

个人信息保护视域下电商平台算法推荐策略的法律规制研究

原欣雅

扬州大学法学院, 江苏 扬州

收稿日期: 2025年6月8日; 录用日期: 2025年6月25日; 发布日期: 2025年7月16日

摘要

电商平台算法推荐技术在提升交易效率的同时, 也引发了个人信息保护等方面的法律挑战。当前法律框架在应对算法治理问题时呈现明显滞后性, 表现为规范体系碎片化、监管手段不足以及司法救济困难等现实困境。算法推荐系统的技术复杂性导致用户知情权与选择权受到实质性削弱, 而平台的数据收集与处理行为往往超出合理边界, 加剧了隐私侵害风险。针对这些挑战, 需要构建多层次的法律规制体系。立法层面应制定专门性规范, 建立算法分级分类管理制度, 明确高风险算法的备案与审查要求; 监管层面需引入技术治理工具, 如算法审计与动态风险评估, 提升监管机构的专业能力; 平台层面应强化合规义务, 落实有限披露原则并完善内部问责机制; 用户权利救济方面可探索举证责任倒置规则, 并发展公益诉讼等多元化救济渠道。电商平台算法治理的完善不仅关乎消费者权益保护, 更对数字经济的健康发展具有重要意义, 通过法律规范与技术治理的协同, 能够实现技术创新与权益保障的平衡, 推动形成公平、透明的数字市场秩序。

关键词

个人信息保护, 电商平台, 算法推荐策略, 法律规制

Research on the Legal Regulation of E-Commerce Platform Algorithm Recommendation Strategy from the Perspective of Personal Information Protection

Xinya Yuan

School of Law, Yangzhou University, Yangzhou Jiangsu

文章引用: 原欣雅. 个人信息保护视域下电商平台算法推荐策略的法律规制研究[J]. 电子商务评论, 2025, 14(7): 1216-1222. DOI: 10.12677/ecl.2025.1472295

Abstract

Algorithmic recommendation technology on e-commerce platforms has triggered legal challenges in the protection of personal information while enhancing transaction efficiency. The current legal framework is lagging behind in dealing with algorithmic governance, which is manifested in the fragmentation of the normative system, insufficient regulatory means and difficulties in judicial relief. The technical complexity of algorithmic recommendation systems leads to a substantial weakening of users' right to know and right to choose, while the data collection and processing behavior of platforms often exceeds reasonable boundaries, exacerbating the risk of privacy infringement. In response to these challenges, a multi-level legal regulatory system needs to be constructed. At the legislative level, specialized norms should be formulated, an algorithm classification and management system should be established, and the filing and review requirements for high-risk algorithms should be clarified; at the regulatory level, technical governance tools such as algorithmic auditing and dynamic risk assessment should be introduced to enhance the professional capacity of regulatory agencies; at the platform level, compliance obligations should be strengthened, the principle of limited disclosure should be implemented, and the internal accountability mechanism should be perfected; and the reversal of the burden of proof can be explored in respect of user remedies. In terms of users' rights relief, the reversal of the burden of proof can be explored, and diversified relief channels such as public interest litigation can be developed. The improvement of algorithmic governance of e-commerce platforms is not only related to the protection of consumers' rights and interests, but also of great significance to the healthy development of the digital economy. Through the synergy of legal norms and technological governance, it can realize the balance between technological innovation and protection of rights and interests, and promote the formation of a fair and transparent digital market order.

Keywords

Personal Information Protection, E-Commerce Platform, Algorithmic Recommendation Strategies, 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. 问题的提出

随着数字经济的蓬勃发展,算法推荐技术已成为电商平台优化用户体验、提升交易效率的核心工具。基于用户行为数据与机器学习技术,平台能够精准预测消费偏好、动态调整商品定价并实现个性化营销,其技术逻辑从“人找信息”转向“信息找人”,重构了传统交易模式。然而,这一技术赋能的另一面,是平台对个人信息的过度攫取与算法权力的无序扩张。根据中国互联网络信息中心(CNNIC)统计,截至2024年12月,我国网络购物用户规模达9.74亿人,较2023年12月增长5947万人,占网民整体的87.9% [1]。在此背景下,技术效率与个人信息权益的冲突日益凸显:一方面,算法推荐策略的隐蔽性与复杂性使普通用户难以理解其决策逻辑,知情同意机制沦为形式;另一方面,平台借助算法优势实施“大数据杀熟”、诱导消费等行为,导致消费者陷入信息茧房与价格歧视的双重困境。技术中立的表象之下,算法已成为平台扩张商业利益、规避法律责任的工具。

