E-Commerce Letters 电子商务评论, 2025, 14(4), 2694-2699
Published Online April 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.1441182

Hans汉斯

效率与权利的博弈：AI个性化营销的隐私风险与合规路径研究

徐　盼

贵州大学法学院，贵州　贵阳

收稿日期：2025年3月11日；录用日期：2025年3月27日；发布日期：2025年4月29日

摘　要

随着人工智能(AI)技术在电子商务领域的深度应用，个性化营销通过用户画像、实时推荐与动态定价显著提升了商业效率，但也引发了用户隐私保护与合规性的双重挑战。本研究以效率与权利的博弈为核心，系统剖析AI驱动营销场景下的隐私风险，包括数据过度收集、算法黑箱化及数据滥用问题，并结合法律框架(如欧盟GDPR与中国《个人信息保护法》)与行业实践，揭示电商平台面临的合规困境。研究发现，当前法律执行中存在“形式合规”与“最小必要原则模糊”等结构性矛盾，而跨境数据流动与平台责任边界模糊则加剧了行业特殊性挑战。为平衡效率与隐私，本文提出三重建构路径：技术层面深化隐私计算(联邦学习、差分隐私)以保障数据安全；治理层面通过透明化设计与算法解释功能破解信任危机；用户权益层面以简化控制选项与数据收益共享机制增强主权意识。研究强调，AI营销的可持续发展需以“效率－隐私－信任”三角平衡为目标，通过技术创新、制度优化与多方协作实现合规与效率的动态统一，为电商平台及监管机构提供理论与实践参考。

关键词

电子商务，人工智能，个性化营销，数据隐私保护，合规策略

The Game between Efficiency and Power: Research on Privacy Risk and Compliance Path of AI Personalized Marketing

Pan Xu

School of Law, Guizhou University, Guiyang Guizhou

Received: Mar. 11th, 2025; accepted: Mar. 27th, 2025; published: Apr. 29th, 2025

文章引用: 徐盼. 效率与权利的博弈: AI 个性化营销的隐私风险与合规路径研究[J]. 电子商务评论, 2025, 14(4): 2694-2699. DOI: 10.12677/ecl.2025.1441182

Abstract

With the deep application of artificial intelligence (AI) technology in e-commerce, personalized marketing has significantly improved business efficiency through user profiles, real-time recommendations and dynamic pricing, but it also raises the dual challenges of user privacy protection and compliance. With the game between efficiency and rights as the core, this study systematically analyzes the privacy risks in AI-driven marketing scenarios, including excessive data collection, algorithm black box and data abuse, and combines legal frameworks (such as EU GDPR and China's "Personal Information Protection Law") and industry practices to reveal the compliance dilemma faced by e-commerce platforms. The study found that there are structural contradictions in the current law enforcement such as "formal compliance" and "ambiguity of the principle of least necessity", while the cross-border data flow and the ambiguity of platform responsibility boundary exacerbate the challenges of industry particularity. In order to balance efficiency and privacy, this paper proposes a threefold construction path: deepening privacy computing (federated learning, differential privacy) at the technical level to ensure data security; At the governance level, the trust crisis is solved through transparent design and algorithm interpretation. At the level of user rights, it enhances the awareness of sovereignty by simplifying control options and data revenue sharing mechanism. The research emphasizes that the sustainable development of AI marketing should aim at the triangle balance of "efficiency-privacy-trust", and achieve the dynamic unity of compliance and efficiency through technological innovation, system optimization and multi-party collaboration, so as to provide theoretical and practical reference for e-commerce platforms and regulatory agencies.

Keywords

E-Commerce, Artificial Intelligence, Personalized Marketing, Data Privacy Protection, Compliance Strategies

1. 引言

随着电子商务的蓬勃发展，人工智能(AI)技术已成为驱动精准营销的核心引擎。以亚马逊为例，其推荐系统贡献了 35%的销售额，凸显 AI 在提升商业效率中的关键作用[1]。然而，技术的深度应用伴随着用户数据的海量采集与分析，使得数据隐私问题日益凸显。全球范围内，用户隐私意识逐渐觉醒，法律框架亦同步收紧：欧盟《通用数据保护条例》(GDPR)确立严格的数据处理标准，中国《个人信息保护法》则通过“告知–同意”原则与数据最小化要求，强化了企业对用户权益的保障义务[2]。技术与法律的交织，将电商平台置于效率与权利博弈的十字路口。

