

人工智能与税务穿透式监管融合应用的思考

梁柳

杭州市烟草公司萧山分公司，综合管理科，杭州萧山市心北路 101 号，
311200，13575785392

摘 要：当前人工智能快速普及，为税务监管转型提供了强有力的技术支撑。本文剖析了双技术协同赋能税务穿透监管的内在逻辑，指出财务数据全生命周期 AI 应用也存在多种安全风险，并从智能风险识别、监管流程再造、数据安全架构、多方协同机制四个维度提出 AI 应用税务穿透式监管的实施路径，为企业税务穿透式监管提供参考。

关键词：税务穿透式监管；人工智能税务应用；智能风险识别

一、基本概述

自 2025 年起，人工智能产业全面进入规模化落地阶段，以多模态生成式大模型为核心的技术体系逐步成熟，AI 在文本生成、数据解析、政策研判、图文识别等方面的能力受到普遍认可，为各行业数字化转型提供智能内容生成与逻辑推理支撑。迈入 2026 年，以 OpenClaw 为代表的开源智能体执行框架快速兴起并迅速出圈，推动人工智能行业完成从“生成式对话工具”向“自主执行智能体”的范式迭代。在此技术浪潮下，财税行业迎来全新的变革契机。当前，税务核查逐步转向穿透式监管模式，要求穿透财务数据表象，还原真实经营业务，精准识别隐性涉税风险。而当前人工智能快速普及的技术浪潮，为税务穿透式监管提供了强有力的技术支撑。如何将人工智能深度融合财税业务，并平衡好自动化效率与财税合规风险，是现代化财税管理的重要时代课题，具备重要的理论研究价值与实务应用价值。

二、AI 技术实现税务穿透式监管降本增效的赋能逻辑

生成式 AI 的认知智能与 OpenClaw 的执行智能形成协同互补，从根源上破解传统税务合规管理的痛点，实现税务监管的全方位降本增效与模式升级。在成本效率层面，双技术协同替代了大量重复性、事务性人工工作，压缩监管核查周期、减少人力投入，实现监管资源的高效配置；在风控质量层面，

生成式大模型精准智能研判叠加 OpenClaw 智能体完整留痕能力，消除传统监管主观性强、漏检率高、证据链不完整的痛点，显著提升涉税风险识别的精准度与合规核查质量；在治理模式层面，双技术协同推动税务监管从传统事后补救式核查，逐步转向事前智能预警、事中动态穿透管控、事后闭环复盘的全周期治理模式，从而实现企业涉税业务全链条、全方位的智能穿透监管，助力企业构建精细化、常态化、合规化的现代税务风控体系。

三、人工智能应用在税务穿透式监管中的实现路径

（一）税务合规风险穿透式识别

依托生成式 AI 重构涉税风险研判体系，实现全维度、深层次穿透式风险识别。

第一，智能自动采集，夯实数据基础。依托内网本地化部署 OpenClaw 智能体，自动对接财务系统、电子发票平台，批量抓取明细账、进销项增值税发票、银行流水、纳税申报表等资料，统一规整为标准化数据格式，大幅缩减基础整理工作耗时，为风险研判提供完整数据源。

第二，模型智能研判，深挖隐性风险。利用本地私有化生成式 AI 模型，实时更新财税法规、会计准则与金税监管指标，动态维护合规判定标准；构建多维度风险识别模型，精准识别税务合规风险点，例如进项抵扣违规、成本列支不合理、税收优惠适用不当等，弥补人工核查穿透性不足的缺陷，并自动生成附带判定依据的风险分析报告。

第三，分级动态预警，精准区分风险等级。按照风险严重程度划分一般合规瑕疵、中度涉税疑点、重大违规风险三类等级，联动 OpenClaw 实时调取存量财税数据开展持续扫描，持续推送动态预警，提升穿透式风险识别的精准性。

（二）智能监管流程再造

通过生成式 AI 与 OpenClaw 的协同配合，实现税务监管全流程自动化，重塑事前、事中、事后全周期穿透监管流程。

第一，前置业务校验，源头防控涉税风险。将智能体嵌入前端涉税业务环节，在合同签订、发票开具、计税核算阶段自动校验业务条款、开票规范与计税标准，从业务源头拦截不合规操作，落实事前穿透管控。

第二，实时交叉核验，自动生成监管底稿。借助 OpenClaw 跨系统调度能力，同步账、票、税、货四类数据并完成交叉比对，实现业务全过程动态穿透核查；生成式 AI 根据风险结果、原始证据与监管规范，自动编制标准化监管底稿，完整填充风险描述、调整分录、核查结论等内容。

第三，自动取证归档，形成完整监管闭环。识别风险后，OpenClaw 自动定位对应原始凭证、银行流水，完成截图、导出取证，建立标准化监管台账，完整留存全流程操作记录与证据链，自动输出最终监管报告，形成风险识别、定位取证、复盘归档的智能化闭环。

（三）构建数据安全架构

针对财务数据泄露、越权调用等安全隐患，依托 OpenClaw 本地部署特性搭建适配税务穿透式监管的数据安全架构，筑牢数据防护底线。

第一，内网私有化部署，隔绝云端外泄风险。将生成式 AI 模型、OpenClaw 智能体统一部署 OA 内网，涉税数据全部本地存储、本地运算，严禁原始涉密数据上传公有云，从传输、存储环节切断数据外泄渠道。

第二，分级最小权限，严控越权访问行为。遵循最小权限原则，将 AI 研判、数据调取、流程执行权限分开管控，仅授权人员可发起监管任务、调用相关数据；按财务、审计、税务岗位划分访问范围，关键操作增设人工审批节点，禁止智能体无授权读写、迁移涉密财务数据。

第三，全链路日志留痕，实现全程可追溯。完整记录 AI 模型调用、智能体操作、数据读取等全部行为日志，生成不可篡改电子存证，所有数据流转、异常操作均可定位溯源，同步满足税务稽查与内部审计留痕要求。

（四）建立协同保障机制

通过制度、人才、技术的协同保障，确保智能监管持续发挥效能、数据安全得到长期保障。

第一，完善配套管理制度，清晰划分各方权责。出台涉税数据安全管理制度，明确智能工具使用、数据调取、权限分配、异常处置规则，厘清财务人员、运维人员、第三方技术人员责任边界，解决人机责任难以界定的问题。

第二，培育复合型人才，夯实专业应用基础。开展 “税务合规+人工智

能+数据安全”的综合培训，补齐财务人员技术短板、技术人员财税知识短板，打造复合型岗位队伍，规范日常操作行为。

第三，持续迭代优化，配套风险应急机制。定期校验本地 AI 模型、排查系统漏洞，结合税收政策更新迭代风控模型，减少算法研判偏差；建立突发事件处置预案，实时监测 AI 运行、数据传输异常，保障智能监管体系稳定、安全运行。