

电商场景中AI智能体的法律责任归属研究

郑泽煜

浙江理工大学法学与人文学院, 浙江 杭州

收稿日期: 2025年11月10日; 录用日期: 2025年11月25日; 发布日期: 2025年12月19日

摘要

人工智能在电商领域的广泛应用, 正在重塑商业模式与消费体验, 同时也对传统法律责任框架带来新的挑战。电商场景中人工智能体具备的自主性与自适应特征, 引发了其法律地位的界定难题, 并催生了归责原则模糊、监管滞后与举证困难等多重困境。在辨析其法律性质与角色分类的基础上, 应明确人工智能体作为特殊客体的有限法律地位, 并构建与其风险等级相匹配的分层责任框架。通过优化归责原则与细化各方注意义务、强化技术赋能监管与多元协同治理等方式, 有效实现权责适配, 以平衡技术创新与消费者权益保护, 为人工智能时代电子商务的健康发展奠定坚实的法治基础。

关键词

人工智能体, 电商平台, 归责原则, 多元共治

Research on the Attribution of Legal Liability for AI Agents in E-Commerce Scenarios

Zeyu Zheng

School of Law and Humanities, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: November 10, 2025; accepted: November 25, 2025; published: December 19, 2025

Abstract

The widespread application of artificial intelligence in the field of e-commerce is reshaping business models and consumer experiences, while simultaneously posing new challenges to traditional legal liability frameworks. The autonomy and adaptive characteristics of AI agents in e-commerce scenarios have raised difficulties in defining their legal status, giving rise to multiple issues such as ambiguous imputation principles, regulatory lag, and evidential difficulties. Based on an analysis of their legal nature and role classification, it is essential to clarify the limited legal status of AI agents as special objects and establish a tiered liability framework commensurate with their risk levels.

By optimizing imputation principles, specifying the duty of care for various parties, strengthening technology-enabled regulation, and promoting collaborative governance, rights and responsibilities can be effectively aligned. This will balance technological innovation with consumer rights protection, laying a solid legal foundation for the healthy development of e-commerce in the era of artificial intelligence.

Keywords

AI Agent, E-Commerce Platform, Imputation Principles, Multi-Stakeholder Collaborative Governance

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

随着人工智能技术的迅猛发展, AI 智能体在电商领域的应用日益广泛, 从智能客服、个性化推荐到自动化定价、虚假评论生成, AI 正深刻重塑着电子商务的运营模式与消费体验。“人工智能具有自适应性, 其算法具有动态性、自主性、迭代性” [1]。这种自适应与自主学习能力使得 AI 智能体能够在无人直接干预的情况下独立作出决策并执行任务, 从而引发了复杂的法律责任归属问题。近年来, 电商平台上已出现多起由 AI 智能体引发的法律纠纷, 包括生成虚假商品图片、制造虚假交易评价、实施价格歧视等行为, 这些案例凸显了现有法律框架在规制 AI 智能体行为方面的滞后与不足。

电商场景中的 AI 智能体已不再是简单的工具, 而是在相当程度上能够自主决策并执行任务的复杂系统。正如有学者所言, “弱人工智能体在一定范围内亦具有一定的认知能力, 可以深度学习并不断适应新的环境, 可以完成高难度的任务, 这一点与一般工具不同” [2]。这种类人化的决策能力对传统法律关系中以“人类行为中心主义”为基础的责任归属规则提出了严峻挑战。有鉴于此, 笔者认为有必要首先厘清电商场景中 AI 智能体的法律地位, 进而系统分析其引发的法律责任归属问题, 并尝试构建合理的责任分配框架, 以期为相关法律制度的完善提供理论支撑。

2. 电商场景中 AI 智能体的法律性质与角色分类

2.1. AI 智能体的法律地位界定

AI 智能体的法律地位界定是解决其责任归属问题的逻辑起点。当前法学界对此存在激烈争论, 主要形成否定说与肯定说两种对立观点。否定说坚持传统民法中主客体二元划分, 认为 AI 仅是人类意志的延伸, 不具有独立法律人格。肯定说明主张基于 AI 的自主性, 应赋予其某种程度的法律人格, 使其能够独立承担责任。

审视这两种观点, 纯粹否定说已难以应对 AI 技术发展带来的法律挑战, 而激进肯定说则可能引发责任虚化风险。较为合理的路径是采纳有限法律人格的折中立场。“人工智能的法律人格与自然人或法人不同, 并不具有承担完全责任的能力与地位” [3]。在电商场景中, 可根据 AI 的自主程度与应用范围, 确认其在一定边界内的法律主体资格。对于仅能执行预设规则的简单 AI (如基础客服机器人), 可视为传统法律意义上的工具; 而对于具有深度学习能力、能够独立作出复杂决策的高级 AI (如个性化推荐系统、自动化定价系统), 则可认定其具备有限法律人格, 在特定范围内承担相应责任。

