

人工智能在电商个性化推荐中的应用、挑战及治理路径

陈英豪, 周蕾蕾

贵州大学管理学院, 贵州 贵阳

收稿日期: 2025年6月6日; 录用日期: 2025年6月20日; 发布日期: 2025年7月14日

摘要

在数字化时代, 人工智能驱动的个性化推荐系统已成为电子商务生态的核心引擎, 通过精准匹配供需关系显著提升商业效率。本文系统探讨人工智能在推荐系统中的技术应用、挑战及治理路径。研究显示, 人工智能等计算机技术通过用户画像的动态构建与行为预测, 实现了对用户的精准推送, 以此大幅增强了用户的参与度与购买意愿。然而, 技术跃进伴随深刻的伦理风险。数据隐私边界的消解、算法偏见对公平性的侵蚀等问题, 均暴露了技术理性对人性尊严与社会公平的威胁。对此, 本文提出“技术创新 - 制度约束 - 公众参与”协同治理框架。强调以“人的主体性”为核心重构智能商业生态, 在技术创新中注入伦理自觉, 最终实现从“流量攫取”向“价值共创”的范式转型。

关键词

人工智能, 电子商务, 个性化推荐, 治理路径

Application, Challenges and Governance Paths of Artificial Intelligence in Personalized Recommendations in E-Commerce

Yinghao Chen, Leilei Zhou

School of Management, Guizhou University, Guiyang Guizhou

Received: Jun. 6th, 2025; accepted: Jun. 20th, 2025; published: Jul. 14th, 2025

Abstract

In the digital age, AI-powered personalized recommendation systems have become the core engine

文章引用: 陈英豪, 周蕾蕾. 人工智能在电商个性化推荐中的应用、挑战及治理路径[J]. 电子商务评论, 2025, 14(7): 878-883. DOI: 10.12677/eci.2025.1472248

of the e-commerce ecosystem, significantly enhancing business efficiency by precisely matching supply and demand. This paper systematically explores the technical applications, challenges, and governance pathways of artificial intelligence in recommendation systems. Research indicates that computer technologies, such as AI, achieve precise user targeting through the dynamic construction of user profiles and behavioral prediction, thereby substantially enhancing user engagement and purchase intention. However, technological leaps forward are accompanied by profound ethical risks. Issues such as the erosion of data privacy boundaries and the undermining of fairness by algorithmic biases expose threats posed by technological rationality to human dignity and social equity. In response, this paper proposes a collaborative governance framework integrating “technological innovation-institutional constraints-public participation.” It emphasizes reconstructing the intelligent business ecosystem around the core principle of “human agency,” infusing technological innovation with ethical awareness, and ultimately realizing a paradigm shift from “traffic extraction” to “value co-creation.”

Keywords

Artificial Intelligence, E-Commerce, Personalized Recommendation, Governance Pathway

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

在数字化生存的当代图景中, 电子商务已从单纯的交易渠道演化为重构人类消费行为的技术生态系统。人工智能驱动的个性化推荐系统, 作为这一生态系统的核心神经中枢, 不仅重塑了“人-货-场”的互动逻辑, 更在深层次上挑战着传统商业伦理的认知边界。这种以算法为媒介的“数字看门人”机制, 正在将海德格尔所言的“技术座架”具象化——技术不仅服务于人, 更通过数据捕获与行为预测建构着人的需求本身。

技术的跃进始终伴随着伦理的诘问。研究显示, 京东商城的推荐算法贡献了超过 10% 的订单量, 而亚马逊的推荐系统更是带来了 35% 的销售额[1]。这些成绩的背后, 是平台对数十亿条用户行为数据的全面追踪和分析。这种追求效率的技术逻辑, 正在数字空间中重现法国思想家福柯所说的“规训权力”: 平台利用推荐算法悄无声息地操控着人们的注意力, 而用户则在“猜你喜欢”这类看似贴心的服务中, 不知不觉地放弃了自己独立思考的能力。正因如此, 欧盟委员会在 2023 年发布的《人工智能法案》修正案中特别指出, 电商推荐系统已被归类为“高风险 AI 系统”, 这意味着对技术的治理开始从单纯的数据安全扩展到对人类认知自主权的保护。

