

科技型企业的商业秘密保护

作者：贾媛媛 陈耀文 王聪睿子

前言

近年来，随着知识产权法律体系建设的逐步完善，我国法院对商业秘密采取“**强保护**”措施，尤其对员工“**跳槽**”带走商业秘密或通过“**挖角**”而不当获取商业秘密的行为进行严厉打击。2020年12月，南京市中级人民法院在“科达”案中判决安徽科达等公司赔偿原告江南环保公司**9600万**人民币，并召开发布会通报此案^[1]。2021年2月，最高人民法院发布了我国商业秘密侵权案史上最高判赔额的“香兰素”案二审判决，支持了原告主张的**1.59亿**损害赔偿并在判决中释明原告可另案主张**惩罚性赔偿**。同时，最高院判令**被告公司**及其**法定代表人**承担连带责任，并认为被告已涉嫌构成**刑事犯罪**，相关线索将移交公安和检察机关^[2]。

随着科学技术的快速发展和科技型人才的快速流动，科技型企业的核心技术人员离职后创业或加入新单位已成为引发商业秘密纠纷的主要情形，科技型企业在对对外进行技术合作或技术许可时，也经常因未妥善保护商业秘密而发生纠纷。一旦产生纠纷，对科技型企业、涉案员工、新单位、技术合作方和许可方，均可能产生重大影响。同时，监管机构、投资人和合作方也会越来越关注科技型企业是否存在商业秘密侵权风险。

综上所述，科技型企业如何合理有效地保护自己的商业秘密、员工于在职期间以及离职时应如何避免侵权，单位在引入技术人才时又应采取哪些措施来避免侵权，都是需要从业者密切关注的问题。本文将在介绍商业秘密相关规定及司法实践的基础上，对这些问题进行探讨。



一、商业秘密案件的司法审判要点

通常，人民法院在审理商业秘密侵权案件时，审理要点包括商业秘密范围、商业秘密权属、侵害商业秘密的行为、责任承担等要件。同样，企业也需要关注司法审判要点，并围绕审判要点进行商业秘密保护制度建设，以避免可能的纠纷或在出现纠纷后进行有效应对。本文结合上述审判要点来梳理和分析企业商业秘密合规中需要注意的事项。

1. 商业秘密的范围

众所周知，专利侵权诉讼中专利权的保护范围需以权利要求书所限定的范围为准。因此，专利的保护范围相对清楚和明确。同时，专利经过国家知识产权局的审查，专利文本和权利人均向大众公示，并以公开换保护。但对于商业秘密而言，在产生纠纷之前，由于商业秘密的秘密属性，公众无法得知其全部内容，也没有经国家机关确认的、具有公示效力的文本对其范围和权利人身份予以明确。因此，在商业秘密侵权案件中，一个重要的环节就是明确商业秘密范围。在这个过程中，通常首先由原告对商业秘密进行主张，人民法院在原告主张的基础上审查其主张的秘密点是否符合商业秘密构成要件。

商业秘密的类型有技术信息、经营信息以及其他商业信息，其具体范围包括^[3]：

- **技术信息**：包括与技术有关的结构、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。
- **经营信息**：主要包括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。

实践中，在上述商业秘密类型的基础上进一步明确商业秘密内容则需要更为复杂的梳理和判断过程。例如，对计算机程序类商业秘密，原告需说明计算机程序中的哪些内容、环节、步骤构成商业秘密。商业秘密范围的界限通常较为模糊，当事人争议较大而确认过程相对复杂，需要多次修改、释明、举证、质证。而如果庭审中最终无法确定商业秘密范围，权利人则将可能面临被驳回起诉的不利结果。

在原告明确商业秘密范围的基础上，人民法院则会进一步审查原告主张的信息是否满足商业秘密的“三性”，即保密性、秘密性及价值性^[4]。

- **保密性**是指被诉侵权行为发生以前应当采取必要的“保密措施”。如果是在被诉侵权行为发生后采取的保密措施，则不满足保密性要求。

- **秘密性**是指涉案信息在被诉侵权行为发生时应当“不为公众所知悉”，即公众通过公开资料或公开渠道无法得知。若某一信息仅涉及产品的尺寸、结构、部件的简单组合，所属领域的相关人员通过观察上市产品即可直接获得，则不满足秘密性要求^[5]。

