

# 隐私号技术在中国本地生活服务行业的深度渗透、模式演进与生态重塑研究

韦俊妮, 李智妍

中国—东盟信息港股份有限公司, 广西南宁, 中国

**【摘要】**在中国数字经济高速发展的背景下,本地生活服务行业已成为个人信息保护的关键场域。截至2024年底,我国即时配送用户规模已达7.2亿人,年订单量突破680亿单,行业在高速增长的同时也面临着隐私泄露、信任缺失等多重挑战。本文基于“技术-商业-治理”三维分析框架,系统考察了隐私号技术从基础隐匿到智能生态构建的演进历程,深入剖析其在重塑平台治理能力、调节多方主体关系、重构行业生态等方面产生的深远影响。研究发现,隐私号技术已从单一通信隐私工具演化为平台信任体系的核心基础设施,其发展路径深刻体现了效率、隐私与安全在数字经济发展中的动态平衡逻辑。研究进一步揭示了技术创新背后的商业策略与治理逻辑,为理解中国特色的平台治理实践提供了理论参考与实证依据。

**【关键词】**隐私号技术; 即时配送; 平台治理; 数字信任; 技术演进

## 1. 隐私号技术的诞生: 数字信任危机下的技术回应

2020-2024年以来,中国本地生活服务行业持续保持高速增长态势,如图一所示,2024年订单量达到680亿,为2020年210亿单量的3.2倍[1]。同时,2024年即时配送市场规模突破1.8万亿元,日均订单量超过1.86亿单。这种以“分钟级送达”为特征的超高效服务背后,是每时每刻都在发生的海量陌生人临时性连接。据中国互联网络信息中心2024年12月发布的《第53次中国互联网络发展状况统计报告》显示,我国外卖用户规模已达5.6亿,占网民整体的51.2%[1]。

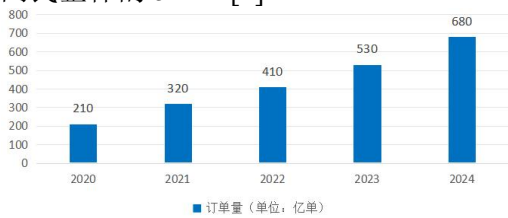


图1. 2020-2024年中国即时配送行业订单量增长趋势

传统基于实体手机号码的连接模式暴露了深层的结构性矛盾。据国家互联网应急中心2024年第三季度报告,涉及外卖、快递等行业的个人信息泄露事件同比增长28.5%,因隐私泄露导致的精准诈骗涉案金额预估超过80亿元[2]。这一“数字信任危机”不仅威胁用户权益,更动摇平台经济的基础逻辑。

在此背景下,隐私号与VoIP技术的应用已演变为平台经济中信任生产与维护的关键

基础设施[3]。2024年《个人信息保护法》实施三周年之际,相关技术应用进入了深度合规与创新并行发展的新阶段。

## 2. 隐私号技术的三阶段跃迁

隐私号技术在过去十年的发展的技术升级,是中国互联网平台在监管环境、市场竞争和商业哲学演变下的一个深刻缩影[4]。其历程清晰地划分为三个阶段,体现了从“被动合规”到“主动运营”,最终迈向“生态智能”的战略跃迁。

(1)第一阶段(2015-2018): 基础隐匿期的风险最小化策略。这一阶段主要应用AXB模式(一对一静态映射)[5]。当时行业处于野蛮生长期,平台首要目标是规避因信息泄露引发的法律与声誉风险[6]。从商业逻辑看,此时的隐私号是典型的“合规成本项”。平台采购号码资源主要基于风险防范的被动决策,而非主动的运营优化工具。