当前法律体系对算法推荐技术的规制呈现明显的滞后性。尽管《个人信息保护法》《电子商务法》等法律确立了数据收集的最小必要原则与用户同意规则，但在实践中，平台往往通过“默认勾选”“隐私政策嵌套”等设计虚置用户选择权。更关键的是，算法黑箱导致侵权行为难以追溯：当用户因动态定价遭受损失时，既无法获取算法决策的具体参数，也难以证明平台主观恶意，最终陷入“有损害无救济”的困境。此外，现行法律对算法责任主体的界定模糊，平台常以“技术自主性”为由将责任转嫁给开发者或用户自身，进一步加剧了执法与司法实践的混乱。这一矛盾的本质，是数字经济创新与个人基本权利保护的张力。算法推荐技术的广泛应用虽推动了商业效率的提升，但其对个人信息自主权、公平交易权的侵蚀已不容忽视。若放任平台以技术创新之名行数据滥用之实，不仅将加剧市场垄断与消费者弱势地位，更可能动摇数字社会的信任基石。因此，如何在促进技术发展与保障个人信息安全之间构建平衡机制，成为数字时代法律规制的核心命题，应探索兼顾效率与公平的规制路径，为完善我国算法治理框架提供理论参考与实践指引。

2. 电商平台算法推荐策略的应用现状与法律问题

2.1. 算法推荐策略的应用场景

数字经济法律问题的特点之一是具有典型的场景性，因此算法治理符合“场景正义”[2]的要求已经成为基本共识。现代电商平台的算法推荐系统已经发展成为一个复杂的智能决策体系。通过对用户多维度的数据采集，包括但不限于浏览轨迹、停留时长、加购行为、历史订单、评价内容、社交互动等，平台能够构建极其精准的用户画像。不仅算法的设计和编写体现设计者的价值选择，而且设计者对用户数据的标注、算法的训练以及用户画像的修正等等，都是基于设计者的某种判断与选择，所有这些都决定了算法运行的底层逻辑[3]。以阿里巴巴的“千人千面”推荐系统为例，该系统每天处理超过 100 PB 的用户数据，能够识别超过 2000 个用户标签维度，这种深度画像带来的营销精准度提升是显而易见的。然而，这种精准营销的背后是对用户隐私的深度侵入。平台不仅收集显性的购买行为数据，还会通过鼠标移动轨迹、页面滚动速度等细微行为推断用户的情绪状态和购买意向。服务于电商平台盈利目标的算法推荐的精准度依赖于海量数据的训练，电商平台通过数据标注以及数据输入，可进一步控制算法决策结果的输出[4]。更值得关注的是，一些平台开始尝试“预测性推荐”，即在用户尚未明确表达需求前，就通过算法预测其潜在需求。这种推荐方式虽然提升了商业效率，但实质上是对用户自主选择权的隐性剥夺。

其次，动态定价算法已经从简单的供需调节发展为复杂的用户价值评估系统。现代电商平台采用的动态定价算法通常会考虑以下因素：用户的购买力(通过设备型号、收货地址等推断)、价格敏感度(通过历史比价行为判断)、购买紧迫性(通过浏览频率和时长评估)等。这种定价策略的隐蔽性在不断增强。早期的价格差异主要体现在直接的标价上，而现在则更多通过优惠券组合、会员折扣等间接方式实现。平台可能对高价值用户发放更大面额的优惠券，而对价格敏感用户则提供小额但更频繁的折扣，这种差异化策略使得价格歧视更难被发现和举证。

算法推荐导致的信息窄化问题已经引起了广泛关注。更值得警惕的是，平台正在将行为心理学原理深度融入推荐算法。通过“稀缺性提示”(如“仅剩 3 件”)、“社会认同暗示”(如“1000 人正在浏览”)、“紧迫感营造”(如“2 小时后涨价”)等设计，算法不仅推荐商品，更在塑造用户的购买决策过程。这种设计使得消费者的自主选择权受到系统性侵蚀。

2.2. 算法推荐策略对个人信息保护的直接威胁

权力与责任具有相辅相成和相互制衡的辩证关系，权力并非仅仅来自于法定，权力的实质是特定主体拥有足以支配他人或影响他人的资源[5]。平台经济作为数字经济的典型形态，电商平台在基于技术和

