E-Commerce Letters 电子商务评论, 2026, 15(2), 261-268
Published Online February 2026 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2026.152154

Hans汉斯

人工智能驱动电商个性化推荐系统的优化路径

——基于用户隐私保护视角

马雪霏

上海理工大学管理学院，上海

收稿日期：2026年1月12日；录用日期：2026年1月23日；发布日期：2026年2月9日

摘　要

随着人工智能技术的快速发展，个性化推荐系统已成为电商平台提升用户体验和商业转化效率的重要技术手段。然而，推荐系统在高度依赖用户数据的同时，也加剧了用户隐私泄露风险，引发了数据滥用、算法歧视和信息不对称等一系列问题。在数据保护法律法规日益完善和公众隐私意识不断增强的背景下，个性化推荐效果与用户隐私保护之间的张力愈发凸显，如何在隐私约束条件下实现推荐系统的持续优化，成为电商平台和学界共同关注的重要议题。本文从用户隐私保护视角出发，系统探讨人工智能驱动电商个性化推荐系统的优化路径。

关键词

人工智能，个性化推荐系统，用户隐私保护，电商平台

Optimization Paths for AI-Driven Personalized Recommendation Systems in E-Commerce

—From the Perspective of User Privacy Protection

Xuefei Ma

School of Management, University of Shanghai for Science and Technology, Shanghai

Received: January 12, 2026; accepted: January 23, 2026; published: February 9, 2026

Abstract

With the rapid development of artificial intelligence technology, personalized recommendation

文章引用: 马雪霏. 人工智能驱动电商个性化推荐系统的优化路径[J]. 电子商务评论, 2026, 15(2): 261-268.
DOI: 10.12677/ecl.2026.152154

systems have become an important technical means for e-commerce platforms to enhance user experience and improve commercial conversion efficiency. However, while relying heavily on user data, these systems have also exacerbated the risks of user privacy leakage, giving rise to a series of issues such as data abuse, algorithmic discrimination, and information asymmetry. Against the backdrop of the increasing improvement of data protection laws and regulations and the growing public awareness of privacy, the tension between the effectiveness of personalized recommendations and user privacy protection has become increasingly prominent. How to achieve the continuous optimization of recommendation systems under privacy constraints has emerged as a key research topic of common concern to both e-commerce platforms and academic circles. From the perspective of user privacy protection, this paper systematically explores the optimization paths of artificial intelligence-driven personalized recommendation systems in e-commerce.

Keywords

Artificial Intelligence, Personalized Recommendation System, User Privacy Protection, E-Commerce Platform

1. 引言

随着人工智能、大数据与算法技术的迅速发展，个性化推荐系统已成为电商平台提升用户体验、增强用户黏性和实现商业价值转化的核心技术工具。通过对用户行为数据、偏好特征和消费历史的深度挖掘，推荐系统能够实现“千人千面”的精准推送，在显著提高交易效率的同时，也深刻重塑了数字经济时代的消费模式。然而，在推荐系统不断强化个性化能力的过程中，用户隐私被持续采集、分析和再利用，由此引发的数据滥用、隐私泄露和算法不透明等问题日益凸显，逐渐成为制约电商平台可持续发展的关键风险因素。一方面，个性化推荐高度依赖大规模、细粒度的用户数据，算法性能的提升往往伴随着对用户隐私的深度介入；另一方面，随着数据保护法律法规的不断完善以及公众隐私意识的显著增强，电商平台在数据收集、处理和使用方面面临更为严格的合规约束与社会监督。在此背景下，如何在保障用户隐私权益的前提下，持续优化人工智能驱动的个性化推荐系统，已不再是单纯的技术问题，而是涉及技术选择、制度设计与平台治理的综合性议题。推荐效果与隐私保护之间是否必然存在“此消彼长”的关系，抑或可以通过系统性优化实现协同共进，成为亟需深入探讨的重要研究问题。

