

算法模型开发的知识产权与安全

作者：杨迅 | 任家谊

近年来金融行业逐渐加强对算法开发，身份识别、智能风控、智能营销、智能客服、智能合规、智能运营六大场景已经实现在银行、保险、证券三个领域全覆盖。中国人民银行 2021 年发布的《人工智能算法金融应用评价规范》以及全国金融标准化技术委员会发布的《移动终端支付可信环境技术规范》《云计算技术金融应用规范》《移动金融基于声纹识别的安全应用技术规范》等文件，明确了相应的技术规范及标准，并引入事前准入、事中监管的方式，为金融行业合规提供了评价规范，有助于金融行业实施好对金融智能算法的风险管理。目前，许多金融机构均设置了专门的技术部门或组建专业团队投入到算法的研发中，创造了相当高效实用的高频算法模型。根据银保监会统计，2020 年银行机构和保险机构信息科技资金总投入分别为 2078 亿元和 351 亿元，同比增长 20% 和 27%¹。

与此同时，算法及算法模型开发本身的知识产权保护成为一个需要关注的问题，具体体现为：算法应如何获得知识产权保护以及如何防范算法模型开发过程中的知识产权风险。

第一部分 算法模型的知识产权保护

由于金融机构的人员变动较为频繁，参与模型开发的技术人员、业务人员，在各个基金公司之间的频繁跳槽，可能导致一家公司正在开发中或开发完毕的算法模型随着人员流动而为其竞争对手所掌握。更有甚者，部分人员在跳槽时带走了原公司开发的软件代码，导致真正投入经费开发的原公司，竹篮打水一场空。于是，用知识产权手段保护算法、算法模型和相应的代码，成为金融机构积极探索的问题。

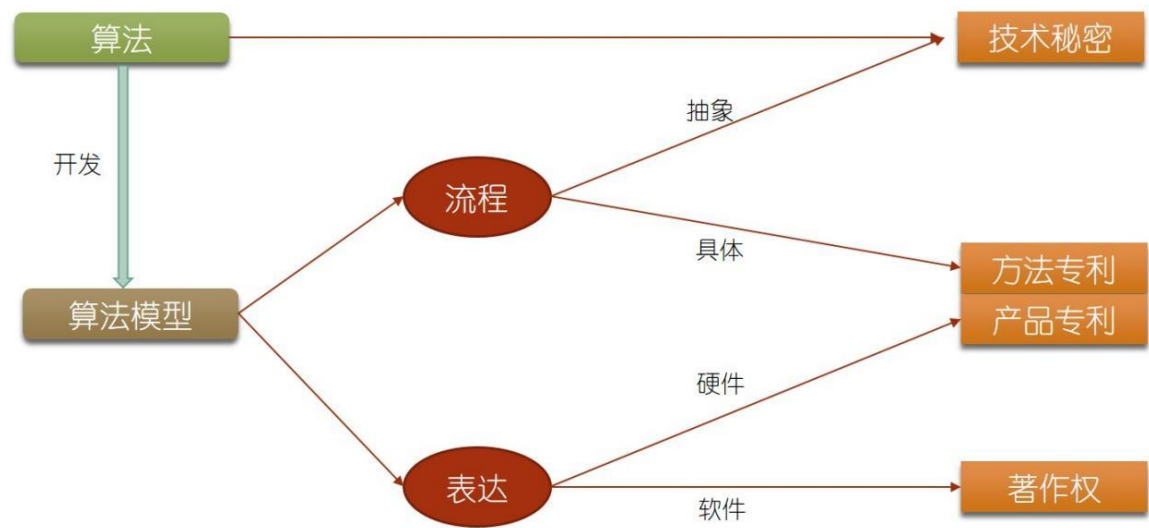
.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

¹ 《金融人工智能研究报告(2022 年)》中国信息通信研究院云计算与大数据研究所人工智能关键技术和应用评测工业和信息化部重点实验室 2022 年 1 月 <http://www.caict.ac.cn/kxyj/qwfb/ztbg/202201/P020220118401482734472.pdf>

