数据合规制度不再是“防御性投入”——速评《商业秘密保护规定》

作者：潘永建 | 邓梓珊

2026 年 2 月 24 日，国家市场监督管理总局发布第 126 号令《商业秘密保护规定》(以下简称“新规”)，自 2026 年 6 月 1 日起施行。新规在保护客体、保密措施、侵权认定、举证规则以及法律责任等方面做了较大的修改，很大程度上体现了《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》(以下简称“司法解释”)的内容，代替了原国家工商行政管理局 1995 年颁布实施的《关于禁止侵犯商业秘密行为的若干规定》(以下简称“旧规”)。

对数据合规从业者来说，新规最具吸引力的看点是：商业秘密保护制度第一次从立法上回应数字经济发展需求——数据、算法、AI 模型、代码等新生产要素被明确保护范围之内；权限分级、数据脱敏、操作日志留痕等新技术手段第一次在部门规章中被规定为“合理保密措施”。本文主要从业务数据合规角度，对新旧规定的三方面重要变化进行解读，并就企业(特别是算法及人工智能应用研发企业)提出合规指引建议。

一. 保护客体的扩张：数据资产的法律身份确认

(一) 清单式列举商业秘密类型

新规第 5 条采用列举方式明确商业秘密的客体范畴，在技术信息项下，首次将“数据、算法、计算机程序、代码”纳入其中；而在经营信息项下，则将“与经营活动有关的数据”也一并纳入其中，意味着数据在商业秘密法体系中有其“技术信息”和“经营信息”的双面法律身份，企业的具体数据类型不同可以选择不同的方式来进行保护。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

对于算法及人工智能应用开发企业，新规的保护范围具有直接针对性——算法、源代码、AI 模型、训练数据、计算机程序等均被明确纳入技术信息范畴。实践中，人工智能企业的核心竞争力往往表现为复合性技术资产，包括算法架构、模型权重参数、训练数据集、微调方法及系统提示词等。新规的前述规定为上述新型商业秘密形态提供了明确的法律依据。需要指出的是，新规并未限定受保护代码或算法的规模或完整度，局部代码片段、中间版本模型及尚未上线的算法原型，只要满足“非公知性要求”，均可主张商业秘密保护。

(二) 阶段性成果与失败数据及方案的价值认定

新规第七条特别规定，生产经营活动中形成的阶段性成果或者失败的实验数据、技术方案等，如能为权利人带来资产增加、营业收入或者利润增长、用户数量增长、成本费用降低、研发时间缩短、交易机会增加、商业信誉或者商品声誉提升等商业利益或者竞争优势的，属于具有商业价值的情形。该条款的制度逻辑在于：失败的实验数据能够为竞争对手节约研发成本和试错时间，避免其重复已知无效的技术路径，因此具备独立的竞争优势价值。对于人工智能开发者而言，模型训练过程中的失败版本、被废弃的算法路径及不合预期的超参数组合，以往被视为沉没成本，且一旦泄露极难救济，新规实施后可作为商业秘密保护的合法对象。

(三) 客户信息保护的精细化

新规第五条将经营信息中的客户信息从传统的“客户名单”扩展为“客户的名称(姓名)、地址、联系方式以及交易习惯、意向、内容等信息”。这意味着企业基于长期交易积累的客户画像、购买偏好、需求规律等深度数据，可独立于客户名单作为商业秘密主张权利，降低了权利主张的整体性门槛。

二. 技术保密措施的法定化：从合同约束到系统防护

新规第九条首次在部门规章层面列举了八类合理保密措施，在 2020 年司法解释的基础上亦进行了完善扩充：

(1) 签订保密协议或者在合同中约定保密义务；
(2) 通过建立规章制度、开展培训、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；
(3) 禁止或者限制进入涉密的厂房、车间、实验室、办公室等生产经营场所或者对其进行区分管理；
(4) 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；
(5) 以标记、分类、隔离、加密、封存、限制能够接触或者获取商业秘密及其载体的人员范围等方式，对商业秘密及其载体进行区分管理；
(6) 对能够接触、获取商业秘密的计算机设备、网络设备、存储设备等，采取禁止或者限制使用、访问、存储、复制等措施；
(7) 要求离职员工登记、返还、清除、销毁其接触、获取的商业秘密及其载体，继续承担保密义务；
(8) 采取其他合理保密措施。

上述保护措施集中体现了数据保护体系建设中最关键的环节，数据分类分级管理、权限管控、数据脱敏、以及操作日志留痕，为企业加快建设、完善数据保护体系制度提供了充分的且有实际效用的理由。该条款释放了三项制度信号。

第一，技术措施与合同约束被置于同等重要的法律地位。旧规时期，相当比例企业的商业秘密保护停留在签订保密协议的层面，一旦发生侵权纠纷后难以证明“采取了合理保密措施”。新法还引入了司法解释中明确的“比例原则”衡量保密措施是否合理。保密措施与商业秘密及载体的性质、商业价值等因素需相适应。这就意味着如果仅有协议而无实际技术管控，可能被认定为未采取合理保密措施，从而影响商业秘密的权利基础。但相应的，所有的数据都应采取同等强度的保密技术手段予以保护，企业可根据数据的价值以及敏感度来决定相应的保护方式。

