
企业如何管理商业秘密及应对泄密事件

陈菲

引言

高度创新的技术信息对一个企业而言，不仅会增强其经济实力，而且很大程度上能够决定一个企业的核心竞争力。相较于专利公开换保护，机密的商业秘密则更不易被竞争企业获取，更能隐藏企业内部核心技术创新，从而巩固自身的竞争资本与市场地位。随着政策的推动以及企业自主意识的提升，近几年来商业秘密诉讼案件越来越多，这一方面表现出企业对商业秘密越发重视，另一方面也表露了各大竞争对手企业对核心技术的窥探和抢夺。企业商业秘密泄密事件频发，这很大程度是由于企业内部商业秘密管理缺失，核心商业秘密泄露使得企业多年心血付之东流，核心竞争力了然无存。那纠纷发生时，企业应如何予以应对，根源问题如何解决，怎样才能对企业内的商业秘密予以强有力的保护与管理，从而更好地防范泄密风险？

一、企业面临巨大的商业秘密泄露风险

自2020年中美贸易协议强调对商业秘密的保护，到近几年《反不正当竞争法》（以下简称“反法”）修改以及《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》的发布等，再到各地政府、各级市监局等都开始发布各类商业秘密的侵权纠纷案件指南、合规管理指引等。可见，整个政策形势都高度重视商业秘密的保护。

而近年来公开的司法数据显示，商业秘密诉讼案件中权利人胜诉的案子甚少，通过北京高级人民法院知识产权庭课题组的统计数据，近些年商业秘密权利人的原告平均胜诉率仅为35%¹。企业可能历经几年甚至十几年的时间与精力潜心研究，终于研发出领先于竞争企业的优势技术，这为企业带来了莫大商机，而管理不当却可能短期就被竞争对手夺取并加以利用。从近年的“香兰素”案、“卡波”案等案件可看出，离职员工泄露原单位的商业秘密并伙同竞争公司利用原单位的

¹ 参见北京市高级人民法院知识产权庭课题组.《反不正当竞争法》修改后商业秘密司法审判调研报告[J]. 电子知识产权,2019(11):65-85.

核心技术，给原单位造成了几百万甚至上亿的经济损失，这些数额还仅是大致可以计算得出的金额，还有巨额的商业秘密可得利益是无法估计的。

商业秘密泄密事件不断以及企业在纠纷中败诉率偏高，究其原因，诉讼中举证难也即缺失对商业秘密权利基础以及三性的证明，其根源还是企业前期的商业秘密管理存在不足。而在如今有政策推动的情形下，企业在实操中具体应该如何操作预防风险发生，面对商业秘密侵权案件时如何应对？基于前述两者原因，企业应注重证据准备，且利用各类维权手段保护自身权益；同时需要日常便注重对内部商业秘密信息及涉密员工进行管理，将泄密风险扼杀于摇篮之中。

二、商业秘密纠纷的应对策略

在商业秘密泄露事件已经发生时，企业可以充分利用法律手段维护自身权益，常用民事和刑事诉讼的手段，近几年利用行政机关处理商业秘密侵权的案件也越来越多。企业应基于泄密事件情况与自身需求，寻求最有利的方式，还可以交叉使用各类维权手段，使自身利益最大化。

（一）民事诉讼中注重对权利基础及三性的证明

关于商业秘密维权，关键是对商业秘密权利基础以及三性的证明。三性即秘密性、保密性、价值性，其中法院一般对价值性的认定不持异议，重点在于前两者的认定。

首先，一大要点却容易被企业忽略的是，在诉讼中关于商业秘密权利基础的证明。在商业秘密三性证明之前，关键前提是对商业秘密权利基础的证明。也即，企业所主张权利的商业秘密到底是什么，秘密点为何，载体为何？有的商业秘密权利人，在起诉时连自身的商业秘密是什么都不清楚，以至于最后只能撤诉或者迎来败诉的结果。如在华永公司等与郭某某案中²，原告虽然主张其“手机psd源文件所体现的各个图层排布、命名及隐蔽性编辑手法等相关技术信息”为其技术信息，但是其既“无法明确图层数量”，也不能“明确该图层命名秘点的具体内容”等，因而法院无法确定秘点内容，故其认为“秘点主张不明确”，从而驳回了原告的起诉。同时，还有如在北京利玛公司诉北京机械研究所案中³，