然而, 在学术界, 关于这一问题的讨论却显得割裂: 一方面, 技术研究主要集中在如何优化模型、提升商业效益(比如用强化学习来调整商品价格), 人工智能通过分析用户的浏览历史、购买记录和搜索行为, 为用户提供定制化的产品推荐, 提高用户参与度和购买率[2]-[4]。另一方面, 伦理层面的批评又往往停留在抽象原则的争论上(例如算法是否公平), 聚焦在深度学习模型决策透明性不足[5]、价格歧视等[6], 这种割裂导致鲜有研究深入剖析推荐算法这一“技术黑箱”如何重塑市场权力结构, 亦缺乏对“个性化服务”与“人的异化”之间复杂关联的反思。本文旨在突破将技术视为中性工具的传统分析框架, 通过批判性审视“技术巨兽”与“人的主体性”之间的持续张力, 揭示 AI 推荐系统在驱动商业效率的同时所隐含的认知控制、数据物化及权力失衡等深层问题, 从而构建一个关注技术伦理影响的理论视角, 为塑

造更具伦理意识的智能商业生态提供理论支撑。

2. 人工智能在推荐系统中的技术应用

2.1. 用户画像与行为预测

人工智能通过协同过滤和深度学习模型(如 Transformer)对用户的浏览记录、点击行为、购买历史及页面停留时长等多维度数据进行深入分析[7]。通过百万级用户数据构建多维标签(如消费频率、退货率、商品偏好),形成动态用户画像,并对未来的行为趋势进行精准预测。例如,淘宝的“猜你喜欢”模块采用实时强化学习算法不断优化推荐策略,根据用户的即时反馈调整推荐内容,从而实现了点击率提升 20% 以上的显著效果(阿里巴巴, 2024 年财报)。

2.2. 多模态内容理解

随着自然语言处理(NLP)和计算机视觉(CV)技术的不断发展,推荐系统已经能够对商品的文字描述、图片、视频等多种形式的内容进行智能解析与语义理解。通过跨模态语义匹配技术,系统可以将不同形式的内容统一映射到相同的语义空间中,从而更准确地匹配用户兴趣。汤志鹏(2021)提出基于 Faster R-CNN 的视频内容检测方案,并结合混合推荐算法提高推荐效果[8];冯勇等(2021)则通过融合视频内容特征与弹幕文本分析,进一步提升了推荐模型的准确率和召回率[9]。这些技术手段为用户提供了更精准的推荐,从而增强其参与度。

2.3. 商业价值转化

人工智能驱动的推荐系统不仅提升了用户体验,也直接推动了平台的商业价值增长。通过精准推荐,系统有效缩短了用户的决策路径,形成了“需求识别-智能推荐-快速消费-数据反馈”的高效闭环。京东的 AI 推荐系统(Telepath 模型)通过深度学习用户行为和商品属性,显著提升了用户活跃度和购买意愿。点击率首次发布后提升 1.59%,第二次发布后提升 2.95%。商品交易总额首次发布后增长 8.16%,第二次发布后激增 41.75%。订单量首次发布后增长 8.74%,第二次发布后增长 41.37% [10]。这种数据驱动的推荐机制,正在成为电商平台实现精细化运营和利润增长的重要支撑。相关的实验显示,优化后的算法可使交易成功率从 38.4%提升至 87.2% [11],点击率与购买转化率显著增长[12]。

3. 伦理挑战与批判性反思

3.1. 数据隐私的边界消解

一是过度采集风险。个性化推荐系统需要收集大量用户个人信息,包括行为数据、消费习惯等,这些信息若未经过加密或脱敏处理,可能被滥用或泄露,从而威胁用户的隐私安全[13]。当前技术已能捕捉用户微观行为痕迹,如页面滚动速度、光标轨迹、设备传感器数据(如加速度计、陀螺仪)等。例如,某新闻 App 通过分析用户订阅频道、社交账号登录记录甚至浏览器书签生成精准画像,而这些数据收集往往未明确告知用户其用途。此外,部分 App 存在“越界索权”现象,如视频软件要求访问运动数据、资讯类 App 开启相机和麦克风权限等,远超业务所需范围。2025 年 4 月,携程金融因通过第三方代码(如信贷评估 SDK)暗中收集设备信息、通讯录等敏感数据被通报,其“打包授权”模式将基础信息与敏感信息合并处理,违反了《中华人民共和国个人信息保护法》最小化原则。

