社会科学进展
2026 年 4 月第 8 卷第 4 期

算法监管与商业秘密保护的冲突及其协同路径

黄　好

武汉工程大学，武汉

摘　要 | 随着算法在数字经济中的广泛应用，算法的法律规制与算法商业秘密保护之间的冲突日益凸显。从算法法律规制与商业秘密保护的内在机理分析，算法同时具备高风险特性与监管要求、高价值属性与保密需求。从算法应用的典型场景出发，“黑箱与透明”“私权与公益”“价值与风险”三组矛盾，是算法监管与商业秘密保护内在冲突的关键症结所在。算法监管与商业秘密保护的协同机制，需要从“算法备案”优化，构建分级分类的算法监管框架；把握“算法公开”限度，厘清“算法公开运行逻辑”边界；“内外监管”协作，打造政府规制与内部监督协同模式；“监管能力”提升，强化算法监管机构专业化水平，四个方面构建。

关键词 | 算法监管；商业秘密；算法黑箱；算法透明

1　问题的提出

作为数字经济的核心要素，算法已深度融入经济社会生活之中。随着生成式人工智能的发展，算法的应用场景将进一步扩展。本文所研究的算法并非广义上“建构社会秩序的一种特殊理性形式[1]”也并非狭义上“已被编码的程序[2]”，而是指人类和机器交互的决策，即人类通过代码设置、数据运算与机器自动化判断进行决策的一套机制[3]。

算法的深度应用带来了精准性推荐、定制化服务等许多正面效应，但也带来了系列连锁负面反应。以外卖、购物等电商平台崛起为例，其依托推荐算法为用户提供精准服务、创造多方收益的同时，也引发了“大数据杀熟”“算法黑箱”等问题。用户逐渐察觉算法推荐的“区别对待”，商家陷入不买“流量推送”就难入推荐榜单的困境，配送算法的优化更让外卖骑手的送餐时间被不断压缩。可见，算法作为提升用户粘性与竞争优势的核心资产，往往被企业视为核心商业秘密严格保护。面对监管，企业常陷入“公开即泄密”与“合规披露”的两难困境。面对用户透明诉求，也多以商业秘密为由拒绝公开，仅赔付或简略说明。本文旨在深入剖析算法监管与商业秘密保护之间的内在冲突，探索二者的协同路径，以期实现各方期待的“算法正义”。

2　算法法律规制与商业秘密保护的内在机理

算法的法律规制与商业秘密保护分别代表着社会公众与算法控制者相对立的价值诉求[4]。前者旨在打破“算法黑箱”，保障公众知情权与数据隐私；后者则基于算法作为“新质生产力”的高价值属性，维护企业保密的正当权益。

作者简介：黄好，武汉工程大学硕士研究生，研究方向：民商法、知识产权。
文章引用：黄好. 算法监管与商业秘密保护的冲突及其协同路径 [J]. 社会科学进展，2026，8（4）：303-307.
https://doi.org/10.35534/pss.0804054

2.1 算法的高风险特性与监管要求

算法是一套基于设计目的的数据处理指令总和，因其本身固有的设计、训练数据、模型结构等特性会产生内生性风险，而其广泛的应用场景也放大了这种风险。

算法运行带来的数据安全风险，凸显现有监管体系仍存在规则细化不足、覆盖不够全面的问题。据Cyber Haven调查，普通公司每周向ChatGPT泄露敏感数据数百次，而ChatGPT将这些数据融入公共知识库，并可能将其共享其他用户。OpenAI就曾因漏洞导致用户聊天记录标题暴露。当前我国算法监管体系的管控对象主要是违法不良信息，面对算法模型深度赋能企业背景下的商业秘密保护、信息泄露与权利救济难题，还缺乏明确规定。此外，算法运行潜在的数据隐私风险，要求监管体系发挥实质性作用。算法运行优化依赖海量数据“投喂”，由此世界范围内普遍建立以“同意与披露机制”为基石的治理体系。该机制的理论基础在于，若企业能够提供充分信息，使个人能够基于知情作出同意决定，则市场可以较小的成本达到监管效果。但对于普通用户而言，若想进入数字世界，必须同意隐私被追踪获利，面临“同意负担”。即便理解条款也无力更改，或被迫接受，或默许不阅读条款的风险，缺乏真正选择权。尽管《互联网信息服务算法推荐管理规定》设置了申诉和投诉举报入口，但重点在于算法服务提供者的义务设置，忽略了对用户“同意负担”的实质审查，难以在个人隐私保护上发挥实质性作用。

