

法律规制与技术治理的双重视角下探究生成式AI在电商中的应用风险

王 静

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年3月10日; 录用日期: 2025年3月28日; 发布日期: 2025年4月29日

摘 要

解构生成式AI在电商领域中的应用场景, 继而剖析场景里易出现的民事、行政、刑事三重法律风险, 而后从规制体系层面入手分析其面临的三重悖论: 首先是技术迭代与法律滞后的结构性矛盾, 在电商应用中AI生成内容的多模态特征远超传统法律规制之射程; 其次是责任认定的算法黑箱困境, 平台以技术中立为由逃避审核义务的现象普遍存在, 这便需要从技术革新入手, 加速司法实践的创新; 最后是全球合规标准的碎片化冲突, 这些问题皆表示单一治理模式已失效, 亟需构建法律、技术与伦理协同的治理范式。

关键词

生成式AI, 法律风险, 协同治理

Exploring the Application Risks of Generative AI in E-Commerce from Dual Perspectives of Legal Regulation and Technological Governance

Jing Wang

School of Law, Guizhou University, Guiyang Guizhou

Received: Mar. 10th, 2025; accepted: Mar. 28th, 2025; published: Apr. 29th, 2025

Abstract

This study investigates the application of generative AI in e-commerce, revealing inherent civil,

文章引用: 王静. 法律规制与技术治理的双重视角下探究生成式 AI 在电商中的应用风险[J]. 电子商务评论, 2025, 14(4): 2579-2583. DOI: 10.12677/ecl.2025.1441169

administrative, and criminal legal risks alongside three interconnected regulatory paradoxes: the structural mismatch between evolving multimodal AI outputs and static legal frameworks, exacerbated by algorithmic opacity that obstructs liability attribution while enabling platforms' procedural evasion under technological neutrality claims, and the irreconcilable fragmentation of global compliance standards. The findings underscore the imperative for a paradigmatic shift from unilateral governance mechanisms toward an adaptive tripartite framework integrating legal constraints, technical transparency protocols, and ethical guardrails—a multidimensional approach critical for addressing the systemic challenges posed by AI-driven commercial ecosystems.

Keywords

Generative AI, Legal Risks, 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

生成式 AI 的爆炸式发展无疑正在重塑全球电子商务的底层逻辑,从智能客服实时响应到虚拟场景的沉浸式展示,从商品描述自动化生成到多模态营销内容的出现, AI 技术正重构着传统的“人-货-场”交互模式,面对运营成本降低转化率提升的红利,其技术革命背后的伦理危机正在悄然浮现。当 AI 生成“完美效果图”掩盖商品真实品质,当 AI 客服的“科学话术”消解消费者理性判断、当其诱导性应答突破法律边界之际,技术红利与伦理风险的角力已然进入白热化。其在电商销售模式中发挥的作用已举重若轻,常见的应用场景有但不限于: ChatGPT 和 Claude 提供的客服问答;利用大语言模型,如 GPT-4 实现更为精准且低成本地为海量产品提供详细描述;通过 Stable Diffusion、DALL-E 等工具生成虚拟模特试穿服装的图片,使用 Midjourney 合成不存在的美容仪器使用效果图;通过文本生成视频工具如 Synthesia、Runway ML 创建产品介绍视频,包括脚本、配音和画面等。上述 AI 的普遍应用使得电商网络实现了最低成本的效率陡增,科技的进步是历史之洪流也是电商发展的红利,其有助于新型电商运营模式的发展,多模态技术联动将会为消费者提供更为沉浸的购物体验。为节约成本而选择智能客服、为海量商品生成产品描述是发展趋势,虚拟试穿等应用也是有利于消费者选择心仪的产品。但是也得在法律允许的范围內考量伦理与利益的平衡才能得到长足发展。使用 AI 技术降低成本提高销量是电商共趋,但是利用技术红利故意面向难以区分 AI 技术的消费者,只会使消费者权益在铺天盖地的虚假描述与难以甄别的 AI 技术运用场景中荡然无存。

