

管理与  
维权  
指引

企业  
商业  
秘密

深圳市中级人民法院

深圳市中级人民法院

深圳市中级人民法院

深圳市中级人民法院

深圳市中级人民法院



► 53个 典型案例 ► 22种 泄密场景 ► 4大 管理体系 ► 3类 维权途径

2025年4月

# 前言

在深入推进中国式现代化建设的伟大征程中，创新已成为驱动国家发展的核心动力。党的二十届三中全会通过的《中共中央关于进一步全面深化改革 推进中国式现代化的决定》明确指出，要构建支持全面创新的体制机制，强化企业科技创新主体地位；要完善市场信息披露制度，构建商业秘密保护制度。在此背景下，加强商业秘密保护，不仅是保护企业合法权益、激励企业创新创造的应有之义，更是推动创新驱动发展战略实施、建设创新型国家的时代之需。

商业秘密作为企业创新成果的重要载体，是企业在激烈市场竞争中保持核心竞争力的关键要素。尤其在高新技术产业蓬勃发展的当下，商业秘密已成为创新主体的核心资产，是企业参与国际市场竞争的重要战略资源，甚至关系企业存亡。据相关数据显示，全球科技企业中，超过80%的关键技术信息是以商业秘密的形式进行保护，而非通过专利途径。因此，加强商业秘密保护，对于保障企业经营发展、激励创新创造、维护市场公平竞争秩序具有重要意义。

近年来，随着新技术的不断发展、全球化竞争的不断加剧，商业秘密侵权案件呈现逐年增多的趋势，给企业造成了巨大的经济损失，甚至引发相关刑事犯罪。实践中，侵权形式多样，包括员工离职带走、在职员工违规泄露以及竞争对手恶意窃取商业秘密等。这些问题不仅反映出部分企业缺乏相应的保护意识，对商业秘密的保护措施不力，同时也凸显了在信息技术飞速发展的背景下，商业秘密保护面临更加复杂的情况和严峻的挑战。

作为中国改革开放的前沿阵地和创新之都，深圳始终致力于打造一流的法治化营商环境，为企业创新发展提供坚实的司法保障。深圳法院在知识产权保护领域积累了丰富的实践经验，尤其是在商业秘密司法审判方面，形成了一系列具有示范意义的裁判规则和实践做法。为进一步提升企业商业秘密保护水平，我们深入研究司法实践中的典型问题，广泛征求企业、法律专家及相关领域专业人士的意见，精心编撰了《企业商业秘密管理与维权指引》，从商业秘密保护的体系构建、运营管理、维权策略等多个维度出发，旨在帮助企业将商业秘密保护融入日常经营管理的各个环节，提升企业应对风险的能力，构建全方位、多层次的商业秘密保护体系。



我们坚信，法治是创新的基石，只有通过完善的法律制度和有效的司法保护，才能激发企业的创新活力，推动创新驱动发展战略的深入实施。我们衷心期望，本指引能够成为企业发展的得力助手，助力企业提升商业秘密自我保护能力，有效防范商业秘密泄露和侵权风险。深圳法院将继续秉持为大局服务、为人民司法的理念，与社会各界携手共进，共同营造尊重创新、保护创新的优良法治化营商环境，为创新驱动发展战略实施、创新性国家建设贡献更多的司法智慧和力量。



# 目录

## 01

### 概要

#### 1.1 商业秘密的概念及特征 /2

##### 1.1.1 秘密性

##### 1.1.2 保密性

##### 1.1.3 价值性

#### 1.2 商业秘密的保护范围 /7

##### 1.2.1 技术信息

##### 1.2.2 经营信息

#### 1.3 商业秘密的归属

##### 1.3.1 雇佣期间商业秘密的归属

##### 1.3.2 兼职期间商业秘密的归属

##### 1.3.3 离职后商业秘密的归属

##### 1.3.4 委托开发关系下商业秘密的归属

##### 1.3.5 合作开发关系下商业秘密的归属

## 02

### 常见的泄密场景

#### 2.1 人员泄密

##### 2.1.1 跳槽泄密

##### 2.1.2 自立门户泄密

##### 2.1.3 内外串通泄密

2.2 信息发布 /19

- 2.2.1 公开披露
- 2.2.2 论文发表
- 2.2.3 媒体泄密
- 2.2.4 外部咨询

2.3 存储泄密 /22

- 2.3.1 载体泄密
- 2.3.2 产品流通

2.4 传输泄密 /24

- 2.4.1 邮件发送
- 2.4.2 微信泄密
- 2.4.3 云盘泄密

2.5 对外合作 /27

- 2.5.1 招投标
- 2.5.2 许可转让
- 2.5.3 服务外包
- 2.5.4 技术出资

2.6 涉外泄密 /29

- 2.6.1 境外诉讼
- 2.6.2 人才引进

2.7 研发测试 /31

- 2.7.1 产品研发
- 2.7.2 游戏内测
- 2.7.3 数据共享

2.8 区域泄密 /34

### 3.1 管理原则 /36

- 3.1.1 分类管理原则
- 3.1.2 最小接触原则
- 3.1.3 全流程管理原则
- 3.1.4 合理利用原则

### 3.2 管理组织 /37

### 3.3 人员管理制度 /38

- 3.3.1 内部人员管理
  - 3.3.1.1 入职管理
  - 3.3.1.2 在职管理
  - 3.3.1.3 离职管理
- 3.3.2 外部人员管理
  - 3.3.2.1 涉密外部活动
  - 3.3.2.2 管理方式

### 3.4 涉密载体管理 /44

- 3.4.1 涉密载体的类型
- 3.4.2 涉密载体的管理

### 3.5 涉密区域管理 /48

## 4.1 行政途径

/51

### 4.1.1 投诉举报

#### 4.1.1.1 管辖

#### 4.1.1.2 立案门槛

#### 4.1.1.3 证据准备

#### 4.1.1.4 行政调查

#### 4.1.1.5 行政处罚

#### 4.1.1.6 行政调解

#### 4.1.1.7 行政责任

### 4.1.2 行政复议与行政诉讼

### 4.1.3 探索行政与司法深度衔接

## 4.2 民事途径

/57

### 4.2.1 协商和解

### 4.2.2 仲裁

### 4.2.3 民事诉讼

#### 4.2.3.1 管辖

#### 4.2.3.2 主体资格

#### 4.2.3.3 证据准备

#### 4.2.3.4 证据保全

#### 4.2.3.5 行为保全

#### 4.2.3.6 预防二次泄密

#### 4.2.3.7 司法鉴定

#### 4.2.3.8 常见抗辩

#### 4.2.3.9 民事责任

## 4.3 刑事途径

/68

### 4.3.1 刑事公诉与自诉

#### 4.3.1.1 管辖

#### 4.3.1.2 公诉与自诉的转换

#### 4.3.1.3 证据准备

#### 4.3.1.4 刑事责任

### 4.3.2 刑事附带民事诉讼

### 4.3.3 刑民交叉的处理思路

#### 4.3.3.1 不同事实的认定

#### 4.3.3.2 在先刑事判决的既判力

## 4.4 维权途径的路径特点

173

附件

法律规范指引



01

# 概要



## 1.1 商业秘密的概念及特征

《民法典》<sup>1</sup>第一百二十三条第二款第五项将商业秘密作为知识产权的保护客体之一。根据《反不正当竞争法》第九条第四款，商业秘密是不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

### 1.1.1 秘密性

秘密性是商业秘密最显著的特征，它是指权利人请求保护的信息在诉侵权行为发生时不为所属领域的相关人员普遍知悉和容易获得的。<sup>2</sup>具体从下列四方面理解：

#### (1) 时间节点

权利人请求保护的信息必须是“在诉侵权行为发生时”不为公众所知悉的。

#### (2) 知悉的人员范围

“不为公众所知悉”中的“公众”并非指一切可能知悉权利人请求保护的客户信息的人员，而是“所属领域的相关人员”。“所属领域”应当是权利人和诉侵权人所属的相关行业领域。

#### (3) 知悉的程度

权利人请求保护的客户信息在诉侵权行为发生时不为所属领域的相关人员“普遍”知悉。

#### (4) 获得的难易程度

权利人请求保护的信息，在诉侵权行为发生时不为所属领域的相关人员“容易”获得。例如通过简单的查询即可获得。

<sup>1</sup>《民法典》第一百二十三条第二款第五项规定，知识产权是权利人依法就下列客体享有的专有的权利：（五）商业秘密。

<sup>2</sup>《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》第三条规定，权利人请求保护的信息在诉侵权行为发生时不为所属领域的相关人员普遍知悉和容易获得的，应当认定为反不正当竞争法规定的商业秘密的“不为公众所知悉”。



### 【典型案例】华某公司诉博某公司侵害技术秘密纠纷案<sup>3</sup>

**案情简介：**华某公司是一家专业从事鲜食玉米种子研究开发和生产经营的公司，培育了优良的玉米自交系品种“W67”和“W68”，并利用这些品种作为亲本培育了杂交玉米新品种“万糯2000”，于2015年11月1日获得植物新品种权。华某公司以博某公司侵害其“万糯2000”玉米品种的亲本“W68”技术秘密为由提起诉讼。博某公司主张“万糯2000”已公开售卖，故“W68”属于公开销售的品种，已被推广应用。法院审理认为，种子“W68”属于不为公众所知悉的育种材料，具有秘密性。

“W68”指代的是育种者控制的特定育种材料，包含特定的遗传信息，但仅凭代号无法知悉或利用这些遗传信息；“W68”的育种过程包括了多个复杂的步骤，不同育种者即使使用相同的育种来源，也难以得到完全相同的品种，公开育种来源并不意味着公众可以轻易获得“W68”的育种材料；“万糯2000”虽作为杂交种已经公开销售，但反向分离出其亲本“W68”的难度极大，因此“W68”具有私密性。

司法实践中，具有下列情形之一的，人民法院可以认定有关信息为公众所知悉：<sup>4</sup>

- （1）该信息在所属领域属于一般常识或者行业惯例的；
- （2）该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；
- （3）该信息已经在公开出版物或者其他媒体上公开披露的；
- （4）该信息已通过公开的报告会、展览等方式公开的；
- （5）所属领域的相关人员从其他公开渠道可以获得该信息的。



<sup>3</sup> 最高人民法院（2022）最高法知民终147号民事判决书。

<sup>4</sup> 《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》第四条规定，具有下列情形之一的，人民法院可以认定有关信息为公众所知悉：（一）该信息在所属领域属于一般常识或者行业惯例的；（二）该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；（三）该信息已经在公开出版物或者其他媒体上公开披露的；（四）该信息已通过公开的报告会、展览等方式公开的；（五）所属领域的相关人员从其他公开渠道可以获得该信息的。将为公众所知悉的信息进行整理、改进、加工后形成的新信息，符合本规定第三条规定的，应当认定该新信息不为公众所知悉。



### 【典型案例】姜某辉等侵犯商业秘密案<sup>5</sup>

**案情简介：**被告人姜某辉、吴某、张某敏等六人均曾任职于华某公司，分别从事技术研发以及研发管理，均与华某公司签订保密协议。被告人在华某公司任职期间，利用职务之便窃取并使用了公司的ifere电路原理图以及两项天线技术方案，擅自使用上述两种职务成果为上海某公司研发智能手表，并以上海某公司的名义申请实用新型专利，导致技术信息被公开，造成了华某公司损失223.2万元。法院审理认为，ifere电路原理图以及两项天线技术均系华某公司投入人力、物力、财力研发而成，具有实用价值，华某公司亦采取了保密措施。其中，ifere电路原理图的各个部件虽是现有、公开技术，但各个部件之间的组合关系具有特定性，不为公众所知悉；被告人使用两项天线技术申请的专利因不具有创造性被宣告无效，亦不影响该技术信息符合非公知性要求。因此，上述技术信息均构成商业秘密。



**【温馨提示】**该案明确了多项公开技术组合的技术方案亦可具有非公知性，被诉侵权人直接、完全使用权利人技术秘密，或者对技术秘密进行部分修改、改进后使用，均属于使用权利人技术秘密的行为。

#### 1.1.2 保密性

商业秘密的保密性是通过权利人采取保密措施得以实现的，是指秘密持有人采取了合理措施进行保密，而非指商业秘密处于绝对秘密、无人可知的状态。<sup>6</sup>

司法实践中，具有下列情形之一，在正常情况下足以防止商业秘密泄露的，人民法院应当认定权利人采取了相应保密措施：<sup>7</sup>

<sup>5</sup> 广东省深圳市中级人民法院（2018）粤03刑终2568号刑事裁定书。

<sup>6</sup> 《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》第五条规定，防止商业秘密泄露，在被诉侵权行为发生以前所采取的合理保密措施，人民法院应当认定为反不正当竞争法第九条第四款所称的相应保密措施。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。

<sup>7</sup> 《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》第六条规定，具有下列情形之一，在正常情况下足以防止商业秘密泄露的，人民法院应当认定权利人采取了相应保密措施：（一）签订保密协议或者在合同中约定保密义务的；（二）通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；（三）对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的；（四）以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；（五）对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的；（六）要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；（七）采取其他合理保密措施的。

- (1) 签订保密协议或者在合同中约定保密义务的；
- (2) 通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；
- (3) 对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的；
- (4) 以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；
- (5) 对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的；
- (6) 要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；
- (7) 采取其他合理保密措施的。



### 【典型案例】维某公司诉贝某公司、李某侵害技术秘密纠纷案<sup>8</sup>

**案情简介：**维某公司是一家生产不间断电源并提供配电及基础设施管理解决方案的企业，其独立研发的用于其特定类型UPS产品中的软件源代码，为其带来较大的经济利益。李某于2011年入职维某公司，主要负责产品的研发工作，并与维某公司签订了《保密协议》。维某公司提交的证据显示维某公司对涉案技术信息采取了保密措施，包括：与员工签署保密条款和保密协议；发布了关于员工行为规范的手册；对员工应遵守员工行为规范进行培训；公司财产及信息采取了物理安全管理措施，包括门禁和信息隔离；对公司秘密信息实施了信息安全网络监管，防止涉密信息泄露，具体包括采取BITLOCKER对硬盘加密；采取DPS对文档加密；采取IPGuard监管措施对公司的设备、网络、及时通讯、移动存储进行管控；要求所有离职员工删除存有公司信息的所有内容等。法院审理认为，维某公司的举证足以证明对涉案技术信息采取了相应的措施，在正常情况下足以防止商业秘密被泄露，认定维某公司请求保护的技术信息具备保密性的构成要件。



**【温馨提示】**商业秘密的“保密性”对于不同企业、不同商业秘密而言没有“通用模板”，企业应当结合自身特点、行业性质和商业秘密的具体内容，将管理经验与法律要求有机结合，通过持续优化和更新保密措施，为商业秘密构建一个动态、有效的长期保护机制，在法律框架内最大限度地维护自身权益。

<sup>8</sup> 广东省深圳市中级人民法院（2020）粤03民初5073号民事判决书。



## 【典型案例】思某公司诉兰某公司侵害技术秘密纠纷案<sup>9</sup>

**案情简介：**思某公司研发的GTR-7001气体透过率测试仪包含了思某公司并未公开、不为公众所知悉的技术秘密。2017年9月，思某公司获知，兰某公司通过恶意发起的诉讼，利用诉讼保全程序非法获取思某公司技术秘密，并在2019年初在市场上公开推出包含与思某公司技术相同的智能模式检测仪器，构成商业秘密侵权。思某公司主张，其已经对上述技术秘密采取了合理的保密措施，包括：与员工签署包含保密条款的《劳动合同》与《企业与员工保密协议》，制定并实施了《公司保密管理制度》，对研发厂房、车间、机器等设置门锁，限制来访者的进出和参观等，还在测试仪特定位置贴上“危险！私拆担保无效！”等内容的标签。法院审理认为，涉案技术秘密的载体为测试仪，该产品一旦售出进入市场流通，就在物理上脱离思某公司的控制，故区别于可始终处于商业秘密权利人控制之下的技术图纸、配方文档等内部性载体。思某公司采取的“对内保密措施”，因脱离了涉案技术秘密的载体（即市场中流通的测试仪产品），与其主张保护的涉案技术秘密不具有对应性，故不属于《反不正当竞争法》规定的“相应保密措施”。同时，涉案技术秘密载体为市场流通产品，属于外部性载体，思某公司为实现保密目的所采取的保密措施，应能对抗不特定第三人通过反向工程获取其技术秘密。而思某公司贴附在产品上的标签并不构成可对抗他人反向工程的物理保密措施，故不符合涉案技术秘密及其载体的性质。法院最终认定，思某公司未采取符合《反不正当竞争法》规定的“相应保密措施”，其主张保护的涉案技术秘密因缺乏“相应保密措施”而不能成立。



**【温馨提示】**权利人采取的保密措施应当与其主张的商业信息的商业性相适应，没有就具体的保密客体作出具体、明确的保密要求，不能认定采取了商业秘密保护要求的保密措施。

### 1.1.3 价值性

商业秘密的价值性在于能够为权利人带来经济利益和竞争优势，使权利人拥有比不知晓或不使用该商业秘密的同行业竞争者更有利的市场地位和竞争优势，包括现有的和潜在的经济利益。<sup>10</sup>

<sup>9</sup> 最高人民法院（2020）最高法知民终538号民事判决书。

<sup>10</sup> 《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》第七条第一款规定，权利人请求保护的信息因不为公众所知悉而具有现实的或者潜在的商业价值的，人民法院经审查可以认定为反不正当竞争法第九条第四款所称的具有商业价值。



## 【典型案例】赛某公司诉华某公司、李某、张某等侵害商业秘密纠纷案<sup>11</sup>

**案情简介：**李某、张某原系赛某公司的总经理、董事，掌握赛某公司重要经营信息等。二人从赛某公司离职前，将赛某公司的熔炼过程记录表等资料上传至张某的个人网盘。赛某公司诉至法院，主张李某、张某违反保密义务，未经许可擅自使用赛某公司保密技术信息等用于华某公司的经营。法院审理认为，赛某公司请求保护的熔炼过程记录表所记载的熔炼合金的原材料成分比例、材料状态、参数、数据等信息的组合，系在熔炼实验或生产过程中所形成，属于实验者或生产者所掌握的特定信息，该等信息虽系过程性数据，并未形成具体而明确的技术方案，但系实验者或生产者在具体的熔炼过程中所获得的技术成果，对于后续实验或生产具有明显的实际效用，应当认定为具有商业价值。



**【温馨提示】**商业价值不等于实用性，这是商业秘密和专利权的区别之一。专利权的实用性要求发明或实用新型能够制造或使用，并能产生积极效果。失败的技术方案是不能取得专利权的，但失败的实验数据和技术方案往往具有商业价值。这是因为，多掌握一项失败的实验数据，就能减少一次试错成本。如果这些失败的实验数据被其他人掌握，就可以避开失败的实验从而节约研发成本。正因如此，我国现行法律已不再强调商业价值需要具备“实用性”的特征，取而代之的是具备“现实的或者潜在的商业价值”。这也提醒企业要注意保存和管理实验中的过程性数据，为企业的研发创新、商业秘密保护提供坚实的数据支撑。

## 1.2 商业秘密的保护范围

### 1.2.1 技术信息

技术信息是指与技术有关的结构、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。<sup>12</sup>

<sup>11</sup> 广东省深圳市中级人民法院（2021）粤03民初1114号民事判决书。

<sup>12</sup> 《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》第一条第一款规定，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。