基于上述现实背景，本文以用户隐私保护为核心分析视角，系统探讨人工智能驱动电商个性化推荐系统的优化路径，旨在回应“如何在隐私约束下实现推荐系统高效运行”的关键问题。本文不仅关注联邦学习、差分隐私、可解释人工智能等新兴技术在隐私保护中的应用潜力，也进一步从制度与治理层面分析数据最小化原则、用户知情同意机制以及算法透明与责任机制对推荐系统优化的支撑作用。通过将技术路径与治理路径纳入统一分析框架，本文力图突破既有研究中技术导向或制度导向单一视角的局限。

在结构安排上，本文首先回顾国内外关于个性化推荐系统与用户隐私保护的相关研究，梳理主要理论框架与研究不足；其次介绍研究设计与分析方法；随后从技术、制度与用户参与等维度，对隐私保护视角下电商推荐系统的优化路径进行系统分析；最后总结研究结论，提出对电商平台实践与未来研究的启示。

2. 国内外研究现状和文献述评

与传统的基于内容过滤的直接分析内容进行推荐不同，协同过滤分析用户的兴趣，在用户群中找出与目标用户相似的用户，综合这些相似用户对不同项目的评分，产生目标用户对这些项目喜好程度的预测，从而产生推荐[1]。推荐系统(RSs)是为帮助用户在互联网上找到他们感兴趣的物品而开发的工具[2]。事实证明，推荐系统通过向用户提供高质量、个性化的物品建议，在缓解互联网上普遍存在的信息过载问题方面发挥了强大作用[3]。推荐算法的历史可以追溯到 1992 年，施乐公司提出了一种基于协同过滤的推荐算法[4]，这种算法最初被应用于垃圾邮件的过滤，并取得了显著成效。推荐算法通过分析用户的历史偏好数据、个人兴趣以及社交网络信息等，从海量的商品或服务中筛选出用户可能感兴趣的内容进行展示。其设计理念在于深入分析和理解用户的消费习惯、个人特征以及社交圈的数据，以此来构建用户的画像，并推送满足用户个性化需求的内容[5]。当涉及到用户必须泄露私人信息这一点时，隐私和安全问题变得非常严峻[6]，因为推荐系统可能会滥用用户提供的信息，将其泄露给第三方以获取经济利益；攻击者可能会利用推荐系统中的安全漏洞，这可能导致所提供信息的潜在被盗[7]，而且恶意用户可能会破坏生成给其他用户的推荐[8]。提出了在联邦推荐中引入双重个性化机制的框架，以更好地在用户与物品层面学习个性化特征，同时保持隐私安全[9]。尽管联邦学习保护原始数据，但其参数更新仍可能泄露隐私信息，需引入如差分隐私等辅助机制。将差分隐私机制与联邦推荐框架整合，证明在最小损害推荐准确度的前提下可显著提高用户隐私保护[10]。从技术中立的角度来看，算法推荐技术是否符合传统平台责任规则中关于技术中立的基本预设，直接关系到其是否需要承担侵权责任，也会影响到平台责任规则的适用。从公共领域保留的角度来看，法律层面关于算法推荐的规制，需要遵循利益平衡原则，在加强网络环境下著作权保护的同时，也应当为社会公众以及平台产业的发展留有充足的空间，从而更好地维护社会公共利益[11]。互联网平台在收集、索取用户个人信息时，用户个人信息的知情同意规则和算法推荐服务提供者的算法告知义务逐渐流于形式[12]。网络平台往往通过网络协议、隐私政策等方式，取得处理用户个人信息的权限，但用户不能对这些条款提出修改和变更意见，而只能概括地表示接受或不接受[13]。

综上所述，人工智能驱动的个性化推荐系统在提升用户体验和商业价值方面取得了巨大成功，同时也带来了深刻的隐私保护挑战。从最初的数据扰动与加密方案到联邦学习与差分隐私等先进技术的引入，再到系统性风险分析与伦理关注，该领域正在形成一个既关注技术优化、也重视用户主体权利与合规治理的综合研究生态。近期系统综述的发布和机器遗忘等技术创新，为构建“隐私保护与推荐效率共存”的推荐系统提供了新的研究方向与思路。即使联邦学习被视为隐私保护的突破，但模型更新本身可能泄露信息，是否需要结合更深层次的安全机制仍有不同观点；技术隐私保护机制能否转化为用户可理解、可控的隐私体验，是从技术可行性向用户信任构建的重要问题，涉及伦理、使用行为与法律规制的多方讨论。

