

# 人工智能行业企业 商业秘密保护指南

上海市市场监督管理局

上海市浦东新区市场监督管理局

2024年11月

## 序言

人工智能是一个多学科交叉融合的新兴科学领域，近年来发展迅猛。人工智能正引领新一轮的科技革命和产业变革，成为发展新质生产力的重要引擎。国家不断鼓励核心硬件产品自主研发，鼓励大型企业加大 5G、大数据人工智能等数字化技术应用力度，支持工业人工智能芯片、工业视觉传感器等基础硬件的研发突破。围绕人工智能形成了基础层、框架层、模型层、应用层的产业链结构。

作为浦东新区的三大先导产业之一，浦东新区政府积极推动人工智能行业技术和应用的发展。尤其是在生成式人工智能技术领域，企业和科研机构在生成式人工智能的研究和应用上加大投入，出现了很多大模型企业，推动生成式人工智能基础设施和公共训练数据资源平台建设，人工智能芯片不断升级迭代。安全可信的芯片、软件、工具、算力人工智能算法、框架、数据资源及配套软件平台等领域都不断涌现大量自主创新技术。

截至 2023 年底，浦东新区的人工智能重点企业超过 600 家，相关产业规模超过 1400 亿元，占上海市人工智能产业规模的四成。2024 年上半年，浦东新区人工智能产业规模达到 696 亿元，其中人工智能服务业实现规模 595 亿元。

本指南以 2023 年 8 月由上海市市场监管局和浦东新区市场监管局发布的《浦东新区企业商业秘密保护指南》为基础，结合人

工智能行业创新性强和产业结构复杂的特点，为企业提供一套更具针对性的商业秘密保护策略。从商业秘密的识别、制度管理、人员管理、信息管理、技术防护措施、国际合作等多个维度，帮助企业建立适合自身需求的商业秘密保护体系。

需要注意的是，若企业未能有效保护其商业秘密，不仅会面临侵权行为的风险，还会在法律诉讼中遭遇多重困难。首先，未加保护的商业秘密可能在法庭上被视为已公开信息，从而丧失法律保护资格。此外，企业在主张权利时，可能面临举证责任的加重，因为未能证明秘密信息曾被有效保护，而使得法庭对其商业秘密性质产生质疑。这种情况下，企业不仅难以获得损害赔偿，甚至可能导致竞争对手继续使用该信息而不受限制。因此，建立健全的商业秘密保护机制，是企业抵御外部侵害和维护合法权益的基础，是确保商业秘密能够在法律框架内得到有效认定和保护的关键举措。

## 人工智能部分内容

### 起草单位

上海融孚律师事务所

### 参与起草人

李莹薇 高容 张志成

# 目 录

1. 概述.....	1
1.1 【人工智能行业】	
1.2 【人工智能产业链】	
1.3 【人工智能行业商业秘密的重要性】	
1.4 【人工智能行业商业秘密的特点】	
1.5 【商业秘密保护与著作权、专利权保护的关系】	
2. 术语和定义.....	2
2.1 【人工智能行业商业秘密】 .....	2
2.2 【涉密载体】 .....	3
2.3 【人工智能数据】 .....	4
2.4 【涉密计算机】 .....	4
2.5 【涉密区域】 .....	4
3. 自我保护.....	4
3.1 【保护策略】 .....	4
3.2 【组织架构】 .....	10
3.3 【制度管理】 .....	11
3.4 【信息管理】 .....	12
3.5 【人事管理】 .....	16
3.6 【物理安全管理】 .....	18
3.7 【研发管理】 .....	19
3.8 【采购承揽】 .....	19
3.9 【销售管理】 .....	20
3.10 【财务管理】 .....	20
3.11 【内控内审】 .....	20
3.12 【对外合作】 .....	22
3.13 【国际合作】 .....	22
【相关案例】 .....	24

4 . 民事保护.....	29
4.1【当事人主体资格】 .....	29
4.2【主管与管辖】 .....	29
4.3【诉讼请求、事实及理由】 .....	29
4.4【证据准备及证明标准】 .....	30
4.5【诉讼过程中的保密措施】 .....	31
4.6【证据保全与行为保全】 .....	32
【相关案例】 .....	33
5. 行政保护.....	37
5.1【查处部门与管辖】 .....	37
5.2【立案】 .....	37
5.3【调查】 .....	38
5.4【行政处罚】 .....	39
5.5【调解和和解】 .....	41
【相关案例】 .....	42
6. 刑事保护.....	47
6.1【侵犯商业秘密罪】 .....	47
6.2【为境外窃取、刺探、收买、非法提供商业秘密罪】 .....	49
6.3【刑事案件管辖】 .....	49
6.4【报案】 .....	50
6.5【立案】 .....	51
6.6【移送追究行政责任】 .....	52
6.7【取保候审】 .....	52
6.8【逮捕】 .....	52
6.9【审查起诉】 .....	52
6.10【审理裁判】 .....	52
6.11【刑民交织】 .....	53
【相关案例】 .....	54
7 . 商业秘密鉴定.....	58
7.1【含义】 .....	58

7.2【鉴定种类】	58
7.3【鉴定程序】	61
8.涉外保护	63
8.1【美国商业秘密保护】	63
8.1【其他发达国家商业秘密保护】	65
8.3【中国企业的应对】	66

## 附录

1. 人工智能行业不同层面企业重要信息商业秘密要件评估表	
2. 浦东新区商业秘密侵权投诉举报受理点	69
3. 上海市商业秘密侵权纠纷民事案件管辖法院	72
4. 浦东新区检察机关、公安机关联系表	73
5. 人民法院诉讼资产网备案的知识产权鉴定机构	74

## 1. 概述

### 1.1 【人工智能行业】

人工智能是人类发展的新领域，人工智能行业是指以人工智能技术研发为重要业务，直接从事人工智能产品或服务创造的企业组成的产业链。包括研究和开发计算机视觉、智能语音、自然语言处理、生物特征识别以及虚拟现实等人工智能技术层的科技企业和科研院校，也包括专注于行业场景应用软件开发的企业。

### 1.2 【人工智能产业链】

人工智能产业链包括基础层、框架层、模型层和应用层四个部分。基础层主要包括算力、算法和数据、芯片和硬件基础设施建设；框架层主要是指用于模型开发的深度学习框架和工具；模型层主要是指大模型等技术和产品；应用层主要是指人工智能技术在行业场景的应用。

### 1.3 【人工智能行业商业秘密的重要性】

人工智能行业对我国加快建设成为制造强国、网络强国和数字中国至关重要。人工智能与其他行业融合的特定场景创新，又能引领其他产业的迅速升级和变革。只有对人工智能技术创新成果加以保护，让人工智能知识产权价值得以体现，才能吸引更多的人工智能技术人才专注于人工智能前沿基础理论的创新和关键核心技术的创新，吸引更多企业加大投入，促进行业快速发展。

### 1.4 【人工智能行业商业秘密的特点】

人工智能技术涉及的领域广，技术迭代快，国际交流合作频繁。开源人工智能技术、人工智能供应链具有全球化的特点。人工智能行

业发展，不可避免的会在全球范围内共享人工智能知识成果。算法透明和开源技术与商业秘密的保护之间存在矛盾。人工智能行业的商业秘密保护需要寻求保护创新和商业利益二者之间的平衡。

人工智能行业人才稀缺，人员流动也是促进行业发展的重要因素之一。企业既要重视商业秘密保护，又要兼顾人才就业权的保障。

人工智能行业的技术秘密更多以电子化和数据化形式存在，容易通过非法下载和信息网络传输实现信息转移。

### **1.5【商业秘密保护与著作权、专利权保护的关系】**

人工智能著作权保护的客体只能以代码化指令序列文字等方式呈现，而不包括任何无法直观展现的算法思想、操作方法等。人工智能专利保护的客体也不能是单纯的算法，而必须是能够与技术特征相结合的技术解决方案。

商业秘密不需要形式上的完整性，任何模块或解决方案的实用信息都可以商业秘密的形式获得保护。所以商业秘密保护对于人工智能行业创新成果的著作权保护和专利权保护构成了非常有益的补充。

## **2. 术语和定义**

下列术语和定义适用于本指南。

### **2.1【人工智能行业商业秘密】**

人工智能行业的商业秘密是指在人工智能开发与应用中形成的不为公众所知悉、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。

不为公众所知悉，是指有关信息不为其所属领域的相关人员普遍知晓和容易获得。

具有商业价值，是指商业秘密通过现在的或将来的使用，能带来现实的或者潜在的经济利益或竞争优势。研发过程中产生的测试失败数据、具有技术特征的算法应用方案等亦可能属于商业秘密范畴。

相应保密措施，是指商业秘密的权利人需采取与信息特性、商业价值等相适应的合理保密措施。合理性可以考量技术或经营信息的特性、权利人保密的意愿、保密措施的可识别程度、他人通过正当方式获得信息的难易程度等要素。

### **2.1.1 【芯片商业秘密】**

不为公众所知悉，具有商业价值，由权利人在技术开发和应用中形成的，采取合理保密措施的系统架构技术信息、电路参数、设计结构、芯片设计数据库文件、代码技术信息等。

### **2.1.2 【生成式人工智能商业秘密】**

不为公众所知悉，具有商业价值，由权利人在技术开发和应用中形成的，采取合理保密措施的源代码、训练数据、优化的模型和独特的算法机制机理等。

## **2.2 【涉密载体】**

以文字、数据、符号、图形、图像、视频和音频等方式记载商业秘密信息的纸介质、磁介质和光介质等。纸介质包括文件、报告、图纸等；磁介质包括服务器、硬盘、软盘、磁带、U盘等存储设备；光介质包括光盘等。特殊涉密载体包括具备高强度加密芯片的移动硬盘或

固态存储设备、分布式存储节点、通过生物特征识别技术的存储载体、量子存储设备等。

### **2.3【人工智能数据】**

用于训练、验证和优化人工智能模型的各种数字化信息集合，包括但不限于文本、图像、音频、视频等形式，涵盖真实世界的观测、用户行为记录及专业领域的特定知识等内容。

#### **2.3.1【验证数据】**

在模型训练过程中，用于评估模型性能、准确性和泛化能力的数  
据。

#### **2.3.2【测试数据】**

在模型训练完成后，对模型的实际应用效果及最终性能进行测试  
和验证的数据。

### **2.4【涉密计算机】**

处理或存储商业秘密信息的台式机、便携机、一体机、平板等各  
类计算机。

### **2.5【涉密区域】**

含有商业秘密信息、人员进入后可能接触到商业秘密的办公区域、  
档案区域、实验室等物理区域。

### 3. 自我保护

#### 3.1 【保护策略】

只有针对公司的核心经营要素，例如技术、经营、客户信息等资产，明确保护的主体，依据这些主体所处载体的不同，如数据库、办公计算机、纸质、云服务等不同场景，方才便于设定合理的保护策略和手段。

##### 3.1.1 【商业秘密保护要素】

实现商业秘密的保护，可归纳为三要素：

a) 机密性。商业秘密不被未授权的主体访问。例如，访问控制，仅高管有权查看保险箱里的文件。加密，一个核心算法被加密存储，盗窃的第三方无解密用的口令，也无权查看。

b) 完整性。商业秘密不被未授权的主体篡改。例如，数字签名，与客户一笔经由网络渠道签署的合同存在争议，若合理使用数字签名技术，可由第三方公证合同的未被篡改和其有效性。

c) 可用性。商业秘密可被授权主体及时可靠的访问。例如，使用备份技术，防止因勒索软件等原因，造成商业秘密信息无法访问。

##### 3.1.2 【小微企业】

小微企业需要管理的商业秘密数量较少，涉及的员工较少，但员工可能身兼数职。保护的核心思路应从可用性着手，避免因天灾人祸的事故，导致商业秘密不可用。

###### 3.1.2.1 【保密条款】

对于可能涉及商业秘密的员工，应签署保密协议，利用法律约束，

进行兜底。

### **3.1.2.2【安全意识培训】**

对所有员工，都应将安全意识培训纳入到入职试用期转正和周期性工作考核中进行。

### **3.1.2.3【备份追踪】**

建立数据备份和恢复机制，防止数据丢失，对数据的访问进行日志记录，可有效应对勒索病毒的威胁，以便及时发现和追踪异常访问行为。定期对信息系统进行安全审计，及时发现和修复安全漏洞，保证商业秘密信息的实时有效可用。

### **3.1.2.4【杀毒软件】**

确保办公计算机杀毒软件有效启用并更新，可有效应对勒索病毒的威胁。

### **3.1.2.5【访问控制】**

确保每个员工使用独立的账号，而非共用一个账号，启用登录日志和行为日志功能。针对单一账号，仅授权其需要访问的最小资源，如客服人员仅能访问客服资源，而非核心财务系统。

### **3.1.2.6【云服务】**

信息化是目前企业经营的核心依托之一，通过采购知名云服务提供商的产品，对于备份、访问控制等都具备较为成熟的方案。如典型的客户管理，可通过企业微信进行集中化管理，避免因员工离职、未有效交接，导致客户流失问题。

### **3.1.2.7【主要风险点及检查措施】**

针对小微企业场景的商业秘密保护方案，其主要的风险点包括：保密协议未签署、安全意识培训不足、备份策略不完善、杀毒软件未部署完全或未启用、系统账号共享行为等。

针对上述风险点，我们可采取的检查措施包括：

a) 定期对新入职员工的保密协议签署进行抽样检查，特别是关键岗位人员，查看其是否签订了有效的保密条款。

b) 每次安全意识培训后保留培训材料和培训人员签到表；定期对培训材料和签到表检查，确认应覆盖人员都参加了培训；不定期组织抽检关键岗位人员进行安全意识考核。

c) 定期检查公司备份机制的运行情况，包括审阅备份日志记录，抽样检查备份文件的完整性和可读性，不定期执行备份文件恢复测试。

d) 如果是集中部署的防病毒软件，可以通过服务端，定期查看杀毒软件在公司设备中的部署情况，并与员工名单或资产清单进行匹配，确保相关设备都有安装；如果是单机版防病毒软件，可定期或不定期根据员工名单或资产清单进行抽检，检查是否有安装防病毒软件，并且设置为即时防护和定期扫描。

e) 定期进行系统账号权限核查，并与员工名单进行匹配，确保账号数量和所有者与员工一致，严格遵循“一人一账号”原则；重点检查已离职员工账号，确认是否已经被删除或禁用。

### **3.1.3 【中型企业】**

需要管理的商业秘密数量较多，涉及的员工较多，需要独立的部门负责。保护的核心思路是全面风险识别和重点风险管控相结合。

在满足小微企业的建设点以外，可考虑如下措施。

### **3.1.3.1【信息安全管理体系建设】**

常见的如《中华人民共和国网络安全法》要求的，应进行网络安全信息等级评估，或国际上广受认可的 ISO27001 认证，亦或某些行业特有的，如 PCI-DSS 支付卡行业安全认证。可通过第三方测评机构对照完整的信息安全管理建设的要求，明确差距，查找不足，通过技术和管理手段，进行重点防护。

### **3.1.3.2【关键岗位背景调查】**

对涉及较多商业秘密的岗位，如数据库管理员、研发人员等，进行入职前的背景调查，防止不法分子以合法身份入职后，伺机盗取商业秘密信息。

### **3.1.3.3【网络隔离】**

对涉及较多商业秘密的信息系统，进行网络隔离，避免同互联网进行直接连接。如采用网络层防火墙。涉密计算机的数据存储应采取严格的物理隔离和安全防护措施，不能与互联网及其他公共信息网络连接，以防止数据被非法获取、篡改或泄露。对于涉密等级较高的计算机，如需要与存储设备连接，可以设置外部光驱，即通过中间设备进行隔离。

### **3.1.3.4【统一账号管理】**

应建立统一账号管理系统，如常见办公环境的微软 AD 域等，所有涉及登录的系统都纳入到此系统中。有效进行员工账号的管理，避免员工离职后账号关闭不及时不全面，导致商业秘密持续泄露风险。

### **3.1.3.5【双因子鉴别】**

对涉及较多商业秘密的信息系统，应启用双因子鉴别，如常见的手机短信验证码、动态数字动态口令等，防止关键岗位的员工因账号被窃，导致商业秘密被第三方窃取风险。

### **3.1.3.6【网络准入】**

因企业规模增大，人员增多，可能有不法分子企图在周围入侵企业内部 wifi，或潜入企业内部，通过网线连接的方式，入侵内网，试图窃取商业秘密。对此，可通过部署网络准入系统的方式，限定当账号有效时，才允许进入企业网络，可为企业办公网筑起第一道防线。

### **3.1.3.7【堡垒机】**

对涉及较多商业秘密的信息系统，应启用加强版的访问控制，针对每次访问，留存访问记录，如配置堡垒机。一方面，规范内部人员有序管理商业秘密，若遇到极端情况，如删除数据等操作，可固定证据，并依据记录，提供数据恢复的思路方案；另一方面，因企业规模增大，商业秘密数量和价值提升，堡垒机可作为有效控制点，防止不法分子的入侵。

备注：“堡垒机”是指具备监控和记录运维人员操作行为功能的网络安全设备。

### **3.1.3.8【应用防火墙】**

部分依托商业秘密开展业务的信息系统，可能对互联网开放，此时，应部署应用防火墙，减轻因自身信息系统的漏洞（如 SQL 注入等）导致商业秘密被批量窃取的风险。

### 3.1.3.9 【软件安全】

对使用的软件进行安全评估，确保软件无安全漏洞，及时更新软件版本，修复已知的安全漏洞。对软件的使用进行授权管理，防止未经授权的复制和使用。

### 3.1.3.10 【数据防泄密系统】

通过对办公计算机部署管理终端、在办公网出口部署网络探针的方式，识别和拦截含商业秘密在内的敏感数据外发行为，减轻被内部员工有意或无意的外传被第三方恶意窃取的风险。

### 3.1.3.11 【主要风险点及检查措施】

针对中型企业场景的商业秘密保护方案，其主要风险点包括：信息安全管理体系不够完善、关键岗位候选人背景调查缺失、网络隔离策略未生效、统一账号管理不完善、双因子鉴别未启用、网络准入策略未生效、数据库异常访问、敏感数据泄露等。针对上述风险点，企业除了采用小微企业的检查措施外，还可采取以下检查措施：

a) 参与第三方机构对公司的信息安全管理体系的认证审核或复核，及时了解信息安全体系的建设情况。

b) 定期对关键岗位的新入职员工进行背景调查复核，确保相关调查执行到位。

c) 保留书面的防火墙配置策略，调整策略时必须要有正式的书面申请和审批。定期审计网络防火墙生产环境配置，检查与书面策略的一致性，并审阅相关策略是否能够有效隔离内外网环境。

d) 定期对域控服务器进行审计，并与员工名单进行匹配，确保所

有在职员工均通过 AD 域进行统一的账号管理；同时检查基础的安全域组策略是否已经部署，如复杂口令策略、最小口令长度策略、口令强制修改策略、口令历史策略、审计策略、禁用共享策略等等。

e) 定期检查双因子鉴别策略设置，确认是否已启用；同时随机抽取用户进行登录测试，查看其双因子认证是否有效。

f) 定期从服务端检查终端准入软件在公司设备中的登录情况，并与员工名单或资产清单进行匹配，检查是否有未经认证的设备入网；同时不定期用非公司设备测试接入公司网络，确认终端准入限制的有效性。

g) 定期检查堡垒机配置，确认公司关键生产服务器均已接入堡垒机，且堡垒机限制对生产服务器的高风险命令直接操作；同时定期对堡垒机日志进行审计，检查是否有异常的线上操作命令。

h) 定期检查数据防泄漏软件在公司设备中的安装情况，与员工名单进行匹配，确保部署的完整性；同时定期审计防泄漏软件的拦截和警告日志，及时发现员工的数据传输异常操作，并对其进行追因溯源调查。

### **3.1.4 【大型企业】**

需要管理海量的商业秘密，涉及的员工数量巨大，存在一定部门墙，导致商业秘密的识别和保护存在盲点。保护的核心思路是全面风险管控。在满足以上建设点以外，可考虑如下措施。

#### **3.1.4.1 【组织保障】**

企业应建立独立的部门，统筹行使商业秘密保护的职责，牵头承

担商业秘密识别、保护、审计等工作。

#### **3.1.4.2【数据分类分级】**

依照国家和行业要求，建立对应的数据分类分级体系，对涵盖商业秘密在内的数据，进行全面标识和分类，以此为依托，进行分级保护。

#### **3.1.4.3【数据不落地】**

对含商业秘密在内的敏感场景，启用云终端等方式，确保员工可用基础上，商业秘密仅可查看不可下载，无有效审批，无法批量导出，防止内外部的商业秘密窃取行为。

#### **3.1.4.4【数字水印】**

在关键应用系统上，启用数字水印技术（如明水印），警示规范员工操作，不进行截屏拍照，也可使用暗水印，在商业秘密流失后追查来源。

#### **3.1.4.5【代理】**

通过使用代理模式，以虚拟号形式进行统一外呼，防止客服人员恶意获取注册用户手机等联系方式，保护客户信息。

#### **3.1.4.6【最小授权】**

通过建立统一身份验证+安全网关+微隔离的形式，授予员工工作所需的必要最小权限，既减轻内部员工恶意嗅探和窃取商业秘密的风险，也提高第三方窃取商业秘密的难度。

#### **3.1.4.7【主要风险点及检查措施】**

针对大型企业场景的商业秘密保护方案，除了中型企业的风险外，

其他风险点还包括：数据分类分级体系的缺失、未经授权的数据落地行为、数字识别技术的缺失、员工账号权限过大等。除了采用小微企业和中型企业的检查措施外，可以额外增加以下检查措施：

a) 定期检查数据分类分级体系是否根据业务的变化进行及时更新，各分类数据是否都已指定明确的所有者。

b) 通过 VDI 等虚拟桌面工具限制数据落地访问；定期审查 VDI 操作日志，确保无异常的数据交互行为。

c) 定期选择关键系统进行随机截屏操作，查看数字水印技术是否启用生效。

d) 定期选择关键系统进行抽样检查，查看敏感信息（如用户个人数据等）是否已脱敏。

e) 根据员工岗位职能制定标准的系统权限角色，形成书面的岗位角色矩阵表；根据业务变化及时更新该矩阵表；申请岗位新增权限时需有书面审批记录；定期进行系统账号权限检查，确保员工系统权限与工作岗位相一致，额外权限均有正式申请和审批，严格遵循最小授权原则。