一、不同阶段和形式的算法模型的知识产权保护

针对算法具体化的不同阶段(从抽象到具体)以及根据算法的表现形式(流程、软件和硬件), 可以采取不同的知识产权手段保护。不同阶段和形式的算法模型简图如下:



二、处于抽象阶段的算法

算法是一组定义明确的程序或指令, 通常用于解决复杂问题或完成任务。就某项投资或者资产管理任务创建一个算法时, 这个算法可能表现为公式、函数、函数组合。这时的算法, 因其仅表现为抽象概念, 还属于思想的范畴。而《中华人民共和国著作权法》(以下简称“《著作权法》”)保护的是作品的表达, 并不延及思想。从专利角度看, 人类“智力活动的规则和方法”亦不是专利保护的主题事项。因此, 抽象阶段的算法目前无法获得专利或著作权的保护, 只能探索被作为商业秘密保护的可能。

算法作为技术信息, 能够为公司带来价值, 且一般均在隐秘状态中不为公众所知悉, 如果企业采取合适的保护措施, 其可以作为商业秘密受到相关法律保护。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》第一条²第一款规定: “与技术有关的算法、数据、计算机程序及其有关文档等信息, 人民法院可以认定构成反不正当竞争法第九条第四款所称的技术信息。”处于隐秘状态的投资模型的算法就属于《反不正当竞争法》第九条第四款规定的商业秘密。

司法实践中, 已有将算法作为商业秘密保护的案例, 具体阐释了算法作为商业秘密被保护的范围, 尤其是与公知领域知识的区别。在深圳市智搜信息技术有限公司诉光速蜗牛(深圳)智能有限公司侵犯

² 《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》第一条与技术有关的结构、原料、组分、配方、材料、样品、样式、植物新品种繁殖材料、工艺、方法或其步骤、算法、数据、计算机程序及其有关文档等信息, 人民法院可以认定构成反不正当竞争法第九条第四款所称的技术信息。与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息, 人民法院可以认定构成反不正当竞争法第九条第四款所称的经营信息。前款所称的客户信息, 包括客户的名称、地址、联系方式以及交易习惯、意向、内容等信息。

商业秘密纠纷案中，法院指出：“以模型选择优化作为核心的算法，即使所采用的模型均为公知信息，但若模型的选择与权重排序需通过大数据的收集、处理和测试等，该算法应视为不为所属领域相关人员普遍知悉和容易获得的信息，不为公众所知悉并可能构成权利人的商业秘密。”可见，虽然某些具体的函数关系、模型可能处于公知领域，但如果算法对这些函数、模型的选择，或者参数的设定，是不为公众所普遍认知的，那么算法本身仍然可以作为商业秘密被保护。

三. 具体的算法模型

当一定的算法具体化，与特定的数据集相结合，就形成了算法模型。算法模型是一组定义明确的指令，它们接受某些输入、操纵并产生输出。换言之，一个具体的算法模型，不仅仅是一个公式或者公式组合，它与特定的数据集相结合，呈现出一定的方法。比如，在投资领域，算法模型需要确定获得信息的来源、处理信息的方式、以及数据的输出。

算法模型可以有两种表现，一种是流程，另一种它的表达形态。

1. 算法模型作为流程的保护

从流程角度来说，算法模型表现为一种方法，具体包括：从哪里获得数据、经过怎样的分析处理、达到怎样的结果以及解决怎样的问题。当这个流程处于相对抽象的阶段，那么其本质和算法差别不大，仍然以商业秘密作为主要的保护方式。

如果作为流程的算法模型足够具体化，能够形成一项技术方案，那么，它就可能成为一项商业方法，成为专利的保护对象。《中华人民共和国专利法》(以下简称“《专利法》”)第二条³规定“发明，是指对产品、方法或者其改进所提出的新的技术方案。”据此，专利保护的技术方案，可以分为产品专利和方法专利。产品专利主要对有形的物质产品、新产品的形状或构造做出专利保护，其技术方案可以申请发明，也可以申请实用新型；而方法专利通常是指制造产品的工艺、流程，方法类创造只能申请发明，不能申请实用新型。