² 参见海顶晟无线网络科技有限公司等与天津浩海九洲科技有限公司等侵害商业秘密纠纷案，天津市第一中级人民法院(2020)津01民终4575号。

³ 参见北京利玛软件信息技术有限公司诉北京机械工业自动化研究所等侵犯商业秘密、不正当竞争纠

因为原告所主张的商业秘密并未提供具体的载体，法院未支持原告主张的情形。这些败诉的案例和情形，都提醒企业一是在诉讼前做好证据准备工作，二是在日常管理中就应对文件做好归档工作。

其次，关于商业秘密的秘密性，也即非公知性。该部分的证明原告常采用委托鉴定机关对涉案商业秘密不为公众所知悉进行鉴定，而相对于原告证无，被告证有则更加容易些，只要找到相关的文献、报告等内容，证明涉案商业信息已被公开，能够被公众容易获得即可。但值得注意的是，在被告证明涉案商业信息时，应证明技术信息或者经营信息整体被公开，而不能将部分内容割裂开来，仅证明原告所有的商业信息的部分内容被公开，并不能否定其商业秘密的秘密性⁴。但是，在反法修法后，原告对秘密性的证明责任有所降低，反法第三十二条规定“商业秘密权利人提供初步证据，证明其已经对所主张的商业秘密采取保密措施，且合理表明商业秘密被侵犯，涉嫌侵权人应当证明权利人所主张的商业秘密不属于本法规定的商业秘密”。因此，原告只需举证其对商业信息采取了保密措施，且初步证明被告侵犯其商业秘密权益，则应由被告证明商业秘密不具有秘密性。可见，反法修法后，原告的举证责任和举证难度极大降低。

最后，关于保密性的证明。原告需出示对企业商业信息保密所采取的保护措施，如企业与员工签订的保密协议、竞业限制协议，企业内部发布的员工保密手册、车间保密指引等相关保密制度与保密手段。而且基于前述提及的反法修改后的第三十二条内容，企业对“保密性”的证明应更加引起重视。对于企业内部管理来说，对企业员工、计算机管理、物理环境、外部合作等方面的保密措施尽量全面；而面对纠纷时，则需要证明企业采取的保密措施程度，与商业秘密价值相匹配。在2020年《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》第五条，也明确规定“人民法院应当根据商业秘密及其载体的性质、商业秘密的商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度以及权利人的保密意愿等因素，认定权利人是否采取了相应保密措施。”以及在香兰素案中，法院判定原告的保密措施是否合理时，也以企业的保护措施与技术信息价值是否相适应来判断⁵。

纷案，北京市第一中级人民法院(2003)一中民初字第5276号。

⁴ 参见高辛茂与一得阁公司、传人公司侵犯商业秘密纠纷案，最高人民法院(2011)民监字第414号。

⁵ 参见上诉人嘉兴市中华化工有限责任公司、上海欣晨新技术有限公司与上诉人王龙集团有限公司、

（二）运用民刑交叉程序及刑事企业合规不起诉手段

对于情节严重的侵犯商业秘密的行为，企业可以采取刑事手段维权。在给商业秘密权利人造成损失数额达到三十万元时，便可达到刑事立案门槛。相较于侵犯商业秘密刑事案件立案追诉标准修改前，五十万的立案金额标准，该修改也有利于商业秘密权利人维权。同时，通过刑事案件借助刑事侦查手段，更便于调取侵害商业秘密的相关证据。而且，通过刑事手段维权后，同样还可以再提起民事诉讼要求被告赔偿侵权损失。反之，在民事经济纠纷案件中，若发现被诉侵权行为已涉嫌侵犯商业秘密犯罪，法院也可以依法将相关线索移送公安机关处理，在香兰素案件中便如此⁶。因此，商业秘密权利人在纠纷发生时，可以交叉利用民刑程序，更大程度维护自身权益。