## **3.2 【组织架构】**

### **3.2.1 【商业秘密保护部门】**

企业应设立商业秘密保护部门或由具备商业秘密保护职能的部门开展商业秘密管理工作。企业的分支机构、子公司和关联企业可参照企业设置商业秘密保护部门。

### **3.2.2【部门职责分工】**

企业应明确各部门的商业秘密保护职责，划分商业秘密保护部门与其他各部门的分工与责任界限。各部门之间应建立常态化沟通与协作机制。

### **3.2.3【岗位职责】**

商业秘密保护部门应履行以下职责：

- a) 界定和管理商业秘密；
- b) 组织员工进行商业秘密保护培训；
- c) 组织制订、实施商业秘密保护措施；
- d) 会同各部门对相关保密制度及其落实情况进行检查、督促及整改。
- e) 完成商业秘密泄露的证据整理、搜集、举证、协助调查取证等工作。

### **3.2.4【人员保障】**

企业应在商业秘密保护部门内配备专职的商业秘密管理人员，或由法务、信息安全等部门人员兼任商业秘密管理工作。

## **3.3【制度管理】**

### **3.3.1【建立保密制度】**

建立适合本企业的保密制度，对涉密数据和信息产生和流转的相关流程进行梳理，制定详细的管理制度，在商业秘密的产生、存储、使用、传输、销毁等各个环节确定具体负责的人员，明确管理职责。

负有管理职责的工作人员有滥用职权、玩忽职守、徇私舞弊等行为的，设置相应处分措施。制度建立时可以参考国家相关的保密法规和标准，更具有可操作性。

### 3.3.2 【应急响应机制】

企业应制定应急响应预案，对于可能出现的涉密数据安全事件，如数据泄露、丢失、被篡改，关键技术人员离职等，制定具有针对性的处理措施，并指定应急处理负责部门。企业可以通过应急演练和培训提高应对突发事件的能力，确保在事件发生时能够快速响应、有效处理，将损失降到最低。

## 3.4 【信息管理】

### 3.4.1 【商业秘密识别】

企业应根据自身的技术类型和所处人工智能产业链中的位置，对经营中形成的技术信息和商业信息进行识别，建立商业秘密清单，确定商业秘密信息、级别、保存期限、涉密人员范围等内容。

#### 3.4.1.1 【技术信息】

**【基础设施及硬件】** 具有创新性的芯片架构等

**【软件信息】** 关键的人工智能程序代码、源代码、应用程序、系统软件等

**【算法和模型】** 独特的算法设计、数据训练方法、基础框架设计、基础大模型设计、调优方案、模型架构和参数等

**【数据】** 经过训练的数据、独特的数据技术、经过标注或具有独

特价值的数据集、测试数据和验证数据等

**【研发信息】** 记录研发过程、技术思路、实验结果等的研发文档、技术报告和系统设计图纸，尚未公开的研究方向、创新想法等

**【技术方案】** 针对人工智能应用的技术解决方案，提升系统性能的独特策略和技巧等

### 3.4.1.2【经营信息】

与经营活动有关的创意、管理、销售、财务、计划、样本、招标投标材料、客户信息等。

**【客户信息】** 对特定客户的名称、地址、联系方式、交易习惯、交易内容、特定需求等信息进行整理、加工后形成的客户信息

**【经营决策】** 战略决策、研发策略、研发方向与领域、投资、股权激励方案、技术规划布局、营销策划、营销方案、预决算报告、信息安全风险报告、运维日志等

**【行业分析】** 人工智能市场的深入分析和市场预测数据、需求趋势预测、重要客户的特殊需求分析等

**【场景需求】** 特殊的场景需求、尚未公开的场景创新

### 3.4.2【商业秘密构成要件】

#### 3.4.2.1【秘密性】

企业识别商业秘密时，需考虑该信息是否为其所属领域相关人员普遍知悉或者从公开渠道容易获得。满足以下条件的，可认定具有秘密性：

a) 不能从公开渠道获得，未在国内外公开出版物或者其他媒体上公开发表过，包括学术论文、专利文献、行业报告、新闻稿等；

- b) 未通过公开的报告会、研讨会、发布会、论坛等方式公开；
- c) 未在国内外销售、展示、试用等过程中向公众公开；
- d) 虽然技术概念、算法原理或数据特征曾在公开渠道讨论或提及，但经特定算法优化、独特的数据集或创新的模型组合方式未被公开的；
- e) 不属于所属领域相关人员普遍掌握的常识或行业惯例。

技术信息如果仅包含基础数据、算法框架、技术组件的简单组合，不能主张具有秘密性。

#### **3.4.2.2【价值性】**

企业在评估信息的商业价值时，应考虑信息是否对企业具有现实和潜在的价值，能否为企业带来经济利益或竞争优势。

a) 企业在开发和应用该项信息时，投入的人力、研发、经营以及其他成本。

b) 该项信息为企业带来的直接经济收益和预期经济收益、成本节约和投资价值等。

c) 该项信息为企业带来的战略价值，包括获得或提升市场地位、市场份额、竞争优势等。

#### **3.4.2.3【保密性】**

确定信息具有秘密性和价值性后，企业应对信息采取相应保密措施。未采取保密措施的应及时补救，并列入商业秘密清单。

#### **3.4.3【分级管理】**

商业秘密管理部门应将商业秘密信息进行分级管理，可按重要性分为核心秘密、重要秘密和一般秘密三个等级，并实行定期复评、动态调整。根据商业秘密的级别，采取不同的保密措施。如企业的商业

秘密同时属于国家秘密的，应按照相关国家保密法规进行管理。

#### **3.4.4【保密期限】**

商业秘密管理部门应根据密级以及商业秘密自身情况确定商业秘密的保密期限。可以确定的时限以“年”“月”“日”计，不可确定的时限应定为“长期”或“永久”。

#### **3.4.5【权限管理】**

商业秘密管理部门应根据商业秘密密级和岗位职责“最小授权”原则，确定可接触的人员范围。

#### **3.4.6【解密管理】**

企业的商业秘密出现下列情形时，商业秘密管理部门可通过消除密级标识、电子文档解密等方式予解密：

- a) 企业认为商业秘密事项已不再具有保护价值的；
- b) 其他特定因素导致商业秘密被公开的。

#### **3.4.7【销毁管理】**

销毁涉及商业秘密的文件（含复制文件）、资料、电子信息、载体和物品，应由商业秘密管理人员列出销毁清单，经商业秘密管理部门审批后实施。销毁过程由商业秘密管理部门全程监督。

文件、资料应粉碎成颗粒状或焚烧处置，电子信息应利用彻底删除软件永久删除。

### **3.5【保密措施】**

商业秘密管理部门应根据商业秘密的性质、载体、密级等制定相应的保密措施。

#### **3.5.1【存储介质加密】**

对重要的服务器、存储设备的访问进行加密，对于损坏或报废的存储介质，要按照保密规定的要求进行物理销毁，或通过专业机构进行安全技术处理，确保数据无法恢复。退出使用的涉密信息设备在经安全技术处理前禁止赠送、出售、丢弃或者改作其他用途。

对商业秘密信息采取加密、加锁、反编译等保护措施或在相关载体上加注保密标志或加密提示。使用安全的文件传输方式，防止信息泄露。

### **3.5.2 【涉密设备管理】**

企业可以对计算机和光驱等电子办公设备进行分级管理，分别设置适用于不同级别的管理方式。

a) 涉密人员的计算机和电子设备应专机专用。多人使用、账号专用的电子设备设置专人管理。

b) 企业应禁用涉密计算机的外接存储功能，限制蓝牙等无线设备的接入，杜绝通过光驱、无线网卡等存储或传输功能泄密，防止摄像头、声卡、话筒等音视频录入功能等。禁止使用非涉密信息系统和非涉密信息设备存储、处理秘密信息。禁止直接使用无线存储设备与涉密计算机连接。

c) 禁止将涉密信息系统、涉密信息设备接入互联网及其他公共信息网络，或将涉密信息系统、涉密信息设备与互联网及其他公共信息网络之间进行信息交换。

d) 禁止擅自卸载、修改涉密信息系统的安全技术程序、管理程序。

e) 涉密信息存储使用的计算机、服务器、存储设备等硬件，应选用符合保密要求的产品，并进行严格的管理和维护。设备应放置在安全可靠的位置，避免受到物理损坏、盗窃或未经授权的访问。定期对设备进行检查和维护，确保其正常运行和数据的安全存储。

### **3.5.3 【区域管理】**

企业应对存放商业秘密的场所进行物理隔离，根据商业秘密信息划分为不同的涉密区域，可按涉密区域、办公区域、外部接待区域三级分区。涉密区域限制来访者，采取基本的物理隔离措施，如门禁、权限控制等，尽可能确保区域内摄像监控全覆盖。

涉密区域可包括厂房、车间、实验室、存储商业秘密信息的数据中心、服务器、档案室等。

## **3.6 【人事管理】**

### **3.6.1 【入职管理】**

**3.6.1.1** 建议企业通过章程、制度、员工手册以及书面通知等方式，明确保密信息的范围以及员工的保密义务。同时应确定相应的保密制度已经实际送达员工并为其所知悉，例如，通过邮件发送或要求员工书面签收，并保存相应记录。对于新入职、转岗到涉密岗位的员工，应与其签订与岗位工作内容相适应的员工保密合同/协议。

人工智能行业催生诸多新兴岗位，如云网智能运维员、生成式人工智能系统应用员、工业互联网运维员、智能网联汽车测试员等。企业应对这些新兴岗位制定明确的岗位职责，确定涉及企业商业秘密的，要与员工签订保密合同/协议。

**3.6.1.2** 高级管理人员、高级技术人员及其他负有保密义务的人员（如职业经理人、技术、采购、销售等涉密重点岗位人员），可与其签订竞业限制协议。

**3.6.1.3** 涉密重点岗位员工入职前宜做背景调查，必要时应要求其作出不侵犯他人商业秘密的承诺。

### **3.6.2【在职管理】**

**3.6.2.1** 员工在职期间，应督促员工遵守企业商业秘密保护制度，做好本岗位商业秘密保护工作：涉密信息及载体应及时上报，由保密员归档统一管理；使用涉密信息应履行登记手续；涉密电子文档、数据按规定途径和要求使用、流转等；离开工作岗位前及时下线工作账户，或设置计算机锁屏等。

企业在员工调岗或发生职务变动时，应及时对员工的涉密情况进行更新，进行动态管理，调整涉密范围。

**3.6.2.2** 在录用潜在竞争性关系企业的员工后，应采取特定的措施，可能包括以下方面：审核待录用的员工与原单位之间的保密约定、保密义务、保密内容及范围，以防范该员工在本企业内部公开或使用原单位的商业秘密；提醒待录用的员工不应将原单位的商业秘密带入本企业进行使用或公开，并要求就本项内容签署保证书；定期对已入职的员工所从事的业务内容进行审核，以排除使用原单位商业秘密。

**3.6.2.3** 商业秘密保护培训宜列入企业年度培训计划，并形成常态、制度化，对每次培训做签到、培训纪要建档保存，做到培训记录留痕。培训内容包括商业秘密的重要性，员工保密义务、保密范围，商业秘密属于企业的职务成果，侵犯企业商业秘密的行为及法律责任等，使在职员工对商业秘密可能泄露的异常状态及承担的法律后果保持足够警觉。

3.6.2.4 应对新入职涉密岗位的人员进行商业秘密保护培训。

3.6.2.5 可采取发放资料、集中培训、网络培训或相结合的方式开展培训，保存培训记录。

3.6.2.6 签订员工保密合同/协议的人员在培训结束后宜进行考核，保存相关考核材料。

### **3.6.3 【离职管理】**

3.6.3.1 涉密岗位员工离职前，企业应主动告知保密义务，以及若违反规定应承担的法律责任。告知离职员工不得有以下行为：复制、带离、损毁、篡改、拍摄涉密文件资料、物品；查阅、拷贝、篡改、发送涉密电子文档、数据；删除、更改账户；披露、使用商业秘密等。

3.6.3.2 涉密岗位员工离职前，企业应提醒离职员工主动移交一切涉密载体和物品，准备离职交接清单并安排人员确认交接完成。涉密物品包括但不限于：涉密文件资料、数据以及载体、物品；账号、密码等账户信息；工作计算机；门禁卡、钥匙等。

3.6.3.3 应在员工离职后采取适当措施进行脱敏，及时收回离职员工的所有访问权限，包括计算机系统、网络、文件存储设备等。更改相关密码和密钥，确保离职员工无法继续访问涉密信息对离职员工使用的计算机、移动设备等进行清理，删除所有涉密文件和数据。并及时通知与离职员工有关的供应商、客户、合作单位等，做好业务交接。

3.6.3.4 应实际开展离职检查，检查的具体内容包括：检查工作计算机数据是否完整；检查工作账户是否有异常操作，如异常查询、下载、拷贝、修改、删除等；检查工作邮箱的邮件收发记录；离职前一定期

限内的涉密文档、数据的查阅和使用情况等。

**3.6.3.5** 应与离职涉密重点岗位工作人员签订竞业限制协议等商业秘密保护确认文书，竞业限制应根据自身需要进行启动或解除。

**3.6.3.6** 应及时掌握离职员工在竞业限制期限内的任职去向。

### **3.7 【研发管理】**

#### **3.7.1 【职务商业秘密】**

职务商业秘密是指员工在劳动关系存续期间，根据劳动合同的约定或在企业指定的工作中研究或开发取得的商业秘密。

#### **3.7.2 【研发成果归属】**

企业与员工就职务商业秘密的归属宜以书面形式进行明确约定，未做约定的，该商业秘密系执行企业的工作任务或主要利用企业的物质技术条件完成的，应视为归属于企业。企业委托第三方开发完成的成果属于商业秘密的，建议对相关成果的归属以书面形式进行明确约定，未做约定的，双方均享有使用和转让的权利。

#### **3.7.3 【研发成果管理】**

确定归属于企业的商业秘密，企业应按照本指南开展商业秘密管理工作。确定归属于员工或第三方的商业秘密，且该商业秘密与企业相关的，企业应与员工或第三方签署保密协议，要求员工或第三方履行保密义务。

### **3.8 【采购承揽】**

### **3.8.1 【委托加工管理】**

涉及商业秘密的委托加工，企业应与加工方签署保密协议或保密条款。

### **3.8.2 【第三方人员管理】**

企业聘任或委托专家、顾问、翻译、律师、会计师等因工作需要可能接触涉密信息的外部人员，宜做背景调查，并签订保密协议、保密条款或保密承诺书。企业可要求前述人员使用企业提供的保密计算机并对信息进行加密，需要通过企业内部网络接入涉密计算机或设备的，应通过堡垒机采取保密措施。

## **3.9 【销售管理】**

### **3.9.1 【客户信息管理】**

对于由客户的名称、地址、联系方式以及交易的习惯、意向、内容等区别于相关公知信息的特殊客户信息组成的客户名单，企业应按照本指南开展商业秘密管理工作。

### **3.9.2 【产品流通管理】**

对于投入市场流通且涉及技术秘密的产品，企业宜采取足以对抗不特定第三人通过反向工程获取该技术秘密的保密措施，如采取一体化结构，产品拆解后技术秘密即被破坏。

## **3.10 【财务管理】**

**3.10.1** 企业宜对涉及商业秘密的财务信息进行严格管理，采取以下保

密措施：

a) 不得在不利于保密的场合谈论涉密财务信息，不得在不利于保密的位置存放纸质涉密财务资料，不得在未经批准的情况下随身携带涉密财务资料。

b) 与财务相关的重要文件、软件、报告应设置秘钥，应指定专人保管，秘钥的密码应定期更换。使用人不得泄露密码，并保证秘钥和密码的使用安全。

c) 对因工作需要需要查阅重大交易记录、重要财务数据的，查阅人应提出申请并逐级审批，经商业秘密管理人员最终审批通过后，方可调阅。

**3.10.2** 应安排专人管理网银业务系统的交易数据，管理人员必须通过严格的资信调查。企业应定期检查，确保网银业务系统的保密性。

### **3.11 【内控内审】**

#### **3.11.1 【检查和评估】**

**3.11.1.1** 企业应定期对商业秘密保护、管理情况进行检查和评估并形成书面报告，检查内容应包括：

- a) 商业秘密保护制度的适宜性、实施情况等；
- b) 商业秘密管理人员的履职情况；
- c) 涉密人员管理情况；
- d) 涉密区域管理情况；
- e) 商业秘密事项的定密、隐密、解密、分级、流转、销毁情况；

- f) 涉密文件资料、计算机的管理情况；
- g) 涉密账户、电子信息、操作系统、办公软件的管理情况；
- h) 电子邮箱、聊天工具、设计软件、存储软件等工具软件使用商业秘密的情况；
- i) 涉密载体、物品的管理情况等。

**3.11.1.2** 企业应采取以下措施并保留记录或原始文件用于检查和评估：

- a) 重要涉密区域的出入口和内部应安装监控系统实时监控；
- b) 涉密网络的出、入口应实时监控；
- c) 涉密计算机的操作；
- d) 存储商业秘密信息的信息系统；
- e) 对外发送商业秘密信息的软件，如电子邮箱、即时通讯软件等。

**3.11.1.3** 企业可根据自身情况，委托第三方专业机构对企业商业秘密管理情况进行评估。

### **3.11.2 【纠正和整改】**

**3.11.2.1** 企业发现有泄密情况及隐患的，应及时采取纠正或预防措施。

**3.11.2.2** 企业应针对定期评估报告发现的管理漏洞制定改进方案、整改计划并严格执行。

**3.11.2.3** 企业应对商业秘密保护制度落实环节中存在的问题对相关责任人进行约谈、问责。

**3.11.2.4** 企业应对整改情况定期进行复查、复评。

### **3.12【对外合作】**

#### **3.12.1【外部人员访问管理】**

**3.12.1.1** 外部人员进入企业应出示证件并履行登记程序，佩戴与企业内部员工不同颜色的出入卡。

**3.12.1.2** 外部人员访问涉密区域应经审批并进行登记，告知其禁止录音、摄影、摄像、使用便携机、移动存储介质等设备，限制手机等器材的拍摄功能，并安排专人全程陪同。

**3.12.1.3** 区分可参观区域和禁止参观区域。外部人员进入企业参观的，应设置专门的参观路线以避免涉密区域（禁止参观区域），参观路线上可能涉及的商业秘密信息应采取隐蔽措施。

#### **3.12.2【项目合作管理】**

**3.12.2.1** 在商务合作、共同研究及涉及商业秘密的交易、公证、保险等活动时，企业应与外部合作方签订保密协议，或在合同条款中规定保密要求，约定保密内容和范围、保密义务及违约责任等。技术交易场所或者中介机构对其在从事代理或者居间服务中知悉的有关当事人的技术秘密，负有保密义务。

**3.12.2.2** 在共同或委托开发的项目合作中，企业应对其进行严格的背景调查，评估其保密能力和商业信誉，同时，企业应采取措施防止侵犯他人商业秘密，签订保密协议对涉及商业秘密等知识产权的权利归属和使用权做出约定。

**3.12.2.3** 涉密项目需要长期向外部合作方提供商业秘密信息的，或因

维修、研发等需要经常进入涉密区域的，企业可要求外部合作方采取以下保密措施：

- a) 与参与项目的外部合作方员工签订个人保密协议；
- b) 使用企业提供的保密计算机；
- c) 使用企业提供的加密系统；
- d) 使用企业提供的加密存储介质；
- e) 对外部人员使用的便携机等设备进行检查。

### **3.12.3 【会议及活动管理】**

在涉及商业秘密的会议或其他活动中，企业宜采取以下保密措施：

- a) 选择具有保密条件的场所；
- b) 尽量避免使用远程视频、音频、电话会议等线上会议方式，如必须采用的，应采取会议密码、屏幕水印等保密措施；
- c) 根据工作需要，限定参加人员的范围，指定参与涉密事项的人员；
- d) 告知参加人员保密要求，必要时签订保密承诺书；
- e) 对涉密文件、资料进行控制，如：确定文件发放范围，做好发放登记；重要涉密文件资料应有明显保密和会后回收标识；休会或会议结束时，及时收回清点、登记。

### **3.13 【国际合作】**

企业应审慎选择国际合作伙伴。企业在与国际企业开展合作之前，应对合作伙伴及其下属控制企业进行背景调查和评估，包括商业信誉、

保密能力等，避免因合伙伙伴的原因致使企业面临被制裁的风险。

企业可以通过查阅相关的行业报告、咨询专业机构或与其他合作伙伴进行交流等方式获取信息，了解合作伙伴在商业秘密保护方面的制度和措施，以及是否有过商业秘密泄露或侵权的不良记录，做好针对商业秘密侵权的风险预案。

## 【相关案例】

### 1. 对企业经营中的电子数据类信息可以采取哪些有效的保密措施？

**来源：**新赛点体育公司案（2018）京73民终686号

**案情简介：**原告公司经营中国高尔夫网，为多家银行的高端客户提供高尔夫球增值服务。被告金某等五人曾分别在原告公司就职，其与原告公司签订的《劳动合同书》《商业秘密保密合同》《员工手册确认书》中明确约定，“乙方在甲方工作期间所获悉的商业秘密，包括但不限于公司资料、文件、信息、软件、数据库及其他公司的信息资料（包括但不限于书面资料、电子文本、照片等）；乙方从甲方获得的与项目有关或因项目产生的任何商业、营销、技术运营数据或其他性质的资料”，并列明了保密义务和例外情形。原告公司将其与高尔夫球场、银行等合作的信息通过MIS系统和21Golf管理系统进行管理，对不同部门、级别的员工根据岗位设置了不同的操作使用权限。被告从原告公司辞职后，加入被告新赛点体育公司（全称：北京新赛点体育投资股份有限公司），将原告公司与相关银行的合作信息、交易价格等披露给新赛点公司，使新赛点体育公司成功以类似价格与特定银行签约成功。法院经审理后认为，原告公司对其主张的与银行合作的信息采取了合理保护措施，该部分经营信息属于商业秘密。新赛点体育公司、金某等5人应承担侵权责任。

**解读：**本案中，原告公司对经营中产生的电子数据信息采取了以下几种叠加的保密措施：第一，在相关协议中对保密信息的范围以及多样化的电子数据载体，采取“列举+兜底”的方式进行具体的约定；第二，对银行、高尔夫俱乐部等相关经营信息通过专门的信息系统进行管理，并对不同部门、级别的员工设置了不同的操作权限；第三，对上述措施做好相关记录，留存证据。在诉讼中相关证据被认定为采取了有效的保密措施，进而认定相关信息属于商业秘密，应受保护。

