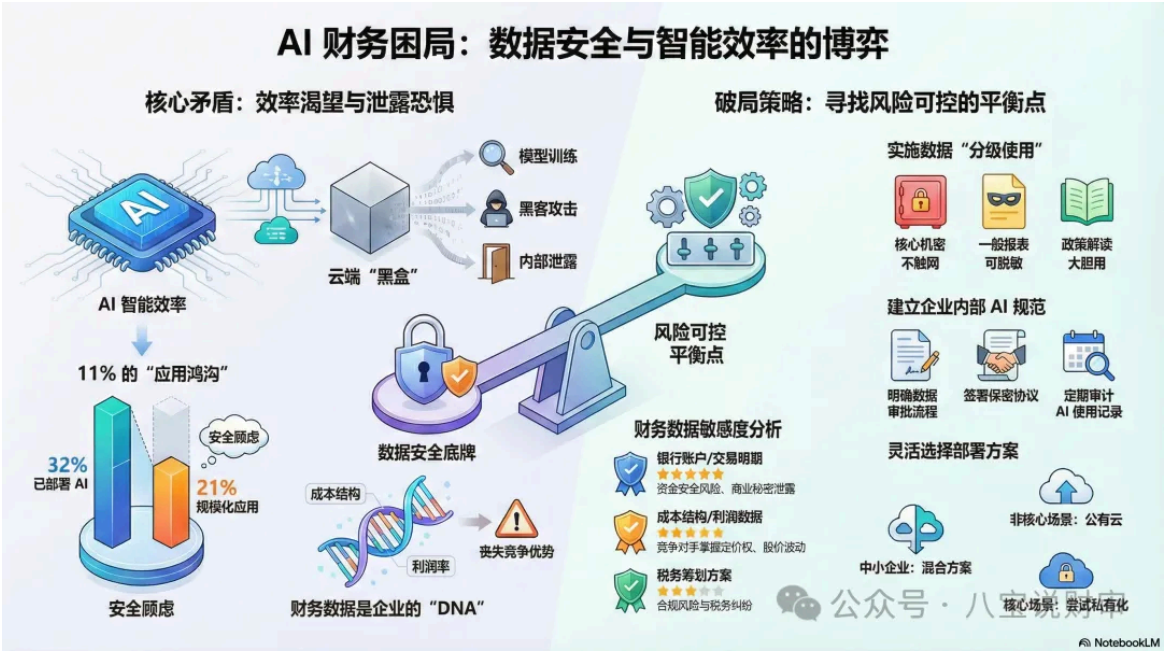
AI财务的最大困境：你的数据，敢发给大模型吗？

原创 八宝说财审 八宝说财审 2026年1月28日 21:58 广东

> 32%的企业已经部署了AI大模型，但只有21%能规模化应用。中间这11%的差距，很大一部分死于同一个问题——**数据安全**。



01 一个CFO的真实纠结

张总是某中型企业的CFO。

他对AI充满期待：自动处理发票、智能分析现金流、预测资金需求……

但他却迟迟不敢下手。

为什么？

> "我们的财务数据是企业的核心机密。银行账户、交易明细、成本结构、利润情况……这些数据发给AI大模型，真的安全吗？

> "万一被拿去训练模型，竞争对手用AI反向推算出我们的底牌怎么办？"

> "出了数据泄露，这个责任谁来担？"

张总的纠结，不是个例。

这是当前AI在财务领域应用的最大困境——

你想用AI，但你的数据不敢给AI。

02 财务数据的特殊性

为什么财务数据这么敏感？

因为它不只是"数据"，而是企业的 **底牌** 。

数据类型	敏感程度	泄露后果
银行账户余额	⭐⭐⭐⭐⭐	资金安全风险
客户交易明细	⭐⭐⭐⭐⭐	客户流失、商业秘密泄露
成本结构	⭐⭐⭐⭐	竞争对手定价策略、盈利模式被掌握

数据类型	敏感程度	泄露后果
利润数据	⭐⭐⭐⭐⭐	股价波动、融资谈判被动
税务筹划方案	⭐⭐⭐⭐	税务风险、合规问题

试想一下：

如果你的供应商知道你的真实采购成本，谈判还能谈吗？

如果你的客户知道你的利润率，议价还能硬吗？

如果你的竞争对手知道你的现金流状况，会不会趁虚而入？

财务数据，是企业的DNA级机密。

一旦泄露，损失的不是钱，是竞争优势。

03 AI大模型的工作逻辑

这里就出现了一个根本性矛盾。

AI大模型需要什么？

需要数据。

需要大量、高质量、真实的数据来学习你的业务模式，才能给出精准的分析和建议。

AI大模型怎么工作？

你把数据发给它 → 它在云端处理 → 返回结果（可能用于模型优化）

问题就在这里：

1. **数据离开你的掌控**：一旦发送，就进入了"黑盒"
2. **处理过程不透明**：你不知道AI怎么用你的数据
3. **模型训练风险**：你的数据可能被"记住"，影响后续输出
4. **云端存储隐患**：服务商被攻击怎么办？内部人员泄露怎么办？

