

# 电商环境下人工智能技术应用的风险和解决路径研究

陈天容

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年3月12日; 录用日期: 2025年3月27日; 发布日期: 2025年4月24日

## 摘要

在数字化时代的浪潮下, 人工智能技术已经成为当下的革命力量。人工智能与电商的深度融合, 不仅为消费者带来了更加个性化的购物体验, 也为企业提供了更高效的运营手段。但是人工智能技术在电商环境中的应用也面临着诸多风险, 例如数据安全, 算法偏见, 法律监管等风险。为推动行业的可持续发展, 我们需要采取有效的措施解决当下存在的问题。本文将深入分析人工智能在电商中的应用现状, 风险和解决路径, 促进二者更好地结合。

## 关键词

电商环境, 人工智能技术, 数据安全

# Research on the Risk and Solution Path of Artificial Intelligence Technology Application in E-Commerce Environment

Tianrong Chen

School of Law, Guizhou University, Guiyang Guizhou

Received: Mar. 12<sup>th</sup>, 2025; accepted: Mar. 27<sup>th</sup>, 2025; published: Apr. 24<sup>th</sup>, 2025

## Abstract

Under the tide of the digital age, artificial intelligence technology has become the current revolutionary force. The deep integration of artificial intelligence and e-commerce not only brings consumers a more personalized shopping experience, but also provides enterprises with more efficient means of operation. However, the application of artificial intelligence technology in the e-commerce

environment also faces risks such as data security, algorithm bias, and legal regulation. In order to promote the sustainable development of the industry, we need to take effective solutions. This paper will deeply analyze the application status of artificial intelligence in e-commerce, risks and solutions, and promote a better combination of the two.

## Keywords

E-Commerce Environment, Artificial Intelligence Technology, Data Security

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

随着电商业务的不断拓展和用户规模的持续扩大, 电商企业面临着日益复杂的挑战。如何在商品种类繁多、用户需求多样化的背景下精准地满足用户需求, 提升用户体验, 成为电商企业急需解决的问题。同时如何优化运营, 降低成本, 提高市场竞争力, 也是电商企业在市场中取得成功的关键因素。在这样的背景下, 人工智能技术凭借其强大的数据处理能力、智能分析能力和自动化决策能力, 成为电商企业应对挑战、实现创新发展的重要角色。当下人工智能技术已经运用到电商领域的多个环节, 比如营销环节和供应链管理方面, 通过运用人工智能技术都能更好地解决问题。

## 2. 人工智能技术在电商环境中的应用现状

### 2.1. 精准化营销和个性化推荐

在电商运营中, 人工智能技术在精准营销与个性化推荐方面发挥着重要的作用。电商市场的竞争日益激烈, 如何更加准确地了解消费者需求, 提高营销效果, 是目前电商企业关注的重点。人工智能算法通过对消费者的注册、浏览记录、购买记录、搜索关键词、停留时间和评论等历史行为数据进行建模, 然后把用户模型中兴趣需求信息和推荐对象模型中的特征信息匹配, 同时使用算法进行计算筛选, 找到用户感兴趣的商品[1], 从而实现个性化推荐和精准营销。实现精准营销的关键就在于在正确的时间通过正确的渠道向正确的用户推荐商品, 从而影响他们的购买决策, 最终达到高效的营销目标[2]。而在信息技术的帮助下, 人工智能个性化是实现精准营销的重要途径, 因此在电商企业也就得到了广泛运用。

我们经常使用的购物平台——淘宝就是通过人工智能技术实现向用户精准的投放广告。淘宝利用深度学习算法对用户的行为数据进行分析, 根据他们的行为特征将用户划分为不同的兴趣群体, 然后针对不同的群体投放个性化的广告。例如对那些经常购买护肤品和化妆品的用户, 淘宝就会更倾向于向他们投放相关的商品, 而对于那些热爱包包首饰的用户, 淘宝就会根据他们各自的爱好推送相应的时尚单品。通过这种精准营销的方式, 既可以提升广告的点击率, 还促进了商品销量的增长。此外, 部分电商平台不仅会向用户推送他们经常购买或关注的商品, 还会根据用户的消费习惯向他们推送与之搭配的商品。若是用户经常购买健身器材, 电商平台可能会向他们推送运动服装或运动饮料等配套的产品。这种个性化推荐就极大的提高了用户发现心仪物品的概率。

