拥抱数字化经济的商业秘密保护——首评《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》(下称"**《保护规定》**")，自 2026 年 6 月 1 日起施行。《保护规定》的出台回应了数字时代商业秘密保护的现实需求，在完善行政执法标准的同时，与《网络安全法》《网络数据安全管理条例》(下称"**《数据条例》**")相衔接。

《保护规定》落实了《反不正当竞争法》的相关规定，将《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》(下称"**《商业秘密司法解释》**")中经司法实践检验的标准吸收转化为行政执法依据，实现了行政保护与上位法以及司法实践的统一。同时，《保护规定》将《网络安全法》《数据条例》对企业提出的网络安全合规要求纳入商业秘密的保护措施的认定范围，比如权限分级、数据脱敏、操作日志留痕等。对企业而言，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。

一. 商业秘密的保护范围

《保护规定》沿用《反不正当竞争法》对商业秘密的定义及《商业秘密司法解释》关于技术信息、经营信息的界定，将数据、算法、计算机程序及其代码明确纳入技术信息的行政执法保护范围，为数字经济场景下企业核心技术资产的行政保护提供了直接的规范依据。

(一) 秘密性

《保护规定》第六条规定了"不为公众所知悉"的时间点与判定标准，与《商业秘密司法解释》第三条、第四条保持一致，明确为公众所知悉的信息经"整理、改进、加工"后形成的新信息，在符合不为所属领域相关人员普遍知悉且不易获得的前提下，可认定为不为公众所知悉。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

对衍生信息秘密性的认定体现了数字经济的特征。比如，单条来源公开的信息——如工商登记数据、学术文献或公开交易记录——本身不满足秘密性要件。但经过企业系统性收集、清洗、标注、整合后形成的数据集，该数据集就可能具有远超个别数据本身的价值，不同于个别数据的性质；只要该数据集在所属领域尚未为相关人员普遍知悉且难以轻易获取，即满足秘密性的认定标准。

(二) 价值性

《保护规定》第七条规定，商业价值是指"具有现实的或者潜在的价值，能为权利人带来商业利益或者竞争优势"，并进一步将生产经营活动中形成的阶段性成果、失败的实验数据及技术方案纳入具有商业价值的情形。

在数字经济背景下，商业价值的衡量不仅仅体现在直接经济利益上，而是呈现出鲜明的互联网经济特征：用户数量增长所带来的流量价值、成本费用降低带来的效率优势、研发时间缩短所体现的市场先占优势，以及交易机会增加所体现的竞争优势等，均可作为价值性要件的认定依据。

(三) 采取相应保密措施

《保护规定》第九条吸收了《商业秘密司法解释》第五条、第六条确立的保密措施认定标准及具体情形，明确保密措施须与所保护的商业秘密及其载体的性质、商业秘密的商业价值等因素相适应——保密协议固然是常见的保密措施，但仅凭协议约定可能不足以达到"相适应的保密措施"之要求。

在此基础上，针对远程办公、跨境协作等数字化工作场景，《保护规定》借鉴了《网络安全法》和《数据条例》下的要求，新增列举了"权限分级、数据脱敏、操作日志留痕"等保密技术措施。在数字经济时代，算法、代码、数据在云端传输已成常态，单纯依赖传统的物理隔离或制度约束已难以有效管控信息泄露风险，上述三项技术措施是企业在数字化场景下管控信息访问、保障信息安全传输和防范泄露风险的核心手段。

二. 商业秘密的侵权认定

《保护规定》第十条至第十四条落实了《反不正当竞争法》第九条第一款至第三款关于侵犯商业秘密行为的规定，在保留不正当获取、违反保密义务披露使用等侵权类型的基础上予以细化，将电子侵入确立为独立的不正当获取手段。

(一) 电子侵入

《保护规定》第十条第二款第三项规定，未经授权或超出授权范围，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，或者通过设置恶意程序、漏洞攻击等技术手段获取商业秘密的，属于不正当获取手段。

具体而言，本项涵盖两类情形：一是完全没有访问资格的外部电子侵入；二是持有一定系统权限但超出授权边界的内部越权访问。以数据爬取为例，通过植入恶意程序或绕过技术保护措施实施的黑客行为，落入本项规范范围；采用技术手段公然爬取他人数据的，虽然该些数据并不在网关之内(即无需绕过网关)，但是若目标数据并没有通过浏览器或移动终端向一般公众(或相关公众)展示或普遍可获得，那么该爬取行为也可能被认为是侵犯商业秘密的行为。