- **价值性**是指涉案信息具有现实或潜在的商业价值。实践中认为只要能够为原告带来竞争优势，即具有价值，如实验数据、产品调试报告，乃至失败的实验数据等阶段性成果，如果能够为他人提供借鉴参考，亦可能被认为具有价值性^[6]。

2.商业秘密的权属

根据实践中常见的权利来源方式，原告可以是商业秘密的权利人或利害关系人^[7]。

权利人是技术秘密和经营秘密的开发者，或者受让人、继承人、权利义务的承继者等。

利害关系人一般为商业秘密的被许可人。但需注意，不同的被许可人具有的诉权不同，具体为：

- 独占使用许可合同的被许可人可以单独作为原告提起诉讼；
- 排他使用许可合同的被许可人可以和权利人共同提起诉讼，或者在权利人不起诉的情况下自行提起诉讼；
- 普通使用许可合同的被许可人可以和权利人共同提起诉讼，或者经权利人书面授权单独提起诉讼。

3.侵犯商业秘密的行为

根据《反不正当竞争法》，侵犯商业秘密行为主要表现为以下形式^[8]：

- 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；
- 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；
- 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；
- 教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密；
- 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。

根据笔者日常处理此类纠纷的经验，对于科技型企业而言，常见的侵权形态包括：

- 离职员工违反保密义务，披露、使用或者允许其入职的新单位（或该员工自己成立的新公司）使用其所掌握的商业秘密；
- 离职员工擅自将原单位的商业秘密申请专利，导致该商业秘密被公开；
- 原、被告为同行业竞争对手，应当知悉某员工非法获取商业秘密，却仍从该员工处获取、使用涉案商业秘密；需要注意的是，即使仅仅非法获取，未对涉案商业秘密进行使用，仍然构成侵权。

4. 侵犯商业秘密应承担的责任

依据《反不正当竞争法》，侵犯商业秘密可能承担民事责任、刑事责任以及行政责任^[9]，具体如下。

- **民事责任：**民事责任通常包括赔偿损失和停止侵权，即不得披露、使用或允许他人使用其接触或获取的商业秘密。如涉案商业秘密与被告的核心业务直接相关，则被告将面临关闭产线，甚至停业的风险。而对于赔偿责任，法律不仅要求对权利人的损失进行“填平”，如果被告恶意侵权且情节严重，还可能面临1至5倍赔偿额的惩罚性赔偿。在“香兰素”案中，法院明确原告可以就《反不正当竞争法》生效之后的侵权行为另案主张惩罚性赔偿^[10]。
- **刑事责任：**如果权利人的损失数额或者被告的违法所得数额达到30万，侵权人或被控侵权方的实际控制人还可能被处以最高刑期为10年的有期徒刑^[11]。
- **行政责任：**权利人在遭遇侵权行为时，可以在有管辖权的监督管理部门就侵害商业秘密的行为进行投诉。行政机关有权对侵权证据进行固定、没收其违法所得并可处以10万-500万元的罚款^[12]。



二、科技型企业的商业秘密制度建设

1. 实务中存在的问题

基于上述司法审判要点并结合笔者在处理类似案件的实践经验，本文在阐述科技型企业的商业秘密制度建设之前，将科技型企业商业秘密的管理中出现的常见问题列举如下：

◇ 商业秘密保护制度不完善

在实务中，一些企业未建立完善的商业秘密保护制度，导致在发生纠纷之时或无法明确商业秘密具体范围、或无法证明已采取合理保密措施、或无法证明商业秘密权属以及涉案离职员工曾接触过涉诉的商业秘密。常见情形包括：

- 技术图纸、立项报告、客户需求、投标文件、代码等载体证据缺失、未署名或署名不规范、缺失完成时间等重要信息；
- 在许可、转让、合作开发或委托开发的情况下，对技术信息的归属未做约定或约定不清，对技术资料的交付情况未做记录或记录不明；
- 劳动合同、保密协议、竞业限制协议、离职/入职交接清单等文件对商业秘密的范围、保密义务等重要条款未约定或约定不清楚；
- 虽已就保密事项制定规章、制度、手册、通知文件等，但无法证明该等规章、制度、手册、通知文件已送达至员工

