

开源软件与法律探析导读

作者：贾媛媛 籍婷 丁畅 王聪睿子

引言

随着计算机、互联网技术的迅猛发展，人工智能、大数据、区块链、云计算、网络安全等新兴数字产业不断涌现，对专业计算机软件的需求显著增加。因开源具备开放、平等、协作、共享的特点，开源模式已经成为全球软件技术和产业创新的主导模式。全球97%的软件开发者和99%的企业使用开源软件[1]，开源软件已经成为软件产业创新源泉和“标准件库”。

与此同时，开源软件相关的合规问题及相关法律纠纷也不断涌现。然而开源软件所涉及的法律问题较为前沿，国内外的司法判例较少，企业在前期往往未予以足够重视，导致后期产生纠纷而影响正常的生产经营。为了帮助企业更好地了解开源软件相关的法律风险，我们将陆续发布开源软件系列文章，介绍开源许可证的类型、具体内容、重点条款解析、典型法律问题，并为企业提供开源合规建议和指引。在本文中，我们将对开源、开源许可证的相关概念、法律性质、以及相关知识产权风险等内容进行介绍。

一、开源的基本概念

1. 开源是什么？

开源一词最初是指开源软件（Open Source Software）。开源软件是可以获取源代码的计算机软件，用户可以查看、修改和分发他们认为合适的代码[2]。

2. 开源软件与闭源软件的区别

在开源软件出现前，绝大多数的商业软件都是专有或闭源软件，即源代码处于保密或封闭状态，且严格限制用户修改、复制或分发软件的权利。彼时的软件漏洞修复和功能更新只能由软件公司完成，从而导致各类软件的迭代与创新进度缓慢。

在这种背景下，乐于推动技术与软件发展的开发者发起了自由软件运动（Free Software Movement），随着相关运动的不断发展与壮大，作为继承“自由”理念和顺应商业需要的结合体，开源软件产生了。如今的开源软件是指依据开源协议进行源代码公开的计算机软件，在开源协议中，开源软件的版权所有者可授予用户查看、修改、复制并向他人分发表开源软件的权利。

3. Free是免费的意思吗？

在很长一段时间内，开源软件都被贴上了“Free Software”的标签。“Free”一词造成了大量困惑，人们会天然将其理解为免费的意思，但实际上，“Free”一词代表可以“自由”使用，而非免费使用。

就此，相关开源协议在协议条款中对该误解进行了澄清。例如，GPL3.0协议包含以下声明：“When we speak of free software, we are referring to freedom, not price.”由此可见，“Free”是指公众复制、修改和发行软件的自由，而非意味着免费。实际上，开源软件的开发商能够利用开源软件进行不同形式的盈利，常见的盈利方式包括开源软件许可、提供技术服务、软硬件结合售卖等，“免费软件实际上可能比付费软件更贵”[3]。

二、开源许可证

1. 什么是开源许可证

开源软件允许用户自由复制、修改和分发源代码，但有些情况下，用户在对源代码进行修改或者将其与自己开发后的软件相结合后，将其封装成闭源的商业产品进行销售。这不仅损害了开源软件贡献者的权益，也与开源软件的自由开放的初衷

背道而驰。在此背景下，开源许可证应运而生，用来保护开源贡献者的权益，以保证开源软件自由传播的延续性。

通常，开源软件的权利人在发布该开源软件时，会根据需要选择特定的开源许可证，并要求该开源软件的使用者按照该开源许可证所列出的条款进行后续的复制、修改和分发。目前，较为常见的开源许可证多达20余种，各开源许可证均根据不同的适用场景规定了不同的条款，例如LGPL许可证主要针对库的使用，AGPL许可证主要针对网络服务。

开源许可证的条款主要包括两方面内容：一方面是规定开源软件使用者的权利，即，可以使用的范围，如复制、修改、使用、分发等；另一方面是规定了开源软件使用者应当承担的义务，包括开放源代码的义务、提供版权声明的义务等。

2. 开源许可证的法律性质

在我国的司法实践中，一些司法案例和专业文章中，倾向于认定开源许可证属于附解除条件的著作权合同。例如：

- 罗盒vs.玩友一案[4]中，广州知识产权法院认定，“GPLV3协议属于附解除条件的著作权合同。许可条款是版权许可的条件，如果用户违背条款规定，那么许可的前提条件已不复存在，则GPLV3协议终止适用，用户获得的授权也将自动终止”。
- 《开源协议适用范围及其对软件著作权侵权判定的影响》一文[5]中，最高人民法院罗瑞雪指出，“开源协议是软件著作权人将其复制权、发行权、修改权等附条件地许可给不特定公众的著作权许可使用合同”。