2. 生成式 AI 电商应用的三维法律风险

随着电商行业的快速发展,国家和地方政府虽说已经出台了一系列政策法规来规范行业秩序,但是 AI 的大量适用已造成了诸多风险破竹之势。首先, AI 生成内容的大肆应用显然已经对消费者决策产生了认知干预,使消费者陷入了拟真性陷阱。其次,当数字人主播大肆出现在直播间,运用 AI 分析其微表情模拟技术,以达到更加有说服力的模式,譬如通过瞳孔聚焦算法可以增强数字人主播的可信度感知[1]。这种运用无疑给了消费者一种权威性错觉。再次, AI 生成的海量评价极有可能引导消费者决策疲劳 2020 年中国消费者协会《“618”消费维权舆情分析报告》指出,流量造假是消费者维权的热点和难点。上述生成式 AI 的应用皆使消费者的认知偏差被放大。

2.1. 民事权益侵害风险

AI 虚构商品成分侵害了消费者的知情权。消费者知情权是消费者权利束中的基础性权利，实现消费者知情权有助于消费者权益的保护，知情权具有前置性[2]。人们在电商平台进行购物时须知商品的真实情况，但是由于 AI 虚构商品成分导致消费者的知情权被严重侵害，致消费者因 AI 的生成式描述购入货不对板的商品。据我国《消费者权益保护法》第 8 条规定：消费者享有知悉其购买、适用的商品或者接受的服务的真实情况。生成式 AI 的使用不应该以消费者的权益为代价从而实现商家的利益翻番。

2.2. 行政监管突破风险

AI 生成“国家级专利”“治愈率 99%”等禁止性宣传用语，明确违反了《广告法》。据《广告法》第九条，禁止使用“国家级”“最佳”等绝对化表述。AI 因数据训练偏差产生违规用语在海量商品的描述中难以逐帧筛查。《广告法》第二十八条明确禁止虚假宣传。AI 生成的“治愈率 99%”等统计数据需提供完整的实验报告、统计样本等证明依据。某药企因生成“临床试验有效率 97%被处罚”，因为其无法提供原始数据支撑。

2.3. 刑事犯罪触发危险

利用 AI 批量生成虚假用户账号、伪造交易记录、虚构商品评价，若形成了规模化的刷单产业链即可能涉及非法经营罪；若通过 AI 技术侵入平台数据修改交易数据则构成破坏计算机信息系统罪；通过虚假交易骗取平台补贴或商家佣金则易构成诈骗罪。利用 AI 生成虚假的报告或伪造商品资质文件，在食品、药品等特殊领域则构成生产、销售伪劣产品罪；如果设计的三方检测机构资质冒用则构成提供虚假证明文件罪；若是伪造海关检验检疫证明等，则构成伪造国家机关公文罪。

3. 生成式 AI 法律规制的三重困境

3.1. 责任主体认定困境

生成式 AI 大规模、深层地在电商领域应用，打破了传统的“人-货-场”的权责关系，这便注定责任主体的认定会存在多重法律争议[3]。于平台责任而言，技术中立抗辩已然被瓦解：《电子商务法》第 38 条要求平台对经营者资质和商品服务合法性承担审核义务，但在 AI 生成内容的场景之下，平台常以“技术中立”为由主张免责，抗辩理由集中于“技术不可控性”即主张 AI 生成内容的实时性以及商品信息的海量性致审核不能及时进行，和“工具属性切割”即强调仅提供了 AI 技术支持，未参与到具体内容的创作。如“阿里云服务器案”中“管道服务”免责原则。但是，随着司法实践的不断深入已经逐步突破中立技术抗辩的边界。司法实践中对于“AI 虚假宣传案”已新增裁判规则：包括但不限于审核平台是否设置主动屏蔽机制尽到算法过滤义务，以及对特定品类譬如保健品等 AI 生成内容增强审核，若未履行则构成《民法典》第 1195 条“应知而放任”的间接故意。于商家责任而言，商家利用 AI 技术生成虚假宣传内容时常以“训练数据偏差”等理由否认主观故意。在司法实践中亦可通过技术可控性审查来核查是否对 AI 模型进行了人工干预，主动设置“美白”“0 副作用”等诱导性种子词；也可以通过经济合理性判断分析异常数据的经济收益，而后可以调取商家从前是否存在行政处罚记录，由此进行历史行为之关联来推定商家的犯罪故意[4]。