且员工已明确知悉具体内容；

■ 所采取保密措施的时间晚于侵权行为发生的时间；

■ 在集团或多个主体共有商业秘密的情况下，有部分主体没有采取合理的保密措施，从而导致涉案信息丧失保密性与秘密性。

◇ 保密意识薄弱

在实践中亦有企业已建立了较为健全的商业秘密保护制度，但因企业和员工的保密意识薄弱，不遵守相关规定，导致其商业秘密被公开。常见情形包括：

■ 企业为宣传目的，主动公开保密信息。如，主动将产品或图纸发布在官网上，或作为宣传资料进行分发；

■ 企业将技术秘密申请专利而导致公开；

■ 企业未对产品的内部结构采取技术措施，导致上市销售后公众可以通过简单拆解就能直接观察到内部结构信息；

■ 员工将商业秘密相关文档上传到私人邮箱、网络存储空间或公共论坛；

■ 员工将商业秘密卖给竞争对手；

■ 员工离职后自立门户或加入新单位，仍然使用原单位的商业秘密或将原单位商业秘密申请专利。

◇ 对司法审判现状缺乏了解

因商业秘密的构成要件较为复杂，侵权行为非常隐蔽，权利人的维权之路往往异常艰辛。据统计，2017年前侵害商业秘密案件中，原告的胜诉率低于15%^[13]。其中主要原因就包括原告无法明确其主张的商业秘密范围（即秘点），或者主张的秘点无法满足秘密性、保密性和价值性的要求。

实务中，一个较为常见的认识误区就是：将载体和秘点混为一谈。商业秘密的秘点指的是具有价值的技术信息或客户信息，而这种有价值的信息通常依附于某种具体载体之上，如以算法为客体的商业秘密依附于代码文件中、工艺流程依附于图纸及相关资料文档。在“香兰素”案中，权利人举证的技术秘密载体为300余张图纸，而其主张了6个秘点。

权利人首先应当收集记载有商业秘密的载体，如图纸、立项报告、客户需求、投标文件、代码等证据作为明确秘点的基础。但在实践中，权利人常因文件管理混乱而导致载体损毁或灭失，从而无法对载体进行举证。此外，对载体的信息进行概括和提炼以明确秘点是一项对技术和法律均要求很高的工作，经常有权利人因缺乏专业知识而无法明确秘点，建议委托专业的知识产权律师或鉴定机构进行该部分工作。

2. 科技型企业的商业秘密制度建设

围绕上述在商业秘密保护实务中存在的问题，我们建议着重从以下角度去建立和完善商业秘密保护制度。

◇ 合同约定

建议企业通过劳动合同、保密协议、竞业限制协议、离职交接清单等一系列合同文件，从不同角度、对不同员工的职位、职责范围、保密义务及保密信息内容进行明确约定，从而对保密信息的全面保护。需要注意的是，实践中需要根据企业和员工的具体情况“定制”合同内容，即对不同职位的员工及其所接触的商业秘密范围进行特别约定，避

免对所有员工使用统一的格式合同而造成部分条款被视为未约定。

◇ 规章制度

建议企业通过章程、制度、员工手册以及书面通知等方式，划定保密信息的范围以及员工的相应保密义务。同时，应当确保相关制度与规定已实际送达且被员工所知悉（例如通过邮件发送或者要求员工签收确认），并保存相应记录。

◇ 场所管理

建议企业对涉密场所与非涉密场所进行明确区分，并对进入涉密场所的人员范围、权限、程序、允许的行为进行明确限制。此外，企业应当注重对物理保护措施和硬件防护设备的布置，如在涉密场所设有标识、门禁、监控等。同时，还应当有专门的管理人员与监督人员对涉密场所的保密制度实施情况进行定期更新和核查。

◇ 文件管理

文件管理是根据文件的涉密级别进行文件标记、分类、加密、管理，以及对接触人员范围进行限制、对文件的保存、流转、查阅进行记录等管理制度。除了纸质文件外，随着电子化的普及，企业还应当重视对电子文件和数据的管理，包括对内部系统及云端服务器中电子文件的查阅、上传、下载等活动进行常态化监管和记录。

◇ 物的管理

对于涉及商业秘密的物品，包括但不限于员工的电脑、生产设备、流程图、操作规程、产品原材料及配方等，企业应制定相关制度以全面管理其存放、使用、更新及销毁等过程。例如，在化工领域企业可将工艺流程中涉及的原材料、化学药品的名称或成分均使用代号进行表示，代号对应的真实名称或成分严格限制知晓人员范围。

