E-Commerce Letters 电子商务评论, 2025, 14(11), 905-911
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14113516

Hans汉斯

人工智能驱动电商领域发展的作用机制、场景运用及面临的风险

唐慧琳

贵州大学公共管理学院，贵州 贵阳

收稿日期：2025年9月18日；录用日期：2025年10月10日；发布日期：2025年11月14日

摘　要

随着人工智能技术的快速发展，其在电商领域的应用日益深入，显著推动了行业的智能化转型。本文系统分析了人工智能驱动电商发展的核心作用机制，包括高效数据采集与分析、自然语言处理、计算机视觉、虚拟现实与知识图谱等关键技术的应用。进一步探讨了人工智能在电商数据分析、个性化推荐、智能客服、虚拟直播和供应链管理等场景中的创新实践。同时，本文结合相关案例与数据，指出其在数据安全、算法偏见、系统脆弱性、虚假信息与责任认定等方面面临的潜在风险，并提出更具针对性与操作性的治理路径与伦理建议，以促进人工智能在电商领域的健康、可持续发展。

关键词

人工智能，电商，作用机制，场景运用

The Role Mechanism, Scenario Applications, and Associated Risks of Artificial Intelligence in Driving the Development of E-Commerce

Huilin Tang

School of Public Administration, Guizhou University, Guiyang Guizhou

Received: September 18, 2025; accepted: October 10, 2025; published: November 14, 2025

Abstract

With the rapid advancement of artificial intelligence (AI) technology, its application in the e-

文章引用: 唐慧琳. 人工智能驱动电商领域发展的作用机制、场景运用及面临的风险[J]. 电子商务评论, 2025, 14(11): 905-911. DOI: 10.12677/ecl.2025.14113516

commerce sector has become increasingly extensive, significantly promoting the intelligent transformation of the industry. This paper systematically analyzes the core mechanisms through which AI drives the development of e-commerce, including the application of key technologies such as efficient data collection and analysis, natural language processing, computer vision, virtual reality, and knowledge graphs. Furthermore, it explores innovative practices of AI in various e-commerce scenarios, including data analysis, personalized recommendations, intelligent customer service, virtual live streaming, and supply chain management. Meanwhile, drawing on relevant cases and data, this paper identifies potential risks in data security, algorithmic bias, system vulnerability, disinformation, and accountability attribution. It further proposes more targeted and actionable governance approaches and ethical recommendations to promote the healthy and sustainable development of artificial intelligence in the e-commerce sector.

Keywords

Artificial Intelligence, E-Commerce, Mechanisms of Action, Scenario Applications

1. 引言

电子商务作为数字经济的重要组成部分，近年来在全球范围内持续高速发展。随着数据规模的急剧增长和用户需求的日益多样化，传统电商模式面临效率瓶颈与体验短板。人工智能技术的兴起为解决这些问题提供了新的可能。通过机器学习、自然语言处理、计算机视觉等技术的深度融合，人工智能正在从数据驱动、流程优化、体验提升等多个维度重塑电商生态。

在学术研究方面，已有诸多文献探讨人工智能在电商中的应用。例如，郝京杰(2019) [1]指出人工智能与物联网结合可显著提升电商运营效率；包俊先与洪虹(2024) [2]研究了生成式人工智能在电商中的实际应用与潜在风险；杨柳(2023) [3]分析了智能技术在电商营销中的发展趋势；潘春会(2024) [4]强调大数据驱动对电商行业的核心作用；姚凯等(2018) [5]则通过多源大数据构建了个性化推荐系统的效果评估框架。这些研究多从技术应用或单一场景出发，缺乏对人工智能驱动电商发展的系统性机制分析，尤其对跨技术融合、多场景协同及其衍生的新型风险缺乏深入探讨。