国外的司法实践中也基本认可开源许可证的著作权许可合同属性，例如：

- 德国Welte诉D-Link一案[6]中将GPL协议认定为附解除条件的合同，其中许可使用条件为解除条件，当被许可人未按许可使用条件使用时，合同解除、终止授权，被许可人继续使用则构成侵权。
- 在美国，虽然开源许可证的法律性质存在争议，但基本也都承认开源许可证具有著作权许可合同属性。例如Jacobsen v. Katzer一案[7]中，加州北区地区法院认为，由于权利人通过开源项目提高了其知名度，可以被认为是开源许可证的对价，因此构成许可协议，超过许可证部分的使用构成著作权侵权。

3. 开源许可证的分类

开源许可证通常被分为宽松式许可证（permissive license）和著佐权许可证（copyleft license）。常见的宽松式许可证包括MIT、BSD、Apache 2.0等，常见的著佐权许可证包括GPL V2.0/3.0、AGPL、SSPL、LGPL等。

开源许可证还可根据是否被OSI（Open Source Initiative 开放源代码促进会）认可而进行分类。常见的被OSI认可的许可证包括GPL V2.0/3.0、Apache 2.0、MIT、BSD、AGPL等，未被OSI认可的许可证包括SSPL等。

另外，除了上述针对软件的开源许可证，随着近些年来人工智能、云计算和大规模预训练模型的迅猛发展，也陆续产生了若干针对模型参数、权重和数据的开源许可证并且越来越受到关注，例如，LLaMA LICENSE AGREEMENT、BigScience RAIL License V1.0[8]等。

4. 开源许可证的传染性条款

在开源许可证所规定的众多条款中，最受关注、也是对企业影响最大的可能就是传染性条款。传染性条款是指使用某一许可证的开源软件，基于该开源软件创作的后续作品的部分或全部都应当同样进行开源。

在实践中，企业往往会在开源软件的基础上，投入大量人力、物力来进行进一步开发，生成与自身的服务或产品相关的定制化软件，这些后期开发的定制化部分则成为企业的核心竞争力，往往作为技术秘密来保护。一方面，如果按照传染性条款的规定，企业需要公开后期开发的源代码，可能会导致企业失去竞争优势，也可能导致企业提供的服务或产品受到第三方的恶意篡改和破坏；另一方面，如果使用开源软件的企业未遵循传染性条款的要求公开软件的源代码，则可能引起开源合规问题或者导致著作权侵权，使企业陷入两难的境地。因此，对于企业来说，在选择使用某款开源软件时，需要深入理解相应的开源许可证的要求，明确所需满足的开源义务，并尽早制定应对策略，以尽量满足传染性条款的要求，同时对企业的核心代码采取合理的保护措施。

传染性条款举例：

- GPLv2许可证规定“将衍生自本程序或其任何部分的任何作品，若进行任何发行或者发布，则作为一个整体免费许可给所有第三方”。GPL仅对通过传统模式分发代码的行为进行了规制，而没有限制通过云服务使用开源软件也需要满足开源义务。因此，AGPL弥补了这一漏洞。
- AGPL规定“如果您对本程序进行了修改，则需要向所有通过计算机网络与本程序的修改版本进行远程交互的用户免费提供相应的源代码”。
- 另外，针对类库引用的LGPL许可证、针对SaaS使用的SSPL许可证等，也有相应的传染性条款。

三、使用开源软件的知识产权风险

由于开源软件的专业性和复杂性，涉及较为前沿的法律问题，国内外的司法实践中涉及开源软件的司法判例相对较少，使得在实际引入开源技术的过程中，企业往往易忽视开源合规的重要性，从而给自身带来知识产权法律风险。下文中将主要介绍使用开源软件涉及的知识产权风险，以供企业了解和参考。

1. 著作权侵权风险

目前，涉及开源软件的著作权侵权风险主要是由违反开源许可证要求而引发的。如前文所述，开源软件权利人在发布开源软件时往往都选择一个开源许可证，用于规定该开源软件的使用范围、许可权利和许可义务。从法律性质的角度，开源许可证可以视为“附条件解除的著作权许可合同”[9]。若用户（也即开源软件使用者）未遵循开源许可证要求提供源代码、安装信息、标注版权信息和修改声明等，则用户违反了开源许可证的条件，将导致授权人与用户之间的著作权许可合同自动解除，用户基于许可证获得的许可即时终止[10]。若用户继续使用相关开源软件，则构成著作权侵权或违约[11]。