◇ 人员管理

在员工离职时，建议企业做好离职交接工作，如确认该员工曾使用的涉密物品、文件已归还，相关账号的权限已关闭，个人电脑中的涉密数据已清理。同时，应当以书面离职交接表格的形式确认上述事项并确保员工完成签字确认。在笔者处理的案件中，因员工离职时间较为久远且纸质文件保存不当导致劳动合同、保密合同等均遗失，仅收集到离职交接表格，清楚地记载了涉案保密信息及涉密物品、文件的交接情况，在诉讼过程中起到了非常重要的作用。

◇ 员工培训

员工培训对于商业秘密保护是一种有效且必要的措施，但在实践中经常被忽略。根据笔者经验，很多离职员工实施侵权行为是由于其对商业秘密的定义、何种行为构成侵权以及应承担何种法律后果缺乏了解。通过员工培训，一方面可以提高员工的合规意识，避免因法律知识的缺乏而实施商业秘密侵权行为；另一方面，通过对近期高额赔偿、构成刑事犯罪等典型案例的介绍，使员工对侵害商业秘密需承担的法律后果有清楚的了解，以起到威慑作用，降低商业秘密泄露风险。此外，员工培训记录也是法院在认定权利人采取保密措施的考量因素。因此，建议企业聘请专业人员对员工进行长期、定期、有效的培训。



三、员工的注意义务

在实践中，除“明知故犯”的故意侵犯，很多情况下，是因为员工不清楚“正当行为”与“侵权行为”的边界，而导致侵权。鉴于此，本文对以下常见情形进行梳理和说明：

◇ 参与商业秘密的研发过程，并不意味着员工可以随意使用

很多技术骨干或者研发部门负责人曾深度参与商业秘密的开发过程，会认为自己研发的成果属于该员工或者可以随意使用。然而这种认知是错误的。多数情况下，企业会与员工签订相关协议，约定知识产权归企业所有，员工负有保密义务且仅能在规定范围内使用。即使对知识产权归属未约定，但如果是利用企业的物质条件，为了完成企业交付任务，所获得的知识产权也应当归属于企业，员工未经授权不得使用。

◇ 将商业秘密发送至个人邮箱是否构成侵权取决于企业的保密制度是否完备

为了工作方便，员工经常会将文件资料发送至个人邮箱中，该行为是否构成侵权取决于企业的保密制度是否完备，以及与企业签订的合同中是否有相关约定。例如，在浙江省高级人民法院审理的一个案件中，企业的保密合同里面明确约定员工可以将工作所需的信息储存在 U 盘等设备中，法院认为类比该规定，员工将信息传输至邮箱的行为和存储到 U 盘设备类似，不构成侵权[浙江省高级人民法院 （2010）浙知终字第267号]。但在最高院最近审结的一起案件中，因保密合同明确约定了涉密信息的有限使用范围与使用方式，且明确规定员工不能够将文件资料发送至个人邮箱或在公司内部进行传播，最高院认为该员工将文件发送到个人邮箱构成侵权^[15]。

◇ 将商业秘密上传至网盘可能构成侵权

如果将商业秘密上传至第三方网盘致使公众能够获知，将可能被认定为侵权。在北京市朝阳区人民法院审理的一起案件中，某员工欲将未发布的影视作品发送给合作方进行处理，但由于专用网盘服务器存在故障，所以该员工将影视作品上传到第三方网盘中，致使公众能够观看、下载。法院认定该员工的行为构成侵权^[16]。

◇ 将商业秘密申请专利可能构成侵权

某些员工认为将商业秘密申请专利而未进行商业使用就不构成侵权。但是，在申请专利的过程中，相关技术会随着专利文本的公布或公告而公开，使商业秘密丧失秘密性。这种行为构成对商业秘密的不当披露，属于侵害商业秘密的行为。

◇ 离职后将商业秘密拷贝至新公司电脑的行为构成侵权

若员工离职后将商业秘密拷贝至新公司的电脑上，即使除该员工外，没有第三人知悉该行为，这种行为实际上也将保密信息传播至原单位以外的范围，构成侵权^[17]，可能被认定为 “以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取原告的商业秘密”^[18]。

◇ 简历中不宜涉及保密信息

在求职过程中，为了展示工作能力员工往往会在简历中描述工作经验和岗位职责。少数情况下，员工也会将重要的项目写在简历中，并且涉及项目细节（比如性能参数、实验步骤、详细客户信息等）。而这种行为可能存在侵权风险，需要注意避免。