本文在既有研究基础上，系统构建了人工智能赋能电商发展的“技术–场景–风险”三维分析框架。第一，揭示 AI 通过数据智能、交互智能与决策智能三大机制重构电商价值链的内在逻辑；第二，全面梳理 AI 在电商前端营销、中端运营与后端供应链中的创新应用场景；第三，深入剖析 AI 规模化应用后面临的数据安全、算法伦理、系统脆弱性等新型风险，并提出协同治理路径。本研究的主要贡献在于整合技术视角与管理视角，为电商企业的智能化转型提供理论支撑与实践指南，同时为人工智能在电子商务领域的合规发展提供风险治理参考。

2. 人工智能技术概述

人工智能(Artificial Intelligence，简称 AI)是计算机科学的一个重要分支，致力于构建能够模仿人类认知与决策过程的智能系统。其核心目标是开发出可理解环境、进行学习、推理并适应变化的机器，使其能够在多种任务中实现类似人类的智能行为。相关研究涵盖机器人技术、语音与图像识别、自然语言处理等多个方向，旨在扩展机器在复杂场景中的感知、分析与交互能力[1]。通过使机器学习和模仿人类的

认知与行为模式，人工智能能够协助人类完成许多复杂且具有挑战性的任务，弥补人类在某些领域的能力局限。自诞生以来，人工智能已广泛应用于众多行业，成为推动科学进步与社会发展的关键力量，并被公认为21世纪最具影响力的技术之一。然而，人工智能并不等同于人类智能，其未来发展仍存在显著不确定性，或能像人那样思考、也可能超过人的智能。

3. 人工智能技术如何驱动电商领域的发展

3.1. 高效数据采集和分析

目前，众多主流搜索引擎和大型电商平台正积极引入生成式人工智能(Generative AI)技术，以实现更高效、更智能的数据采集与热点分析，从而显著提升商业信息推送的精准度和用户转化效率[2]。其工作原理主要包括：数据识别与采集(利用网络爬虫、API接口和多模态感知技术，持续获取文本、图像、音频和用户行为日志等原始信息)、数据特征提取(将原始数据转化为机器可理解和处理的特征表示)、数据生成(基于学习到的特征和模式，生成新的数据或内容)、生成结果质量控制(确保生成内容符合准确性、相关性和伦理规范等要求)、迭代反馈(借助反馈数据持续优化模型表现)。

3.2. 自然语言处理技术的成熟

自然语言处理技术是一种实现人类语言与计算机系统之间交互的关键技术，主要包括语音识别、语义理解等功能。在电子商务领域，该项技术能够协助企业精准捕捉用户的需求与偏好，从而推动客户服务、个性化推荐等环节的智能化升级。目前，诸多主流电商平台已广泛引入自然语言处理技术，典型应用包括阿里巴巴的“智能客服”与京东的“小白”智能助手，它们通过自然语言对话方式为用户提供高效、便捷的在线支持[3]。

3.3. 计算机视觉技术的实践

计算机视觉(Computer Vision, CV)是一门研究如何让机器“看见”并“理解”数字图像和视频内容的科学。它旨在复制乃至超越人类视觉系统的能力，其核心目标不仅仅是“捕获”图像(这是摄像头的功能)，更是对图像中的内容进行识别、分类、分析、重构乃至决策。深度学习(Deep Learning)与卷积神经网络(CNN, Convolutional Neural Network)是当前CV领域最主流和强大的技术。CNN通过多层的“卷积”操作，能够自动、高效地从原始像素中分层提取特征(从边缘到形状再到完整物体)，极大地提升了识别的准确率。

3.4. 虚拟现实技术的结合

VR是一种通过计算机生成高度仿真的三维虚拟环境，并借助头戴式显示器、手柄控制器、触觉反馈设备等交互装置，为用户提供沉浸式、交互式体验的综合性技术[4]。其核心技术架构包括三维环境建模、实时图形渲染、空间定位追踪、多模态交互以及物理引擎仿真等关键模块，此类技术共同构成了虚拟现实系统的底层支撑框架。同时，基于分布式网络架构的多用户协同引擎，异地师生可共享同一虚拟实验环境，从而实现实时协作与数据同步。简单来说，人工智能(AI)与虚拟现实(VR)技术的结合，旨在创造出一个不仅能够沉浸其中，更能感知、理解、学习并与用户进行智能交互的虚拟世界。AI是让VR世界变得“聪明”和“有活力”的大脑。