二是数据的再次利用风险。随着数据共享和跨平台使用,个人隐私数据的“再次利用”增加了泄露的可能性[14]。欧盟《通用数据保护条例》(GDPR)要求数据使用需明确告知目的,但平台常以“服务优化”为名模糊化处理。例如,TikTok 曾试图以“合理利益”为基础处理用户数据用于定向广告,遭意大

利监管机构警告, 因其未清晰说明数据用途及用户反对权。并且, 平台隐私协议中常规定数据可有条件共享, 但共享范围和安全标准不透明。例如, 用户浏览婚恋平台的痕迹可能被转售给其他机构用于精准营销, 而用户难以追踪数据流向。

3.2. 算法偏见与歧视强化

一是价格歧视。动态定价算法基于用户支付意愿差异化报价, 2021 年亚马逊“大数据杀熟”事件引发多国监管调查。亚马逊通过分析用户浏览历史、设备类型(如 iOS 用户比安卓用户支付意愿更高)、地理位置等数据, 对同一商品实施差异化定价。2021 年, 美国联邦贸易委员会(FTC)对亚马逊展开调查, 欧盟则依据《数字服务法案》要求平台公开定价算法逻辑, 防止滥用动态定价权。就国内而言, 2024 年 11 月启动的“清朗·网络平台算法典型问题治理”专项行动明确禁止利用算法实施大数据杀熟, 要求平台公示价格计算规则, 并建立用户申诉渠道。

二是造成窄化效应。推荐系统通过算法精准推送内容, 使用户陷入“信息茧房”和“过滤气泡”, 导致用户仅接触到符合其已有兴趣和观点的信息, 从而限制了视野的广度和多样性[15]。社交媒体通过推荐算法(如 TikTok 的 For You 页面)构建“信息孤岛”。欧盟《数字服务法》要求平台提高推荐算法透明度, 但多数平台仍以“服务优化”为由模糊算法逻辑。TikTok 就曾因用户无法关闭个性化推荐被投诉, 后迫使其在欧盟推出“取消推荐”的选项。

三是其成瘾性设计。尼尔·埃亚尔的“钩子模型”(触发-行动-可变奖励-投入)被广泛应用于电商设计[16]。例如, 淘宝的《合成大蛋糕》游戏就通过即时奖励(如得分、成就)刺激用户持续参与。此外, 短视频电商还会通过“限时折扣”“好友拼单”等设计, 利用害怕错过的心理诱导冲动消费。例如, 拼多多的“砍价免费拿”功能通过社交裂变制造紧迫感, 用户为完成目标可能过度分享链接。

4. 治理路径：技术、法律与伦理的协同

人工智能在电子商务推荐系统中的治理需要技术革新、法律约束与伦理准则的协同配合, 构建多维度、动态化的治理框架。这一框架既要保障技术创新带来的商业效率, 也需防范技术滥用对社会公平与个人权利的系统性侵蚀。

4.1. 技术透明性与可解释性

当前, 推荐系统普遍存在“黑箱化”问题, 用户难以理解算法决策逻辑。为此, 可解释性人工智能(XAI)技术的应用至关重要, 通过可视化解释推荐理由, 增强用户信任[17]。技术的自我纠偏构成了治理的深化实施层, 需建立分层的 XAI 应用体系: 在基础层, 利用 SHAP 值可视化等技术(如京东“推荐因子透视”)实时展示用户特征的具体影响(如“消费能力标签影响度 35%”); 在场景层, 嵌入对抗性测试工具(如阿里 FairRec 系统)自动检测价格歧视与信息茧房倾向; 在决策层, 开发反事实解释模块(如亚马逊 What-If 面板), 模拟用户行为改变对推荐结果的影响(例: “若您月消费降至 2000 元, 推荐商品将减少奢侈品 40%”), 从而实现更主动的算法治理与风险防范。此外, 开源算法框架的推广可促进技术民主化。阿里巴巴于 2024 年开源其部分推荐模型代码, 并联合高校建立“可解释 AI 实验室”, 推动学术界与企业界的协作研究。技术透明化还需嵌入用户控制机制, 如亚马逊推出的“推荐偏好设置”功能, 支持用户手动调整兴趣标签权重, 减少算法对个人行为的单向操控。

