E-Commerce Letters 电子商务评论, 2025, 14(12), 5092-5097
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14124464

Hans汉斯

人工智能在电子商务中的法律风险及应对策略

郭雨晖

贵州大学法学院，贵州 贵阳

收稿日期：2025年11月12日；录用日期：2025年11月24日；发布日期：2025年12月29日

摘 要

随着人工智能技术在电子商务领域的深度融合与应用，其在提升用户体验、优化运营效率和驱动商业创新的同时，也带来了一系列复杂且亟待解决的法律风险，本文旨在系统分析当前人工智能在电子商务领域的应用以及现实存在的法律风险，并提出相应的应对策略，以促进电子商务行业的健康与可持续发展。保障电商企业在享受人工智能技术红利的同时，高度重视其伴随的法律风险，通过技术、管理与法律手段的综合运用，实现创新与合规的平衡，从而在激烈的市场竞争中行稳致远。

关键词

电子商务，人工智能，法律风险

Legal Risks of Artificial Intelligence in E-Commerce and Corresponding Response Strategies

Yuhui Guo

Law School of Guizhou University, Guiyang Guizhou

Received: November 12, 2025; accepted: November 24, 2025; published: December 29, 2025

Abstract

With the in-depth integration and application of artificial intelligence (AI) technology in the field of e-commerce, while it enhances user experience, optimizes operational efficiency, and drives business innovation, it also brings about a series of complex legal risks that urgently need to be addressed. This paper aims to systematically analyze the current application of AI in the e-commerce sector and the existing legal risks in practice, and propose corresponding response strategies to promote the healthy and sustainable development of the e-commerce industry. It is intended to

文章引用: 郭雨晖. 人工智能在电子商务中的法律风险及应对策略[J]. 电子商务评论, 2025, 14(12): 5092-5097.
DOI: 10.12677/ecl.2025.14124464

ensure that e-commerce enterprises, while enjoying the dividends of AI technology, attach great importance to the accompanying legal risks. By comprehensively applying technical, management, and legal means, enterprises can achieve a balance between innovation and compliance, thereby maintaining stable development and achieving long-term success in the fierce market competition.

Keywords

E-Commerce, Artificial Intelligence (AI), Legal Risks

1. 人工智能在电子商务中的应用概述

(一) 人工智能的基本概念

人工智能(Artificial Intelligence, AI)作为一项前沿技术，正在深刻改变传统商业模式的运作逻辑。从本质上看，人工智能是指由人造系统所展示的智能行为，包括感知环境、学习理解、推理判断和决策执行等能力。在电子商务领域，人工智能的核心价值在于其能够通过算法模型处理海量数据，识别潜在规律，并模拟人类的认知过程，从而完成各种复杂任务。近年来，随着生成式 AI (Generative AI)技术的突破，人工智能不再局限于辅助决策，更拓展到内容创作、自然语言交互等更高层次的智能活动，为电商行业带来了全新的发展机遇[1]。

从技术架构来看，电商领域的人工智能系统主要建立在机器学习、自然语言处理、计算机视觉和推荐算法等核心技术之上。这些技术使得电商平台能够理解用户的文字和语音查询，分析商品图片和视频内容，预测消费偏好，并生成个性化的营销材料。值得注意的是，随着大语言模型(Large Language Models)的持续迭代与多 Agent 协作技术的成熟，电商 AI 正从传统被动应答工具全面升级为主动服务的“智能业务代理”，逐步重塑电商行业的价值链和生态结构。

(二) 人工智能在电子商务中的实际应用

人工智能技术在电子商务中的应用已渗透到用户交互、商家运营、物流配送和客户服务等全链路场景，形成了完整的应用生态。在 2025 年双 11 大促期间，AI 技术的规模化落地尤为明显，成为电商行业效率革命的重要驱动力。

在用户端，AI 导购工具已成为提升购物体验的关键抓手。淘宝天猫推出的“AI 万能搜”、“AI 帮我挑”等工具，通过自然语言理解、多模态交互、个性化推荐三大技术支柱，重新定义了“导购”的核心价值。数据显示，这些 AI 导购应用能够支持用户使用自然语言表达复杂需求，如“适合 30 岁女性的 500 元生日礼物”或“155 cm 小个子穿的显腿长加绒牛仔裤”，并能在几秒内提供精准的商品推荐和对比信息。据统计，今年“双 11”上线的“AI 万能搜”已帮助用户解决了近 5000 万个消费需求，AI 清单为用户定制化提供了约 200 万份购物清单。这种对话式购物模式大幅降低了用户的决策成本，提高了购买效率[2]。