3.5. 知识图谱技术的运用

在电商领域的核心功能在于通过构建大规模、结构化的实体关系网络来实现深层次的语义理解与智能推理。它不仅仅是对商品进行基础分类，而是将商品、用户、品牌、属性、使用场景乃至外部知识融为

一体，形成一个互联互通的知识系统。例如，对于一款“手机”，知识图谱不仅能识别它属于“电子产品”类别，更能建立其与“充电器、手机壳、耳机”等配件的互补关系，与“华为、苹果”等品牌的关联关系，与“5G 技术、OLED 屏幕”等技术特性的归属关系，甚至与“户外拍摄、游戏性能”等使用场景的适用关系。

4. 人工智能在电商领域的创新性应用

4.1. 电商数据分析

人工智能技术可以帮助电商企业整理和清洗大规模数据。面对电商交易规模扩大所带来的海量数据挑战，企业可借助人工智能实现自动化数据清洗与整合，有效提升数据的质量、一致性与可信度。在此基础上，人工智能进一步支持对电商数据进行分类与挖掘，通过机器学习算法识别产品特征和消费者行为模式，从而帮助企业更精准地把控消费需求，优化商品定位与营销策略。此外，人工智能还能够实现库存智能预测，分析影响库存水平与周转效率的关键因素，助力企业提升供应链管理能力。

4.2. 个性化产品推荐系统

用户行为分析和个性化推荐是大数据技术的核心应用[5]。电商平台通过采集和分析用户的浏览、搜索、购买等行为数据，能够深入洞察用户的兴趣偏好与行为习惯。依托这些数据，平台可借助机器学习与数据挖掘技术，为用户提供高度个性化的商品及服务推荐。此类推荐不仅显著改善用户体验，也有效提升了购买转化率。例如，亚马逊(Amazon)的推荐系统贡献了其总销售额的 30%以上，通过分析用户的历史交易和浏览行为，电商平台可精准推荐符合其兴趣的商品，从而增强用户的购买意愿与满意度。

随着深度学习与知识图谱等技术的不断发展，推荐系统已逐渐从基于历史数据的静态模式演进为融入实时反馈的动态场景模式。静态推荐依赖于充分收集的用户历史行为，通过监督学习模型训练出用户对商品的偏好，进而筛选出可能感兴趣的商品；而动态推荐则进一步引入实时行为数据，持续更新用户画像，以实现更精准的推荐效果。此外，现有研究不仅限于利用平台内部数据，还尝试整合来自其他网站的用户行为信息，以优化推荐效果，并通过实地实验探索多源大数据驱动的个性化推荐对消费者行为的影响机制[6]。

4.3. 智能客服与虚拟导购

人工智能的早期应用是电商平台客服与导购功能，其主要作用是通过自然语言处理技术模型接收、分析和回应用户的提问和需求。AI 客服能处理大量常见咨询，提供 7 × 24 小时服务，据京东数据显示，其 AI 客服“京小服”年均处理咨询量超 10 亿次，有效解决了大部分常规问题[7]。它们不仅能理解自然语言，还能处理复杂需求，AI 客服正从回答问题向解决问题演进；数字人技术和多模态大模型的结合，创造了虚拟导购。淘宝的“数字人导购”TaoAvatar 基于 3D 高斯重建、语音多模态大模型等技术开发，用户佩戴 XR 设备后可与之自然交互，进行虚拟试穿、试驾等。

4.4. AI 数字人直播

AI 数字人直播是依托生成式人工智能技术构建的虚拟数字化形象，能够实现商品展示、讲解及用户交互等功能，具备持续播出能力强、人力投入成本较低等优势。虚拟主播的涌现，成为人工智能赋能电商直播的又一创新应用。借助计算机图形学、语音合成与自然语言处理等关键技术，平台可生成形象逼真、行为自然的虚拟主播，支持 24 小时不间断直播。该类主播不仅能够依据预设流程介绍产品，还可实时响应用户互动，甚至基于用户反馈动态调整直播内容与表达策略，为用户带来高度个性化的沉浸式购