提高人工智能技术的深度应用, 电商企业不仅可以更准确地满足用户需求, 还能大幅度的提升营销效率, 为消费者创造更智能化, 个性化的购物体验。

## 2.2. 智能客服和服务优化

在电商领域中，智能客服作为人工智能技术的重要突破，正在改变传统客服的模式与效率。随着电商业务的快速发展，越来越多的消费者在电商平台上购物，导致客户咨询量呈爆发式增长。传统的人工客服难以满足 24 小时不间断服务、快速响应等需求，因此智能客服应运而生。所谓的智能客服就是可以通过自然语言学习和机器学习实现与客户的智能交互，为客户提供高效、准确和个性化的服务。

智能客服的出现很好的解决了即时回答用户的问题，利用先进的自然语言处理技术，快速了解用户的问题，对客户疑问进行解答并给出精准的回复，大大减少了客户等待的时间。其次智能客服与用户聊天时，可以深入地了解用户的购买习惯，浏览情况和个人偏好更好的为用户推荐商品[3]。以京东电商平台上的智能客服 JIMI 就是一个典型的例子。JIMI 能够很好的理解用户的自然语言提问，实现 24 小时无限量的服务无论是售前咨询，售后服务，还是其他常见的问题都能快速给出准确的回答。例如，当用户询问其某款手机的参数时，它可以迅速地调取商品的参数信息告诉购买者。

智能客服不仅可以提供高效的，准确的服务，还可以充当“保镖”的角色。比如支付宝的“小蚂答”，如果它检测到用户的账户存在风险时会自动启动一键挂失功能，冻结账户；在用户遇到诈骗的情况时，“小蚂答”还可以帮助用户一键报案，减少损失[4]。同时智能客服还可以实现与人工服务无缝对接。对一些复杂难懂的问题，智能客服会将问题自动转给人工并将之间的对话一并转交，使人工客服能够快速了解问题背景，提高问题解决的效率。这种人机协作的模式，充分发挥了智能客服的高效性和人工客服的灵活性，为客户提供了更加优质的服务。

通过智能客服的广泛应用，电商企业不仅能够降低人工客服成本，还能提升服务效率和质量，满足消费者对即时响应和个性化服务的需求。

## 2.3. 供应链管理和物流优化

在电商的供应链管理中，人工智能技术有着不可或缺的作用。它通过对销售数据、市场趋势、用户行为等数据进行多层次的分析，人工智能可以实现需求预测、库存优化和物流配送的智能管理，提高供应端的效率和灵活性，降低成本。在面对错综复杂的业务流程，如订单处理，库存管理和物流配送这些环节时，电商企业就急需需要人工智能这样的技术来梳理和优化这些环节。正是人工智能与电商平台的深度融合，不仅提升了电商平台的运营效率，而且还让电商平台得到高质量的运行和发展。

在库存管理方面，人工智能技术可以推动智能化存储管理，实时检测库存情况。通过分析销售数据和订单信息，自动调整商品的存放地域和商品的数量，这样可以在很大的程度上减少人为的因素[5]。电商平台可以利用算法对后台的库存进行实时分析，综合考虑商品的销售速度，季节变化，优惠力度等因素，动态调整库存的数量。例如当某款商品的销售数量增加，人工智能会及时提醒商家增加该商品的库存量；而当商品的销售量下降时，系统则会建议商家减少库存，避免商品积压。在智能化的库存管理下，优化了仓储运营效率，降低库存成本。

在物流配送方面，人工智能技术同样也展现出了强大的潜力。对于电商企业的发展来说，物流的高效运行也是促进企业效益稳定提高的关键因素之一。电商企业可以利用人工智能技术进行预测分析。例如，人工智能技术可以提前预计销售订单上的交货日期，并且依据气候条件、交通运输状况等变数实时进行调整，科学安排物流运输路径，从而有效缩短运输时间并节省开支[6]。在城市地区部分电商企业已经开始采用无人车来配送商品，进一步提高了配送的效率，降低了物流的人工成本。电商企业在人工智能的协助下，不仅仅提高了物流的智能化水平，还为消费者带来了更快速、更便捷的配送体验。

