企业数据商业秘密司法认定研究

陆满鑫

沈阳工业大学文法学院，辽宁沈阳，110870；

摘要：在数字经济时代，企业数据作为核心生产要素，其商业秘密保护对维护市场公平竞争与企业创新活力至关重要。当前我国企业数据商业秘密司法认定面临诸多难题，秘密性要件中“公众”“普遍知悉”标准模糊，价值性要件缺乏适配不同行业的统一评估尺度，保密性要件因数据载体多样化导致“合理保密措施”认定困难。本文立足司法实践，围绕三大要件展开研究，提出明确数据组成区别化的秘密性标准、细化行业特性差异化的价值性标准、完善不同载体类型化的保密性标准等优化路径，以期为完善相关司法规则、推动数据要素市场健康发展提供理论参考与实践指引。

关键词：企业数据；商业秘密；司法认定

DOI：10.69979/3029-2700.26.02.074

1 企业数据商业秘密保护概述

数据作为新生产要素，伴随第四次信息革命和产业革命到来，已成为数字经济时代的核心生产要素，对实体经济与虚拟经济发展、市场主体竞争优势获取具有关键作用。然而，受数据竞争市场驱动，部分企业通过非法抓取、诱导员工泄露等不正当手段侵占他人数据，不仅侵犯数据生产者劳动成果，更打破投入到收益再到投入的良性循环，导致数据配置效率下降、市场失灵。

鉴于此，本文以企业数据商业秘密的司法认定为研究核心，首先梳理企业数据商业秘密法律保护的理论基础，进而系统检视当前司法实践中秘密性、价值性、保密性要件认定存在的问题，最终探索针对性的优化路径，以期为完善企业数据商业秘密保护的司法规则、推动数据要素市场健康发展提供理论参考与实践指引。

2 企业数据商业秘密司法认定问题检视

2.1 秘密性要件司法认定标准模糊

数据时代的技术革新与数据生产要素化，推动数据在开发利用、交易流转、协同计算等过程中不断打破由单一主体控制信息的原始格局。企业与用户、平台与合作方、跨行业机构间的高频数据交互，这种变革既源于数据价值挖掘对跨域资源的依赖，也因数据交易流通中权属拆分、利益共享的需求而加剧，最终形成多主体深度参与的多样化、复杂化数据组成。根据 2025 年现行有效的《中华人民共和国反不正当竞争法》第十条规定，“本法所称的商业秘密，是指不为公众所知悉、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”，明确将“不为公众所知悉”“具有商业价值”“经权利人采取相应保密措施”列为三大要件，其中“不为公众所知悉”是秘密性认定的基础。但该法及配套司法解释均未对“公众”“相关人员”“普遍知悉”等核心术语的内涵作出明确界定，进一步导致司法实践中面对多主体深度参与的多样化、复杂化数据组成产生的认定标准混乱与裁判说理不足。

从“不为其所属领域的相关人员普遍知悉”这一法定要件的适用来看，术语模糊性在多主体数据场景中引发的争议更为突出。“普遍知悉”的程度判断同样面临法律适用难题。当待认定数据包含“公开基础信息与非公开衍生信息”时，现行法律未明确“部分公开成分是否影响整体数据的秘密性”，部分法官为规避对“普遍”这一模糊概念的论证，直接援引司法解释中的列举情形机械比对，忽视非公开衍生部分的商业价值与权利人的保密努力。最高法在审理中明确指出，秘密性认定需穿透单一信息要素的公开属性，综合考量权利人在配方研发、原料筛选中的人力物力投入，以及与核心员工签订保密协议等措施的有效性，最终认可了涉案信息的秘密性。这一裁判逻辑恰恰直指当前数据融合场景下的认定痛点——仅以部分公开数据片段否定整体集合的秘密性，本质上是对“普遍知悉”标准的机械适用。

2.2 价值性要件司法认定标准宽泛

数字经济时代，区块链、人工智能、大数据服务等新兴行业加速崛起，各行业数据的生成方式、使用场景与价值发挥方式存在显著差异，这使得企业数据的商业价值要件的商业秘密司法认定面临突出困境。商业价值

是与秘密性、采取合理保密措施并列的构成要件，是指数据需能为企业带来直接经济利益或市场中的竞争优势。然而新兴行业与传统行业之间、新兴行业与新兴行业之间的特性差异越来越大导致该要件的司法认定标准存在困难。