该条款与《网络安全法》(2025 年修正)第二十九条及《数据条例》第八条第一款关于禁止非法侵入他人网络、窃取网络数据的规定相互呼应，使同一侵权行为可能同时触发商业秘密与网络安全两套法律责任体系。当企业发现电子侵入行为时：

(1) 在商业秘密保护层面，可依据《反不正当竞争法》《保护规定》向市场监督管理部门举报，寻求商业秘密行政保护；亦可提起民事诉讼，主张损害赔偿。
(2) 在网络安全层面，可依据《网络安全法》向公安机关报案，追究侵权方的行政责任；涉嫌构成犯罪的，依法追究刑事责任。

(二) 超越授权权限

《保护规定》第十条第二款第四项规定，未经授权、超出授权范围或授权期限届满后，擅自将商业秘密下载或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电子设备，构成不正当获取手段。例如：

(1) 员工在项目结束后、离职前，将工作系统中的文件批量下载至个人网盘或设备；
(2) 被许可方在技术许可协议届满后，未按约定删除涉密技术文件，而是转存至内部服务器继续留用；
(3) 合作方在合同终止后，将合作期间接触的对方商业秘密保留在自有系统中。

上述情形的认定关键在于信息是否已转移至权利人无法有效管控的存储介质。一旦超出权利人的控制边界，无论事后是否实际加以利用或披露，侵权行为即告成立。

同样，超越授权范围或授权期限届满后擅自留存、传输商业秘密的行为，也可能同时触发商业秘密侵权、网络安全违规与合同违约三个层面的法律责任：

(1) 在商业秘密保护层面，权利人可依据《反不正当竞争法》及《保护规定》向市场监督管理部门举报或提起民事诉讼。

(2) 在网络安全层面，擅自将数据传输至不受控存储空间的行为，可能同时违反《数据条例》第十二条关于数据处理者须按照约定目的和方式处理数据的义务，触发行政责任。

(3) 在合同层面，若相关协议中已约定保密义务或数据处置要求，上述行为同时构成违约，企业可另行主张违约损害赔偿。

(三) 帮助侵权

《保护规定》第十三条规定，经营者不得教唆、引诱、帮助他人违反保密义务或权利人的保密要求，获取、披露、使用或允许他人使用权利人的商业秘密，包括：以明示或暗示方式怂恿、指使他人侵权；以物质奖励或职位许诺为手段诱导他人侵权；明知或应知他人侵权，仍提供资金、技术或设备支持等情形。

因此，竞争对手企业若以高薪或职务晋升为诱导，明示或暗示招募对象携带原单位商业秘密入职，招募方本身即构成本条规定的引诱侵权。

(四) 第三人"明知或应知"侵权

《保护规定》第十四条规定，第三人明知或应知他人实施了第十条至第十三条所列侵权行为，仍获取、披露、使用或允许他人使用该商业秘密的，同样构成侵犯商业秘密。判断是否"明知或应知"，应综合考量商业信息的保密程度、获取渠道与方式的合理性、交易价格、第三人与权利人的关系及行业惯例等因素。

在数字经济环境下，很多企业会采购数据，若供应方系通过非法爬取、越权系统访问或其他侵权手段取得相关数据，而企业在具备"明知或应知"条件的情况下仍予购入并投入使用，即可能被认定为帮助实施侵权，面临连带追责。因此，除要求供应方提供数据来源合法性声明外，企业在数据采购环节还应当进一步核查：供应方的数据来源说明及可供查证的支撑材料、数据采集所依据的授权文件或合法爬取凭证、所购数据集与市场同类产品的价格合理性对比等。

三. 数字化时代的商业秘密保护措施

《保护规定》第九条新增针对远程办公、跨境协作等场景采取"权限分级、数据脱敏、操作日志留痕"等技术保密措施的规定。这三项技术要求既是企业在数字化场景下进行商业秘密保护的有效手段，也是《网络安全法》《数据条例》对企业提出的网络安全合规要求——企业落实网络安全合规义务的过程，本身就是构建商业秘密保护体系的有效路径。

(一) 权限分级

权限分级管理要求企业对数据进行分级分类，依据岗位职能和实际业务需要，按照最小必要原则向员工授予相应的信息系统访问资格，确保每位人员仅能接触与本职工作直接关联的数据范围。