3.2. 电子证据固化困境

由于 AI 技术的动态性与其黑箱特征，可能致传统证据规则面临系统性挑战。首先是电子证据存证困境。因为电商平台的商品页常常动态更新，导致 AI 生成的内容可随时被覆盖，而且因为深度学习模型的

参数调整可以改变输出结果，但是训练的过程记录很难可视化，如 Transformer 模型的多头注意力机制就难以还原。其次是传统司法应对已经无法适配相应的 AI 发展，故司法实践需要创新。现杭州互联网法院联合蚂蚁链已经建立了“AI 生成内容全链路存证”机制，这种机制可以记录 AI 生成内容从初始版本到最终发布的 12 项元数据。另有通过非对称加密确保存证内容不可被篡改的哈希值校验。深圳中院也开启了技术审计制度，通过“算法镜像封存”要求被告企业提交相关文件。

3.3. 跨境合规适配困境

AI 在全球范围内的监管规则呈碎片化趋势，故跨境电商便出现了“合规鸿沟”。欧盟颁布的《AI 法案》形成了高压监管规则。要求所有 AI 生成内容须添加不可移除的数字化标签，例如 Meta 因为没有标注 AI 生成商品图被罚款。中国关于 AI 立法具有滞后性，《生成式 AI 服务管理办法》仅设定原则性框架，但是缺乏在电商应用场景中的规范指引。现存地方层面的司法创新，如广州互联网发布《涉 AI 电商案件审理指南》新增了“跨境合规映射”规则，对于同时违反中国与目标市场法律的行为加重处罚，同时也允许企业以遵守更为严格法域标准作为免责抗辩。

4. 风险协同治理路径的三维构建

4.1. 破解责任主体认定困境：法律规制的刚性框架建设

修订《广告法》第 28 条，增设 AI 生成内容的特别条款：增设强制标注要求，规定所有 AI 生成的产品描述以及用户评价需标注“AI 生成”不可覆盖的标识；同时可增设穿透批露义务，即商家需公开 AI 模型训练数据来源以及筛选标准。同时对标电子商务领域，可以制定《电子商务 AI 应用管理条例》来建立分级管理制度。在医疗美容、金融产品等对社会以及人体健康会产生较重影响的领域划分至高风险场景；对于服装设计、文案生成等可能会对相对应市场竞合产生影响的领域划分为中风险区域从而实施备案制管理；对于客服应答、物流跟踪等涉及人数范围比较小影响比较小的领域可划分为低风险场景仅需实行事后抽查。

最高法院可以出台《AI 电商纠纷案件审理指南》，可以通过最高法的价值取向完善司法实践：首先确立惩罚性赔偿量化标准：将 AI 生成的内容的传播量与商家主观恶意进行叠加计算；其次商家需要自证已采取“合理技术措施”防范虚假内容生成，即推崇过错推定原则，举证清单需要包括商家训练 AI 的数据清洗日志以及算法过滤规则等。