在电商平台、市场调研机构等以市场信息为重要商业秘密的行业，市场信息对其能否在市场竞争中能否取得一定优势起到了核心命脉的作用。例如某生鲜电商基于城市居民购买频次、品类偏好形成的备货数据，可降低库存损耗率，直接提升盈利水平。因此此类数据多为企业通过投入大量人力、物力开展用户追踪、市场调研所积累，例如电商平台的区域用户画像数据、调研机构的细分领域风险报告等。但司法实践中，该商业价值究竟对企业的竞争力存在多大影响，对企业在市场中的生存死亡产生多大影响的认定存在明显难点。一方面，不同行业对市场信息的时效性要求差异较大；另一方面，部分公开数据经整合分析形成的衍生信息，其稀缺性与公共领域信息的边界模糊，难以直接判断是否具备商业秘密所需的价值独占性。

2.3 保密性要件司法认定标准笼统

当前商业秘密的信息载体已呈现显著多样化态势，涵盖物理载体、电子载体及隐性知识载体等多种类型。物理载体侧重空间隔离与标识管理，电子载体依赖技术屏障的强度与稳定性，隐性知识载体则强调义务人的认知与行为约束。

载体的差异直接导致“合理保密措施”的认定面对差异化的难题。对于物理载体，若采取保险柜存储、涉密区域门禁等措施，且标注“保密”标识，通常可认定合理，但未进行交接登记的 U 盘等移动载体可能因管控疏漏被否定；隐性知识载体需通过专项保密培训、客户档案分级管理等证明保密意图，仅签订通用保密协议而无具体指向性措施时，往往难以被认可。

这种立法层面的粗疏难以适配载体多样化带来的认定需求。物理载体的移动性与电子载体的技术迭代性、隐性知识载体的非物化性，使得统一的“合理”标准缺乏可操作性。由此导致权利人举证难度不均，部分企业因措施未达法官个案认知的“合理”标准败诉，或为满足模糊标准过度投入合规成本，最终影响商业秘密保护的公正性与效率。

3 企业数据商业秘密司法认定优化路径

3.1 明确数据组成区别化的秘密性标准

在数据要素流通与多主体协同开发的背景下，数据组成方式日益呈现出多主体贡献、多类型融合、多场景共享的多样化特征，这种变化在法律层面直接加剧了商业秘密“秘密性”认定的困境。现行法律对商业秘密秘密性的认定标准，仍停留在单一主体控制的传统场景，未适配多方参与的数据形态。亟需围绕“不为公众所知悉”这一核心要件明确区别化标准，细化不同数据组成的差异化认定标准。

区别化标准的核心是针对不同属性数据组成的商业数据，设定认定标准梯度化的“不为公众所知悉”认定标准。按数据的产生来源划分，商业数据可以分为由原始基础数据组成的数据和在原始数据基础上产生的衍生加工数据。原始数据由例如用户姓名、联系方式等公开可采集的信息组成，衍生加工数据由经过企业在原始数据的基础上进行清洗、分析、开发等系统化实质性加工的数据组合而成。二者本身就由不同属性的数据类型组合而成，二者“不为公众所知悉”的认定标准也应有所区别。对于原始数据组成的商业秘密，脱敏处理也是其秘密性的来源之一。脱敏处理的核心是剥离数据中能直接或间接定位到具体主体的信息，去掉识别性，确保数据无法关联到特定对象，这种无法还原性也能产生原始数据数据集合的秘密性，同时保留数据的统计或分析价值。

3.2 细化行业特性差异化的价值性标准

不同行业的数据价值生成逻辑存在本质差异。例如电商、市场调研行业的价值源于信息差带来的市场预判优势，算法驱动型行业的价值依赖智力与劳动投入形成的技术壁垒。若沿用统一的价值性认定标准，既会导致低价值数据被过度保护，也可能让高投入数据因无法量化价值而错失保护。因此，应基于各行业数据的竞争优势来源，构建根据价值来源区分认定维度并细化举证规则的差异化价值性认定标准体系，同时契合商业秘密制度保护创新与维护市场秩序的双重目标。

对于在电商平台、市场调研机构等以市场信息为重要商业秘密的行业，其数据商业价值的核心是通过独有信息抢占市场决策先机，故应当充分考虑信息稀缺性与时效性对市场竞争优势的催生。可以通过举证将“抽象价值”转化为“具体关联”，避免企业仅以数据投入成本高为由主张价值。对于稀缺性的举证应当要求企业提供数据采集的“独特渠道证明”，如与独家合作商户签订的信息共享协议、针对特定人群的定向调研问卷，证

