 软件的合规风险，为大家简要介绍了 GPL 类开源软件的合规问题。

本文，我们将从开源生态及其参与者们的角色出发，结合实务中企业在开源合规建设中遇到的问题，和大家一起探讨企业构建开源合规制度需要关注的问题，为企业的开源合规建设提供具有可操作性的建议。

汉坤知识产权团队持续关注开源合规建设，并计划发表汉坤开源系列文章，以期为企业开源合规提供指引和启示。该系列文章将聚焦于开源软件在具体应用场景下的合规建议，如“SaaS 业务形态下云服务厂商面临的开源挑战”、“特殊传染性开源协议的分析及风险规避建议”、“企业‘开源出去’的流程和注意事项”等实务问题。

一、机遇与风险并存的“开源宝藏”

（一）开源的源起和现状

开源源于上世纪 70-80 年代开发者们对于软件从免费转向收费且不再提供源代码这一现象的不满。1983 年，Richard Matthew Stallman 通过 GNU 计划（GNU Project）发起自由软件运动（Free Software Movement），推广自由软件精神，即给予使用者自由的软件，并反对不附带源代码的闭源软件[2]。由于“Free”一词可能给人造成“免费”的误解，且可能被认为带有政治意味，“开源软件（Open Source Software）”一词逐渐替代了“自由软件（Free Software）”一词，并于 1998 年由开源代码促进会（Open Source Initiative，OSI）给出了明确定义[3]。其实，不论是开源软件抑或是自由软件，其本质都是希望通过知识共享共同推动技术进步，而正是这样的核心理念，吸引了越来越多的开发者加入开源的行列。

1992 年，适用 GPL 协议的 Linux 0.12 的发布[4]为开源提供了重要的基础设施，开启了开源的快速发展期。随着 Apache HTTP Server、MySQL 等优质开源项目的流行，以及 GitHub、Gitlab 等大型代码托管平台的出现，开源愈发受到认可与重视。在“打造数字经济新优势”写入“十四五”规划的大背景下

[1] 实习生林磊对本文的写作亦有贡献。

[2] 参见 https://www.gnu.org/gnu/gnu.html。

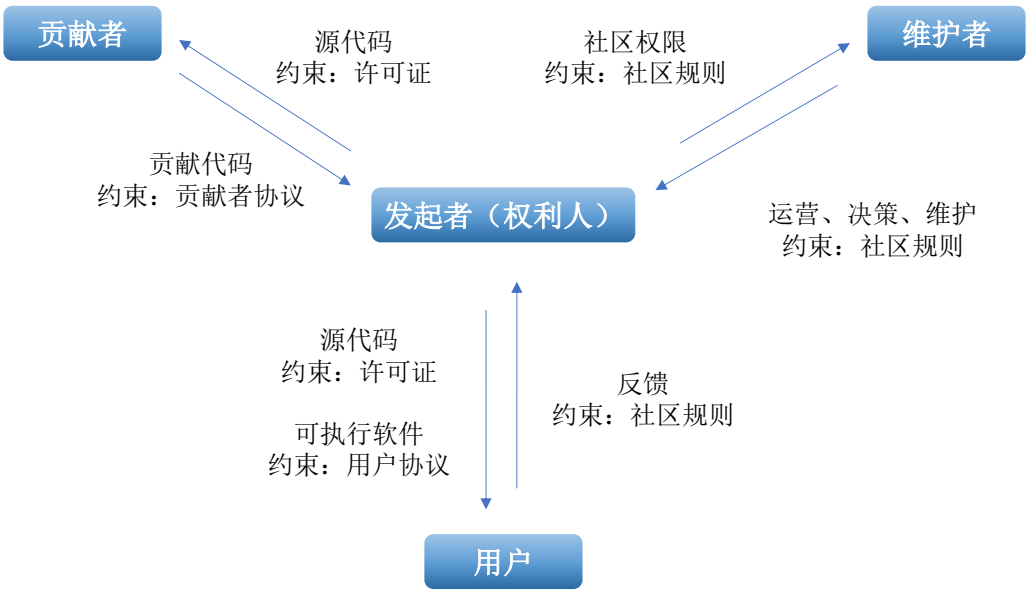
[3] 参见 https://opensource.org/history。

[4] 参见 https://mirrors.edge.kernel.org/pub/linux/kernel/Historic/old-versions/RELNOTES-0.12。