### 【典型案例】吉某公司诉威某公司侵害商业秘密纠纷案<sup>13</sup>

**案情简介：**吉某公司是一家集汽车整车、动力总成和关键零部件设计、研发、生产、销售和服务于一体的全球企业集团。2016年，吉某公司旗下成都高某汽车公司约40名高级管理人员和技术人员先后离职并加入威某集团及其关联公司。2018年，吉某公司发现这些离职员工在威某公司利用其掌握的新能源汽车底盘应用技术，申请了12项底盘专利，并迅速推出了威某公司EX系列电动汽车。吉某公司认为威某公司涉嫌侵犯其技术秘密，遂诉至法院，要求威某公司停止侵权并赔偿损失。法院经审理查明，威某公司的12件实用新型专利文件部分披露了吉某公司涉案图纸及数模承载的技术秘密。从尺寸公差、材料标号、工艺技术要求、零部件标识位置、分拆图标及位置布局、图纸标记等细节进行判断，威某公司EX5型号电动汽车底盘零部件图纸及数模与吉某公司的涉案12套图纸及数模中的前稳定杆总成图纸及数模、后桥总成-安装支架（左右同）图纸及数模、后螺旋弹簧上隔振垫图纸及数模、机械转向器带横拉杆总成图纸及数模、前悬架左下摆臂总成图纸及数模、后螺旋弹簧下隔振垫图纸及数模、前稳定杆左衬套图纸及数模、后桥总成图纸及数模等均存在大量完全相同的技术信息，其中包括吉某公司特有的技术信息，足以证明威某公司在其电动汽车底盘及底盘零部件制造中使用了吉某公司涉案技术秘密。法院最终认定威某公司构成故意侵权，侵权情节恶劣，判决威某公司赔偿吉某公司约6.4亿元，并适用惩罚性赔偿。

#### 1.2.2 经营信息

经营信息是指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。其中，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。<sup>14</sup>



### 【典型案例】瑞某公司诉明某公司等侵害经营秘密、技术秘密纠纷案<sup>15</sup>

**案情简介：**瑞某公司起诉明某公司以及加入了该公司的10名前员工，主张这些员工违反了签订的保密协议，将瑞某公司的技术秘密和客户具体信息让明某公司进行使用。为此，瑞某公司提交了客户具体信息以及交易

<sup>13</sup> 最高人民法院（2023）最高法知民终1590号民事判决书。

<sup>14</sup> 《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》第一条第二款规定，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。

<sup>15</sup> 最高人民法院（2020）最高法知民终726号民事判决书。



情况。法院审理认为，瑞某公司所主张的客户信息不仅包含基础信息（如客户名称、地址、联系方式），还包括深度信息（如客户需求习惯、交易习惯、市场信息等）。这些信息不易从公开渠道获取，且客户数量众多，交易关系稳定，在竞争中为瑞某公司带来了实际或潜在的商业价值，瑞某公司也采取了多种保密措施来保护客户信息，包括签订保密协议、员工手册、保密义务培训、使用加密的OA系统管理信息，并与离职员工签署保密承诺书和竞业限制协议。故瑞某公司主张的客户信息构成经营秘密。



#### 【典型案例】华某公司诉麦某公司等侵害商业秘密纠纷案<sup>16</sup>

**案情简介：**华某公司起诉麦某公司及其相关员工，指控相关员工在离职后成立并加入麦某公司，侵犯了华某公司的商业秘密，其中包括与43家客户交易相关的详细信息。法院审理认为，华某公司提供的信息包含订单日期、单号、品名、货品规格、销售订单数量、单价、联系人、电话等内容，但这些信息均为一般性罗列，并没有反映某客户的交易习惯、意向及区别于一般交易记录的其他内容。而且麦某公司提供的对比表中显示，43家客户名单中重要信息相关联系人及电话号码与华某公司请求保护的大部分不同。法院考虑到行业特点以及相关证据，如果没有涵盖相关客户的具体交易习惯、意向等深度信息的情况下，难以认定华某公司提交的信息属于《反不正当竞争法》保护的商业秘密。



**【温馨提示】**客户信息要构成商业秘密，必须通过投入一定的人力、物力并经过反复接触、交易，从而形成相对长期稳定的客户信息资料。如果只是客户信息的一般性罗列，并没有反映某客户的交易习惯、意向及区别于一般交易记录的其他内容，则难以纳入商业秘密的保护范围。这也提醒企业应在日常的经营活动中，主动有意识的把有价值的经营信息整理、分类、归纳、收集，并采取合理适当的保密措施，防患于未然。

<sup>16</sup> 最高人民法院（2019）最高法民再268号民事判决书。

## 1.3 商业秘密的归属

商业秘密的归属即商业秘密归谁所有、使用，产生的收益如何分配。确定商业秘密的归属有利于企业明确人员管理、合同管理中的权利义务关系，既能保障自身取得的权利，还能防止侵害他人的权利，或花费过多的精力保护本不属于自己的利益。商业秘密的归属一般根据以下情形来确定。

### 1.3.1 雇佣期间商业秘密的归属

在雇佣关系存续期间，单位员工完成的商业秘密到底归属于员工还是单位，需要区分该技术成果属于职务技术成果还是非职务技术成果。职务技术成果是执行法人或者非法人组织的工作任务，或者主要是利用法人或者非法人组织的物质技术条件所完成的技术成果。<sup>17</sup>对于非职务技术成果，其使用权、转让权属于完成技术成果的个人，完成技术成果的个人可以就该项非职务技术成果订立技术合同。<sup>18</sup>

关于技术成果的完成是否“主要是利用法人或者非法人组织的物质技术条件”的问题，司法解释作出了进一步细化。包括职工在技术成果的研究开发过程中，全部或者大部分利用了法人或者非法人组织的资金、设备、器材或者原材料等物质条件，并且这些物质条件对形成该技术成果具有实质性的影响；还包括该技术成果实质性内容是在法人或者非法人组织尚未公开的技术成果、阶段性技术成果基础上完成的情形。<sup>19</sup>

但下列情况除外：

(1) 对利用法人或者非法人组织提供的物质技术条件，约定返还资金或者交纳使用费的；

(2) 在技术成果完成后利用法人或者非法人组织的物质技术条件对技术方案进行验证、测试的。

<sup>17</sup> 《民法典》第八百四十七条规定，职务技术成果的使用权、转让权属于法人或者非法人组织的，法人或者非法人组织可以就该项职务技术成果订立技术合同。法人或者非法人组织订立技术合同转让职务技术成果时，职务技术成果的完成人享有以同等条件优先受让的权利。职务技术成果是执行法人或者非法人组织的工作任务，或者主要是利用法人或者非法人组织的物质技术条件所完成的技术成果。

<sup>18</sup> 《民法典》第八百四十八条规定，非职务技术成果的使用权、转让权属于完成技术成果的个人，完成技术成果的个人可以就该项非职务技术成果订立技术合同。

<sup>19</sup> 《关于审理技术合同纠纷案件适用法律若干问题的解释》第四条规定，民法典第八百四十七条第二款所称“主要是利用法人或者非法人组织的物质技术条件”，包括职工在技术成果的研究开发过程中，全部或者大部分利用了法人或者非法人组织的资金、设备、器材或者原材料等物质条件，并且这些物质条件对形成该技术成果具有实质性的影响；还包括该技术成果实质性内容是在法人或者非法人组织尚未公开的技术成果、阶段性技术成果基础上完成的情形。但下列情况除外：（一）对利用法人或者非法人组织提供的物质技术条件，约定返还资金或者交纳使用费的；（二）在技术成果完成后利用法人或者非法人组织的物质技术条件对技术方案进行验证、测试的。

此外，专利在获得授权或公开之前，如果符合商业秘密的构成要件的，亦可以主张获得商业秘密的保护，所以也可以参照《专利法》的相关规定确定商业秘密的职务技术成果的归属。参照《专利法》第六条<sup>20</sup>和《专利法实施细则》第十三条<sup>21</sup>的规定，认定构成商业秘密的职务技术成果的归属：

(1) 执行本单位的任务或者主要利用本单位的物质技术条件所完成的商业秘密，包括：①在本职工作中完成的商业秘密；②履行本单位交付的本职工作之外的任务所完成的商业秘密；③退休、调离原单位后或者劳动、人事关系终止后1年内完成的，与其在原单位承担的本职工作或者原单位分配的任务有关的商业秘密。

(2) 如果使用本单位的物质技术条件完成商业秘密的员工与本单位订立合同，对商业秘密的归属作出了约定，则商业秘密的归属按合同约定执行。



**【温馨提示】**《民法典》允许职务技术成果的归属可以由单位和研发者进行约定，既可以约定属于单位，也可以约定属于个人，也即适用约定优先的规则。该规则明显有别于《专利法》关于职务发明创造的专利申请权和专利权归单位的强制规定。但是，《民法典》是规范当事人之间契约关系的法律。在当事人没有约定职务技术成果归属时，应当参照《专利法》的规定，由单位享有职务技术成果。两种情形下应当采用不同的处理规则，企业应当根据不同情形采取与之相适应的保护手段。

### 1.3.2 兼职期间商业秘密的归属

如果兼职员工在用人单位平均每日工作时间不超过四小时，每周工作时间累计不超过二十四小时的，双方之间可能形成非全日制劳动关系。<sup>22</sup>即使兼职员工没有成为公司的正式员工，在兼职期间形成的技术成果归属问题分析也适用职务技术成果归属的相关规定。

<sup>20</sup> 《专利法》第六条规定，执行本单位的任务或者主要是利用本单位的物质技术条件所完成的发明创造为职务发明创造。职务发明创造申请专利的权利属于该单位。申请被批准后，该单位为专利权人。该单位可以依法处置其职务发明创造申请专利的权利和专利权，促进相关发明创造的实施和运用。非职务发明创造，申请专利的权利属于发明人或者设计人；申请被批准后，该发明人或者设计人为专利权人。利用本单位的物质技术条件所完成的发明创造，单位与发明人或者设计人订有合同，对申请专利的权利和专利权的归属作出约定的，从其约定。

<sup>21</sup> 《专利法实施细则》第十三条规定，专利法第六条所称执行本单位的任务所完成的职务发明创造，是指：（一）在本职工作中作出的发明创造；（二）履行本单位交付的本职工作之外的任务所作出的发明创造；（三）退休、调离原单位后或者劳动、人事关系终止后1年内作出的，与其在原单位承担的本职工作或者原单位分配的任务有关的发明创造。专利法第六条所称本单位，包括临时工作单位；专利法第六条所称本单位的物质技术条件，是指本单位的资金、设备、零部件、原材料或者不对外公开的技术信息和资料等。

<sup>22</sup> 《中华人民共和国劳动合同法》第六十八条规定，非全日制用工，是指以小时计酬为主，劳动者在同一用人单位一般平均每日工作时间不超过四小时，每周工作时间累计不超过二十四小时的用工形式。



### 【典型案例】万某公司诉周某民等侵害商业秘密纠纷案<sup>23</sup>

**案情简介：**万某公司与周某民签订了《聘用合同书》，约定万某公司聘请周某民利用业余时间万为某公司进行网站制作和软件程序的开发。在上述《聘用合同》到期之后，合同双方未续签，但周某民仍继续为万某公司工作。之后周某民离开万某公司，另行搭建网站，使用了在万某公司兼职期间完成的软件程序，并获取了万某公司的用户信息数据库。万某公司起诉周某民侵犯商业秘密。周某民主张，其与万某公司不存在劳动关系，在兼职期间完成的软件和程序并非职务技术成果，搭建的网站也并非公司网站而是个人网站，由其与万某公司共有，周某民自行使用相关软件、程序和网站数据库信息的行为不构成侵权。法院审理认为，涉案网站的域名系由万某公司注册并拥有，并以万某公司作为网站的实际经营者对外进行商业运作。周某民系万某公司员工，参与涉案网站的技术开发、维护及商业运营等行为属于公司员工履行工作职责的行为，技术成果归属于万某公司。

#### 1.3.3 离职后商业秘密的归属

离职员工在新用人单位利用自身的基本技能为新用人单位创造收益时也伴着侵犯原用人单位商业秘密的风险。这是因为，员工在职期间为企业完成商业秘密的过程中也获得了个人基本技能的提升，导致员工基本技能的形成与企业商业秘密的形成过程紧密相关。换言之，员工在工作岗位中所掌握的知识、经验和技能中有一部分可能也构成企业的商业秘密。当员工离职后在新用人单位使用其基本技能时可能涉及对原用人单位商业秘密的使用，由此产生离职员工与原用人单位的商业秘密侵权纠纷。



### 【典型案例】某省食品公司等诉圣某公司、马某庆不正当竞争纠纷案<sup>24</sup>

**案情简介：**某省食品公司主要从事海带出口业务，马某庆为某省食品公司的员工，专门负责对日海带业务。马某庆于2006年12月与某省食品公司合同期满后离开了该公司加入以其侄子陈某荣为唯一股东的圣某公司，并且获得原本分配给某省食品公司的2007年度海带出口配额。某省食品公司认为马某庆的行为构成不正当竞争，故诉至法院。法院审理认为，虽然可以认定马某庆本人在原单位工作期间即筹划设立了圣某公司，意图与原单位开展竞争。但是，职工在职期间筹划设立新公司，为

<sup>23</sup> 上海市高级人民法院（2011）沪高民三（知）终字第100号民事判决书。

<sup>24</sup> 最高人民法院（2009）民申字第1065号民事裁定书。

自己离职后的生涯作适当准备，并不当然具有不正当性。此外，作为具有学习能力的劳动者，职工在企业工作的过程中必然会掌握和积累与其所从事的工作有关的知识、经验和技能。除属于单位的商业秘密的情形外，这些知识、经验和技能构成职工人格的组成部分，是其生存能力和劳动能力的基础。职工离职后有自主利用其自身的知识、经验和技能的自由，因利用其自身的知识、经验和技能而赢得客户信赖并形成竞争优势的，除侵犯原企业的商业秘密的情况外，并不违背诚实信用的原则和公认的商业道德。最终认定圣某公司、马某庆的行为不构成不正当竞争。

### 1.3.4 委托开发关系下商业秘密的归属

委托开发关系下商业秘密的归属由当事人自行约定，当事人可以约定技术成果归属于委托人，也可以约定归属于被委托人。如果没有约定或约定不明的，委托人和被委托人都有使用和转让的权利，即由当事人共同拥有。但是，被委托人在向委托人交付研究成果之前，不得转让给第三人。<sup>25</sup>另外，除当事人另有约定以外，委托开发中完成的技术成果的专利申请权属于被委托人。



#### 【典型案例】嘉某公司诉共某公司、派某公司侵犯商业秘密案<sup>26</sup>

**案情简介：**嘉某公司与共某公司签订《软件开发合作协议》及《补充协议》，约定合作开发的软件所有权由嘉某公司享有，未经嘉某公司书面同意，共某公司不得将合作开发软件成果及其组成部分以任何方式披露给第三方，也不得自己或许可第三方使用或者用于本委托协议约定以外的任何用途。2007年12月，派某公司派吴某开始和嘉某公司洽谈关于代理嘉某公司软件产品销售合作事宜。2008年1月，派某公司申请计算机软件著作权登记，申请登记的软件名称为《能耗监测管理平台软件》。嘉某公司遂指控共某公司违反双方的保密协议，将所有嘉某公司的商业秘密披露给派某公司使用，派某公司是在明知或应当知道共某公司披露其商业秘密的权利人是嘉某公司的情况下，仍然使用该商业秘密，并在市场上与嘉某公司形成竞争，构成共同侵权。法院审理认为，由于涉案软件是共某公司根据嘉某公司的要求专门进行编写，不为公众所知悉，能够为嘉某公司带来经济利益并且具有实用性，符合商业秘密

<sup>25</sup> 《民法典》第八百六十一条规定，委托开发或者合作开发完成的技术秘密成果的使用权、转让权以及收益的分配办法，由当事人约定；没有约定或者约定不明确，依据本法第五百一十条的规定仍不能确定的，在没有相同技术方案被授予专利权前，当事人均有使用和转让的权利。但是，委托开发的研究开发人不得在向委托人交付研究开发成果之前，将研究开发成果转让给第三人。

<sup>26</sup> 广东省高级人民法院（2011）粤高法民三终字第141号民事判决书。

的保护条件。根据嘉某公司与共某公司所签订的合同，该商业秘密的权利人是嘉某公司，共某公司对嘉某公司的商业秘密负有永久性的保密义务。在案证据可以认定共某公司在协议履行过程中，违反合作协议约定的保密条款，擅自向派某公司披露了嘉某公司的商业秘密；派某公司明知或者应当知道共某公司向其泄密的软件属于嘉某达公司商业秘密的情况下，仍然使用该商业秘密，构成共同侵权，应当承担相应的民事责任。

### 1.3.5 合作开发关系下商业秘密的归属

合作开发技术成果的商业秘密归属规则与委托开发的规则类似。如果双方没有就商业秘密权属作出明确约定，那么基于共有关系，任何一方均有权自行使用或以普通许可方式许可他人使用商业秘密，而不会对商业秘密的侵权。



#### 【典型案例】铭某公司诉林某彬侵犯商业秘密纠纷案<sup>27</sup>

**案情简介：**2010年开始，王某与ACI公司发生业务往来，并雇佣林某彬为业务助理，协助处理ACI公司相关业务。2012年7月，王某与铭某公司法定代表人刘某及案外人林某永签订《合作协议》，以在铭某公司下设业务六部的形式，共同组建外贸团队经营外贸业务，由王某担任铭某公司总经理，林某彬担任业务六部经理。2013年4月，王某将其与刘某、林某永合作一事告知ACI公司，ACI公司遂开始与铭某公司发生业务往来。其后，王某与刘某发生矛盾，王某离开铭某公司，成立J&S公司。林某彬得知后也离开铭某公司，加入J&S公司，双方共同竞争铭某公司的客户ACI公司，引发诉讼。铭某公司主张，涉案经营信息主要由铭某公司男鞋业务部成员共同获取并形成，王某作为铭某公司总经理，林某彬作为铭某公司男鞋业务部经理，对涉案经营信息的取得和形成，也付出了努力，但这些努力属于其职务行为，故涉案经营信息应属铭某公司所有。法院审理查明，从铭某公司和林某彬提供的相关邮件记录、聊天记录来看，涉案经营信息包括与ACI公司之间的客户信息、产品信息、供应商信息、报价信息等商业信息，均系合作团队取得和使用。根据2012年7月签订的《合作协议》，合作方共同承担风险，共同分享利益，在合作经营期间取得和形成的以涉案经营信息为核心的商业秘密，也属于合作方的重大利益，故王某对该商业秘密也享有共有权。但是，合作团队中的刘某系铭某公司法定代表人，合作团队的业务六部也设在铭某公司

<sup>27</sup> 浙江省温州市中级人民法院（2020）浙03民终513号民事判决书。



内部，相关订单以铭某公司名义签订，业务六部日常办公保障等也由铭某公司提供，铭某公司和合作团队在相关经费结算上也非泾渭分明，故本案并非典型的业务挂靠关系，铭某公司在涉案经营信息的取得和形成中也有重大贡献，对涉案商业秘密也有共有权。基于此，法院认定王某对其合作经营期间形成的以涉案经营信息为核心的商业秘密享有共有权，故林某彬将涉案经营信息发给王某，属于王某对其商业秘密权利的正当支配和使用。铭某公司主张林某彬侵害其商业秘密并要求停止侵权、赔偿损失的相关诉请，缺乏事实和法律依据，法院不予支持。





02

## 常见的泄密场景

## 2.1 人员泄密

人员泄密是商业秘密泄露中最常见且高风险的方式，例如员工可能在离职前复制或窃取公司的技术文档、客户名单、市场策略、财务数据等敏感信息，或者使用远程访问工具获取公司使用云服务储存的数据，并用于自己创业、加入竞争对手或出售给第三方公司。企业应采取有效措施加强内部管理，提高员工保密意识，确保商业秘密的安全。

### 2.1.1 跳槽泄密

跳槽泄密是指原单位员工跳槽到与原单位生产或经营同类产品、从事同类业务的具有竞争关系的其他用人单位后，依据其在原单位掌握的商业秘密，在现单位开展相关业务的情形。



#### 【典型案例】嘉兴某公司等诉王某公司等侵害商业秘密纠纷案<sup>28</sup>

**案情简介：**傅某自2008年起担任嘉兴某公司香兰素车间副主任，主要负责相关生产设备的维修维护工作，能够接触到该公司生产香兰素的技术秘密。傅某在离职前拒绝签订保密协议，并在离职后将技术秘密披露给了嘉兴某公司的竞争对手王某公司，导致嘉兴某公司的市场份额大幅下降。法院审理认为，傅某未按照该公司的要求签订保密协议，结合其辞职后进入王某公司香兰素车间工作的事实，可以认定其蓄意拒签保密协议。傅某无权获取、披露、使用或者许可他人使用，但其仍实施了被诉侵害涉案技术秘密的行为，有明显的主观恶意，因此法院判决王某公司、傅某等连带赔偿嘉兴某公司各项损失和支出共计1.59亿元。