从《网络安全法》的角度，该法第二十三条第四项要求网络运营者采取数据分类措施。《数据条例》第九条要求网络数据处理者采取访问控制、加密、备份等技术措施，保护网络数据免遭非法获取或泄露。根据《个人信息保护合规审计管理办法》及其附件《个人信息保护合规审计指引》，在个人信息保护合规审计中，是否合理制定个人信息处理操作权限亦属重点核查事项。

从商业秘密保护的角度，权限分级管理一方面可以限制商业秘密的接触范围，直接减少泄露风险；另一方面，在商业秘密涉嫌被侵犯时，权限记录是证明权利人对相应商业信息采取保密措施的直接证据。

在操作层面上，企业只需建立一套权限分级管理体系，即可同时满足网络安全合规与商业秘密保护的要求。例如：以岗位为维度，明确不同岗位可访问的系统范围；设置访问权限动态调整机制，在人员调动、岗位变更及离职时及时调整或撤销访问权限；对涉密文件的对外传输行为设置技术拦截或审批管控等。上述措施在网络安全和商业秘密保护领域均需落实，企业无需为此分别建立独立的管理体系。

但需要注意的是，网络安全和商业秘密保护的分级标准不同，进而影响权限设置的依据，企业不能简单以网络安全的数据分类标准替代商业秘密的分级判断。网络安全合规下，分级依据是数据对国家安全、公共利益及个人权益的影响程度；商业秘密保护下，分级标准由企业自主判断，以信息对企业竞争优势的重要程度为依据。从企业实际管理出发，应综合考虑国家、公共利益和企业自主利益的多维度分级分类，在满足《网络安全法》下信息分类分级的监管要求的同时，做好商业秘密的保密分级安排。

(二) 数据脱敏

数据脱敏是指对某些敏感信息通过脱敏规则进行数据变形，实现敏感隐私数据的可靠保护。

《网络安全法》(2025 年修正)第四十四条第一款规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。据此，经适当脱敏处理后的数据，在特定流通场景下对外披露，不构成对个人信息的违规提供。

在商业秘密保护框架下，企业可以将脱敏版本提供给合作方用于开展合作或提交监管机构用于审计核查，同时主张原始数据所包含的敏感信息始终处于保密状态，对外披露的脱敏版本不构成秘密性的丧失。

因此，建议企业根据商业信息的内容，按照不同使用场景制定差异化的脱敏规则，对外合作、监管报送、内部测试各有侧重，并将脱敏操作同步纳入日志记录范围，实现全流程可追溯管理。

(三) 操作日志留痕

操作日志留痕要求在信息系统层面对用户或系统的各类操作行为进行记录并保存相关数据，以便事后能够追溯和审查操作行为的具体内容、时间、操作主体等信息。

《网络安全法》第二十三条第三项明确要求网络运营者采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。这一规定将操作日志留痕确立为网络安全的法定义务。

从商业秘密保护角度，操作日志承担以下核心功能：(1)侵权行为的证据固化。日志记录可以直接证明侵权人的访问时间、下载行为及传输目的地。在商业秘密涉嫌被侵犯时，《保护规定》要求权利人向市场监督管理部门举报时提供商业秘密涉嫌被侵犯的具体线索，日志记录是"有渠道获取"要件的直接证明；(2)对内的监督和预防。员工知悉操作行为被全程记录，本身即对潜在的信息外泄行为，尤其是临近离职前的批量下载行为形成威慑。

需要注意的是，网络安全和商业秘密保护对日志留存期限的要求存在差异。《网络安全法》规定不少于六个月。从商业秘密保护角度，由于侵权行为往往在发生后相当一段时间才被发现，建议企业对涉及核心商业秘密的系统适当延长日志留存周期，以确保在启动维权程序时仍能调取有效的历史操作记录。

四. 结语

《商业秘密保护规定》的出台，不仅体现在商业秘密保护客体的范围扩展与行政处罚体系的标准化，更在于从制度层面明确了数字经济时代商业秘密保护的内在逻辑——企业在落实网络安全合规义务过程中所构建的技术管控体系，同步也在为商业秘密的维权主张积累保密措施充分性证明与证据储备。履行网络安全合规义务与构建商业秘密保护体系，在数字化时代已是一体两面。

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	北京	深圳
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	伦敦	
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	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