4.2. 法律规制与行业自律

法律在规范技术应用时, 必须清晰划定边界并实施动态监管以应对层出不穷的新型风险。这一原则在全球数据隐私保护领域已有实践: 欧盟《通用数据保护条例》确立的“数据最小化”和“目的限定”原

则提供了重要范本;《中华人民共和国个人信息保护法》第二十四条则明确禁止“大数据杀熟”,要求平台公开算法歧视判定标准与申诉渠道。有效的技术治理体系还需行业自律作为有力补充。国际商业机器协会(ICBA)发布的《AI 伦理实施指南》倡导企业建立伦理审查委员会并对推荐算法进行人权影响评估;企业层面,拼多多 2025 年推出的“算法伦理白皮书”承诺限制用户数据跨业务共享并设立独立第三方审计机构,展现了企业自我规制的潜力。在此基础上,我们认为法律规制的核心应聚焦于构建算法审计双轨制:一方面建立企业自审机制,要求年交易总额(GMV)超百亿的平台设立伦理委员会并按季度提交使用专业工具(如 MIT 的 Audit-AI)的算法偏见检测报告;另一方面实施第三方强制审计,当用户投诉率超过预设阈值(如 5%)时,由国家认证机构参照欧盟 DSA 第 27 条熔断机制要求,启动基于区块链存证的独立审计。同时,用户行为疲劳防控措施必须严格落实,依据《互联网推荐系统管理规定》第八条,系统应于每日 21:00 后自动切换至“多样性模式”,并在用户连续浏览同品类内容超 30 分钟后强制插入跨兴趣内容(例如向数码产品用户推荐园艺信息),以保障用户福祉与选择多样性。

4.3. 伦理框架与社会共治

用户认知能力的提升是构建算法治理坚实社会根基的关键,其核心在于将公众从治理的被动客体转化为能动的参与主体。实现这一目标需要多维度协同推进。教育是基础,必须系统性地强化算法素养,这包括将相关内容纳入基础教育体系,如欧盟“数字公民计划”在中小学课程中教授识别推荐系统偏见与诱导机制;中国消费者协会的“反算法陷阱”公益项目通过案例教学揭示“过滤气泡”与成瘾性设计的危害。其次,社会共治的关键是通过数据资产化运营赋予用户数据主权与经济激励,可借鉴贵阳大数据交易所(2025)试点的用户数据银行机制,用户授权数据形成“数字资产”,平台调用时需支付数据积分(如 1 积分 = 0.1 元折扣券),用户可随时冻结敏感数据访问,该模式已显著抑制数据滥用(据《贵阳数据要素市场化报告》,相关投诉下降 76%)。此外,通过协同治理平台为用户提供便捷的参与和救济途径,例如在数据追踪工具(如京东“数据沙盒”)中集成功能,支持用户一键申诉至网信办算法治理中心。唯有通过这种系统性提升素养、提供工具、建立保障制度和完善参与机制的综合路径,方能有效将用户认知转化为治理力量,使其真正成为算法时代的能动主体。

综上,技术、法律与伦理的协同治理需突破单一维度的局限,形成“技术创新-制度约束-公众参与”的闭环。唯有如此,才能在商业效率与社会价值之间达成动态平衡,推动人工智能推荐系统向“以人为本”的智能生态演进。