物体验。《2024 年中国直播电商市场数据报告》也显示，2024 年，直播电商交易规模达到 53,256 亿元，同比增长 8.31%；直播电商用户规模达 6.2 亿人，同比增长 14.81%；直播电商行业企业规模达 7.6 万家，同比增长 216.66%。

4.5. 供应链管理自动化

人工智能的创新性体现为其角色从“前端销售助手”向“后端决策大脑”的深刻转变，实现了对整个供应链体系的预测、自治与全局优化。具体而言，AI 通过融合分析海量多维数据(包括历史销售记录、平台搜索趋势、社交媒体热点甚至天气预报等外部变量)实现对商品未来销量的精准预测，从而指导自动化采购与库存管理，推动企业向“零库存”或“最小库存”的精细化运营目标迈进，阿里巴巴的菜鸟网络通过 AI 预测，将仓储前置准确率提升了 20%，大幅降低了物流成本。在此基础上，系统可依托智能动态定价模型，综合实时竞争对手价格、市场需求波动、库存水位及用户画像等信息，自动调整商品售价，以最大化利润或高效清理库存。真正构建起一个响应敏捷、成本优化、决策智能的现代化电商供应链系统。

5. 人工智能驱动电商领域发展过程中面临的风险及解决路径

5.1. 面临的风险

生成式人工智能在电商行业中的快速应用，不仅给电商行业带来了巨大的商机，还带来了许多风险，部分人利用这些便利的手段对消费者进行欺诈，容易造成使用风险，风险主要包括以下几个方面：

1. 数据安全与隐私泄露风险

人工智能系统需依托海量用户数据开展模型训练与优化，其采集和处理的范畴广泛涵盖用户个人信息、交易记录、搜索偏好、社交关系链等敏感信息，据《2023 年数据泄露成本报告》显示，全球平均数据泄露成本高达 445 万美元，创历史新高[8]。在数据流转与存储过程中，若加密技术落后、访问权限控制不严或发生内部管理漏洞，极易造成大规模数据泄露事件，甚至被不法分子非法获取和恶意利用。此类安全缺陷不仅直接侵害用户隐私权，还可能违反《网络安全法》《个人信息保护法》等法律法规，导致企业面临高额行政处罚、民事赔偿及品牌信誉崩塌等多重危机，最终动摇消费者对数字交易环境的基本信任。

2. 算法偏见与歧视风险

机器学习模型的高度数据依赖性使其无法避免训练数据中潜藏的社会偏见与结构性歧视问题。若训练样本中存在历史上对某一性别、地域、年龄或收入群体的系统性忽略或歧视，算法在进行用户画像、个性化推荐、动态定价或服务分配时，便可能延续并放大这些偏见，导致特定群体遭受不公平待遇。研究显示，一些电商平台的招聘算法曾对女性候选人简历进行降权处理；而在商品推荐中，系统对低收入群体持续推送低价低质商品，容易形成“信息茧房”与“消费陷阱”；动态定价系统可能基于用户设备类型、地理位置等隐含特征实施差异定价，构成价格歧视。这类偏见不仅违背公平原则，还可能引发舆论危机与监管审查。

3. 技术依赖与系统脆弱性风险

随着人工智能在电商客户服务、智能推荐、仓储物流及供应链决策等核心业务中深度嵌入，整个平台运营体系对其产生高度依赖性。一旦关键算法因设计缺陷、数据污染或版本迭代错误而导致预测失灵，或遭到对抗性攻击(如恶意输入误导模型判断)，就可能引发连锁性的运营故障，例如大规模错误推荐、客服对话混乱、库存预测严重偏差、价格设置失误等。这类技术失效在高度自动化的环境中传播极快，若缺乏有效的人工介入和应急机制，可能迅速演变为系统性业务中断，造成重大经济损失并严重损害用户