同时，在企业作为被告方时，现今还可以利用“企业合规不起诉”的方式。企业合规不起诉是指，企业在经营活动中涉及犯罪时，若符合法律规定的条件，企业可以在一定考察期限进行整改和合规建设，从而决定是否对企业不起诉或从宽量刑处理。而根据《关于建立涉案企业合规第三方监督评估机制的指导意见（试行）》第四条规定，企业适用合规不起诉的条件是（1）涉案企业、个人认罪认罚；（2）涉案企业能够正常生产经营，承诺建立或者完善企业合规制度，具备启动第三方机制的基本条件；（3）涉案企业自愿适用第三方机制。因此，在商业秘密犯罪中，企业在作为被告嫌疑人时，可以采取以上措施，结合商业秘密合规管理措施，争取不被起诉的结果。

（三）利用行政处罚手段快速解决纠纷

利用行政手段维护权利人的商业秘密权益，是相对便捷的一种方式。企业可以向行政机关投诉，通常是向地方市场监督管理局提交初步的商业秘密及侵权行为存在的有关证据，行政机关进而对违法行为进行查处，责令侵权人停止违法行为、没收违法所得、处以罚款等等。根据反法第四条规定，县级以上政府的行政机关便有相关管理职能。同时，国家工商行政管理局发布的《关于禁止侵犯商业秘密行为的若干规定》明确了行政机关的职能范围，以及权利人提供证据的要求；

宁波王龙科技股份有限公司、喜孚狮王龙香料（宁波）有限公司、傅祥根、被上诉人王国军侵害技术秘密纠纷案，最高人民法院(2020)最高法知民终 1667 号。

⁶ 参见嘉兴市中华化工有限责任公司等与王国军等侵害技术秘密纠纷案，最高人民法院（2020）最高法知民终 1667 号。

2020 年国家市场监督管理总局发布的《商业秘密保护规定（征求意见稿）》相关条款，进一步细化了权利人举证的具体事项。

相比民诉或刑诉案件漫长的审理周期，行政手段立案快、审理周期短，更加高效。利用行政手段，可以更加高效地取得禁令。而且通过行政调查，也更容易取得侵犯商业秘密的证据，以便在后续民事诉讼中加以利用。同时，通过行政查处的调查，认为侵权人的行为已经符合刑事犯罪的条件，可以将案件移送公安机关立案侦查。因此，权利人在结合民事和刑事交叉保护权利同时，还可以参考借助行政手段维权。

三、企业应加强商业秘密管理体系构建

基于前述谈及的商业秘密维权手段及应对，为了避免商业秘密泄密风险，以及为了更好地应对后续可能面临的商业秘密纠纷，企业在前期管理过程中，就应当合理地采取相应措施管理公司的商业秘密，建立商业秘密管理体系。商业秘密管理体系中涉及两个关键工作，一是对商业秘密权利基础的确定，主要涉及对商业秘密载体的识别与盘点等工作；二是对企业商业信息的合规管理，主要涉及企业采取保密手段。

（一）确定商业秘密权利基础

前文提及企业在主张自身权利时，由于无法确定商业秘密到底是什么，而导致不利后果。基于此，企业在前期管理时，就应重视对商业秘密的识别、盘点与归档。从项目的立项、开发、试产、量产、销售等各个阶段进行检视，对可能涉及商业秘密的计划书、产品分析报告、产品设计图、实验记录、研发纪要、产品说明书等文件予以梳理，识别其中可能涉及商业秘密的文件，予以合理恰当地整理归档。

识别与盘点企业商业秘密。其中对于商业秘密的识别较难，一般企业员工可能无法识别哪些属于商业秘密，尤其是否属于企业核心的技术信息，哪些属于公知信息或企业不予以保护的信息。此阶段，建议可以成立一个技术委员会，或者请公司的专业技术人员，根据企业自身技术信息的特点，整理出各个产品阶段需要以商业秘密保护的文件和内容有哪些，形成商业秘密盘点表。后续各部门人员根据相应的盘点表内容，以此整理相关文件，并进行归档工作。如此，公司的商业秘密内容就可以有条不紊地予以存放，不论是对公司自身管理还是应对此后的