5. 结论

人工智能驱动的个性化推荐系统深刻重构了电子商务的供需匹配逻辑,其技术效能的跃升与伦理风险的凸显,共同揭示了技术工具理性与社会价值理性之间的深刻张力。数据隐私边界的消解、算法偏见的系统性强化以及用户认知自主权的隐性让渡,则进一步暴露了技术单向度发展对社会公平与人性尊严的潜在威胁。针对上述挑战,本文提出的“技术创新-制度约束-公众参与”协同治理框架,为破解效率与伦理的二元对立提供了实践路径。然而,人工智能推荐系统的演进不应止步于效率的迭代。归根结底,唯有在技术创新中注入伦理自觉,在制度设计中嵌入人文关怀,方能实现智能商业从“流量攫取”向“价值共创”的范式转型——这一转型既是技术发展的必然选择,更是数字文明迈向成熟的必经之路。

参考文献

- [1] Nguyen, T.T., Dang, M.T., Luong, A.V., et al. (2019) Multi-Label Classification via Incremental Clustering on an Evolving Data Stream. *Pattern Recognition*, 95, 96-113. <https://doi.org/10.1016/j.patcog.2019.06.001>
- [2] He, X., Liao, L., Zhang, H., Nie, L., Hu, X. and Chua, T.S. (2017) Neural Collaborative Filtering. *Proceedings of the*

26th International Conference on World Wide Web, Perth, 3-7 April 2017, 173-182.

<https://doi.org/10.1145/3038912.3052569>

- [3] 赖小馨. 基于人工智能的个性化推荐系统在电子商务中的应用[J]. 知识经济, 2024(6): 37-39.
- [4] Panigrahi, D. and Karuna, M. (2021) A Review on Leveraging Artificial Intelligence to Enhance Business Engagement in Ecommerce. *International Journal of Research Publication and Reviews*, 2, 239-250.
- [5] 高广尚. 可解释推荐模型中的可解释性方法研究综述[J]. 数据分析与知识发现, 2024, 8(8): 6-19.
- [6] 承上. 人工智能时代个性化定价行为的反垄断规制——从大数据杀熟展开[J]. 中国流通经济, 2020, 34(5): 121-128.
- [7] 项亮. 推荐系统实践[M]. 北京: 人民邮电出版社, 2012.
- [8] 汤志鹏. 短视频中的内容检测与个性化推荐算法研究[J]. 信息与电脑(理论版), 2021, 33(13): 39-42.
- [9] 冯勇, 邹宝旭, 徐红艳. 视频内容特征与弹幕文本相结合的短视频推荐模型[J]. 辽宁大学学报(自然科学版), 2021, 48(2): 108-115.
- [10] Wang, Y., Xu, J., Wu, A., Li, M., He, Y., Hu, J., et al. (2018) Telepath: Understanding Users from a Human Vision Perspective in Large-Scale Recommender Systems. *Proceedings of the AAAI Conference on Artificial Intelligence*, 32, 467-474. <https://doi.org/10.1609/aaai.v32i1.11243>
- [11] 成保梅. 基于协同过滤的电子商务个性化推荐算法研究[J]. 现代电子技术, 2019, 42(20): 37-39+44.
- [12] 兰玮霞. 某大型 3C 电商平台在电子商务环境下的供应链管理创新实践探索[J]. 消费电子, 2025(2): 146-148.
- [13] 王国霞, 王丽君, 刘贺平. 个性化推荐系统隐私保护策略研究进展[J]. 计算机应用研究, 2012, 29(6): 2001-2008.
- [14] 郭楚怡. 个性化推荐系统对个人信息的“三次使用”: 大数据时代的隐私保护难题[J]. 科技传播, 2021, 13(18): 159-161.
- [15] 黄英辉, 刘辉, 王伟军, 等. 心理图式在应对推荐系统用户过度特化问题中的作用: 基于机器学习的实证研究[J]. 图书与情报, 2024(4): 118-130.
- [16] 尼尔·埃亚尔, 瑞安·胡佛. 上瘾: 让用户养成使用习惯的四大产品逻辑[M]. 北京: 中信出版社, 2017.
- [17] Fassiaux, S. (2023) Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach. *European Journal of Risk Regulation*, 14, 710-730. <https://doi.org/10.1017/err.2023.58>