

电子商务领域人工智能应用的法律规制

沈倾城

浙江理工大学, 法学与人文学院, 浙江 杭州

收稿日期: 2024年12月16日; 录用日期: 2025年1月3日; 发布日期: 2025年2月19日

摘要

电子商务与人工智能的交汇催生了新的商业生态, 引发了法律规制的紧迫需求。文章深入探讨了人工智能在电子商务领域的广泛应用, 从智能推荐系统到智能客户服务, 再到智能供应链管理与智能财务管理, 展现了人工智能为电子商务带来的革命性变革。然而, 随之而来的隐私保护、数据安全、算法偏见等问题凸显了现有法律体系的不足。文章还强调随着算法信任成为电子商务中交易信任的基础, 智能合约的自动执行特性限制了合同自由原则, 引发法律效力问题。为应对这些挑战, 文章建议构建包含明确人工智能法律地位、制定准入标准、确立数据隐私和安全保护规则以及加强监管机制的法律框架, 以保障消费者权益, 维护市场公平竞争。

关键词

电子商务, 人工智能, 法律规制

Legal Regulation of Artificial Intelligence Applications in E-Commerce

Qingcheng Shen

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

Received: Dec. 16th, 2024; accepted: Jan. 3rd, 2025; published: Feb. 19th, 2025

Abstract

The intersection of e-commerce and artificial intelligence (AI) has given rise to a new commercial ecosystem, creating an urgent need for legal regulation. This article explores the widespread applications of AI in the e-commerce sector, ranging from intelligent recommendation systems and smart customer service to AI-driven supply chain and financial management, illustrating the revolutionary transformations brought by AI to e-commerce. However, accompanying issues such as privacy protection, data security, and algorithmic bias highlight the deficiencies in the existing legal framework. The

article further emphasizes that as algorithmic trust becomes the foundation of transactional trust in e-commerce, the automatic execution characteristics of smart contracts limit the principle of contractual freedom, raising concerns about legal validity. To address these challenges, the article advocates for the establishment of a legal framework that includes the clear legal status of AI, the formulation of access standards, the establishment of rules for data privacy and security protection, and the strengthening of regulatory mechanisms to safeguard consumer rights and maintain fair market competition.

Keywords

E-Commerce, Artificial Intelligence, Legal Regulation

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. 人工智能在电子商务领域的应用与挑战

1.1. 智能推荐系统的发展与影响

随着电子商务的快速发展,智能推荐系统成为提升用户体验、增强用户黏性的重要工具。这些新系统最主要的功能就是借助人工智能技术计算物品之间的相似度来进行页面推荐[1]。辅之以集成大数据分析、机器学习等人工智能技术,电子商务经营者能够根据历史用户的浏览记录、购买记录、搜索记录等多维度的用户数据,精准预测偏好与需求,从而展示针对数据来源用户的个性化商品推荐,进一步提高商品的曝光率和销售转化率。智能的电子商务个性化推荐系统工作原理包含四个步骤,首先收集用户行为数据收集;然后,计算相似度权重;再次,预测评分;最后,生成推荐列表。个性化智能推荐系统的出现,既是技术进步的结果,也源于市场需求。在海量商品信息和有限用户注意力的背景下,如何快速吸引用户、提高用户满意度,成为电商经营者的关键竞争力。

然而,个性化推荐系统的广泛应用也引发了许多法律与伦理挑战。由于算法的复杂性、隐秘性和专业性,难以实现因果关系溯源,消费者权益在网络平台上难以得到有效保障。不当使用用户信息不仅可能侵害用户权益,还容易扰乱市场秩序,成为经营者在追求利润最大化过程中忽视社会责任的借口,甚至造成公共利益受损的法律风险[2]。其中最显著的便是数据安全与隐私保护问题。为了实现精准推荐,系统需要收集大量用户数据,包括但不限于个人浏览记录、购物记录、地理位置信息等,这些数据相当一部分是以用户“个人偏好”数据为由总涵括,但是,这些“个人偏好”数据往往和用户隐私有着密切的关系,如果相关数据被泄露将会进一步危害到用户的隐私安全。