4.2. 突破电子证据固化困境：技术赋能的动态保障

生成式 AI 超强的模仿创作能力具有“双刃剑”属性，即 AIGC 技术使虚假信息更“真实”、更具欺骗性，而且在多模态情境下可以采用文本、语音、视频“半真半假”的形式欺骗用户，故更需要技术革新提供更为坚实的保障[5]。首先，根据上述分类管理级别，对于高风险类的项目实施“双轨四步审核制”，第一步运用 AI 工具进行初次审核以此过滤掉明显的违法内容；第二步则聘请相关行业的人员进行第二步人工复核，建立审核负责机制，譬如保健品广告需要执业药师来签字确认。第三步确立合理的期限间隔以及比例，对已经通过上述两步审查之内容进行抽样复查。对于同类问题连续出现三次的，利用熔断机制对于这种现象进行触发式关闭。其次，构建“AI 信用分”体系，违约生成内容可进行扣分，对于低于及格线之商家，限制其 AI 功能之使用，将此连接到商家的信用分系统[6]。

各大平台皆可以推动“三色标识系统”的建立，将 AI 生成内容以未经人工审核、经过基础过滤、已经通过全链路验证分别标识为红色警示、黄色提示、绿色通过三种。这便能更好地保障消费者的知情权。而后设立“AI 维权快速通道”：若存在争议内容，用户有权一键冻结，触发后 AI 生成页面将转为风险提示。

示页面，引入第三方鉴证机构在 48 小时内出具技术分析报告。

4.3. 消弭跨境合规适配困境：平台治理的生态重构

推动 WTO 电商谈判形成标准互认机制，建立“白名单”共识；将医疗、金融等场景列为全球高风险类别从而统一风险分类标准。在执法层面，可以构建“AI 生成内容联合监管云”促进跨境执法协作，国际范围内达成协议可以共享高风险模型特征库，也方便建立跨境电子取证通道。在跨境管辖衔接方面，面对海外市场的生成内容可以采取“行为发生地 + 结果影响地”复合管辖标准。同时司法实践应更新其陪审制度，实行“双轨制”技术陪审，计算机专家负责解析被告所运用 AI 背后的算法逻辑，行业专家则评估技术应用的合理性。参考北京互联网法院进行“算法沙盘推演”。司法机关可从指导案例制度的创新运用中来确立裁判规则。

5. 结语

电商领域中生成式 AI 的嵌入是技术赋能的革命性突破，但同时亦带来法律规制与伦理治理的严峻考验。本文通过法律与技术视角揭示了其三重风险形态：技术性异化导致的认知干预风险、算法黑箱致使的权责断裂风险以及制度之后滋生的跨境合规风险，故本文提出应构建“法律 - 技术 - 平台”协同治理的立体框架[7]：在法律规制层面通过《电子商务 AI 应用管理条例》建立风险分级管理，并推动过错推定原则在司法实践中的应用；在技术治理层面则强化区块链存证与数字水印技术的深度结合，构建覆盖“数据输入 - 模型训练 - 内容输出”的全链路回溯体系；在平台责任层面推行“三色标识系统”与“AI 信用分”制度将技术合规纳入平台信用体系，通过“双轨四步审核制”实现风险动态管控。只有实现法律规制的刚性约束、技术治理和商业伦理三者的有机统一才能在技术革新与权益保护之间找到动态平衡点，为生成式 AI 驱动的电商新模式筑牢发展基石。

参考文献

- [1] 公正. 虚拟数字人主播的表情生成技术研究[J]. 电视技术, 2024, 48(8): 216-218, 223.
- [2] 陈燕红. 论消费者知情权的权利实现[J]. 暨南学报(哲学社会科学版), 2013, 35(11): 69-75.
- [3] 王家宝, 武友成. 共生视角下直播电商治理的创新机制[J]. 管理现代化, 2021, 41(5): 44-46.
- [4] 郑宁, 葛扬. 电商直播的法律规制及完善途径[J]. 社会治理, 2021(3): 21-27.
- [5] 李白杨, 白云, 詹希旎, 等. 人工智能生成内容(AIGC)的技术特征与形态演进[J]. 图书情报知识, 2023, 40(1): 66-74.
- [6] 邓锦雷. 强化对直播带货的柔性约束[J]. 人民论坛, 2020(23): 60-61.
- [7] 陈云. 协同治理视域下直播电商监管探析[J]. 国家治理, 2024(11): 52-60.