在人工智能技术的帮助下，电商企业不仅能够精准营销，为客户个性化推荐商品，还能更加智能为客户提供服务，提高客户的满意度。最后通过实时监测库存情况，为商家提高最优的运输路线，使之快速适

应市场变化。这种技术与业务的融合，正在推动电商行业向更高效，更智能的方向发展。

### 3. 人工智能技术在电商环境下的风险

#### 3.1. 数据安全和隐私风险

人工智能是一把双刃剑，它在为电商企业提供强大的助力时，也存在着许多风险与挑战，尤其是在数据安全和隐私保护方面。电商企业在利用人工智能技术实现高质量运行时，人工智能可能会侵犯消费者的隐私和权益。电商平台积累了大量的用户数据，人工智能要为电商平台提供用户更精准的信息，必然会通过机器学习算法收集和分析用户的数据信息。而在数据收集过程中，存在着授权不明确、隐私保护不足的问题。

人工智能收集数据过程中的授权问题是一个重要的风险点。许多电商平台在收集用户数据时，虽然会向用户展示隐私政策，但这些政策太过于复杂，许多用户不愿意去阅读或者无法理解其中的含义。但如果用户不同意平台收集他们的个人信息，通常情况下无法正常使用平台的相关功能，所以他们只能选择同意。但这种“同意即使用”的模式，实际上剥夺了用户对个人数据的真正控制权。更严重的是，当数据被人工智能收集后，用户往往无法了解他们是如何处理、存储和保护含有个人隐私的数据，因此一旦数据受到非法侵入，用户的个人敏感信息就可能遭到篡改、窃取，从而侵犯用户的隐私权益[7]。当下，数据已经成为推动创新和发展的重要资源，而数据存储技术则扮演着关键的角色。数据存储是通过计算机系统或其他存储介质来存储和保存数据的[8]。如果电商企业对数据存储保护不足，就会进一步加剧这种风险。如果数据存储系统的加密算法不够强大，黑客可能会通过技术手段破解，从而获取用户数据，这不仅会对用户的财产安全造成了严重的威胁，同时用户还可能面临着身份被盗用、信用卡欺诈等风险，从而承担法律责任的。

数据滥用问题也是在电商领域中不可忽视的问题。一些电商企业会将用户数据用于用户毫不知情的商业目的，例如将数据出售给第三方广告商以获取经济利益。这样的行为不仅违反了用户隐私政策，还导致用户收到大量的垃圾广告，影响用户的体验感。例如，用户在使用某个电商平台后，其他平台或应用中会出现大量相关的广告，这正是数据滥用的体现。

#### 3.2. 算法风险

人工智能在电商环境中的应用，尤其是在对用户行为分析和个性化推荐方面，虽然极大地提升了用户体验和营销效率，但同时也带来算法偏见与歧视的问题。人工智能在进行深度学习的过程中使用了大量来自特定领域的的数据，为想要的结果做出最佳决策。但深度学习只能在特定领域做出决策、预测和分类[9]，因此可能会出现并放大现有的社会偏见，导致不公平的推荐或歧视性内容，给用户带来不公正的电商体验。例如，用户可能因为算法偏见而无法看到与他们相关或感兴趣的内容，或者被错误地排除在某些营销活动之外[10]。电商平台在收集用户数据时就存在局限性，无法全面、准确地反映用户群体的多样性。如果用户群体的样本数量过少，或者数据收集过程中本身存在选择性偏差，那么算法就可能对这些群体产生偏见。比如以性别为例，在推荐时尚类商品时，算法可能会更倾向于推荐女性款式的商品，而忽视男性用户的需求，导致男性用户在购物过程中得到的推荐结果不够精准和全面。

