

电商平台用户隐私条款的规制困境与完善路径构建

李 春

江苏大学法学院, 江苏 镇江

收稿日期: 2025年10月11日; 录用日期: 2025年10月23日; 发布日期: 2025年11月24日

摘 要

随着电子商务的快速发展, 平台收集用户数据与隐私保护之间的矛盾日益凸显。本文分析了电商平台隐私条款的规制困境, 包括条款模糊性、用户被动地位及算法不透明等问题。提出应从优化隐私政策、推动算法透明、完善监管体系等多维度构建综合治理路径, 以实现数据利用与隐私保护的平衡, 促进数字经济健康发展。

关键词

电商平台, 隐私条款, 个人信息保护, 数据治理, 用户权益

Regulatory Dilemmas and Improvement Path Construction of User Privacy Policies on E-Commerce Platforms

Chun Li

School of Law, Jiangsu University, Zhenjiang Jiangsu

Received: October 11, 2025; accepted: October 23, 2025; published: November 24, 2025

Abstract

With the rapid development of e-commerce, the contradiction between platform collection of user data and privacy protection has become increasingly prominent. This article analyzes the regulatory dilemmas of privacy clauses on e-commerce platforms, including ambiguity of clauses, passive position of users, and opacity of algorithms. It proposes to construct a comprehensive governance path from multiple dimensions, such as optimizing privacy policies, promoting algorithm transparency,

and improving the regulatory system, in order to achieve a balance between data utilization and privacy protection and promote the healthy development of the digital economy.

Keywords

E-Commerce Platform, Privacy Clause, Personal Information Protection, Data Governance, User Rights

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

在数字化商业浪潮中，电子商务平台迅速崛起，已成为大众消费的主要途径。用户通过平台获取商品与服务的同时，也留下了日益增长的个人数据轨迹。诸如消费记录、支付详情、浏览行为等敏感信息不断累积，逐步构建出反映个人偏好与习惯的用户数字画像[1]。在此背景下，如何有效保障用户在交易过程中产生的各类隐私数据，成为亟待解决的关键议题。

根据《中华人民共和国民法典》总则部分的规定，电子商务运营者在开展个人信息处理活动前，须履行告知职责，清晰说明信息使用的目标、手段与范畴，并获取用户明确许可，切实维护个人信息权益。

《中华人民共和国刑法》同时明文禁止任何机构或个人非法买卖、提供或公开公民个人信息[2]。

现阶段，电子商务平台在数据价值开发与用户权利维护之间面临现实矛盾[3]。平台既需要借助数据分析优化服务体验，又可能因信息收集或使用边界的模糊而危及用户隐私安全[4]。目前，针对平台收集用户信息行为的规范体系，主要建立在以《个人信息保护法》为核心的法律框架之上[5]。因此，深入探索电商平台用户隐私的法律保障体系，对营造安全、可靠的线上交易环境具有紧迫的现实意义。

本文选取淘宝、京东、拼多多与亚马逊等代表性电商平台的用户隐私文本作为研究样本，通过系统梳理与对比分析，揭示各平台在隐私保护措施上的异同，评估其可能导致的数据风险，并归纳现行制度中存在的主要缺陷。结合对用户隐私关注点与保护期望的调研，为优化平台数据治理模式提供决策依据。

本研究的价值主要体现在以下维度：在技术层面，致力于完善数据安全防护体系与隐私政策的清晰化呈现；在运营层面，建立标准化的平台数据处理流程；在行政层面，构建针对平台数据活动的长效监管机制；在法律层面，明确隐私权的保护范围，推进分级分类的保护策略，并完善侵权后的救济途径。

2. 电商平台隐私条款的现行规范分析

在数字化治理架构中，个人信息保护制度的核心载体表现为隐私政策，其在全球法律比较视角下展现出多元化的法律特征与功能定位。隐私政策作为保障用户个人信息安全的关键制度设计，同时构成落实信息透明化与用户自主决策机制的核心载体[6]。各类信息处理主体通常采用“隐私声明书”或“数据保护告知”等不同形式来呈现制度安排，其本质上构成了对个人信息全生命周期处理活动的系统性规范保证[7]。特别需要指出的是，我国《个人信息保护法》第十四条明确规定的告知同意机制，为个人信息处理活动提供了合法性基础，要求信息处理主体必须严格遵循“全面告知-自主选择”的双重要件，在开展具体数据处理前获得信息主体的明确授权[8]。