信息优势构建的算法生态系统中整体上处于绝对优势地位[6]。从数据收集的初始环节开始,平台即通过多维度、全周期的信息采集机制实现对用户隐私的全面渗透。在数据采集层面,算法推荐系统依托分布式数据抓取技术,不仅获取用户显性的交易数据和浏览记录,更通过行为轨迹分析、环境信息采集等技术手段,持续收集包括但不限于设备信息(如IMEI、MAC地址)、生物特征(如指纹、面部识别数据)、社交关系(如通讯录、好友列表)等敏感信息。这种过度收集行为实质上突破了《个人信息保护法》确立的最小必要原则,形成了数据采集的范围失控现象。在数据处理环节,平台通过分布式计算和机器学习技术,对原始数据进行深度挖掘与交叉分析,构建具有预测能力的用户画像模型。这一过程涉及对个人信息的二次加工和聚合利用,往往超出用户最初的数据授权范围。特别值得关注的是,平台普遍采用渐进式画像技术(Progressive Profiling),即在用户使用过程中不断补充和修正画像维度,使数据收集呈现动态扩张的特征。这种处理方式不仅导致个人信息使用目的的持续泛化,更使得用户难以对其数据的最终用途形成明确认知。

算法推荐策略对个人信息保护的直接威胁还表现在同意机制的形式化问题。平台通过复杂的界面设计和信息架构,实质性地削弱了用户的知情同意能力[7]。具体表现为:隐私政策文本采用专业化法律术语和技术概念,可读性显著降低;同意流程设置多重交互障碍,如将拒绝选项置于次级界面或要求多次确认;默认设置偏向数据收集,利用用户的行为惯性获取默示同意。这种设计模式本质上构成了对同意要件的实质性架空,使得《个人信息保护法》确立的知情同意原则沦为形式合规的工具。此外,平台通过模糊化的授权条款,将用户数据在关联企业、第三方服务提供商等主体间进行多级流转。这种共享行为往往缺乏明确的目的限定和使用约束,导致个人信息脱离原始收集场景后的使用完全失控。更严重的是,部分平台通过算法接口开放(API)等方式,实现数据的实时共享和联合建模,形成了去中心化的数据利用网络,使得传统的个人信息边界保护机制完全失效。

算法推荐系统对个人信息的威胁还体现在其固有的不透明性上。深度学习等复杂算法的决策过程难以追溯,用户既无法了解哪些具体数据影响了推荐结果,也难以判断数据使用的合法性和正当性。这种黑箱效应不仅阻碍了用户行使访问权、更正权等法定权利,更使得数据滥用行为难以被发现和举证。平台往往以保护商业秘密或算法专利为由,拒绝披露推荐系统的关键参数和运行逻辑,进一步加剧了信息不对称的问题。

算法推荐对个人信息的威胁正在从单一的数据安全风险向复合型权益侵害转变。个人信息不仅面临泄露、篡改等传统安全威胁,更成为平台实施精准营销、差别定价等行为的工具,最终导致用户的人格尊严和自主决策权受到系统性侵蚀。这种侵害模式具有累积性和隐蔽性的特点,单个数据处理行为可能看似无害,但通过算法的持续学习和反馈,最终形成对用户隐私的全面控制。

3. 电商平台算法推荐法律规制的现实困境

电商平台算法推荐的法律规制困境,本质上是传统法律框架与数字技术特性的结构性错位。这种错位在立法、执法与司法层面呈现递进式冲突,形成系统性规制盲区。

3.1. 立法层面:规范供给不足

在立法层面,现有规范体系呈现出明显的碎片化特征,《民法典》《电子商务法》《数据安全法》以及《个人信息保护法》等法律虽然各自确立了相关基本原则,但缺乏针对算法推荐这一特定技术应用的系统性规制框架。各法律规范之间的衔接存在实质性漏洞,例如《电子商务法》第三十九条虽然规定“电子商务平台经营者应当根据商品或者服务的价格、销量、信用等以多种方式向消费者显示商品或者服务的搜索结果”,但未对算法推荐的具体透明度要求作出可操作的规定;而《个人信息保护法》第二十四

条虽然确立了自动化决策的相关规则，却未充分考虑电商场景下算法推荐的特殊性。更为深层次的矛盾在于算法透明义务与商业秘密保护之间的价值冲突，现行法律既要求平台保障用户的知情权，又缺乏对算法披露范围与程度的明确指引，导致平台往往以保护商业秘密为由规避实质性的透明度要求，形成“原则性规定多、操作性规则少”的立法困境。