在商家端，AI 工具全面覆盖了运营、营销、客服等关键环节。在运营方面，阿里妈妈推出的“货品全站推”和超级经营智能体“万相台 AI 无界”帮助商家实现精准投放，使成交转化率整体增长 10%，ROI (投资回报率)同比增长超 15%。在营销内容生成方面，AI 工具能自动生成商品描述、营销文案和图片素材，商家营销素材日均节省成本超 4000 万元。在客服领域，AI 客服系统如“店小蜜 5.0”能够理解复杂

的用户咨询，如商品成分、凑单满减规则等，并将商家的转化效率提升 30%，一半的售后问题都能自动化解决[3]。

此外，AI 技术在跨境电商中的应用也成效显著。德国本土家居品牌 HomeZeit 使用亚马逊的 Content Generator 工具后，上线两周内转化率从 9.8%上升至 11.4%，广告点击转化成本(ACoS)下降约 8%，内容生成所用时间缩短了 65%。第三方数据机构 Statista 报告显示，2024 年全球采用 AI 工具的跨境电商企业，选品成功率平均提升 53%，用户复购率提高 28%，物流周转效率加快了 34%。这些数据充分证明了 AI 技术在电商领域的实际价值[4]。

从长远来看，电商与 AI 的融合正在推动行业从“流量运营”向“用户决策效率运营”转变。中国国际电子商务中心电商首席专家李鸣涛指出，基于 AI 的全方位支撑，未来电商购物的个性化体验将进一步提升，AI 购物智能体将成为新的网上购物流量入口，标志着智能体时代的开始。这种变革不仅重塑了消费者购物体验，也重新定义了电商竞争的核心要素——从价格和规模转向效率和质量[5]。

2. 人工智能在电子商务中的法律风险

(一) 数据隐私与保护

随着 AI 技术在电商领域的深度应用，数据隐私与保护问题日益凸显，成为制约行业健康发展的关键因素。AI 系统的运行依赖于海量用户数据，包括个人信息、行为轨迹、消费习惯、社交关系等敏感信息。这些数据在收集、处理和分析过程中，若未采取适当保护措施，极易引发个人信息泄露和滥用风险[6]。

大数据杀熟是 AI 电商中最为典型的数据滥用行为之一。基于对用户消费能力、价格敏感度的分析，AI 算法可以推测出各个消费者对于商品的最高意愿价格，从而实现差异化定价。对于同一件商品，不同用户看到的价格可能相距甚远，其中高频消费者、高端设备用户往往成为“大数据杀熟”的主要对象。这种行为首先侵犯了消费者的个人信息权益，违反了《消费者权益保护法》第二十九条规定，即经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。

同时，大数据杀熟还侵犯了消费者的公平交易权和知情权[7]。《消费者权益保护法》第十条明确规定，消费者享有公平交易的权利。公平交易指交易时质量、价格、计量三方面均要公平，实质确定了交易需统一定价，商品服务的价格仅受质与量的影响，消费者本身的偏好、购买力、交易记录等，均不能在定价时予以考量。而 AI 算法将消费者编织在信息茧房中，让其产生商品或服务为统一定价、不存在差异的错觉，最终作出消费决策，侵犯了消费者知情权，同时也干涉了以知情权实现为前提的自主选择权。

在现有法律框架下，我国已出台《个人信息保护法》《网络安全法》等基础性法律，对个人信息处理活动设定了明确规范。但在 AI 电商场景中，这些原则性规定面临落地难的挑战。一方面，AI 算法的黑箱特性使得数据处理过程不透明，用户难以了解个人信息被如何利用；另一方面，多头收集、隐蔽处理等行为增加了监管难度。例如，AI 系统可能通过融合多个来源的数据，生成超出原始授权范围的新信息，这种隐性数据加工行为尚无明确法律规制[8]。

(二) 知识产权侵权

AI 技术在电商中的应用引发了多维度知识产权侵权问题，尤其在生成内容和商品展示两个领域风险突出。在生成内容方面，AI 工具可以大规模生成商品描述、营销文案和用户评价，这些内容若未经授权使用了受版权保护的素材，或模仿他人注册商标，可能构成侵权[9]。