通过对国内主流电子商务平台数据保护条款的详细调研发现，不同平台在政策框架设计上普遍包含数据采集、加工处理、共享流转、安全保障及权益维护等核心内容模块，但在具体执行标准上表现出明

显区别。在信息采集维度,各平台均要求获取基础身份信息以保障服务正常运行,但对于补充信息的采集规则则体现出差异化的管理思路。具体来说,淘宝平台注重保障用户对个人信息的自主控制权,京东平台强调遵循最小必要原则收集信息,拼多多平台在提升服务质量的同时充分尊重用户选择意愿,而亚马逊平台则因其跨国经营特性需要遵循不同法域的合规要求。

在数据开发利用层面,各平台呈现出明显的战略差异。部分平台倾向于深度挖掘用户数据的商业价值,用于个性化推荐和精准营销活动(亚马逊、淘宝);而另一些平台则更加重视数据使用的合规边界,严格限定数据处理的应用场景(京东)。在数据共享机制设计方面,亚马逊平台明确规定未经用户明确授权不得向任何第三方提供数据,其他平台则在获得用户同意的基础上与业务合作伙伴建立数据共享关系。需要关注的是,不同平台在数据安全技术措施的披露透明度上存在较大差距,部分平台提供了详尽的技术实施方案(亚马逊),部分平台则仅作出原则性承诺(淘宝、京东、拼多多)。

当前隐私政策在落地实施过程中面临诸多合规性难题。虽然各平台都在制度层面建立了完整的政策体系,但普遍存在条款表述笼统、关键信息缺失等问题。多数政策文件未能准确列明采集信息的具体类别、处理方式及存储时限等核心要素,这与要求的明确性原则存在偏差。在实际操作层面,平台往往面临双重困境:若过度追求政策文本的简洁性,通过大量重点标注方式提示用户,反而可能造成信息过载,影响用户的准确理解;而若过度压缩政策内容,又可能因专业概念缺乏通俗解释,导致普通用户难以把握条款实质内涵。因此,此类隐私条款的实际效力往往不尽如人意,既难以满足法律法规及行业惯例对表述明确性、提示显著性的基本要求,又难以在规范严谨与用户友好之间取得平衡。正如学界所指出的,“过度追求文本的精确性可能导致实质内容的空洞化”。在平台业务形态持续演进、数据应用场景不断拓展的背景下,仅靠隐私政策的表面合规显然已不足以构建真正有效的个人信息保护体系[9]。

根据对各平台数据安全风险的评估比较显示,不同平台基于其商业模式、技术实力和管理体系的差别,面临着各异的数据保护挑战。用户规模庞大、交易环节复杂且接入多方商家的平台面临较高的数据泄露概率;依赖物流配送体系的平台在运输环节存在数据安全漏洞;采用社交电商模式的平台面临独特的信息共享风险;而开展跨国业务的平台则需要应对跨境数据流动带来的复杂合规要求。这些差异不仅体现了各平台在数据保护策略上的不同侧重,也为监管部门完善法律制度提供了实践参考。

3. 电商平台利益与用户隐私权益冲突

3.1. 平台数据收集与用户隐私利益

在当前的数字经济生态中,电子商务平台作为关键的数据处理中枢,依托其在组织架构、技术能力与资本规模上的显著优势,不仅全面主导用户数据的处理流程,更在其构建的服务场域中实际履行着“私营规则制定者”的职能,从而形成一种以企业权力为主导的“信息控制力”。相比之下,个体用户在技术与资源层面天然处于弱势,在整个数据被收集、分析与应用的过程中缺乏实质性的参与途径和有效的控制手段。这种结构性的力量不对等,构成了平台大规模采集数据与用户个人信息难以得到充分保护之间的深层矛盾。

该矛盾在商业实践中表现得尤为明显,平台以营利为核心目标,结合其在交易过程中形成的信息优势与强大的数据分析能力,必然倾向于利用这些条件来提升收益并扩大用户规模。中国消费者协会2018年发布的《100款APP个人信息收集与隐私政策测评报告》显示,超过90%的被调查移动应用存在超越合理范围收集用户个人信息的现象,普遍存在违规获取数据的情况。这一现状恰如学者所言:“在由平台构建的数字生态中,双方的角色如同‘棋手’与‘棋子’。平台既是规则的制定者,也拥有信息优势,而用户则往往只能在此既定规则下行动,这种先天格局决定了双方的权力并不对等。”[10]

