

商业秘密风险防范制度建设——再评《商业秘密保护规定》

作者：杨迅 | 张莹

2026 年 2 月 24 日，国家市场监督管理总局发布《商业秘密保护规定》(以下简称“《规定》”), 并将于 2026 年 6 月 1 日起正式施行。《规定》细化了《反不正当竞争法》关于商业秘密的保护规定, 吸收借鉴了近年来司法实践中的成熟经验, 为行政执法提供了明确的依据。然而, 《规定》的价值并不止步于执法层面——它所确立的认定标准、侵权行为类型与保护措施要求, 更是企业建立内部商业秘密风险防范体系的重要指引。

我们此前已评述了《规定》中有关商业秘密保护与网络安全合规要求的衔接问题(见[《拥抱数字化经济的商业秘密保护》——首评《商业秘密保护规定》](#))。在此基础上, 本文将结合现有司法实践, 梳理企业在商业秘密保护方面面临的主要风险, 并就如何建立有效的制度防范机制提出参考建议。

一. 《商业秘密保护规定》纵览

商业秘密并非严格意义上的知识产权, 但是却具有与知识产权类似的性质: 它如专利一样保护技术方案, 但不需满足专利的“三性”和授权程序; 它又是最天然的“知识产权”, 发源于普遍商业道德的基本准则。同时, 商业秘密的保护也最具有综合性, 以《反不正当竞争法》为核心规范, 同时涉及网络安全、劳动管理等多个领域的法律要求。

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

1. 商业秘密保护的法律体系和立法进程

我国商业秘密保护的法律体系以《反不正当竞争法》为核心，辅以《民法典》《刑法》《劳动合同法》等相关规定，共同构成多层次的保护框架。近年来，随着国内外经济形势的发展变化，我国对商业秘密的保护力度不断加强：2017 年《反不正当竞争法》修订增设“互联网专条”，专门规制利用网络从事生产经营活动中的不正当竞争行为；2019 年《反不正当竞争法》再次修订，将“电子侵入”作为获取商业秘密的不正当手段，同时提高了侵权赔偿上限，并增加举证责任转移制度；2020 年《刑法修正案(十一)》进一步加大了侵犯商业秘密罪的刑事追诉力度；2020 年最高人民法院发布《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》(以下简称“《商业秘密司法解释》”)，为商业秘密民事案件提供了系统性的裁判依据。

在此背景下，1998 年修订施行的《关于禁止侵犯商业秘密行为的若干规定》已明显滞后于实践需要。此次《规定》的出台填补了这一空白，使商业秘密保护规则在法律、司法解释与部门规章三个层面实现了有效衔接。

2. 《商业秘密保护规定》的性质

《规定》属于部门规章，直接适用于市场监管机关的行政执法活动，具有明确的行政法律效力。在司法层面，法院在认定相关事实和适用法律时并不受《规定》约束，但其对商业秘密认定标准、保护措施要求及侵权行为类型的细化，事实上为司法机关的裁量判断提供了重要参考框架。

从企业合规视角而言，《规定》不仅仅是外部监管规则，更是企业内部合规体系建设的重要参照，据此评估现有商业秘密保护机制是否满足行政和司法层面的合规要求：一方面，《规定》为企业提供了具体、可操作的合规指引，明确了监管机关在执法时的审查要点；另一方面，《规定》也揭示了企业商业秘密保护体系中的常见漏洞与薄弱环节，为企业完善内部制度建设提供了重要依据。

二. 《商业秘密保护规定》下保护商业秘密的主要风险

《规定》在明确执法标准的同时，也进一步揭示了企业在商业秘密保护实践中面临的系统性风险。总体而言，企业面临两类核心风险：一是自身商业秘密遭受泄露或被侵犯的风险；二是在经营活动中侵犯他人商业秘密的法律风险。

自身商业秘密遭受泄露或被侵犯的风险

1. 商业秘密认定风险

根据《反不正当竞争法》第 10 条第 4 款，《规定》第 5 条第 1 款，商业秘密须同时具备秘密性、保密性与价值性。《商业秘密司法解释》第 4 条列出了不能作为商业秘密主张保护的信息，包括：

该信息属于所属领域的一般常识或行业惯例；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等。可知，并非所有的内部信息均能受到商业秘密制度的保护，企业须能够清晰界定其主张保护的信息范围，并证明该信息符合上述构成要件。

在实践中，企业的专有商业信息与普通业务信息往往混杂共存，缺乏清晰界定。当商业秘密争议诉诸司法时，权利人在主张权利时，需要确定商业秘密的载体、具体内容(秘密点)，并说明其具备秘密性、保密性和价值性的法定条件。若企业事前未对内部信息资产进行系统梳理，不仅在诉讼中难以形成有效的初步举证，更将直接影响诉前行为保全申请的成功率。

2. 保护措施适当性风险

根据《反不正当竞争法》第 10 条第 4 款，《规定》第 9 条和《商业秘密司法解释》第 5 条和第 6 条，权利人须就商业秘密采取“相应保密措施”，保密措施需要与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相适应。