AI 模特滥用是电商领域特有的知识产权风险点。AI 模特本是电商行业的技术创新产物，合理运用可大幅降低实拍成本、丰富展示场景。然而，某些商家将这项技术异化为“造假工具”，利用 AI 模特打造“零瑕疵”形象，刻意掩盖商品真实状态。更有甚者，直接使用 AI 生成与名人相似的肖像进行商品推广。

如“奥运冠军”推荐土特产、“知名主持人”推荐保健品等，这些带货的“名人”均系 AI 生成，在 AI 技术加持下，甚至有“演员”在同一时间现身多个直播间推广不同产品[10]。

这种行为侵犯了被仿冒者的人格权。《民法典》第一千零一十九条规定，任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权。第一千零二十三条规定，对自然人声音的保护，参照适用肖像权保护的有关规定。商家未经允许用 AI 技术生成名人肖像与声音宣传商品，使被仿冒者的人格形象与商品形成紧密关联，使消费者误以为该名人系商品的推荐者，利用其形象、社会影响力等吸引消费者关注，增加交易机会，已经侵犯其肖像权及声音权；若所推荐商品为假冒伪劣产品，导致被仿冒者社会评价降低，则还侵犯其名誉权。

与此同时，AI 生成的内容本身也面临版权归属不明确的问题。当 AI 系统自动生成商品描述、营销文案或图片时，这些内容的著作权主体难以确定。目前我国司法实践普遍认为，AI 本身不能成为作者，但对于在创作过程中发挥实质性智力贡献的人类认定标准不一，导致 AI 生成物的法律保护存在不确定性。

(三) 产品责任与合同风险

AI 电商的兴起带来了产品责任认定和合同风险分配的新挑战。当 AI 系统的推荐或决策导致消费者损失时，责任主体难以确定。例如，若 AI 导购推荐的商品存在质量问题，或 AI 客服提供错误信息导致消费者作出不当购买决定，受害者应向谁追究责任？是基于产品缺陷向 AI 系统开发者索赔，还是基于服务过错向电商平台追责？现行法律对此类情形尚无明确规定。

在合同缔结方面，AI 代理行为可能引发合同效力争议。随着 AI agent 技术的发展，用户越来越多地授权 AI 助手代理完成购物决策甚至下单支付。当 AI 基于预设指令或自主学习作出购买行为时，该行为的法律效果是否完全归属于用户，存在解释空间。特别是在 AI 出现算法错误、系统故障或被恶意操控等情况下，签订的合同是否有效，消费者能否撤销，均需法律进一步明确[11]。

另一方面，一些消费者也开始利用 AI 技术牟取不正当利益，AI 造假骗取退款就是典型例子。收到完好的商品后，为获取不当利益，部分消费者通过向 AI 软件下达指令的方式，伪造商品质量问题，生成诸如发霉水果、碎掉的杯子、破裂的镜子等图片，提交平台，以达成仅退款目的。

这类“薅羊毛”行为的后果可能比消费者想象中更加严重。在民事层面，消费者虚构商品质量问题骗取退款，违反诚实信用原则，属于欺诈行为。若是金额较大或情节严重，消费者行为依然受到治安管理处罚法甚至刑法规制。根据 2026 年 1 月 1 日起施行的新治安管理处罚法第五十八条规定，消费者的诈骗行为会被处五日以上十日以下拘留或者二千元以下罚款，情节较重的，处十日以上十五日以下拘留，可以并处三千元以下罚款。如果数额足够大，诈骗财物价值达到 3000 元以上，则可能达到刑事立案标准，构成诈骗罪。

(四) 不正当竞争和滥用

AI 电商环境下的不正当竞争行为形式多样，且具有更强的隐蔽性和技术性。除前述大数据杀熟外，还包括算法共谋、流量劫持、AI 虚假评价等多种形式。

算法共谋是指竞争商家的 AI 系统通过自动监控和调整价格，实现隐性联合定价，消除市场竞争。这种行为实质上是传统垄断协议的技术变种，但由于缺乏明示的意思联络，且由算法自动执行，导致反垄断执法面临认定难题。流量劫持表现为通过 AI 技术操纵平台推荐算法，不当获取流量优势。例如，利用 AI 生成虚假用户行为数据，欺骗推荐系统，使特定商品获得更高排名。亚马逊近期对 Perplexity AI 的诉讼揭示了 AI 代理可能引发的不正当竞争风险。亚马逊在起诉中指控 Perplexity 的 Comet 浏览器伪装成 Google Chrome，同时部署 AI 代理进入亚马逊电商平台，访问私人客户账户并代表用户进行购买。这种配置使 Comet 在访问亚马逊商店时，不使用独特的浏览器标识符，而是传输与 Google Chrome 相同的“用