[5]，随着数据合规、进出口管制等领域的制度完善以及司法实践的不断探索，可以预见，开源将以更为规范、安全、稳定的形态迎来蓬勃发展的新阶段。

（二）开源生态及其参与者们

开源生态以开源社区为基础。开源社区的参与者主要可分为发起者、贡献者、维护者与用户等不同角色，其示意图如下。其中，发起者通过上传初始源代码建立开源项目，通常即为开源项目著作权人与开源社区管理人；贡献者通过开源社区获得受开源许可证限制的源代码，在接受《贡献者协议》后提交贡献代码；维护者依据社区规则取得相关社区权限，以开展社区运营、决策与维护；用户可以在接受用户协议后直接使用开源项目生成的可执行软件，也可以进一步通过开源社区获得受许可证限制的源代码，并且作为产品的最终使用者，能够依照社区规则提供有关错误、漏洞、性能等方面的反馈，帮助项目进一步改进。



随着开源经济的快速发展，各开源企业已逐步探索出了各类以新型开源产品和服务为基础的商业模式。例如，以 Red Hat[6]、MySQL[7]为代表的支持服务订阅模式，向使用其开源产品的用户提供付费的专业技术支持与咨询服务；以 Gitlab[8]、Cloudera[9]为代表的 Open Core 模式，仅对核心基础部分开源，而对其他可选高级模块与服务闭源进行销售；以 Databricks[10]、MongoDB[11]为代表的 SaaS 模式，直接将开源软件作为服务托管在云平台上，向客户提供付费 SaaS 服务等。当然，各个企业的商业模式并不唯一，且仍在持续探索中。例如，通过 Serverless 等新型架构进一步提供差异化产品及服务，又如，通过开源获取生态流量入口后利用流量变现获取利润等。由此可见，开源的商业模式仍存在极大的想象与探索空间。

---

[5] 国务院《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》提出：“支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务。”

[6] 参见 https://www.redhat.com/zh/services。

[7] 参见 https://www.mysql.com/services/。

[8] 参见 https://about.gitlab.com/company/stewardship/。

[9] 参见 https://www.cloudera.com/products/pricing/product-features.html。

[10] 参见 https://www.databricks.com/product/pricing。

[11] 参见 https://www.mongodb.com/pricing。

除了注重营利的开源企业，开源基金会作为非营利性组织在开源生态中也扮演着重要角色。基金会通过会员费、接受企业捐赠等方式获取资金，以孵化进入基金会的开源项目，通过持续的监督和指导，帮助开源项目建设成熟的开源社区，以实现开源项目发展的持续性，同时也推进了开源项目的迭代与推广。

（三）开源许可证

开源许可证也称开源协议，是开源理念下的一项重要成果。如前所述，开源本质上是希望通过知识共享推动技术进步，而并不是要对抗承载于智力成果之中的知识产权，开源也同样需要通过法律保护开发者的合法权益。为了在保护开发者合法权益的前提下充分保障用户自由使用软件的权利，与著作权（Copyright）相对应的著佐权（Copyleft）概念应运而生[12]，通过开源许可证的方式，在保护作者专有权利的同时也进行了自我权利限制，保障了用户分享与修改软件的自由。各开源社区、知名大学与团体组织制定了一系列的开源许可证，各个许可证的权利义务条款规定各不相同，往往能够体现出不同的考量。例如，GPL 许可证强调互惠性，因此其在条款中便规定，用户修改后发布的软件必须同样适用 GPL 许可证[13]，以此进一步促进开源。

在“罗盒案”[14]中，深圳市中级人民法院对开源许可证的法律性质做出了明确论述，即开源许可证具有合同性质，用户在对源代码进行复制、修改或发布时，许可证成立并生效。用户有权在遵守许可证规定的前提下行使某些权利，但也必须承担相应的义务。例如，用户有权修改与分发适用 GPL 许可证的开源软件，但修改后的软件必须同样以 GPL 许可证开源。若用户违反了许可证的规定导致许可终止，则用户的行为将因失去权利来源而构成侵权，进而需要承担侵权责任。