实践中，保护措施的适当性一直是司法实践中争议的焦点。在(2020)最高法知民终 538 号案中，最高院明确指出，权利人虽与员工签署了保密协议、制定并施行了保密管理制度、对研发厂房加设门锁限制来访，但上述措施均与权利人主张保护的技术秘密及其载体不具有对应性，不属于《反不正当竞争法》规定的“相应保密措施”。最高院在(2016)最高法民申 2161 号裁定中亦明确，劳动合同中仅有原则性保密条款，不足以构成对特定技术信息或经营信息进行保密的合理措施。

实践中，企业存在以格式劳动合同中的原则性保密条款替代针对具体商业秘密的保密安排、将签署保密协议等同于保密措施完备的误区，忽视了保密措施须与具体商业秘密信息及其载体相匹配的基本要求。一旦涉诉，存在因保密措施认定不足而不被认定为商业秘密的风险。

3. 侵权行为举证风险

权利人对所主张的商业秘密侵权行为负有举证责任。《反不正当竞争法》第 39 条规定了举证责任转移制度：权利人提供初步证据证明已采取保密措施且合理表明商业秘密被侵犯后，举证责任转移至涉嫌侵权人。《规定》第 20 条在行政执法环节引入了该机制：权利人提供初步证据证明涉嫌侵权人使用的信息与其商业秘密实质相同、且涉嫌侵权人具有获取该商业秘密的条件的，市场监管部门即可推定存在侵权行为，举证责任随之转移至涉嫌侵权人。然而，上述制度并不免除权利人提供初步证据的责任。

实践中，部分企业事前缺乏对商业秘密流转全链路的系统性记录，一旦发现遭受侵权，往往存在难以追溯他人获取、披露商业秘密的具体情况，尤其难以证明商业秘密系经由特定行为外泄，以及相关损害与侵权行为之间的因果联系的风险。

此外，若企业在劳动合同、保密协议或内部规章制度中，将特定行为(如未经授权接触保密信息、违规存储数据、私自传输文件等)明确界定为违约行为或违反劳动纪律的行为，则在诉讼或劳动仲裁中，也可直接以行为违规为由追究责任，在一定程度上避免商业秘密侵权认定的举证困难，降低维权成本与诉讼风险。

4. 数字经济环境下的电子化泄密风险

《规定》第 10 条新增“以电子侵入方式”获取商业秘密的侵权行为类型，并在第 2 款中对不正当手段进行细化：在无授权的情况下“擅自进入权利人的数字化办公系统、服务器、邮箱、云盘、应用账户等”或“擅自将商业秘密下载或者传输至不受权利人控制的电子邮箱、云盘等网络存储空间或者电子设备”。

随着企业信息化程度的持续深化，商业秘密载体已从传统纸质文件全面转向电子系统，商业秘密的泄露风险亦随之呈现出新的特征：其一，外部网络攻击手段日趋复杂，商业秘密系统性泄露的潜在损失大幅上升；其二，内部人员通过即时通讯工具、个人云盘或电子邮件等途径外传数据，行为隐蔽性强，取证难度高；其三，远程办公模式的普及进一步扩大了数据访问暴露风险。因此，结合《网络安全法》下关于数据分级分类和权限分配要求，保护系统安全、管控系统权限成为防止商业秘密泄密的重要一环。

侵犯他人商业秘密的法律风险

5. 员工流动带来的商业秘密侵权风险

员工流动是企业经营中的常态，但也是商业秘密侵权风险的高发环节。《规定》第 14 条第 2 款明确，第三人明知或者应知商业秘密权利人的员工、前员工、合作方或者其他单位、个人实施了侵犯商业秘密的违法行为，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。

对企业而言，在招募员工时，其一，若主动招募掌握竞争对手商业秘密的员工，并利用其所掌握的信息获取竞争优势，将直接构成侵权；其二，即便企业并无主观故意，若未建立有效的入职背景审查机制，在不知情的情况下使用了员工从原单位携带的商业秘密，同样可能被认定为“应知”而承担侵权责任。

6. 第三方采购中的商业秘密侵权风险

企业在采购第三方数据、技术或相关信息资产时，同样面临隐性的商业秘密侵权风险。根据《规定》第 14 条第 2 款，若供应商所提供的数据或信息含有他人商业秘密，而采购企业未对信息来源的合法性进行必要审查，则可能以“使用他人商业秘密”为由被追责，即便采购企业本身并无主观恶意。

因此，企业不能简单以不知情为由，向供应商采购可能含有他人商业秘密的数据、技术和其他信息资产，而应当采取审慎措施，防控侵权风险。

三. 商业秘密风险防范制度

针对上述风险，仅依赖保密协议等单一合同安排已难以满足商业秘密保护的现实需要。企业应将商业秘密保护纳入系统性的制度建设框架，从信息梳理、内部管控、人员管理到第三方风险防控，建立企业内部商业秘密风险防范机制。