户代理”字符串，使得 AI 代理的请求看起来像是人类顾客的浏览行为。这种行为不仅涉嫌违反《计算机欺诈和滥用法案》，更重要的是对亚马逊的广告商业模式构成了直接威胁。

AI 电商环境下的滥用案例尤为繁多，根据北京市互联网法院 2025 年 9 月 11 日上午召开的涉人工智能案件审理情况新闻发布会上公布的典型案例，原告在教育、育儿领域具有一定知名度和社会影响力，2024 年，原告李发现被告某文化传媒有限公司在其运营的某网络平台店铺中，通过使用原告的公开演讲、授课视频，并配以与原告声音高度近似的 AI 合成声音，对其销售多本的家庭教育类图书进行宣传推介。原告认为被告未经许可使用原告的肖像和通过 AI 合成的声音制作宣传产品，使原告的人格形象与其商业宣传对象形成紧密关联，从而使消费者误以为原告是其销售图书的代言人或推介者，利用原告人格形象、专业背景和社会影响力吸引关注，增加交易机会，侵犯了原告的肖像权和声音权。被告作为图书销售者，与视频发布者(某带货主播)之间为委托关系，共同完成销售活动，被告对主播发布的视频具有审查义务和能力，对涉案视频的发布应当承担赔礼道歉、赔偿损失等侵权责任。

3. 人工智能在电子商务中法律风险应对策略

(一) 电商领域制定专项法规与运营规范

人工智能在电子商务中的应用往往超出了传统法律框架的覆盖范围，现有法规如《电子商务法》或《个人信息保护法》虽提供基础保障，但缺乏针对 AI 特性的专项规定。因此，制定专项法规与运营规范是应对法律风险的首要策略。专项法规应聚焦于 AI 的独特属性，如算法的透明性、可解释性和公平性。例如，可借鉴欧盟《人工智能法案》的“风险分级”模式，将电商 AI 系统划分为高风险(如信用评估)和低风险(如产品推荐)类别，并施加不同程度的义务。还应当细化关于“电商平台算法透明度”的相关规定，将有可能涉嫌违规的行为列明清楚。运营规范则需明确企业在开发、部署 AI 系统时的具体标准，包括数据采集的合法性、算法测试的合规性以及用户知情同意的要求。同时，法规应鼓励“设计即合规”(Privacy by Design)原则，将法律要求嵌入技术开发流程，避免事后补救。在中国语境下，可结合《网络安全法》和《电子商务法》修订，增设 AI 专项条款，确保法规与产业发展同步。总之，专项法规与运营规范的制定不仅能填补法律空白，还能为电商企业提供明确的行为指引，降低合规不确定性带来的风险。

(二) 明确电商涉嫌违规的处罚标准和监管要求

在 AI 驱动的电子商务中，违规行为可能表现为算法操纵市场、虚假广告或数据滥用，但其认定和处罚常因标准模糊而面临挑战。因此，明确处罚标准和监管要求是确保法律威慑力和公平性的关键。处罚标准应基于“过罚相当”原则，根据违规行为的性质、情节和危害后果分级设定。例如，对轻微算法偏见可处以警告或罚款，而对严重数据泄露或欺诈行为则适用高额罚金、业务暂停甚至刑事责任。监管要求方面，需强化事前预防和事中监控，包括要求电商平台定期提交 AI 系统审计报告、公开算法决策逻辑，并建立快速响应机制处理用户投诉。监管机构(如国家市场监管总局)应制定细化的执法指南，明确 AI 违规的认定流程和证据标准，避免执法随意性。此外，可引入“吹哨人”制度鼓励内部举报，增强社会监督。通过清晰的标准和监管要求，不仅能提升法律执行的透明度，还能促使企业主动合规，防范 AI 技术滥用导致的系统性风险[12]。

(三) 提升电商领域人工智能的技术水平

技术本身是法律风险的重要源头，但通过提升 AI 技术水平，可以转化为风险防控的有效工具。电商领域 AI 的技术提升应聚焦于可解释性、公平性和安全性。可解释 AI (XAI)技术能使算法决策过程透明化，帮助法官和监管者追溯责任，例如在合同纠纷中厘清自动化决策的过错。公平性技术则通过去偏算法和多样性训练，减少性别、地域等歧视风险，符合《反歧视法》的基本要求。安全性方面，需加强数据加密和访问控制，防止黑客攻击导致的信息泄露。政府和企业应合作推动研发投入，例如设立 AI 伦理实