当前矛盾的核心在于，电商平台如何平衡 AI 驱动的营销效率与用户隐私信任？一方面，个性化营销依赖用户画像与行为数据分析，但过度收集或滥用数据可能引发隐私泄露风险，例如算法标签化与自动化决策导致的“信息茧房”问题[3]；另一方面，现有研究多聚焦单一维度：或探讨 AI 算法的技术优化，或分析法律条款的合规边界，缺乏对电商场景中技术逻辑与法律框架的交叉性研究。例如，GDPR 虽强调数据主体权利，但其宽泛的“个人信息”定义与模糊的“可识别性”标准，导致企业在匿名化处理中面临实践困境。这种割裂式研究难以回应电商平台在动态数据处理中的复杂挑战。

2. 电商场景下 AI 个性化营销的实践与风险

人工智能技术的深度渗透重构了电子商务营销范式，通过算法驱动决策与多维度数据聚合，AI 不仅实现了消费者需求的精准捕捉，更重塑了商品分发与定价逻辑。从用户画像的精细化建模到实时推荐系统的动态响应，再到价格策略的智能调优，AI 技术正以效率为核心突破传统营销边界。然而，数据采集边界的模糊性与算法决策的隐蔽性亦使消费者隐私权面临被侵蚀的潜在威胁，如何在技术创新与合规约束间建立平衡机制，成为电商平台可持续发展的关键命题。

2.1. 电商 AI 营销的核心应用

2.1.1. 用户画像：基于购买历史、浏览行为的标签化

基于多维度行为数据的标签化分析是 AI 营销的基础性技术。通过整合用户浏览轨迹、购买记录及社交互动信息，电商平台采用聚类算法(如 K-means)和分类模型(如决策树)生成精细化用户画像。例如，淘宝的“千人千面”系统通过动态更新用户标签，识别消费偏好与潜在需求，实现商品展示的差异化匹配。此类技术不仅依赖海量数据积累，还需通过特征工程优化数据质量，然而，过度依赖敏感信息(如地理位置、支付习惯)可能引发隐私泄露风险，需在数据采集阶段嵌入合规约束。

2.1.2. 实时推荐：动态调整商品展示

2025 年电商领域的实时推荐系统已突破传统协同过滤的局限性，转向深度强化学习与时间序列分析的融合应用。以拼多多“秒杀算法”为例，其通过实时分析用户点击流量数据，结合库存波动与促销策略，动态调整商品排序权重。此类系统需解决冷启动与数据稀疏性问题，例如引入用户短期行为反馈(如页面停留时长)作为补充特征，并通过在线学习机制快速更新模型参数[4]。值得注意的是，实时推荐对算力要求极高，部分平台采用边缘计算技术降低延迟，但算力集中化可能加剧数据垄断争议。

2.1.3. 定价策略：大数据驱动的动态定价

大数据驱动的动态定价通过需求预测模型与市场供需关系分析实现价格弹性优化。携程“大数据杀熟”事件揭示了该技术的伦理困境：算法基于用户设备类型、历史支付意愿等非透明变量进行歧视性定价，导致消费者信任流失[5]。当前技术迭代中，部分平台尝试引入公平性约束机制，例如限制价格波动阈值或公开基础定价规则，但算法黑箱特性仍使监管面临挑战。研究表明，动态定价需兼顾效率与透明度，如采用差分隐私技术模糊化用户特征，或在价格决策中嵌入第三方审计节点[6]。

2.2. 隐私风险的具体表现

在 AI 驱动的个性化营销场景中，隐私风险主要表现为数据过度收集、算法黑箱化及数据滥用三方面，其具体特征与危害性如下。

2.2.1. 数据过度收集：强制获取非必要信息

当前电子商务平台普遍存在超越服务功能需求收集用户敏感信息的行为。例如，某社交电商 App 在用户注册时强制要求授权访问通讯录与地理位置，而此类权限与其核心业务逻辑无直接关联。研究表明，59%的 App 存在过度收集位置信息问题，28%涉及通讯录权限滥用，甚至工具类应用亦存在此类违规行为[7]。这种“全量采集”模式违背了《个人信息保护法》确立的“最小必要原则”，导致用户隐私暴露面呈指数级扩张。

2.2.2. 算法黑箱化：用户知情权缺失

个性化推荐算法的决策逻辑缺乏透明度，形成新型数字霸权。以抖音电商为例，其推荐机制通过深度学习模型构建“信息茧房”，但用户既无法获知数据加工规则，亦难以追溯特定商品推送的决策依据。

算法黑箱化导致两大风险：其一，用户画像构建过程中可能嵌入歧视性参数；其二，决策偏差引发的权益损害缺乏救济路径。实证研究表明，68%的用户对推荐算法产生被操控感，进而催生隐私焦虑[8]。