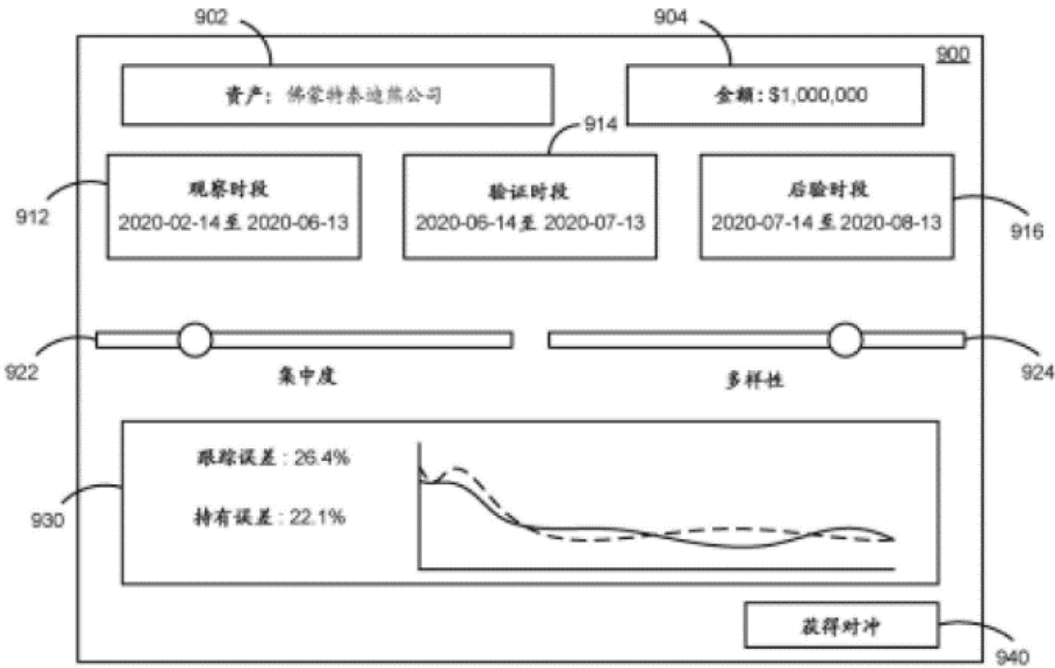
商业方法可以是《专利法》所保护的技术方案，是方法专利保护的對象。2017年4月1日修订的《专利审查指南》第二部分第一章第4.2节第(2)项新增一段：“涉及商业模式的权利要求，如果既包含商业规则和方法的内容，又包含技术特征，则不应当依据专利法第二十五条排除其获得专利权的可能性”。

能够获得专利保护的商业方法，必须是具体的，且与一般商业惯例具有显著区别特征的方法，其往往体现为一种解决某个特殊问题的技术方案。最高人民法院(2021)最高法知行终 382 号行

³ 《中华人民共和国专利法(2020 修正)》第二条本法所称的发明创造是指发明、实用新型和外观设计。发明，是指对产品、方法或者其改进所提出的新的技术方案。实用新型，是指对产品的形状、构造或者其结合所提出的适于实用的新的技术方案。外观设计，是指对产品的整体或者局部的形状、图案或者其结合以及色彩与形状、图案的结合所作出的富有美感并适于工业应用的新设计。

政判决指出：“在判断一件专利申请是否构成技术方案与一件专利申请是否具备创造性时，……前者主要考察方案的手段集合与要解决的问题之间是否体现受自然规律约束的关系，后者则主要考量方案的手段集合与要解决的技术问题对本领域技术人员而言是否显而易见。……判断包含非技术特征的发明专利是否属于专利法保护的技术方案时，考查该发明是否仅仅在形式上具备技术特征、其非技术特征如算法特征或商业规则和方法特征等是否仅仅属于利用计算机实现的常规规则和方法等……”可见，一项算法模型，如果要作为商业方法专利获得保护，其必须是一项具体的商业解决方案，具体内容上不能是已知算法、商业规则的简单重复或计算机代码形式的重现，而需要对现有技术解决方案具有某种程度上的突破。在投资领域，一些量化投资模型就不能仅仅体现在用计算机程序重现传统的投资方式，而必须是借助计算机的性能，对现有投资解决方案的突破。