此外,算法复杂不可见导致的偏见问题也不容忽视。由于算法本身可能存在的设计缺陷或训练数据的偏差,导致某些群体被系统性地忽视或歧视,这不仅损害了用户体验,也可能加剧社会不平等。互联网信息服务提供者不应仅以取悦用户为目标,还应承担启发民智、保障用户知情权等社会责任,履行相应的社会义务。如果个性化推荐算法从投入使用之初就存在侵害用户选择权、用户知情权,甚至危害社会公共利益的情况,应当及时接受算法监管。

1.2. 智能驱动业务流程的发展与挑战

人工智能除了对外提高电子商务经营者的销售水平,还可以对内增强电子商务经营者的自动化工作

能力。人工智能驱动的业务流程优化包括智能客服、智能供应链管理、智能财务等方面。智能化客户服务的兴起,是人工智能技术在电子商务客户服务领域的一次重大突破。基于自然语言处理(NLP)和机器学习技术,智能化客服系统能够自动识别、理解和回应客户的查询与问题[3]。人工智能的大语言模型可以很好地处理自然语言,提高了回答问题的准确性和智能化程度,采用智能化客服技术对于电子商务经营者来说不仅提高了服务效率,还降低了人力成本。在高峰时段,智能客服也能够同时处理大量查询,避免人工客服过长的等待时间并提升用户体验。此外,智能客服系统通过持续学习和优化,将不断提升服务的个性化和精准度,从而为客户提供更加定制化的解决方案。但是当智能化客服在处理敏感问题时,如账户安全、退款政策等,如何平衡自动化服务与用户隐私保护,同样考验着法律与技术的边界。

智能化供应链管理在电子商务业务链中扮演着至关重要的角色,在智能化转型的过程中,供应链管理借助人工智能技术将仓储、分拣、配送等环节逐步能够实现高度的自动化,从而显著提升物流效率并降低运营成本。例如,无人机配送与智能仓储机器人等前沿技术的应用,不仅有效缩短了配送时间,还减少了因人工操作引发的错误。然而,这些技术的广泛应用也带来了诸多法律挑战:无人机配送面临的重大问题即安全性与隐私侵犯的风险,还有智能机器人在执行任务过程中的侵权责任归属问题,以及在自动化系统发生异常时,如何有效进行应急处理等。因此,如何平衡技术创新与法律风险,确保智能化供应链管理的可持续发展也成为了电子商务智能化转型的一大痛点。

智能化财务管理能够集合发票识别、账单匹配、凭证生成等功能,完成大量重复性工作,并从历史数据中学习各部门的支出模式,并根据业务发展规划与市场趋势生成更加精细化、动态化的预算方案,这一部分涉及经营者数据区块链存储与智能生成合约问题。智能合约是一种由特定事件触发的、具备追踪能力的、获得多方认可的自动化程序,它部署在区块链网络上,能够给予预设条件自动管理和执行资产交易[4]。其智能性表现在允许计算机“阅读”合同,并自动执行各项条款。智能合约虽然具有匿名性,但是电话号码、住址、电子邮件、银行账号等可能会因为交易需要被包含在合约的执行逻辑或关联数据中[5]。如何确保这些业务数据的安全,防止数据泄露或滥用,是经营者与监管机构必须面对的难题。

2. 电子商务中人工智能应用的法律风险与规制

2.1. 隐私保护与数据安全问题

在电子商务领域,权利主体的广泛性是其显著特征,涵盖了所有参与网络购物的电商平台消费者。随着网络购物逐渐成为现代社会生活的重要组成部分,电子商务领域的市场秩序稳定性对社会的影响日益显著,大部分的个人隐私从以往的结构化数据(身份证号、出生年月、家庭住址)扩展到如今可以捕捉的非结构化数据(如声音、长相、社交媒体、留言评论、快递、购物记录)[6]。由于数据的流动性,隐私也脱离了原有的固定范围,而呈现出“液态性”的变化趋势,整合型隐私成为数字化社会隐私的主要类型[7]。此外,电子商务领域的交易具有快速完成和地域限制减少的特点,相较于传统交易方式,显著提高了交易效率。当人们的交往空间从地理空间转变为符码空间,人们的社会关系也转化为数字关系[8]。在电子商务交易中,无论买卖双方的地理位置如何,地域因素对交易的影响已被极大降低。电子商务以交易为本质,相比传统基于双方合意的交易方式,算法信任已构成了电子商务买卖双方交易信任的基础[9]。然而,由于算法可能导致的信息不对称,这一信任基础的稳固性会因为算法技术本身的缺陷而遭受攻击。综上所述,电商环境的复杂性使得对电子商务领域中准确落实隐私保护的形势更加严峻。