3. 人工智能驱动电商个性化推荐系统面临的主要挑战(隐私保护视角)

3.1. 算法黑箱特性导致隐私风险难以识别与追责

在人工智能驱动的电商个性化推荐系统中，算法黑箱特性已成为引发用户隐私风险的重要结构性因素。算法黑箱原指人工智能系统中输入与输出之间的隐层机制，难以被外界观察和理解，导致决策过程缺乏透明性，可能引发数据不可控、结果与事实相悖等问题，并形成信息泄露、劳动控制、就业歧视等风险[14]。所谓“算法黑箱”，是指推荐算法在数据输入、特征处理、模型训练和决策输出等关键环节中，其运行逻辑高度复杂且不透明，外部主体(包括用户、监管机构乃至部分平台管理者)难以准确理解和解释

算法如何基于用户数据生成推荐结果。在深度学习等复杂模型被广泛应用的背景下，算法黑箱问题尤为突出。首先，算法黑箱特性加剧了用户隐私风险的隐蔽性。在电商推荐系统中，用户数据往往经历多轮清洗、特征提取和模型训练，其使用方式不再直观可见。即便平台在形式上遵循了隐私政策和用户授权程序，算法仍可能通过对多源数据的关联分析，推断出用户未明确披露的敏感信息，如消费能力、生活方式甚至潜在偏好。这类隐私风险并非源于单一数据滥用行为，而是嵌入在算法运行逻辑之中，具有高度的隐蔽性和累积性，使得风险难以及时识别。大数据差异化定价此类问题聚焦电商、出行平台。一是动态价格歧视，通过对用户行为画像，精准实施浏览频次定价、跨设备差异化定价等隐蔽策略。二是优惠机制黑箱，未公示差异化优惠规则，优惠券发放逻辑及失效原因缺乏透明解释[15]。其次，算法黑箱削弱了用户对自身隐私状况的感知与判断能力。由于推荐逻辑不透明，用户通常只能看到推荐结果，而无法了解这些结果背后的数据来源和推断过程。当个性化推荐不断“精准命中”用户需求时，用户往往难以区分这是合理的数据利用，还是对个人隐私的过度挖掘。这种信息不对称使用户在事实上处于被动地位，难以对平台的数据使用行为作出有效监督，也难以通过自主选择来规避潜在隐私风险。最后，算法黑箱特性显著增加了隐私侵权责任认定和追责的难度。在推荐系统运行过程中，隐私风险可能源于模型设计缺陷、数据处理规则不当，或算法特定情境下产生的非预期推断结果。然而，由于算法决策路径不可解释，外部主体难以证明隐私侵害是由何种具体算法机制或数据处理行为所导致。这不仅给用户维权带来障碍，也使监管机构在开展算法审计和责任认定时面临技术和证据层面的双重挑战，从而削弱了隐私保护制度的实际执行力。《网络信息内容生态治理规定》的第十条、第十一条和第十二条对推荐算法的应用与管理提出了明确要求，强调需建立人工干预与用户自主选择相结合的算法推荐机制[16]。《网络安全法》明确规定，平台必须采取有效的技术措施保障数据安全，防止用户数据的泄露和滥用[17]。