另外，若用户在使用过程中违反了各开源许可证的兼容性要求，也可能会因违反开源许可证而引发著作权侵权问题。关于开源许可证的兼容问题，我们将在后续的文章中详细论述。

近年，国内外涌现出的涉及开源协议的司法判例，主要以因违反许可证要求而引发的著作权侵权案件为主。例如：

- **罗盒vs.风灵**一案[12]中，原告罗盒独立开发了涉案软件“罗盒”插件化框架虚拟引擎系统V1.0，并在GitHub上公开了涉案软件的源代码，附加了LGPL3.0开源许可证，后续又将许可证变更为GPL3.0。被告风灵违反开源许可证的要求，使用了附带GPL3.0协议的开源代码，却拒不履行GPL3.0协议规定的使用条件。因此，深圳市中级人民法院认定“根据GPL3.0协议第8条自动终止授权的约定及《民法总则》第一百五十八条的规定，被告福建风灵公司通过该协议获得的授权已因解除条件的成就而自动终止。被告福建风灵公司对VirtualApp实施的复制、修改、发布等行为，因失去权利来源而构成侵权”。
- **罗盒vs.玩友**一案[13]中，被告玩友的涉诉侵权软件中使用了附带GPL3.0协议的开源代码，却未遵循许可证向用户开放源代码，广州知识产权法院认定被告玩友的上述行为违反了开源许可证。对此，权利人存在违约救济和侵权救济两种方式。在原告罗盒主张侵权救济的情况下，广州知识产权法院认定被告玩友的行为侵害了原告罗盒涉案软件的信息网络传播权。
- **Artifex Software, Inc.诉Hancom, Inc.**案[14]中，被告Hancom公司出售的Office软件程序中，使用了Artifex公司所开发的附带AGPL、商业双许可的Ghostscript工具，却未遵循许可证开放修改的源代码，也未支付商业许可费。对此，Artifex将Hancom起诉至美国加利福尼亚北部地区法院，最终法院认定，Hancom未获得商业许可协议，视为其同意AGPL许可协议条款，认定被告既构成版权侵权，也构成合同违约。
- **Free Software Foundation诉Cisco System, Inc.**案[15]中，Cisco在其Linksys路由器的内置软件中使用了基于GPL和LGPL的开源代码，却拒绝公开源代码。对此，Free Software Foundation将Cisco诉至美国纽约南区联邦地区法院。最终双方达成和解，Cisco支付一笔费用并且承诺公开源代码。

除了因违反开源许可证而引发著作权侵权的情形之外，有些专业文章也提到了因开源软件本身含有侵权代码而导致后续使用行为亦构成侵权的情形[16]。具体来说，对于开源软件来说，参与开发的贡献者往往人数众多。由于开源软件的发布并未要求贡献者只能上传其享有权利的代码，且贡献者也不承担瑕疵担保责任以及保留著作权标记。因此，实践中，一个开源软件中

可能会存在部分侵权代码，例如从第三方不当获取并披露的代码，这种情形下，即使用户完全遵循开源许可证的要求，可能导致侵犯第三方著作权的责任。目前，笔者并未发现有代表性的权威司法判例，故此处仅简单介绍，并不做深入探讨。

2. 专利侵权风险

使用开源软件的专利侵权风险主要包括来自开源软件权利人的专利侵权风险和来自第三方专利权人的专利侵权风险[17]。

来自开源软件权利人的专利侵权风险指的是，开源软件的著作权权利人同时持有某项专利，且该专利所保护的技术方案可以通过运行相应开源软件而实现。这种情况下，开源软件的权利人也可能依据该专利向开源使用者发起专利侵权诉讼，即便开源软件使用者遵循开源许可证的要求而不构成著作权侵权。例如，部分开源许可证（如BSD、MIT等）没有相关的专利条款，也即没有强制授予专利许可和禁止提起专利主张的条款，开源软件权利人可以向开源代码使用者提起专利诉讼并收取专利许可费。

来自第三方专利权人的专利侵权风险指的是，第三方专利权人，其并不是开源软件的贡献者，不受开源许可证的约束，依据其持有的专利向开源使用者发起专利侵权诉讼。例如，2010年3月美国苹果公司诉HTC案中，苹果公司在美国特拉华联邦地区法院分别以两份诉状，起诉HTC基于安卓操作系统的手机侵犯其专利权，涉案专利共计22件，包括手机的使用界面、系统基础架构及硬件等技术。2012年11月，HTC和苹果公司达成全球性和解，撤销当前所有诉讼，并签署为期10年的许可协议[18]。