由此可见，对于涉及开源的企业而言，无论是作为开源软件的使用者，抑或是开源软件的发布者，开源合规都是需要给予足够重视的问题。

二、实务中的开源风险与合规建设

开源软件的高度依赖性使得开源软件的合规风险问题已经在各行各业逐渐凸显。然而，由于企业普遍缺乏对于开源软件的正确认识和风险防控，加上企业内部对开源软件的管理并不规范，因此催生出了许多开源软件的使用风险。随着赔偿额等侵权代价的逐步增加，国内外的开源软件相关诉讼已经开始逐步凸显，开源软件的著作权人也将在行权方面投入更多的时间和精力。

（一）实务中常见的开源风险

企业引入开源软件时，由于缺乏对各类许可证规定的权利和义务的深入了解，以及在风险控制上的一些错误认识，企业在使用开源软件的过程中极易触碰到**著作权**风险，构成违约、侵权，甚至将导致产品下架、巨额赔偿的后果，严重影响了企业的生产经营活动。

*例如，*开源软件许可证可能基于使用场景的不同对使用者提出了不同的许可证义务，而企业往往对此并不熟悉。

---

[12] 参见 https://www.gnu.org/licenses/copyleft.en.html。

[13] 参见 GPL 3.0 许可证第 5.c 条，https://www.gnu.org/licenses/gpl-3.0.html，GPL 2.0 许可证亦有类似规定。

[14] 参见济宁市罗盒网络科技有限公司诉被告福建风灵创景科技有限公司等侵害计算机软件著作权纠纷案，广东省深圳市中级人民法院（2019）粤 03 民初 3928 号民事判决书。

- 一些特殊的开源软件许可证对于开源软件的使用方式有具体限定，例如，Elastic License[15]禁止将目标代码用于 SaaS 服务，同时禁止在非测试环节对软件进行修改。而且，开源软件的许可证也可能会根据项目管理者的实际需求而变更，比如 MongoDB 就在 2018 年将许可证由 AGPL 变更为 SSPL。因此，准确识别开源许可证的性质并进一步分析其风险以规避侵权风险是非常重要的。

- 企业对于正在开发的产品或服务中的技术细节在法律上的认定缺乏准确的认识，例如，公司的具体适用场景是否会触发开源许可证义务中的“分发”条件。

再例如，开源社区可能存在将第三方代码以自己的名义进行开源的情形。此时，由于权利来源本身存在瑕疵，软件使用者难以在法律上主张获得了合法的授权，因而后续对开源代码的使用行为都可能构成侵权。这也就要求企业在引入开源软件时，建立相应的审查和引入标准，尽量不使用来源不明，权属不清的开源软件。

除上述最常见的著作权侵权风险外，使用开源软件还会有**专利、商标侵权**的法律风险。例如，由红帽公司发布的开源代码中往往存在红帽公司的商标信息，这就要求使用者在使用以及再发布相关代码时剔除红帽公司的商业标识，以防形成“使用红帽公司商标再发布程序或其组件”的外观，进而被要求承担商标侵权责任[16]。再例如，有些开源许可证（如 GPL v2[17]）并未对专利授权进行明确安排。如果开源软件原著作权人还申请了相关专利，并主张专利侵权的，开源软件使用者难以直接依据许可证的授权条款进行有效的不侵权抗辩。

另一个可能的风险是自有代码的不当泄露导致原本拟作为**商业秘密**保护的技术信息的秘密性的丧失。例如，如果企业未形成完善的对外开源制度，企业员工在向开源社区做贡献时，可能会不当地将企业原本拟作为商业秘密保护的代码对外披露，破坏了相关代码的秘密性。再例如，我们熟知的具有“强传染性”的 GPL 协议可能导致企业被迫开源自己的源代码，进而造成企业商业秘密的泄露。因此，对于企业来说，仅仅“识别”出 GPL 类开源软件是远远不够的。正如我们上文所提到的，由于底层代码的不可替代性，企业无法直接脱离 GPL 类开源软件的使用，因此势必需要采用技术手段“隔离”开源软件以规避“传染”的风险。

除一般性的知识产权侵权风险外，企业的开源软件风险还可能来自于开源软件中的**安全漏洞**。开源软件由于缺少持续性的维护和系统性的代码安全审查，容易存在一些安全漏洞。例如，对于这种由于外部侵权代码导致的“不清洁”问题，开源软件作者并不会对此承担任何责任，企业需要自行对开源代码进行内部的代码筛查工作来避免可能的侵权风险。此外，由工业和信息化部、网信办和公安部出台的《网络产品安全漏洞管理规定》[18]还对企业的漏洞汇报义务提出了要求，即要求企业发现或者获悉安全漏洞的，立即通知产品提供者，并在 2 日内向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关漏洞信息。