### 2.1.2 自立门户泄密

自立门户泄密是指原单位员工利用自己掌握或通过不正当手段获取的原单位商业秘密，违反保密义务自己开设与原单位业务相似或相同的公司的情形。

<sup>28</sup> 最高人民法院（2020）最高法知民终1667号民事判决书。



### 【典型案例】香港某甲公司诉魏某乙等侵害商业秘密纠纷案<sup>29</sup>

**案情简介：**魏某甲、魏某乙、胡某曾为香港某甲公司董事，2007年他们在深圳成立深圳某公司，2011年，三人在深圳成立另一家香港某乙公司，魏某乙通过邮件告知香港公司客户自己和香港某甲公司关键人员将转移到新成立的香港某乙公司，告知客户与香港某乙公司进行交易。法院审理认为，魏某乙、胡某违反保密义务，向香港某乙公司、深圳某公司披露并允许使用其所掌握的香港某甲公司的客户名单经营秘密，香港某乙公司、深圳某公司不当使用了上述经营秘密，魏某乙、胡某及香港某乙公司、深圳某公司共同侵害了香港某甲公司的商业秘密。

#### 2.1.3 内外串通泄密

内外串通泄密是指存在与被侵权单位有竞争关系的另一方，以提供技术支持、物质奖励、许诺职位等方式贿赂、利诱被侵权单位员工违规窃取或违约披露被侵权单位商业秘密的情形。



### 【典型案例】厦门某公司诉深圳某公司、汪某、彭某、汤某侵害商业秘密纠纷案<sup>30</sup>

**案情简介：**厦门某公司为一家家政服务公司，为了实现对家政员工的有效管理，将员工ID、员工手机号码、员工工作岗位等信息录入中控后台Simba系统，并实时动态更新。2021年6月，汤某入职厦门某公司，双方签订《员工保密协议》，约定汤某未经厦门某公司许可不得擅自使用或向任何第三方透露公司的服务模式、员工待遇、服务方式、员工培训模式及培训内容、员工管理资料、规章制度等管理信息。其后，汤某违反保密义务，擅自向深圳某公司员工汪某、彭某提供其用于登录厦门某公司后台系统的账号、密码和验证码，获取了厦门某公司的员工ID、员工手机号码、员工工作岗位等信息，用于深圳某公司的招聘工作。法院审理认为，深圳某公司、汪某、彭某、汤某构成共同侵权，应共同承担停止侵权、赔偿损失的法律责任。



<sup>29</sup> 最高人民法院（2021）最高法知民终312号民事判决书。

<sup>30</sup> 广东省深圳市中级人民法院（2023）粤03民初6939号民事判决书。

## 2.2 信息发布

### 2.2.1 公开披露

公开披露是指将原本应保密的信息以某种方式主动向公众或特定群体公开，使得所属领域的相关人员可以从公开渠道获得该信息的情形。



#### 【典型案例】电某公司诉张某祥、李某锋等侵犯商业秘密纠纷案<sup>31</sup>

**案情简介：**电某公司是一家从事生产和销售微量元素分析仪器及医疗电子仪器的公司，一款名为MP系列溶出分析仪是其主导产品。张某祥、李某锋在电某公司从事溶出分析仪的技术工作，与电某公司签订的劳动合同中均约定有保密条款和竞业限制条款。电某公司发现，张某祥、李某锋借用他人名义成立得某仪器厂，生产与电某公司相同产品“微量元素分析仪”，遂向公安机关报案。侦查人员在李某锋处获取得某仪器厂生产的“微量元素分析仪”电路原理方框图，与电某公司提供的电路图相比，两种产品在基本原理、电路结构上一致。在法院审理过程中，电某公司自认其1991年电位溶出分析仪发明专利中即包含了电路图。法院审理认为，电某公司主张他人侵犯其商业秘密，应当首先证明其案涉技术信息构成商业秘密，但是电某公司本案主张的商业秘密信息已经其1991年电位溶出分析仪发明专利文献公开，且电某公司自己生产的商品上记载了元器件的详细特定参数，打开商品即可看见。因此，电某公司主张的技术信息已通过公开渠道即可获得，不具备“不为公众所知悉”的特征。

### 2.2.2 论文发表

论文发表是指科研人员通过论文发表将开发过程中泄密信息予以公开，导致企业商业秘密泄露的情形。

<sup>31</sup> 山东省高级人民法院（2009）鲁民三终字第167号民事判决书。



### 【典型案例】郝某某侵害商业秘密案<sup>32</sup>

**案情简介：**西北某公司是一家以从事铁路、航空航天和其他运输设备制造业为主的高新技术企业。2016年，该公司获得某项目立项，并与其他单位联合研发，根据协议约定，研发过程中形成的相关技术信息及成果均属商业秘密。2015年至2018年，郝某某担任西北某公司软件工程师，参与研发该项目。在此期间，郝某某为了晋升学位和职称，违反公司保密规定，利用职务便利秘密窃取该研发项目的设计开发文档、关键设备、参数等内容，用于撰写自己的硕士毕业论文。2020年1月至8月，该论文先后发表于知网、万方数据等知名网站，被多人浏览、下载，致使该研究项目失去新颖性，后续申请专利、申报奖项受阻。经第三方机构评估，该技术成果泄露，令涉事公司损失200余万元。2020年8月，西北某公司到公安机关报案。2023年8月，郝某某被执行刑事拘留。2024年11月，法院经审理认为，郝某某违反保密义务及权利人有关保守商业秘密的要求，以盗窃等不正当手段获取权利人的商业秘密并披露、使用该商业秘密，给权利人造成重大损失，其行为已构成侵犯商业秘密罪，据此依法判处郝某某有期徒刑1年并处罚金2万元。

#### 2.2.3 媒体泄密

媒体泄密是指通过媒体渠道，包括但不限于报纸、杂志、电视、广播以及互联网上的社交媒体、新闻网站等，未经授权公开了涉密信息的情形。特别是当商业秘密通过互联网被广泛传播，为公众所知悉时，可能导致权利人彻底丧失秘密性，进而在相关领域失去领先性，值得引起企业重视。



### 【典型案例】某汽车公司实车拍摄照片被泄露案

**案情简介：**关某为某汽车公司员工，与某媒体公司员工包某共同负责某汽车公司实车照片拍摄，双方在拍摄前均签署《保密承诺书》。2023年12月，某汽车公司发现其首款车型实车拍摄照片在发布前夕被恶意泄露。后经该公司保密管理团队查实，某媒体公司员工包某、某汽车公司员工关某在签署《保密承诺书》的情况下，未经许可有意泄露保密拍摄内容，某汽车公司将依据双方签署的《保密承诺书》追究该两人及所属媒体公司的泄密责任。

<sup>32</sup> 《以案说法 | 如此“作文”，可不行！》，2024年11月21日发布于“陕西高院”微信公众号。

## 2.2.4 外部咨询

外部咨询泄密是指员工在接受外部有偿咨询的过程中，有意或无意泄露商业秘密，导致企业的商业秘密被外部咨询方非法获取、使用或公开披露的情形。



### 【典型案例】刘某诉奥某公司劳动争议纠纷案<sup>33</sup>

**案情简介：**刘某在奥某公司担任高管，多次担任服装行业龙头企业等企业和协会的供应链顾问或总裁，具有深厚的行业背景和资历，且在入职公司前，已作为公众人物接受各大服装平台的访问和访谈，分享自己行业的经验。2021年8月，刘某收到奥某公司审计监察部发出的《监察调查告知承诺书》，并安排工作人员与刘某进行了面谈。面谈中刘某承认参与了4、5次访谈，每次1000元辛苦费，总价约5000元，大体聊了一些供应链基本打法、合伙人名字、供应商分布及大致数量。随后，奥某公司向刘某发出《解除劳动关系通知书》，称刘某利用在工作期间获得的信息、经验、资源或职务，在某平台接受付费咨询，在与公司无关的外部事务中为自己谋求私利，严重违反公司“利益冲突”相关制度及规定。刘某向劳动人事争议仲裁委员会申请仲裁，仲裁请求被驳回。刘某不服诉至法院。法院审理认为，奥某公司解除与刘某的劳动关系，并不违反《劳动合同法》第三十九条的规定，判决驳回刘某的全部诉讼请求。



**【温馨提示】**对于员工在职期间违反保密义务的，企业既可以提起劳动争议诉讼，也可以提起侵害商业秘密诉讼。相较而言，企业作为用人单位在劳动争议案件中具有举证优势，一般只要举证劳动者有违反保密义务的行为即可，而关于遵守保密协议或保密协议无效的事实，都由劳动者承担举证责任。例如在上述案件中，法院并未对刘某所披露的内容是否属于商业秘密作出认定，而是认为刘某的访谈内容确实存在披露patpat运营的相关情况，属于未经公司批准参加付费访谈活动并对外披露公司敏感信息的行为，违反了公司有关制度和规定，因此公司解除劳动合同并不违法。

<sup>33</sup> 广东省广州市中级人民法院（2023）粤01民终32726号民事判决书。

## 2.3 存储泄密

### 2.3.1 载体泄密

载体泄密是指商业秘密的物理或电子形式载体，如技术文档、技术图纸、计算机程序、生产的设备、产品等，在未经授权的情况下被非法获取、复制、使用或披露的情形。



#### 【典型案例】正某公司诉福某公司、马某、刘某等侵犯商业秘密案<sup>34</sup>

**案情简介：**刘某是正某公司的前员工。离职后，入职福某公司。趁人不在，潜入正某公司的办公室，拷贝正某公司与国外客户的销售经营信息的电子邮件。之后，刘某以正某公司电子邮件的格式、交易方法等客户经营信息内容为参照，用福某公司的产品名称、数量、库存商品最低成本价等信息制作成“模式化”（即固定邮件格式）的电子邮件，向从正某公司窃取的100多家国外客户发送了电子邮件。此后，福某公司陆续与国外一些客户取得联系并成交了出口脱水蔬菜的业务。正某公司据此主张福某公司、刘某侵害其商业秘密。法院审理认为，福某公司聘用马某和刘某时知道其曾为正某公司职工，并掌握该公司的经营信息，故其在尚无充分客户信息来源情况下成交大量外销业务，福某公司应当履行必要的审查职责。但福某公司对马某、刘某的行为未进行询问或审查，更未采取进一步措施制止，主观上存在过错。故福某公司对马某、刘某二人披露和使用正某公司商业秘密的不正当竞争行为应当承担民事责任赔偿损失。

### 2.3.2 产品流通

产品流通泄密是指在产品从生产、存储、运输到销售的整个流通过程中，企业的商业秘密可能因产品被拆解、反向工程等手段而被未经授权的第三方获取或公开的情形。



<sup>34</sup> 最高人民法院（2007）民三终字第1号民事判决书。





### 【典型案例】思某公司诉兰某公司侵害技术秘密纠纷案<sup>35</sup>

**案情简介：**思某公司研发的GTR-7001气体透过率测试仪包含了思某公司并未公开、不为公众所知悉的技术秘密。2017年9月，思某公司获知，兰某公司通过恶意发起的诉讼，利用诉讼保全程序非法获取思某公司技术秘密，并在2019年初在市场上公开推出包含与思某公司技术相同的智能模式检测仪器，构成商业秘密侵权。思某公司主张，其已经对上述技术秘密采取了合理的保密措施，包括：与员工签署包含保密条款的《劳动合同》与《企业与员工保密协议》，制定并实施了《公司保密管理制度》，对研发厂房、车间、机器等设置门锁，限制来访者的进出和参观等，还在测试仪特定位置贴上“危险！私拆担保无效！”等内容的标签。法院审理认为，涉案技术秘密的载体为测试仪，该产品一旦售出进入市场流通，就在物理上脱离思某公司的控制，故区别于可始终处于商业秘密权利人控制之下的技术图纸、配方文档等内部性载体。思某公司采取的“对内保密措施”，因脱离了涉案技术秘密的载体（即市场中流通的测试仪产品），与其主张保护的涉案技术秘密不具有对应性，故不属于《反不正当竞争法》规定的“相应保密措施”。同时，涉案技术秘密载体为市场流通产品，属于外部性载体，思某公司为实现保密目的所采取的保密措施，应能对抗不特定第三人通过反向工程获取其技术秘密。而思某公司贴附在产品上的标签并不构成可对抗他人反向工程的物理保密措施，故不符合涉案技术秘密及其载体的性质。法院最终认定，思某公司未采取符合《反不正当竞争法》规定的“相应保密措施”，其主张保护的涉案技术秘密因缺乏“相应保密措施”而不能成立。

<sup>35</sup> 最高人民法院（2020）最高法知民终538号民事判决书。

## 2.4 传输泄密

### 2.4.1 邮件发送

邮件发送泄密是指员工违反公司的相关保密要求，将含有商业秘密的文件通过电子邮件发送至个人邮箱或其他无关人员，使得该商业秘密脱离权利人的原始控制，导致商业秘密存在可能被披露和使用的风险的情形。



深圳市中级人民法院

**【典型案例】大连某数据平台管理中心诉崔某某侵害技术秘密纠纷案<sup>36</sup>**

**案情简介：**大连某数据平台管理中心为防止信息泄露，对于员工外发电子邮件实施后台监控，从而发现了崔某某擅自通过公司电子邮箱将公司技术信息发送至私人邮箱，并获取了其外发电子邮件的路径和内容。法院认定崔某某的行为构成“盗窃权利人商业秘密”，判决崔某某赔偿大连某数据平台管理中心经济损失25万元及制止侵权行为所支付的合理开支1.5万元。

深圳市中级人民法院



深圳市中级人民法院

**【温馨提示】**员工在工作中必须严格遵守保密规定，无论出于何种原因，都不得将公司内部商业秘密发送至个人邮箱或其他可能导致信息泄漏的平台。企业也应在保密协议中详细列举可能构成商业秘密侵犯的行为，以明确员工的保密义务。

### 2.4.2 微信泄密

微信泄密是指将企业的商业秘密通过微信非法向他人披露的情形，这可能包括将包含商业秘密的文件、信息、图像或音频通过微信聊天、微信群、朋友圈等途径发送等，导致信息的保密性被破坏。

深圳市中级人民法院



深圳市中级人民法院

<sup>36</sup> 最高人民法院（2021）最高法知民终1687号民事判决书。



### 【典型案例】某禽业公司诉龙某竞业限制纠纷案<sup>37</sup>

**案情简介：**某禽业公司是一家以养殖、批发、零售鸡、鸡蛋及相关技术咨询服务为主营业务的公司。龙某于2017年入职该公司从事销售工作，双方通过签订《劳动合同书》，约定了龙某的保密义务、竞业限制等内容。在职期间，龙某负责该公司的鸡蛋产品销售工作。为方便业务接洽，龙某组建“报单”微信群，该群内人员主要为某片区的蛋类购买客户，亦有该禽业公司销售主管石某等在内。客户在群内发布产品需求，龙某在群内进行接单，形成了较为固定的销售模式。龙某辞职后，并于次月到开展同类业务的“某庆福蛋品”公司工作。龙某将某禽业公司管理人员石某从该“报单群”移出，将群名称变更为“某庆福蛋品报货群”，自己的微信名称变更为“某庆福蛋品龙某187XXXX6715”，在该群内继续销售蛋品。某禽业公司发现该情况后，向法院提起诉讼，请求判令龙某立即停止违约行为，履行与其关于竞业限制的约定，支付违反竞业限制违约金并赔偿损失。法院审理认为，龙某属于法律规定的其他负有保密义务的人员，违反竞业限制义务，已侵犯了用人单位商业秘密，判决龙某支付某禽业公司违约金20000元。



### 【典型案例】金某公司诉吴某侵害商业秘密纠纷案<sup>38</sup>

**案情简介：**吴某于2018年5月23日入职金某公司，岗位为营业员。吴某在金某公司工作期间，曾长期使用金某公司用于拓展业务的微信号。2023年4月22日，吴某未离职之时，金某公司工作人员发现，吴某擅自以个人名义，向与金某公司保持稳定交易关系的特定客户销售“5G产品”。2023年5月15日，吴某提出离职申请。2023年5月17日，吴某使用金某公司业务微信号，擅自以金某公司名义建立新的微信群，将特定客户引流至新建立的微信群后，将金某公司业务微信号退群，解散原有的客户微信群，将部分客户“拉黑”，并私下销售与金某公司生产经营的同类产品。2023年5月27日，金某公司与吴某签订《员工离职协议》，双方在离职协议约定了保密条款，保密内容包括客户资料、销售数据等，吴某于当日离职。法院审理查明，吴某在销售所谓的5G产品时使用的仍然是工作手机微信而并非吴某的私人微信，微信聊天记录无法证明吴某实施了非法使用其客户信息；吴某使用工作手机另建微信群亦是使用金某公司的名义，金某公司并未举证证明其另建微信群实施非法使用其客户信息的行为。因此，判决驳回了金某公司的全部诉讼请求。

<sup>37</sup> 四川省简阳市人民法院（2021）川0180民初2434号民事判决书。

<sup>38</sup> 广东省深圳市中级人民法院（2024）粤03民终20220号民事判决书。



**【温馨提示】**客户微信群是企业与客户交流沟通信息的渠道，作为公司长期经营积累的客户资源明显具有商业价值。在司法实践中，针对交易习惯、意向、内容等相对固定的客户微信群，并且符合“不为公众知悉”“具有商业价值”“采取相应保密措施”三大构成要件的客户微信客户群，通常认定为属于用人单位商业秘密范畴予以保护。

深圳市中级人民法院

### 2.4.3 云盘泄密

网络云盘泄密是指通过云存储服务，未经授权或违反保密规定，将含有商业秘密信息的数据上传至云端，导致信息被非法访问、泄露或滥用的情形。由于网络云盘是一种很常见的存储工具，具有无实体盘、存储空间大且可随时上传下载等优势，但同时也因安全保密系数低容易遭受攻击，已成为发生频率较高的泄密渠道，将涉密信息上传至网盘无异于将其置于“高速裸奔”的状态下，导致泄密事件层出不穷。



### 【典型案例】新某公司诉派某公司侵害商业秘密纠纷案<sup>39</sup>

深圳市中级人民法院

**案情简介：**新某公司系涉案电影的制片者之一。2016年9月，新某公司与派某公司就涉案电影音频后期制作事宜签订《音频制作委托合同》，其中的保密条款约定，双方均应永久保守因履行上述合同从对方获得的包括涉案电影全片素材等秘密。在合同履行过程中，新某公司多次通过现场手递手交付的方式将涉案电影素材交予派某公司执行后期制作，此外，新某公司与涉案影片的其他参与方均签署了保密协议，采取了较为严格的保密措施。派某公司接受新某公司的委托后，违反保密约定将其中部分后期制作工作外包给案外人缪某所在公司实际执行。2017年3月，在新某公司将新一版涉案电影素材交付派某公司进行后期制作后，派某公司将涉案电影全片素材命名为“W\*Z”（即涉案电影名称的拼音首字母）通过某网盘传输给案外人缪某进行后期制作，该素材内容在某网盘中保存至2017年5月。在涉案素材在某网盘保存期间，虽然派某公司为网盘设置了密码，但仍被案外不法分子破解，并最终导致影片素材在涉案电影公映前通过互联网流出，且有人公开售卖，影响范围较广。法院审理认为，本案双方主要依赖手递手方式现场传递涉案素材，且有关电影拍摄的主要内容在公映之前必然属于制片者最为核心的经营信息，派某公司将涉案素材上传至某网盘，并以“W\*Z”即涉案电影名称的拼音首字母为名的行为，显然与上述经营信息的重要程度不相匹配，其对于涉案素材泄露在主观上存在重大过失，其行为亦构成侵犯商业秘密，最终判决派某公司赔偿新某公司经济损失300万元。