诉讼，都极其有益。同时，对于有条件的企业，可以对整理归档的商业秘密文件内容，通过区块链等方式保全商业秘密文件内容，对其予以存证。

定期检视商业秘密盘点归档工作。为了保障企业以上工作的可持续性，企业还应对以上措施加以定期更新与核查的工作。考虑到公司的项目进程变化、技术迭代更新，商业秘密的盘点表也应定期更新。同时，对于各部分的盘点、归档工作，也应定期进行检查，对是否落实盘点事项、是否达标等事项予以核查，让商业秘密的识别和确定工作能够更加完善的落实。

(二) 加强对商业秘密的保护措施

为加强对商业秘密的保护，企业还应注重对商业秘密相关制度和物理环境管理等予以建设。一是增加保密措施可以为核心商业秘密加以保护屏障，阻止外部窃取；二是提升内部人员对商业信息的保密意识，防止泄密；三是增加商业秘密的“保密性”，满足司法层面对商业秘密的要求。

商业秘密泄密风险源于两个层面，其一是源于公司内部，也即是公司内部员工违反保密义务而泄密；其二源于公司外部，或是公司与外部公司进行合作时，不慎泄密，或是商业间谍窃取商业秘密。

首先，关于来源于员工泄密的风险，企业应加强对企业内部保密制度的建设。根据司法案例统计数据表明，84%的商业秘密纠纷案件的源头都是员工泄密⁷，因此企业对于员工的保密管理乃重中之重。对员工的保密管理，应贯彻入职、在职和离职阶段。入职时与员工签订保密协议、竞业限制协议，并伴随相关的入职保密培训；在职时仍应定期做商业秘密宣导，并对其办公设备加以保密管理；离职时应落实离职脱密的程序，通过离职访谈、文件和涉密设备梳理和交接、签订保密承诺书等方式，防止员工离职携带保密文件。而且，为了便于对商业秘密更好的保密管理，较好的方式是对员工的保密级别分类分级，以不同职别员工承担不同程度的保密义务为标准，对其进行分级管理。同时，企业应有员工商业秘密手册，对于公司的保密制度、相关保密措施、应急管理等事项予以明确的规定，使员工更加清晰地认识商业秘密并配合进行管理。

其次，关于来源于企业外部的商业秘密泄露风险。在企业与外部合作时，应

⁷ 参见视点 | 2022 年度商业秘密保护合规报告，<https://mp.weixin.qq.com/s/Hz638L0tY-Yjyd2yx6csHQ>，2023 年 3 月 10 日发布；2022 年商业秘密合规年度报告，<https://mp.weixin.qq.com/s/KJwBamJouLZ0xCpJfDbKZQ>，2022 年 12 月 23 日发布。

注意在洽商过程中不应泄露商业秘密，在合作签订协议时加以保密条款。并注意在传输和转达合作文件时，区分办公传输设备和规定的传输途径，而非使用个人邮箱等方式予以交互，全过程注意文件留存留痕。同时，在商务交流过程中，如对外访谈、交流或对外开放时，注意对外部访客的保密管理，避免在对外讲座或宣传过程中不慎泄密技术秘密。对于可能面临的黑客或商业间谍的窃取行为，应加强对内外网络隔离的区分设置，对电脑及打印机等设备加设保密软件，加强防火墙软件的使用以及定期更新防病毒软件等。

再次，还应加强对企业物理环境的保密管理。确定涉密的车间、厂区、办公楼等区域，对该些区域予以划分并分级管理。对于进出控制、安保设施、保密标识等予以设立，区分访问权限。并且对于此类的涉密区域，结合前述的访客管理，避免通过对外开放交流访问的时候，不慎泄密。

四、结语

为了避免商业秘密泄露给竞争企业，甚至失去秘密性的风险，企业应做好充分的内部管理，需在公司内做好前端的商业秘密管理，从内部员工管理、对外合作商管理、物理环境等多方面层层保密；同时对可能面临的纠纷予以合理应对，也即在后端诉讼中运用民刑行政多重手段充分维护自身权益。后端维权中的司法要求为前端的商业秘密管理提供思路，前端的商业秘密管理为后端的维权做好基础与铺垫。企业应对前后端两方面的工作予以兼顾，才能更全面有力地维持并加强企业的核心竞争力。