为了实施精准营销和提供个性化服务,电商平台广泛应用大数据算法,对用户的搜索、浏览、购买

等行为数据进行深入挖掘,通过识别消费趋势、建立用户标签体系,甚至推测个人偏好与身份特征。这种做法在提升商业运营效率的同时,也使个人信息泄露与算法歧视等风险显著增加。尤其值得注意的是,平台使用的大数据算法通常以不透明的“黑箱”模式运行,其内在逻辑与决策机制既不向用户公开,也难以被监管部门全面审视。这种不透明性导致用户无法了解自身数据被如何使用,更难识别算法判断中可能存在的偏见或不公[11]。

在司法实践中,这种权力失衡引发的侵权争议日益增多。以“罗某诉某科技有限公司隐私权、个人信息保护纠纷案”为例,该案作为最高人民法院 2025 年发布的指导性案例 265 号,明确了个人信息收集的“必需性 + 自愿性”双重合规标准。法院指出,判断信息收集是否“必需”应结合行业规范和产品功能,例如学习教育类 APP 仅需手机号即可提供基本服务;同时,若未提供拒绝填写非必要信息的选项(如“跳过”),用户被迫同意应视为无效。法院最终认定科技公司未经同意收集用户职业、学龄等画像信息构成侵权,判决其删除数据并赔偿损失¹。

需要明确的是,用户权益与平台对数据的开发利用并非绝对对立。在合法合规的框架下,对涉及用户隐私的数据进行必要处理,其隐私限度的适度调整并不必然损害用户的整体权益。然而,在缺乏有效制约机制的情况下,平台既可能通过严格自律来保障用户权益,也可能为追求更大商业利益而选择忽视用户隐私保护[12]。实践中,平台往往将用户数据应用于初始收集目的之外的其他商业场景,如行为分析、广告推送等,这种行为不仅加剧了用户对隐私安全的忧虑,也持续削弱其对平台的信任基础。

3.2. 用户被动保护隐私

在电商平台中,用户对个人数据的收集、使用与共享普遍处于被动状态,其控制权与知情权未能得到充分保障。以杭州互联网法院审理的“吴某诉某电商平台及付费通公司个人信息侵权案”为例,原告在未充分知情的情况下,其姓名、身份证号等敏感信息被某电商平台擅自共享至第三方支付及银行机构,甚至在尝试注销账户时遭遇障碍。法院最终认定两被告在信息处理中缺乏合法性基础,构成共同侵权,判令其承担赔礼道歉与赔偿合理维权支出的责任²,该案揭示出该电商平台在数据共享告知与用户控制机制方面存在的系统性缺陷。这种被动性首先体现在隐私政策获取与阅读的环节,尽管平台通常设有独立的隐私政策,但其访问路径往往被深藏。根据相关研究方法,部分 APP 需要用户进行多达四次点击才能找到隐私政策,导致绝大多数用户因过程繁琐而选择跳过阅读,直接使用服务[13]。这种设计使得用户在未能了解条款内容的情况下,便默许了平台的数据处理行为。

其次,即使用户试图主动管理隐私,也常常面临设置复杂、操作困难的挑战。尽管部分平台提供了隐私设置选项,但这些设置通常缺乏清晰的说明与引导,选项含义晦涩,布局分散,使用户在配置过程中容易困惑甚至放弃。以淘宝平台为例,其隐私设置功能并未配备必要的解释说明,导致用户难以有效理解和运用这些工具来保护自己的信息。最终,用户在数据如何处理、被谁共享等关键问题上缺乏实质控制力,陷入了“形式上可选择、实质上难操作”的被动局面。

3.3. 隐私条款模糊不清

电商平台隐私条款普遍存在的“模糊性”,是损害用户知情权与判断力的另一关键问题。这种模糊性首先体现在文本的表述上。许多条款大量使用法律专业术语,且对“必要的个人信息”、“与合作伙伴共享”等关键概念缺乏通俗化的解释,给用户的阅读理解设置了高门槛[14]。

更深层的问题在于内容本身的笼统与不明确。许多政策对数据收集范围和使用目的的说明过于宽泛,

¹(2022)京 04 民终 494 号民事判决。

²杭州中院(2021)浙 01 民终 12780 号。

未能清晰、具体地列明将收集的个人信息类型及其对应的使用场景。例如，条款中可能仅模糊表述为“为改善服务体验收集您的相关信息”，却未指明具体是设备信息、浏览记录还是社交关系。这种宽泛的授权使用户无法准确判断自己的哪些信息将被收集、作何用途，从而难以评估隐私泄露的真实风险[15]。