## 2. 通过发放员工手册约定的竞业限制是否有效？

**来源：**杭州某舞蹈培训公司诉左某竞业限制案(2012)浙杭民终字第 2913 号

**案情简介：**2011 年 7 月杭州某舞蹈培训公司与左某签订书面《劳动合同书》及《保密协议》，但未约定竞业限制条款。2012 年 2 月左某申请离职，于同年 5 月到另一舞蹈学校从事教学工作。杭州某舞蹈培训公司诉至法院，提交《员工手册》一份，上面约定了竞业限制的时间、地域范围、补偿金额和支付时间，但未能证明左某实际签收过该《员工手册》。法院认定原告提交的证据不能充分证明载有竞业限制条款的《员工手册》被左某签收，判决原告败诉。

**解读：**企业与劳动者约定竞业限制，应尽可能在《劳动合同》《保密协议》或《竞业限制协议》中，对竞业限制的范围和期限等作出明确约定，而不是仅体现在单方发放的《员工手册》中。

如果《员工手册》中对竞业限制的具体内容、时间、区域、补偿金的金额及支付进行了明确约定，而且《员工手册》有员工的书面签收确认，应视为有效，对员工具有约束力，建议企业留存相关的书面签收确认单。

## 3. 企业和员工约定了竞业限制条款，但没有实际支付竞业限制补偿款的，能否要求员工承担竞业限制的违约责任？

**来源：**A 珠宝公司诉马某、B 珠宝公司不正当竞争纠纷案（2006）苏民三终字第 0018 号

**案情简介：**2001 年，A 珠宝公司与马某签订协议，聘请马某为公司的副总经理，同时约定马某因解聘、辞职、退休等原因离职起二年内，不能自行从事同类业务或受雇于与 A 珠宝公司同类业务的公司。2004 年，马某与他人成立 B 珠宝公司，马某担任法定代表人。B 珠宝公司与 A 珠宝公司经营范围均与生产销售金属首饰、工艺品相关。A 珠宝公司将马某与 B 珠宝公司诉至法院，诉讼中，法院查明竞业限制协议中未约定补偿金，其亦未实际向马某支付补偿金。故法院认定竞业限制条款无效，马某无需承担违约责任。

**解读：**根据权利义务对等原则，企业应主动向员工支付竞业限制补偿金。如果竞业限制协议中未约定补偿内容（包括补偿金的计算方式、支付时间等），或虽然约定，双方劳动合同关系结束后没有实际给予劳动者竞业限制补偿金的，劳动者无需承担违反竞业限制的违约责任。

#### 4. 企业能否以奖金、分红等代替竞业限制补偿金？

**来源：**A 印刷公司诉薛某、B 印刷公司不正当竞争纠纷案（2006）苏民三终字第 0027 号

**案情简介：**薛某曾任 A 印刷公司技术质量部部长，并为公司的股东之一。2003 年，薛某提出辞职并至某 B 印刷公司担任总经理助理职务。后 A 公司以薛某违反竞业限制约定为由诉至法院，同时 A 公司认为薛某在 A 公司任职期间所获得的奖配股、红利筹等应视为竞业限制补偿金。法院判决 A 公司败诉。

**解读：**本案中企业支付的奖配股、红利被法院认为系员工基于股东身份获得，不能视为公司对员工支付的竞业限制补偿金。建议企业对竞业限制补偿金进行明确清晰的约定并单独支付。竞业限制补偿金的金额应能体现对劳动者就业自由限制的合理补偿，如果过低其效力也可能受到质疑。

#### 5. 企业销售环节的单个或少量客户信息能否作为商业秘密保护？

**来源：**上海可可庄公司案（2008）沪一中民五（知）终字第 3 号

**案情简介：**吴某原为可可庄公司的员工，在可可庄公司工作时与某外国客户进行了长时间的联系以及业务洽谈。后吴某离职，自行出资设立公司，并与该外国客户发生了一笔交易，该交易与吴某在可可庄公司工作时与该客户业务洽谈有关。经查明，原告可可庄公司对其客户名单采取了保密措施，包括：在业务员参加广交会等各种会展后将客户的名片装订成册，同时将客户的信息整理后输入数据库中；通过公司服务器为业务员设置电子邮箱，以便于业务员与客户进行业务联系，邮箱设置时由原告法定代表人设定密码，除原告法定代表人及

业务员本人外，他人无法看到业务员邮箱中的邮件内容。法院审理后认定该特定外国客户的信息构成商业秘密，吴某的行为构成商业秘密侵权。

**解读：**客户名单是否能作为商业秘密保护，主要取决于客户信息的深度，而非客户的数量。少量甚至单个客户的信息如果能为企业带来商业价值且采取了相应保密措施，也可以受到保护。

## **6. 市场流通产品贴“危险！私拆担保无效！”警示标志可否视为采取了相应的保密措施？**

**来源：**济南思克公司与济南兰光公司侵害技术秘密纠纷案（2020）最高法知民终 538 号

**案情简介：**思克公司生产并在市场上销售气体透过率测试仪。该测试仪生产过程中使用了思克公司的技术秘密。思克公司向法院起诉称，被告兰光公司通过恶意发起的诉讼、利用另案的保全程序取得原告生产的测试仪，获取了原告的技术秘密，并运用在被告产品生产中，构成商业秘密侵权。原告提出，对上述技术秘密已经采取合理的保密措施，包括：原告在测试仪的特定位置贴有标签，载明“危险！私拆担保无效！”“SYSTESTER 思克品质保证撕毁无效”等内容；在与客户签订的《设备购销合同》中约定，“该气体透过率测试仪产品的转让不意味着客户公司取得该产品的任何知识产权，且客户公司需承担确保该产品技术机密信息安全以及不得将技术机密信息提供给任何第三方的合同义务”。

法院审理后认为，原告与客户签订的合同，仅具有约束客户的效力，由于《设备购销合同》并未限制客户对所购买的产品进行处分、转让，故不特定第三人可通过市场流通取得该产品，且不受《设备购销合同》的约束。另一方面，原告在测试仪上贴的标签内容属于安全性提示与产品维修担保提示，且无法约束后续受让产品的不特定第三人，故不构成以保密为目的的保密防范措施。最终，法院认定原告未采取相应的保密措施，其主张的技术信息不构成受反不正当竞争法保护的商业秘密。

**解读：**对于承载了技术秘密的产品，一旦进入市场流通，就脱离了权利人的物理控制，其采取的保密措施应与始终处于权利人控制之下的技术图纸、配方文档等内部性载体相区别。我国法律规定，他人通过自行开发研制或反向工程获得被诉侵权信息的，不构成商业秘密侵权。因此，权利人对市场流通产品这类外部性载体采取的保密措施，应足以对抗不特定第三人通过拆卸、测绘、分析产品获得产品的相关技术信息（即反向工程）。比如采取一体化结构生产，拆解产品将破坏技术秘密等。仅在产品上贴“危险！私拆担保无效！”的标签，更多属于产品安全性提示，且系思克公司的单方声明，不能约束后续通过转让等途径取得产品的他人对产品进行拆解等自由处分行为，故不属于与商业秘密的性质、载体相适应的保密措施。

## 7. 客户数据或营销获客渠道是否属于AI平台公司的商业秘密？

**来源：**AI平台型企业客户数据和营销获客渠道商业秘密纠纷（北京知识产权法院发布的侵犯商业秘密十大典型案例）

**案情简介：**赵某是某AI信息平台公司员工，公司明确了赵某的保密义务，并对公司的商业秘密采取了保密措施。赵某将某信息公司《市场花费台账模板2018-7月》excel文件等经营秘密违法披露给竞争对手某广告有限公司。某广告公司获悉后主动联系其中记载的渠道商寻求商务合作。信息公司以赵某、某广告公司的行为侵犯商业秘密为由诉至一审法院，请求判令赵某、某广告公司停止侵犯商业秘密行为、永久删除承载商业秘密的文件、共同赔偿经济损失50万元及合理开支3.0768万元。

法院认为，赵某和某广告公司均违反《中华人民共和国反不正当竞争法》第九条第三款的规定，故判令赵某、某广告公司停止侵犯商

业秘密行为、分别赔偿经济损失5万元、15万元，共同赔偿合理开支3.0768万元。

**解读：**客户数据或营销获客渠道属于AI平台型企业从事经营活动的必要支撑，客户数据或营销渠道的精准程度同时也是数字经济时代背景下企业市场竞争优势的重要体现，在符合秘密性、价值性、保密性的条件下，构成受法律保护的商业秘密。员工或前员工提供工作中接触的客户数据或营销渠道等经营信息给竞争公司，员工与竞争公司共同构成侵犯商业秘密主体。

## 4. 民事保护

### 4.1 【当事人主体资格】

#### 4.1.1 【一般情形】

商业秘密的权利人及被许可使用人有权作为原告提起侵害商业秘密诉讼或申请商业秘密仲裁。其中独占许可被许可人可单独起诉，排他许可被许可人可与权利人共同起诉或在权利人不起诉情况下自行起诉，普通许可被许可人可与权利人共同起诉或经权利人书面授权单独起诉。

#### 4.1.2 【确认不侵害商业秘密之诉】

被商业秘密权利人发送侵权警告的相对方可向权利人发出诉权行使催告。若权利人未在合理期间内起诉，则该相对方有权提起确认不侵害商业秘密之诉。

### 4.2 【主管与管辖】

#### 4.2.1 【主管】

若原、被告间存在合同关系且就商业秘密问题存在有效仲裁条款，宜向仲裁机构提起仲裁。若原、被告间存在劳动合同关系，原告主张被告违反竞业限制协议，应适用劳动争议解决程序，不宜直接起诉。

#### 4.2.2 【管辖】

因侵害商业秘密案件属于侵权之诉，依法由侵权行为地或被告住所地法院管辖。

侵权行为地包括侵权行为实施地和侵权结果发生地，如非法获取

商业秘密地、侵权产品制造地等，但不宜至原告住所地、侵权产品销售地、收货地等地法院起诉。

在本市范围内，技术秘密民事纠纷案件由上海知识产权法院管辖，但诉讼标的额在 2 亿元以上或者诉讼标的额在 1 亿元以上的涉外、涉港澳台及当事人一方住所地不在本市的技术秘密民事纠纷案件由上海市高级人民法院管辖；经营秘密民事纠纷案件一般由各区法院按辖区管辖。也就是说，侵权行为地或被告住所地在浦东的经营秘密民事纠纷案件由浦东新区人民法院管辖。

#### **4.3 【诉讼请求、事实及理由】**

##### **4.3.1 【明确秘点】**

原告应在一审法庭辩论终结前明确商业秘密的具体内容即秘点。建议出具书面的秘点说明，指出哪些技术、经营或其他信息需要保护，这些信息与原告提交的信息载体间是何关系，并将其中的公有领域信息予以剔除，而非笼统地将某载体如文件、图纸、软件整体主张为商业秘密。

##### **4.3.2 【明确行为类型】**

原告应明确其主张的侵权行为类型，是非法获取、披露、使用、允许他人使用还是教唆、引诱、帮助他人违反保密义务侵害商业秘密，并明确各被告是否共同侵权及是否承担连带责任。

##### **4.3.3 【明确责任承担方式】**

原告应提出明确、具体、可执行的责任承担方式，包括停止侵害、赔偿损失及合理开支等。

因侵犯商业秘密受到损害的权利人的赔偿数额，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。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难以确定的，由法院根据侵权行为的情节判决给予权利人五百万元以下的赔偿。

侵权人恶意实施侵犯商业秘密行为，情节严重的，法院可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。

合理开支系权利人为维权支出的费用，包含取证费、律师费、翻译费、侵权产品购买费、差旅费等。

案件受理费、保全费属于诉讼费，由法院依职权处理，无需作为诉请提出。诉讼过程中产生的司法鉴定费，法院根据诉讼结果决定如何负担。备注：根据《上海市浦东新区建立高水平知识产权保护制度若干规定》第十条规定，故意侵犯商业秘密，情节特别严重的，法院可在按照上述方法确定数额的五倍以上十倍以下确定赔偿数额。上述金额难以确定，由法院根据侵权行为的情节判决给予权利人一千万元以下的赔偿。

#### **4.4【证据准备及证明标准】**

##### **4.4.1【原告的证明责任】**

当事人对自己提出的主张应及时提供证据。原告应在法院确定的举证期限届满前提出证据，无正当理由逾期提供证据可能不被采纳或虽被采纳但受到训诫、罚款处罚。

##### **4.4.2【权利证据】**

原告可提供开发商业秘密的证据以证明所有权，例如研发报告、证人证言、客户或经营信息表格、交易合同及发票等；可提供转让、许可或授权合同等证据以证明使用权。

#### **4.4.3【秘密性、价值性及保密性】**

原告应证明其主张的商业秘密具备三个特征，即不为公众知悉、具有商业价值以及采取保密措施。对于技术信息可采用类似权利要求方式固定秘点或由第三方专业机构出具检索报告；对于经营信息应列明每个秘点的名称及内容。商业价值的证明可提供开发成本或获利的相关证据佐证。保密措施需达到在特定范围内足以达到防止泄露的合理标准，如提供协议、规章、标注、权限等形式的证据。

#### **4.4.4【客户信息的证明标准】**

对于属于经营秘密的客户信息，内容除名称、地址、联系方式外，还应满足深度信息和交易稳定性的要求，能体现出客户特别需求、交易习惯等特殊信息。

#### **4.4.5【被告的证明责任】**

若原告提供初步证据证明其主张商业秘密的具体内容、已采取的保密措施以及被侵权事实，则被告应证明原告主张不属于商业秘密或者系合法获得。

#### **4.4.6【侵权推定】**

若原告证明被告信息与原告商业秘密相同或实质性相同，且被告有接触原告商业秘密的条件后，除非被告能证明其有合法来源，否则法院可推定被告采取不正当手段侵犯商业秘密。

#### **4.4.7 【惩罚性赔偿的证明标准】**

原告主张惩罚性赔偿应证明被告恶意实施商业秘密侵权行为且情节严重。

#### **4.5 【诉讼过程中的保密措施】**

##### **4.5.1 【不公开审理】**

当事人可以视情况向法院申请不公开审理。

##### **4.5.2 【人员限制】**

当事人可以申请法院对接触涉及商业秘密相关证据或信息的诉讼参与人员范围做出相应限制。

##### **4.5.3 【涉密证据质证】**

当事人可以对证据交换和质证方式提出意见，在法庭主持下确定涉密证据的开示方式。

##### **4.5.4 【裁判文书上网屏蔽】**

涉及商业秘密的裁判文书上网公开时法院会进行相应的信息屏蔽处理。

#### **4.6 【证据保全与行为保全】**

##### **4.6.1 【证据保全】**

在证据可能灭失或以后难以取得的情况下，当事人可以在诉讼过程中向法院申请保全证据。商业秘密侵权诉讼的证据保全主要集中在被告侵权行为及被告侵权获利两方面，常见的有被告往来邮件、合同、生产技术资料、财务账册等。原告应明确秘点并提供被告侵权及存在取证困难或证据灭失风险的初步证据，并且在举证期限届满前提出证

据保全申请，否则可能不被法院准许。

原告能够自行获得或公证固定的证据，无需向法院申请证据保全，可自行至市场监管、税务、海关等部门调取。

证据保全可能需要提供担保，复杂情况会涉及鉴定或审计。

#### **4.6.2 【行为保全】**

在侵权行为可能对原告合法权益造成难以弥补的损害或使案件裁决难以执行情况下，原告可向法院申请对被告采取行为保全措施。

## 【相关案例】

### 1. 违反竞业限制义务是否等于侵犯商业秘密？

**案情简介：**被告系原告公司员工，与原告签有竞业限制协议。离职后，被告成立与原告存在竞争关系的公司。原告以商业秘密侵权诉至法院，认为被告在公司经营中必然会使用到原告的商业秘密，但没有得到法院支持。

**解读：**违反竞业限制协议的行为可能同时构成违约与商业秘密侵权。但并不是所有的违反竞业限制协议的行为都能构成商业秘密侵权。如果原告不能证明自己拥有商业秘密，且被告采取了不正当手段侵犯其商业秘密，则不能主张商业秘密侵权，只能提起违反竞业限制的违约之诉。

### 2. 商业秘密的载体是否等同于商业秘密？

**案情简介：**原告诉称，被告自2006年5月起在原告处从事电脑动画和效果图制作工作，其制作的动画展示了高科技生态低碳建筑 技术安装体系施工流程。被告离职后将包含上述施工流程的动画以光盘形式广为散发。原告主张该动画文件是原告的商业秘密，未得到法院支持。

**解读：**动画文件仅仅是原告主张商业秘密的载体。商业秘密的载体和具体内容不能等同。原告主张商业秘密，除提供商业秘密载体外，还应明确商业秘密的具体内容，仅仅载体本身不能构成商业秘密。

### 3. 未明确商业秘密具体内容的法律后果是什么？

**案例：**M公司诉S公司等侵犯商业秘密纠纷案

**案情简介：**该案中原告主张两种产品的技术配方、技术诀窍是其技术秘密，但仅提交了说明书和产品标签，未得到法院支持。

**解读：**说明书和产品标签中仅有对产品配方、成分等概括性的描述记载，而无技术配方、技术诀窍的具体内容。原告主张技术配方、技术诀窍构成其商业秘密，应明确构成商业秘密的技术配方和诀窍是什么，即应明确商业秘密的具体内容。否则，法院无法判断其主张商业秘密的信息是否符合法律规定的构成要件，被告也无法针对性地提出公知技术信息等抗辩。

### 4. 已经公开的信息能否构成商业秘密？

**败诉案例1：**被告离开公司前，将原告客户发给原告的招股说明书发送给了案外人。原告认为，客户不希望其发给原告的内容被同行所知，原告对此负有保密义务，同时该招股说明书对原告而言也是重要的商业机会，因此被告行为构成商业秘密侵权。法院经审理查明，该说明书“项目背景”部分明确标注了该方案系向国内知名管理咨询公司、IT系统开发商公开征集。故法院没有认定该招股说明书构成商业秘密。

**败诉案例2：**原告主张项目方案、合作方的时间安排、制度汇编和公司组织结构等构成经营秘密。法院经审理查明，项目方案系原告向国内公开征集，制度汇编涉及的各项管理规定多为业内公知的一般性

操作规范，公司组织结构等在原告公司的自建网站上可以查阅，该四项信息均不构成商业秘密。

**败诉案例3：**原告将已申请专利的技术主张商业秘密，没有得到法院支持。

**解读：**商业秘密应具有秘密性，已经通过网络或其他途径公开了的信息不构成商业秘密。对于专利技术而言，由于专利申请均会向社会公布，已经申请专利或正在专利申请中的技术均不宜主张商业秘密。

## 5. 权利人自行披露的信息能否认为他人非法获取？

**案情简介：**原告系案外人D公司的独家经销商，原告曾与D公司签订协议，约定在合作期间，原告的客户信息是共享的，原告会将其交易的具体信息（包括采购联系人、电话、电子邮箱、产品、价格、一年的销售额等）抄送给D公司，也不要求其保密。D公司每月会与原告一起去拜访客户。被告S公司系D公司投资设立的子公司。原告认为S公司取得原告的客户信息系非法，构成商业秘密侵权，但未得到法院支持。

**解读：**D公司取得原告的客户信息系原告自行披露，原告亦未与D公司签订保密协议。S公司系D公司投资成立的子公司，其从D公司取得原告的客户信息并不违法，具有合法的来源。

## 6. 仅说明客户名称能否被认定为商业秘密？

**案情简介：**原告系多年从事进出口业务的公司，被告以前系原告

业务员。原告提交了10家客户名称，认为该10家客户名称是商业秘密，被告与其他公司串通，与原告客户交易，构成商业秘密侵权。但法院没有支持其主张。

**解读：**客户名称本身并不能构成商业秘密，能够作为商业秘密保护的客户名单一般是指客户的名称、地址、联系方式以及交易的习惯、意向、内容等构成的区别于相关公众信息的特殊客户信息。对于该些信息原告应进行举证或说明，否则难以认定其构成商业秘密。

### 7. 主张特定客户属于商业秘密是否应证明该客户与原告存在长期稳定的交易关系？

**案情简介：**被告曾是原告员工，在原告处工作期间成立公司并与某客户进行交易。原告认为该客户是原告的商业秘密，被告构成侵权，但原告仅提供了某年自己与该客户交易的两张总价为5000多元的凭证。法院没有认定该客户信息构成原告的商业秘密。

**解读：**原告要主张某特定客户信息构成其商业秘密，应证明该客户与原告存在长期稳定的交易关系，否则诉请难以得到支持。

### 8. 使用公开模型的人工智能算法是否属于商业秘密？

**来源：**智搜公司诉光速蜗牛公司等侵犯商业秘密案（广东高院发布的数字经济知识产权保护典型案例）

**案情简介：**智搜公司是互联网高科技公司，主要产品有“天机”APP以及AI写作机器人，采用自主开发的大数据追踪系统，实现智能跟

踪、个性化推荐、智能摘要等功能。光速蜗牛公司采用与智搜公司实质相同的推荐算法，用于融资、推出APP应用程序，并向深圳市科技创新委员会提交《深圳市技术创新计划创业资助项目申请书》，从中非法获利。智搜公司向法院起诉，主张光速蜗牛公司非法使用其商业秘密，请求判令光速蜗牛公司立即停止侵权，并赔偿智搜公司经济损失100万元。

法院认为，光速蜗牛公司在其开发的“学点啥”APP中使用实质相同的被诉侵权推荐算法，无法说明研发过程和提供研发记录，并聘用了三名原智搜公司研发团队人员，侵犯了智搜公司的商业秘密，构成不正当竞争行为。遂判决光速蜗牛公司停止侵犯商业秘密的行为，下架侵权APP产品，赔偿智搜公司经济损失及合理维权费用合计20万元。

**解读：**智搜公司请求法院保护的涉案技术信息为“天机—大数据追踪引擎”搜索算法。以模型选择优化作为核心的算法，即使所采用的模型为公知信息，但若模型的选择与权重排序方案需通过大数据的收集、处理和测试等方能获得，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。涉案算法可用于更精准的检索及向用户提供信息，能为智搜公司带来商业收益和竞争优势。智搜公司已对涉案算法采取合理保密措施。最终法院认定涉案算法符合商业秘密的全部构成要件，属于智搜公司的商业秘密。

## **9. 从多份不同文件总结提炼的技术信息可作为技术秘密保护**

**来源：**原告B公司与被告程某某、A公司侵害技术秘密纠纷案

**案情简介：**B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 B 公司员工，劳动合同约定其负有保密义务，并由 B 公司支付相应保密费用。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。程某某从 B 公司离职后入职 A 公司，并向 A 公司披露前述技术秘密。A 公司使用前述技术秘密生产、销售产品。B 公司以程某某、A 公司侵害技术秘密为由，起诉请求法院判令程某某、A 公司停止侵权，赔偿 B 公司经济损失 6,800 万元及合理开支 100 万元，赔礼道歉并消除影响。