四、新单位的注意义务

对于离职员工入职的新单位而言，同样要注意避免触碰法律红线，否则有可能被认定为商业秘密侵权。

◇ 主张不知悉无法规避法律风险

新单位也应当警惕由新员工所带来的法律风险，不能简单地以不知悉为由规避法律责任。法院在认定新单位是否明知或应知员工以不正当手段获取他人商业秘密时，往往会结合客观事实进行综合判断。例如，如某员工入职后在极短的时间内研发了相关产品，新单位作为同一行业的竞争对手应当了解该研发周期不符合行业惯例且应当意识到可能存在不正当使用他人商业秘密的情况，则有可能被认定为“明知或应知”该技术信息为他人商业秘密。

因此，在员工入职时，新单位应当对其进行背景调查，询问其与前单位的保密协议、竞业限制协议等文件的签署情况。同时应当在员工入职前对员工进行商业秘密培训，书面告知其不可在工作中违反与原单位的约定或使用他人的商业秘密，善尽注意义务。

◇ 通过“挖角”来获取他人商业秘密构成侵权

如企业故意通过“挖角”的方式，企图走捷径来不当获取他人的先进技术，则极有可能侵害他人商业秘密。与上述情形类似，法院综合考虑多种因素和证据判断企业是否存在“挖角”的主观故意。例如在“香兰素”案中，被告在该员工仍在原告处任职时即与之接触，并与该员工签订协议开发与原告类似的技术；同时，被告从该员工处获取过包含商业秘密信息的载体，在“挖角”之后短期内即向市场推出了和商业秘密权利人类似的产品。根据上述证据，法院认定被告具有侵权故意^[19]。

◇ 新单位实际控制人可能也需承担法律责任

新单位的实际控制人也需要重视个人承担商业秘密侵权责任的风险。如果新单位的实际控制人意图通过“挖角”积极参与教唆、引诱、帮助离职员工不正当获取他人商业秘密并为己用，且为此成立公司专门从事侵权行为，那么新公司的行为也体现了实际控制人的意志。此时，实际控制人也应当承担侵权责任^[20]。



结语

对科技型企业来说，商业秘密可以为其带来巨大的经济利益和市场份额，是企业的核心竞争力。自2019年《反不正当竞争法》修订以来，最高院、各地方法院和市场监管部门先后发布了相应的司法解释、审判指南、部门规章和典型案例，说明商业秘密保护对于企业长远成长乃至国家经济健康发展的重要性。然而，随着科学技术的快速发展和科技型人才的快速流动，因员工离职带走商业秘密或竞争对手“挖角”而产生商业秘密纠纷的情形越来越多，侵权手段愈加隐秘和多样化，对企业如何建立健全的商业秘密保护制度也带来了新的挑战。本文结合司法审判要点和处理商业秘密纠纷的实践经验，对实践中遇到的一些常见情形和应当注意的问题进行了简要的探讨，以为科技型企业在商业秘密保护制度建设过程中提供一些思路和建议。同时，也欢迎各位读者扫码观看本文作者贾媛媛律师在知享课堂录制的同名视频课程。

点击文末“[此处](#)”观看《科技型企业的商业秘密保护》视频课程

1.南京市中级人民法院（2019）苏01民初2893号

2.最高人民法院（2020）最高法知民终1667号

3.《江苏省高级人民法院侵犯商业秘密民事纠纷案件审理指南（修订版）》第2.2条

4.中华人民共和国《反不正当竞争法》第九条第四款、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、四、五、六、七条

5.《江苏省高级人民法院侵犯商业秘密民事纠纷案件审理指南（修订版）》第2.8.2条

6.上海市浦东新区人民法院 （2012）浦刑（知）初字第42号

7.《江苏省高级人民法院侵犯商业秘密民事纠纷案件审理指南（修订版）》第1.4条

8.中华人民共和国《反不正当竞争法》第九条

9.中华人民共和国《反不正当竞争法》第二十九条

10.同注2

11.最高人民法院、公安部《关于修改侵犯商业秘密刑事案件立案追诉标准的决定》

12.中华人民共和国《反不正当竞争法》第二十一条

13.马东晓. 在中国进行商业秘密维权[EB/OL]. 2017[2022]. <https://law.asia/zh-hans/%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86%E7%BB%B4%E6%9D%83/>.

14.浙江省高级人民法院 （2010）浙知终字第267号

15.最高人民法院（2021）最高法知民终1687号

16.北京市朝阳区人民法院 (2017)京0105民初68514号

17.同注15

18.中华人民共和国《反不正当竞争法》第九条

19.同注2

20.同注2

2022-11-25