验室或资助开源工具开发，同时将技术标准与法律要求对接，如通过认证机制建立合规技术。值得注意的是，技术提升不是孤立的，需与法规协同：例如，法规可强制要求高风险 AI 系统通过第三方测试，而技术研发则提供实现路径。通过技术进步，电商 AI 不仅能降低法律风险，还能增强用户信任，促进行业可持续发展。

(四) 加强监管与执法力度

监管与执法是法律风险应对的“最后一公里”，在 AI 电商场景下，传统监管模式往往滞后，因此需加强力度并创新方法。监管机构应转向“智能监管”，利用大数据和 AI 工具进行实时监测，例如通过算法扫描电商平台识别潜在违规广告或定价垄断。执法方面，需强化跨部门协作，如市场监管、网信和公安部门的联合行动，以应对跨境数据等复杂问题。同时，执法应注重比例原则，避免过度干预市场创新。例如，对初创企业可采取“监管沙盒”模式，允许其在可控环境中测试 AI 应用，而对大型平台则实施严格问责。在国际层面，中国可积极参与全球监管对话，借鉴欧美经验，构建跨境执法合作机制。加强监管与执法不仅能及时遏制 AI 滥用，还能通过典型案例形成判例法，丰富法律实践。最终，目标是构建一个动态、高效的监管生态系统，确保 AI 电商在法治轨道上运行。

(五) 推动行业自律与标准化建设

行业自律与标准化是法律框架的重要补充，能弥补立法滞后性和监管盲区。在 AI 电商领域，企业通过自律机制主动约束行为，可降低外部监管成本。行业自律包括制定行为准则、伦理指南和自律公约，例如电商协会牵头发布《AI 应用自律宣言》，要求成员企业承诺算法公平和用户数据保护。标准化建设则涉及技术和管理标准的统一，如参考国际标准化组织(ISO)的 AI 伦理标准，制定本土化电商 AI 标准体系，覆盖数据管理、算法评估和应急响应等环节。政府可发挥引导作用，通过政策激励(如税收优惠)鼓励企业参与标准化进程，并建立认证标志提升市场认可度。此外，行业自律需与公众参与结合，例如设立用户反馈平台，增强社会共治。通过自律与标准化，不仅能提升行业整体合规水平，还能培育“负责任创新”的文化，为 AI 电商的长期发展奠定基础。

参考文献

[1] 张芮涵. 人工智能技术在电子商务中的应用策略[J]. 商场现代化, 2025(18): 46-48.

[2] 李海岚. 重庆人购物有了新体验——5 秒生成清单 AI 消费伙伴“很懂你” [N]. 重庆日报, 2025-11-24(008).

[3] 李洁. 生成式人工智能时代高职院校电子商务数智化人才能力图谱构建研究[J]. 信息系统工程, 2025(9): 173-176.

[4] 杨亚姣. 浅析人工智能时代高职电子商务人才培养模式[J]. 中国储运, 2025(9): 173-174.

[5] 陈莉霞. 人工智能时代电子商务发展路径分析[J]. 老字号品牌营销, 2025(16): 59-61.

[6] 黄佳怡. 智能合约在电子商务争议解决中应用的法律困境及应对[J]. 知与行, 2025(4): 68-78.

[7] 曹晓雨, 陈聪违. 人工智能技术在电子商务个性化推荐中的应用与优化策略[J]. 营销界, 2025(13): 137-139.

[8] 束姝妹, 李艳阳. 人工智能赋能电子商务: 变革驱动、创新实践与挑战应对[J]. 广东经济, 2025(11): 53-55.

[9] 陈莉霞. 人工智能技术在电子商务领域中的应用分析[J]. 数字技术与应用, 2025, 43(5): 39-41.

[10] 李土金. 人工智能引领电子商务产业智能化转型与升级探究[J]. 国际商务财会, 2025(21): 70-73+77.

[11] 安容宇, 王可心. 大数据与人工智能在种业电子商务中的应用: 精准营销与预测分析[J]. 分子植物育种, 2025, 23(19): 6677-6682.

[12] 黄文镜. 人工智能+背景下高职电子商务专业人才培养的优化路径研究[J]. 中国电子商情, 2025, 31(19): 19-21.