上海知识产权法院经审理认为，B 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，B 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、A 公司侵犯。程某某、A 公司虽然认为所有秘点均已被现有文献所披露，但提交的证据并不足以证明该主张，故涉案信息构成 B 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 A 公司披露涉案技术秘密的行为构成侵权。A 公司与 B 公司具有同业竞争关系，应当知道 B 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、A 公司停止侵权，共同赔偿 B 公司经济损失 100 万元及维权合理开支 30 万元。程某某、A 公司不服，提起上诉。二审法院判决驳回上诉，维持原判。

**解读：**技术秘密通常以图纸、工艺规程、实验数据等形式体现，权利人从其多份技术资料等载体文件中总结、概括、提炼秘密信息的，只要这种总结、概括、提炼在载体文件中均有对应或者能够结合技术常识推断出来，就应当允许将其具有秘密性的信息的技术方案请求保护。权利人从其不为公众所知的多份技术文件中合理提炼出的技术方案，只要不为所属领域相关人员普遍知悉和容易获得，就可以作为技术秘密予以保护。

## 10. 举证责任转移的适用

**来源：**原告 Y 公司、Y 上海公司与被告孙某某侵害技术秘密纠纷

案

**案情简介：**Y公司许可Y上海公司使用其商业秘密。孙某某曾在Y上海公司担任服务工程师、服务主任等职务，劳动合同约定了孙某某应当承担的具体保密义务。Y上海公司制定的《员工手册》《使用技术资源规定》等均规定了相关保密制度。Y公司、Y上海公司主张的载有涉案技术信息的图纸存储于公司网络系统中，仅经Y上海公司授权的员工可登录进入。Y上海公司发现，孙某某从其公司系统中大量下载含有商业秘密的图纸并转存至私人存储设备，遂向孙某某发送了解除劳动合同通知。Y公司、Y上海公司认为，孙某某的行为使公司的商业秘密处于随时可能被外泄的危险境地，故起诉请求判令孙某某停止侵权并赔偿Y公司、Y上海公司合理开支100万元。孙某某认为Y公司、Y上海公司诉称的技术信息并不构成商业秘密，但未提交证据。

上海知识产权法院经审理认为，Y公司、Y上海公司已明确其主张的商业秘密范围并采取合理保密措施，在案证据也表明，孙某某从Y上海公司系统中下载了载有涉案商业秘密的技术图纸并转存至外接存储设备，使得Y公司、Y上海公司对涉案商业秘密失去控制，面临随时被披露和使用的风险，可见Y公司、Y上海公司所主张的商业秘密已被侵犯。孙某某虽然认为Y公司、Y上海公司所主张的涉案技术信息已进入公有领域，但未提供任何证据予以证明，故应当认定涉案信息构成商业秘密，孙某某的行为构成侵权，遂判令孙某某不得披露、使用或者允许他人使用涉案商业秘密，向Y公司、Y上海公司提交存储有涉案商业秘密的载体并赔偿Y公司、Y上海公司合理维权费用30万元。孙某某不服，提起上诉。二审法院判决驳回上诉，维持原判。

**解读：**《中华人民共和国反不正当竞争法》第三十二条规定了举证责任的转移，即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。本案商业秘密的载体为技术图纸，Y公司、Y上海公司对此已采取合理的保密措施，孙某某从公司系统中下载载有涉案商业秘密的技术图纸并转存至外接存储设备，可见相关商业秘密已被非法获取，此时证明涉

案信息不构成商业秘密的举证责任转移至孙某某处。孙某某虽然认为 Y 公司、Y 上海公司所主张的技术信息已经进入公有领域，但未提供任何证据予以证明，故应当认定涉案技术信息不为公众所知悉，构成商业秘密。

## 11. 非法获取商业秘密行为的赔偿数额认定

**来源：**原告 M 公司、K 公司与被告王某某侵害技术秘密纠纷案

**案情简介：**M 公司、K 公司共同投入资金研发了涉案 195 个技术文件。王某某原系 K 公司员工，该公司《员工守则》规定，如果员工违反保密义务，应向公司支付 5 个月的工资作为违约罚款；如果员工行为对公司的损害超过了其违约金额，还需赔付公司损失的额外部分。王某某在 K 公司任职期间，多次将包括涉案 195 个技术文件在内的总计 900 多份公司机密文件擅自转移至若干个未经 M 公司、K 公司授权的 USB 存储设备。王某某签署《确认函》承认上述事实并承诺配合删除前述机密文件，但后又以其不再是公司员工无协助返还义务为由，既未向 M 公司、K 公司返还用于保存前述机密文件的 USB 存储设备，亦未提供前述机密文件已被删除的证据。M 公司、K 公司认为，王某某以不正当手段获取涉案 195 个技术文件的行为侵害了 M 公司、K 公司的商业秘密，故起诉请求判令王某某立即停止侵权，赔偿 M 公司、K 公司经济损失及合理开支 500 万元。

上海知识产权法院经审理认为，涉案 195 个技术文件中的技术信息属于 M 公司、K 公司的商业秘密，王某某擅自将涉案技术信息转存至未经 M 公司、K 公司授权的 USB 存储设备中，在签署《确认函》后又拒绝配合，其行为侵害了 M 公司、K 公司的商业秘密，应当承担停止侵权、赔偿损失的民事责任，遂判令王某某停止侵权，赔偿 M 公司、K 公司经济损失 26 万元及合理开支 24 万元。一审判决后，双方当事人均未上诉。

**解读：**在非法获取商业秘密行为构成侵权且没有使用行为的情况下，本案从被诉侵权行为致使涉案商业秘密处于不可控的危险境地，增加了权利人防止涉案商业秘密被他人获取、披露、使用的压力与负

担等因素来考量赔偿的必要性，并综合涉案商业秘密的类型、内容、数量，涉案侵权行为的性质、情节、后果，参考K公司《员工守则》中有关员工违反保密义务的罚则规定确定赔偿数额。

## 12. 产品配方可以构成商业秘密

**来源：**原告T公司与被告X公司侵害技术秘密纠纷案

**案情简介：**T公司主张其投入大量人力、物力研制麻辣烫汤底配方，所打造的麻辣烫品牌在外卖平台的麻辣烫类目评价中位列前茅。T公司诉称其前员工张某某在职期间通过不正当手段窃取T公司的五款麻辣烫汤底配方，并在离职后与X公司使用T公司的麻辣烫汤底配方经营麻辣烫，侵害了T公司的商业秘密，请求判令X公司停止侵权并赔偿T公司经济损失及合理开支546,000元。

上海知识产权法院经审理认为，T公司主张的涉案五款麻辣烫汤底配方具有独特的配料及比例，能为其带来市场竞争优势，具有商业价值，T公司对此也采取了相应的保密措施，构成技术秘密。被诉侵权配方使用了T公司涉案配方的配料及相应比例，T公司前员工张某某具有接触涉案配方的可能并帮助X公司经营麻辣烫产品，X公司亦未提供自行研制获得被诉侵权配方的证据，可以认定其使用了涉案技术秘密用于其麻辣烫产品，侵害了T公司享有的技术秘密。鉴于涉案店铺已停止经营，故对T公司的停止侵权诉请不予支持。法院根据涉案技术秘密的类型、商业价值、X公司的侵权故意、侵权行为持续时间、侵权范围、侵权产品的销售金额等因素酌情确定X公司赔偿T公司经济损失及合理开支共计15万元。一审判决后，双方当事人均未上诉。

**解读：**本案系涉及麻辣烫汤底配方的商业秘密纠纷案。本案判决认定T公司的麻辣烫汤底具有独特的配料及比例，可以构成商业秘密。经对T公司汤底配方与在市场监督管理机关调取的被诉侵权汤底配方进行了细致比对，认定X公司使用了与T公司相同或者实质相同的汤底配方，构成商业秘密侵权。考虑到涉案汤底配方的商业价值、X公司存在主观故意、侵权行为时间较短等因素，最终判令X公司赔偿T公司15万元。本案判决表明，“小配方”也可以得到“大保护”，体现

了法院加大知识产权司法保护的力度。

### 13. 单一潜在客户的采购意向可作为商业秘密获得保护

**来源：**原告M公司与被告李某某等侵害经营秘密、不正当竞争纠纷案

**案情简介：**M公司授权案外人Z公司参与某市地铁项目的投标。李某某、张某某、施某某为M公司的员工，劳动合同中约定了保密义务。李某某利用担任M公司销售经理的便利，在代表M公司参与某市地铁项目投标工作中，冒用M公司名义推荐A公司给Z公司，最终Z公司与A公司就某市地铁项目签约并采购了A公司的产品。期间，张某某、施某某以T公司员工的身份与Z公司就产品问题进行沟通。之后，Z公司与M公司就李某某冒用M公司名义提供A公司产品达成《谅解备忘录》。经查，A公司系李某某前妻朱某某担任唯一股东的公司。李某某、张某某、施某某从M公司辞职后到T公司工作，T公司协助A公司履行合同。T公司的股东和法定代表人为李某某的父亲潘某某。M公司认为，李某某、张某某、施某某违法将M公司的商业秘密泄露给朱某某及A公司并允许其使用，T公司、潘某某提供配合与协助，七被告的行为已严重侵害M公司的商业秘密，故起诉请求判令七被告停止侵权，共同赔偿M公司经济损失3,626,148.81元及合理开支2,041.92元。

一审法院认为，M公司实际掌握的经营信息即Z公司在某市地铁项目中向M公司采购其产品的意向，属于M公司的商业秘密。李某某、张某某在M公司工作期间掌握了涉案商业秘密，A公司提供的产品与M公司涉案商业秘密内容实质相同且无合法来源，T公司明知所获知的涉案商业秘密归M公司所有却使用上述信息协助履行合同，李某某、张某某、A公司、T公司的行为共同侵害了M公司的商业秘密，遂判决李某某、张某某、A公司、T公司共同赔偿M公司经济损失300万元及合理开支2,041.92元并刊登声明、消除影响；朱某某、潘某某分别对A公司、T公司的付款义务承担连带责任。双方当事人均不服，提起上诉。

上海知识产权法院经审理认为，M公司所主张的经营信息具有秘

密性、价值性和保密性的特点，构成商业秘密。本案各被告未能提供充分证据证明其通过合法方式取得涉案商业秘密，且各被告共同侵害了M公司的涉案商业秘密，应当向M公司承担赔偿责任，遂判决驳回上诉，维持原判。

**解读：**本案对于单一潜在客户的采购意向是否构成商业秘密进行了深入分析，准确把握了商业秘密构成的实质要件，认定此类信息可为权利人带来一定的价值或者竞争优势，符合秘密性、价值性和保密性的特征，构成商业秘密。同时，本案各被告共同实施侵害商业秘密的行为具有一定的复杂性和隐蔽性，本案判决厘清了各被告间具体实施的行为，清晰界定了各被告之间的法律关系，并据此准确认定各被告的法律责任。

#### **14. 销售代理商为供货商开发客户时形成的客户信息可作为商业秘密获得保护**

**来源：**原告F公司与被告Y公司等侵害经营秘密纠纷案

**案情简介：**F公司自2004年10月起代理销售G公司生产的某品牌产品并提供技术服务，双方合同约定，鉴于F公司对相关客户既往所做的贡献，G公司与该类客户进行直接交易须按销售额向F公司支付一定比例的手续费。双方合同持续至2010年3月31日。2010年4月1日，G公司向客户发函称其已终止与F公司的代理关系，将由新的代理商Y公司提供服务。2010年4月1日起，G公司与Y公司建立代理合作关系，所有区域内的客户资料双方共享。Y公司的法定代表人孙某曾系F公司副总经理，二者签订的协议书中约定孙某应对公司营业资料、客户信息等保密。孙某于2009年6月与F公司解除劳动关系，于同年8月设立Y公司。孙某在某市场监督管理局于2012年对其的询问笔录中陈述，其自2002年3月起在F公司工作，主管公司的销售业务，客户均由其联系，其离职后主动找G公司洽谈并签订了代理协议；Y公司自2009年9月至2010年12月间共向139家客户销售过G公司的产品，与F公司提供给某市场监督管理局的名单相比，有48家客户相同；自2010年4月开始，共计发生经营额900多万元。部分客户于2016

年出具证明称公司需特定采购 G 公司的产品，其采购是基于对产品的需求和认可，而不是针对销售服务方的选择。F 公司认为，被告的行为侵犯了其对涉案 48 家客户享有的经营秘密，故起诉请求判令被告停止侵权并赔礼道歉，赔偿 F 公司经济损失 349 万元及合理开支 309,401.70 元。

一审法院判决驳回 F 公司的全部诉讼请求。F 公司不服，提起上诉。

上海知识产权法院经审理认为，F 公司在为 G 公司开拓中国市场过程中所积累的涉案 48 家客户的联系方式、交易习惯、交易需求、交易价格等经营信息均是需要与客户进行多轮接触、沟通并付出一定成本才能获得，其中的相关深度信息一般仅由 F 公司内部相关人员所掌握，符合商业秘密关于“不为公众所知悉”的法定条件；F 公司掌握的客户信息有助于其在与 G 公司销售代理关系存续期间维系现有客户，虽代理关系终止后，F 公司所掌握的客户信息对其可能不再具有带来竞争优势的价值，但对新的代理商而言，若能获得该信息，则可减少与客户重建联系的时间和成本，这也是销售代理商合同中约定 G 公司就其与部分客户发生直销时需向 F 公司支付销售手续费的原因之一，故涉案客户信息在 G 公司重新确定代理商时尚具有一定的商业价值；F 公司对其主张的客户信息采取了保密措施。因此，涉案 48 家客户信息可以认定为 F 公司的商业秘密予以保护。孙某能接触到 F 公司的经营秘密，离开 F 公司后 1 个多月便成立 Y 公司，此后不久即与涉案 48 家客户中的部分客户发生交易往来，可认定孙某违反保守商业秘密的要求向 Y 公司披露了 F 公司的经营秘密，Y 公司明知孙某的行为涉嫌侵犯 F 公司的商业秘密仍获取并使用，构成侵权，应共同承担民事责任，遂判决撤销一审判决，判令 Y 公司、孙某共同赔偿 F 公司经济损失及合理开支共计 30 万元。

**解读：**供货商固然有选择并更换代理商的权利，但在终止与原代理商的销售代理关系后，其重新确定的代理商或者该代理商的相关工作人员是否与原代理商存在关系并可能知悉由原代理商开发的客户深度信息，直接影响到是否涉嫌侵犯原代理商经营秘密的判断。此类案

件审理过程中，不能因交易产品为供货商生产的产品而当然地认为购买该产品的客户及其信息均属供货商所有，而应对客户名单的形成过程、供货商与销售代理商针对客户开发所作的约定、承担保密义务主体的确定、客户信息在代理商更换时的商业价值等进行综合分析后，给予销售代理商在为供货商开发客户过程中所形成的客户信息必要的保护。

## 15. 主动交易抗辩的审查认定

**来源：**原告 S 公司与被告张某某、W 公司侵害经营秘密纠纷案

**案情简介：**S 公司的主营业务为化学类产品经销，张某某曾系其销售人员，双方劳动合同约定了保密义务。张某某在履职期间设立 W 公司并担任法定代表人，后又将股权转让给其岳母朱某某并由朱某某担任法定代表人。2015 年 12 月底，张某某曾数次赴 S 公司的客户 J 公司等处出差，并参加有关展会。2016 年 4 月，W 公司向 J 公司销售了一批化学品，销售合同的主要内容与 S 公司和 J 公司间销售合同的内容基本一致。S 公司认为，张某某、W 公司侵害其经营秘密，故起诉请求判令张某某、W 公司停止侵权，赔偿 S 公司经济损失 78,200 元及合理开支 4,000 元。案件审理中，张某某、W 公司提交一份由 J 公司出具的情况说明，主要内容为：公司经由业内朋友介绍，知悉 W 公司也在经营 J 公司需求的原料，故由 J 公司采购部与其联系了解相关供货状况，之后自愿与其开展业务。J 公司负责人经法庭传唤未出庭就该证明材料出庭作证。

一审法院认为，S 公司主张的客户名单构成商业秘密，张某某、W 公司的行为构成侵害商业秘密。尽管 J 公司出具了情况说明，但并未证明 J 公司之前是基于对张某某的个人信赖才与 S 公司进行市场交易，且 J 公司与本案处理结果存在一定的利害关系，在无其他证据予以佐证的情况下，不能仅凭该情况说明即认定 W 公司对涉案客户信息具有合法来源。遂判决张某某、W 公司停止侵权，共同赔偿 S 公司经济损失 5 万元及合理开支 4,000 元。张某某、W 公司不服，提起上诉。

上海知识产权法院经审理认为，J 公司虽然出具了主动交易的说

明，但却无法明确该说明中“经由业内朋友介绍”中的“业内朋友”为何人，且其负责人未到庭作证，在没有其他证据佐证的情况下，仅凭该说明并不足以证明张某某、W公司的主张，遂判决驳回上诉，维持原判。

**解读：**本案涉及的主要法律问题是，在侵害客户信息类商业秘密案件中，对被告提出的主动交易抗辩的审查判断，以及当被告的主动交易抗辩不成立时，原告是否需要证明被告存在引诱客户的行为。本案判决明确了在对被告提出的主动交易抗辩的审查判断时，应当综合考量各方当事人提供的证据，并基于高度可能性的证明标准进行认定，而不应要求原告举证证明被告对客户实施了引诱行为。

## 16. 个人信赖抗辩的审查与认定

**来源：**原告R公司与被告L公司等侵害经营秘密纠纷案

**案情简介：**R公司自2015年开始先后与在本案中主张的6个客户发生交易，沟通及交易的电子邮件、买卖合同、报关单等载有客户名称、产品规格型号、价格、联系人、联系地址、电子邮箱等内容，并通过某外贸管理云平台登记总结了以上客户信息，进入该平台需输入账号及密码，在涉案档案信息的右上角标注有“TOP SECRET”标识。R公司还在新员工入职基本信息登记表及日常例会中要求员工承担保密义务。吴某某于2014年12月入职R公司，在外销部任职，2019年6月提出辞职后于次月解除劳动关系。L公司成立于2019年3月，吴某某之妻黄某某担任法定代表人。报关单显示，2019年6月至2020年11月期间，R公司主张的6家客户中，有5家客户均与L公司有过出口相同产品的交易，总计金额达1,500余万美元。R公司认为，三被告的行为侵害了其涉案商业秘密，起诉请求判令三被告停止侵权、连带赔偿经济损失1,361余万元及合理开支56万元。三被告共同辩称，R公司主张的客户信息不构成商业秘密；客户系基于对吴某某的信赖而自愿、主动与L公司交易；R公司主张的经济损失缺乏依据。

一审法院经审理认为，除未与L公司发生交易的客户外，其余5家客户的相关深度信息构成受法律保护的商业秘密。吴某某在R公司

处任职期间掌握了涉案商业秘密，其配偶黄某某投资设立与R公司经营范围相似的L公司，并在成立后较短时间内分别与涉案客户签订了大额合同，有违一般企业投入宣传、寻找客户、联系客户、接洽商谈等运营常规，L公司亦未提交有效证据证明其如何与客户建立起交易关系，故法院认定三被告系采取不正当手段披露和使用了R公司商业秘密，构成侵权。三被告辩称客户系自愿、主动与其交易，但并未提交证据，遂判令三被告停止侵权，连带赔偿R公司经济损失450万元及合理开支25万元。三被告不服，提起上诉。

上海知识产权法院经审理认为，关于涉案5家客户的开发过程，被告方在二审中先是辩称客户系基于对吴某某的个人信赖而与L公司交易，后又称涉案客户系黄某某自行开发，但未提交任何证据予以证明。本案所涉行业系对个人技能依赖度并不高的外贸行业，在该些客户与R公司的交易中，并无证据显示涉案客户系基于对吴某某个人的信赖而与R公司进行交易，相反，是R公司将其已获得的涉案客户交由吴某某维系。三被告为证明客户系基于对吴某某的个人信赖而与L公司交易，提交了2份证人证言，在证人未出庭作证，亦无其他证据予以佐证的情形下，法院对该证据难以采纳。且从证人证言中并不足以得出涉案客户系基于对吴某某个人的信赖而与R公司进行交易，并在吴某某离职后自愿选择与L公司进行交易，故三被告的个人信赖抗辩不成立，遂判决驳回上诉，维持原判。

**解读：**个人信赖抗辩一般适用于较为强调个人专业技能的行业领域，如律师、医生等。对于普通销售等不十分强调个人专业技能的领域，由于客户亦可能因销售人员个人的人格魅力、销售技巧、服务态度等而对其产生信赖，故亦可成立个人信赖抗辩，但应根据《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》第二条第二款的规定对证据进行严格审查。客户出具的书面说明属于证人证言，若证人未能出庭作证，也无其他证据予以佐证，则仅凭客户出具的书面证言不能认定个人信赖抗辩成立。若证据显示员工系利用权利人所提供的物质条件、交易平台才获得特定客户信息或者特定交易机会的，一般也不能成立个人信赖抗辩。

## 5. 行政保护

### 5.1 【查处部门与管辖】

#### 5.1.1 【查处部门】

市场监管部门为侵犯商业秘密行为的查处部门。市市场监管部门负责指导、协调本市侵犯商业秘密行为的预防和查处工作，查处本市重大、跨区等侵犯商业秘密行为。区市场监管部门负责本行政区域内侵犯商业秘密行为的预防和查处工作。

#### 5.1.2 【管辖】

侵犯商业秘密行为由违法行为发生地的县级以上市场监管部门管辖。违法行为发生地包括违法行为着手地、实施地、经过地、结果地。

### 5.2 【立案】

市场监管部门可依据监督检查职权或者通过投诉、举报、其他部门移送、上级交办等途径发现涉嫌侵犯商业秘密的违法行为线索。实践中较常见的途径是举报。

#### 5.2.1 【举报渠道】

权利人可通过以下渠道向市场监管部门举报：

a) 实名注册并登录全国 1235 平台（网址：[www.12315.cn](http://www.12315.cn)）进行举报。

b) 拨打上海市场监管部门投诉举报热线 021-12315 或市民热线 021-12345 进行举报。

c) 向辖区内市场监管部门进行举报。

### 5.2.2【举报材料】

权利人请求市场监管部门查处涉嫌侵犯商业秘密行为的，应提供商业秘密的具体内容、已采取的保密措施以及被侵权事实等初步材料。权利人合理表明商业秘密被侵犯，可提供以下证据之一：