此外，条款的呈现形式单一、可读性低，进一步加剧了理解的困难。冗长的文本缺乏图表、摘要等可视化方式的引导，目录导航功能也往往残缺不全。所有这些因素共同作用，使得隐私条款成为一纸用户“看不懂”也“看不透”的模糊协议，用户在其中难以获得真正有效的信息，其知情同意在很大程度上流于形式。

4. 电商平台用户隐私保护体系路径构建

4.1. 优化隐私政策

当前，电商平台推行的隐私政策作为具有格式合同性质的规范性文件，其制定过程存在明显的单向性特征这类政策由平台依据相关法律法规单方面拟定，用户仅在注册环节通过点击同意方能获得服务访问权限，从法律性质上构成了双方合意的契约关系[16]。然而，这种制定模式的局限性直接影响了政策的实际效力，导致用户难以在信息处理活动中实现真正的意思自治，这不仅削弱了用户的自主选择权，也违背了契约自由的基本精神。

为突破这一困境，应当从政策制定机制与内容呈现方式两个维度进行系统性改进。在制定环节，平台应建立常态化的用户参与渠道，通过公开征求意见、组织听证会等形式，使消费者能够在政策形成阶段表达诉求从源头上确保双方利益的均衡协调。在内容设计层面，需着力提升文本的可读性与友好度。具体而言，应优化访问路径设计，将隐私政策入口置于界面显著位置，减少用户操作层级；同时采用逻辑清晰的框架结构，配以通俗易懂的表达方式，并运用字体加粗、色彩区分等可视化技术对核心条款进行重点标注，帮助用户准确理解涉及数据收集、使用及共享的关键事项。

在规则设置方面，应当严格遵循《网络安全法》第四十一条确立的用户控制原则，构建分级分类的信息收集机制。平台必须明确区分核心功能与增值服务，禁止通过捆绑附加功能索取非必要信息。无论处理何种类型个人信息，都应当向用户完整披露处理依据，采取对权益影响最小的方案，并在获取明确授权后实施[17]。同时要完善授权撤回机制，通过设置便捷的取消通道保障用户的持续控制权，不得以服务降级等手段变相强制获取同意。

此外，应建立配套的维权保障体系，设立专门投诉受理通道，确保用户救济途径畅通。政策版本更新时，需突出显示修订内容并提供即时反馈渠道，便于用户了解变更事项并进行沟通咨询。通过构建从政策制定到执行监督的全流程优化机制，才能真正实现隐私政策从形式合规到实质有效的转变。

4.2. 推动算法透明化

在电子商务活动中，算法生成个体特征标识及其动态调整的全过程应当保持充分的公开性与可解释性。从历史沿革来看，电商平台的治理机制长期在非公开状态下运行，但为有效制约其可能存在的暗箱操作倾向，平台需要着力提升其私权力运行的透明度，采取多元化的信息披露手段，将算法规则的制定逻辑与决策依据纳入公众监督范畴。增强信息透明度不仅是保障用户知情权与参与权的制度基础，更是构建平台公信力的核心要素。具体而言，当算法通过数据分析进行用户画像时，其运行机理及输出结果应当面向用户公开，确保可能引发歧视性待遇或超出必要范围收集个人信息的行为得到有效识别与规制。

在当前电商生态内，用户普遍缺乏对算法处理过程的实质影响能力。复杂算法系统的“黑箱”特性导致其内部逻辑与决策路径对外部观察者形成认知壁垒。这种不透明性加剧了个人隐私遭受侵害的潜在风险。因此，提升算法的可解释性已成为当务之急。从比较法视角观察，域外立法实践已形成可资借鉴

的监管范式。以欧盟《人工智能法案》为例，该法案要求被认定为高风险的人工智能系统在进入市场前必须完成合规性评估，确保符合特定技术标准。该法案特别规定，受欧盟现行产品安全法规约束的人工智能产品与服务，均需接受第三方监管体系的持续监督[18]。

借鉴这一监管思路，我国电商平台应当承担起说明算法运行机制的责任义务。具体而言，平台需要公开其算法自动采集的数据类别及使用目的，确保数据收集环节的透明性；同时应当披露基于数据分析进行个性化推荐的具体标准及其权重设置，允许社会各界对数据处理实践开展审查，并评估其对个体权益的潜在影响[19]。

此外，平台还应当清晰阐释如何依据既定标准对用户进行画像，以及如何基于此开展精准营销等商业活动。明确个体特征识别与使用的判定依据，对防范基于敏感个人特征的歧视性对待具有关键作用。