明数据无法通过公开渠道或常规调研获取。对于时效性的举证需提交数据与经营决策的直接关联证据。

医疗 AI、金融科技、自动驾驶等以算法程序为核心竞争力的行业，其数据价值的核心是通过持续劳动投入形成的技术壁垒，因此着眼于劳动成本与商业价值关联度量化需建立劳动投入合理性与实际应用效果的动态关联标准，避免仅以投入成本高或技术先进单一维度认定价值，同时防止无效投入数据挤占保护资源。此类行业的数据价值源于投入与效果的正向循环，即劳动投入决定技术精度，技术精度决定商业收益。若仅投入大量工时却未提升技术效果，则不具备商业秘密价值。举证责任也应当进行细化要求，通过投入证据与效果证据的相互印证，证明价值的真实性。投入证据是指企业对劳动投入的举证，例如企业明确记载投入的具体维度与合理性。效果举证是指以算法程序的应用效果为证明对象进行的举证，效果举证需提交数据在实际场景中的价值转化具体证据，避免空泛主张技术价值。两种证据相互印证才能证明投入与效果之间的关联关系，进而证明劳动投入对价值性的催生。

3.3 完善不同载体类型化的保密性标准

司法实践中应基于载体的物理属性、技术特征与管控逻辑，建立差异化的保密措施审查标准，实现通过区分载体类型，进而区分保护需求，最终审慎认定措施合理性的认定逻辑。对于物理载体，应当重点审查保密措施对空间隔离与流转管理的实施程度，例如针对纸质文件、实物样品等物理载体，企业是否对涉密区域采用门禁分级管理、采用指纹与密码双重验证的分级模式，对纸质文件、实物样品采用保险柜存储，是否定期盘点，在文件上标注保密标识且限定知悉范围，再结合交接登记台账等证据，来认定其保密措施具备合理性；对于员工经验、技术诀窍等非物化信息，审查企业是否通过专项保密培训明确客户沟通话术、生产工艺诀窍等隐性知识的具体指向范围，是否建立划分技术岗与销售岗知识边界的岗位保密职责清单；

另一方面，在司法认定过程中应优化权利人的举证指引，通过要件化举证降低证明难度。司法实践中可引导权利人以载体性质识别为出发点进而对保密措施实施的现实作用进行举证，最终证明确实存在保密隔离效果为最终目的展开举证。例如首先明确主张保护的商业秘密属于云储存载体中的商业秘密信息，其次提供云储存服务商的相关资质和服务协议，以及对云储存服务商的保密能力尽到了合理审查义务，最终证明云储存的相关流程完备稳定，确有一定实际效果，例如提供过往未发生泄露、异常访问被拦截等能证明措施实际效果的记录。

4 结语

企业数据作为数字经济时代的核心生产要素，其商业秘密的司法认定不仅是知识产权保护领域的关键议题，更直接关系到数据要素市场的有序运行与企业创新活力的释放。当前，法律条款对“普遍知悉”“合理保密措施”的细化仍显不足，跨行业数据价值评估的客观标准尚未形成，多主体协同场景下的利益平衡机制也需进一步完善，这些问题仍需在后续立法修订与司法实践中持续探索。未来，需以司法解释为抓手，进一步明确不同数据类型的认定规则；以行业需求为导向，构建适配电商、AI、金融等领域的数据价值评估体系；以技术发展为支撑，完善电子载体、隐性知识载体的保密措施审查标准，最终实现企业数据商业秘密“保护”与“流通”的动态平衡。

参考文献

[1]咎祯媛.企业数据不正当竞争的法律规制路径[J].中国价格监管与反垄断,2025,(10):58-61.

[2]李晓菲,蒋万庚.新质生产力视域下企业数据的赋权正当性与制度构想[J].山西大同大学学报(社会科学版),2025,39(04):32-38.

[3]马一德,汪婷.生成式人工智能驱动下企业数据商业秘密保护制度调适[J].山东师范大学学报(社会科学版),2025,70(04):107-120+181.

[4]胡开忠.数据知识产权赋权理论之质疑[J].法学,2025,(10):114-131.

[5]马一德,汪婷.生成式人工智能驱动下企业数据商业秘密保护制度调适[J].山东师范大学学报(社会科学版),2025,70(04):107-120+181.

[6]崔国斌.新酒入旧瓶：企业数据保护的商业秘密路径[J].政治与法律,2023,(11):2-23.

作者简介：陆满鑫（1997-），女，汉，硕士在读，研究方向为：法学