3.2. 监管层面：执行效能低下

在监管层面，行政规制面临着技术复杂性与监管能力不足的双重制约。算法推荐系统所具有的技术黑箱特性使得传统监管手段难以实现有效穿透，监管部门既无法准确掌握算法运行的实际逻辑，也难以评估其具体影响。现有的事后监管模式与算法实时动态调整的特性之间存在本质矛盾，监管措施往往滞后于技术发展。同时，行政监管机构普遍面临专业技术人才匮乏和技术手段不足的困境，各级市场监管部门和网信部门缺乏足够的算力支持和数据分析能力来应对平台算法的复杂性。监管资源的有限性也导致执法难以常态化，当前主要依靠专项行动式的集中整治，缺乏持续性的监督机制。此外，跨部门监管协调机制尚未有效建立，网信、市场监管、工信等多个部门之间的权责边界模糊，容易出现监管重叠或监管真空。

3.3. 司法层面：裁判标准模糊

司法救济层面面临着举证责任分配与损害认定的系统性难题。由于算法决策过程的不透明性，用户往往难以证明特定损害与算法推荐行为之间的因果关系，传统的“谁主张谁举证”原则在算法侵权案件中面临适用困境。法院在审理此类案件时，往往因缺乏专业技术支持而难以对算法是否构成歧视或欺诈作出准确判断。在损害量化方面，算法推荐造成的损失往往具有无形性和扩散性特征，既包括直接经济损失，也涉及隐私侵害、选择自由受限等难以货币化的权益损害，现行法律缺乏科学的量化标准。此外，算法侵权的集体救济机制尚不完善，代表人诉讼和公益诉讼在实践中的适用仍面临诸多障碍，导致多数小额分散的损害难以获得有效救济。

3.4. 平台层面：合规动力缺失

平台企业作为算法推荐系统的开发者和运营者，天然具有通过算法最大化商业利益的动机，这种动机与个人信息保护和消费者权益保障的社会目标之间存在根本性张力。在实践中，平台往往采取“合规形式主义”的策略，即通过表面符合法律要求的隐私政策和用户协议来规避实质性的合规义务，而算法的实际运行则仍然遵循利润最大化逻辑。平台内部设立的算法伦理委员会和合规部门普遍缺乏独立性和权威性，其审查标准往往让位于商业考量。更为深层的问题在于，当前缺乏有效的激励机制促使平台进行实质性的自我规制，合规成本与收益之间的不平衡导致平台更倾向于采取最低限度的合规策略。行业自律规范的发展也相对滞后，尚未形成具有约束力的技术标准和行为准则，平台间的“竞次效应”进一步削弱了自我规制的实际效果[8]。

4. 电商平台算法推荐策略的法律规制路径

4.1. 立法完善：构建分层规制体系

针对电商平台算法推荐的法律规制，应当首先从立法层面构建系统化、精细化的规范体系。当前亟需对电商场景下的算法应用设立针对性规范，重点明确算法推荐服务提供者的主体责任边界。在立法技术上，应当采取“风险分级”的规制思路，根据算法推荐的影响范围和风险程度实施分类管理：对于涉及个人敏感信息处理或可能显著影响用户重大权益的高风险算法(如定价算法、信用评估算法等)，应当建

立事前备案制度，要求平台向监管部门提交算法基本原理、主要参数及影响评估报告；对于一般性推荐算法，则采取事后监管模式，重点规范其数据收集和处理行为。这种分层规制的优势在于既能确保对高风险算法的有效管控，又可避免对技术创新造成过度抑制。同时，立法应当着重解决现有法律间的协调问题，在《个人信息保护法》确立的基本原则框架下，细化《电子商务法》中关于算法透明的具体要求，形成逻辑自洽、层级分明的规范体系。

4.2. 监管创新：技术赋能与协同治理

提升监管效能的关键在于推动监管模式的技术转型和机制创新。首先应当建立专业化的算法审计制度，通过引入第三方技术机构对电商平台算法进行合规性审查，重点评估其是否存在歧视性、欺骗性设计。审计标准应当包括算法设计的公平性、数据使用的合法性以及推荐结果的合理性等维度。其次，可借鉴金融监管领域的“监管沙盒”机制，在可控环境中测试新型推荐算法的实际效果，通过“试点-评估-推广”的渐进式路径平衡创新与风险防控。在监管手段上，应当充分利用大数据分析技术，构建算法监管信息平台，实现对电商平台推荐系统的动态监测和风险评估。同时，需要建立跨部门的协同治理机制，明确网信办、市场监管总局、工信部等部门的监管职责分工，形成信息共享、执法联动的综合治理格局。特别值得注意的是，监管创新应当注重保持技术中立原则，避免对特定算法技术预设价值判断，而应聚焦于算法应用产生的实际效果。