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

b) 有证据表明商业秘密已经被涉嫌侵权人披露、使用或有被披露、使用的风险；

c) 有其他证据表明商业秘密被涉嫌侵权人侵犯。

### 5.2.3【核查期限】

市场监管部门自发现线索或收到材料之日起十五个工作日予以核查，并决定是否立案。特殊情况下可延长十五个工作日。检验、检疫、鉴定以及权利人辨认或者鉴别等所需时间，不计入前述期限。

权利人举报后如对主张的涉密信息进行相关鉴定的，鉴定所需时间不计入核查期限。

### 5.2.4【立案条件】

经核查，符合下列条件的违法线索，应立案：

a) 有明确的违法嫌疑人；

b) 有证据初步证明存在侵犯商业秘密行为；

c) 属于本部门管辖；

d) 在给予行政处罚的法定期限内。

注：《中华人民共和国行政处罚法》第三十六条规定，违法行为在二年内未被发现的，不再给予行政处罚。

### **5.3【调查】**

市场监管部门调查涉嫌侵犯商业秘密行为时，可采取现场检查、询问、查询和复制资料、查封或扣押财物、查询经营者银行账户等措施。

#### **5.3.1【现场检查】**

市场监管部门执法人员进入涉嫌侵犯商业秘密的经营者经营场所进行检查，并制作现场笔录，载明时间、地点、事件等内容。

#### **5.3.2【查封和扣押】**

经权利人申请并提供初步证明，市场监管部门可将在调查过程中发现的与涉嫌侵犯商业秘密行为有关的场所、设施或财物进行查封或扣押。对涉案的合同、票据、账簿、凭证等资料，执法人员采取信息化手段或者通过影印、复印等方式能够及时有效固定证据的，不予实施查封、扣押措施。

涉嫌侵犯商业秘密行为涉及计算机存储信息的，可能需要查封、扣押相关计算机服务器、主机、硬盘等存储设备。查封、扣押后及时通过复制、镜像、摄像、截屏、数据恢复等方式固定证据。

查封、扣押应当符合《中华人民共和国行政强制法》的规定。

#### **5.3.3【委托鉴定】**

权利人、涉嫌侵权人可以委托有法定资质的鉴定机构对权利人的

信息是否为公众所知悉、涉嫌侵权人所使用的信息与权利人的信息是否实质相同等专门性事项进行鉴定。权利人、涉嫌侵权人可就上述鉴定结论向市场监管部门提出意见并说明理由，由市场监管部门进行审查并决定是否采纳。

#### **5.4 【行政处罚】**

市场监管部门对确有依法应给予行政处罚的侵犯商业秘密行为，根据情节轻重及具体情况，做出行政处罚决定。

##### **5.4.1 【行为类型】**

侵犯商业秘密行为类型主要有违法获取、违法披露、违法使用、合法获取违法使用、第三人侵权、教唆帮助类侵权等。

不得实施下列侵犯商业秘密的行为：

a) 经营者以盗窃、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；

b) 经营者披露、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；

c) 经营者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；

d) 经营者教唆、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；

e) 经营者以外的其他自然人、法人和非法人组织实施前款所列违

法行为的，视为侵犯商业秘密；

f) 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a)项所列违法行为，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。

#### **5.4.2【违法行为认定】**

权利人能证明涉嫌侵权人所使用的信息与自己主张的商业秘密实质上相同，同时能证明涉嫌侵权人有获取其商业秘密的条件，而涉嫌侵权人不能提供或者拒不提供其所使用的信息是合法获得或者使用的证据的，市场监管部门可以根据有关证据，认定涉嫌侵权人存在侵权行为。

#### **5.4.3【行政责任】**

市场监管部门认定当事人的行为构成侵犯商业秘密的，应当责令停止违法行为，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。

##### **5.4.3.1【责令停止违法行为】**

视当事人侵权行为的具体情形，市场监管部门可责令当事人返还或销毁载有商业秘密的图纸、软件或其他有关载体，不得继续披露、使用或允许他人使用商业秘密。

当事人利用权利人的商业秘密生产的产品，尚未销售的，应监督当事人销毁，但是权利人同意收购或同意当事人继续销售的除外。

##### **5.4.3.2【没收违法所得】**

国家市场监督管理总局《商业秘密保护规定（征求意见稿）》（2020

年9月4日公告)第三十四条规定,侵犯商业秘密的违法所得是侵权人违法生产、销售商品或提供服务所获得的全部收入扣除侵权人直接用于经营活动的适当的合理支出。该规定与现行有效的《工商行政管理机关行政处罚案件违法所得认定办法》中认定违法所得的基本原则一致。

当事人没有违法所得或违法所得无法准确认定的,不做没收违法所得的处罚。

#### **5.4.3.3【罚款】**

对侵犯商业秘密行为应处以十万元以上一百万元以下的罚款;情节严重的,处以五十万元以上五百万元以下的罚款。目前尚无对“情节严重”的法律规定或有权解释,执法实践中一般适用十万元以上一百万元以下的罚款幅度。

#### **5.4.3.4【列入严重违法失信名单】**

根据《市场监督管理严重违法失信名单管理办法》规定,对侵犯商业秘密这种严重破坏公平竞争秩序的不正当竞争行为,市场监管部门按照从重处罚原则处以罚款的,应将当事人列入严重违法失信名单,通过国家企业信用信息公示系统公示,并实施相应管理措施。

市场监管部门收到法院的生效法律文书,要求对相关经营者、人员实施严重违法失信名单管理的,参照该办法执行。

#### **5.4.3.5【移送追究刑事责任】**

市场监管部门在对当事人做出行政处罚后,认为当事人可能构成犯罪的,应移送公安机关追究刑事责任。经公安机关侦查、检察院提

起公诉，法院判决当事人犯侵犯商业秘密罪并处罚金的，市场监管部门已经给予当事人罚款的，应折抵相应罚金。

## **5.5 【调解与和解】**

### **5.5.1 【调解】**

权利人因损害赔偿问题向市场监管部门提出调解要求的，市场监管部门可以进行调解。

### **5.5.2 【和解】**

在侵犯商业秘密行政案件查办过程中，权利人和当事人在双方自愿的基础上可以自行和解。和解不影响案件是否构成侵犯商业秘密的定性，但可作为处罚裁量的因素加以考虑。

## 【相关案例】

### 1. 主张保护的商业秘密是专利技术是否应当立案？

**来源：**王某某、上海 YG 公司诉上海市某区市场监管局不履行法定职责案（2014）虹行初字第 217 号

**案情简介：**2014 年 8 月 11 日，某区市场监管局收到上海 YG 公司提交的《侵犯商业秘密处理请求书》，要求调查上海 HS 车窗厂、厦门 JL 旅行车有限公司上海分公司侵犯王某某技术秘密的行为。经初步核查，王某某主张的技术秘密系其于 1996 年申请的“铝合金防盗玻璃窗”专利技术（《实用新型专利证书》第 28\*\*49 号）。某区市场监管局认定王某某持有的专利技术不属于商业秘密，被举报人不存在侵犯商业秘密的违法行为，遂于 2014 年 8 月 21 日作出不予立案决定。王某某、上海 YG 公司不服，向法院起诉。法院经审理认为：被告作为行政机关，对于侵犯商业秘密的投诉、举报，具有受理并作出行政处理的法定职权，其作出不予立案决定并无不当，驳回原告的诉讼请求。

**解读：**任何一件侵犯商业秘密案件成立，首先是确定主张商业秘密保护的信息是否属于商业秘密。如果商业秘密不存在，那么无论寻求何种途径，都得不到法律的救济。

### 2. 现场检查需要取得哪些资料？

**来源：**某低温设备有限公司侵犯商业秘密案成工商处〔2018〕276 号

**案情简介：**2018 年 7 月 11 日，成都市某区市场监管局接举报称，四川某低温设备有限公司（以下称当事人）通过不正当手段获取了四川 SJ 低温设备制造股份有限公司（以下称权利人）的商业秘密（技术信息），在某地从事液氮冰淇淋机和液氮罐的生产。

经调查，当事人系由王某与陈某共同投资。在此之前，王某原为权利人的生产部经理，陈某原为权利人的营销人员。二人在职时与权

利人均签有《劳动合同》《员工保密协议》和《企业商业秘密竞业保密协议》。这些协议将涉密的技术信息，包括技术方案、配方、工艺流程、图纸和技术文档确定为权利人的商业秘密。员工对此负有保密义务，且自离职之日起三年内不得从事相同职业的工作，为此权利人每月支付保密费和竞业禁止补偿费。

在当事人生产现场查获由权利人署名的 72 份图纸，经四川某司法鉴定所鉴定，结论是该 72 份用于生产液氮罐和液氮冰淇淋机的图纸属于权利人所有的技术秘密。对此鉴定意见当事人无异议，承认这些图纸是其离职前带走的。案发时，当事人处于试生产阶段，没有成品上市，尚未给权利人造成直接经济损失。

**解读：**本案得以顺利办结的原因之一在于有效组织实施了现场检查，取得了关键证据。该局接到举报后，并没有立即采取行动，而是通过两天的观察，找到当事人的实际生产地址（当事人既不在其登记注册地也不在权利人举报的地址生产），避免一击不中、打草惊蛇，减少关键技术秘密被当事人销毁的风险。现场检查时重点明确，注意收集各类技术信息的载体，取得了最关键的由权利人署名的 72 份图纸。最后，办案人员制作现场笔录，当事人对整个检查过程予以确认。

### 3. 仅非法获取但未使用商业秘密是否构成侵犯商业秘密行为？

**来源：**郑某某侵犯商业秘密案玉市监处罚〔2021〕2021828 号

**案情简介：**当事人郑某某于 2020 年 4 月入职 XF 公司，从事技术员岗位工作，主要工作是样品的图纸绘制、更改等。当事人入职后虽未与 XF 公司签订专门的保密合同，但在劳动合同的补充协议中规定对公司的机密性文件要绝对保密。XF 公司为保护图纸不被窃取，在公司的计算机内安装了数据防泄密系统，该系统有文件自动加密功能，计算机内的所有文件包括图纸必须依托该系统打开，否则即使外泄文件也无法打开变成乱码。当事人利用工作之便，违反公司保密规定将打印好的图纸用自己的智能手机拍摄保存，另将生产车间用过的 15 张图纸偷拿回家，后又用虚拟打印机将图纸另存为 PDF 格式的方式绕过公司的数据防泄密系统，将一张排气阀图纸保存到自己的存储器中。当

事人秘密窃取公司图纸后，全部保存到自己的手机中，经整理图纸多达 523 张。据当事人陈述其秘密窃取图纸是出于个人学习的目的，未对外出售或泄露。

办案机关依法对当事人侵犯商业秘密的行为作出行政处罚。

**解读：**员工离职前违规获取公司大量敏感信息（含商业秘密）是目前多发常见的现象。此种行为离追究刑事责任尚有距离，贸然提起民事诉讼又成本较高，许多企业往往以内部处理为主。对此类单纯获取但没有证据证明有泄露或使用商业秘密的行为，可尝试向市场监管部门举报以获得行政保护。

#### 4. 合法获取、非法使用商业秘密是否构成侵犯商业秘密行为？

**来源：**南京某电子设备有限公司侵犯商业秘密案雨市监处罚（2021）10290 号

**案情简介：**当事人南京某电子设备有限公司在加工承揽权利人定制的 XF05C 机箱产品时，获得了该产品的设计图纸。在完成与权利人之间的合同后，当事人又承揽了南京另一家公司的 XF05C-JY 骨架产品定制业务。经鉴定，权利人的 XF05C 机箱存在不为公众所知悉的技术秘点，并采取了必要的保密措施。而当事人为另一客户制作的 XF05C-JY 骨架上使用了与权利人相同的技术秘密。

办案机关依法对当事人侵犯商业秘密的行为作出行政处罚。

**解读：**本案是加工承揽领域常见的违反保密义务侵犯商业秘密典型案件。当事人依据合同获取了权利人的技术秘密后违反保密义务，使用该技术秘密生产产品牟利，构成侵犯商业秘密行为。

#### 5. 当事人拒不配合的情况下，如何认定侵犯商业秘密行为成立？

**来源：**上海 FH 智能有限公司侵犯商业秘密案沪市监松处〔2020〕272020000100 号

**案情简介：**2012 年 11 月至 2017 年 2 月期间，李某在权利人公司担任“机械工程师”一职，并签订了《保密协议》与《IT 安全管理制度》。李某任职期间参与了木封边机产品的设计研发工作。

2016年8月1日,当事人法定代表人孙某某与李某签订《协议书》,双方约定孙某某出资200万元,李某提供直线自动木封边机技术,合作开办公司。2016年11月10日,孙某某与宋某注册成立上海FH智能设备有限公司(当事人),李某任总经理,全面负责木封边机生产、销售业务。

据鉴定机构鉴定,权利人木封边机产品使用的“涂胶单元”等属于不为公众所知悉的技术信息。当事人生产的木封边机使用的相关技术与权利人的技术信息相同。

同时,在当事人处查获的移动存储盘中保存的24张技术图纸(3D模型)所载的技术信息与权利人木封边机的技术图纸(3D模型)所载的技术信息实质上相同。

办案机关依法对当事人侵犯商业秘密的行为作出行政处罚。

**解读:** 在本案查办过程中,当事人关闭公司、解散员工,以各种手段阻碍调查,并辩称相关产品技术系通过反向工程研发。办案机关先使用直接证据推翻当事人反向工程研发的辩解,后运用推定原则,认为李某某有接触权利人技术秘密的条件,且不能证明其掌握的与权利人技术秘密实质上相同的技术信息有合法来源,认定侵犯商业秘密行为成立。

## 6. 行政保护的作用是不是简单地一罚了之?

**来源:** 敖某等三人侵犯商业秘密案(湖)市监经处字第〔2018〕1、2、3号

**案情简介:** 敖某作为湖州市某电子科技公司的工艺装备部长和原料生产线项目执行人,与公司签订企业员工保密协议和项目保密协议。协议明确约定敖某在任职期内完成与公司业务相关的发明创造、技术秘密或其他商业秘密信息均为职务成果,公司享有知识产权。敖某在该公司研发出被列为企业核心商业秘密的原料除杂加工工艺后,为了牟取私利,与该公司的原料供应商掌某合伙在江苏省连云港市建厂,并将其掌握的生产工艺秘密传授给工厂管理人员孙某,利用该项工艺生产原料。截至案发,该厂共生产成品原料200吨,尚未对外销售。

办案机关认为，敖某违反保密义务，将其掌握的被所在公司列为商业秘密的原料生产工艺泄露给掌某和孙某，孙某利用该工艺生产原料。敖某、掌某和孙某均构成侵犯商业秘密行为。

**解读：**本案的一大亮点是办案机关在案件查办过程中积极斡旋，安排相关人员会见恳谈，主动调和权利人与当事人之间的矛盾，最终促成多方达成谅解协议。敖某、掌某和孙某三人承诺严格保守已获取的商业秘密，否则将承担法律责任并赔偿300万元。权利人将三人合办的工厂作价收购，继续利用该工艺生产原料。达成和解后，权利人商业秘密被继续泄露的风险极大降低。

## 7. 离职高管窃取权利人源代码后成立新公司开发软件构成侵犯商业秘密

**来源：**重庆趣房科技有限公司侵犯商业秘密案（市场监管总局公布的侵犯商业秘密典型案例）

**案情简介：**重庆某科技有限公司（权利人）前高管刘某某离职前指使下属员工获得公司“全房通”系统软件源代码，离职后收购重庆趣房科技有限公司（当事人）并招募权利人软件开发人员，在明知该源代码属于权利人技术秘密的情况下，违反保密协议，允许他人（当事人）使用上述技术秘密用于同类型软件“趣管房”系统的开发。权利人向市场监管部门举报。执法机关认为，当事人的行为构成侵犯商业秘密，依法责令当事人停止违法行为，处罚款50万元。

**解读：**自行开发的计算机软件其核心部分源代码，是企业的重要技术秘密，具有极大商业价值。企业应对软件源代码采取必要的保护措施。尽管不能完全杜绝“内鬼窃密”，但案发后可以寻求行政保护，

对侵权人的违法行为予以行政处罚，并及时制止侵权行为降低损失。

## 6. 刑事保护

### 6.1 【侵犯商业秘密罪】

《刑法》（2020年修正）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：

a) 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；

b) 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；

c) 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。

备注：采取非法复制、未经授权或者超越授权使用计算机信息系统等方式窃取商业秘密的，应当认定为“盗窃”。

#### 6.1.1 【犯罪构成】

6.1.1.1 侵犯商业秘密罪的犯罪主体为一般主体，包括自然人与单位。凡年满 16 周岁的自然人及非完全丧失辨认与控制能力的精神病人，均可构成本罪。

6.1.1.2 本罪要求行为人在主观方面为故意，即行为人明知自己的行为侵犯了他人的商业秘密，过失行为不构成本罪。

**6.1.1.3 侵犯商业秘密罪的犯罪对象为商业秘密，刑法所保护的商业秘密与《反不正当竞争法》界定的商业秘密相同。商业秘密是否成立是认定是否构成侵犯商业秘密罪的前提条件。**

### **6.1.2【犯罪行为】**

刑法中构成侵犯商业秘密罪的行为方式与《反不正当竞争法》规定的行为方式不尽相同。主要包括非法获取、非法披露、非法使用、非法允许他人使用四种类型。

### **6.1.3【刑事追诉标准】**

《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）》（2020年9月14日起施行，以下的简称《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”（情节严重）：

（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”（情节特别严重）。

备注：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。

2023年1月18日,《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(征求意见稿)》向社会公开征求意见,其中对属于“情节严重”的情形增加了两种,一是一年内以不正当手段获取商业秘密三次以上的;二是二年内因侵犯商业秘密行为受过行政处罚二次以上,又实施侵犯商业秘密行为的。

#### 6.1.4【权利人损失数额认定】

商业秘密权利人的损失数额,应按照下列方式认定:

a) 以不正当手段获取权利人的商业秘密,尚未披露、使用或者允许他人使用的,损失数额可根据该项商业秘密的合理使用许可费确定;

b) 以不正当手段获取权利人的商业秘密后,披露、使用或者允许他人使用的,损失数额可根据权利人因被侵权造成销售利润的损失确定,但该损失数额低于商业秘密合理许可使用费的,根据合理使用许可费确定;

c) 违反约定、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,损失数额可根据权利人因被侵权造成销售利润的损失确定;

d) 明知商业秘密是不正当手段获取或者是违反约定、权利人有关保守商业秘密的要求披露、使用、允许使用,仍获取、使用或者披露的,损失数额可根据权利人因被侵权造成销售利润的损失确定;

e) 因侵犯商业秘密行为导致商业秘密已为公众所知悉或者灭失

的，损失数额可根据该项商业秘密的商业价值确定。商业秘密的商业价值，可以根据该项商业秘密的研究开发成本、实施该项商业秘密的收益综合确定。

权利人因侵权造成销售利润的损失，可根据权利人因被侵权造成销售量的减少的总数乘以权利人每件产品的合理利润确定；销售数量减少的总数无法确定的，可根据侵权产品销售量乘以权利人每件产品的合理利润确定；权利人因被侵权造成销售量减少的总数和每件产品的合理利润均无法确定的，可根据侵权产品销售量乘以每件侵权产品的合理利润确定。商业秘密系用于服务等其他经营活动的，损失数额可根据权利人因被侵权而减少的合理利润确定。

商业秘密的权利人为减轻对商业运营、商业计划的损失或者重新恢复计算机信息系统安全、其他系统安全而支出的补救费用，应当计入给商业秘密的权利人造成的损失。

#### **6.1.5 【侵权人违法所得数额认定】**

侵权人的违法所得数额，应按照下列方式认定：

a) 因披露或者允许他人使用商业秘密而获得的财物或者其他财产性利益的价值；

b) 因使用商业秘密所获得的利润，该利润可以根据侵权产品销售量乘以每件侵权产品的合理利润确定。

#### **6.1.6 【共同犯罪】**

如果明知他人实施侵犯商业秘密的犯罪行为，而为其提供贷款、资金、账号、发票、证明、许可证件，或提供生产经营场所或运输、

储存、代理进出口等便利条件、帮助的，以侵犯商业秘密罪的共犯论处。

## **6.2 【为境外窃取、刺探、收买、非法提供商业秘密罪】**

《刑法》（2020年修正）增设了第二百一十九条之一 9 为境外的机构、组织、人员窃取、刺探、收买、非法提供商业秘密的，处五年以下有期徒刑，并处或单处罚金；情节严重的，处五年以上有期徒刑，并处罚金。

需要注意的是，本罪没有情节后果要求，行为人一经实施，即构成本罪。情节的严重程度，仅是加重处罚的考量因素，不属于本罪的犯罪构成要件。

## **6.3 【刑事案件管辖】**

### **6.3.1 【地域管辖】**

侵犯知识产权犯罪案件由犯罪地公安机关立案侦查。必要时，可以由犯罪嫌疑人居住地公安机关立案侦查。

侵犯商业秘密犯罪案件的犯罪地，包括侵权产品制造地、储存地、运输地、销售地，销售侵权产品的网站服务器所在地、网络接入地、网站建立者或管理者所在地，权利人受到实际侵害的犯罪结果发生地。

### **6.3.2 【级别管辖】**

侵犯商业秘密罪的最高刑期为十年有期徒刑。根据《上海市高级人民法院 上海市人民检察院 上海市公安局关于办理商业秘密刑事案件若干问题的通知》，2024年1月1日起对侵犯技术秘密的刑事案件进行提级管辖。具体而言，关于技术秘密的刑事案件原则上由市公安局立案侦查，市人民检察院第三分院进行审查逮捕和审查起诉。但市

公安局也可以将案件线索下发区公安分局立案侦查，由所在地基层人民检察院进行审查逮捕，并自作出决定之日起三日内上报市人民检察院第三分院备案；审查起诉的，自三日内报请市人民检察院第三分院审查起诉。市人民检察院第三分院也可指定基层人民检察院管辖。市第三中级人民法院管辖由市人民检察院第三分院提起公诉的第一审商业秘密刑事案件。