1. 商业秘密梳理与分类分级制度

商业秘密保护体系建设的起点，在于对商业秘密进行系统梳理。企业应参照《规定》关于商业秘密认定要件的规定，对各业务单元的核心信息资产进行全面盘点，区分可受保护的商业秘密与一般业务信息，明确各项商业秘密的内容范围及其载体形式。

在分类层面，企业可按照信息性质将商业秘密区分为技术秘密(如核心研发配方、工艺参数、源代码、技术图纸等)、经营秘密(如客户名单、定价策略、供应商信息、商业计划等)等类别。商业秘密的分类工作可同时服务于《数据安全法》下的数据分类要求，企业可在同一流程中统筹完成商业秘密识别与重要数据识别。

在分级层面，企业应在上述分类的基础上，参照数据分级的逻辑，根据各项商业秘密的重要程度及泄露后对企业竞争优势和经营利益可能造成的实际损害，在每类商业秘密内部按秘密、机密、绝密三个级别进行分级，针对不同密级在访问权限、存储方式、传输要求及保密标识等方面设定差异化的保护要求，并严格限定各密级信息的可接触人员范围。

此外，企业应根据业务发展、技术迭代及信息重要程度的变化，定期对商业秘密分类分级结果进行复核更新，确保保护措施与实际风险持续匹配。

2. 商业秘密保护制度与内部规程建设

在完成商业秘密梳理的基础上，企业应针对不同类别的商业秘密，制定相应的保护规程，将技术管控措施与管理制度安排有机结合。

在技术层面，应根据商业秘密的重要程度，配套采取访问权限控制(基于最小权限原则)、数据传输加密、操作行为日志记录、异常访问告警等措施。上述技术措施与《网络安全法》下的网络安全保护义务高度重合，《规定》亦已将权限分级、操作日志留痕等网络安全合规措施纳入商业秘密保护措施的范围，企业在履行网络安全合规义务的同时，可同步满足商业秘密保护措施的要求。

在管理层面，除保密协议外，企业还应在劳动合同、员工手册及内部规章制度中，明确界定具体违规行为(如未经授权访问保密信息、违规外传数据、私自留存商业信息等)及相应的行为后果。

此外，企业还应建立离职员工商业秘密管理规程，涵盖离职前的商业秘密载体收回、信息系统权限注销，以及竞业限制条款的执行安排，形成完整的全生命周期保护机制。

3. 关键岗位员工的背景审查机制

对于拟招募的关键岗位人员——尤其是技术研发、核心销售及重要业务岗位——企业应在入职前开展系统的背景审查，评估潜在的商业秘密交叉风险。具体而言，审查内容应包括：该员工在前用人单位的具体职能与职责范围、所接触或掌握的核心信息类型，以及其工作内容与本单位研发、经营活动之间的重叠程度。

如果审查发现存在商业秘密交叉风险时，企业应在劳动合同及入职承诺书中明确约定：员工不得将前用人单位的商业秘密用于本职工作；如发现拟开展的工作可能涉及此类信息，应及时主动报告。上述约定不仅有助于管控企业自身的侵权风险，亦在客观上约束了员工从事相关违规行为的空间。

4. 第三方采购的商业秘密风险评估机制

在采购第三方数据、技术或相关信息资产时，企业应将商业秘密合规审查纳入供应商评估流程。对供应商所提供信息的来源合法性、知识产权权属及是否存在商业秘密侵权风险，开展必要的尽职调查，不能以“不知情”为由规避法律责任。

在合同安排层面，采购合同中应明确约定：供应商须就所提供信息的来源合法性作出明确陈述与保证，并在信息存在商业秘密瑕疵时承担相应赔偿责任。对于涉及数据采购的情形，还应结合《数据安全法》关于数据来源合法性的要求，同步评估数据合规风险。此外，企业在接收外部技术或数据时，应建立内部评审程序，并保留完整的审查记录，以备监管审查或侵权纠纷之需。

四. 结语

《商业秘密保护规定》的施行，既强化了行政执法的规范性，也为企业提供了系统梳理和完善内部商业秘密保护机制的重要契机。商业秘密保护的有效性，根本上取决于企业事前建立健全的制度体系，而非事后的被动维权。

建议企业在《规定》正式施行前，对商业秘密进行系统梳理与分级分类；在劳动合同和内部规章制度中明确违规行为的法律后果；建立关键岗位员工的入职背景审查机制；将商业秘密风险评估纳入第三方采购的合规审查流程。上述举措与《网络安全法》《数据安全法》等法律框架下的合规义务高度契合。履行网络安全合规义务本身即是构建商业秘密保护体系的有效路径，二者在数字化时代已是一体两面。企业可统筹规划、协同推进，在满足合规要求的同时，切实提升商业秘密保护的实效。

如您希望就相关问题进一步交流，请联系：



杨 迅

+86 21 3135 8799

xun.yang@llinkslaw.com

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

上海

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

北京

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

深圳

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

香港

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

伦敦

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



www.llinkslaw.com



Wechat: LlinksLaw

本土化资源 国际化视野

免责声明:

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

© 通力律师事务所 2026