2.2.3. 数据滥用风险：营销数据流向第三方

数据流转过程中的安全边界模糊化加剧了滥用风险。某头部电商平台曾发生用户行为数据泄露事件，超 2 亿条包含购物偏好、设备标识等敏感信息的数据包在暗网流通，溯源发现系第三方广告监测 SDK 存在安全漏洞所致[9]。更值得警惕的是，开放平台接口使得用户数据可在未经二次授权情况下被关联企业共享，形成跨域数据监控网络。此类风险已催生新型犯罪模式，2022 年网络黑产中 32%的案件涉及合法获取数据的非法使用[10]。

3. 电商隐私保护的法律与行业挑战

3.1. 法律冲突点

其一，同意机制失效：电商平台冗长隐私条款的“形式合规”。欧盟《通用数据保护条例》(GDPR)第 7 条要求数据主体同意需“自由、特定、知情且明确”，但实践中电商平台常将冗长的隐私条款嵌套于用户协议中，导致“知情同意”沦为形式合规。研究表明，超 80%的用户未完整阅读隐私政策即勾选同意，其决策权被冗长文本稀释，形成“同意疲劳”[11]。例如，GDPR 虽要求企业提供“一键撤回”功能，但多数平台将该选项隐藏于二级菜单，实质上削弱了用户控制权。这种合规表象与实质权利保护的割裂，暴露了法律执行中的结构性矛盾。

其二，最小必要原则模糊：数据收集范围与营销目的的关联性争议。数据收集范围与营销目的的关联性判定缺乏明确标准，典型如“人脸识别用于优惠券发放”场景。尽管 GDPR 强调数据处理的“目的限定”原则，但生物识别信息的使用边界仍存争议。例如，某电商平台以“提升用户体验”为由采集用户面部特征，却未证明该数据与优惠券发放的必要性关联，引发监管质疑[12]。这种模糊性导致企业常以“业务创新”为名扩大数据采集，而监管机构因技术认知滞后难以精准裁量，形成法律适用的灰色地带。

3.2. 行业特殊性挑战

其一是跨境数据流动：跨境电商(如 SHEIN)面临欧盟 GDPR 与中国数据出境安全评估的双重压力。

跨境电商企业(如 SHEIN)需同时满足欧盟 GDPR 与中国《数据出境安全评估办法》的要求，面临制度冲突。例如，GDPR 要求数据主体可随时撤回同意，而中国规定重要数据出境需通过安全审查，两者在操作层面存在张力[13]。在这种情况下，跨境电商很有可能因未通过中国数据出境评估而暂停欧盟业务，损失扩大，凸显双重监管的成本压力。此外，GDPR 的域外效力与我国数据主权主张的博弈，进一步加剧了企业的合规不确定性[14]。

其二是平台责任边界的认定难题：电商平台是否需为商家违规使用数据担责？电商平台是否需为入驻商家违规使用数据担责，尚未形成统一裁判标准。以拼多多商户数据泄露事件为例，平台主张其仅提供技术服务，但法院认为平台未尽到数据接口权限审核义务，需承担连带责任[15]。此类争议暴露了现行法律中“技术中立”原则与“实质控制”标准的冲突。欧盟近年通过“守门人制度”强化平台责任，但我国《电子商务法》第 25 条仅作原则性规定，导致司法裁量缺乏一致性依据。

4. 电商合规策略：技术、治理与用户赋权

4.1. 技术优化路径

隐私计算技术的深化应用是平衡数据效用与隐私保护的核心策略。在跨平台数据合作场景中，电商

企业应构建联邦学习框架，通过分布式模型训练实现数据“可用不可见”。例如，京东与品牌方基于水平联邦学习(HFL)进行联合需求预测，各参与方仅共享加密的梯度参数而非原始数据，既提升供应链协同效率，又规避数据泄露风险。此外，差分隐私技术的本地化部署可优化用户行为分析。以苹果SKAdNetwork 为例，电商广告归因通过添加统计噪声模糊个体轨迹，使广告主仅获取聚合效果数据，有效抑制用户画像的精准追踪。技术实施中需结合场景动态调整隐私预算(ε 值)，在数据精度与隐私强度间实现帕累托最优。

4.2. 平台治理创新

透明化设计是破解“算法黑箱”信任危机的关键。平台需建立用户数据看板，如淘宝“隐私实验室”可视化数据流向，明确标注数据采集目的、处理周期及第三方共享范围，降低用户认知负荷。同时，算法解释功能的强制性嵌入成为合规刚需。欧盟《数字服务法案》(DSA)要求电商平台提供“为何看到此商品”的简明说明，此类设计可借鉴至商品排序、价格歧视等场景，通过自然语言生成技术输出非技术性解释。在权限管理层面，分级授权机制需区分功能必要性：基础服务(如购物车)默认开放，而个性化推荐等非必需功能应实施“二次授权”，采用动态弹窗与渐进式引导提升用户控制感知。