“是否赋予人工智能体法律人格, 对外是研发与运用人工智能的前提, 对内则是确立人工智能体权

利、义务乃至责任的基础”[4]。在此基础上,特别是在电商场景中,明确 AI 智能体的法律地位,已成为构建其法律责任体系的逻辑起点。相应地, AI 智能体的法律地位界定应当遵循功能主义路径,即不追求统一的人格认定标准,而是根据具体应用场景中的功能与自主程度进行差异化界定。例如,对于仅能进行简单问答的客服 AI,其法律责任应由背后的运营者承担;而对于能够自主学习用户偏好并生成个性化内容的推荐算法,则可以考虑在一定条件下认定其具有一定的责任能力。

2.2. 电商场景中 AI 智能体的角色分类

在复杂的电商生态中, AI 智能体根据其功能与自主程度,扮演着多种角色,不同角色对应的责任风险与归属逻辑亦不相同。

辅助决策与执行工具是 AI 智能体的基础形态。例如,用于库存管理、价格自动调整、订单处理的系统。这类智能体自主性相对较低,其行为通常在预设的参数和算法内运行,可视为经营者手臂的延伸。其产生的法律后果,如因价格设置错误导致的合同纠纷,原则上应直接由使用该工具的经营者承担。

独立交互与服务提供者则体现了 AI 智能体的进阶应用。以智能客服为代表。这类智能体具备更高的自主性,能够与消费者进行实时、动态的对话,处理咨询、投诉甚至达成交易意向。“在混合在线客服提供模式下,人工客服、智能客服的使用对消费者购买转化有显著的正向作用,人工客服与智能客服的使用之间存在替代关系”[5]。当智能客服提供错误信息误导消费者购买商品,或未能妥善处理个人数据时,责任如何在其开发者、部署者(平台或商家)之间划分则成为难题。

自动化营销与决策引擎是电商场景中最为复杂的 AI 智能体类型。例如个性化推荐系统。“人工智能的发展为个性化推荐带来新的挑战,基于人工智能的个性化推荐系统自主学习能力更强,对数据的处理速度更快,可以实时地跨平台处理数据,给消费者推送最让其感兴趣的产品和服务”[6]。这类系统决策过程复杂且不透明,可能引发歧视性定价、信息茧房、甚至操纵消费者选择等问题。其行为往往不是单一指令的结果,而是算法模型与海量数据交互后的涌现行为,使得追溯最终责任主体变得异常困难。对不同角色进行准确的分类,是后续分析责任困境与构建差异化规制路径的前提。

3. 电商场景中 AI 智能体法律归责的困境

3.1. 法律主体资格缺失与责任链条断裂

当前法律体系并未普遍承认 AI 智能体的法律主体资格,这直接导致了在损害发生后责任链条的断裂风险。根据传统民法与侵权法理论,责任须由具有法律人格的主体(自然人、法人)承担。当 AI 智能体,特别是高度自主的智能体,因其决策和行为造成损害时,例如推荐算法导致用户购买假冒伪劣商品并造成人身伤害,或者自动化交易系统发生错误导致用户重大财产损失,受害者面临的首要问题是谁应为“机器”的行为负责。AI 智能体的核心特征在于“在实际运行中可以脱离人类操控独立进行活动,此特征致使现行法律秉承的主观过错侵权责任理论适用遇见障碍,因为人工智能体的行为没有特定主体对其进行控制”[7]。商家可能辩称损害源于算法的“自主决策”而非其直接指令;平台可能以技术中立为由免责;开发者则可能主张其无法预见产品在所有场景下的具体应用。这种责任主体的模糊性,使得人工智能的自主决策和系统互联等技术特征给人工智能侵权责任的认定和分配带来挑战[8]。即便对人工智能法律主体地位和责任能力持有限肯定立场的学者,在论及人工智能的责任时,亦不得不承认,无论是何种归责类型,总体均需要适用“穿透人工智能面纱”的原则确定归责路径,在查证因果关系的基础上,确定人工智能责任背后的实际责任主体[9]。然而,在电商跨平台、多主体的复杂环境中,“穿透”并追溯至最终控制者或受益者,在实践中面临技术和法律的双重障碍。