<sup>39</sup> 北京市朝阳区人民法院（2017）京0105民初68514号民事判决书。

## 2.5 对外合作

### 2.5.1 招投标

招投标泄密是指企业在参与招投标活动中，可能因提交含有商业秘密的投标文件或相关项目资料，而面临商业秘密泄露的风险的情形。若未能对涉密信息采取有效的保密措施，可能导致竞争对手获取并使用这些秘密信息，进而损害企业的合法权益。



深圳市中级人民法院

#### 【典型案例】程某中等与虹某公司等侵害商业秘密纠纷案<sup>40</sup>

**案情简介：**程某中、绿某公司在公开媒体邀请合作投资伙伴共同开发涉案房地产项目。应虹某公司法定代表人吴某的要求，程某中先后向其传真项目利润分析报告、《绿某公司意向书》等开发项目的详细资料。《意向书》中约定，提供的内容属于商业秘密，虹某公司对程某中提供的有关开发项目资料内容承担保密义务。在吴某收到两份项目利润分析报告内一周，吴某与政府就开发工程有关事宜会谈，虹某公司即决定投资涉案房地产项目，并由虹某五原分公司开发销售房地产项目，获巨额利润。法院认为，涉案商业秘密的商业价值主要体现在为房地产开发企业选择投资项目、做出投资决策提供帮助。虹某公司通过磋商获悉了程某中、绿某公司的涉案商业秘密，并违反程某中、绿某公司有关保守商业秘密的要求擅自使用其掌握的涉案商业秘密，构成侵害商业秘密。

### 2.5.2 许可转让

许可转让泄密是指在商业秘密的许可或转让过程中，由于相关方未能妥善遵守保密义务或未能采取足够的保密措施，导致商业秘密被非法披露或使用的情形。这可能涉及到未经授权的第三方获取商业秘密，或者被许可人超越了许可协议的范围使用商业秘密。

深圳市中级人民法院

级人民法院

<sup>40</sup> 最高人民法院（2013）民三终字第6号民事判决书。



### 【典型案例】花某公司诉盘某公司等侵害技术秘密纠纷案<sup>41</sup>

**案情简介：**花某公司是“有客多”小程序源代码的权利人，盘某公司与花某公司签订了《源代码使用许可合同》，约定盘某公司可以获取涉案软件源代码。然而，在取得源代码后，盘某公司未按照合同约定遵守保密义务，将源代码披露在公共网站上，使其成为了开源软件。花某公司的商业秘密泄露后，该产品总收入持续下降，从高峰时期的半年近350万下降到半年108万左右。法院审理认定侵权成立，并综合考虑了小程序生命周期等因素，判决盘某公司赔偿花某公司经济损失及合理维权费用共计500万元。盘某公司不服，上诉至最高人民法院，最高人民法院二审判决，驳回上诉，维持原判。



#### 2.5.3 服务外包

服务外包泄密是指企业将某些业务流程、技术支持或服务等服务外包给第三方服务提供商时，由于缺乏适当的保密措施或管理不善，导致商业秘密被外包服务提供商或其员工非法获取、使用或披露给未授权的第三方的情形。



### 【典型案例】君某公司诉泽某公司、大某公司侵害技术秘密纠纷案<sup>42</sup>

**案情简介：**君某公司研发了饲料胍基乙酸产品，君某公司与泽某公司签订有关胍基乙酸战略合作协议、加工协议，约定未经君某公司许可，泽某公司不得将胍基乙酸出售给除君某公司之外的任何第三方，并约定了合同期限和保密期限为3年。双方合作终止后，泽某公司与大某公司签订胍基乙酸产品许可合同。于是，君某公司诉至法院，主张泽某公司、大某公司侵害其商业秘密。法院审理认为，泽某公司违反保密约定，在战略合作协议、加工协议约定的保密期限内单独使用了涉案商业秘密，构成侵害君某公司商业秘密，应当承担的相应的民事责任。在战略合作协议、加工协议约定的保密期限内和保密期限届满后，泽某公司与大某公司共同实施了侵害君某公司商业秘密行为，应当承担连带赔偿责任。

<sup>41</sup> 广东省深圳市中级人民法院(2019)粤03民初4519号民事判决书。

<sup>42</sup> 最高人民法院(2020)最高法知民终621号民事判决书。

## 2.5.4 技术出资

技术出资泄密是指企业在技术出资的过程中，作为技术出资的商业秘密被非法获取、使用或披露给未授权的第三方的情形。技术出资是一种创新的资本运作方式，不仅能够促进科技成果的转化，还能为企业带来新的增长动力。然而，技术秘密在出资以后容易面临被泄露的风险，值得企业引起重视。



### 【典型案例】梦某公司诉翔某公司、柳某等侵害商业秘密纠纷案<sup>43</sup>

**案情简介：**金某公司董事长朱某经人介绍认识了柳某，双方磋商后，合意注册成立梦某公司，由柳某团队以马某公司名义代为履行技术入股，朱某团队由金某公司代为履行出资入股。柳某向梦某公司交付部分涉案技术秘密，梦某公司建设了部分生产线。此后梦某公司在与案外人协商融资的过程中披露了涉案技术秘密的出资评估报告，金某峰于2016年1月知悉了锂电池项目，与柳某协商后，由柳某携锂电池正极材料等制备技术与金某峰合作，双方组建翔某公司，开始投产生产锂电池，造成梦某公司部分建成的生产线瘫痪。梦某公司遂以侵犯商业秘密为由，起诉翔某公司、柳某等人。法院审理认为，涉案商业秘密部分由柳某代表马某公司交付给梦某公司，部分尚未交付。对于部分已经交付的商业秘密，梦某公司享有知识产权（即商业秘密知识产权）；对于尚未交付的部分商业秘密，梦某公司对马某公司享有取得商业秘密的合同债权（即商业秘密合同债权）。本案中，翔某公司、柳某、金某峰既侵害了梦某公司的商业秘密债权，又侵害了梦某公司的商业秘密知识产权，故判决翔某公司、柳某、金某峰连带赔偿梦某公司经济损失5000万元。

## 2.6 涉外泄密

### 2.6.1 境外诉讼

境外诉讼泄密是指在跨国或涉及不同法域的法律诉讼过程中，企业在提交证据、进行辩论或其他诉讼活动时，可能会无意中或由于缺乏适当的保密措施，导致商业秘密被披露给诉讼对方或其他未授权人员，从而造成商业秘密的泄露的情形。例如，在美国民事诉讼的证据开示程序中，当事方和某些非当事方有义务根据证据开示请求开示证据。证据开

<sup>43</sup> 最高人民法院（2021）最高法知民终814号民事判决书。



示的范围很广，通常与索赔或辩护相关且与案件需要相关的任何不受法律特权保护的事项都需要开示。在经过当事方协商后，如请求方认为被请求方无合理理由而拒绝开示，可以向法院提出动议，请求法院强制要求开示。如果法院审理后命令被请求方开示证据而被请求方仍故意不开示，可能会受到法院的制裁。如果中国的当事方在参加诉讼时未能合理应对以及妥善保护这些信息，就可能导致商业秘密的二次泄露。



### 【典型案例】欧特克（Autodesk）诉中望软件侵犯著作权和盗用商业秘密纠纷案<sup>44</sup>

**案情简介：**在加州北区联邦地区法院审理的一起侵犯著作权和盗用商业秘密纠纷案中，Autodesk有一款用于辅助设计的明星软件产品，声称中望软件在开发软件产品时，大量复制了Autodesk的源代码。Autodesk由此基于侵犯著作权和盗用商业秘密起诉中望软件。在诉讼过程中，Autodesk要求中望软件开示后者位于中国的软件源代码。中望软件主张，其作为一家正在成长的科技公司，源代码的向外输出可能会影响中国国家和经济的发展，故源代码应该属于中国《保守国家秘密法》下的国家秘密。然而，法院认为中望软件并未充分说明为何中国可能将该公司的源代码认定为国家秘密，且没有提供专家意见或法律渊源以支持其论点，或回应Autodesk专家的相反意见。最终法院强制中望软件开示证据。

## 2.6.2 人才引进

人才引进泄密是指企业在海外人才引进的过程中，未对引进人才的背景、原所在国法律法规、以及与原雇主的合同约定进行充分审查，可能导致违反相关国家的法律法规而面临被诉风险。这也提醒我国企业在引进海外人才时，需要提前关注人才引进国就竞争限制和商业秘密问题所制定的法律法规和政策趋势，防患于未然。



### 【典型案例】美国PPG集团诉江苏铁锚公司侵犯商业秘密案<sup>45</sup>

**案情简介：**2015年7月，美国PPG集团在宾夕法尼亚西区联邦地区法院起诉江苏铁锚公司，指控江苏铁锚公司雇佣了PPG集团的前雇员Thomas Rukavina，并通过该雇员获取了PPG集团的Opticor相关技术。

<sup>44</sup> Autodesk, Inc. v. ZWCAD Software Co., No. 5:14-CV-01409-EJD, 2015 WL 2265479 (N.D. Cal. May 13, 2015).

<sup>45</sup> PPG Indus. Inc v. Jiangsu Tie Mao Glass Co. Ltd, 47 F.4th 156 (3d Cir. 2022).



PPG集团并没有向法院提供证据以证明其实际损失，而主张江苏铁锚公司通过侵犯商业秘密获得不当得利。2021年6月，法院将PPG集团Opticor相关技术的研发费用作为评估江苏铁锚公司不当得利的基准，认定PPG集团的实际研发费用为约880万美元，判决江苏铁锚公司告向PPG集团支付约880万美元的补偿性赔偿约1800万美元的惩戒性赔偿，共计约2680万美元。



【典型案例】ASML诉XTAL盗窃商业秘密案<sup>46</sup>

**案情简介：**ASML公司是一家总部位于荷兰的半导体设备制造商，在全球光刻机市场上占据领先地位。2016年，ASML公司起诉XTAL公司，指控其通过聘用ASML前员工窃取商业秘密。为证实XTAL公司诱使ASML公司前员工违反诚信义务盗取核心OPC技术及商业机密，并利用这些技术以低价与ASML公司长期客户三星达成合作，ASML公司向法庭提交了在其前员工所持有的设备上存储有ASML商业秘密的证据。2018年11月28日，美国加州圣克拉拉联邦法院认定XTAL公司盗窃知识产权的行为属于恶意，裁定XTAL公司赔偿8.45亿美元。XTAL公司因破产无法支付赔偿，其知识产权最终被ASML公司接管。

2.7 研发测试

2.7.1 产品研发

产品研发泄密是指企业在产品研发过程中，由于管理不善、保密措施不到位或内部人员故意泄露等原因，导致产品的设计、配方、工艺、技术参数、试验数据等未公开的关键信息被非法获取或公开的情形，给企业带来经济损失或竞争优势的丧失。



<sup>46</sup> ASML US, Inc. v. XTAL, Inc., No.16-CV-295051 (Santa Clara Sup. Ct. May 3, 2019)



### 【典型案例】赛某公司诉华某公司、李某、张某等侵害商业秘密纠纷案<sup>47</sup>

**案情简介：**李某、张某原系赛某公司的总经理、董事，掌握赛某公司重要经营信息等。二人从赛某公司离职前，将赛某公司的熔炼过程记录表等资料上传至张某的个人网盘。赛某公司发现后诉至法院，主张李某、张某违反保密义务，未经许可擅自使用赛某保密技术信息等用于华某公司的经营。法院审理认为，赛某公司请求保护的熔炼过程记录表所记载的熔炼合金的原材料成分比例、材料状态、参数、数据等信息的组合，系在熔炼实验或生产过程中所形成，属于实验者或生产者所掌握的特定信息，该等信息虽系过程性数据，并未形成具体而明确的技术方案，但系实验者或生产者在具体的熔炼过程中所获得的技术成果，对于后续实验或生产具有明显的实际效用，应当认定为具有商业价值。李某、张某无正当理由，将公司的技术秘密擅自上传至个人网盘，使得相关信息脱离权利人的控制，即便其初始取得行为合法，也无实际披露、使用或允许他人使用上述技术秘密的行为，但明显存在披露风险或可能性，仍然应当认定为《反不正当竞争法》所规制的侵害商业秘密的行为，判决李某、张某停止侵权，并共同赔偿赛某公司经济损失及合理维权开支合计10万元。

深圳市中级人民法院

#### 2.7.2 游戏内测

游戏内测泄密是指游戏公司在游戏内测环节中，被内测玩家“剧透”游戏测试图片、视频等信息侵犯商业秘密的情形。游戏内测作为游戏正式上线前的重要环节，也是游戏开发周期中不可或缺的一环。司法实践中，将未公开的游戏角色、场景通常被认定为商业秘密范畴并加以保护。



### 【典型案例】某游戏公司诉陈某侵害商业秘密纠纷案<sup>48</sup>

**案情简介：**某游戏公司曾招募了多名游戏玩家参与发行前的测试，并与参与玩家签署了保密协议。2024年3月，某游戏公司通过监控发现陈某在参与某款游戏内测期间，擅自拍摄、录制了游戏画面并存储了还未公开的游戏设计，随时有向他人泄露的风险。于是某游戏公司向法院提起诉讼，主张陈某擅自获取并披露的未公开游戏角色、形象、技能及游戏画面等信息属于反不正当竞争法保护的商业秘密；陈某的偷录、偷摄行为违反了保密义务，以盗窃手段获取、披露并允许他人使用这些信息，侵犯了公司的商业秘密，请求判令陈某立即停止侵权行为，赔偿经

深圳市中级人民法院

<sup>47</sup> 广东省深圳市中级人民法院（2021）粤03民初1114号民事判决书。

<sup>48</sup> 上海市浦东新区人民法院（2024）沪0115行保2号民事裁定书。

济损失50万元，并刊登声明消除影响。法院审理认为，某游戏公司主张的案涉内容构成《反不正当竞争法》规定的商业秘密，陈某实施了以不正当手段获取并披露某游戏公司商业秘密的行为，构成侵权。最终判决陈某立即停止侵犯某游戏公司享有的商业秘密的不正当竞争行为，赔偿某游戏公司经济损失及为制止侵权行为所支付的合理开支共计50万元，并在判决生效之日起三十日内发布声明消除影响。

### 2.7.3 数据共享

数据共享泄密是指企业在合作研发的情形中，因与合作方共享研发数据导致商业秘密泄露的情形。数据共享可以显著提高合作研发效率，加速产品上市时间。但在数据共享过程中，如果数据共享平台或系统没有适当的访问控制或监管措施，研发人员可能会访问到敏感信息，导致商业秘密泄露。



#### 【典型案例】程某侵犯商业秘密案<sup>49</sup>

**案情简介：**某公司与一家通信公司为合作关系，共享服务器内的研发数据。程某是某公司原技术工程师，负责芯片硬件开发编程工作，配有公司服务器的登录账户，并具有查看、使用服务器内研发数据的权限。2021年6月，程某发现服务器存在漏洞，因觉得公司待遇低，便想窃取公司的研发数据，以备未来到其他公司工作时使用。程某多次绕开公司终端监控软件监管，将研发数据下载至其办公电脑，再传输至其个人电脑，还部分复制到个人移动硬盘。期间，程某先后通过上述方式盗窃某公司及这家通信公司研发数据378个，其中包括了系统“源代码”。2022年5月，这家通信公司发现了程某盗窃公司“源代码”的情况，便向公安机关报案，民警随后将其抓获。案发时，未发现程某披露、使用或允许他人使用其窃取的技术资料。经鉴定和评估，程某盗窃的这家通信公司“源代码”属于不为公众所知悉的技术信息，合理许可使用费为1436万元。法院审理认为，程某在公司仅负责编程工作，其在无公司合法授权的情况下复制、下载、传输公司技术秘密的行为，构成侵犯商业秘密罪，情节特别严重，故判处有期徒刑，并处罚金。

<sup>49</sup> 广东省东莞市第二人民法院（2022）粤1972刑初3545号刑事判决书。

## 2.8 区域泄密

区域泄密是指企业的涉密区域，由于未采取适当的物理隔离和防护措施，如门禁系统、监控设备等，导致遭受非法入侵或盗窃进而泄露商业秘密的情形。企业的研发部门、财务部门、营销部门等是企业日常工作中经常产生、传递、使用和管理商业秘密的关键区域，这些区域中存储和处理的信息往往具有高度的敏感性和商业价值，企业应当对上述区域采取有效的保密措施防止商业秘密泄露。



### 【典型案例】博某公司诉黄某秀侵害商业秘密纠纷案<sup>50</sup>

**案情简介：**博某公司是生产、销售运动用品的公司，其在开放式车间放置充气 and 消气两套设备，进入车间的人员均可接触到，博某公司为此设备安装了监控。黄某秀是其员工，与公司签署过《保密协议》，约定维护公司的商业秘密。工作期间，黄某秀用手机在车间内拍摄上述设备。博某公司以黄某秀侵害商业秘密为由向法院起诉。法院认为，博某公司在开放式的车间放置涉案设备，不能避免未签订《保密协议》的员工和外来人员接触涉案设备，采取的保密措施不足以确保涉案设备信息秘密不被第三人知悉，不符合合理保密措施的构成条件。因此，涉案设备不符合商业秘密的法定条件，判决驳回博某公司的全部诉讼请求。



<sup>50</sup> 广东省惠州市中级人民法院（2021）粤13民终6409号民事判决书。

03

企业商业秘密  
保护体系的建设

## 3.1 管理原则

### 3.1.1 分类管理原则

商业秘密的分类管理原则强调对商业秘密进行细致的分类，以便根据不同类型的商业秘密采取不同的保护措施和管理策略。这一原则的核心在于识别商业秘密的不同类型（如技术秘密、经营秘密等）和重要性（如绝密、机密、秘密、一般等），并据此制定差异化的保护方案。首先是确定商业秘密的类型，然后应当根据信息的敏感度和对企业的价值，将商业秘密分为不同的级别，每个级别对应不同的保密措施和访问权限。对于被确定为商业秘密的信息，应在其载体上明确标识保密级别。此外，企业应建立商业秘密清单，确定保密期限，记录绝密级别商业秘密的详细信息，包括其分类、创建日期、负责人、访问记录等。

### 3.1.2 最小接触原则

在商业秘密管理中，“最小接触原则”是一个关键的概念，该原则是指：只有那些真正需要知道商业秘密信息的员工才能接触到这些信息。通过贯彻最小接触原则，企业可以有效地减少商业秘密泄露的风险，保护企业的核心竞争力。同时，这也有助于企业提高员工对商业秘密保护的意识，形成一种保护企业资产的文化。基于最小接触原则，企业在保护商业秘密时，需要有效控制商业秘密的接触范围。企业可开展商业秘密评估工作，分析在经营活动中产生的技术信息和经营信息，筛选出涉密信息。确定商业秘密的范围可以参考的因素包括但不限于：

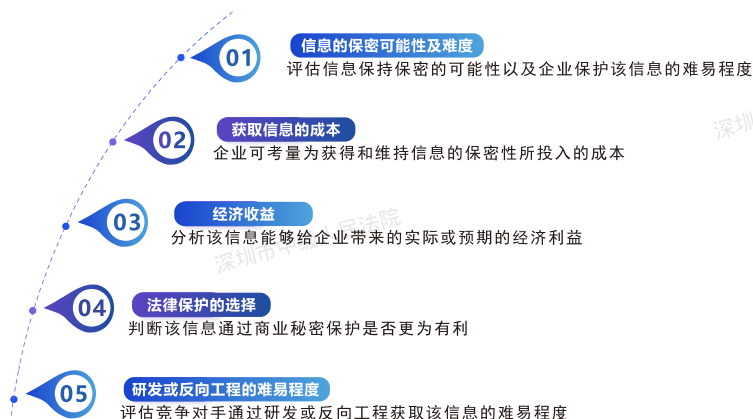


图1 确定商业秘密的范围图示

### 3.1.3 全流程管理原则

商业秘密管理的全流程管理原则侧重于对商业秘密从产生到销毁的整个生命周期进行全方位的管理和控制。这一原则的核心在于确保商业秘密在各个环节都得到有效的保护和管理，防止商业秘密的泄露和滥用。