关于侵犯经营秘密的刑事案件，原则上由区公安分局、基层检察院、基层法院进行受理，但不宜受理的除外。

#### **6.4 【报案】**

对涉嫌构成侵犯商业秘密犯罪的行为，任何单位和个人有权利也有义务向公安机关报案。

商业秘密权利人发现有自然人或者单位侵犯其商业秘密且情节严重的，可以依照管辖规定向公安机关报案。

##### **6.4.1 【报案材料】**

报案人在向公安机关报案时，需要提供必要的证据材料，证明有犯罪事实的存在。根据侵犯商业秘密罪的构成特点，报案材料应尽量涵盖以下五方面：

a) 商业秘密客观存在的证明。包括商业秘密的类型、名称及内容，涉案技术信息或经营信息不为公众所知悉的鉴定意见，对上述信息采取相关保密措施的规章制度、保密协议等。

b) 商业秘密权属关系的证明。包括权利人的名称、住所及联系方式，商业秘密的研发、创制过程证明材料，如项目立项书、研发证明、制作人证言等。

c) 侵权事实存在的证明。包括证明犯罪嫌疑人有条件获取权利人

商业秘密的材料、证明犯罪嫌疑人披露或使用权利人商业秘密的材料、证明犯罪嫌疑人所侵犯的商业秘密与权利人的商业秘密实质相同的鉴定、证明权利人因侵权行为遭受重大经济损失的评估材料等。

d) 犯罪嫌疑人的相关情况。报案人在能够确定嫌疑人的情况下，应尽量向公安机关提供犯罪嫌疑人的姓名、所在单位、住址等信息。

e) 其他与证明案件事实有关的材料。如刑事立案前进行民事诉讼的相关判决、材料等。

报案人应尽可能提供翔实、充分的报案材料，帮助公安机关尽快锁定犯罪嫌疑人、查明案件真相、缩短侦办周期，从而减少权利人因侵权行为所遭受的损失。

#### **6.4.2 【鉴定意见】**

鉴定意见是非常重要的定案证据。实践中主要涉及三类鉴定：

a) 商业秘密存在的鉴定。此类鉴定帮助公安机关确定商业秘密是什么以及秘密点如何体现等基础问题。

b) 商业秘密实质相同（同一性）的鉴定。此类鉴定是确定犯罪行为存在的重要依据。只有犯罪嫌疑人侵犯的商业秘密与权利人请求保护的商业秘密实质相同，才可能构成侵犯商业秘密罪。

c) 权利人损失价值评估。此类评估决定了刑事案件是否构成犯罪及追诉量刑基准。

提示：在鉴定过程中秘点选取要合理。在梳理秘点时，首先要考虑侵权人有可能侵害了哪些技术信息；其次要考虑在后期比对时，对于动态的技术信息，如一些生产流程中的工艺参数，是否可能从侵权

人处获得；最后要考虑秘点覆盖的范围大小、数量多少。如果秘点太多则鉴定费用高，太少又可能达不到维权目的。

## **6.5【立案】**

公安机关接到报案后，应对报案材料进行审查，决定是否立案。

### **6.5.1【刑事立案条件】**

符合下列条件的，应当立案侦查：

a) 有犯罪事实，即已有证据证明犯罪事实已客观存在，而非毫无根据的主观臆测。

b) 需要追究刑事责任，即犯罪嫌疑人的犯罪行为应受到刑事处罚。

c) 有管辖权，公安机关只能管辖具有管辖权的案件，对于不属于自己管辖的案件应移送有管辖权的公安机关。

## **6.6【移送追究行政责任】**

公安机关立案后，经侦查认为犯罪嫌疑人的行为未达到刑事追诉标准的，应当移送同级市场监管部门追究行政责任。

## **6.7【取保候审】**

立案后公安机关为防止犯罪嫌疑人逃避侦查，可采取取保候审的强制措施，即责令其提出保证人或交纳保证金，并出具保证书，保证随传随到，对其不予羁押。取保候审通常对犯罪较轻，不需要逮捕，但需要对其行动自由作一定限制的犯罪嫌疑人采用。

## **6.8【逮捕】**

对有证据证明有犯罪事实，可能判处有期徒刑以上刑罚的犯罪嫌

疑人，公安机关采取取保候审尚不足以防止发生下列社会危险性的，应予以逮捕：

- a) 可能实施新的犯罪的；
- b) 有危害国家安全、公共安全或社会秩序的现实危险的；
- c) 可能毁灭、伪造证据，干扰证人作证或串供的；
- d) 可能对被害人、举报人、控告人实施打击报复的；
- e) 企图自杀或逃跑的。

### **6.9 【审查起诉】**

检察院应对公安机关侦查终结移送起诉的案件进行审查，核实犯罪事实和证据、犯罪性质和罪名是否适当，并依法决定是否对犯罪嫌疑人提起公诉、不起诉或撤销案件。

商业秘密权利人应积极配合检察院在审查起诉期间的补充侦查、证据收集等工作，做好出庭的准备工作，保证刑事诉讼程序的顺利进行。

### **6.10 【审理裁判】**

法院作为审判机关根据检察院移送起诉的案件事实、证据材料等对案件进行全面审查，并可以补充调取庭审需要的证据材料。经开庭审理后，法院就商业秘密刑事案件的被告是否有罪、构成何罪及判处何刑罚等实体问题作出依法判决。

商业秘密权利人应积极配合法院的刑事审判工作，涉及商业秘密的案件，当事人申请不公开审理的，可以不公开审理。

### **6.11 【刑民交织】**

商业秘密案件既涉及民事法律中的侵权问题，又涉及刑法规定的侵犯商业秘密犯罪，是典型的“刑民交织”案件。我们认为可采取“刑民并行”（刑事附带民事诉讼）为原则，以“先刑后民”或“先民后刑”为例外的思路。

#### **6.11.1【先民后刑】**

对于侵犯经营信息类商业秘密案件，权利是否存在、权利归属以及商业价值如何需要原被告双方充分举证，“先民后刑”可能更有利于查明事实。

#### **6.11.2【先刑后民】**

对于侵犯技术类商业秘密案件，较易达到刑事追诉标准又需要技术侦查手段的介入，“先刑后民”可能更利于权利保障。

#### **6.11.3【民刑办案融合】**

浦东新区检察院已设立知识产权刑事、民事、行政、公益诉讼检察职能“四合一”集中履行的派出检察院（张江检察院），浦东新区法院知识产权庭已实行知识产权刑事、民事、行政“三合一”的审判机制，为本区商业秘密案件刑民交织问题的解决提供了现实途径。

## 【相关案例】

### 1. 游戏代码是否属于商业秘密？

来源：陆某甲、陆某乙侵犯商业秘密案（2020）沪 0110 刑初 869 号

案情简介：2018 年 9 月起，被告陆某甲成立上海 A 网络科技有限公司（以下简称 A 公司），后违反与原工作单位上海 B 信息科技有限公司（以下简称 B 公司）签订的保密协议，使用 B 公司研发的《龙珠传奇》游戏的前端代码，开发《龙珠 Z 战士》游戏并上线运营。期间，被告陆某乙明知上述前端代码为原工作单位 B 公司开发且签订过保密协议，仍帮助陆某甲在 A 公司的上述游戏中予以使用。经统计，A 公司通过《龙珠 Z 战士》在各个平台的发行，违法所得近 150 万元。2020 年 11 月，法院判处被告陆某甲、陆某乙构成侵犯商业秘密罪。

解读：游戏软件涉及重要玩法、游戏框架等影响游戏运行的关键程序代码可以构成商业秘密。这些关键程序代码关乎向玩家正常呈现游戏的效果，其商业价值毋庸置疑，因此 A 公司将这些代码存储在源代码版本控制系统中，并采用不同开发人员、不同账号密码管理的保密措施。而行为人违反约定，利用这些核心代码开发了新的手机游戏，并对外销售牟利，属于侵犯商业秘密的行为。在商业秘密刑事案件中要严格界定商业秘密范围，如侵权软件与权利人软件代码构成实质性相同，且系核心、不可分割的秘点，应认定侵权软件侵犯了权利人的完整商业秘密。

检察机关在办理本案过程中，发现权利单位有三处管理疏漏导致行为人轻易获得代码：（1）保密教育不到位。权利单位虽与行为人签订保密协议，但并不知晓商业秘密的范围及保密措施情况。（2）保密措施不到位。权利单位除与员工签订保密协议、在服务器上为项目组成员设置账号和密码以及员工离职后回收计算机外，并未采取其他更有效的保护措施，且服务器只保存上传记录，无下载记录。（3）监督

管理不到位。行为人在公司期间可以自由下载相关代码，既无下载记录留存，也无下载介质限制，更无人员予以监管。

## 2. 侵犯客户名单等经营信息是否构成侵犯商业秘密罪？

**来源：**施某侵犯商业秘密案（2019）沪 0109 刑初 991 号

**案情简介：**2015 年 9 月，被告施某入职上海某管理咨询有限公司（原公司），并与该公司签订劳动合同及相关保密协议。后被告施某在公司担任项目经理期间，于 2017 年 10 月私自设立上海 SY 管理咨询有限公司，从事与原公司性质相同的业务，并违反保密约定，使用其所掌握的原公司的客户名单，与原公司的客户开展业务。经审计，SY 公司使用被告施某所掌握的原公司的客户名单开展经营活动，违法所得 100 余万元。

2020 年 1 月，法院判决被告施某犯侵犯商业秘密罪，判处有期徒刑一年，缓刑一年，并处罚金十万元。

**解读：**单纯的客户名称、地址、电话等简单经营信息，因缺乏需求类型、交易习惯、购买频率、经营规律、价格承受能力等深度信息，不符合商业秘密的认定标准，不属于商业秘密。但符合商业秘密特性的经营信息仍是商业秘密的重要组成部分。倘若权利人付出一定的商业努力，使经营信息具备不为公众所知悉的深度内容，能为权利人带来现实的或潜在的经济利益或竞争优势，应认定为商业秘密。本案中，法院认为被告施某违反约定及权利人有关保守商业秘密的要求，使用其所掌握的商业秘密，给商业秘密的权利人造成重大损失，其行为已构成侵犯商业秘密罪。

## 3. 因侵权造成的权利人销售利润损失难以计算时如何认定？

**来源：**万超公司、于某某、贾某某侵犯商业秘密案（2018）沪 0107 刑初 1289 号

**案情简介：**2012 年 4 月至 2014 年 2 月，被告于某某在权利人恩坦华公司担任高级产品工程师，曾接触恩坦华公司汽车天窗机械组、汽车天窗遮阳帘驱动系统等一系列技术信息。2014 年 3 月，于某某从

恩坦华公司离职，随即受被告贾某某经营的被告单位万超公司聘用，负责汽车全景天窗研发工作。于某某违反与恩坦华公司保密约定，将恩坦华公司技术信息披露并用于万超公司相关天窗产品的研发。万超公司法定代表人贾某某明知于某某可能存在非法披露他人技术秘密的情况，仍将相关数据资料用于万超公司汽车天窗产品的研发及生产销售。后贾某某、于某某又以共同发明人身份，对部分技术申请专利。经鉴定，万超公司的部分汽车天窗产品、相关专利及计算机内部分电子数据，与恩坦华公司技术信息实质相同。2015年9月至2018年6月期间，万超公司销售相关产品净利润达1200万余元。

2020年1月，法院认定各被告构成侵犯商业秘密罪，判处万超公司罚金四百万元；判处于某某有期徒刑五年，并处罚金五十万元；判处贾某某有期徒刑三年缓刑三年，并处罚金三十五万元。

**解读：**当权利人因侵权造成的销售利润损失难以计算时，可以参考侵权人的销售获利认定权利人损失数额。《解释三》规定以商业秘密的合理许可使用费及权利人因被侵权造成的销售利润损失计算损失数额，但基于商业秘密的类型不同、侵权行为多样、有关损失的证据难以收集等情况，需要结合个案具体分析，按照最合适的计算方式来确认权利人损失数额。从行为逻辑来看，侵权人的巨大获利通常使得权利人通过正常交易行为获得的收益减少，而侵犯商业秘密罪保护的法益是有关知识产权交易的市场经济秩序，其中必然包含权利人因商业秘密可获得的收益，因此损失的认定可以参考侵权人的获利数额。

#### 4. 公司创始人复制传输AI芯片核心代码构成侵犯商业秘密罪

**来源：**人工智能芯片核心代码下载传输案（浦东检察院商业秘密保护典型案例）

**案情简介：**A公司是一家专注于视觉人工智能芯片研发及销售的企业，主要研发视觉人工智能处理器NPU（嵌入式神经网络处理器）芯片，属前沿的芯片技术领域，曾凭借AI芯片研发入围中国AI芯片企业50强，

是国家认证的高新技术企业。其机房内存储了大量该公司芯片研发核心代码在内的大量保密数据，这些数据是A公司的核心竞争力和重要命脉。为防止核心技术代码泄露，A公司为其设置了多层级的保密管理及相应的服务器安全策略。2022年11月，工作人员查看机房时发现，机房内竟多出一台电脑。从2022年年中起，该服务器中存储的包含芯片研发核心代码在内的大量保密数据被复制传输至这台电脑并上传到云端，而频繁登陆服务器进行传输的账号指向一人——A公司创始人之一、首席运营官、公司股东郭某。A公司随即报案。通过技术性审查与专业鉴定，郭某窃取的技术信息具有非公知性，与A公司代码具有同一性。同时，发现郭某以核心人员身份出现在B科技公司宣传资料中，并参与对外融资，时间与其复制数据的时间高度重合。经评估，涉案技术信息的合理许可使用费为230余万元。2024年4月16日，浦东新区法院开庭审理并当庭判决郭某犯侵犯商业秘密罪，判处郭某有期徒刑二年，缓刑二年，并处罚金十万元。

**解读：**本案中，郭某作为公司创始人之一和高管，利用超级管理员权限窃取公司核心技术秘密，如果没有被及时发现，将对公司造成致命损害。这为公司保密制度的落实敲响了警钟，要严格实施物理隔离、控制网络访问及数据传输等技术措施，定期开展涉密检查。对于公司保密制度需要及时让全体员工知晓和签收，对于关键岗位人员包括高管，还应在权限管理的基础上进行行为监控。

## 5. 窃取权利人的源代码开发新产品并销售给权利人的客户构成侵

## 犯商业秘密罪

**来源：**徐某、杨某侵犯商业秘密案（深圳市宝安区人民法院发布的知识产权刑事犯罪典型案例）

**案情简介：**徐某、杨某曾分别任甲公司的产品部经理和研发部负责人，二人在任职期间均签订了《保密合同》。甲公司向二人按月发放基本工资10%的保密费。2015年3月，徐某离职后成立乙公司。2016年1月，杨某受邀从甲公司离职加入乙公司，离职时将甲公司的个人定位器源代码和MCU目标代码等保密资料秘密带出。乙公司利用这些保密信息开发了两种型号的车载定位器，销售给甲公司的客户。经鉴定，源代码资料中26个定位器源代码文件和甲公司某个人定位器主控芯片的源代码文件一致；乙公司使用的定位器MCU目标代码与甲公司的MCU目标代码一致；其中通用于车载和个人定位器的20个公共源代码文件在2018年11月28日之前（鉴定意见出具前）不为公众所知悉且具有实用性，系甲公司采取了保密措施的商业秘密。经审计，2016年5月至9月，乙公司销售给甲公司客户的两款产品金额共计3422687元。

法院认为，杨某明知自己掌握的技术信息属于其之前任职公司的商业秘密，仍违反保密义务，秘密窃取后出卖给徐某；徐某明知杨某出卖的技术信息属于其之前任职公司的商业秘密，仍出资购买。二人的犯意联络和主观故意明显，将窃取的商业秘密用于车载定位器产品上，相关产品投入市场销售，获取非法利益。法院以侵犯商业秘密罪判处徐某、杨某有期徒刑二年十个月，并处罚金五十万元。

**解读：**企业核心研发人员离职后，利用原公司构成商业秘密的源

代码在新公司开发同类软件，进而生产出两款产品非法牟利，并且销售给原公司的客户，抢占原公司的市场份额，行为隐蔽且性质恶劣。法院依法判处徐某、杨某有期徒刑并处罚金。

## 7. 商业秘密鉴定

商业秘密鉴定是商业秘密维权、司法执法活动中证明事实的重要手段。

### 7.1 【含义】

商业秘密鉴定是指鉴定机构运用科学技术或专门知识对涉案技术信息或经营信息的相关专业性技术问题进行鉴别和判断，并出具鉴定意见的活动。

### 7.2 【鉴定种类】

商业秘密维权和司法执法活动中常用的鉴定包括非公知性鉴定、同一性鉴定和商业秘密侵权损失鉴定等。

#### 7.2.1 【非公知性鉴定】

是对商业秘密权利人所主张的技术信息或经营信息是否属于“不为公众所知悉”的鉴定。

**7.2.1.1** “不为公众所知悉”是商业秘密构成的首要条件。不具有秘密性的信息，即使对企业具有商业价值也采取了保密措施，也不可能构成商业秘密。秘密性要求有关信息不为所属领域的相关人员普遍知悉和容易获得，一般是指特定信息在本行业内不是众所周知，而不是绝对无人知悉。只要存在“普遍知悉”或“容易获得”一种情况就不满足秘密性的要求。

**7.2.1.2** 非公知性的判定，实务中可从以下几个方面进行综合分析：

- a) 该信息在所属领域是否属于一般常识或行业惯例;
- b) 进入市场后相关公众是否可以通过观察产品直接获得;
- c) 是否无需付出一定的代价而容易获得。

**7.2.1.3** 技术信息的非公知性鉴定涉及的领域非常广泛，包括计算机软件、机械、化工、生物医药等各方面，技术性越强的商业信息对鉴定机构的专业要求越高，因此在选择鉴定机构时，要注重待鉴定密点的具体内容与鉴定机构、鉴定人员的专业领域是否匹配。

**7.2.1.3** 技术查新报告可作为鉴定参考资料。技术查新报告一般在专利审查中运用，是查新机构根据查新项目的查新点与所查数据库等范围内的文献信息进行比较分析，对查新点作出新颖性判别。虽然商业秘密的非公知性与专利的新颖性要求并不相同，但是在文献检索方法上可以相互借鉴。技术信息的非公知性鉴定报告中经常涉及对近似文献的检索，既可以由鉴定机构自行进行近似文献检索，也可以委托其他检索机构出具检索报告。

司法或行政机关通过比较检索报告与鉴定报告的分析过程和结论，可以增强对密点技术特征的全面认识，同时要注意审查检索报告中关键词的选取和数量与密点的技术特点是否匹配、查新日期是否在案发之前、查新数据库是否涵盖主要数据库及密点关联技术领域、涉外密点是否检索相关外文数据库等。

**7.2.1.4** 在进行非公知性鉴定时，除了利用文献数据库进行检索以外，还应当通过互联网检索类似技术、浏览相关行业期刊出版物、收集相关展会资料等方式进行排查，并将检索过程和结论在鉴定报告中予以

体现。

**7.2.1.5** 实践中可能存在产品技术秘密因使用或者销售公开的情况。

在刑事案件办理过程中，为进一步排除公开的可能性，检察机关可能需要组织侦查机关、鉴定人员实地进行设备拆卸勘测，确定通过一般测绘和观察无法准确获取密点信息。

### **7.2.2【同一性鉴定】**

同一性鉴定，是指通过对检材与样本所示的技术信息进行比较，从而认定二者是否相同或者实质相同。

#### **7.2.2.1【检验项目选择】**

分析检材和样本，根据检材和样本的内容选择以下一项或多项内容进行检验：

a) 结构间的比对样本所示的技术参数与检材所示的技术参数一一比较，对于存在相同或实质相同的技术参数需要进行说明。

b) 成份间的比对样本所示的配方成份或者其含量与检材所示的配方成份或者其含量一一比较，对于存在相同或实质相同的配方成份或者其含量需要进行说明。

c) 生产工艺、方法间的比对样本所示的生产工艺、方法与检材所示的生产工艺、方法一一比较（一般需要生产设备运行过程中进行检测），对于存在相同或实质相同的生产工艺、方法需要进行说明。

d) 软件间的比对。参照《软件相似性鉴定实施规范》（SF/Z JD0403001-2014）。

#### **7.2.2.2【比对结果】**

鉴定意见应分别列出检材与样本技术信息是否相同、实质相同、相似及不同，并对存在相同或者实质相同的部分进行说明。

### 7.2.2.3【知识产权鉴定机构】

非公知性鉴定和同一性鉴定都属于技术性鉴定。鉴定机构可通过人民法院诉讼资产网（<https://www.rmfysszc.gov.cn>）自主查询选择。

查询步骤如下：1. 登陆人民法院诉讼资产网； 2. 点击“司法技术”； 3. 点击左侧“专业机构”； 4. 在“专业类别”一栏勾选“知识产权”并点击确定； 5. 点击搜索。

上海市目前共有 11 家知识产权鉴定机构可供选择，其中浦东新区 3 家。（查询日期：2024 年 11 月 28 日）

### 7.2.3【商业秘密侵权损失鉴定】

被害人的损失金额以及被告的违法所得是侵犯商业秘密犯罪案件中重要的入罪标准，也是关系到被告定罪量刑的重要标准。对被害方而言，被害人要收集证据向公安机关报案，需要对损失的金额进行审计或评估，证实其损失金额达到该罪的入罪标准。在商业秘密侵权的民事诉讼中，法院也需要依据权利人的损失数额或者侵权人的违法所得数额来确定判决赔偿的数额。

商业秘密诉讼中损害赔偿额的认定，实际上就是将无形的商业秘密用具体的经济数值来替换，与知识产权资产评估之间存在较大的重合性。资产评估是确定商业秘密价值的重要手段。资产评估在商业秘密诉讼中的适用，既为立法所认可，也已在司法审判中有了一定的实践基础。

### 7.2.3.1 【资产评估】

评估需要由专门的资产评估机构进行评估。资产评估机构可通过人民法院诉讼资产网 (<https://www.rmfysszc.gov.cn>) 自主查询选择。

查询步骤如下:1. 登录人民法院诉讼资产网; 2. 点击“司法技术”; 3. 点击左侧“专业机构”; 4. 在“专业类别”一栏勾选“资产评估”并点击确定; 5. 点击搜索。

上海市目前共有 6 家资产评估机构可供选择, 其中浦东新区 1 家。  
(查询日期: 2024 年 12 月 6 日)

### 7.2.3.2 【会计审计】

审计是由有司法会计资格的会计师事务所来进行审计。会计审计机构可通过人民法院诉讼资产网 (<https://www.rmfysszc.gov.cn>) 自主查询选择。

查询步骤如下:1. 登录人民法院诉讼资产网; 2. 点击“司法技术”; 3. 点击左侧“专业机构”; 4. 在“专业类别”一栏勾选“会计审计”并点击确定; 5. 点击搜索。

上海市目前共有 8 家会计审计机构可供选择。(查询日期: 2024 年 12 月 6 日)