4.3. 用户权利救济：司法与替代性方案

完善的权利救济机制是算法规制体系的重要保障。在诉讼程序方面，应当针对算法侵权的特殊性探索“举证责任倒置”规则，当用户提出初步证据证明可能遭受算法歧视时，由平台承担算法合规性的证明责任。这一制度设计能够有效缓解用户在举证能力上的结构性弱势。同时，应当完善集体诉讼制度，允许消费者组织代表不特定多数用户提起算法侵权诉讼，解决个体诉讼成本过高的问题。在司法技术层面，建议在法院系统设立专门的技术调查官制度，为法官审理算法案件提供专业支持。除司法救济外，还应当发展多元化的替代性纠纷解决机制，例如建立电商算法争议仲裁中心，通过专业、快捷的非诉途径解决算法纠纷。另外，可考虑创设算法侵权专项救济基金，为受算法侵害的用户提供及时补偿，再通过代位追偿机制向责任平台追索。

4.4. 平台责任强化：合规义务的具体化

平台作为算法推荐系统的实际控制者，应当承担与其技术能力相匹配的法律责任。首要的是细化算法透明化义务，要求平台在不披露核心商业秘密的前提下，向用户提供算法推荐的基本原理、主要考虑因素及个性化特征等关键信息，确保推荐结果具有最低限度的可解释性。这种有限披露原则既保护了企业的合法权益，又保障了用户的知情权。平台内部应当设立具有独立性的算法伦理委员会，由技术专家、法律顾问和外部学者共同组成，负责对推荐算法的伦理合规性进行审查。同时，需要建立完善的内部问责机制，明确算法开发、测试、部署各环节的责任主体，确保算法问题可追溯、可追责。在组织架构上，平台应当设立专门的算法合规官职位，直接向董事会汇报，避免合规职能被商业目标边缘化。此外，建议建立算法影响评估制度，要求平台在重大算法变更前进行系统性风险评估，并将评估结果纳入企业年度社会责任报告。

5. 结语

互联网技术的迅猛发展会“废除所有能够带来稳定和秩序的传统故事和符号，而重新讲述一个关于技能、技术知识和消费美梦的故事”[9]。电商平台算法推荐技术的法律规制问题，集中体现了数字经济

时代技术创新与权益保障之间的深刻矛盾。现如今，算法推荐系统已发展成为集数据采集、行为预测和决策引导于一体的复杂技术体系，对个人信息保护、消费者权益和市场秩序产生多维影响。传统法律规制模式面临规范供给不足、监管效能低下和司法救济滞后等结构性困境。构建有效的法律规制体系需要采取分层治理思路。立法层面应当建立专项规制框架，实施基于风险等级的分类管理制度；监管层面需引入技术治理手段，通过算法审计和监管沙盒等创新机制提升监管效能；平台层面要强化合规义务，建立算法透明化和内部问责机制；用户权利救济方面则应完善举证责任分配规则，发展多元化纠纷解决机制。随着《个人信息保护法》等法律法规的实施，具有中国特色的算法治理路径正在形成。这一进程不仅关乎电商行业健康发展，更对构建数字社会治理体系具有重要意义。未来需要持续关注算法伦理标准、跨境规制协调等前沿问题，通过多学科交叉研究和各方协同合作，推动技术创新与权益保护的动态平衡，实现算法治理体系的不断完善。

基金项目

2024 年江苏省研究生科研与实践创新计划项目，项目名称：大数据时代个人信息权益的私法保护研究，项目编号：SJCX24-2172。

参考文献

- [1] 中国互联网络信息中心. 第 55 次中国互联网络发展状况统计报告[R]. 2025: 33.
- [2] 丁晓东. 论算法的法律规制[J]. 中国社会科学, 2020(12): 138-159+203.
- [3] 任安麒. 网络服务平台算法推荐的著作权侵权认定规则[J]. 北京航空航天大学学报(社会科学版), 2023, 36(3): 190-198.
- [4] 王叶刚. 个人信息处理者算法自动化决策致害的民事责任——以《个人信息保护法》第 24 条为中心[J]. 中国人民大学学报, 2022, 36(6): 47-59.
- [5] [德]尤尔根·哈贝马斯. 作为“意识形态”的技术和科学[M]. 李黎, 郭官, 译. 上海: 学林出版社, 1999: 76.
- [6] 张凌寒. 算法权力的兴起、异化及法律规制[J]. 法商研究, 2019, 36(4): 63-75.
- [7] 万方. 个人信息处理中的“同意”与“同意撤回”[J]. 中国法学, 2021(1): 168.
- [8] 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.
- [9] 尼尔·波兹曼. 技术垄断: 文明向技术投降[M]. 蔡金栋, 译. 北京: 机械工业出版社, 2013: 21.