2017上半年电商行业就发生过一起严重的用户信息泄漏安全事件。小红书用户的个人信息遭到泄露后,接到了诈骗分子的来电。诈骗分子以退款为名,诱使受害者通过蚂蚁借呗、来分期、马上金融等多个网络借贷平台进行操作,导致用户遭受了不同程度的经济损失。¹数据泄露几乎是当下电商市场的通病,

¹ 来源于 https://www.sohu.com/a/202882466_99960664, 最后访问日期 2024 年 12 月 12 日。

而数据泄露中受害最大的是处于被动的消费者。而随着智能推荐系统、自动化客服、供应链优化、智能财务管理等技术的广泛应用,海量用户数据的收集与处理已成为常态。然而,数据的不当使用不仅威胁到个人隐私,还可能引发数据泄露、滥用以及算法偏见等一系列问题,对消费者的权益构成严重威胁。

人工智能应用在电子商务领域中引发法律风险主要来源于数据输入端、数据训练端与数据存储端。如智能推荐系统在未经用户充分知情同意的情况下进行的数据收集就可能侵犯个人隐私,违反了《电子商务法》等相关法律法规中关于数据保护的基本原则。《电子商务法》第六十九条指出电子商务经营者拥有数据权利,给我国个人信息保护与经营者数据利用双重架构提供了一定的法律空间^[10]。在当前的法律框架下,剥离掉个人信息的电子商务数据可以在没有用户同意的前提下自由流通和使用,许多电子商务经营者会通过去标识化、匿名化手段进一步处理、转化为自身电子商务数据。但是智能推荐系统的基本组成就是用户同意,并且用户基于消费者合法选择权益可以向电子商务经营者主张适用不针对其个人特征的推荐选项,电子商务经营者也有提供此类选项的法定义务。用户对电子商务经营者而言应当享有对智能推荐系统数据的在先权利,换言之如果电子商务经营者没有尽到对智能推荐系统数据的安全保障义务造成数据泄露甚至其他法律风险的,应当承担法律责任。

2.2. 算法透明度与责任归属问题

随着人工智能技术在电商行业的深度融合,算法决策的黑箱特性日益凸显,其背后的责任归属也成为亟待解决的法律难题。这种算法不公开不透明性不仅削弱了用户对决策过程的了解与信任,也增加了算法偏见、歧视等问题的隐蔽性,对消费者权益构成潜在威胁。由于算法对数据和算力的掌握,使得原有匿名化处理、知情同意等个人数据和隐私保护的措施形同虚设。《电子商务法》中的算法监管条款也主要部署了算法的事前监管,实现了事前监管和结果监管并重^[11]。

算法透明度的原则性要求就是在智能推荐、智能客服、智能供应链管理、智能财务管理等人工智能应用场景中,即使算法模型复杂、内部逻辑不明朗也有强制公开义务。法律规制应对算法透明度提出更高要求,旨在确保人工智能决策的可解释性与公正性。此外,法律还应鼓励经营者采用可解释性算法设计,即在算法设计初期即考虑其决策过程的可解释性,使用户能够理解推荐背后的原因,从而维护用户的选择权与知情权。

中国、美国和欧盟在算法透明度与责任归属问题上的法律规制也各具特色。中国强调算法的公开透明,要求经营者确保决策过程的可解释性;²美国则通过司法判例明确算法责任,将算法错误视为服务瑕疵,确定责任归属;³欧盟在 GDPR 框架下,要求算法决策提供充分说明,确保个人数据权利的保护。⁴这些国际实践为我国在算法透明度与责任归属的法律规制上提供了有益借鉴,强调了透明度、公正性与责任明确的综合考量。