同时在电商的精准营销和个性化推荐中，算法黑箱的问题也是长期存在。电商平台通过收集用户的浏览记录、购买记录、搜索关键词等多方面的数据，利用深度学习算法进行分析并为用户推荐商品。而这些算法过程包含了大量的参数和计算过程，由于算法黑箱的存在，导致无法对外展示具体分析和运行的过程。在这样情况下他们也就无法理解自己为什么会收到某条广告或推荐内容，这种不透明性不仅让用户对推荐结果的信任度降低，也使得电商企业会面对用户的质疑和投诉。

### 3.3. 法律与监管风险

人工智能技术在电商领域飞速发展，虽然为电商行业带来了巨大的创新和效率提升，但相关的法律法规未能及时跟上技术的步伐，导致出现了法律法规滞后与监管空白的问题，这种滞后性给电商行业的健康发展带来了潜在风险。

目前，人工智能与电商行业融合有着更好的发展前景，但是在这方面还存在法律法规不足的缺陷。虽然一些国家和地区出台了数据保护的相关法律。如欧盟的《通用数据保护条例》虽然对收集数据目的和对保留数据的必要期限做出了限制<sup>1</sup>，以及中国的《个人信息保护法》同样对数据的收集，存储和处理做了严格的规定<sup>2</sup>。但人工智能在某些特殊的场景下仍然存在着法律适用不明确的情形。例如，在个性化推荐中，人工智能需要收集大量用户的数据，但法律并没有给出清晰的界定哪些数据可以被使用、使用的限度以及如何确保用户的知情权和选择权，这模糊性就会导致数据滥用侵犯用户权益。

在算法监管方面，法律规定也存在明显的空白。目前人工智能在电商中的商品推荐，搜索排名，定价方案方面都发挥着关键作用，但由于没有专门的法律对算法的设计、开发、使用和监督进行规范。算法的透明度和公平性，产生的偏见和歧视等问题，都缺乏相应的法律约束。例如，大数据杀熟的情形。某些电商平台可能会通过算法对不同用户群体进行差异化定价，导致价格歧视问题。这种不公正，不合理的算法行为，会严重影响市场的公平竞争和消费者的利益。

人工智能技术快速发展的同时也衍生出了其他的分支，生成式人工智能就是其中的一个重要分支。而生成式人工智能的发展也带来了新的法律风险。目前有部分人利用生成式人工智能技术的换脸功能生成商品短视频或是带货短视频，存在侵犯他人肖像权的问题，更有甚者利用这个功能去破解手机上的面容识别功能，给电商交易环节带来了很大的法律风险[11]。例如，发生在重庆的 AI 换脸案例。张某系网红博主，近期发现重庆米某有限责任公司在其快手平台“AI 换脸猫”小程序中，使用她的肖像制作换脸视频，进行商业广告引流宣传，获取商业广告收益<sup>3</sup>。近两年来发生了大量的类似案件，由于法律对生成式人工智能的规定还存在不足，使得监管机构在面对人工智能技术在电商领域的应用时，缺乏有效的监管手段和依据。这不仅影响了市场的秩序，也损害了消费者的信任。

## 4. 应对人工智能技术下风险的法律路径

### 4.1. 强化用户权利和保护措施

为防止电商平台利用人工智能技术收集用户数据的隐私，应完善人工智能收集个人信息的法律保障体系，并加强风险的预防法律功能。同时在数据的收集，存储和使用的各个环节，立法者应当明确规定电商平台可以收集哪些数据，使用的限度以及如何保护用户的选择权和同意权。

在收集数据过程中，立法者要强化用户作为数据主体的权利。收集数据除了征得用户的同意外，还应当确保其拥有知情权，即电商企业应采用“明示同意”的原则收集个人信息，如果用户不同意收集数据，平台也不能因此阻止用户对平台功能的正常使用。同时向用户明确告知数据使用的具体目的和方式，获得用户的明确授权。例如，平台在用户注册或使用服务时，以清晰、简洁的语言向用户说明数据将如何被使用，并提供易于理解的隐私政策。同时，如果权利人发现电商平台有滥用数据的行为，法律应当确保用户有删除权和对数据使用之后的访问权。例如，用户应有权要求平台删除其个人数据，并有权查看平台如何使用其数据，以防止个人信息泄露。