### 3.1.4 合理利用原则

商业秘密保护的合理利用原则是指在确保自研保密信息不被泄露和授权获得的他人保密信息合法使用的前提下，企业应当有效利用这些信息以实现商业价值的最大化。第一，合法使用，确保所有商业秘密的披露和使用都符合法律法规的要求、相关协议的约定授权范围和使用期限内，即不侵犯他人的知识产权或违反相关法律，也不超范围披露和使用他人的知识产权。第二，最小化披露，在与第三方合作或进行交易时，只披露必要的商业秘密信息，并确保对方了解保密的重要性和相关信息的授权使用范围和期限。第三，风险评估，在披露自研保密信息和使用他人保密信息之前，进行风险评估，识别潜在的泄露和违约以及超范围使用风险，并制定相应的预防措施。

## 3.2 管理组织

### 专门的商业秘密管理机构

负责包括但不限于以下商业秘密管理工作：

- 企业商业秘密管理制度的建立、实施与完善
- 涉密信息、人员、载体、区域的管理
- 商业秘密管理的宣传、培训和考核
- 协同法务、人力、信息安全等机构共同管理
- 商业秘密合规审查，防控企业侵权风险
- 监督商业秘密管理工作的执行，对企业商业秘密管理体系进行评估与完善

### 企业最高管理者

- 应具备商业秘密管理意识
- 保障商业秘密管理工作的资源投入
- 将商业秘密管理要求融入企业的经营过程

### 各运营部门

- 各运营部门的管理者应作为部门内商业秘密管理的负责人
- 各运营部门内应指定商业秘密管理人员，负责商业秘密管理制度在本部门的落地

图2 管理组织图示



企业应提供建立、实施、维持与完善商业秘密管理制度所需的人力资源，构建一套由企业最高管理者、专门的管理机构及各运营部门内的管理人员组成的体系化管理组织，负责企业的商业秘密管理工作。

(1) 企业最高管理者应具备商业秘密管理意识，保障商业秘密管理工作的资源投入，将商业秘密管理要求融入到企业的经营过程中，并持续改进。

(2) 企业应建立专门的商业秘密管理机构，由企业最高管理者或其他高级管理者作为机构负责人，主导企业的商业秘密管理工作。在商业秘密管理机构内，可根据职能分工，设置不同的工作小组，履行以下职责：

- ①企业商业秘密管理制度的建立和完善；
- ②涉密信息、涉密人员、涉密载体、涉密区域的识别与管理；
- ③与商业秘密管理有关的宣传、培训和考核工作；
- ④协同法务、人力、信息安全等机构，处理泄密事件和法律维权工作；
- ⑤企业对外合作及人员聘用中的合规审查工作，防控企业侵权风险；
- ⑥监督商业秘密管理工作的执行，对企业商业秘密管理体系进行评估。

(3) 企业应指定各运营部门的管理者作为部门内商业秘密管理的责任人，并在各运营部门中指定专职或兼任的商业秘密管理人员，负责商业秘密管理制度在本部门的落地。同时，企业应内部公布商业秘密或信息安全违规管理相关规定，并授权法务部或者信息安全部例行审查违规行为并依据内部规定进行问责。

## 3.3 人员管理制度

### 3.3.1 内部人员管理

为了有效预防和控制商业秘密相关风险，企业需要有组织、有计划地进行人员管理。通过制定明确的制度，企业可以识别潜在风险，建立风险应对措施，并设立违规责任追究机制。在人员管理中，商业秘密风险通常表现为因员工行为或管理疏忽导致的商业秘密泄露、被盗用或滥用，进而引发法律纠纷或造成经济损失。常见的人员管理相关商业秘密风险包括但不限于未对招聘员工进行充分的背景调查以及员工离职后泄露商业秘密。

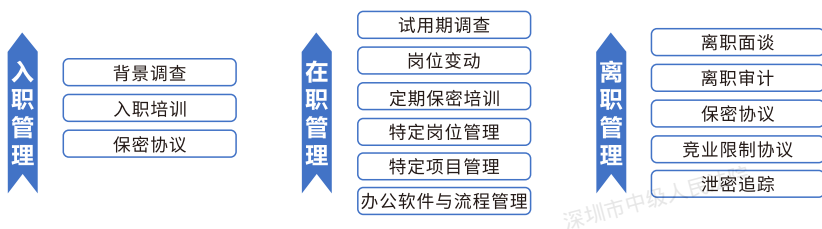


图3 内部人员管理图示

### 3.3.1.1 入职管理

(1) 背景调查：在全球化的商业环境中，企业招聘的员工来自全球各地，在引进人才之前，应进行背景调查来排查风险。企业在得到职位候选人授权后可进行详细的背景调查，确保其没有可能对本企业商业秘密构成威胁的历史或潜在可能性。对于曾在竞争对手企业工作过的候选人，入职前应要求其签署承诺书，保证尊重和保护第三方知识产权，并明确相关后果，以避免侵害本企业的商业秘密，并降低本企业对外侵权风险。背景调查包括但不限于以下内容：



图4 背景调查管理图示

➤ 对于涉外人才引进，还可进行下列背景调查：

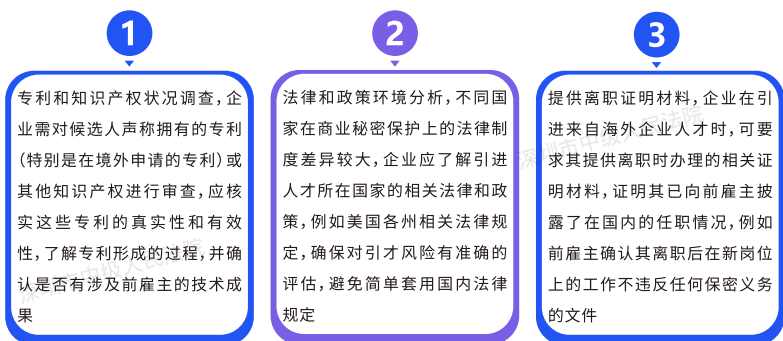


图5 涉外人员背景调查管理图示

(2)入职培训：采取多种形式、多种措施，对新员工进行全面的商业秘密保护的培训，强调保密的重要性和企业的保密管理规章制度。

(3)保密协议：要求新员工签署保密协议或包含保密条款的劳动合同，明确其保密条款和违反协议的后果。

### 3.3.1.2 在职管理

(1)试用期管理：对试用期员工实施IT权限限制监控，限制其对核心敏感信息的访问，直至其转正并融入团队。

(2)岗位变动：当员工岗位发生变动时，重新评估其对商业秘密的访问权限，并根据新的职责调整保密培训内容。

(3)定期保密培训：根据员工的部门和层级，制定定期的保密培训计划，以更新员工的保密知识和技能，强化保密意识。

(4)特定岗位管理：对企业中研发、商务、财务等部门内的核心岗位及重要涉密人员，应制定特殊的保密管理措施，并定期开展专项保密培训。

(5)特定项目管理：对于参与特定项目的员工，提供专项保密培训，明确项目中的保密要求和限制。确有必要时，需签署针对特定项目的保密协议。

(6)办公软件与流程管理：对内部使用的办公软件和办公流程进行安全管理，如设置访问权限、数据加密、监控异常访问行为等。



### 【典型案例】合某材料厂等诉东某公司、周某、陈某甲、陈某乙、李某侵害商业秘密纠纷案<sup>51</sup>

**案情简介：**合某材料厂、星某公司、中某公司均为化学材料公司，涉案产品为PBT改性产品，系中某公司主导生产，其他两家提供技术、人员服务。周某等人原为合某材料厂、星某公司、中某公司高管，并签订了相关保密协议。后周某等人自合某公司、星某公司、中某公司离职后加入东某公司。合某公司、星某公司、中某公司认为，周某等人接触并掌握其商业秘密，且均对其商业秘密负有保密义务，而东某公司利用其员工，非法使用其经营客户资料的行为，侵害了其商业秘密，遂将东某公司及周某等人诉至法院。法院审理查明，星某公司、中某公司在2003年《保密协议》中的确提出了保密要求，但该《保密协议》要求保密的相对人仅为周某一人。而从该五人的工作经历来看，知悉或可能知悉涉案技术信息的主体至少包括周某、陈某甲、陈某乙、李某等四人。因此，在有多人知悉或可能知悉涉案技术信息的情况下，星某公司、中某公司仅对其中一个相对人提出保密要求，不符合保密措施的“合理性”要求，也不能认定其已采取了合理的保密措施。此外，虽然周某等人长期在合某公司、星某公司、中某公司处工作，并担任重要职位，但基于公司法所规定的董事、监事、高级管理人员忠实义务中的保密义务，并不能完全体现商业秘密的权利人对其主张商业秘密所保护的信息采取保密措施的主观意愿和积极态度，不能构成作为积极行为的保密措施，显然亦不能免除权利人诉讼中对商业秘密采取合理保密措施的证明责任。法院最终认定合某公司、星某公司、中某公司并未采取合理的保密措施，驳回了三公司的诉讼请求。



**【温馨提示】**企业应当重视保密措施的覆盖，避免出现同一保密项目仅与部分员工签署保密协议等情况，否则就有可能不被认为采取合理的保密措施。

#### 3.3.1.3 离职管理

(1) 离职面谈：涉密人员离职前应与之谈话，告知其保密义务、禁止行为以及违反保密义务的法律后果，确保员工了解离职后的保密义务的具体内容。

(2) 离职审计：进行详细的离职审计，检查员工是否已妥善交接所有商业秘密资料，并确保没有未授权的复制或转移。

<sup>51</sup> 最高人民法院（2017）最高法民申1602号民事裁定书。

(3)保密协议：重申保密协议的条款，确保员工明白即使离职，保密义务仍然有效。

(4)竞业限制协议：根据实际需要，决定是否对离职员工（高级管理人员、关键技术人员等）启动竞业限制。如果适用，需向员工解释竞业限制协议的详细内容，确保其知悉在特定时间内不得为竞争对手工作或泄露商业秘密的保密义务。

(5)泄密追踪：定期追踪涉密岗位的离职员工离职前一定期限的文档下载、拷贝和外发行为进行追踪监控，发现潜在侵权行为。



深圳市中级人民法院

**【温馨提示】**公司董事、监事、高级管理人员的变动和离职，是商业秘密被泄露或者不当使用的主要途径之一。建议企业可以通过与员工签订竞业限制协议、保密协议或类似条款对核心商业秘密进行重点管理和保护。保密协议和竞业限制协议是企业用来保护商业秘密的两种不同的法律工具，往往需要组合使用。保密协议侧重于保护商业秘密不被泄露，适用范围较广，可以包括员工、合作伙伴等所有与企业有保密信息接触的个人或实体。竞业限制协议侧重于防止前员工利用企业的商业秘密进行竞争，通常只针对企业的高级管理人员、关键技术人员或其他能接触核心商业秘密的员工，并且需要给予一定经济补偿。企业需要考虑员工的合法权益，确保协议内容清晰明确，符合法律规定，避免因不合理的限制而影响协议的法律效力。



### **【典型案例】嘉兴某公司等诉王某公司等侵害商业秘密纠纷案<sup>52</sup>**

**案情简介：**傅某自2008年起担任嘉兴某公司香兰素车间副主任，主要负责相关生产设备的维修维护工作，能够接触到该公司生产香兰素的技术秘密。傅某在离职前拒绝签订保密协议，并在离职后将技术秘密披露给了嘉兴某公司的竞争对手王某公司，导致嘉兴某公司的市场份额大幅下降。法院审理认为，傅某未按照该公司的要求签订保密协议，结合其辞职后进入王某公司香兰素车间工作的事实，可以认定其蓄意拒签保密协议。傅某无权获取、披露、使用或者许可他人使用，但其仍实施了被诉侵害涉案技术秘密的行为，具有明显的主观恶意，因此法院判决王某公司、傅某等连带赔偿嘉兴某公司各项损失和支出共计1.59亿元。

<sup>52</sup> 最高人民法院（2020）最高法知民终1667号民事判决书。



【温馨提示】该案中，嘉兴某公司制定的保密措施文件包括但不限于：《文件控制程序规定》《记录控制程序规定》《设备/设施管理程序规定》《食品安全、质量和环境管理手册规定》《各部门岗位职责规定》《职工手册规定》《档案与信息化管理安全保密制度》《保密协议》等，这也提醒企业应当全方面对商业秘密的范围和员工的保密义务作出约定。

### 3.3.2 外部人员管理



图6 外部人员管理图示

#### 3.3.2.1 涉密外部活动

企业在对外交往中应当注意一方面保护己方的商业秘密，防范泄露秘密信息；另一方面，避免在对外交往中不当披露和使用他人保密信息，导致商业秘密纠纷和诉讼。涉及到商业秘密的常见活动有：涉密产品参展、项目交流、招投标、签约、项目实施、商业秘密的许可转让以及企业并购等。企业在和外部人员如专家、顾问、翻译、律师等有合作时，应进行背景调查，并签订保密协议。企业在接受外部单位的检查、审计等活动前，也应预先签订保密协议。

### 3.3.2.2 管理方式

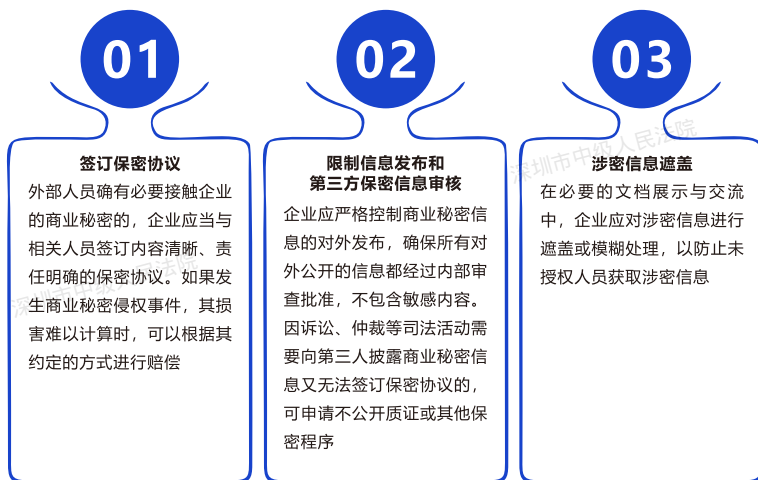


图7 管理方式图示

## 3.4 涉密载体管理

### 3.4.1 涉密载体的类型

商业秘密是一种包含技术信息、经营信息等在内的商业信息，信息是抽象的，故权利人实施的商业秘密保护措施需要围绕相关的涉密载体展开，而管理涉密载体的第一步便是识别出相关涉密载体，当前常见的涉密载体包括但不限于：纸质文件、计算机、智能手机、生产设备、模型、产品、原材料、移动存储介质、信息系统。<sup>53</sup>



**【温馨提示】**商业秘密和承载商业秘密的涉密载体是不同的，商业秘密是一种抽象的信息，记载或者体现在某种有形或可感知的载体上。比如：某种化合物为公众所知悉，其本身可能是商业秘密的载体，而不可能成为商业秘密的保护对象，可以作为商业秘密保护的只能是该物质的配方、制造、加工或者储藏的工艺等。

<sup>53</sup>《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》第六条第四、五项的规定，以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的，对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的，在正常情况下足以防止商业秘密泄露的，人民法院应当认定权利人采取了相应保密措施。



### 3.4.2 涉密载体的管理

为保障商业秘密安全，企业应对涉密载体的全流程进行严格管理，确保各个环节都符合安全要求。涉密载体管理的具体流程可参考如下步骤：

(1) 管理职责与权限设置：企业应指定专人负责管理涉密载体，包括涉密计算机、智能手机、文档等。在管理过程中，应明确各岗位的职责与权限，确保涉密载体的使用、配置、维护、回收、销毁等各个环节有专人负责，禁止未经授权的人员接触或处理涉密载体；

(2) 硬件配置与使用管理：涉密载体应统一管理，禁止员工私自处理或更改载体配置；涉密载体例如计算机应设置专用的登录账号和密码，确保只有授权用户可以访问；同时涉密区域内应禁止录音录像等，防止涉密信息泄露；

(3) 信息系统与软件安全措施：对于计算机信息系统，应根据涉密信息的级别配置合格的保密设备和软件，防止泄密和窃密；操作系统和办公软件需定期更新和检查，确保无安全漏洞；使用单位邮箱和加密软件时，应具备关键字过滤、外发邮件审批等保密功能，禁用或者限用外部即时通讯工具和网络硬盘等可能导致泄密的软件来对外传输涉密文件；

(4) 访问权限与日志管理：建立健全的访问控制制度，对涉密信息系统和载体的访问进行严格管理；指定专员管理涉密信息系统的访问权限，在权限到期、人员离职或项目变更时及时回收或调整权限；应保留权限管理的记录日志，定期检查用户权限设置和使用情况，及时发现漏洞；

(5) 涉密载体的使用和流转：确保只有授权的人员在规定的区域和时间内使用涉密载体；涉密载体在使用过程中，应防止和外部设备连接和网络访问；对于流转中的涉密载体，应设置专用通道和传输工具，以防未经授权的人员接触和使用载体。



对于涉及商业秘密的各项载体，企业应根据商业秘密及其载体的性质，制定具体制度管理其建立、分类、存储、接触、使用、更新及销毁的过程。<sup>54</sup>

- (1)标识管理：企业应及时确定涉密载体，并对其进行标记、分类，注明密级、保密期限等信息。
- (2)分类管理：企业应将内部性载体与外部性载体进行区分管理，分别制定不同的保密措施，以使保密措施与涉密载体具有对应性。
- (3)存储管理：企业应将涉密信息存储于经授权的信息系统和存储设备内，实施隔离、加密、封存等保密措施。
- (4)权限管理：企业应对涉密文件、设备、数据库或信息系统的接触与准入进行限制，如执行密码口令、限制获取的人员范围、限制使用、访问、存储、复制等管理措施。
- (5)安全管理：企业应及时对信息系统进行病毒检杀、漏洞修复。
- (6)销毁管理：涉密载体的销毁应经商业秘密管理组织审批后实施，销毁过程应由商业秘密管理组织全程监督。

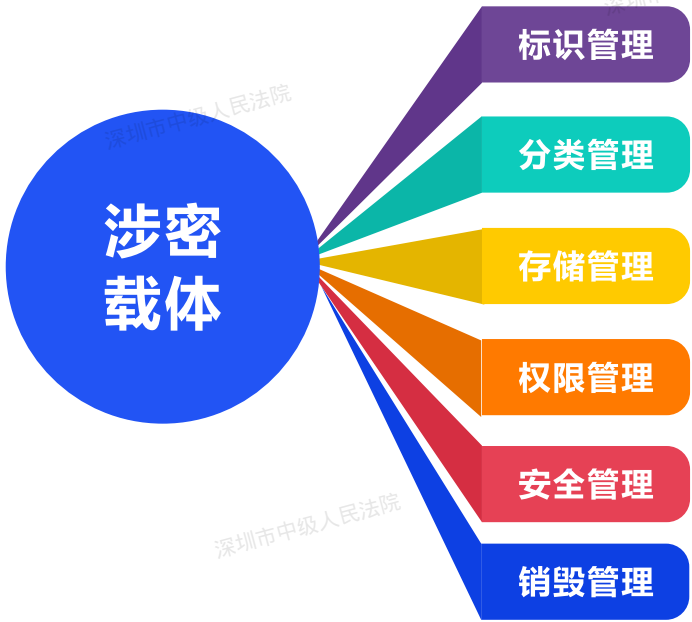


图8 涉密载体管理图示

<sup>54</sup> 同上注。



**【温馨提示】**商业秘密权利人所采取的保密措施，不应是抽象的、宽泛的、脱离商业秘密及其载体而存在的保密措施，而应当是具体的、特定的、与商业秘密及其载体存在对应性的保密措施。



### **【典型案例】零某公司诉鼎某公司、周某、魏某、赵某、李某侵害技术秘密纠纷案<sup>56</sup>**

**案情简介：**周某、魏某、赵某、李某原为零某公司员工，从事产品研发及销售工作，从零某公司离职后设立鼎某公司。零某公司遂起诉主张上述人员及鼎某公司生产、制造、销售的电源模块侵害了零某公司技术秘密。该案中，零某公司主张保护的技术秘密，其载体包括两方面内容，一是产品技术图纸，另一是根据该产品技术图纸制造的产品，且这些产品均已市场流通。法院审理认为，根据技术图纸制造的产品在争议发生前均已进入市场流通，故涉案技术秘密的载体为相应进入市场流通的电源模块产品，而产品一旦售出进入市场流通，就在物理上脱离零某公司的控制，故区别于可始终处于商业秘密权利人控制之下的技术图纸、配方文档等内部性载体。零某公司主张其采取的内部保密措施，因脱离涉案技术秘密的载体（即市场中流通的电源模块产品），与其主张保护的涉案技术秘密不具有对应性，不属于该案中针对市场流通产品的“相应保密措施”，最终认定涉案技术秘密不构成商业秘密。