第二，权限分级成为合规的底线要求。企业应当根据最小权限原则，依据岗位职责、涉密等级及业务需要，差异化授予系统访问权限。核心算法、核心数据集及训练环境的访问应严格限制，并建立审批与复核机制。

第三，操作留痕是事后举证的重要依据，在发生泄密纠纷后，企业能否证明已经采取了合理的保密措施，很大程度上依赖于日志记录的有效性和可回溯性。新规定已将操作日志留痕作为法定合理措施之一，企业应对涉密数据访问、下载、传输等重要操作实施全程留痕，应当保存不少于 6 个月的日志记录。

三. “接触+实质相似”推定规则的建立

新规第二十条确立了推定侵权规则：权利人能够证明涉嫌侵权人所使用的信息与商业秘密实质性相似，且涉嫌侵权人有接触商业秘密的条件，市场监管部门即可推定侵权行为成立，举证责任转移至涉嫌侵权人，由其证明信息具有合法来源。值得注意的是，旧规所采用的表述是“获取”商业秘密，而司法解释针对员工或前员工采用的表述是“接触”，可见新规采用了范围更大的表述。

这一规定大大减轻了权利人的举证负担。在 AI 企业的算法剽窃或者模型盗用案件中，只要权利人能够证明“被告有机会接触到自己的算法或者训练数据”并且“被告的输出结果与自己的结果实质性相同”，就可以适用推定制度。就“有机会接触”这一要件而言，该条规定再一次印证了企业数据分类分级、权限管控及日志留痕的重要性。

四. 企业数据合规实务建议

基于新规的制度变化，建议企业从以下六个方面完善商业秘密保护体系。

(一) 系统梳理涉密数据资产并进行分类分级管理

(1) 建议企业参照新规第五条规定的保护对象清单，对涉及 AI 开发与运维的信息进行盘点：关键算法、关键模型及其相关参数;
(2) 程序代码及相关代码库;
(3) 用于训练的人工智能算法的数据样本(包括基础数据、标记数据);
(4) 用于测试或者验证人工智能算法的数据样本(包括中间数据、无效数据);
(5) 用于运行人工智能应用的关键词表、决策树等；用户画像的相关数据;
(6) 用户消费记录等消费偏好数据;
(7) 供应链、成本数据等。

在此基础上进行分类分级管理，明确各项资产所属所有者、密级、所在位置、允许访问人员范围，确认这些具有商业价值的信息是否满足新规保护条件。

(二) 部署与密级相匹配的技术防护措施

根据新规第九条第四项的要求，建议企业落实以下技术措施:
(1) 权限分级：落实最小权限原则，核心算法及数据集应采用审批后访问模式，远程访问须经多因素认证。
(2) 数据脱敏：用于开发测试环境的非生产数据应当实施脱敏处理，避免涉密信息在非受控环境中暴露。
(3) 操作留痕：对涉密数据的创建、访问、修改、下载、传输、删除等关键操作实施全流程日志记录，日志留存不少于六个月，并定期审计。
(4) 部署数据防泄漏系统：对涉密数据的外发行为(邮件、云盘、外部存储设备、打印等)实施监控与阻断，建立异常行为预警机制。

(三) 完善内部制度体系与对外协议文本

企业应当建立或修订商业秘密管理制度，明确定密标准、密级划分、权限管理、载体流转、远程办公、跨境协作、泄密报告及责任追究等核心内容。三类核心协议须同步更新:
(1) 劳动合同与保密协议：明确数字化资产的保密义务、离职后保密期限、涉密载体返还及数据删除责任。
(2) 竞业限制协议：精准适用于核心算法工程师、模型训练人员等核心涉密岗位。
(3) 对外合作协议：在与云服务商、数据标注商、模型微调服务商等第三方合作时，明确约定数据使用范围、保密义务、侵权责任及审计条款。

(四) 构建覆盖人员全周期的管理机制

(1) 入职环节：对核心涉密人员进行背景调查，签订保密协议，完成保密告知与岗前培训。
(2) 在职环节：定期开展商业秘密保护培训，将保密履职情况纳入绩效考核。

(3) 离职环节：严格执行交接流程，收回全部涉密载体，关闭系统/云端权限，督促删除个人设备中的涉密数据，执行离职保密告知与合规审查，必要时启动离职审计。

(五) 建立存证机制与应急预案

根据新规第四条鼓励企业通过认证、存证等方式强化商业秘密保护的精神，建议企业对核心商业秘密通过具有公信力的第三方存证平台进行事前存证，留存“在何时、由谁、以何种形式持有该秘密”的完整证据链。同时建立商业秘密泄密应急预案，明确事件响应流程、证据固定机制(特别是电子证据)、内部调查程序及外部举报渠道。

(六) 关注司法实践动态

最近的司法案例也传递出了清晰的导向。比如，2026 年广州知识产权法院在“虚拟数字人”技术秘密案中采用惩罚性赔偿判赔四百九十五万元，其中，原告构建起的保密制度包括保密协议、数据库私有化部署、分级权限管控、加密通信传输，在一定程度上被法院采信作为“采取了合理的保密措施”。该案例正说明了人民法院对于是否采取合理的保密措施的认定，并不仅仅看公司有没有制定保密制度，而要看该保密制度在实践中是否能够产生有效的管控痕迹。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

邓梓珊
+86 21 6043 3793
susan.deng@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