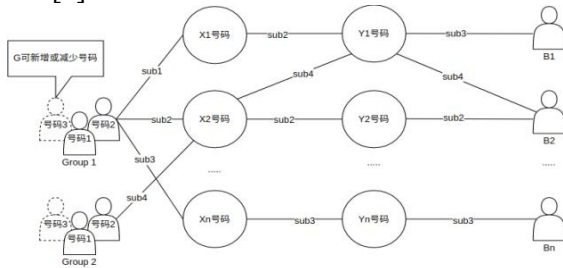
(2)第二阶段(2018-2021): 效率优化期的精细化运营。随着市场竞争白热化与订单量呈指数级增长,单纯的“隐匿”已无法满足需求。平台运营的重心转向降本增效与体验优化。AXxYB(分机号)模式的普及标志着这一转变。通过软件定义网络(SDN)等技术,实现了单一主号下动态分配分机号,将号码资源复用率推升至每日180-240次。此时,隐私号从“成本项”转型为“效率工具”,其价值体现在直接的经济效益上:如表一所示,AXxYB(分机号)模式大幅降低号码采购的边际成本,

优化资源利用率；同时，标准化的中间号也减少了因直接泄露手机号引发的纠纷，提升了配送、服务环节的顺畅度[7]。平台的决策逻辑从被动的风险防范，转变为主动的运营效率计算。

**表 1.AXXYB 模式与传统 AXB 模式成本效益对比 (2024 年)**

对比维度	AXB 模式	AXxYB	改进幅度
号码复用率	3-5 次/日	180-240 次/日	提升 60 倍
号码采购成本占比	6.82% 0.6%-0.8%	0.15%-0.25%	降低 67%
转单处理时间	45-60 秒	<5 秒	提升 90%
系统绑定成功率	92.5%	99.8%	提升 7.9%

(3)第三阶段 (2021-2025)：生态构建期的智能化与一体化。当效率提升见顶，行业竞争进入生态与体验维度时，GXYB (共享小号) 模式应运而生。其革命性在于核心理念从“号码”转向“身份”。如图二所示，快递小哥对应的是一个 G，可以通过 X 号码联系收件人，一个虚拟号码不再绑定一个快递小哥，X 号码可以与无数个快递小哥绑定，X 号码的复用率不在绑定在快递小哥和订单身上，而是取决于 X 号码的通话次数，成为一个独立“身份”的存在[8]。



**图 2.GXYB 模式**

### 3.隐私号对即时配送的生态重塑

#### (1)提升平台治理能力

隐私号技术在即时配送行业的深度渗透，已从最初单一的通信隐私保护工具，演变为平台进行精细化治理、构建数字信任生态的核心基础设施。这一转变标志着平台治理模式从传统的人工巡查、事后追溯，升级为全流程、智能化、数据驱动的预防性治理范式。2024 年的行业数据显示，头部平台的智能语音质检系统日均处理通话量已突破 2000 万通，识别准确率达到 94.5%，这不仅是技术能力的体现，更是平台治理权力在微观层面的一次重大延伸[9]。这一系统通过对海量通话内容的自动分析，能够实时识别出服务态度问题、承诺未兑现、违规索要个人信息等超过 30 类风险场景，

并自动触发预警、介入甚至生成处置建议。例如，当系统识别到配送员与用户因地址不清发生争执时，可自动向双方推送标准化的解决指引，或直接转接人工客服介入，从而在纠纷升级前将其化解，如表二所示 2024 年主要平台在引入隐私号治理功能之后，客户满意度都达到了 89%以上。这种基于隐私号通话数据的治理，使得平台能够以前所未有的粒度“看见”并管理发生在数百万次终端交互中的服务过程，将原本不可控的线下服务环节纳入了标准化的数字管理体系。

**表 2.2024 年主要平台隐私号治理功能对比**

平台	日均通话量	质检覆盖率	纠纷解决效率	客户满意度
美团	850 万通	100%	<4 小时	92.3%
饿了么	620 万通	98.5%	<6 小时	90.8%
达达	380 万通	95.2%	<8 小时	89.5%

更重要的是，隐私号技术构筑了一道防止平台核心资产——客户关系与交易数据——外流的“数字护城河”。通过控制通信中介，平台确保了服务关系始终在自身的生态系统内闭环运行，有效防范了配送员与用户建立直接联系后可能发生的“跳单”行为[10]。据 2024 年《本地生活服务行业数字化安全报告》估算，有效的隐私号系统每年可为大型平台避免因客户流失造成的直接经济损失超过 15 亿元。这种技术锁定效应，在提升用户粘性的同时，也强化了平台对服务提供者（骑手）的议价能力与管理权威。平台通过隐私号系统收集的通信时长、响应模式、沟通质量等数据，正日益成为算法调度、绩效评估乃至保险定价的关键依据，从而在更深层次上重构了平台、劳动者与用户之间的权力关系与依赖结构[11]。