3.2. 归责原则适用模糊与过错认定困难

在侵权责任领域,归责原则的选择与过错的认定是核心问题。对于 AI 智能体引发的损害,适用过错责任原则、过错推定责任还是无过错责任(严格责任),目前尚无定论。有学者主张,“从有利于鼓励人工智能发展需要出发,不宜科以生成式人工智能服务提供者严格责任,而应当对其适用过错责任”[10]。若适用传统的过错责任原则,原告则需证明被告(如开发者、使用者)存在主观过错。然而, AI 系统的行为逻辑,特别是深度学习算法的“黑箱”特性,使得证明特定主体的主观过错极为困难。更深层次的困境在于传统侵权法中以“理性人”为基准的过错认定标准难以直接适用于 AI 场景。需要为相关主体确立专门的合理注意义务标准。这一标准不应局限于行业普遍水平,而应基于 AI 技术的潜在风险设定更高的专业要求。具体而言,开发者的注意义务应包括算法设计的公平性审查和充分的安全测试;而电商平台等使用者的义务则体现为对 AI 系统运行后果的持续监督,包括建立监测评估机制,主动审查并纠正推荐算法可能产生的歧视性或操纵性结果。当前,这种专业注意义务的具体边界在司法实践中仍属模糊地带,亟需通过立法和案例予以明确,为过错认定提供清晰的法律标尺。

3.3. 监管滞后与举证责任分配失衡

面对日新月异的 AI 技术及其在电商领域的深入应用,现有监管体系呈现出显著的滞后性。当前监管规则主要针对静态且行为模式相对固定的传统业态,难以有效应对具备高度自主演进能力的 AI 系统。监管机构普遍缺乏必要的技术手段,无法对海量且实时变化的 AI 决策行为实施持续监测与精准评估。与此同时,在诉讼程序中,举证责任的分配失衡进一步加剧了维权困境。依据“谁主张,谁举证”的基本原则,消费者需要证明 AI 智能体的行为与损害结果之间存在因果关系,并证明责任主体存在过错。然而,这对处于信息和技术双重劣势的消费者而言构成了难以逾越的障碍。其既无法获取 AI 系统的核心算法、训练数据及决策日志等关键证据,也不具备专业能力对这些技术资料进行有效解读。这种深刻的信息不对称实质上架空了消费者的救济权利,使其在维权过程中面临系统性困难。监管能力的不足与举证责任的失衡相互叠加,共同构成了规制 AI 智能体风险、保障消费者权益的制度性短板。

4. 电商场景中 AI 智能体法律归责的重构

4.1. 明确法律地位并构建分层责任框架

破解 AI 智能体责任归属困境的首要步骤,是厘清其法律地位。现阶段,普遍赋予 AI 智能体完全法律人格既不现实,也可能引发道德风险。更为可行的路径是,在法律上明确其作为“特殊客体”或“电子代理人”的地位,同时为未来可能出现的超强人工智能预留制度空间。有学者展望,“在未来赋予适格的通用人工智能体以民事主体地位,不仅具备可行性,而且具备正当性,因而,通用人工智能体在未来的民事法律关系中存在拥有民事主体地位的可能”[11]。基于此,应构建一个与 AI 智能体角色分类相适应的分层责任框架。对于辅助性工具类智能体,坚持“工具论”,其行为后果直接归属于控制者和使用者。对于具有较高自主性的交互与服务类、决策类智能体,则可以引入“风险开启者”或“利益享有者”责任理论。“唯有将侵权责任配置给那些能够控制、分散人工智能应用风险的人,才能更好地预防、减少损害的发生,最大程度救济受害人,协同实现侵权责任法与人工智能法的目标”[12]。这意味着,开发者、销售者、部署者(平台/商家)和使用者,应根据其对 AI 系统的控制力、获益程度以及专业能力,在不同场景下承担主要或连带责任。这种分层框架旨在实现责任与控制力、收益的匹配,确保受害者能够找到明确的追责对象。

4.2. 优化归责原则与注意义务标准

在归责原则上,不宜“一刀切”地适用单一原则,而应根据 AI 智能体的应用风险等级进行差异化配

置。对于高风险应用(如涉及人身安全、重大财产交易的自动化决策),可考虑适用过错推定责任或无过错责任,以强化对受害者的保护并激励相关方提升安全标准。对于一般风险的应用,则可主要适用过错责任原则,但需配套进行举证责任倒置或缓和,具体而言,应由被告(开发者、使用者等)证明其已尽到法律所要求的注意义务,自身不存在过错。这便对“注意义务”的内涵与标准提出了具体要求。注意义务的设定应客观化、具体化,即“以行为人是否违反客观的注意义务为标准,判断行为人是否存在过错”[13]。对于 AI 开发者,其注意义务应包括算法设计的合规性与安全性测试、数据来源的合法性、对潜在风险的充分警示等。对于电商平台或商家等使用者,其注意义务则应包括对所用 AI 系统的审慎选择、定期维护与更新、对系统输出结果的合理监督,以及在特定场景下的人工介入机制。例如,平台对个性化推荐算法可能产生的歧视性结果,负有持续的监测和纠正义务。通过明确并细化各方的注意义务标准,为过错认定提供清晰、可操作的指引。