2.3. 智能合约的法律效力问题

智能驱动业务的基本流程就是自动化实施民事行为(在系统中可以表现为执行确定性业务程序)并可以自动履约产生合法有效的法律效力,其背后最大的人工智能技术支持就是智能合约系统。人工智能主导的自动化决策具有以下特点:第一,系统是决策主体;第二,在确定性业务规则的前提下,系统会自动进行重复性决策;第三,系统能够进行深度学习^[12]。智能合约系统既可以支持内部的数据预测与调整,

²《电子商务法》第十八条和第三十三条、《个人信息保护法》第二十四条第一款和第三款、《关于加强互联网信息服务算法综合治理的指导意见》的基本原则和《互联网信息服务算法推荐管理规定》第十二条、第十六条和第二十四条均有体现。

³Lohr v. Federal Communications Commission (1993)、Seibel v. BHI, Inc. (2001)、Zamora v. Uber Technologies Inc. (2019)、FTC v. Uber Technologies (2021)等案件均有体现。

⁴GDPR 第 5 条数据处理的原则、第 13 条和第 14 条透明度要求,第 15 条数据主体的访问权和第 22 条自动化决策要求均有体现。

例如资金管理、供应链管理，也可以支持外部的数据交易，例如互联网保险产品等完全线上投保线上理赔。

智能合约自动执行条款采用的是“if A then B”的计算机程序运行规则，即在满足条件 A 的情况下，自动执行行为 B。这类自动执行条款实质上是一种义务负担行为，尤其是在删除了“if then”这一代码逻辑时，自动执行条款就变成合约双方需要承担 A 与 B 对应的行为义务，这也解释了智能合约为何能够应用于众多场景[13]。在最理想的状态下合同双方都实现了必要且充分的 A 和 B 对应的行为义务，基于智能合约可以及时生效及时执行，合约的履约将在瞬间完成，不存在迟延履行或事实不能履行等特殊情形。但是正是由于其及时生效及时执行的特性，执行程序难以终止，财产转移程序不可逆转。智能合约一旦生效，即构成对合约各方权利义务的固定化，从而限制了当事人之间就合同条款进行后续协商的可能性。此种机制不仅剥夺了合同当事人依法享有的撤销权、变更权及解除权等基本权利，而且对合同自由原则构成了实质性限制。

3. 构建电子商务领域人工智能应用的法律框架

3.1. 明确人工智能应用的法律地位

在国际上，一些国家和地区已经开始尝试为人工智能赋予法律主体地位，以便明确责任归属，保护消费者权益。例如欧盟的《欧盟机器人民事法律规则》立法建议⁵和俄罗斯的“格里申法案”⁶，都是尝试在法律上确立人工智能的特殊地位，以应对由此产生的法律挑战。

在电子商务领域，确立人工智能法律主体地位的关键问题在于人工智能主体的权利与义务的界定。

在权利方面，人工智能系统在执行其功能时，可能会产生某种形式的价值，这可能涉及知识产权，如创新的算法、生成的内容等。因此，法律应当考虑赋予人工智能在一定范围内享有知识产权或同等含义的财产性利益，无论是作为独立的创作者，还是作为人类开发者或所有者的延伸。此外，人工智能可能会在执行过程中生成某些创新成果，例如内容创作或算法优化，法律应为其提供一定的知识产权保护，以激励技术创新。同时，为了保护人工智能的“安全”和“健康”，法律可能需要赋予其某些保护性权利。例如，防止不当的修改、复制或滥用，以及确保其算法的持续更新和维护，以保持人工智能技术的先进性和竞争优势。这些权利的设定，将有助于人工智能在一定程度上“自己创造价值”并“保护自己的价值”，同时也确认了其价值贡献。