（二）建立全面的企业级开源风险防控机制

面对引入开源软件所带来的潜在的诸多风险，企业需要设计开源软件全生命周期的合规管理，包括从选型、引入、使用、管理、维护到退出，订制全方位的企业级开源风险防控制度。在构建开源合规制

[15] 参见 https://www.elastic.co/cn/licensing/elastic-license。

[16] 参见 https://www.redhat.com/licenses/APAC_EULA_RHEL_Chinese_20101110.pdf?oh=www.redhat.fr。

[17] 参见 https://opensource.org/licenses/gpl-2.0.php。

[18] 参见 http://www.gov.cn/zhengce/zhengceku/2021-07/14/content_5624965.htm。

度时，公司一般需要关注以下事宜：

- **结合公司的组织架构设计合规方案。**具体来说，应结合企业的具体角色和商业模式设计合规方案，如集团公司统一管理开源合规、子公司申请上报合规制度等。此外，如果相关技术由供应商提供，则需要在供应商管理体系中体现开源软件规范使用的相关要求。进一步地，对于企业内部的不同业务线和需求链的特殊需求，如游戏业务、云服务等，也需要单独设计相应的合规执行方案。

- **设立专门的开源管理办公室来统一协调，构建技术人员、法务人员以及外部律师的沟通渠道。**一方面，技术人员需要接受内部的开源合规培训，增强开源合规意识。具体合规流程上需要满足以下几点要求：一是技术人员在使用开源软件前需经过合规团队或法务团队的审核与批准，避免出现随意使用未经评估的开源软件的情况；二是在某一场景下使用开源软件获得批准，并不代表所有场景都获得了批准，开源合规审核需要“一事一议”；三是所有软件在对外发布前都需要经过合规团队或法务团队的审核与批准，以确保软件产品在对外发布前已履行开源许可证的要求；四是在产品更新迭代时，要对新引入或者发生变化的开源软件重新进行审核与批准。另一方面，内部法务团队可以编制“开源许可证权利义务速查表”，并与技术人员准确沟通使用场景，根据技术团队提供的使用信息，结合具体的开源软件许可证，具体分析评估风险并提出合规方案。适当地，企业可以引入外部律师来把控开源软件使用风险。

- **充分利用 Black Duck 等软件成分分析工具协助开源风险管理。**企业可以根据自身需求设定可接受的安全漏洞等级，通过第三方分析工具获得漏洞清单以及代码库中的许可证信息后，及时对漏洞进行归纳和梳理，并对技术人员进行安全漏洞培训。如果识别出的安全漏洞尚未被收录，技术人员可以根据采用业界普遍使用的 CVSS（Common Vulnerability Scoring System）标准开展安全漏洞评估[19]，避免使用高风险的开源软件。

三、合规风险防范下的未来展望

开源近年来的飞速发展，除了得益于科技的进步之外，开源本身“开放”的底层理念也起到了重要作用。开放而分散的开源社区能够吸引来自全球各地的志同道合的开发者与普通用户，通过协作与迭代的方式不断地优化产品，而优质的产品进一步对外产生影响力与吸引力，使社区进一步壮大，如此形成良性循环。

近期大热的 Web 3.0 与 DAO 理念也为开源未来的发展方向提供了另一种可能。开源本质上的“开放式协同合作”与 Web 3.0 和 DAO 理念本质上非常契合，均是寻求一种去中心化的开放合作机制。Web 3.0 下企业已经不必再拘泥于以前的商业模式，最终用户能够与发起人在激励机制中协调一致，这与开源软件发起人和贡献者甚至用户之间的协作方式是非常相似的。在去中心化的世界里，开源软件源代码的“透明性”也能够带来更多的信任。随着科技与理念的不断更新与完善，开源的未来发展充满了令人向往的畅想与期待。

然而，这些畅想与期待离不开对途中各类风险的严格防范。若不能妥善处理开源的相关风险，企业的发展也将失去合规这一稳固的基石。在开源生态未来的发展道路上，汉坤将始终专注于为各类疑难法律问题提供有效的解决方案，助力企业的平稳运行。

[19] 参见 https://www.first.org/cvss/calculator/3.1。

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