3.2. 隐私保护技术与推荐性能之间的权衡难题

在人工智能驱动的电商个性化推荐系统中，隐私保护技术的引入为缓解用户数据泄露风险提供了重要工具，但同时也带来了推荐性能与系统效率方面的现实挑战。当前普遍面临的一个核心问题就是隐私保护是否必然以牺牲推荐性能为代价，以及这种“性能损失”在多大程度上是不可避免的。从技术机理上看，个性化推荐系统的性能高度依赖于高质量、细粒度和连续性的用户数据输入。推荐模型通过学习用户行为模式和偏好特征，不断优化预测精度。然而，多数隐私保护技术的基本思路在于减少数据可用性或降低数据精确度，例如通过限制数据收集范围、分散数据存储或对数据和模型参数进行扰动。这种对数据完整性和准确性的干预，客观上削弱了模型学习用户真实偏好的能力，从而可能导致推荐准确率、覆盖率或实时性下降。在商业场景中，各类企业正通过采集用户的浏览轨迹、消费记录及交易模式等数据，运用行为分析技术构建用户画像，并实施精准化的定向营销[18]。企业通过收集用户行为数据构建精细化画像，但算法决策往往嵌入社会固有偏见，导致系统性歧视，制造或者加剧社会不平等[19]。亚马逊被曝其招聘算法对女性求职者降权评分，因其训练数据源自男性主导的科技行业历史招聘记录[20]。此类“算法偏见”不仅侵犯个人平等权，更将现实社会的不公移植至数字空间。基于用户数据实施差异化定价已成为行业潜规则。若企业将大数据技术异化为操控工具，假借“个性化服务”之名实施心理干预或非自愿引导，此类技术滥用不仅会导致负面影响的持续叠加，还可能引发系统性风险，侵蚀个体的生活自主权与人格发展空间[21]。以差分隐私为例，该技术通过在数据或模型更新过程中引入随机噪声，从理论上保证单个用户信息难以被识别。尽管差分隐私在隐私保护层面具有严格的数学保障，但噪声的引入不可避免地影响模型参数的精度。当隐私保护强度提高时，噪声水平随之增加，推荐结果的稳定性和精准度往往受到明显影响。这种“隐私预算”与推荐性能之间的此消彼长关系，使差分隐私在实际电商推荐场景中的应用面临取舍难题。联邦学习作为另一种重要的隐私保护技术，通过“数据不出本地”的方

式避免集中存储用户数据，在理论上降低了隐私泄露风险。然而，在实际运行中，联邦学习推荐系统需要在分布式环境下进行多轮参数通信，不仅增加了系统的计算和通信成本，还可能因用户设备异构、数据分布不均等问题，影响模型的收敛速度和最终性能。此外，联邦学习本身并不能完全消除隐私风险，往往需要与差分隐私等技术结合使用，而多种隐私机制叠加可能进一步放大性能损失。在现实应用层面，这种权衡问题对电商平台形成了显著制约。一方面，平台需要通过高质量推荐维持用户活跃度和商业收益；另一方面，过度强化隐私保护可能导致推荐体验下降，进而影响用户满意度和平台竞争力。这使得部分平台在实践中倾向于采取“最低合规”策略，即在满足基本法律要求的前提下，尽量减少对推荐系统性能的影响，从而削弱隐私保护技术的实际效果。

3.3. 用户隐私认知不足与参与度有限

在人工智能驱动的电商个性化推荐系统中，用户不仅是数据的提供者和推荐服务的接受者，也是隐私保护实践中不可或缺的主体。然而，在现实运行中，用户对自身隐私权益的认知普遍不足，参与隐私治理和算法调节的意愿与能力有限，这在一定程度上削弱了隐私保护机制的实际效果，并加剧了推荐系统运行中的结构性风险。从问题表现来看，尽管电商平台普遍通过隐私政策、用户协议和弹窗提示等方式告知数据收集与使用规则，但相关信息往往以专业术语呈现，内容冗长且结构复杂，普通用户难以充分理解算法推荐背后的数据逻辑与潜在风险。多数用户在使用平台服务时，往往出于便利性考虑直接“默认同意”隐私条款，而未能形成对个人数据使用范围、算法决策机制及其可能后果的清晰认知。这种“形式合规而实质不知情”的现象，使用户在隐私保护问题上处于被动地位。从成因分析看，用户隐私认知不足既源于信息不对称，也与个性化推荐系统的技术复杂性密切相关。推荐算法通常具有高度抽象和自动化特征，其决策过程难以通过直观方式向用户解释，进一步放大了用户对算法运行机制的理解障碍。同时，平台在商业竞争压力下，往往更强调推荐效率和用户黏性，而对隐私教育和用户赋权投入不足，导致用户缺乏参与隐私管理的有效工具和激励机制。在参与度层面，即便部分平台为用户提供了隐私设置、个性化推荐调节或数据管理选项，用户的实际使用率仍然偏低。一方面，隐私管理操作往往分散在多个界面之中，增加了用户的操作成本；另一方面，用户普遍担心关闭数据授权或限制推荐功能会显著降低使用体验，从而形成“隐私–便利”之间的心理权衡。这种理性选择倾向使用户在现实中更倾向于放弃主动参与隐私保护。用户隐私认知不足与参与度有限还对推荐系统的整体治理效果产生连锁影响。一方面，缺乏用户反馈和参与，使平台难以及时识别隐私风险和算法偏差，增加了系统性隐患；另一方面，用户在隐私保护中的弱势地位，可能削弱其对平台和算法推荐结果的信任感。一旦隐私事件发生，用户往往表现出强烈的不信任甚至抵触情绪，进而影响平台声誉与长期发展。在理论讨论中，部分研究将这一问题归因于“技术中心主义”导向，即推荐系统设计过度依赖算法自动决策，而忽视用户作为价值主体的角色。相较之下，以“以用户为中心”的隐私保护理念强调，应通过提高算法透明度、简化隐私管理工具和增强用户知情权与选择权，提升用户参与隐私治理的可能性。这一视角认为，用户隐私认知的提升并非阻碍推荐系统效率，而是构建可持续信任关系的重要前提。