体验。

4. 虚假信息与欺诈风险

生成式人工智能技术的滥用正成为电商生态的新威胁。恶意行为者可利用 AI 生成技术批量制造高度逼真的虚假商品评论、伪造商品展示图片或视频、模仿真实用户聊天记录以进行刷单炒信，甚至生成针对性的欺诈性营销内容与钓鱼链接。据《2024 年网络黑色产业链报告》估算，AI 生成的虚假评论和商品图片占比已接近 15%，且识别难度不断加大。由于生成内容日益难以被普通用户辨别，此类行为不仅严重误导消费者购买决策、损害其财产安全，更从根本上侵蚀电商平台赖以生存的诚信环境和评价体系，助长“劣币驱逐良币”的不良市场态势，为平台治理带来前所未有的挑战。深度伪造(Deepfake)技术已可生成近乎完美的商品试用视频与主播讲解内容，结合 ChatGPT 类模型生成 persuasive 的虚假文案，形成“假内容 + 真流量”的黑色产业链，传统基于规则的内容审核系统难以有效识别。

5. 责任认定与伦理缺失风险

当人工智能系统自主做出错误或有害决策时——例如错误扣费、误判用户违规并禁言、实施歧视性定价或泄露敏感信息——其责任主体的认定变得极其复杂。是归责于算法设计者、模型训练数据提供方、电商运营平台，或是将 AI 视为独立的法律主体？当前法律框架并未给出清晰答案。同时，相应的伦理准则缺失，如何确保 AI 决策符合公平、透明、问责和人类福祉等基本原则尚未形成共识。这种模糊性使得纠纷处理陷入困境，用户维权困难，最终将侵蚀消费者对人工智能应用的接受度和信任感，阻碍技术的健康可持续发展。

5.2. 解决路径

1. 强化数据安全与隐私保护

电商平台应建立全方位的数据安全防护体系，核心技术手段包括采用联邦学习、差分隐私等隐私计算技术，确保在数据融合分析过程中实现可用不可见，最大限度降低原始数据泄露风险。具体而言，可在用户行为分析、联合建模等场景部署联邦学习系统，原始数据不出域，仅交换加密后的模型参数或梯度。同时，应严格实施数据分类分级管理制度，建立基于角色的最小权限访问控制机制，并配备完善的数据加密传输与存储方案，对于个人敏感信息(如身份证、银行卡号)应采用国密算法进行加密存储，并设置严格的访问日志审计。定期开展数据安全影响评估、渗透测试和合规性审计，确保数据处理全流程符合《网络安全法》《个人信息保护法》《数据安全法》等法律法规要求，构建用户信任的数据保护环境，可考虑每年至少进行一次全面的数据安全审计，并聘请第三方专业机构进行渗透测试。并可引入“隐私-by-design”理念，在系统设计初期即嵌入数据保护机制、建立数据溯源与审计日志，实现数据流动全程可追踪、对敏感数据实施脱敏处理与生命周期管理。

2. 确保算法公平与透明

为解决算法歧视问题，应在模型训练阶段引入偏见检测机制和公平性约束条件，通过数据平衡、特征选择等技术手段从源头控制偏见产生。例如，在训练推荐模型时，可采用“对抗性去偏”技术，或在损失函数中加入公平性正则项。建立完善的算法审计与评估体系，定期对推荐、定价等关键模型的决策结果进行公平性评估和影响分析。建议每季度对核心算法进行一次公平性审计，使用“差异影响”(Disparate Impact)等指标量化评估算法对不同人群的影响。同时大力推进可解释 AI 技术的应用，通过可视化、自然语言解释等方式使算法决策过程变得可理解、可追溯，向用户解释“为什么给您推荐这个商品”时，可展示“因为您浏览过 A 商品，且与 B 商品有较高关联度”等可理解的依据。并建立算法备案和公示制度，接受监管部门和社会公众的监督。

3. 提升系统鲁棒性与应急能力

通过对抗性训练增强模型抵御恶意攻击的能力，对核心 AI 系统实施全面的压力测试和故障注入测试，模拟高并发、异常数据输入、网络延迟等极端场景，检验系统容错能力。构建多层次系统韧性架构，设计包括降级开关、熔断机制和回滚方案在内的应急响应体系，确保在 AI 系统出现异常时能够快速切换至备用方案或人工处理流程。建立 7 × 24 小时监控预警中心和应急处置团队，制定详细的应急预案并定期组织演练，最大限度保障业务连续性和系统可靠性。引入异常检测模型实时监控 AI 输出偏差、部署模型监控平台(如 ModelDB、MLflow)实现版本管理与性能追踪，在关键决策环节设置人工复核节点。