3. 商标侵权风险

使用开源软件的商标侵权风险主要包括假冒和反向假冒两种。

假冒，指的是开源软件的使用者未经授权擅自使用开源软件权利人的商标进行宣传，导致商标侵权。与著作权和专利不同的是，大部分开源许可证不会授予开源软件使用者商标许可[19]。因此，若开源软件的使用者未经许可使用开源软件权利人的商标，可能导致商标侵权风险。

反向假冒，指的是开源软件使用者未经权利人同意擅自用自己的商标替换权利人的商标，导致商标侵权。具体而言，实践中，许多企业意图避免商标假冒带来的侵权纠纷，简单地去掉开源软件中权利人的商标，加上自己的商标集成到新发布的版本中，这可能导致反向假冒的商标侵权。

4. 商业秘密泄露风险

如上所述，涉及开源软件的商业秘密风险，主要是指受开源许可证传染性条款的影响，用户为了不违反开源许可证而被迫公开其后期开发的源代码[20]，而这些后期开发的源代码满足秘密性、保密性和价值性的要求，原本是可以作为商业秘密保护的。常见的传染性较强的开源许可证包括：GPL V2.0/3.0, AGPL, SSPL等。在实践中，当开源软件的权利人发现用户违背开源许可证的要求未公开源代码时，可能会通过发送律师函、在公开渠道进行指责或直接向法院起诉的方式，要求用户公开源代码[21]。

此外，开源软件的使用者也可能因开源软件自身的技术缺陷[22]，导致自己的商业秘密被泄露。如前文所述，对于开源软件来说，参与开发的贡献者往往人数众多，且贡献者并不承担瑕疵担保责任。因此，开源软件中可能存在恶意代码、电脑病毒、安全漏洞等。若用户引入了上述开源软件，需要对该软件进行安全性测试，以避免因开源软件的技术缺陷而产生的商业秘密泄露风险。

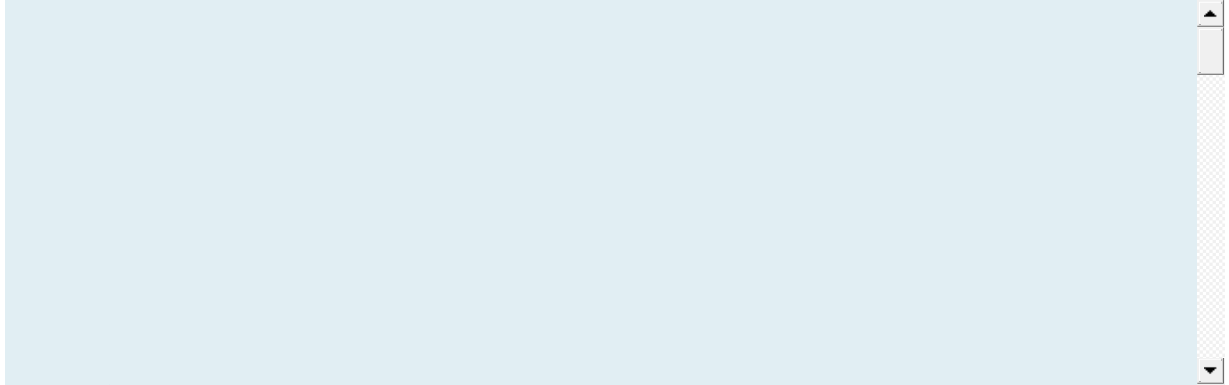
另外，在实践中，企业的员工擅自将含有后期开发的代码上传到共享网盘、开源社区的情况也屡见不鲜，也会导致商业秘密泄露[23]。因此，建议企业对其开发的代码加强保护以及对能够接触到代码的相关人员进行培训和监督。

结语

十四五规划中提出“加快繁荣开源生态、建设开源社区……培育重点开源项目，例如互联网、云计算、大数据、人工智能、自动驾驶、区块链、操作系统等领域”，开源技术的重要价值日渐凸显。

然而，开源软件本身的专业性和复杂性，且其所涉及的法律问题较为前沿，相关法律法规的出台存在滞后性，我国的司法案例相对较少，许多企业对开源软件的法律风险缺乏足够认识，在使用开源软件的过程中未对开源合规问题予以足够重视，加之国际形势的影响，国内外开源软件开发商对国内企业提起的维权行动越来越多，尤其在企业融资、IPO上市的关键时机，给企业带来巨大损失。

与其亡羊补牢，不如未雨绸缪。笔者希望通过本文，帮助企业更好的了解使用开源软件的注意要点及相关法律风险，以尽早制定合规策略，及时进行合规核查和整改。我们将在后续的文章中持续介绍开源许可证的类型、具体内容、重点条款解析、典型法律问题、并为企业提供合规建议和指引。



*本文首发于知产力

2023-11-13