法律应规定电商平台在数据处理过程中遵循数据最小化原则，只需要收集完成特定目的所需要的最

<sup>1</sup> 参见《通用数据保护条例》第五条。

<sup>2</sup> 参见《个人信息安全法》第 13 条，第 17 条。

<sup>3</sup> 参见重庆江北区人民法院(2023)渝 0105 民初 36081 号。

少数据以确保最低限度的减少对个人隐私的泄露。同时应当制定具体化和明确化的隐私保护，将可能泄露个人信息的数据加密化和匿名化。最后，法律应当确定电商企业在处理数据的责任，在数据处理过程中，电商企业有权保护用户的个人隐私和相关数据的安全，如果在使用过程中侵犯他人隐私或相关信息和数据泄露造成严重后果的，采用过错推定的归责原则，实行举证责任倒置，企业如果不能证明自己没有过错的，法律应追究责任，让其承担法律后果。

对数据的保护也可以从技术方面突破，我们可以建立消费者个人数据安全认证机制，在消费者进行电商交易活动之前进行安全认证，完成交易活动之后，该安全认证机制自动对消费者的浏览足迹进行清除，防止黑客利用技术手段盗窃数据[12]。其次，建立完善的网络监管体系，当系统检测到黑客攻入的时候，在黑客产生影响之前对其实施攻击，同时自动追踪攻击的来源，一旦捕获应采取法律手段严惩不贷。

## 4.2. 算法优化的法律路径

在数字时代，随着智能技术算法适用的领域不断扩大，算法歧视和偏见以更隐蔽和更广阔的方式影响着人们的生活。因此我们需要强化对算法技术的管制以及从法律层面去应对算法歧视和偏见的困境。

为了避免算法歧视对消费者造成的恶性后果，电商平台应当要提高自身的算法意识，加强算法运用的自我监督，电商平台建立自身审查机制的运行，定期评估算法的运行情况。由于存在算法黑箱，导致用户对算法过程一无所知，而平台本身的算法技术人员更了解算法的运行，因此由电商平台定期向相关部门提交算法运行机制的报告。其次，对于市场监管部门来说，应当建立起针对算法歧视行为的有效监管体制，革新监管规则，细化监管分工。监管部门需要提高自己的监管科技，运用算法监管技术对企业提供的算法运行检查报告等进行安全性、公平性的评估，并实时监控市场中可能出现的算法歧视风险[13]。

为避免算法歧视和偏见，我们可以建立算法责任体系和举证规则。为了维护消费者的合法权益，我们应当明确责任主体，是算法设计者在设计之初就对人工智能输入了歧视的因素，还是电商平台为了追逐利益在算法运行时输入了相关的歧视指令。如果我们只从某个方面进行预防和整治并不会得到完全的控制，因此我们需要合理分配不同主体的责任。而当用户的合法权益收到侵害时，他们往往会选择向法律求助，因此分配举证规则是有必要的。由于算法技术的复杂性和算法黑箱的原因，普通人无法理解和证明算法歧视的存在，因此我们可以采取举证责任倒置的方式，要求电商平台和算法技术人员去证明并不存在歧视的行为会更加合理。

## 4.3. 完善法律与监管体系

目前我国没有一部完整的《人工智能法》，而对人工智能领域的规定相对比较分散，从现有的法律框架来看，主要是从《网络安全法》，《数据安全法》和《个人信息安全法》分别从网络，数据，个人信息方面对人工智能进行规范和制约。对算法的治理主要是通过《互联网信息服务算法推荐管理规定》来要求算法备案，公平审查防止大数据的歧视问题。

由于人工智能在电商领域的广泛应用，这些法律规定就存在着许多不足。因此我们就需要完善法律体系，应对技术发展带来的各种风险和挑战。

利用人工智能收集数据时，立法应明确数据的所有权、使用权和管理权，同时必须获得用户的明确授权，并保障用户的知情权和选择权。明确规定哪些个人数据可以被收集，收集之后使用的限度以及如何保护个人数据。如果用户不同意收集的数据有权随时撤回同意，并要求平台删除其个人数据。对于算法监管方面，虽然《互联网信息服务算法推荐管理规定》规定了网络部门同电信，公安，市场等有关部门建立算法分级分类的安全管理制度<sup>4</sup>，以及算法服务提供者应当通过互联网信息服务算法备案系统进行