在义务方面，人工智能主体应当承担与其功能和影响力相匹配的义务。例如创设透明度义务，要求人工智能系统在执行决策时，能够提供可理解的解释，以确保消费者能理解其推荐、决策或服务的依据。此外，人工智能还应履行数据保护义务，确保在处理个人数据时遵守相关法律法规，尊重数据主体的隐私权，并在出现数据泄露或滥用时，承担相应的责任。为此，法律应当确保人工智能系统在数据使用过程中具备可解释性，以便在出现问题时，能够明确追溯责任。

3.2. 制定人工智能应用的准入标准

在目前阶段，人工智能应用在某些特定领域实施市场准入制度，未来的政策还需关注人工智能技术在设计阶段的法律嵌入，要求设计研发者在研发过程中充分考虑法律价值，确保技术设计与应用符合法律与伦理标准，预防潜在的法律风险。

这包括在技术设计阶段就考虑隐私保护、数据安全和算法公正性等法律要求，确保开发者在设计时

⁵ 来源于 <https://op.europa.eu/en/publication-detail/-/publication/19ea0f1c-9ab0-11e6-868c-01aa75ed71a>，最后访问日期 2024 年 12 月 12 日。

⁶ 来源于 http://robopravo.ru/proiekty_aktov 和 <https://vk.com/robolaw>，最后访问日期 2024 年 12 月 12 日。

就已经考虑了技术可能带来的法律后果，并进行相应的风险评估和合规性审查。例如，在人工智能技术的研发过程中，应当加入数据保护、隐私权保护和伦理审查等环节，确保这些问题得到充分考虑和解决，防止技术发展后造成的法律困境或社会问题。

为了完善电商平台的主体责任制度，政策建议应明确相关主体的法律义务和责任，尤其在数据安全和个人信息保护方面。同时，立法应聚焦技术研发，提高智能技术的安全性和可靠性，不断厘清人工智能的准入范围，明确人工智能算法运行的界限，确保技术合理运用，维护市场公平竞争，保障消费者权益。

3.3. 确立数据隐私和安全保护规则

为了应对算法黑箱、数据安全、算法偏见等问题，政策建议应侧重于算法的透明度和公平性，通过立法明确算法信息披露义务，保障消费者的知情权和选择权。例如，应要求平台和开发者在算法决策过程中清楚地披露算法的决策逻辑、使用的数据类型以及可能产生的影响，确保消费者能够理性选择是否接受相关服务。

同时，建立算法审核和监督机制，定期评估算法的公正性和安全性，确保算法决策不受偏见影响，保护消费者免受算法歧视。此外，应强化数据保护法规，明确数据收集、存储、使用的原则与边界，保障个人数据权利，防止数据滥用。此外，应推动与国际数据保护标准的对接，如 GDPR，进一步明确数据在跨境流动过程中的法律要求与安全防护措施。

在电子商务中，当算法决策导致消费者权益受损时，责任归属问题变得尤为复杂。算法错误、偏见或数据泄露等事件，可能源自算法设计、数据处理或系统维护等不同环节，涉及开发者、平台运营商、数据处理者乃至用户自身。确定责任主体，不仅需要技术层面的深入分析，更涉及法律的责任分配原则，应考虑过错原则、合同义务和产品责任等方面的具体规定。

法律规制应通过立法明确算法责任归属，建立合理责任分配机制。例如，在智能客服与自动化物流中，若系统错误导致服务失误或财产损失，应根据过错原则，综合考虑系统设计、数据处理、用户行为等多方面因素，确定责任主体。同时，法律还应要求经营者建立有效的内部监管与外部审查机制，定期评估算法系统的安全性和合规性，以确保技术应用符合法律与伦理标准。

3.4. 加强人工智能应用的监管机制

面对算法透明度与责任归属的法律挑战，未来的法律规制需更加灵活与前瞻。一方面，应明确设计者在研发阶段的法律嵌入义务，确保算法设计与应用符合法律价值与伦理标准。研发者应当在设计之初就考虑到法律、伦理以及社会影响的多维要求，确保技术的合法性、透明性、公正性和可解释性。例如，研发过程中可以采用法务顾问参与审查、伦理委员会进行评估等方式，确保技术设计符合数据保护法、消费者权益保护法以及其他相关法律要求。另一方面，需关注算法公正性与责任分配，通过立法强化算法的透明度，建立算法责任的明确规则，同时鼓励经营者采取技术措施确保数据安全，建立数据泄露的及时报告与应对机制，以维护消费者权益，推动电子商务行业的健康、有序、可持续发展。