### **【典型案例】某甲公司诉程某某、某乙公司侵害商业秘密纠纷案<sup>56</sup>**

**案情简介：**某甲公司系某技术秘密权益人，相关技术信息体现于该公司的多份研发记录文件中，以上文件均标明了密级。程某某原系某甲员工，劳动合同约定其负有保密义务，并由某甲支付相应保密费用，双方签订的《关于商业秘密、知识产权、无利益冲突协议》对商业秘密的范围及程某某承担保密义务的方式作了明确约定。后程某某从某甲公司离职后入职某乙公司，并向某乙公司披露前述技术秘密。某乙公司使用前述技术秘密生产、销售产品。某甲公司以程某某、某乙公司侵害技术秘密为由，将程某某、某乙公司诉至法院。法院审理认为，某甲公司提交的多份研发记录文件可以证明其长期从事与涉案商业秘密相关的技术研发，且体现了涉案商业秘密的主要内容。证据显示，某甲公司对其主张的商业秘密采取了合理保密措施，且商业秘密已被程某某、某乙公司侵犯。程某某、某乙公司虽然认为所有密点均已被现有文献所披露，但

<sup>55</sup> 最高人民法院（2021）最高法知民终1440号民事判决书。

<sup>56</sup> 该案例入选上海市第三中级人民法院、上海知识产权法院2024年4月公布的一批商业秘密典型案例。

提交的证据并不足以证明该主张，故涉案信息构成某甲公司的技术秘密。程某某对涉案技术秘密负有保密义务，其向某乙公司披露涉案技术秘密的行为构成侵权。某乙公司与某甲公司具有同业竞争关系，应当知道某甲公司在本案中主张的技术信息构成商业秘密，但仍予以获取并使用，构成侵权，遂判令程某某、某乙公司停止侵权，共同赔偿某甲公司经济损失100万元及维权合理开支30万元。

### 3.5 涉密区域管理

企业内部的厂房、车间、办公室等生产经营场所中，可能包含以下重要涉密区域：核心产品的研发、生产、展览区域；存储有涉密信息的数据中心、文档中心；存放重要设备、原材料、模型、产品的仓库等。对于涉密区域，企业应制定具体制度对其进行管理。<sup>57</sup>

(1)隔离管理：企业应使用独立、封闭区域作为涉密区域，对涉密区域和非涉密区域应进行明确区分，并在涉密区域进行物理隔离，设置醒目标识与禁入提示。

(2)门禁管理：企业可在涉密区域设置门禁系统，应制定准入审批流程，对进入涉密场所的人员范围、权限等进行明确限制，确有必要的，应安排专人陪同进入。

(3)安防管理：企业应在涉密区域设置录像监控及警报等安防机制，并根据需要配备专门的安保人员，限制手机、平板、智能手表等电子设备的携带。

(4)应急管理：企业应针对涉密区域建立专门的应急管理预案，在确保管理人员人身安全的前提下，做好商业秘密保护工作。

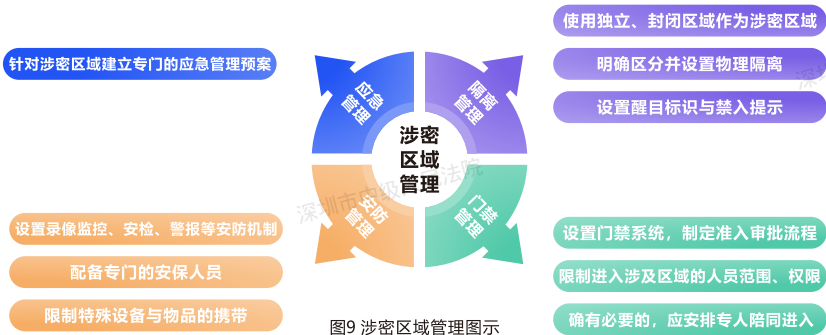


图9 涉密区域管理图示

<sup>57</sup> 《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》第六条第三项规定，对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的，在正常情况下足以防止商业秘密泄露的，人民法院应当认定权利人采取了相应保密措施。



### 【典型案例】圣某公司诉陈某刚、晋某公司侵害技术秘密纠纷案<sup>58</sup>

**案情简介：**圣某公司系“硝基苯法合成RT培司工艺”和“利用RT培司生产橡胶防老剂4020工艺”的技术秘密权利人。圣某公司主张，案外人翔某公司的法定代表人兼实际控制人陈某刚指使该公司两名员工通过利诱圣某公司技术人员窃取涉案技术秘密，用于建造、使用涉案生产设备，严重侵害其技术秘密；翔某公司另案被判决构成侵害商业秘密犯罪后申请破产清算，但又另行成立晋某公司，取代翔某公司继续实施侵权行为，遂提起诉讼。法院审理查明，圣某公司及相关主体采取了多项内部管控措施。对于办公场所、车间电脑、纸质文档均采取了加密措施，对于生产、办公场所实行登记管理制度，来访者参观应由专人陪同，特殊安全区域（如研发部）实行控制，确有需要才被允许进入；实行涉密文件分级管理制度，涉密文件必须存放在上锁的区域；不准员工个人电脑保留保密数据，不准无关人员进入计算机房接触保密信息；明确员工离职后仍应遵守保密义务等。结合圣某公司实施的其他保密措施认定圣某公司主张的22个技术信息符合技术秘密构成要件。



<sup>58</sup> 最高人民法院（2022）最高法知民终816号民事判决书。

04

企业  
维权

## 4.1 行政途径

企业商业秘密被他人不正当竞争行为侵犯的，可以向市场监督管理部门投诉举报，由市场监督管理部门进行认定查处后实施行政处罚。对市场监督管理部门作出的行政处罚决定不服的，可依法提起行政复议或行政诉讼。

### 4.1.1 投诉举报

商业秘密的权利人认为其商业秘密受到侵害时，可以向市场监督管理部门投诉举报侵权行为，经调查侵权行为成立的，侵权人应当承担相应的行政责任。

#### 4.1.1.1 管辖

举报由被举报行为发生地的县级以上市场监督管理部门处理。<sup>59</sup>向市场监督管理部门提出举报的，应当通过市场监督管理部门公布的接收举报的互联网（如12315平台）、电话（12315专用电话）、传真、邮寄地址、窗口等渠道进行。深圳地区还可通过“深圳12345”微信公众号，按照页面提示填写相关信息，上传请求书、相关证据等附件。

#### 4.1.1.2 立案门槛

根据深圳地区实践，行政立案应符合以下条件：



图10 立案门槛管理图示

权利人申请立案后，市场监督管理部门自收到立案材料之日起15个工作日内予以核查，并决定是否立案；特殊情况下，可以延长15个工作日内决定是否立案。

<sup>59</sup> 《市场监督管理投诉举报处理暂行办法》第二十五条规定，举报由被举报行为发生地的县级以上市场监督管理部门处理。法律、行政法规、部门规章另有规定的，从其规定。第三十一条第二款规定，举报人实名举报的，有处理权限的市场监督管理部门还应当自作出是否立案决定之日起五个工作日内告知举报人。



### 4.1.1.3 证据准备

权利人通过行政路径保护商业秘密时需要提交的证据材料主要包括以下几种：

(1) 请求保护的商业秘密权利主体资格。请求人应为此商业秘密的权利人，或者与权利人具有独占使用许可、排他使用许可关系的被许可人。普通使用许可合同的被许可人须经权利人书面授权。

(2) 请求保护的商业秘密应符合商业秘密的法定构成要件。包括该商业秘密的产生过程、载体、具体秘密点内容、商业价值、不为公众所知悉以及对其采取的具体保密措施等。

(3) 被举报人具有接触或实施侵犯该商业秘密行为的相关证明材料。

(4) 被举报人使用的技术信息和经营信息与投诉人请求保护的技术信息和经营信息具有一致性或相同性。

(5) 其他表明商业秘密被侵犯的证据。

行政执法案件的证明标准相对较低，一般要求权利人提供侵权行为可能存在的初步证据（一般符合秘密性证据）即可。

### 4.1.1.4 行政调查

在行政执法案件中，市场监管部门依法享有行政强制调查权，可以有效弥补权利人私力取证的不足。根据《反不正当竞争法》第十三条<sup>60</sup>的规定，监督检查部门调查涉嫌不正当竞争行为，可以采取下列措施：

(1) 进入涉嫌不正当竞争行为的经营场所进行检查；

(2) 询问被调查的经营者、利害关系人及其他有关单位、个人，要求其说明有关情况或者提供与被调查行为有关的其他资料；

(3) 查询、复制与涉嫌不正当竞争行为有关的协议、账簿、单据、文件、记录、业务函电和其他资料；

(4) 查封、扣押与涉嫌不正当竞争行为有关的财物；

(5) 查询涉嫌不正当竞争行为的经营者的银行账户。

<sup>60</sup> 《反不正当竞争法》第十三条第一款规定，监督检查部门调查涉嫌不正当竞争行为，可以采取下列措施：（一）进入涉嫌不正当竞争行为的经营场所进行检查；（二）询问被调查的经营者、利害关系人及其他有关单位、个人，要求其说明有关情况或者提供与被调查行为有关的其他资料；（三）查询、复制与涉嫌不正当竞争行为有关的协议、账簿、单据、文件、记录、业务函电和其他资料；（四）查封、扣押与涉嫌不正当竞争行为有关的财物；（五）查询涉嫌不正当竞争行为的经营者的银行账户。

#### 4.1.1.5 行政处罚

行政处罚适用一般程序或者简易程序。一般程序需自立案之日起90日内作出处理决定，因案情复杂或者其他原因，不能在规定期限内作出处理决定的，经市场监督管理部门负责人批准，可以延长30日。简易程序<sup>61</sup>可以当场作出行政处罚决定。根据深圳地区实践，行政处罚的一般程序包括：立案、调查取证、案件核审、处罚/听证<sup>62</sup>告知、处罚决定与执行及结案等环节。具体流程如下图：



<sup>61</sup> 深圳地区行政处罚简易程序的适用情形：违法事实证据确凿并且执法有法定依据，对自然人处以二百元以下、对法人或者其他组织处以三千元以下罚款或者警告的行政处罚的，可以当场作出行政处罚决定。

<sup>62</sup> 《深圳市行政听证办法》第二十二规定，具有下列情形之一的，行政机关应当根据行政相对人或者利害关系人的申请组织听证；行政机关认为有必要的，也可以依法提起听证：（一）拟作出较大数额罚款、没收较大数额违法所得、没收较大价值非法财物、降低资质等级、吊销许可证件、责令停产停业、责令关闭、限制从业等行政处罚的；（二）拟作出的行政许可直接涉及行政相对人之间重大利益关系的；（三）法律、法规或者规章规定的其他情形。



### 【典型案例】深圳某游戏公司侵犯他人商业秘密及著作权案<sup>63</sup>

**案情简介：**投诉人深圳某甲公司反映深圳某乙公司涉嫌窃取和侵犯其公司产品软件的商业秘密及软件著作权等知识产权。经市场监管部门现场检查发现，深圳某乙公司在开发一款与深圳某甲公司爆款游戏产品类似的竞技类游戏，尚未上市；经鉴定机构鉴定，深圳某甲公司涉案技术信息的密点在2023年2月9日前不为公众所知悉，具有非公知特性。经调查，深圳某乙公司该款游戏开发团队项目负责人黄某曾就职于深圳某甲公司，在职期间签署了保密协议。经鉴定机构数据提取及鉴定，深圳某乙公司公司服务器及员工电脑均大量存在与深圳某甲公司高度一致的代码等技术信息，且已应用到与深圳某甲公司同类型的手机游戏项目中。经评估机构评估，深圳某甲公司涉案商业秘密研发成本为260万元、许可使用费为1000万元。市场监管部门审查认为，深圳某乙公司使用以不正当手段获取商业秘密的行为，给深圳某甲公司所造成的损失价值已达到刑事追诉标准，依法将该案移送公安机关侦办。

#### 4.1.1.6 行政调解

行政调解一般适用于基于消费者权益争议引发的行政投诉，调解需经投诉人和被投诉人同意，由市场监督管理部门或由其委托的消费者协会、依法成立的其他调解组织等单位代为调解。实践中，在行政举报案件中也可以在市场监督管理部门的组织下进行调解。调解不成的，权利人可以另行提起诉讼。



### 【典型案例】深圳某科技公司侵犯他人商业秘密案<sup>64</sup>

**案情简介：**深圳市市场监管部门根据深圳市某科技公司的举报，深入核查出竞争对手公司安插在该公司内部、多次窃取商业报价的卧底员工，并依法对该员工和竞争公司进行行政处罚。在市场监管部门的行政调解下，双方自愿达成《和解协议》，由涉案供应商赔付该公司520万元赔偿金，保护了该公司的商业秘密，助力该公司于2023年底顺利上市。



<sup>63</sup> 该案例入选深圳市市场监督管理局2024年6月公布的一批侵犯商业秘密典型案例。

<sup>64</sup> 该案例入选广东省市场监督管理局公布2023年度广东省商业秘密保护大事件。

#### 4.1.1.7 行政责任

市场监督管理部门可依据《反不正当竞争法》第二十一条<sup>65</sup>责令经营者以及其他自然人、法人和非法人组织停止违法行为，没收违法所得或罚款。

(1) 责令停止违法行为。包括但不限于以下两种情况：

① 责令并监督侵权人将存有商业秘密的图纸、软件及其他有关资料返还权利人；② 监督侵权人销毁使用权利人商业秘密生产的、流入市场将会造成商业秘密公开的产品，但权利人同意收购、销售等其他处理方式的除外。

(2) 没收违法所得。违法所得是指实施违法行为所取得的款项，应当理解为实施违法行为的全部收入，而不应当理解为扣除成本的“获利”。

(3) 罚款。一般情形处十万元以上一百万元以下的罚款；情节严重的，处五十万元以上五百万元以下的罚款。

#### 4.1.2 行政复议与行政诉讼

申请行政复议，当事人对行政机关作出的行政处罚决定、行政强制措施不服的，可以自知道或者应当知道该行政行为之日起六十日内向作出决定的行政机关提出行政复议申请。

提起行政诉讼，可分为以下三种情况：

(1) 对行政复议机关作出的复议决定不服的，当事人可以自收到复议决定书之日起十五日内，依法向人民法院提起行政诉讼。

(2) 行政复议机关决定不予受理或者受理后超过行政复议期限不予答复的，当事人可以自收到不予受理决定书之日起或者行政复议期满之日起十五日内，依法向人民法院提起行政诉讼。

(3) 当事人对行政处罚决定和行政强制措施不服的，应当自知道或者应当知道该行政行为之日起六个月内，直接向人民法院提起行政诉讼。



**【温馨提示】**当事人申请行政复议，行政复议机关已经依法受理的，在行政复议期间不得向人民法院提起行政诉讼。当事人向人民法院提起行政诉讼，人民法院已经依法受理的，不得申请行政复议。

<sup>65</sup> 《反不正当竞争法》第二十一条规定，经营者以及其他自然人、法人和非法人组织违反本法第九条规定侵犯商业秘密的，由监督检查部门责令停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处五十万元以上五百万元以下的罚款。

#### 4.1.3 探索行政与司法深度衔接

近年来，深圳市场监管部门、法检部门致力探索建立行政与司法深度衔接机制，增强打击合力。一方面，行政案件中发现涉嫌犯罪的，办案机关应当依相关规定及时移送司法机关。另一方面，司法机关在诉讼案件中发现行政执法线索的，也可以及时移送市场监管部门。以深圳法院为例，深圳法院目前已建立与深圳市场监管部门的协作机制，在诉前调解阶段，主动将涉及外部协查案件的材料推送至市场监管部门，第一时间为市场监管部门提供精准的行政执法线索，通过多元化、高效率的途径加速纠纷的化解进程，进一步优化了市场环境，提升了司法与行政执法的协同效能。此外，在当事人因客观原因无法取得相关行政执法案件的有关证据时，可以依据《民事诉讼法》的相关规定向法院申请调查取证。



#### 【典型案例】堃某公司等侵犯商业秘密系列案<sup>66</sup>

**案情简介：**李某于2012年入职豪某公司担任机械工程师，双方签订了劳动合同、保密协议。2016年，李某与他人共同成立堃某公司，于2017年从豪某公司离职，进入堃某公司担任总经理，主要负责公司的技术研发和销售经营。李某违反豪某公司有关保守商业秘密的要求，利用其掌握的豪某机械“HOMAG封边机”的技术信息和图纸，通过堃某公司生产封边机并对外销售，造成豪某机械经济损失。2020年12月，上海市市场监督管理局认定堃某公司构成侵犯商业秘密的违法行为，责令堃某公司立即停止违法行为，并处罚款150万元。堃某公司不服上述行政处罚决定，向上海某区人民法院提起诉讼。法院审理认为，上海市场监督管理局作出的被诉行政处罚决定，事实清楚、法律适用正确、裁量适当，故判决驳回堃某公司诉讼请求。2021年11月，豪某公司以堃某公司侵犯其商业秘密为由，向上海知识产权法院提出诉讼。法院审理认为堃某公司通过李某获取并使用了涉案技术秘密，其行为构成侵权，据此全额支持了豪某公司主张的经济损失及维权合理开支200万元。2022年2月，上海某区人民检察院以被告人李某犯侵犯商业秘密罪向人民法院提起公诉。法院以犯侵犯商业秘密罪判处被告人李某强有期徒刑，并处罚金；违法所得依法予以追缴；扣押在案的侵权产品、犯罪工具及供犯罪所用的本人财物，依法予以没收等刑事处罚。

<sup>66</sup> 该案例入选上海市市场监督管理局2024年9月公布的商业秘密保护十大典型案例。



【温馨提示】该案提醒企业可以通过知识产权民事保护、行政执法监督、刑事打击“三位一体”的举措，整体协同联动进行商业秘密维权，切实维护企业的合法权益。

## 4.2 民事途径

企业商业秘密被他人的不正当竞争行为侵犯的，可以向人民法院提起民事诉讼。

### 4.2.1 协商和解

在权利人发现侵权行为的初期，权利人与侵权人可以本着真实自愿的原则协商解决，其目的是使权利人付出最低的成本而实现利益的最大化，常见的方式包括发送律师函、商务谈判等等。协商解决一般仅适用于侵权影响较小的情况。在侵权人已经给企业造成严重损失的情况下，双方往往较难达成和解。