4. 构建综合治理体系防范虚假信息

研发并部署深度伪造检测、生成内容识别、行为模式分析等 AI 反制技术，构建虚假信息识别与处置的技术防线，可引入检测模型如 GPTZero 用于识别 AI 生成文本，或利用数字水印技术追踪图片视频来源。完善“AI 初审 + 人工复核 + 用户举报”的多层次审核机制，建立虚假内容特征库和共享平台，对于疑似虚假内容，系统自动标记并优先推送至人工审核队列；同时建立跨平台共享的“虚假内容特征库”，提升识别效率。孙周指出，《办法》通过明确要求平台通过技术手段阻断 AI 假冒他人营销(如深度伪造)，并对 AI 生成人物图像/视频进行显著标识，防止虚假宣传。出现违法问题时，责任归属于使用该技术的直播间运营者[9]。

加强与监管部门、行业协会、同行企业的协同治理，建立跨平台联防联控机制，共同打击利用 AI 技术进行的网络欺诈行为，维护健康的电商生态环境。

5. 明确责任框架与贯彻伦理准则

推动建立健全人工智能法律法规体系，明确开发者、部署者、使用者等各方主体的法律责任边界。建议在《电子商务法》修订中增设 AI 应用专章，明确平台对 AI 决策结果的主体责任，以及在何种情况下可以追溯至算法设计者。企业内部设立 AI 伦理委员会，制定符合社会主义核心价值观的 AI 伦理准则，并将其融入产品设计、开发、测试、部署的全生命周期，伦理准则应具体化，例如规定“禁止使用 AI 进行大数据杀熟”、“确保 AI 决策过程可追溯”等。在关键决策环节设置必要的人类监督和干预机制，确保人类始终掌握最终控制权，实现人工智能发展与风险管控的平衡。对于涉及高额交易、用户封禁、敏感信息处理的 AI 决策，必须设置人工审核确认环节，参考欧盟《人工智能法案》建立基于风险的 AI 监管分类制度、推行算法备案与透明度报告制度、建立 AI 事故强制报告与联合调查机制、鼓励企业通过伦理认证提升品牌信任。

参考文献

[1] 郝京杰. 人工智能和物联网在电商领域的应用[J]. 中国新通信, 2019, 21(20): 120-121.

[2] 包俊先, 洪虹. 生成式人工智能在电商行业中的应用现状和风险研究[J]. 老字号品牌营销, 2024(7): 55-57.

[3] 杨柳. 人工智能技术在电商营销中的应用与未来发展趋势分析[J]. 上海商业, 2023(10): 70-72.

[4] 王雪滢. 虚拟环境下基于手柄控制器的目标选择技术研究[D]: [硕士学位论文]. 长春: 吉林大学, 2024.

[5] 潘春会. 大数据驱动下的电商行业发展与应用研究[J]. 活力, 2024, 42(3): 28-30.

[6] 姚凯, 涂平, 陈宇新. 基于多源大数据的个性化推荐系统效果研究[J]. 管理科学, 2018, 31(5): 7-19.

[7] 亿邦动力. 京东双 11 智能客服回应用户问询超过 10 亿次[EB/OL]. https://www.ebrun.com/ebrungo/zb/533848.shtml, 2023-11-11.

[8] 财联社. IBM: 2023 全球数据泄露的平均成本达到 445 万美元 创该报告有史以来以来最高记录[EB/OL]. https://www.cls.cn/detail/1414396, 2023-07-25.

[9] 法治日报. 打击数据造假、遏制 AI 滥用、填补私域盲区 直播电商监管将出“组合拳” [EB/OL]. http://www.legalweekly.cn/hlws/2025-06/19/content_9202537.html, 2025-06-19.