2.2 算法的高价值属性与保密需求

算法的高价值属性决定了企业的保密需求。一方面，算法的价值性来源于企业巨额的人力、物力与资本投入。即便基础技术源于公共资源，但从源代码到目标模型仍需大量数据调试与参数优化，其智力成果属性已获司法判例认可。另一方面，算法的“高价值性”表现为其带来的经济效益与竞争优势。以搜索引擎为例，算法差异直接决定了用户体验、用户群体及市场份额。适应市场的算法能形成竞争壁垒，一旦泄密，对企业竞争地位的毁损将难以估量。因此，企业普遍具备强烈的算法商业秘密保密需求。

算法的高价值与保密需求契合商业秘密的构成要件。同时，受制于“智力活动规则”属性及信息公开要求，算法难以归入版权与专利保护范畴，反不正当竞争法保护的事后性与传统民法对无形财产认识的局限性，也使得商业秘密保护成为算法最无争议且适宜的保护模式[5]。国内司法解释已明确将算法纳入技术信息范畴，域外立法与实践也普遍将算法纳入商业秘密保护范围，体现了国际共识。

3 算法监管与商业秘密保护的内在冲突

在“算法+应用场景”结构中，算法作为赋能工具，应用场景作为赋能领域，二者形成“方式”与“领域”的叠加关系[6]。因场景价值多元，监管需超越单纯技术视角。

3.1 黑箱与透明：算法运行机制与透明中立竞争冲突

算法的“黑箱”特性，即内隐性及知识产权保护需求与市场竞争的透明性要求存在显著冲突。

如Epic Games诉Apple案中，Apple被指利用App Store算法通过限制开发者、优先推荐自家应用以垄断市场。法院虽未认定苹果违反反垄断法，但指出其部分政策不公平，并发布禁令要求苹果允许开发者提供其他支付选项。Topkins案中，定价算法被用于隐匿价格共谋以规避监管。亚马逊招聘算法及Facebook广告算法则因训练数据偏差导致性别及种族歧视，暴露了算法的非中立性。这些问题既源于算法技术复杂性与场景价值冲突，亦源于企业对数据算法的非对称优势。监管部门易被边缘化，且受限于技术手段落后，难以对算法进行及时审查与纠偏。

3.2 私权与公益：企业保密需求与公众算法知情冲突

“算法共谋”“算法歧视”等行为引发了公众对算法规制的呼声，但实务中法院常以商业秘密保护为由拒绝算法披露诉求，易被公众误解为“算法霸权”的保护伞，私权与公益冲突突出。

亿桐公司与百度公司服务合同纠纷案中，百度公司以商业秘密保护为由拒绝披露其反作弊机制所涉及的算法、公式、逻辑等。法院认为，百度公司享有对其核心技术进行商业秘密保护的权利，支持了百度公司的主张。该案反映出用户或企业与算法平台之间的弱势地位。这种弱势不仅表现为事前严重的信息不对称与知情同意权的实质剥夺，还体现为事后救济中算法解释权、算法结果拒绝权流于形式。尽管《个人信息保护法》第二十四条第三款规定赋予用户算法解释权，但受限于“重大影响”等前置条件，权利适用范围被限缩且偏向事后性。

传统的商业秘密法律规范所调整的私权与公共利益关系，主要局限于商业道德和市场交易秩序[7]。而当对算法予以商业秘密保护时，所涉私人利益与公共利益就扩展到了更为广阔的平等权、自由权等基本权利领域。当二者冲突时，司法实务倾向于优先保护商业秘密私权，呈现出“商业秘密私权保护优先于公共利益”的价值取向。

3.3 价值与风险：企业核心技术与监管泄密风险冲突

商业秘密保护与算法监管的紧张关系还表现为企业核心技术所带来的商业效益与监管可能引发的泄密风险之间的冲突。

算法公开的不合理限度会增大企业核心技术泄露的风险。在北京理正软件股份有限公司侵害商业秘密纠纷案中，法院认定被告利用涉案商业秘密的算法逻辑思路，用不同程序设计语言开发新功能软件，构成侵权责任。此类案件表明，无论是监管要求的源代码披露，还是私人侵权行为导致的源代码泄露，都可能导致他人通过“换皮”操作规避侵权责任，突破商业秘密保护边界。

监管强度不足同样会破坏商业秘密保护与监管间的平衡。2021年，国家网信办对滴滴出行启动全面调查。经查明，滴滴出行不仅存在违法收集用户信息、过度收集精准位置信息、对乘客出行意图进行算法分析等16项违法事实，存在被监管部门认定为严重影响国家安全的数据处理活动。对于像滴滴这样具备社会动员能力的算法提供者，若以其核心技术涉商业秘密为由而不设置相应监管义务，就可能为大型算法平台违法违规利用算法收集数据提供掩护，对国家安全构成严重威胁。