### 7.2.3.3 【选择合适的鉴定方式】

案件究竟是选择评估, 还是选择审计? 计算损失的方式不同应采用不同的鉴定方式。

a) 假定某技术信息被公开披露, 失去秘密性了, 此种情形宜以该技术的商业价值来计算损失, 通常来说就是以研发费用来计算, 此时需要评估机构对这一项技术的价值进行评估。

b) 如果侵权人采取了不正当手段获取技术信息，但未披露和使用，或虽使用了但侵权产品尚未上市，此种情形宜按该项技术的合理许可费来计算损失，通常按照普通技术许可计算许可费，此时也需评估机构进行评估。

c) 假如侵权人已经使用或已经允许他人使用了技术信息，侵权产品已投放市场，此种情形应以权利人减少的销售量，或者侵权人销售侵权产品的销售量，以司法审计的方式，委托会计师事务所进行审计。

### **7.3 【鉴定程序】**

#### **7.3.1 【委托主体】**

##### **7.3.1.1 【刑事民事案件委托主体】**

侵犯商业秘密刑事案件和民事案件中涉及的知识产权鉴定属于司法鉴定。司法鉴定机构应统一受理办案机关的司法鉴定委托。公安机关、检察机关和法院根据需要可以委托鉴定机构进行鉴定。很多商业秘密案件的权利人在报案之前，已经自行委托鉴定机构进行鉴定，并将鉴定意见作为报案的重要证据之一。办案机关依据报案材料决定立案后，应另行委托鉴定。

##### **7.3.1.2 【行政案件委托主体】**

商业秘密权利人向市场监管部门举报的，可以自行委托鉴定机构出具鉴定意见。市场监管部门对鉴定意见进行审查，并经被举报侵权人认可的，可以采纳作为定案证据。被举报侵权人对权利人提供的鉴定意见不予认可且有合理理由的，市场监管部门根据需要可以委托鉴

定机构（权利人委托鉴定机构以外的其他鉴定机构）鉴定。

### **7.3.2【委托形式要求】**

鉴定机构决定受理鉴定委托的，应当与委托人签订鉴定委托书。鉴定委托书应当载明委托人名称、鉴定机构名称、委托鉴定事项、鉴定用途、鉴定材料的提供和退还、鉴定风险，以及双方商定的鉴定时限、鉴定费用及收取方式、双方权利义务等其他需要载明的事项。

### **7.3.3【选定专家、查新检索和检测机构】**

鉴定机构根据委托事项和要求，推荐相关专业技术领域的查新检索机构、检测机构或鉴定专家，并经委托人确认后确定。

### **7.3.4【回避制度与保密义务】**

委托人认为查新检索机构、检测机构、鉴定专家与刑事民事案件当事人有利害关系，需要回避的情形，经委托人确认，鉴定机构可以另行选定。

查新检索机构、检测机构、鉴定专家应恪守保密义务，不得擅自留存、泄露受委托鉴定的技术信息。

### **7.3.5【鉴定方式】**

技术鉴定一般采用检测鉴定、专家评议鉴定的方式。

**7.3.5.1** 凡通过检测机构测试、检验能达到鉴定要求的技术鉴定，应采用检测鉴定。检测机构对检测结果出具书面检测报告。

**7.3.5.2** 专家评议鉴定，一般由两名以上专家组成鉴定组，按鉴定程序进行鉴定，对鉴定结果出具书面鉴定意见。

### **7.3.6【技术听证及现场勘验】**

鉴定机构根据需要可启动技术听证程序，就技术问题听取权利人和涉嫌侵权人对涉案技术信息的分析和意见、组织现场勘验，并邀请委托人一同参与听证、勘验过程。

### **7.3.7【出具鉴定意见】**

承担任务的查新检索机构、检测机构、鉴定专家应当在鉴定机构的鉴定意见上签名、盖章。鉴定机构对出具的鉴定意见承担相应法律责任。

### **7.3.8【鉴定意见的专家质证】**

法院根据案件事实查明需要，可以通知鉴定机构派员出庭接受质询，鉴定人也应当出庭接受当事人质询。鉴定意见要经过庭审双方当事人质证才能作为定案证据。

## 【相关案例】

### 1. 如何证明技术图纸上载明的技术信息属于非公知性信息？

**案情简介：**某公司多年来生产并销售其自主研发并自行生产的某种先进设备。任职于该公司多年的核心技术人员离职后，带走了该公司保密的技术图纸，在他处设立新厂生产销售相同的设备。该公司向公安机关报案该离职技术人员涉嫌侵犯其商业秘密。公安机关需要确认涉案技术信息是否属于技术秘密，委托某鉴定机构就技术信息是否属于非公知性信息出具鉴定意见。

鉴定机构出具以下意见：该公司研发的垃圾处理焚烧工艺、设计计算方法、组装调整方法及组装手册、成套 CAD 机械图及其图纸中所涉及的机械零部件尺寸公差等技术要求、与装配和结构位置关联的其他技术要求等工艺参数信息，是该公司在其产品运行实践中，通过长期的经验积累和根据客户反馈信息作出相应改进调整后逐渐形成的，也是其设备运用的关键信息，不会对外公开此类自主研发产生的技术信息和产品的生产技术图纸。涉案技术信息不为该专业领域的普通技术人员普遍了解和掌握，不可能通过公开渠道直接、容易获得。

公安机关采纳了鉴定机构的意见，认为报案人的技术信息是不为公众所知悉的信息，具有秘密性。

**解读：**公安机关委托鉴定机构对涉案技术信息进行非公知性鉴定，得到涉案技术信息不为该专业领域的普通技术人员普遍了解和掌握、也不可能通过公开渠道直接、容易获得的鉴定结论。除非涉嫌侵权人能够作出反证，公安机关可以依据该鉴定意见认定涉案技术信息具有秘密性。

### 2. 技术信息的同一性鉴定

**来源：**吴某侵犯商业秘密案沪浦检刑诉（2012）4086号起诉书

**案情简介：**2010年9、10月间，吴某利用其上海某公司担任合成研究员的工作便利，先后数次采用拆换其他研究人员办公用保密电

脑硬盘的方法，窃取上海某公司为其他公司研发的资料，其中包括化合物结构式及其合成信息。2011年3月至6月间，吴某为虚假宣传个人研发能力，将窃取的新型化合物结构式中的89个在互联网公开披露，除第56号结构式外的其余88个结构式与辉瑞公司的相应结构式具有同一性。

吴某的披露行为导致该些结构式不能申请专利，使得被害单位辉瑞公司及上海某公司的研发失去意义，导致上海某公司直接经济损失人民币268万余元。

2013年10月22日上海市浦东新区人民法院判决：吴某犯侵犯商业秘密罪，判处有期徒刑三年六个月，并处罚金人民币十万元。判决宣告后，吴某提出上诉。2014年7月24日上海市第一中级人民法院终审裁定：驳回上诉，维持原判。

**解读：**实践中，商业案件委托就相关专业技术问题进行鉴定对象一般为其技术信息是否为非公知技术，若判定是不为公众所知悉的技术信息，随后就权利人所拥有的技术信息与侵权人所披露使用的技术信息进行比对分析是否相同或相似。由于本案中控辩双方对于结构式的同一性问题认定存在较大争议，所以法院先行判定其是否具有同一性，然后再确认其是否构成商业秘密，这种判定方法具有一定的灵活性，也说明商业秘密案件的判定的先后次序并无严格约定。

鉴定意见结论中，关于化合物的同一性认为，从有机化学的专业角度，用结构式表示有机化合物的结构时，为了书写简便，除完整的结构式外，还可以使用结构简式表述。也就是说同一个有机化合物可以使用几种符合规则的不同结构型式来表示。因此，化合物的同一性反应在化学结构式上，是指化学结构式的一致性，或化学结构式的等同性（虽然化学结构式的表示方式不同，但其书写符合有机化合物结构式的基本规则，运用命名规则具有相同的化学名称，包括手性碳的绝对构型，因此也是相同的结构）。由此，本案中涉及含手性中心化合物、互变异构体、化合物外消旋体的同一性鉴定，最终鉴定结论认为：被告人披露的结构具有同一性。

法院最终认为，对于有争议的结构式是否具有同一性的认定，经

过庭审对鉴定意见的充分质证后采信了公安机关委托的鉴定机构所做出的判定，除一个结构式不同外，其余结构式与被害单位的相应结构式具有同一性。

### 3. 如何认定权利人因侵权遭受的损失？

**来源：**富某公司、方某某等7人侵犯商业秘密案（上海三中院、上海市检三分院2022年侵犯知识产权十大典型案例）

**案情简介：**瑞某公司主要从事一次性卫生用品生产设备生产线的研发、制造和销售。平某（另案处理）原系瑞某公司机械设计部经理，于2013年6月离职后加入同样从事卫生用品生产设备经营的被告单位富某公司担任技术指导。后平某将其从瑞某公司获取的若干技术秘密非法披露给富某公司经营人被告人方某某，并交由被告人龚某某、胡某某等6人（均从瑞某公司离职加入富某公司）使用。方某某明知上述技术信息系瑞某公司商业秘密，仍指使龚某某等人将其中部分技术秘密用于并销售给江苏、杭州等地客户，还指使胡某某等人将另外部分技术秘密以富某公司名义申请专利并公开披露。

经审计，富某公司销售侵犯商业秘密的设备，造成瑞某公司损失数额达1220余万元；经评估，富某公司申请并公开的商业秘密商业价值合计2019万余元。

2021年12月，上海市人民检察院第三分院以富某公司、方某某等7人涉嫌侵犯商业秘密罪提起公诉。2022年3月，上海市第三中级人民法院以侵犯商业秘密罪判处被告单位富某公司罚金1000万元，7名被告人被判处有期徒刑三年至一年不等，并处罚金800万元至30万元不等，适用缓刑。被告单位及被告人未提出上诉，判决已生效。

**解读：**本案中，被告单位富某公司通过两种方式侵犯瑞某公司的商业秘密。针对富某公司以不正当手段获取并使用商业秘密的行为，法院根据权利人因被侵权造成销售量减少的总数乘以权利人每件产品的合理利润，得出权利人的损失数额。针对富某公司将部分以上述手段获取并使用的商业秘密，通过申请专利的形式对外披露的行为，因侵犯商业秘密行为导致商业秘密被公众所知悉，通过委托专门的资产

评估机构根据商业秘密的研发成本、实施该项商业秘密的收益等综合确定商业秘密的商业价值。两者所得总和即为权利人的损失数额。法院据此判决富某公司构成侵权商业秘密罪并处罚金。权利人后继可以再提起民事诉讼，要求富某公司赔偿损失。

## **8. 涉外保护**

中国企业在海外经营或国际贸易中应高度关注与重视商业秘密纠纷风险，了解各国商业秘密保护环境，实施相应的商业秘密保护措施，做好风险防控，并制定维权策略。

### **8.1 【美国商业秘密保护】**

#### **8.1.1 【立法】**

##### **8.1.1.1 【统一商业秘密法】**

1979 年，美国颁布《统一商业秘密法》，是首部对商业秘密的专项立法，系统确立了商业秘密的保护范围以及侵犯商业秘密的行为方式。根据《统一商业秘密法》的定义，商业秘密是指任何有独立的实际或潜在的经济价值，并且通过正常的途径无法获知，有必要采取措施保持其秘密性的信息，包括配方、模式、汇编、程序、设备、方法、技术或流程等等。因此商业秘密的三大特性是价值性、非公开性和秘密性。

##### **8.1.1.2 【经济间谍法】**

1996 年，美国颁布《经济间谍法》，首次将盗窃或侵犯商业秘密的行为规定为刑事犯罪。《经济间谍法》规定了经济间谍罪和一般商业秘密盗窃罪，两者的区别在于如果盗窃商业秘密的犯罪行为是为了使任何的外国政府、外国机构或外国代理人受益，则以经济间谍罪论处。

根据2013年修订后的《经济间谍法》，犯一般商业秘密盗窃罪，个人最高会被处以十年监禁，公司犯罪最高会被处以五百万美元的罚金。犯经济间谍罪，个人最高会被处以五百万美元罚金并处以最高十五年监禁，公司犯罪最高会被处以一千万美元或被盗商业秘密价值三倍中较高者的罚金，法院还可没收非法所得。

### **8.1.1.3【保护商业秘密法】**

2016年，美国颁布《保护商业秘密法》，对盗窃商业秘密案件的联邦管辖权、案件执行、境外案件报告、国会相关共识以及行为规范、责任豁免等进行详细规定。

该法改变商业秘密案件原由各州管辖的原则，将商业秘密案件提升到联邦层面，首创有关商业秘密的民事诉讼案由。《保护商业秘密法》为起诉侵犯商业秘密案件、获得民事救济提供统一的联邦法律依据，同时建立起商业秘密保护的统一标准。侵犯商业秘密的行为方式包括：明知或应知通过不正当手段（偷窃、贿赂、虚假陈述、违反或诱使违反保密义务、通过电子侵入或其他手段进行的间谍活动）获得他人商业秘密；在未获得明示或默示同意的情况下，披露或使用他人的商业秘密。

提示：美国关于商业秘密定义和侵权行为类型的法律规定与我国大体相似。对于有涉美业务的国内企业而言，应采取实际措施确保自身信息的秘密性和安全性，同时避免侵犯美国企业的商业秘密。

### **8.1.2【救济途径】**

在美国，当权利人商业秘密被侵犯时，可选择三种救济途径，分

别是民事诉讼、刑事程序以及申请美国国际贸易委员会发起337调查。

#### **8.1.2.1【民事诉讼】**

商业秘密权利人对侵犯其商业秘密的行为人可提起民事诉讼。权利人可以获得的救济包括禁令救济、损害赔偿金、律师费补偿等。

法院可以向被告发布禁止侵害的禁令，包括临时禁令、预备性禁令和长期性禁令，其期限和适用条件也有所不同。

损害赔偿金在美国可以单独请求，也可以同禁令一起主张。赔偿数额按照实际损失、不当得利以及许可收费损失的先后顺序确定。在恶意侵犯商业秘密的情形下，法院可判决被告按前述赔偿数额两倍以内支付惩罚性赔偿。法院还会判决给予胜诉方合理的律师费补偿。

#### **8.1.2.2【刑事程序】**

美国司法部可向法院提起侵犯商业秘密的刑事指控。在刑事程序中，司法部要承担举证责任，证明被告实施侵犯商业秘密的犯罪行为，并且具有恶意的作案动机。

因盗窃商业秘密被刑事起诉的案例，包括可口可乐公司前全球研究首席工程师游晓蓉博士，被控犯盗窃商业秘密罪、经济间谍罪和电信诈骗罪，最终被判处 14 年监禁和20万美元罚金；俄克拉荷马石油公司科学家谭宏进，被控犯盗窃商业秘密罪，最终被判处2年监禁和15万美元罚金。

#### **8.1.2.3【337调查】**

337调查指依据美国《1930年关税法》第337节的有关规定，如果进口贸易中存在侵犯知识产权或者其他不正当竞争行为，当事人可以

向美国国际贸易委员会（United States International Trade Commission，以下简称ITC）申请启动行政调查。ITC也可自行决定开展行政调查。

337调查大多涉及与知识产权保护有关的指控。相较于漫长的司法程序，337调查可速战速决，通常在一年半左右审结，已成为美国知识产权保护的利器。自1986年中国企业首次接受337调查以来，一直是337调查的主要对象。

337调查的主要程序包括：申请、立案、应诉、听证前会议、取证、听证会、行政法官初裁、委员会复议并终裁、总统审议。如果任何一方当事人对ITC的裁决结果不服，可以向美国联邦巡回上诉法院提起上诉。

排除令（Exclusion Order）是337调查中ITC最具杀伤力的处罚措施，由美国海关执行，它将直接导致外国企业相关产品无法进入美国市场。

### **8.1.3 【长臂管辖】**

美国通过立法和法院判例扩大其管辖权，为司法和执法部门的域外管辖行为提供法律依据，以实现其长臂管辖的目的。依据美国《保护商业秘密法》及《经济间谍法》，如果侵害地在美国，商业秘密是在美国未经授权获得、披露或使用的，则无论侵权人的原籍国在何地，都可能被判向美国公司负担损害赔偿甚至惩罚性赔偿。

## **8.2 【其他发达国家商业秘密保护】**

## **8.2.1 【德国商业秘密保护】**

### **8.2.1.1 【立法】**

2019年4月26日，《德国商业秘密法案》生效，开启了德国以单行法保护商业秘密的新篇章。在此之前，德国的商业秘密侵害主要通过反不正当竞争法和刑法来规制。

《德国商业秘密法案》是对欧盟商业秘密保护指令（第2016/943号欧盟指令）的具体实施。商业秘密获得保护的前提是商业秘密合法持有人已经根据具体情况采取了适当的保密措施对其进行保密。《德国商业秘密法案》为保护商业秘密提供了新的民法基础，还同时规定了刑法条款，意味着侵犯商业秘密将会受到刑事处罚。

### **8.2.1.2 【救济途径】**

根据《德国商业秘密法案》，商业秘密权利人可以申请对侵权人采取临时禁令，有权要求销毁或归还包含商业秘密的文件或物件，并要求召回、下架、移除或销毁侵权商品。

商业秘密权利人可以申请损害赔偿。关于赔偿金额，权利人可以在“权利人的利润损失”、“虚拟但合理的许可费用”以及“侵权人获得的利益”这三种计算方法中选择一种对自己最有利的计算方法。

## **8.2.2 【日本商业秘密保护】**

### **8.2.2.1 【立法】**

日本主要通过《不正当竞争防止法》来规制侵犯商业秘密的行为，将其作为典型的不正当竞争行为。《不正当竞争防止法》第二条规定，商业秘密是指作为秘密进行管理，尚未众所周知的生产方法、销售方

法及其他经营活动中实用的技术上或经营上的情报。

日本现行刑法中没有直接针对侵犯商业秘密行为的条款。但司法实践中可以适用背信罪、泄露秘密罪和贿赂犯罪等罪名对商业秘密进行间接保护。

#### **8.2.2.2【救济途径】**

如果商业秘密被侵害，权利人可以通过民事救济途径向法院申请禁令，并可以要求赔偿损失。

如果侵权行为涉嫌构成犯罪，权利人可以向警方报案，要求追究刑事责任。相关刑事制裁包括对个人最高十年监禁和最高3000万日元的罚金，对公司最高10亿日元的罚金。此外，法院可以没收侵权人因非法披露或使用商业秘密而获得的收入。

自2015年《不正当竞争防止法》修订以来，检察官不需要商业秘密权利人的指控，也可以独立提起诉讼。但实践中，检察官仍然需要商业秘密权利人的合作，以便在刑事诉讼中收集足够的证据来证明所指控的行为。

#### **8.3【中国企业的应对】**

商业秘密纠纷的复杂性高，涉及的司法程序耗时长，非常耗费精力。企业一旦成为被告，可能会面临市场份额减少、利润损失、经营能力削弱的不利局面。即便最终被法院认定不构成犯罪，企业也要应对高额的诉讼费用和复杂的涉外司法程序，企业信誉也会受到质疑。

参与国际竞争的中国企业应尽早做好准备，包括了解各国法律、

定期自查评估、审慎进行招聘等。若受到指控，建议聘请专业律师，积极应诉。

### **8.3.1 【了解各国法律】**

对于一些正在走出国门的中国企业来说，即使企业主要的生产经营活动仍在国内，只要企业已经有开拓海外市场的初步计划，就应将海外涉诉的风险纳入考量，从而有意识地学习了解对应国家的法律，了解哪些信息可能构成受法律保护的商业秘密，以及如何处理这些信息才能够达到合规标准。

### **8.3.2 【实施自查评估】**

如果中国企业在外国法院被提起侵犯商业秘密的指控，中国企业应首先明确涉及的信息是否符合商业秘密的法定条件。如果能证明以下事实，将有利于后续应对：

a) 不具有秘密性。如果涉及信息在被指控的行为发生时已经是众所周知的信息，那么就不构成商业秘密。比如在互联网、学术期刊可以公开检索到的信息就不具有秘密性。企业还可以尝试证明对方没有对涉及信息采取保密措施，或是涉及信息不具有商业价值。

b) 有合法来源。如果中国企业可以证明自己是通过合法途径取得的信息，比如从第三方善意取得或通过自行研发、反向工程取得，就可以证明侵权行为不存在。

### **8.3.3 【聘请专业律师】**

聘请具有涉外应诉能力和经验的律师，显得尤为重要。律师可以帮助企业分析起诉状、制定整体应对策略。企业应成立内部专项小组，

包括法务部门、业务部门及其他相关部门的成员，配合律师开展应诉工作。律师受保密义务的约束，企业不必过于担心商业秘密会被泄露，对律师需要了解的事实应当如实告知。

#### **8.3.4【审慎招聘】**

企业在招聘曾就职于外国企业的员工时，应当持审慎态度。要先确定该员工没有竞业限制或其他约束，也不会携带前公司的商业秘密加入公司。

##### **8.3.4.1【详尽背景调查】**

在招聘过程中，企业应对候选人进行详尽的背景调查，了解其履历的真实性、从原单位离职的原因、是否和原单位签订过保密协议和竞业限制协议，并了解候选人是否有因涉嫌窃取商业秘密等不当行为被调查、起诉的记录。

##### **8.3.4.2【关注来自于竞争对手的员工】**

如果企业决定从国内外的竞争对手公司招聘员工，尤其是可能持有对方保密信息的员工，更需要审慎考虑、排除风险。企业在劳动协议中要明确约定，员工在公司工作期间不得违反与任何第三方的保密协议，要求员工承担前雇主要求的保密义务，不得向现雇主泄露其知晓的商业秘密。

#### **8.3.5【寻求外部支持】**

企业在接到国外法院或者执法机构的应诉或配合调查的通知后，可以联系负有支持经济发展职责的有关行政机关或者社会团体共同应对。我国的商务部（贸易救济调查局）、地方商务部门、行会商会等

可能为企业提供必要的支持。

### 【相关案例】

**案例：**美国 PPG 集团诉江苏铁锚公司侵犯商业秘密案（PPG Industries Inc v. Jiangsu Tie Mao Glass Co Ltd）

**案件号：**2: 15-CV-00965

**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，指控被告雇佣了原告的前雇员 Thomas Rukavina，并通过该雇员获取了原告的 Opticor 相关技术。原告并没有向法院提供证据以证明其实际损失，而主张被告通过侵犯商业秘密获得不当得利。

2021 年 6 月，法院将原告 Opticor 相关技术的研发费用作为评估被告不当得利的基准，认定原告的实际研发费用为约 880 万美元，判决被告向原告支付约 880 万美元的补偿性赔偿和约 1800 万美元的惩戒性赔偿，共计约 2600 万美元。