<sup>4</sup> 参见《互联网信息服务算法推荐管理规定》第 23 条。

备案<sup>5</sup>。但随着社会的不断发展,这些法律规定不足以解决当下的问题。立法部门应当制定专门的算法规定,规范算法的设计、开发、测试和应用。要求企业在使用算法时必须公开算法的基本原理和数据来源,增强算法的透明度。部门化的监管容易对综合型的算法出现监管竞合,而对新型的算法出现无人监管的局面。在这样的情况下就可能会出现监管的空白。因此建立算法统一的监管机构,对可能影响用户权益和市场公平竞争的算法进行监管和审查评估,例如,可以委托对综合型和新型算法都了解的第三方机构对电商平台进行监管,确保算法的公平性、公正性和合法性。

对生成式人工智能造成新的法律风险,如侵犯肖像权、破解面容识别功能等。我们可以采取多层次的战略和措施。对生成式人工智能的应用实施分类分级监管,制定相应规则和指引,确保不同级别的服务得到适当的监管与指导。例如,对于涉及用户肖像的生成式人工智能应用,应制定严格的审核机制,防止侵犯他人肖像权。同时,面对伦理法规的“硬法缺失”,呼吁立法机构建立并完善伦理准则、规则和问责机制,以明确人工智能相关主体的权责边界,全面保障各方的法定权益[14]。对于用户侵犯他人信息,造成他人权益受损的,法律一定追究其责任。

## 5. 结论

在当下快速发展的电子商务时代,人工智能技术成为引领行业变革的核心动力,它们不仅通过数据挖掘和智能管理提升了电商平台的运营效率,而且更全面地渗透到电商平台的各个环节。从精准营销,个性化推荐,供应链管理和物流优化,极大提高了消费者的购物感受,而且这两大技术的融合为电商企业创新注入了新的活力。虽然人工智能的广泛应用给用户带来的风险与挑战,但随着人工智能技术的不断进步和法律法规的逐步完善,电商行业将迎来更加广阔的发展空间。

## 参考文献

- [1] 张小梅,许桂秋.商务智能方法与应用[M].北京:人民邮电出版社,2019:16-18.
- [2] 田昌聪.电商平台人工智能个性化推荐对APP持续使用意愿影响的实证研究[D]:[硕士学位论文].武汉:华中农业大学,2023.
- [3] 王宁宁.大数据与人工智能在电商运营模式中的应用及影响[J].商业经济研究,2025(2):38-41.
- [4] 张泽谦.人工智能:未来商业与场景落地实操[M].北京:人民邮电出版社,2019:130-131.
- [5] 付咸瑜.探究人工智能技术在跨境电商中的应用与创新[J].商场现代化,2024(19):64-66.
- [6] 杨妮.大数据时代人工智能在电子商务领域的应用研究[J].营销界,2024(16):56-58.
- [7] 苏子龙.生成式人工智能的数据安全风险防控与法律规制研究[J].通信与信息技术,2024(5):95-98,110.
- [8] 薛达,韦艳宜.一本书读懂AIGC:探索AI商业化新时代[M].北京:机械工业出版社,2024:29-31.
- [9] 李开复.AI未来[M].杭州:浙江人民出版社,2018:21-22.
- [10] 毛雪.人工智能助力网络直播营销:应用场景与前景展望——以抖音电商为例[J].商场现代化,2024(19):79-83.
- [11] 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.
- [12] 杨虹,钟小飞.电子商务消费者个人数据安全危机的对策研究[J].图书情报导刊,2017,2(3):61-67.
- [13] 汤雪纯.算法歧视的法律规制[D]:[硕士学位论文].济南:山东财经大学,2023.
- [14] 徐伟,李文敏.生成式人工智能法律风险的源头治理[J].行政与法,2025(2):92-104.

<sup>5</sup> 参见《互联网信息服务算法推荐管理规定》第24条。