4. 人工智能驱动电商个性化推荐系统的优化路径

4.1. 技术层面——构建隐私友好的推荐系统

在人工智能驱动的电商个性化推荐系统中，隐私保护与推荐性能之间存在天然的张力。为了在保障用户隐私的前提下实现高效推荐，技术层面的优化路径成为平台实践的重要方向。通过构建隐私友好的推荐系统，可以在最大程度上降低用户数据泄露风险，同时保持推荐算法的精准性与响应效率。首先，引入隐私计算技术是技术优化的核心手段之一。

联邦学习(Federated Learning)通过在用户终端本地完成模型训练，仅上传模型参数更新而非原始数据，实现了“数据不出本地”的数据处理模式。这种方式在一定程度上避免了集中式数据存储带来的泄露风险，同时允许系统在多源数据下进行全局模型优化。与传统集中式训练相比，联邦学习能够在不暴露用户原始行为数据的情况下，持续改进推荐算法的预测精度。

差分隐私(Differential Privacy)技术为推荐系统提供了可量化的隐私保护保障。通过在数据输入、模型梯度或输出结果中引入噪声，差分隐私可以在数学上控制单个用户信息被识别的可能性。在推荐系统中，差分隐私不仅能有效降低用户敏感信息暴露的风险，还能够通过调整噪声强度，实现“隐私预算”的灵活分配，从而在一定程度上平衡推荐性能与隐私保护之间的矛盾。

可解释人工智能(Explainable AI, XAI)的应用有助于提升算法透明度与用户信任度。推荐系统通过提供可理解的推荐理由或特征贡献说明，使用户能够洞察其数据在模型决策中的作用。这不仅增强了用户对平台数据使用的感知和控制能力，也降低了算法黑箱带来的潜在隐私风险，有助于平台构建可审计、可追责的推荐机制。此外，多技术协同是构建隐私友好推荐系统的重要策略。例如，将联邦学习与差分隐私结合，可在保证数据不集中存储的基础上引入额外的数字隐私保障；同时，引入可解释性模型，可使技术与用户层面的信任机制相互支撑，从而在推荐系统的整体设计中形成多层次的隐私防护体系。

4.2. 制度与治理层面——完善算法与数据治理机制

在人工智能驱动的电商个性化推荐系统中，单靠技术手段难以彻底解决隐私保护问题。隐私风险不仅涉及数据收集与处理，还包括算法设计、运行决策和责任追溯。因此，从制度和治理层面完善算法与数据管理机制，是构建隐私友好型推荐系统的重要路径之一。

首先，落实数据最小化与用途限制原则是制度优化的核心要求。电商平台应明确推荐系统所需的数据类型、收集频率及存储时长，严格限定数据使用范围，避免过度采集和长期滞留用户敏感信息。这不仅符合数据保护法律法规(如 GDPR、CCPA 等)对数据最小化的要求，也能从制度上降低潜在隐私风险，为技术保护提供基础保障。