**解读：**诉讼中美国法院根据权利人的实际研发费用确定补偿性赔偿数额。中国企业败诉后还被判支付高昂的惩戒性赔偿。这一案例再次给中国企业敲响警钟，应在招聘国际人才时严格审慎，避免侵犯他人商业秘密。

**案例：**美国钢铁公司向 ITC 申请针对商业秘密侵权对中国宝钢公司发起 337 调查

**案件号：**337-TA-1002

**案情简介：**2016 年 5 月 26 日，美国钢铁公司（U.S. Steel Corporation）向 ITC 申请，对中国输美碳钢及合金钢产品发起 337 调查。原告就被告中国宝钢公司依靠中国钢铁协会合谋操纵产品价格和出口量、标记虚假原产地以规避美国双反税令以及被告通过黑客攻击原告三个诉点提出控诉，请求 ITC 发布普遍排除令及禁止令。2017 年 2 月 22 日，ITC 行政法官裁定，终止关于被告商业秘密诉点的调查。

这也是美国 337 调查历史上，中国企业首次获得商业秘密类案件的胜诉。

**解读：**近年来，中国钢铁产品在国际市场上具有较强的竞争优势，因而遭到美国、欧洲等多个国家和地区的抵制。此次宝钢在 337 调查中获胜意义重大。面对 337 调查，中国企业要善于利用美国当地的法律以及相关国际规则，研究、搜集证据，确定抗辩策略，积极应对此类调查。同时，中国企业也要注重日常的知识产权保护工作，加强数据和证据的留存，这样才能在面对调查时好整以暇，拿出充分证据，取得对自身有利的裁决结果。

**案例：**摩托罗拉诉海能达盗窃商业秘密案 (Motorola Solutions, Inc. v. Hytera Commc' ns Corp)

**案件号：**1: 17-cv-01973

**案情简介：**中国海能达通信股份有限公司于 2000 年进入美国市场，四年后成立美国子公司，此后市场布局遍布全球。2017 年 3 月，海能达的竞争对手美国摩托罗拉公司在美国联邦法院对海能达提起盗窃商业秘密的指控。

海能达雇佣了曾任职于摩托罗拉的 3 名工程师，法院认定他们的侵权责任可以推定至他们的现任雇主海能达。2020 年 2 月 15 日，美国法院作出一审裁决，认定海能达及其在美子公司侵犯了摩托罗拉的多项商业秘密及著作权，应向摩托罗拉支付损害赔偿 3.46 亿美元及惩罚性赔偿 4.19 亿美元，合计约人民币 53 亿元。海能达将寻求上诉。

**解读：**在本案中，即使海能达可能存在的相关侵权行为全部发生在美国境外，但美国法院认定海能达在美国的产品销售、广告、维修等行为是在美国境外侵犯商业秘密行为的延伸，并以此确定了美国法院的长臂管辖权。这一点需要中国企业警醒。

**案例：**美国超导诉华锐风电盗窃商业秘密案 (AMSC v. Sinovel Wind Group LLC)

**案件号：**0578 3: 13CR00084-001

**案情简介:**美国超导公司和中国华锐风电公司于2005年开始合作,美国超导向华锐风电提供风机设计和技术服务,同时为数千台风机提供电控核心部件和控制软件。2011年合作终止。美国超导随后发现,华锐风电的两名高管说服美国超导的一名负责人加入华锐风电并秘密下载源代码,窃取美国超导的知识产权。2011年6月,美国超导在华锐风电生产的涡轮机中发现了美国超导软件的复制版本。2018年1月,华锐风电和前述三名员工在美国地区法院被判犯有盗窃商业秘密罪和电汇欺诈罪。

**解读:**这一案件反映出部分中国企业商业秘密保护意识的淡薄。本案中,被告两名高管与原告前员工之间的互联网聊天记录和电子邮件被原告获取并作为证据提交,起到关键性的作用。原告不但在美国提起诉讼,还在中国发布了多起针对华锐风电的诉讼。商业秘密作为一种极具价值的无形财产,对企业发展、国家发展的重要性不言而喻。中国企业不仅要为应对商业秘密涉外纠纷做好准备,也要保护好自己的商业秘密,维护自己在海外市场的合法权益。勇于面对,敢于维权。

人工智能行业不同层面企业重要信息商业秘密要件评估表

	基础层企业	框架层企业	模型层企业	应用层企业
<b>秘密性 评估</b>	核心算法、数据处理技术、硬件设计和制造工艺等是否不为公众所知悉。尤其是经过大量的研发和实践积累的特定的高效数据清洗算法、数据存储架构设计、特定的芯片架构、高性能服务器的内部构造等。	开发框架的独特架构和优化策略是否不为公众所知悉，尤其是框架实现高效的并行计算、内存管理等技术细节，框架的接口设计和扩展能力等。	模型的结构和参数组合是否为公众所知悉，模型的训练数据和训练方法是否为公众所知悉。	在特定行业的应用解决方案和业务流程是否为公众所知悉，场景应用的创新是否尚未公开，用户数据分析和处理方法是否具有独特性、秘密性。
<b>价值性 评估</b>	该技术是否能提高数据的处理和存储效率，是否可以提升人工智能模型的训练和推理速度，以及为上层提供稳定的计算能力等。评估基础层的技术创新的成本与投入，及一旦被公开可能导致企业的商业价值或竞争优势减损。	框架是否能创造高效的开发环境，降低人工智能模型开发的难度和节约成本。评估框架的商业和竞争力价值。	模型是否能为企业带来商业价值，尤其是在图像识别、自然语言处理等方面是否能提高生产效率、改善用户体验。评估模型的不断改进和优化是否可以保持企业在市场中优势地位。	应用场景是否提高了行业效率，提高了性能，降低了开发成本等，应用层的创新对于开拓新的市场和业务领域的商业和竞争价值。

<p style="text-align: center;"><b>保密性 评估</b></p>	<p>是否对研发团队的组成、研发进度和技术路线等研发过程进行严格保密。是否对硬件制造环节加强管控，是否能有效防止研发技术、工艺和设计图等外泄。是否建立了完善的数据中心的物理安全和网络安全保障措施，是否能有效防止数据被窃取或破坏。</p>	<p>是否对框架的源代码设立严格的访问控制和修改权限。是否有效保护了框架的文档和技术说明。密切关注开源动态，关注他人是否可以从开源项目中获取框架的关键技术。</p>	<p>对模型的训练过程是否采取了严格的保密措施，包括训练数据的来源、处理方法和训练参数等。是否采用加密技术保护模型的参数和结构，有效防止被窃取或篡改。是否对模型的部署和使用进行了严格的权限管理，有效防止未经授权的访问和使用。</p>	<p>是否采用加密技术、访问控制等手段保护用户数据的隐私和安全。是否对应用的界面设计和用户体验等进行保密。是否与合作伙伴签订了严格的保密协议，是否有效确保应用解决方案在合作过程中不被泄露。</p>
--	--	--	--	--

附录2

浦东新区商业秘密侵权投诉举报受理点

号	受理机构	地址	联系人	固定电话
1	浦东新区 投诉举报中心	洋泾街道杨高中路 2900 号 2 号门		12315/12345
2	陆家嘴市场 监督管理所	陆家嘴街道乳山路 235 弄 2 号	阮迪	58312017
3	洋泾市场 监督管理所	洋泾街道栖山路 171 号	陈晖	58511383
4	花木市场 监督管理所	花木街道牡丹路 185 号	张赢	50451101
5	潍坊市场 监督管理所	潍坊街道潍坊路 131 弄 2 号	束方庆	50938202
6	塘桥市场 监督管理所	塘桥街道南泉路 1325 号	康友维	50942073
7	上钢市场 监督管理所	上钢新村街道成山路 200 号	陈晨	20255727

8	金杨市场 监督管理所	金杨新村街道栖山路 1025 号	施振欣	68536013
9	沪东市场 监督管理所	沪东新村街道利津路 255 号	赵琳	58710105
10	浦兴市场 监督管理所	浦兴路街道五莲路 1336 号	陈为庆	58592278
11	东明市场 监督管理所	东明路街道灵岩南路 1313 号 4 楼	徐文杰	50187301
12	南码头市场 监督管理所	南码头路街道临沂路 128 号一、二层	刘畅	50837857
13	周家渡市场 监督管理所	周家渡街道昌里东路 210 号	王永	68700511
14	惠南市场 监督管理所	惠南镇北门大街 168 号	邬海华	58000623
15	周浦市场 监督管理所	周浦镇周祝公路 1378 号	倪振青	58151337
16	康桥市场 监督管理所	康桥镇秀浦路 2388 号 9 号楼	顾洋舟	61182321 -205
17	金桥市场 监督管理所	金桥镇永建路 102 号 309 室	龙金林	50312565

18	北蔡市场 监督管理所	北蔡镇五星路 677 弄 17 号楼	王志军	58432703
19	航头市场 监督管理所	航头镇航头路 1198 号	许姚	58229122
20	三林市场 监督管理所	三林镇三林路 85 号	张昊	58493404
21	唐镇市场 监督管理所	唐镇南曹路 470 号	顾晓斌	58582187
22	高桥市场 监督管理所	高桥镇和龙路 338 号	徐昊	58670511
23	张江市场 监督管理所	张江镇建中路 1 号	许益	58959046
24	祝桥市场 监督管理所	祝桥镇卫亭路 1029 号	沈幸军	58102650
25	新场市场 监督管理所	新场镇新环西路 1185 弄 1173 号	甘焊堃	68090737
26	泥城市场 监督管理所	泥城镇泥城路 101 号	张明圣	58072621
27	高东市场 监督管理所	高东镇赵高公路 1295 号	叶军	68480229

28	曹路市场 监督管理所	曹路镇金钻路 62 号	邓悦人	58631253
29	高行市场 监督管理所	高行镇东靖路 1831 号	汤恒南	58309353
30	万祥市场 监督管理所	万祥镇宏祥北路 83 弄 32 幢	于士	58043292
31	老港市场 监督管理所	老港镇良欣路 456 号	顾庆旦	58051454
32	大团市场 监督管理所	大团镇南团公路 3030 号	闫少文	58081093 -8205
33	合庆市场 监督管理所	合庆镇前哨路 200 号	胡剑	58975729
34	宣桥市场 监督管理所	宣桥镇沪南公路 8666 弄 11 号楼 4 楼	苗春雨	68009942
35	书院市场 监督管理所	书院镇万松路 319 弄 3 幢	李杰	58040075
36	川沙市场 监督管理所	川沙新镇华夏东路 2378 号 206	丁戟	68404288
37	南汇新城 市场监督管理所	南汇新城镇环湖西三路 869 号二楼	帅银平	20936502 -8036

38	保税区分局	华申路 80 号 3 幢 6 层	王政强	50193525
39	度假区分局	申迪北路 700 号 4 号楼	杨正元	20991761

附录3

上海市商业秘密侵权纠纷	法院名称	地址	联系电话
-------------	------	----	------

民事案件管辖法院序号			
1	上海知识产权法院	上海市浦东新区张衡路 988 号	021-58951988
2	上海市浦东新区人民法院	上海市浦东新区丁香路 611 号	021-38794518
3	上海市闵行区人民法院	上海市闵行区莘庄镇雅致路 99 号	021-64120000
4	上海市徐汇区人民法院	上海市徐汇区龙漕路 128 号	021-34168168

5	上海市长宁区人民法院	上海市长宁区虹桥路 1133 号	021-52574999
6	上海市金山区人民法院	上海市金山区金山大道 2288 号	021-67965888
7	上海市奉贤区人民法院	上海市奉贤区解放东路 199 号	021-37190666
8	上海市松江区人民法院	上海市松江区南青路 701 号	021-67735555
9	上海市杨浦区人民法院	上海市杨浦区河间路 29 号	021-31372000
10	上海市虹口区人民法院	上海市虹口区北宝兴路 531 号	021-36123300
11	上海市黄浦区人民法院	上海市黄浦区延安东路 1234 号	021-53584777
12	上海市静安区人民法院	上海市静安区共和新路 3009 号	021-26120000
13	上海市普陀区人民法院	上海市普陀区铜川路 1433 号	021-22273333
14	上海市宝山区人民法院	上海市宝山区友谊路 989 号	021-26078989
15	上海市嘉定区人民法院	上海市嘉定区德富路 1221 号	021-59521000
16	上海市青浦区人民法院	上海市青浦区城中北路 555 号	021-69201478

17	上海市崇明区人民法院	上海市崇明区崇明大道 7600 号	021-59611568
----	------------	-------------------	--------------

附录4

### 浦东新区检察机关、公安机关联系表

对外接待机构	办公地点	办公时间	联系方式
上海市浦东新区人民检察院 12309 检察服务中心	上海市浦东新区蔡伦路 68 号	工作日 上午 9:00-11:00 下午 13:30-16:30 (周五下午 13:30-16:30)	021-50137200
上海市公安局浦东分局经侦支队	上海市浦东新区康桥路 1710 号	工作日 上午 9:00-11:30 下午 13:30-17:00	021-22041240

附录 5

## 人民法院诉讼资产网备案的知识产权鉴定机构

(查询日期: 2024 年 11 月 28 日)

序号	机构名称	地址	联系人	联系电话
1	上海辰星电子数据司法鉴定中心	上海市浦东新区张江高科技园毕昇路 339 号	孙杨	18502128165
2	上海汉光知识产权数据科技有限公司	中国(上海)自由贸易试验区蔡伦路 333 号 5 幢 609 室	胡惠	021-52666106
3	上海科际知识产权服务中心(有限合伙)	中国(上海)自由贸易试验区新片区环湖西二路 888 号 C 楼	赵婉明	021-53863703
4	上海市计算机行业协会	上海市浦东新区海宁路 1399 号 901 室	于翔	021-50815662
5	上海市知识产权服务中心	上海市徐汇区漕宝路 650 号东幢 2 楼	董黎	13761898760
6	上海技术交易所有限公司	上海市杨浦区国权北路 1600 号湾谷科技园 B5 号楼 304A	宋毅	021-65682551
7	上海公沁扬知识产权服务有限责任公司	上海市长宁区 988 号 12 楼 C 座	陆昱	13601652288
8	上海硅知识产权交易中心有限公司	上海市徐汇区宜山路 333 号 1 幢 1705 室	徐步陆	021-61154610
9	上海洁湛知识产权服务有限公司	上海市静安区南京西路 1486 号 SOHO 东海广场 3102-04 室	蒋坡	021-52821776

10	上海科鉴知识产权服务有限公司	上海市徐汇区漕宝路 400 号 2406 室	叶枝灿	13761153117
11	上海新威知识产权服务有限公司	上海市虹口区东体育会路 816 号置汇谷 C 座	马丽华	021-31273006
12	中国电子信息产业发展研究院	北京市海淀区万寿路 27 号院	孙文婷	010-68209275
13	中国信息通信研究院	北京市海淀区北花园路 52 号	闫坤	15210111088
14	国家工业信息安全发展研究中心	北京市石景山区鲁谷路 35 号	潘妍	010-88686227
15	北京国威知识产权鉴定评估中心有限责任公司	北京市海淀区知春路 1 号学院国际大厦 10 层 1009	王楠	13691312045
16	北京菲沃德知识产权咨询有限公司	北京市海淀区西四环北路 125 号 1 幢六层 6043	李克	010-88589011
17	北京国创鼎诚知识产权应用技术研究院	北京市东城区胜古中路 1 号蓝宝商务大厦 A 座 321 号	武斌	010-84670710
18	北京京州知识产权服务中心有限公司	北京市海淀区海淀南路甲 21 号中关村知识产权 大厦 A 座 102 室	张旗	13810718940
19	中国版权保护中心	北京市丰台区汽车博物馆西路 9 号院 6 号楼	刘雅琳	13311256366
20	首都知识产权服务业协会	北京市海淀区海淀南路甲 21 号中关村知识产权 大厦 A 座 3 层	杜艺莹	010-66139027

21	浙江省知识产权研究与服务中心	浙江省杭州市滨江区丹枫路 399 号知识产权大厦 1 号楼 4 楼	唐灵	0571-88917569
22	浙江省机电产品质量检测所有限公司	浙江省杭州市滨江区庙后王路 125 号 1 幢 1-4 层	史桢超	0571-88014128
23	浙江省版权协会	浙江省杭州市拱墅区大关路 189 号万通中心 5 幢 303 室	胡伟林	0571-88135633
24	杭州中知鉴证科技有限公司	浙江省杭州市拱墅区东新路 240 号兔狗创新大厦附楼 3A 层	张主任	18966480087
25	杭州索图知识产权服务有限公司	浙江省杭州市拱墅区东新路 533 号蔚蓝国际大厦 1 号楼 2007 室	张得明	0571-88015657
26	杭州市知识产权保护中心	浙江省杭州市滨江区丹枫路 399 号知识产权大厦 1 号楼 10 楼	潘伟祥	13957154409
27	浙江现代智慧城市研究院	浙江省杭州市西湖区文一西路 522 号西溪科技园 3 幢 2 单元 5 楼	张韧佳	13606521632
28	浙江方圆检测集团股份有限公司	浙江省杭州市西湖区天目山路 222 号 4 号楼 6 楼	陈勇	13957166587
29	逐思科技服务（杭州）有限责任公司	浙江省杭州市西湖区金沙曲苑 11 号-1	朱秀颖	0571-85853700
30	国鉴博智科技（浙江）有限公司	浙江省杭州市余杭区杭州市临平区余杭经济技术开发区红丰路 509 号一号楼 A202	贺主任	0571-86385122
31	浙江科证技术咨询服务有限公司	浙江省杭州市上城区环站东路 768 号东站花园商务中心 2 幢 3A11	高丽	0571-88110363

32	杭州律证检测技术有限公司	浙江省杭州市拱墅区汉鼎国际大厦 1110 室	丁庆明	15858251991
33	微谱检测鉴定评估（杭州）有限公司	浙江省杭州市滨江区浦沿街道伟业路 3 号 C 幢 801 室	杜鹏飞	13681691203
34	浙江联合应用科学研究院	浙江省杭州市拱墅区永华街 198 号泰地洄龙湖 邸 37 幢	付元杰	18058181879
35	杭州澜芯慧控科学技术有限公司	浙江省杭州市上城区九环路 48 号 5 幢 2 层 268 室	赵明	15605889089
36	浙江省知识产权保护中心	浙江省杭州市西湖区文二路 218 号	周旭昊	13958821589
37	浙江华证知识产权服务有限公司	浙江省丽水市莲都区花园路 422 号兴业大厦 254 室	杨晓波	17365881319
38	宁波科集技术服务有限公司	浙江省宁波市高新区扬帆路 999 弄 5 号 508-10 室	周佳	0574-87919769
39	浙江湖州明鉴鉴定评估事务所（有限合伙）	浙江省湖州市吴兴区浙江省湖州市奚塘景城 35 幢五苗圩路 31 号-4	秦巧丽	17739773358
40	浙江湖州万物原因鉴定评估有限公司	浙江省湖州市吴兴区清丽家园 20 幢 809 室-13	秦立生	19357165899
41	江苏省科协企业创新服务中心	江苏省南京市建邺区梦都大街 50 号东楼 518	王晓忠 周辉	13016955002
42	山东知识产权司法鉴定中心	山东省济南市历城区舜华路 2020 号	刘洁	0531-88198563

43	山东知鉴知识产权司法鉴定有限公司	山东省济南市历城区舜华路 2020 号	刘洁	0531-68792110
44	山东国润资产评估有限公司	山东省济南市高新技术产业开发区新泺大街 088 号鲁商福瑞达广场 A 座 1005 室	乔守朋	15553115392
45	山东科技事务司法鉴定所	山东省济南市高新技术产业开发区舜华路 2000 号舜泰广场 3 号楼 7 层	王怡然	15965627110
46	华知鉴(山东)知识产权咨询服务有限公司	山东省济南市历下区经十路 15982 号第一大道 1701 室	王怡然	0531-86920987
47	山东天德汇资产评估有限公司	山东省济南市历城区华龙路 1110 号三威大厦 804 室	窦希文	13805314560
48	广东省知识产权保护中心	广东省广州市越秀区先烈中路 100 号大院 60 栋 9 楼	梅颖娟	020-87681613
49	深圳市公标知识产权鉴定评估中心	广东省深圳市福田区深南中路 1033 号档案大厦 9 楼东侧	邓光昀	13928498890
50	四川汇西知识产权鉴定评估有限公司	四川省成都市武侯区天府五街菁蓉汇 7 号楼 5 层知识产权公共服务平台 504 室	田晓玲	19302856707
51	四川西部知识产权鉴定评估有限公司	四川省成都市金牛区马家花园路 2 号第 9 层 908-909 号	张锋	028-87656123
52	江西清析知识产权服务有限公司	江西省南昌市红谷滩区红谷大道中段 1568 号	许文友	17775205527
53	江西诚誉质量检测有限公司	江西省南昌市西湖区桃花路与芳湖路交叉口硕 丰西湖里 1 栋 1 单元 1304 室	吴天	

54	江西汇测检测技术有限公司	江西省南昌市西湖区桃花路与芳湖路交叉口西湖里1栋1303室	吴飞	17375424768
55	江西鑫宁检测技术有限公司	江苏省苏州市昆山市徐公桥路2号中茵国际广场F519室	项工	13381739076
56	江西原因质检鉴定中心有限公司	江西省上饶市信州区志敏大道475号数字经济产业园A栋8楼03-2室	秦立生	18198989098
57	中知林牧畜农渔科学技术研究(江西)有限公司	江西省上饶市信州区高铁经济试验区茶圣东路文创中心4号楼439室	秦秀英	18924015341
58	江西知鉴知识产权服务有限公司	江西省上饶市信州区滨江西路66号3幢3007	顾大雁	13371890102
59	西知鉴知识产权鉴定评估(重庆)有限公司	重庆市渝北区回兴街道宝圣大道209号西正街A座18-8	曾得国	023-67253442
60	昆明鸿润资产评估有限公司	云南省昆明市青年路145号盛迪大厦二楼	李俊	0871-63137751
61	湖南湘鉴知识产权鉴定评估中心有限公司	湖南省长沙市天心区劳动西路342号湖南省企业服务大楼	鲁鹏	0731-85417803
62	湖南正源司法鉴定服务有限公司	湖南省长沙市雨花区湘府东路二段200号华坤大楼823室	杨世超	0731-85453600
63	湖北中新科维检验检测有限公司	湖北省宜昌市西陵区湖北省宜昌市高新区兰台路13号易联科技园	覃光军	0717-6228598
64	中国检验认证集团厦门有限公司	福建省厦门市湖里区东渡路116号中检大厦1-7楼	徐祥	18905921792

65	贵州省知识产权研究会	贵州省贵阳市观山湖区贵阳市黔灵山路 357 号 德福中心 7 号楼 4 层	赵茂森	0851-84122691
----	------------	--	-----	---------------