比如，美国高盛公司获得授权的“基于正则化的资产对冲工具”的专利(见下图)，不仅仅是传统资产对冲配置代码化的反映，还是经过训练的正则化工具，其突破了传统对冲配置计算方法的诸多弊端。



2. 算法模型作为表达的保护

算法模型的另一个层次是表达，即算法模型以某种特定的形态具体化，形成产品。算法的表达包括两个类型：一个是硬件的表达，一个是软件的表达。从硬件表达来说，它通过一些机器设备实现商业流程，该等设备可能受到产品专利的保护，更常见的是，模型最后以计算机软件代码的形式表现，此时，软件的形式可受到著作权的保护。通常，软件一经创造就能自动获得著作权保护，不过，如软件完成著作权保护中心的登记，将能获得更好、更强的保护。

第二部分 算法模型开发中的知识产权风险防范

当确认算法模型受到知识产权保护之后，随之而来的问题即是：如何确定算法模型知识产权的归属？尤其是在算法模型开发过程中，如何确保公司将拥有相关算法模型的知识产权，以及如何防范知识产权风险。

一. 知识产权归属

算法模型的开发通常有两种形式：一种是委托开发，一种是内部开发。

委托开发指的是一方单位提出研究开发任务，由其他单位进行研究开发，完成发明创造。根据《民法典》第八百五十九条的规定，“委托开发完成的发明创造，除法律另有规定或者当事人另有约定外，申请专利的权利属于研究开发人。研究开发人取得专利权的，委托人可以依法实施该专利。”《专利法》和《著作权法》也有类似规定。

换言之，如果没有相反约定，纵然委托开发的企业提供了开发资金，所开发的算法模型的相关知识产权归属于受托人。这也意味着，在一般情况下，如委托人希望其委托开发成果的知识产权归属于自己，则委托开发合同必须载有开发知识产权归属的条款，确保该等知识产权归属于委托人。

内部开发指的是在公司内部组成一个开发团队，由这个团队来根据公司特定的需求开发算法模型。根据《专利法》和《计算机软件保护条例》的规定，通常而言，以专利或软件著作权形式存在的知识产权，只要是基于员工与公司的劳动关系而产生的，专利和软件著作权均属于公司。

不过，算法模型的表现形式，可能不仅仅是专利或受著作权保护的软件作品，比如算法模型可能有一些说明性的文档，这些说明性的文档相关的著作权在《著作权法》的默示规定中，就并不当然归属于公司。因此，对公司而言，更加安全的做法是：在相关开发人员的劳动合同中，或在专项开发任务的有关协议中，特别约定知识产权的归属，即，在该等协议中约定有关知识产权归属公司或者由员工承诺转让给公司。

二. 知识产权风险防范

合同文本上的知识产权归属，并不能完全保障公司全面、现实地掌握开发成果的知识产权。例如，虽然有的公司在纸面上要求开发人员把软件著作权和其他相关知识产权转让给公司，但实际上源代码一直为相关开发者所实际掌握，开发者离职之后，自然而然地将源代码带去新公司。纵然，理论上原公司拥有了该算法模型的知识产权，但却难以举证该模型到底是什么。

这就要求公司建立严谨的开发流程。在开发过程中间，将源代码的备份作为必须的工作步骤。一方面，让公司能够及时掌握开发的进程以及开发的源代码，避免员工突然离职造成的损失；另一方面，日常对软件开发过程的备份，本身也是企业独立开发的证明，能够在一定程度上对抗可能发生的“商业秘密”或“著作权”侵权指控。

此外, 对于开发的流程管理, 还需要防止对软件的污染。具体方式则为对开发行为的管控, 比如, 禁止开发人员从第三方获取来历不明的、知识产权属性不明的第三方代码, 以及许可证与商业目的相冲突的开源代码, 以减少或防止最终产品的污染或侵权风险。

如您希望就相关问题进一步交流，请联系：



杨 迅

+86 21 3135 8799

xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: LlinksLaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2023