你想用AI的能力，但不想让AI"记住"你的数据。

这是一道无解的题吗？

04 企业为什么不敢用？

毕马威的调研报告显示，**近四分之三的领导阶段企业**制定了负责任的AI使用政策。

这些政策的核心是什么？

数据管控。

具体表现：

❌ **拒绝使用公有云大模型**：数据不敢发到第三方服务器

❌ **敏感字段脱敏处理**：但脱敏后，AI分析效果大打折扣

❌ **只用于非核心场景**：比如写报告摘要，不敢做决策分析

❌ **自建私有化部署**：但成本高昂，中小企业玩不起

澳洲一家银行的案例很典型：

> "我们用AI做税务合规的努力，受到了'将AI集成到现有系统'和'数据安全'双重阻碍。最后只能在非敏感数据上小规模试点。"

结果就是：AI被"阉割"使用，价值大打折扣。

05 大模型厂商的承诺

面对这个困境，AI厂商们也在想办法：

承诺1：数据不被用于模型训练

OpenAI、微软、谷歌都承诺企业数据不会被用于训练公开模型。

但问题来了：

- 承诺怎么验证？
- 服务商被收购怎么办？
- 政策变化怎么办？

承诺2：数据加密存储

采用端到端加密，确保数据安全。

但矛盾的是：

加密后的数据，AI怎么分析？

承诺3：私有化部署

允许企业在本地服务器部署大模型。

但问题来了：

- 成本：动辄几十万上百万
- 算力：中小企业玩不起

- 维护：需要专业技术团队

中小企业陷入两难：

用公有云？不安全。

私有化部署？太贵。

06 技术能解决问题吗？

技术圈正在探索几种解决方案：

方案1：联邦学习

数据不出本地，只交换模型参数。

听起来很美好，但财务场景下几乎不现实：

- 每个企业的财务数据结构差异巨大
- 模型参数本身可能泄露数据特征
- 技术复杂度极高

方案2：差分隐私

在数据中加入"噪音"，保护隐私。

但这与财务分析的要求相悖：

财务要的是精准，不是"差不多"。

方案3：本地小模型

在本地部署小型大模型。

现状：

- 效果远不如云端大模型
- 硬件要求高
- 更新迭代慢

🧬 方案4：可信执行环境（TEE）

在硬件层面创建"黑盒"环境，数据在里面处理，外部无法窥探。

这是目前最有希望的方向，但：

- 技术还不成熟
- 成本很高
- 业界缺乏统一标准

技术可以缓解问题，但无法彻底消除矛盾。

07 困局之下，企业怎么办？

没有完美方案，但可以找到 **风险可控的平衡点** 。

🧬 策略1：分级使用

数据敏感度	处理方式	AI应用
核心机密（银行账户、交易明细）	本地系统，不上传AI	❌ 不使用
敏感数据（成本、利润）	脱敏+加密后使用	⚠️ 谨慎使用

数据敏感度	处理方式	AI应用
一般数据（报表摘要、趋势分析）	可上传	✅ 可以使用
非敏感数据（行业知识、政策解读）	自由使用	✅ 大胆使用

策略2：选择靠谱的服务商

- 看安全认证（ISO27001、SOC2等）
- 看数据政策（是否承诺不用于训练）
- 看服务协议（数据所有权、泄露责任）
- 看技术实力（加密、权限控制、审计日志）

策略3：建立内部AI使用规范

- 明确哪些数据可以用AI，哪些不行
- 建立数据审批流程
- 定期审计AI使用情况
- 签署保密协议（对内对外）

策略4：混合方案

- 非核心场景用公有云AI（成本低、效果好）
- 核心场景用私有化部署（安全可控）
- 逐步试点，小步快跑

08 未来会怎样？

这个困境会持续很久。

但有几个趋势值得期待：

趋势1：监管会更完善

欧盟的AI法案、中国的数据安全法，都在推动AI厂商建立更透明的数据使用规则。

趋势2：技术会继续进步

TEE、联邦学习等技术会逐步成熟，降低使用门槛。

趋势3：市场会分层

- 大企业：私有化部署+定制化模型
- 中小企业：混合方案，分级使用
- 特定行业：出现垂直领域的安全AI解决方案

趋势4：新商业模式会出现

比如"数据信托"模式：第三方机构托管数据，AI用完即删，永不存储。

09 写在最后

AI在财务领域的应用困境，不是技术问题，而是 **信任问题** 。

你想用AI，但你不敢信任它。

这种信任的建立，需要：

- AI厂商的透明承诺和技术保障
- 监管部门的政策规范
- 企业的风险管控能力

- 时间和实践的检验

短期内，这个困境无解。

但长期看，它会推动AI技术朝着更安全、更可控的方向发展。

对于财务人来说，重要的不是等待完美方案，而是——

在风险可控的前提下，开始尝试。

因为：

> 你的竞争对手可能也在纠结，但谁先找到平衡点，谁就获得了先发优势。

如果这篇文章对你有启发，欢迎点赞、转发。

关注我们，陪你一起在AI时代做好数据安全与效率提升的平衡。