4.3. 用户权益增强

简化控制选项需突破“隐蔽设计”惯性。Instagram 的“敏感内容控制”模式证明，一键关闭个性化推荐的显性入口可提高用户主权意识，电商平台应将该功能置于账户设置首页，并配以情景化示例说明其影响。此外，数据收益共享机制的探索需重构数据价值链。日本乐天“数据积分兑换”模式将用户行为数据转化为可交易的虚拟资产，电商企业可参考此类“数据贡献度计量模型”，允许用户通过数据授权换取折扣、优先服务或公益捐赠额度，实现隐私权益的经济转化。该机制需嵌入区块链技术确保贡献记录的不可篡改性，并通过智能合约自动执行收益分配。

5. 总结

在电子商务领域，人工智能(AI)技术的广泛应用正在重塑个性化营销的格局。然而，AI 驱动的个性化营销在提升效率和用户体验的同时，也引发了隐私保护和合规性方面的挑战。电商 AI 营销的可持续性依赖于“效率–隐私–信任”三角平衡。AI 技术通过数据分析和算法优化，能够精准预测消费者需求，提升营销效率和客户体验。然而，这种高效性往往伴随着对用户数据的大量收集和分析，这可能引发隐私泄露和数据滥用的风险。因此，企业在实施 AI 营销时，必须在提升效率和保护隐私之间找到平衡点。短期内，企业需强化法律执行，确保合规操作；长期来看，则需探索隐私计算技术的突破，以实现高效、安全的个性化营销。通过多方协作和技术进步，AI 营销将在保障用户隐私的前提下，继续为电子商务行业带来深远影响。

致　谢

衷心感谢期刊编辑及匿名评审专家对本文的严谨审阅与建设性意见，你们专业细致的指导使本文在电子商务法律规制与营销策略的交叉研究维度上获得了显著提升。

参考文献

[1] 刘权. 最严数据法律将如何影响数字经济企业[J]. 中国工程咨询, 2018(7): 108-111.

[2] 施建俊, 王瑾. 个人信息保护法解读: 常见合规场景与应对[J]. 信息安全与通信保密, 2021(11): 19-29.

[3] 王莹. 算法侵害类型化研究与法律应对——以《个人信息保护法》为基点的算法规制扩展构想[J]. 法制与社会

发展, 2021, 27(6): 133-153.

[4] 田江, 魏乐, 卢格润. 个性化推荐与智能化应用[J]. 中国工业和信息化, 2022(12): 67-71.

[5] 孙奇涛. 贴身服务与潜在伤害: 精准营销中的隐私消费研究[D]: [硕士学位论文]. 沈阳: 沈阳师范大学, 2021.

[6] 刘婷婷. 基于同态加密的聚类算法及其在精准营销中的应用研究[D]: [硕士学位论文]. 南京: 南京邮电大学, 2021.

[7] 陶凤. 隐私保护从“剪刀手”开始[J]. 青年记者, 2019(27): 52.

[8] 肖玉琴. 网络行为广告感知特性对消费者犬儒反应的影响: 隐私担忧的中介效应[J]. 国际新闻界, 2023, 45(5): 121-139.

[9] 关振智. Android 跨组件隐私泄露检测关键技术研究[D]: [硕士学位论文]. 北京: 北京邮电大学, 2023.

[10] 韩轶. 网络数据安全领域的企业刑事合规体系建构[J]. 江西社会科学, 2023, 43(1): 53-61.

[11] 邹珊, 傅思宇, 罗珏, 等. PR 数据主体同意制度剖析及应对策略——以谷歌案为例[J]. 成都理工大学学报(社会科学版), 2020, 28(1): 61-67.

[12] 林凌, 贺小石. 人脸识别的法律规制路径[J]. 法学杂志, 2020, 41(7): 68-75.

[13] 俞胜杰, 林燕萍. 《通用数据保护条例》域外效力的规制逻辑、实践反思与立法启示[J]. 重庆社会科学, 2020(6): 62-79.

[14] 李鑫. 《通用数据保护条例》实施对中国出口效率的影响[J]. 中国流通经济, 2024, 38(10): 98-114.

[15] 李旻. “网络用户隐私权”在跨境电商中的侵权法律适用研究[D]: [博士学位论文]. 上海: 华东政法大学, 2021.