监管机构还应当加强对人工智能系统的日常审查与动态监控，建立灵活且有效的合规框架。由于技术进步的快速性，现有法律框架可能面临滞后性，因此，立法机构应定期评估和修订相关法律，以适应新兴技术的发展。例如，可以通过设立专门的监管机构，负责监督人工智能的应用和发展，确保技术在实际应用中不偏离法律和伦理的要求。

此外，针对算法透明度的强化不仅仅是披露算法的基本逻辑，还应包括对算法决策影响的全面审查。例如，平台和企业应当提供算法决策的可解释性，明确告知消费者如何收集、使用数据，及其对决策结

果的影响。这可以通过“算法说明书”或“透明报告”的形式呈现，使消费者能够理解决策的背景和依据，增强消费者对人工智能技术的信任。

4. 结论

人工智能技术以其深度学习算法为原理，实现海量数据集的深度学习、统计编程和预测分析，在智能化工具、服务、采销、仓储等方面推动电子商务领域的创新。然而，这一技术的应用也带来了隐私保护、数据安全和算法透明度等法律挑战。为了应对这些挑战，需要构建一个全面的法律框架，明确人工智能的法律地位，制定市场准入标准，确立数据隐私和安全保护规则，并加强监管机制。这一框架对于保护消费者权益、维护市场公平竞争以及促进电子商务的健康可持续发展至关重要。未来，需求导向的智能决策、全链条系统优化、B2B 企业级应用等领域将成为人工智能在电子商务中的重要发展方向，然而现有法律体系的滞后性、国际规制的不一致性以及技术与法律的脱节，提示我们需在全球层面加强合作，以确保人工智能技术的发展既能促进商业创新，又能保护个人隐私，确保数据安全，并在透明度和责任归属方面取得平衡，实现技术进步与法律规制的和谐统一。

参考文献

- [1] 王伟. 人工智能在电子商务个性化推荐系统中的应用与优化[J]. 高科技与产业化, 2024, 30(9): 60-61.
- [2] 王娅. 个性化推荐服务的法律风险及其规制进路[J]. 北方论丛, 2024(6): 73-82.
- [3] 谢永江, 杨永兴, 刘涛. 个性化推荐算法的法律风险规制[J]. 北京科技大学学报(社会科学版), 2024, 40(1): 77-85.
- [4] 陈颢. 关于区块链智能合约的合同属性问题[J]. 山东社会科学, 2023(5): 91-99.
- [5] 赵丽君. 智能合约的应用风险及法律规制[J]. 理论观察, 2024(11): 139-143.
- [6] 张媛媛, 邹静. “技术-隐私”视域下数字社会隐私保护的路径创新[J]. 社会科学研究, 2022(6): 25-34.
- [7] 顾理平. 数字化时代隐私内涵的演进嬗变与研究的前沿问题[J]. 新闻与写作, 2022(1): 4-13.
- [8] 代砚春, 孙美玲. 数字异化的生成及消解路径[J]. 长白学刊, 2022(3): 59-67.
- [9] 袁康. 可信算法的法律规制[J]. 东方法学, 2021(3): 5-21.
- [10] 袁泉. 电子商务法视野下的个人信息保护[J]. 人民司法, 2019(1): 13-16, 20.
- [11] 张凌寒. 《电子商务法》中的算法责任及其完善[J]. 北京航空航天大学学报(社会科学版), 2018, 31(6): 16-21.
- [12] 荆宝森, 李小春, 张瑞. 基于价值创造的智能人机协同[J]. 财务与会计, 2022(9): 10-14.
- [13] 许中缘, 郑煌杰. 智能合约的治理逻辑: 法律性质、风险类型、化解路径[J]. 学术交流, 2024(2): 67-79.