综上，亟需在保护核心技术以维持竞争优势，与防止技术滥用及保障透明度之间找到平衡点，合理界定算法公开限度与监管强度。

4 算法监管与商业秘密保护的协同路径

通过对算法监管与商业秘密保护内在冲突的场景化分析，从“算法备案”优化、“内外监管”协作、“算法公开”设限、“监管能力”提升四个角度，构建协同体系具有重要价值。

4.1 “算法备案”优化：构建分级分类的算法监管框架

第一，适当拓宽算法备案制度适用范围。当前算法备案制度的适用对象仅限于具备舆论属性或社会动员能力的算法推荐服务提供者。但单一标准可能遗漏那些在市场运作、消费者权益保护等方面同样具有显著影响的算法服务。以电子商务为例，推荐、定价算法虽不直接涉及舆论或社会动员，但对市场竞争和消费者权益具有重大影响。因此，应当引入市场秩序、用户权益、劳动者保护等多重标准，拓宽备案适用范围[8]。

第二，以风险与场景为基准，明确算法分级分类标准，细化算法自评估报告。算法自评估报告作为备案的主体内容，应当以其为着力点建立健全分级分类标准。一方面，可借鉴欧盟《人工智能法案》的风险分级制度，将人工智能技术分为不可接受的风险、高风险、有限风险、低风险四个等级，结合国内科技发展实际划定算法风险等级制度[9]。另一方面，在《算法管理规定》规定的生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类五大类基础上，结合《互联网平台分类分级指南（征求意见稿）》进行场景分类，进而对算法自评估报告内容重点进行设定[10]。

4.2 “算法公开”设限：厘清“算法运行逻辑”公开边界

“算法公开”的内容，应从聚焦于算法本身到公开其运行逻辑。强制公开作为商业秘密的核心技术违背市场理性，过度扩大算法披露范围只会给企业带来过重负担。算法运行逻辑是指算法在处理数据和做出决策时所遵循的一系列步骤和规则，将其作为替代方案，既能减轻因算法公开引发的泄密风险，也能减轻企业说明负担。对公众而言，产生实质影响且能够理解的是算法在做出决策时所依据的信息及运行逻辑，而非复杂的代码文件[4]。

“运行逻辑”的描述需要以场景划定边界。其一，在《用户使用协议》场景中，算法运行逻辑重点在于“事前知情”，应当以全面、简明易懂为要，针对关键决策因素进行重点说明，但无需提供具体数值或公式。其二，在算法解释权行使场景中，运行逻辑的描述应侧重于决策部分，详细概述决策过程与依据，必要时披露对应的异常数据，但无需披露具体算法细节。其三，在算法备案制度中，运行逻辑的描述应重在算法的主要用途、应用场景及合规性声明。

4.3 “内外监管”协作：打造政府规制与内部监督协同模式

人工智能的快速发展，使得监管部门难以对算法进行持续性、穿透式的直接监督。因此，有必要转向多元主体共同参与、内外监管协同并进的新型治理模式。

健全企业内部监督体系，压实主体责任。技术上，企业应根据指引开展全流程算法影响评估，建立内部备案机制以固定问责点[8]。管理上，一是坚持价值引领，将算法伦理嵌入章程，通过人工干预优化机制，避免偏见歧视；二是完善内部纠察机制，建立类似审计的开发运营纠察制度及内部问责机制；三是建立标准体系，探索形成国家、地方及企业标准。

完善算法安全评估机制，构建全周期算法监管体系[11]。事前评估环节，应构建以模型鲁棒性测试、数据合规性审查、策略合理性分析及人工干预有效性验证为主体的评估体系，从源头疏解潜在安全风险。事中监测环节，需要依托实时数据追踪、安全审计日志分析、用户行为异常监测及滥用场景模拟等技术手段，形成动态风险预警机制。针对事后反馈环节，建议设立“用户同意负担审查小组”，定期审查算法服务平台的用户协议和隐私政策的公平性、透明度及用户权益保障情况。

4.4 “监管能力”提升：强化算法监管机构专业化水平

算法监管水平取决于算法监管能力。当前需要强化监管机构间的协同机制，提升各方监管能力，使监管人员能够真正懂技术、会监管。

其一，提高技术监管能力。通过汇集知识产权法

https://doi.org/10.35534/pss.0804054

律、经济、管理专家及算法领域行业专家，组建平台化的专家智库资源，引入第三方评估和认证。加快引进具备计算机科学、人工智能、法律和伦理学等多学科背景的专业人才，定期对现有监管人员进行专业培训，持续提升专业化水平。