4.3. 强化多元共治与技术赋能监管

应对 AI 智能体带来的法律挑战,不能仅依靠司法事后救济,必须强化事前事中的监管,并构建多元共治的体系。监管机构自身必须进行技术赋能,利用大数据、区块链、可解释 AI 等技术手段,开发能够对 AI 算法进行审计、对数据流进行追踪的监管科技(RegTech)工具。这有助于穿透算法的“黑箱”,实现对 AI 行为的部分可追溯、可解释,为归责提供证据支持。在监管策略上,应强调协同治理。电商平台作为交易的组织者和数据的掌控者,处于治理的前沿阵地,应承担起首要的平台管理责任。平台应建立针对平台内商家使用 AI 智能体的合规指南、风险监测系统和违规处罚机制。行业协会应牵头制定技术伦理标准与行业最佳实践。此外,应鼓励第三方专业机构开展 AI 系统的安全与合规认证。消费者教育和舆论监督也同样重要,提升公众的风险意识和维权能力。通过形成政府监管、平台自治、行业自律、社会监督相结合的多元共治格局,才能实现对电商场景中 AI 智能体风险的全链条、系统性治理。

5. 结语

电商场景中 AI 智能体的法律责任归属问题,是技术革新对传统法律体系发起的一次深刻拷问。其自主性、自适应性与“黑箱”特性,动摇了建立在人类理性与直接控制基础上的传统归责模型,进而引发法律主体资格缺失、归责原则模糊、监管滞后与举证困难等多重挑战。为破解这一困境,我们应秉持审慎而开放的态度,在明确“当下的人工智能体归根结底还是人类创造的服务于人类的工具”[14]这一基本定位的前提下,积极探索制度层面的创新。具体而言,未来的出路在于构建一个层次分明、权责清晰的法律框架:一方面,应确立 AI 智能体的特殊法律地位,并依据其功能角色与风险等级建立分层的责任分配机制;另一方面,需优化归责原则体系,细化客观化的注意义务标准,为司法实践中的过错认定提供明确指引。同时,还应强化技术赋能监管,推动形成多元主体协同共治的治理格局,以凝聚制度合力。唯有如此,方能在激励技术创新的同时,有效保障社会公平与消费者权益,为电子商务在人工智能时代的稳健发展筑牢法治根基。

参考文献

- [1] 王莹. 算法侵害责任框架刍议[J]. 中国法学, 2022(3): 165-184.
- [2] Vladeck, D.C. (2014) Machines without Principals: Liability Rules and Artificial Intelligence. *Washington Law Review*, 89, 117-150.
- [3] 袁曾. 人工智能有限法律人格审视[J]. 东方法学, 2017(5): 50-57.
- [4] 彭诚信, 陈吉栋. 论人工智能体法律人格的考量要素[J]. 当代法学, 2019, 33(2): 52-62.
- [5] 李顺, 李莉, 陈白雪. 混合在线客服对消费者购买转化的影响研究[J]. 数据分析与知识发现, 2023, 7(3): 69-79.

-
- [6] 吕巍, 杨颖, 张雁冰. AI 个性化推荐下消费者感知个性化对其点击意愿的影响[J]. 管理科学, 2020, 33(5): 44-57.
- [7] 卢嘉程. 人工智能体侵权责任承担可行路径研究[J]. 东南大学学报(哲学社会科学版), 2018, 20(S2): 58-63.
- [8] 陈晨. 人工智能侵权中的责任主体及归责原则[J]. 中外法学, 2025, 37(2): 363-380.
- [9] 袁曾. 生成式人工智能的责任能力研究[J]. 东方法学, 2023(3): 18-33.
- [10] 王利明. 生成式人工智能侵权的归责原则与过错认定[J]. 中国法律评论, 2025(4): 15-30
- [11] 杨震, 吴睨. 通用人工智能体在民事法律关系中的地位[J]. 广西社会科学, 2025(2): 1-10
- [12] 郑志峰. 人工智能应用责任的主体识别与归责设计[J]. 法学评论, 2024, 42(4): 123-137.
- [13] 程啸. 侵权责任法[M]. 北京: 法律出版社, 2021: 301.
- [14] 郝铁川. 不可幻想和高估人工智能对法治的影响[N]. 法制日报, 2018-01-03(10).