#### (2)从业人员面临双重境遇

对于规模已超过 1500 万的即时配送从业人员而言，隐私号技术的普及带来了一个复杂而矛盾的现实：它既是一面抵御外部风险的“盾牌”，也可能成为一把强化内部控制的“双刃剑”。从积极层面看，隐私号显著改善了骑手的职业安全与工作体验。调查数据显示，使用隐私号后，从业人员遭遇电话骚扰的比例从 43%大幅下降至 5.2%[12]。这意味着，骑手的个人生活空间与工作边界得以重新区隔，避免了因号码泄露带来的无休止的推销、诈骗甚至人身安全威胁。特别是在处理投诉或争议订单时，隐私号提供的临时通信通道和自动录音功能，在保护骑手隐私的同时，也为其在面对不实指控时提供了关键的自证工具，一定程度上

平衡了其在服务关系中的弱势地位。此外，支持多终端绑定的先进隐私号模式（如 GXYB 模式），解决了因设备故障、电量耗尽导致的“失联”困境，提升了工作的连续性与灵活性，这是技术对劳动者基础工作条件的一种切实改善。

然而，硬币的另一面是技术监控的无孔不入及其带来的心理异化。2024 年发布的《数字时代劳动者权益保障白皮书》尖锐地指出，高达 86.7% 的骑手认为基于隐私号通话的监控“带来了较大的心理压力”。这种压力远非简单的被监视感，它源于几个更深层的结构性矛盾。首先，监控的量化与绩效化：通话中的各项指标——如接起速度、沟通时长、话术规范程度、语气情绪（通过声纹分析）——被平台算法持续采集、分析，并可能直接关联到配送员的评分、派单优先级乃至收入。这使得每一次沟通都异化为一场被量化的绩效表演，骑手不得不进行持续的“情感劳动”以维持系统认可的服务形象，导致自主性与真实性的消解。其次，证据的不对称与解释权的丧失：虽然录音可作为证据，但其采集、存储、解释的主动权完全掌握在平台手中。当发生纠纷时，平台算法对录音片段的截取与解读可能无法完整还原语境，劳动者缺乏对自身数据档案的访问权和异议权，陷入了一种“数字全景监狱”的无力感。最后，社会关系的数据化剥离：隐私号在阻断骚扰的同时，也彻底阻断了服务结束后骑手与用户间任何自发、非功利性联系的可能。一切互动都被预先设定、即时生效、旋即消失的技术协议所中介，人际交往被简化为纯粹的功能性数据交换。长此以往，这种工具性联结的普遍化，可能侵蚀劳动者从工作中获得社会认同与意义感的基础，加剧职业的孤独感与异化。

因此，隐私号技术所塑造的骑手境遇，本质上是数字时代技术治理逻辑下劳动者处境的缩影：技术在提供保护与便利的同时，也通过数据的采集、算法的评估与流程的固化，将劳动过程更深地卷入资本的控制与优化体系之中。

#### 4. 趋势与未来展望

在多方的关注下，隐私号技术的演进正处在一个从“管控增效”向“平衡赋能”转型的关键节点。当前，技术一方面助力平台实现治理能力的跃升与风险的有效控制，另一方面也在劳动过程数字化监控中衍生出劳动者异化与权益失衡等深层矛盾。解决这一矛盾，是未

来技术演进与制度创新的核心方向[13]。

首先，技术将向“精准赋能”与“权益穿透”方向发展，以解决劳动者境遇的复杂性。针对当前监控带来的心理压力与算法黑箱问题，未来的隐私号系统将集成“可控透明度”机制。例如，通过区块链赋能的隐私计算技术，骑手可拥有一个属于个人的、加密的“服务数字档案”，其中记录经其授权共享的通话质量标签（非原始录音）[14]。当平台算法调用该数据进行评估时，过程可被记录且可审计，劳动者同时享有对不公评估的算法解释权与申诉渠道。这将使隐私号从平台单方控制的治理工具，转变为平衡劳资权责的“可信中介”，在保护用户隐私的同时，也保障劳动者的数据主权与公平待遇。