其次，建立算法审计与责任追溯机制是实现可控推荐的关键。制度设计应要求平台对推荐算法的输入、输出及决策逻辑进行定期审计，重点检查数据使用合规性、模型偏差、歧视风险以及潜在的隐私泄露隐患。通过建立审计报告和责任追溯体系，可以在隐私事件发生时明确平台或算法开发者的主体责任，为监管机构提供技术与证据支持。这种机制不仅提升了透明度，也为用户维权提供了制度依据。

第三，强化用户知情同意与自主选择权。在推荐系统运行过程中，应通过简明易懂的隐私政策、交互式授权界面和灵活的设置选项，让用户明确了解其数据的收集、使用方式以及可能的推荐效果。同时，赋予用户控制权，例如允许用户选择参与数据收集的程度、调整推荐偏好或推出个性化推荐服务，这有助于增强用户参与感和信任感。

最后，制度与治理优化还应关注跨部门与行业协同。电商平台、监管机构、第三方评估机构和行业协会应形成协同机制，共同制定算法安全与数据保护标准。通过标准化规范和跨平台评估，可以减少各平台在隐私保护上的信息不对称，推动整个行业形成良性竞争与可持续发展环境。

4.3. 用户层面——增强用户参与与信任构建

在人工智能驱动的电商个性化推荐系统中，用户不仅是数据的提供者，也是推荐系统价值实现和隐私治理的核心主体。然而，研究显示，用户在隐私认知和参与度方面普遍不足，这直接影响推荐系统的隐私保护效果和平台的信任建设。因此，从用户层面提升参与和信任，是构建隐私友好型推荐系统的重要优化路径。

首先，提供灵活的隐私偏好与推荐控制功能是增强用户参与的关键措施。平台应允许用户对数据收集类型、数据使用范围及个性化推荐强度进行自主设置。例如，用户可以选择仅使用部分历史行为数据进行推荐，或调整推荐算法的个性化程度。这种“可调节性”既保障了用户对自身数据的控制权，也在不显著削弱推荐效果的前提下，实现了用户自主参与与隐私保护的平衡。

其次，提升隐私风险提示与用户教育是增强信任的必要手段。平台可以通过交互式界面、可视化图表或简明易懂的提示信息，让用户了解推荐算法的运行逻辑、数据使用方式以及潜在风险。通过教育和信息透明化，用户能够理解平台数据处理的规则，并对自身数据的使用结果形成理性判断。这不仅增强了用户对平台的信任，也促使用户在隐私管理上采取主动行为，从而形成良性循环。

最后，构建用户反馈与参与机制可以进一步强化系统的可持续优化能力。平台可以建立隐私意见收集渠道、推荐结果评价系统以及数据使用问卷等，让用户直接参与到算法优化和隐私治理中。通过这种参与，用户不仅感知到自身的控制权，还能为平台提供行为数据以改进推荐算法，形成“信任–参与–优化”的闭环。此外，用户参与与信任构建还需与技术与制度路径相互配合。可解释算法、透明数据处理流程以及完善的隐私政策，为用户提供清晰的信息支撑，使其在参与过程中有明确依据；制度化的责任追溯与审计机制，则为用户信任提供保障，使其相信平台在数据使用上的行为是可监督、可问责的。

5. 结论与展望

综上所述，本文通过系统分析人工智能驱动的电商个性化推荐系统在隐私保护视角下的优化路径，为理论研究提供了框架参考，为实践应用提供了可操作的方案，同时为未来研究指明了可深化的方向。通过技术、制度和用户三维协同推进，电商个性化推荐系统有望在保护用户隐私的前提下，实现高效、透明和可信的可持续发展。未来研究应以理论创新、实证验证和用户体验优化相结合为目标，不断完善电商个性化推荐系统在隐私保护条件下的可持续发展路径，为平台运营、政策制定及用户体验提升提供更有力的支持。

参考文献

[1] 吴颜, 沈洁, 顾天竺, 等. 协同过滤推荐系统中数据稀疏问题的解决[J]. 计算机应用研究, 2007, 24(6): 94-97.