其二，强化监管机构间的协同机制。依据《算法管理规定》，我国已构建起以网信部门为核心、多部门协同配合的“一主多辅”监管格局。在此基础上，应当着力破除部门间的信息与数据壁垒，依托技术支撑构建多部门协同的网络化监管体系[12]。同时，针对算法风险突发性强、隐蔽性高的特点，还应加快推进跨区域、跨部门的协同机制建设，完善线索通报、证据移交、案件协查、联合执法等关键协作制度。

5 结语

算法治理的本质是在技术效率与权利保障、商业私益与公共福祉之间寻求动态平衡。算法监管与商业秘密保护的冲突并非“零和博弈”。“黑箱与透明”“私权与公益”“价值与风险”三组矛盾的揭示说明，冲突的根源在于场景错位与工具单一。本文主张将冲突从权利对抗转向场景协同，提出“算法运行逻辑”作为调和算法解释权与商业秘密保护的中介变量，进而构建“备案优化、公开设限、内外监管、能力提升”的协同框架。展望未来，随着人工智能新业态的涌现，冲突形态也将不断演变，唯有持续推动技术迭代与制度回应之间的对话，才能动态地保障算法正义。

参考文献

[1] Beer D. Power through the algorithm? Participatory web cultures and the technological unconscious [J]. New Media & Society, 2009, 11 (6): 985–1002.
[2] Gillespie T. The relevance of algorithms[M]//Gillespie T, Boczkowski P J, Foot K A, eds. Media Technologies: Essays on Communication, Materiality, and Society. Cambridge: The MIT Press, 2014: 167.
[3] 陈景辉. 算法的法律性质：言论、商业秘密还是正当程序?[J]. 比较法研究, 2020, (2): 120–132.
[4] 刘琳. 算法解释权与商业秘密保护的冲突化解[J]. 行政法学研究, 2023, (2): 168–176.
[5] 孙建丽. 试论算法的法律保护模式[J]. 电子知识产权, 2019, (6): 39–47.
[6] 林洹民. 自动决策算法的风险识别与区分规制[J]. 比较法研究, 2022, (2): 188–200.
[7] 冯晓青. 商业秘密保护中的公共利益[J]. 人民司法, 2006, (10): 89–91.
[8] 张惠彬, 何易平. 平台算法监管的困境与出路——基于美国算法监管模式的研究[J]. 科学学研究, 2024, 42 (7): 1419–1428, 1448.
[9] European Commission. Artificial Intelligence Act [M]. European Union, 2021, URL.
[10] 陈兵, 董思琰. 常态化监管与算法分类分级治理模式更新[J]. 学术论坛, 2024, 47 (3): 46–55.
[11] 中国网信网. 专家解读丨加强算法安全科研攻关 推进算法综合治理 [EB/OL]. (2022–01–04) [2026–04–01]. https://www.cac.gov.cn/2022–01/04/c_1642894653573489.htm.
[12] 肖红军, 商慧辰. 平台算法监管的逻辑起点与思路创新[J]. 改革, 2022, (8): 38–56.

The Conflict between Algorithmic Regulation and Trade Secret Protection and its Collaborative Path

Huang Hao

Wuhan University of Engineering, Wuhan

Abstract: With the wide application of algorithms in the digital economy, the conflict between the legal regulation of algorithms and the protection of algorithmic trade secrets has become increasingly prominent. From the analysis of the internal mechanism of algorithmic legal regulation and trade secret protection, the algorithm has both high-risk characteristics and regulatory requirements, high-value attributes and confidentiality requirements. Starting from the typical scenarios of algorithm application, the three contradictions of 'black box and transparency' , 'private rights and public welfare' , and 'value and risk' are the key crux of the internal conflict between algorithm supervision and trade secret protection. The coordination mechanism of algorithm supervision and trade secret protection needs to be optimized from 'algorithm filing' to construct a hierarchical and classified algorithm supervision framework; grasp the limit of 'algorithm disclosure' and clarify the public boundary of 'algorithm operation logic' ; 'Internal and external supervision' collaboration to create a collaborative model of government regulation and internal supervision ; the improvement of 'regulatory capacity' and the strengthening of the professional level of algorithmic regulatory agencies are constructed in four aspects.

Key words: Algorithm supervision; Commercial secrets; Algorithm black box; The algorithm is transparent

https://doi.org/10.35534/pss.0804054