### 【典型案例】新某医用氧设备公司、陆某琪诉瑞某供氧设备公司、李某献、李某红侵害技术秘密纠纷案<sup>67</sup>

**案情简介：**新某医用氧设备公司、陆某琪系“径向进气类紊流智能可调吸附式富氧技术”的权利人，其认为，李某献在担任新某医用氧设备公司高管期间，违反保密协议及保密规定，私自设立瑞某供氧设备公司，并招募掌握涉案技术秘密的新某医用氧设备公司技术骨干李某红等人，大量生产、销售侵害涉案技术秘密的医用分子筛制氧设备，遂提起诉讼，请求判令李某献、李某红、邯郸市瑞某供氧设备公司停止侵害并连带赔偿损失500万元。在该案起诉前，新某医用氧设备公司、陆某琪与瑞某供氧设备公司、李某献在更早的一起技术秘密侵权纠纷中签订《和解协议书》，确认瑞某供氧设备公司、李某献不构成侵权，且未要求瑞某供氧设备公司、李某献停止使用涉案技术信息。法院审理认为，基于前案《和解协议书》既不能认定新某医用氧设备公司、陆某琪已经与瑞某供氧设备公司、李某献达成转让或者许可实施涉案技术秘密的协议，也不能推定新某医用氧设备公司、陆某琪明确同意瑞某供氧设备公司、李某献在支付前案和解款后可以在后续生产经营过程中自由、无偿地使用涉案技术秘密，更不意味着新某医用氧设备公司、陆某琪对于瑞某供

<sup>67</sup> 最高人民法院（2023）最高法知民终120号民事判决书。

氧设备公司、李某献给付和解款及签收前案民事调解书后，对于后续针对涉案技术秘密可能发生的新的侵权行为预先放弃司法救济。故改判李某献、李某红、瑞某供氧设备公司立即停止侵害涉案技术秘密；李某献、瑞某供氧设备公司连带赔偿500万元；李某红对上述赔偿数额中的100万元承担连带赔偿责任。

#### 4.2.2 仲裁

劳动合同或保密协议中有约定仲裁条款，或者发生纠纷后双方就纠纷的解决达成仲裁协议的，应当按照约定向相关仲裁机构申请仲裁。劳动仲裁由劳动合同履行地或者用人单位所在地的劳动争议仲裁委员会管辖。其他商事仲裁则应由仲裁协议约定的仲裁机构管辖。商事仲裁实行“一裁终局”制度，裁决自作出之日起即与人民法院生效的法律文书具有同等法律效力，当事人持有仲裁裁决书可以向人民法院申请强制执行。



**【温馨提示】**对于劳动者与用人单位之间的因竞业限制协议引发的纠纷，如果用人单位以违约为由主张权利，则属于劳动争议，应当通过劳动争议处理程序解决；如果用人单位以侵犯商业秘密为由主张权利，则属于不正当竞争纠纷，人民法院可以直接予以受理。

#### 4.2.3 民事诉讼

##### 4.2.3.1 管辖

###### (1) 地域管辖

因侵犯商业秘密提起的诉讼，由侵权行为地或者被告住所地人民法院管辖。<sup>68</sup>侵权行为地，包括侵权行为实施地、侵权结果发生地。<sup>69</sup>侵权结果地应当理解为侵权行为直接产生的结果的发生地，不能简单地以原告受到损害就认定原告住所地是侵权结果发生地。

侵权行为实施地和结果发生地通常是重合的，亦即，使用商业秘密的过程，一般是制造侵权产品的过程，当侵权产品制造完成时，使用商业秘密的侵权结果即同时发生。由于销售侵犯商业秘密所制造的侵权产品不属于《反不正当竞争法》第九条规定的“使用”商业秘密的行为，不宜将该侵权产品的销售地视为使用商业秘密的侵权结果发生地。

<sup>68</sup> 《民事诉讼法》第二十九条规定，因侵权行为提起的诉讼，由侵权行为地或者被告住所地人民法院管辖。

<sup>69</sup> 《民事诉讼法司法解释》第二十四条规定，民事诉讼法第二十九条规定的侵权行为地，包括侵权行为实施地、侵权结果发生地。



## (2) 级别管辖

深圳市中级人民法院知识产权法庭管辖深圳市辖区内第一审技术秘密纠纷民事案件以及50亿元以下超出基层法院管辖标的的经营秘密纠纷案件。对上述技术秘密纠纷民事一审判决不服的，向最高人民法院知识产权法庭提起上诉。深圳市各区法院审理各自辖区内标的额在1000万元以下的第一审经营秘密纠纷民事案件。<sup>70</sup>



### 4.2.3.2 主体资格

提起侵害商业秘密纠纷的原告可以为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权利人，也可以为商业秘密的被许可人。具有下列情形之一的，被许可人具备原告诉讼主体资格：<sup>71</sup>

(1) 商业秘密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；

(2) 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；

(3) 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。



**【温馨提示】**如果使用许可合同对许可方式没有约定或者约定不明确，应当视为普通使用许可。

### 4.2.3.3 证据准备

权利人可根据维权方案，确定证据收集的内容、范围和方式：

<sup>70</sup> 《最高人民法院关于北京、上海、广州知识产权法院案件管辖的规定》第一条、第二条、《最高人民法院关于同意广东省深圳市两级法院继续管辖专利等知识产权案件的批复》、《最高人民法院关于第一审知识产权民事、行政管辖的若干规定》第一条、《最高人民法院关于调整高级人民法院和中级人民法院管辖第一审民事案件标准的通知》第一条。

<sup>71</sup> 《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》第二十六条规定，对于侵犯商业秘密行为，商业秘密独占使用许可合同的被许可人提起诉讼的，人民法院应当依法受理。排他使用许可合同的被许可人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的，人民法院应当依法受理。普通使用许可合同的被许可人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的，人民法院应当依法受理。



图12 证据准备图示

适用举证责任倒置的情形：<sup>72</sup>

(1)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。

(2)商业秘密权利人提供初步证据合理表明商业秘密被侵犯，且提供以下证据之一的，涉嫌侵权人应当证明其不存在侵犯商业秘密的行为：

①有证据表明涉嫌侵权人有渠道或者机会获取商业秘密，且其使用的信息与该商业秘密实质上相同；

②有证据表明商业秘密已经被涉嫌侵权人披露、使用或者有被披露、使用的风险；

③有其他证据表明商业秘密被涉嫌侵权人侵犯。

针对上述“有证据表明商业秘密已经被涉嫌侵权人披露、使用或者有被披露、使用的风险”的情形，权利人可以进一步提供证据材料以证明“商业秘密已经被涉嫌侵权人披露、使用或者有被披露、使用的风险”。例如：

<sup>72</sup> 《反不正当竞争法》第三十二条规定，在侵犯商业秘密的民事审判程序中，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。商业秘密权利人提供初步证据合理表明商业秘密被侵犯，且提供以下证据之一的，涉嫌侵权人应当证明其不存在侵犯商业秘密的行为：（一）有证据表明涉嫌侵权人有渠道或者机会获取商业秘密，且其使用的信息与该商业秘密实质上相同；（二）有证据表明商业秘密已经被涉嫌侵权人披露、使用或者有被披露、使用的风险；（三）有其他证据表明商业秘密被涉嫌侵权人侵犯。

- ①被告生产的含有原告商业秘密的产品、产品手册、宣传材料、计算机软件、文档；
- ②被告与第三方订立的含有原告商业秘密的合同；
- ③被告所用被诉侵权信息与原告商业秘密相同或实质上相同的鉴定报告、评估意见、勘验结论；
- ④包含原告商业秘密的产品说明书、宣传介绍资料；
- ⑤针对原告商业秘密的密钥、限制访问系统或物理保密装置等被破解、规避的记录；
- ⑥能反映原告商业秘密被窃取、披露、使用的证人证言；
- ⑦被告明知或应知他人侵犯商业秘密仍提供帮助或提供便利条件的相关材料；
- ⑧被告教唆、引诱、帮助他人侵犯商业秘密的录音录像、聊天记录、邮件；
- ⑨可以证明被告实施侵犯商业秘密行为的其他证据。



#### 【典型案例】龙某公司诉元某公司、刘某喜等侵害技术秘密纠纷案<sup>73</sup>

**案情简介：**刘某喜等人在龙某公司任职期间参与了“地测空间管理信息系统”有关技术的研发，后加入元某公司。龙某公司认为元某公司在其软件产品中利用了龙某公司的技术秘密，故提起诉讼。一审法院以证据不足为由，判决驳回其诉讼请求。龙某公司不服，提起上诉，主张其相关流程、逻辑关系、算法等也构成技术秘密，应予救济。最高人民法院二审认为，技术秘密的本质是技术信息，软件的流程、逻辑关系、算法等原则上构成相对独立的技术信息。龙某公司主张有关流程、逻辑关系、算法等构成技术秘密，应当具体说明并举证，因其未能尽到举证和说明义务，遂判决驳回上诉，维持原判。

#### 4.2.3.4 证据保全

在证据可能灭失或者以后难以取得的情况下，当事人可以在诉讼过程中向人民法院申请保全证据，人民法院也可以主动采取保全措施。当

<sup>73</sup> 最高人民法院(2020)最高法知民终1472号民事判决书。

事人可以在起诉前申请证据保全，也可以在起诉后申请证据保全。申请证据保全的，应当在举证期限届满前向人民法院提交书面申请。<sup>74</sup>

商业秘密纠纷案件中申请证据保全的，应当在保全申请中明确商业秘密的具体内容，同时提供载有商业秘密的文档、计算机软件、产品、数据库等证据。

4.2.3.5 行为保全

对于可能因当事人一方的行为或者其他原因，使判决难以执行或者造成当事人其他损害的案件，当事人可以向人民法院申请裁定责令其作出一定行为或者禁止其作出一定行为；当事人没有提出申请的，人民法院在必要时也可以裁定采取保全措施。<sup>75</sup>当事人可以在起诉前申请行为保全，也可以在起诉后申请行为保全。

诉前行为保全是利害关系人因情况紧急于诉前向人民法院申请禁止被申请人为一定行为的保全措施，以避免其合法权益受到难以弥补的损害。在侵害商业秘密纠纷案中，如果涉案秘密在诉讼前夕存在被进一步泄露的风险，对权利人造成难以弥补的损害，权利人可以及时向法院申请行为保全。法院在审查诉前行为保全申请时，一般考虑如下因素：

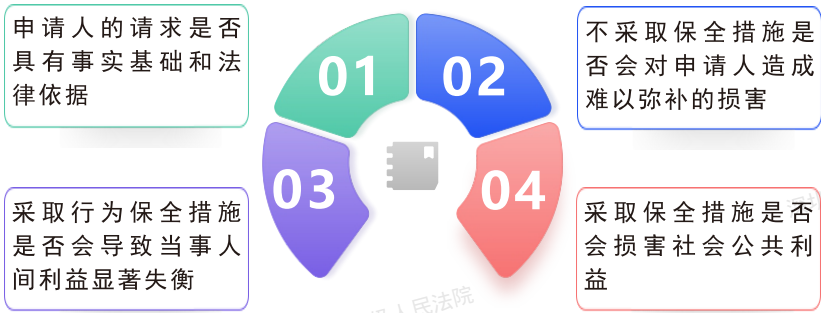


图13 行为保全考虑因素图示

<sup>74</sup> 《最高人民法院关于民事诉讼证据的若干规定》第二十五条规定，当事人或者利害关系人根据民事诉讼法第八十一条的规定申请证据保全的，申请书应当载明需要保全的证据的基本情况、申请保全的理由以及采取何种保全措施等内容。当事人根据民事诉讼法第八十一条第一款的规定申请证据保全的，应当在举证期限届满前向人民法院提出。法律、司法解释对诉前证据保全有规定的，依照其规定办理。

<sup>75</sup> 《民事诉讼法》第一百零三条第一款规定，人民法院对于可能因当事人一方的行为或者其他原因，使判决难以执行或者造成当事人其他损害的案件，根据对方当事人的申请，可以裁定对其财产进行保全、责令其作出一定行为或者禁止其作出一定行为；当事人没有提出申请的，人民法院在必要时也可以裁定采取保全措施。



## 【典型案例】某游戏公司诉陈某侵害商业秘密纠纷案<sup>76</sup>

**案情简介：**某游戏公司曾招募了多名游戏玩家参与发行前的测试，并与参与玩家签署了保密协议。2024年3月，某游戏公司通过监控发现陈某在参与某款游戏内测期间，擅自拍摄、录制了游戏画面并存储了还未公开的游戏设计，随时有向他人泄露的风险。某游戏公司遂向法院提出诉前行为保全申请。法院审理认为，某游戏公司合法享有的该款游戏及其角色设计，属于不为公众所知悉、具有商业价值并经权利人采取相应保密措施的经营信息，即属于反不正当竞争法规定的商业秘密。陈某存在实施了擅自摄录行为的较大可能性，如不加以规制，将会破坏游戏的平衡性和公平性、降低游戏的热度和关注度、打乱游戏公司的商业和经营安排、贬损游戏公司的商业信誉和社会评价。于是，法院在接到申请后的48小时内依法作出裁定，责令陈某不得披露、使用、允许他人使用其在参与某款游戏内测过程中擅自摄录的游戏内容。



### 4.2.3.6 预防二次泄密

为防止商业秘密在诉讼过程中被二次披露，权利人可向法院申请不公开审理和保密申请。向法院提出保密申请的，可以：

(1) 申请法院告知对方承担保密义务。具体形式可以是法院记入笔录，由诉讼参与人签字，或者由诉讼参与人签署承担保密责任的承诺书等书面文件；



(2) 申请法院对相关证据保密。具体形式可以是裁判文书中不披露商业秘密实质性内容、卷宗标注密级、保密证据归入副卷等；

(3) 根据具体案情，还可考虑提出证据保全、财产保全、延期举证、申请证人出庭、申请专家辅助人、技术鉴定、价值评估、调查令、临时禁令等各种申请；

(4) 对于涉及专业知识的，可申请一至两名具有专门知识的人员出庭就案件的专门性问题进行说明。此类专业人员不属于事实证人，其所作的说明属于技术性解释。出庭的专家辅助人之间以及其与当事人、鉴定人之间，可以相互询问。

<sup>76</sup> 上海市浦东新区人民法院(2024)沪0115行保2号民事裁定书。

#### 4.2.3.7 司法鉴定

侵犯商业秘密民事纠纷案件中的司法鉴定一般涉及以下内容：

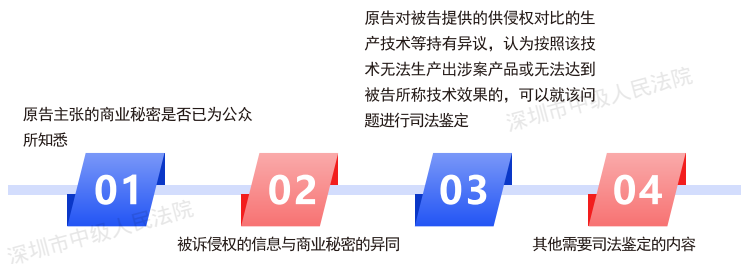


图14 司法鉴定图示

对于商业秘密案件审理中涉及的技术事实查明，可以通过技术咨询、技术调查官辅助审理、技术鉴定、当事人聘请专家辅助人等多种方式辅助解决。

当事人申请鉴定，应当在人民法院指定期限内书面提出，并预交鉴定费用。逾期不提出申请或者不预交鉴定费用的，视为放弃申请。<sup>77</sup>



#### 【典型案例】马某公司诉洛某公司、睿某公司、吕某华、周某、蔡某群侵害商业秘密纠纷案<sup>78</sup>

**案情简介：**加拿大某模具公司是涉案“热流道喷嘴”技术秘密的权利人，马某公司获得了该技术秘密的独占许可。吕某华从马某公司离职后，通过其儿子设立洛某公司，并实际控制睿某公司，生产车间挂睿某公司厂牌，营业执照登记信息为洛某公司。经营过程中，吕某华还招聘了周某、蔡某群等原马某公司员工。2018年6月，经马某公司举报，市场监管部门委托北京某知识产权司法鉴定中心，对马某公司主张的涉案技术秘密进行鉴定，鉴定意见为相关技术信息不为公众所知悉。马某公司遂提起诉讼。法院审理认为，洛某公司、睿某公司、吕某华、周某、蔡某群侵害包括上述技术秘密在内的涉案商业秘密，判决洛某公司、睿某公司、吕某华、周某、蔡某群停止侵害、共同赔偿损失及维权合理开支200万元。

<sup>77</sup> 《最高人民法院关于民事诉讼证据的若干规定》第三十一条规定，当事人申请鉴定，应当在人民法院指定期间内提出，并预交鉴定费用。逾期不提出申请或者不预交鉴定费用的，视为放弃申请。对需要鉴定的待证事实负有举证责任的当事人，在人民法院指定期间内无正当理由不提出鉴定申请或者不预交鉴定费用，或者拒不提供相关材料，致使待证事实无法查明的，应当承担举证不能的法律后果。

<sup>78</sup> 最高人民法院（2022）最高法知民终26号民事判决书。

### 4.2.3.8 常见抗辩

#### (1) 自行开发研制

开发者通过自行开发研制方式获得的商业秘密，尽管与权利人的商业秘密相同或者实质相同，但不应当认定为侵犯商业秘密的行为。



#### 【典型案例】明某公司诉尤某、纳某公司侵害技术秘密纠纷案<sup>79</sup>

**案情简介：**明某公司主张尤某在明某公司任职期间，通过破解公司电脑接触到涉案技术秘密，其所在的纳某公司在其离职后短期内即生产出与明某公司的结焦抑制剂配方高度相似的同类产品。尤某则辩称其系通过自己的聪明才智掌握了结焦抑制剂作用原理。法院审理认为，明某公司主张的配方信息，包括客户名称、发货日期、数量及针对客户需求的配方，其配方的成分及配比系根据客户锅炉结焦形成的原因结合应用场景所形成，需要付出时间和成本进行研发才能够获得。如无一定的研发投入及技术积累，短期内难以开发出适合特定客户需求的结焦抑制剂产品。尤某从明某公司离职后仅四个月，其成立的公司即转型生产出结焦抑制剂产品，而尤某此前并无结焦抑制剂的相关知识背景与从业经历，其公司也未能提供研发资料证明其产品的研发过程。如果没有掌握发货统计表中的客户及所对应的配方信息，被告短期内难以开发出同类产品。尤某辩称其通过自己的聪明才智掌握了结焦抑制剂作用原理的理由明显与常理不符。



**【温馨提示】**在司法实践中，自行研发的技术来源抗辩是否能够得到法院支持，应当综合考虑研发者的技术能力、技术水平、技术规模，以及研发者和权利人之间的竞争关系，是否存在不当窃取、盗窃权利人的商业秘密的可能性。为此，研发者可以提供自行开发研制的研发费用、开发文件、研发记录、音视频文件予以证明。

#### (2) 反向工程

是指通过技术手段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息。<sup>80</sup>通过反向工程获得被诉侵权信息的，

<sup>79</sup> 最高人民法院（2022）最高法知民终275号民事判决书。

<sup>80</sup> 《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》第十四条规定，通过自行开发研制或者反向工程获得被诉侵权信息的，人民法院应当认定不属于反不正当竞争法第九条规定的侵犯商业秘密行为。前款所称的反向工程，是指通过技术手段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息。被诉侵权人以不正当手段获取权利人的商业秘密后，又以反向工程为由主张未侵犯商业秘密的，人民法院不予支持。



不属于侵犯商业秘密行为。但是，侵权人以不正当手段知悉了权利人商业秘密之后，又以反向工程为由主张其行为合法的，或者法律、行政法规对某类客体明确禁止反向工程的，则反向工程抗辩不能成立。此外，反向工程应当是实际发生的，而不能是仅仅一种技术手段可能性，如被诉侵权人当庭抗辩只需要拆解权利人投入市场的产品再行组合即可完成，而没有提供可以证明被诉侵权人对该产品进行了反向工程研究的数据记录、资金投入及生产试验等方面的证据，法院一般不予支持。



### 【典型案例】青岛某公司诉郭某等侵害技术秘密纠纷案<sup>81</sup>

**案情简介：**郭某原为青岛某公司员工，其到北京某公司任职后二年内仍对青岛某公司的技术秘密负有保密义务，北京某公司申请名称为“一种用于模制纵向轨枕的模具”的实用新型专利，该专利与青岛某公司的技术秘密具有同一性。青岛某公司认为郭某、北京某公司侵害其商业秘密。在该案审理过程中，郭某提出反向工程抗辩。法院审理认为，鉴于郭某在青岛某公司任职期间实际接触过涉案模具技术图纸，且北京某公司、郭某等未提交其确实是通过反向工程手段实际获取涉案技术秘密的证据，故对其反向工程抗辩不予支持。