其次，治理模式将从“平台中心管控”迈向“多方共治的生态化治理”。当前平台通过隐私号实现的精细化治理，虽然高效，但其规则制定与执行的单边性也引发了争议[15]。展望未来，隐私号系统产生的聚合化、脱敏化的交互数据流，将成为行业公共治理的基石。监管部门、行业协会、工会组织可基于此数据，共同制定更科学的服务标准、劳动定额与争议解决准则。例如，通过分析海量匿名化通话时长数据，可以确立不同配送场景下的合理沟通时间范围，防止平台制定过于严苛的响应标准。这意味着，隐私号技术催生的“数据富矿”，其价值将被引导用于构建一个更公平、更透明、规则共建的行业生态，而不仅仅是强化单一平台的竞争优势。

#### 5. 结语

隐私号技术的持续演进，本质上是对数字时代“信任”基础设施的重构与升级。它不再仅是信息隐匿的技术工具，更应成为连接用户、劳动者、平台与监管方的“信任调节器”与“治理赋能器”。其发展的终极评价，不应仅局限于订单完成效率或隐私泄露率等单维指标，而应综合考量其是否在提升商业效率、保障个人尊严、维护劳动权益、履行合规责任等多个目标之间取得了动态、可持续的平衡。

这要求技术设计者、商业实践者与政策制定者共同秉持“负责任创新”的理念，在技术演进中注入更多人文关怀与制度智慧。隐私号技术若能在效率与公平、控制与赋能、商业价值与社会责任之间找到恰当的平衡点，则有望从一项优秀的商业解决方案，升华为支撑数字经济包容性、可持续性发展的社会型技术基础设施。

展望未来,隐私号的生态化发展仍处于进行时。其演进路径将继续受到技术突破、市场竞争、政策规制与社会期待等多重力量的塑造。唯有通过持续的制度创新、技术优化与多元共治,隐私号技术才能真正实现从“解决平台痛点”到“承载行业责任”的跨越,助力构建更具包容性、公平性与韧性的数字服务生态。

### 参考文献

- [1] 张华,刘敏.数字化转型中的隐私保护与商业创新[J].管理世界,2024,40(7):112-125.
- [2] 丁晓东.个人信息保护的中国路径:从《网络安全法》到《个人信息保护法》[J].比较法研究,2021(6):1-15.
- [3] 郑宇,王芳.5G时代隐私通信技术的发展趋势[J].电信科学,2024,40(3):45-52.
- [4] 蔡维山.数字经济背景下平台责任的重构[J].法学研究,2022,44(2):87-105.
- [5] 黎志远,薛家顺.隐私号业务平台的PaaS+SaaS化架构设计与实现[J].中国新通信,2019,21(17):63-65.
- [6] 李佳梅,张小洪,陶然.快递行业用户隐私泄露现状及其产生的社会问题[J].科技经济导刊,2017(19):267-269.
- [7] 周涛,刘洋.人工智能在隐私通信中的应用研究[J].通信技术,2024,57(8):1023-1029.
- [8] 赵欣,王磊.基于区块链的隐私号可信存证系统研究[J].计算机科学,2024,51(6):328-335.
- [9] 孙晓霞,李刚.数字劳动者权益保障机制研究[J].中国人力资源开发,2024,41(4):56-64.
- [10] 刘权.网络平台的公共性及其实现——以电商平台为例[J].法学研究,2020,42(2):20-37.
- [11] 陈思.平台经济中的个人信息保护:基于隐私号的实证研究[J].法学论坛,2024,39(2):88-97.
- [12] 黄磊.隐私保护平台实现的探索和思考[J].邮电设计技术,2019(5):23-26.
- [13] 马亮.数字政府与平台治理:创新、挑战与展望[J].公共管理学报,2023,20(1):1-12.
- [14] 肖振,李航.基于区块链的劳动者数字权益保障平台架构研究[J].信息安全,2024,24(9):78-85.
- [15] 王琳,郭凯.数字经济协同治理:理论框架与实践路径[J].经济学家,2023,35(6):95-104.