[2] Ricci, F., Rokach, L. and Shapira, B. (2021) Recommender Systems: Techniques, Applications, and Challenges. In: Ricci, F., Rokach, L. and Shapira, B. Eds., *Recommender Systems Handbook*, Springer, 1-35. https://doi.org/10.1007/978-1-0716-2197-4_1

[3] Bobadilla, J., Alonso, S. and Hernando, A. (2020) Deep Learning Architecture for Collaborative Filtering Recommender Systems. *Applied Sciences*, **10**, Article 2441. https://doi.org/10.3390/app10072441

[4] 李君, 倪晓军. 融合注意力机制的知识图谱推荐模型[J]. 软件导刊, 2023, 22(3): 118-124.

[5] 苏争, 殷悦. 楚天都市报极目新闻视频号运营策略[J]. 中国记者, 2022(6): 112-117.

[6] Nguyen, T.T., Quoc Viet hung, N., Nguyen, T.T., Huynh, T.T., Nguyen, T.T., Weidlich, M., *et al.* (2024) Manipulating Recommender Systems: A Survey of Poisoning Attacks and Countermeasures. *ACM Computing Surveys*, **57**, 1-39. https://doi.org/10.1145/3677328

[7] Wang, J. (2018) Privacy-Preserving Recommender Systems Facilitated by the Machine Learning Approach. Ph.D. Thesis, University of Luxembourg.

[8] Kotb, H.M., Gaber, T., AlJanah, S., Zawbaa, H.M. and Alkhathami, M. (2025) A Novel Deep Synthesis-Based Insider Intrusion Detection (DS-IID) Model for Malicious Insiders and AI-Generated Threats. *Scientific Reports*, **15**, Article No. 207. https://doi.org/10.1038/s41598-024-84673-w

[9] Agarwal, U. and Gupta, A. (2025) Federated Learning Infrastructure for Privacy-Preserving Personalized Shopping in E-commerce. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, **6**, 59-64. https://doi.org/10.63282/3050-9262.ijaidsml-v6i4p108

[10] 徐子行, 楚兆伟, 世阳松. 一个有效的联邦建议框架, 实现差异化隐私[J]. 电子学, 2024, 13(8): 1589.

[11] 冯晓青. 网络平台算法推荐著作权侵权认定及其规制[J]. 政法论丛, 2025(5): 60-76.

[12] 孙雪玲, 王黎黎. 算法推荐对用户权益的侵害与保护路径探究[J]. 互联网天地, 2023(4): 20-27.

[13] 张惠彬, 仲思睿. 数字经济时代算法推荐技术的应用风险与规范进路[J]. 杭州师范大学学报(社会科学版), 2022, 44(5): 122-130.

[14] 袁曾. 算法黑箱的治理迷思与破解[J]. 中国海商法研究, 2025, 36(4): 22-31.

[15] 刘卓月, 张亚飞, 王志伟. 互联网信息服务算法治理: 从专项行动迈向常态化长效化治理[J]. 中国信息安全, 2025(12): 53-57+62.

[16] 木巴拉克·马合木提. 智能推荐算法的法律规制分析——以电商平台引入 AI 为例[J]. 中国价格监管与反垄断, 2025(9): 115-117.

[17] 亓蕾. 算法推荐法律规制的核心问题与实践应对——以网络平台侵权责任界定为视角[J]. 人民司法, 2024(16): 64-70.

[18] 丁晓东. 用户画像、个性化推荐与个人信息保护[J]. 环球法律评论, 2019, 41(5): 82-96.

[19] 张新宝. 论个人信息权益的构造[J]. 中外法学, 2021, 33(5): 1144-1166.

[20] 钛媒体 APP. 亚马逊 AI 招聘工具被曝性别歧视, 检测到女性就打低分[EB/OL]. 2018-10-10. https://www.sohu.com/a/258656369_116132, 2026-01-25.

[21] 玛农·奥斯特芬. 数据的边界: 隐私与个人数据保护[M]. 曹博, 译. 上海: 上海人民出版社, 2020: 47.