### (3) 合法授权

是指通过签订商业秘密许可或转让合同，从商业秘密的原始权利人（或有权处置人）处获得商业秘密于一定期限之内的使用权或所有权。

### (4) 个人信赖

是指客户基于对职工个人的信赖而与职工所在单位进行交易，该职工离职后，能够证明客户自愿选择与其自己或者其新单位进行交易的，应当认定没有采取不正当手段。被诉侵权人往往可以提供所涉行业领域强调个人技能的行业特点说明，客户明确其系基于对员工个人的信赖自愿选择交易的声明、说明或者聊天记录、往来邮件，与相关客户的交易未利用权利人所提供的物质条件、交易平台的文件、沟通记录等证据材料予以证明。

<sup>81</sup> 北京市高级人民法院（2017）京民申4800号民事裁定书。

### 4.2.3.9 民事责任

根据《反不正当竞争法》第十七条的规定，侵害商业秘密的民事责任包括停止侵权、返还财产及赔偿损失。

(1)停止侵权。对于侵害商业秘密行为判决停止侵害的民事责任的，停止侵害的时间一般持续到该商业秘密已为公众所知悉时为止。

(2)返还财产。当非法泄露、获取他人商业秘密的侵权行为已实施完毕，但商业秘密尚未被公开，其秘密价值尚存时，权利人可向法院请求责令侵权人返还商业秘密，包括追回已经转移的物品，或者销毁体现商业秘密的载体如文件、实物复制品等。

(3)赔偿损失。因不正当竞争行为受到损害的经营者的赔偿数额，按照其因被侵权所受到的实际损失确定；实际损失难以计算的，按照侵权人因侵权所获得的利益确定。赔偿数额还应当包括经营者为制止侵权行为所支付的合理开支。合理开支一般包括以下费用：①公证费；②因调查取证或出庭而发生的交通费、食宿费、误工费；③档案查询费、材料印制费；④翻译费；⑤律师代理费；⑥原告为制止侵权行为支付的其他合理费用。

(4)惩罚性赔偿。经营者恶意实施侵犯商业秘密行为，情节严重的，可以在按照上述方法确定数额的一倍以上五倍以下确定赔偿数额。赔偿数额还应当包括经营者为制止侵权行为所支付的合理开支。

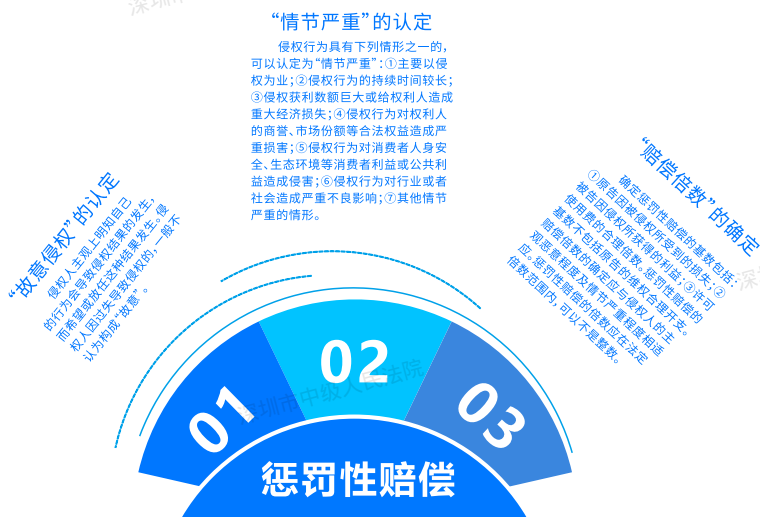


图15 惩罚性赔偿的认定图示

## 4.3 刑事途径

企业商业秘密被他人不正当竞争行为侵犯，被侵权行为符合刑事案件立案追诉标准的，权利人可以直接向公安机关报案。

### 4.3.1 刑事公诉与自诉

#### 4.3.1.1 管辖

依据《刑事诉讼法》第十九条至第二十八条的规定，侵犯商业秘密刑事案件的侦查由公安机关进行，具体由犯罪行为地、犯罪结果地和犯罪嫌疑人居住地的公安机关管辖。

犯罪行为地是指侵犯他人商业秘密行为的实施地，包括：

- (1) 采用盗窃等不正当手段获取他人商业秘密和披露、使用采用以上手段获取的商业秘密的实施地；
- (2) 共犯为他人犯罪行为提供原材料、机械设备等帮助条件的实施地；
- (3) 通过网络传播、披露他人商业秘密的，上传资料的电脑终端所在地为实施地，终端所在地无法查明时，网络服务器所在地为实施地。

犯罪结果地是指犯罪行为直接产生的结果的发生地，不能认为权利人损失，就将其所在地视为犯罪结果地。

#### 4.3.1.2 公诉与自诉的转换

在侵犯商业秘密犯罪中，被害人可以直接向公安机关报案，依法追究犯罪嫌疑人侵犯商业秘密的刑事责任。对于被害人有证据证明对被告人侵犯商业秘密的行为应当依法追究刑事责任，而公安机关或者人民检察院不予追究被告人刑事责任的案件，被害人或其法定代理人也可以直接向人民法院提起诉讼。<sup>82</sup>

刑事自诉相对于公诉案件具有较强的自主性，被告人可以反诉，自诉人也可以与被告人和解、调解，或撤回起诉。

<sup>82</sup> 《中华人民共和国刑事诉讼法》第二百一十条规定，自诉案件包括下列案件：（一）告诉才处理的案件；（二）被害人有证据证明的轻微刑事案件；（三）被害人有证据证明对被告人侵犯自己人身、财产权利的行为应当依法追究刑事责任，而公安机关或者人民检察院不予追究被告人刑事责任的案件。



### 【典型案例】郑某为境外刺探、非法提供商业秘密案<sup>83</sup>

**案情简介：**被告人郑某某于2017年8月至2020年期间，担任上海某甲公司工程师一职，并签订了《劳动合同》《离职保密承诺书》等，对上海某公司的商业秘密负有保密义务。2021年8月，被告人郑某某接受某咨询中介公司的邀请，成为该公司的行业专家顾问。其间，郑某某于2022年2月接受了上海某乙公司（外国法人独资）的电话访谈，在明知实际咨询方系境外组织的情况下，仍将刺探掌握的有关上海某甲公司在先进工艺研发进展和投产规划、现有产品实际产能等商业秘密通过咨询中介公司非法提供给境外的组织、人员，并从中牟利。2022年11月，检察院以为境外刺探、非法提供商业秘密罪对郑某某提起公诉。2023年7月，法院以为境外刺探、非法提供商业秘密罪判处郑某某有期徒刑，并处罚金。

#### 4.3.1.3 证据准备

刑事公诉与自诉的立案要求	
有犯罪事实，需要追究刑事责任	
刑事公诉与自诉共同的证据准备	刑事自诉立案需要增加的证据
✓ 商业秘密构成要件的证据； ✓ 商业秘密被侵犯的证据； ✓ 是否已达到入罪金额或入罪情节。	✓ 明确的被告； ✓ 商业秘密与侵权信息构成实质性相似； ✓ 情节轻微(3年以下)或不予追究的证据。
刑事公诉的举证责任及后果	刑事自诉的举证责任及后果
公安机关立案后，对案件事实进行侦查、取证。	缺乏罪证的自诉案件且自诉人提不出补充证据的,应当说服自诉人撤回自诉，或者裁定不予受理。 <sup>84</sup>

自诉案件当事人因客观原因不能取得的证据，申请人民法院调取的，应当说明理由，并提供相关线索或者材料。人民法院认为有必要的，应当及时调取。<sup>85</sup>

<sup>83</sup> 该案例入选上海市市场监督管理局2024年9月公布的商业秘密保护十大典型案例。

<sup>84</sup> 《中华人民共和国刑事诉讼法》第二百一十一条规定，人民法院对于自诉案件进行审查后，按照下列情形分别处理：（一）犯罪事实清楚，有足够证据的案件，应当开庭审判；（二）缺乏罪证的自诉案件，如果自诉人提不出补充证据，应当说服自诉人撤回自诉，或者裁定驳回。

<sup>85</sup> 《关于办理侵犯知识产权刑事案件适用法律若干问题的解释》第四条规定，人民法院依法受理侵犯知识产权刑事自诉案件，对于当事人因客观原因不能取得的证据，在提起自诉时能够提供有关线索，申请人民法院调取的，人民法院应当依法调取。

#### 4.3.1.4 刑事责任

根据《刑法》第二百一十九条的规定，对侵犯商业秘密行为且情节严重的，处三年以下有期徒刑，并处或者单处罚金；情节特别严重的，处三年以上十年以下有期徒刑，并处罚金。<sup>86</sup>

其中，情节严重是指：①给商业秘密的权利人造成损失数额或者因侵犯商业秘密违法所得数额在三十万元以上的；②直接导致商业秘密的权利人因重大经营困难而破产、倒闭的；③造成商业秘密的权利人其他重大损失的。情节特别严重是指：给商业秘密的权利人造成损失数额或者因侵犯商业秘密违法所得数额在二百五十万元以上。<sup>87</sup>

不仅如此，对法人犯罪也有适用双罚制的规定。单位侵犯他人商业秘密的，对单位判处罚金，并对其直接负责的主管人员和其他责任人员，同样依照上述规定处罚。<sup>88</sup>

#### 4.3.2 刑事附带民事诉讼

被害人可以在侵犯商业秘密罪的刑事诉讼过程中提起附带民事赔偿诉讼。<sup>89</sup>

在侵犯商业秘密罪中，只有因侵犯商业秘密犯罪行为导致商业秘密已为公众所知悉或者灭失的，才符合《刑事诉讼法司法解释》第一百七十五条中规定的“财物被犯罪分子毁坏”，该商业秘密的研究开发成本等商业价值才属于前述司法解释中的“物质损失”。除此之外，其他侵犯商业秘密的犯罪行为导致的权利人的损失，例如市场份额的减少、销售利润的下降等，均不属于刑事附带民事诉讼范畴，人民法院应当不予受理。

<sup>86</sup> 《刑法》第二百一十九条规定，有下列侵犯商业秘密行为之一，情节严重的，处三年以下有期徒刑，并处或者单处罚金；情节特别严重的，处三年以上十年以下有期徒刑，并处罚金：（一）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的；（二）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的；（三）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的。//明知前款所列行为，获取、披露、使用或者允许他人使用该商业秘密的，以侵犯商业秘密论。//本条所称权利人，是指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。

<sup>87</sup> 《知识产权刑事案件司法解释（三）》第四条规定，实施刑法第二百一十九条规定的行为，具有下列情形之一的，应当认定为“给商业秘密的权利人造成重大损失”：（一）给商业秘密的权利人造成损失数额或者因侵犯商业秘密违法所得数额在三十万元以上的；（二）直接导致商业秘密的权利人因重大经营困难而破产、倒闭的；（三）造成商业秘密的权利人其他重大损失的。给商业秘密的权利人造成损失数额或者因侵犯商业秘密违法所得数额在二百五十万元以上的，应当认定为刑法第二百一十九条规定的“造成特别严重后果”。

<sup>88</sup> 《刑法》第二百二十条规定，单位犯本节第二百一十三条至第二百一十九条之一规定之罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照本节各该条的规定处罚。

<sup>89</sup> 《刑事诉讼法司法解释》第一百七十五条规定，被害人因人身权利受到犯罪侵犯或者财物被犯罪分子毁坏而遭受物质损失的，有权在刑事诉讼过程中提起附带民事诉讼；被害人死亡或者丧失行为能力的，其法定代理人、近亲属有权提起附带民事诉讼。因受到犯罪侵犯，提起附带民事诉讼或者单独提起民事诉讼要求赔偿精神损失的，人民法院一般不予受理。



### 【典型案例】沃某公司诉赵某等侵害商业秘密刑事附带民事诉讼纠纷案<sup>90</sup>

**案情简介：**赵某是沃某公司的一名技术研发员，在职期间参与研发了一项新型生产技术，并与沃某公司签订技术秘密转让协议，将这项保密技术以200万元的价格转让给沃某公司，并约定由沃某公司独占使用。但赵某私自留存了该项技术秘密的文件，并将该技术秘密用于生产、销售相关产品牟取私利。沃某公司向公安机关报案后，赵某被公安机关依法抓获。检察院指控赵某犯侵犯商业秘密罪向法院提起公诉。在刑事案件审理过程中，沃某公司向法院提起刑事附带民事诉讼，要求赵某赔偿因其因犯罪行为导致的利润损失。由于刑事附带民事诉讼的受理条件是被害人因人身权利受到犯罪侵犯或者财物被犯罪分子毁坏而遭受物质损失。沃某公司主张的物质损失是因赵某的犯罪行为造成其市场份额、销售单价减少的经济损失，并不是因为技术秘密被公开，丧失秘密性而遭受的物质损失。因此，法院以沃某公司提起的诉讼不属于刑事附带民事诉讼的受理范围为由，裁定不予受理该刑事附带民事诉讼。

#### 4.3.3 刑民交叉的处理思路

知识产权刑民交叉案件的程序衔接以“先刑后民”为主，以“刑民并行”为必要补充。即知识产权刑民交叉案件属于“同一事实”的，应当采用“先刑后民”模式，属于“不同事实”或者民事案件构成必须以刑事案件的裁判结果为依据，应当采用“刑民并行”模式。

##### 4.3.3.1 不同事实的认定

结合知识产权审判的特点，知识产权刑民交叉案件的“同一事实”“不同事实”的认定标准往往考虑被侵害的知识产权客体是否同一。只有同一主体侵害了同一知识产权具体客体，例如同一个编号的商标权、专利权或者相同内容的商业秘密等，并同时具备“同一事实”的其他认定标准时，才属于知识产权刑民交叉案件中的“同一事实”，采取“先刑后民”模式。如果侵害的客体不同，例如商标号、专利号不同，或者权利人在刑事程序中主张保护的是技术信息秘密，在民事程序中主张保护的是经营信息秘密，则属于“不同事实”，应当采用“刑民并行”模式。



<sup>90</sup> 广东省深圳市中级人民法院（2022）粤03刑终1721刑事裁定书。



## 【典型案例】慈某公司诉必某公司技术秘密许可使用合同纠纷案<sup>91</sup>

**案情简介：**慈某公司以必某公司违反二者签订的《采购协议》《保密协议》中约定的保密义务为由，向一审法院提起技术秘密许可使用合同纠纷诉讼。在一审审理期间，公安机关针对必某公司涉嫌侵犯商业秘密罪立案侦查并函告一审法院。一审法院认为，公安机关侦查的事实涵盖了涉案协议和图纸相关内容，与其所审理的侵害商业秘密民事案件事实具有重合之处，故裁定移送公安机关处理。必某公司不服，向最高人民法院提起上诉。最高人民法院二审认为，本案系技术秘密许可使用合同法律关系，公安机关立案侦查的必某公司涉嫌商业秘密犯罪，系必某公司涉嫌侵犯慈某公司的商业秘密的侵权法律关系。二者所涉法律关系不同，仅仅是二者所涉案件事实具有重合之处，慈某公司与必某公司之间的涉案民事法律关系并不受影响。一审法院应将与本案有牵连，但与本案不是同一法律关系的犯罪嫌疑线索、材料移送公安机关，但也应继续审理本案所涉技术秘密许可使用合同纠纷。故最高人民法院裁定撤销一审裁定，指令一审法院审理。

### 4.3.3.2 在先刑事判决的既判力

#### (1) 在先有罪刑事判决

认定被告人/被告单位构成侵犯商业秘密罪的在先刑事判决对犯罪事实的认定对民事诉讼产生绝对的既判力，权利人在民事侵权诉讼审理中对于有罪刑事判决认定的事实无需进行额外的举证。在先有罪判决确定的犯罪数额对在后民事诉讼不产生绝对的既判力。

#### (2) 在先无罪刑事判决

被害人主张保护的信息不属于商业秘密，或者被告人/被告单位没有实施被指控的侵犯商业秘密犯罪行为，从而宣告被告人/被告单位无罪的，该无罪判决对于民事侵权诉讼具有绝对的既判力，人民法院可直接根据刑事判决所认定的事实认定被告人/被告单位未实施相应的侵权行为。

人民法院以证据不足宣告被告人/被告单位无罪的，该刑事判决对民事诉讼程序不具有既判力，人民法院在侵害商业秘密民事侵权诉讼中应当对被控侵权事实独立进行审查、认定。

<sup>91</sup> 最高人民法院（2019）最高法知民终333号民事判决书。



## 4.4 维权途径的路径特点

	行政途径	民事途径	刑事途径
立案门槛	提供有违法行为的初步证据。	采用立案登记制,对立案进行形式审查。	经过公安机关审查后,认为确有犯罪事实、需要追究刑事责任的,才能决定予以立案。
证明标准	市场监管部门依法享有行政强制调查权,可以有效弥补权利人私力取证的不足。	权利人需自行明确商业秘密的内容,自行收集证据举证证明主张保护的信息构成商业秘密、侵权行为的具体表现、侵权损失数额,举证不能将承担不利的法律后果。有条件适用举证责任倒置。	虽然权利人仅需完成其享有商业秘密、被告人/被告单位实施了侵害商业秘密的犯罪行为、其遭受的经济损失达到刑法追诉金额的初步举证责任即可,但刑事诉讼要求证据确实、充分,需达到排除合理怀疑的严格证明标准。
赔偿范围	一般对行为人处十万元以上一百万元以下的罚款;情节严重的,处五十万元以上五百万元以下的罚款。	权利人因被侵权所受到的实际损失、侵权人因侵权所获得的利益、法定赔偿(五百万元以下)。行为人故意侵害商业秘密,情节严重的,权利人有可能获得高达五倍的惩罚性赔偿。	仅对被告人/被告单位定罪量刑,不处理权利人经济赔偿问题,权利人获偿范围有限,往往难以填平损失,更不包括惩罚性赔偿。
维权周期	取证查处快,维权周期短。	6-12个月,可能因公告送达管辖权异议、申请追加当事人、延长举证期限、司法鉴定、中止审理等事由被延长。	侦查期限2-7个月,审查起诉期限1-2个月,法院审理期限3-6个月。如需进行补充侦查、发现漏罪、查明被告人身份的情形,前述期限将相应延长。

附件

法律  
规范  
指引

法律法规及规范性文件	简称
《中华人民共和国民法典》	《民法典》
《中华人民共和国刑法》	《刑法》
《中华人民共和国反不正当竞争法》	《反不正当竞争法》
《中华人民共和国专利法》	《专利法》
《中华人民共和国著作权法》	《著作权法》
《中华人民共和国公司法》	《公司法》
《中华人民共和国劳动合同法》	《劳动合同法》
《中华人民共和国民事诉讼法》	《民事诉讼法》
《中华人民共和国刑事诉讼法》	《刑事诉讼法》
《最高人民法院关于审理技术合同纠纷案件适用法律若干问题的解释》	《关于审理技术合同纠纷案件适用法律若干问题的解释》
《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》	《民事诉讼法司法解释》
《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》	《刑事诉讼法司法解释》
《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释(三)》	《知识产权刑事案件司法解释(三)》
《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解释》	《关于审理侵犯商业秘密民事案件适用法律若干问题的解释》
《中华人民共和国专利法实施细则》(国务院)	《专利法实施细则》
《关于办理侵犯知识产权刑事案件适用法律若干问题的解释》(最高人民法院、最高人民检察院、公安部)	/
《市场监督管理投诉举报处理暂行办法》(国家市场监督管理总局)	/
《深圳市行政听证办法》(深圳市市场监督管理局)	/

深圳市中级人民法院

深圳市中级人民法院



深圳市中级人民法院

深圳市中级



深圳市中级人民法院

深圳市中级人民法院

级人民法院