通过确立电商平台在算法透明度方面的法定义务，可以有效监督各类数据处理行为的合规性。这种制度安排不仅能够保障用户的基本权利，更能够推动电子商务平台在数据处理实践中实现程序公正与社会责任的有效统一。

4.3. 完善分级监管体系

当前行政监管机制正面临从被动响应向主动引领的重要转型期。在这一背景下，构建科学完善的分级监管体系显得尤为迫切。该体系应当基于企业规模、数据处理能力及用户影响程度等多元维度，建立层次分明的监管框架。

对于日均活跃用户超过百万的大型电商平台，建议实施更为严格的季度合规审计制度。这类平台应当定期提交由具备资质的独立第三方机构出具的隐私政策影响评估报告，全面评估其数据处理活动的合法性与合理性。考虑到此类平台在行业内的示范效应和广泛影响力，还可引入“合规责任人”制度，要求企业指定高级管理人员专职负责隐私政策的制定与执行。

针对中小微企业特点，可设计更为灵活的“阶梯式监管”机制。具体而言，建立基于用户投诉数量、问题严重程度和整改情况的多维评估体系，设置动态调整的监管介入值。当企业相关指标达到预设标准时，监管机构应及时启动调查程序，并提供针对性的合规指导。这种差异化监管策略既能有效防范风险，又能避免给中小企业造成过重负担。

从实施层面看，建议开发统一的监管信息平台，实现企业合规情况的动态监测。该平台可自动采集企业的用户规模、投诉数据、整改情况等信息，为分级监管提供数据支持。同时，建立企业合规档案，将历次检查结果、整改情况等信息纳入其中，作为确定监管频次和力度的重要参考。

根据工业和信息化部 2023 年发布的监管通报数据显示，移动应用违规收集位置信息、过度索取权限等问题仍较为突出[20]。这一现状凸显了建立“必要信息”判定标准的重要性。建议依据“目的限定”基本原则，建立服务类型与数据字段的对应关系矩阵。以典型场景为例：导航类应用收集用户位置信息属于业务功能实现的必要范畴，而数字阅读平台要求获取终端设备通讯录权限则明显超出了合理边界。通过实施差异化的监管策略，既能够有效减轻中小微企业的合规负担，又能对大型平台形成必要的约束力，从而实现监管资源优化配置与监管效能提升的双重目标。

5. 结论

本研究通过系统性的规范分析和实证考察，深入探讨了电商平台用户隐私条款在规制层面的现实困境及其优化方案。研究发现，当前用户隐私保障主要面临三重挑战：隐私政策形式化严重、平台与用户权力不对等、算法决策透明度不足。这些问题导致用户在数据处理中处于被动地位，告知同意原则在实际运行中难以发挥应有作用。基于实证分析，本文提出应优化隐私政策设计与呈现方式，通过优化隐私

政策的架构设计与展示形式提升用户可理解性, 构建算法透明化运行机制以增强用户控制力。本研究的创新在于突破了单一规制模式, 提出了技术与制度协同、多方主体共治的解决方案。需要指出的是, 本研究主要聚焦于国内主流电商平台的隐私条款文本与用户认知, 尚未充分考察中小型平台及跨境场景下的差异化实践, 对算法透明机制的讨论也多集中于理论层面, 其具体技术实现与合规成本仍需进一步验证。展望未来, 可进一步探讨跨境数据流动规制与国内隐私保护的衔接问题, 关注人工智能生成内容、联邦学习等新兴技术对隐私保护框架的冲击, 并可结合行为经济学与实验方法, 评估不同告知机制对用户真实选择行为的影响, 为构建平衡数据利用与隐私保护的治理体系提供更坚实的理论支撑与实践路径。

参考文献

- [1] 顾炜江. 基于序贯博弈模型分析技术保护电子商务中的网络隐私[J]. 山东农业大学学报(自然科学版), 2014, 45(4): 595-600.
- [2] 周拴龙, 王卫红. 中美电商网站隐私政策比较研究——以阿里巴巴和 Amazon 为例[J]. 现代情报, 2017(1): 137-141.
- [3] 成燕, 梅姝娥, 促伟俊. 电子商务中消费者隐私和信息保险的作用机制及影响[J]. 系统管理学报, 2020(2): 308-317.
- [4] 李伦, 李军. 相称原则: 电子商务隐私保护的伦理原则[J]. 伦理学研究, 2014(5): 85-88.
- [5] 王正鑫. 超越个人信息保护: 电商平台非个人信息处理的法律规制[J]. 数字法治, 2023(5): 178-193.
- [6] 高秦伟. 个人信息保护中的企业隐私政策及政府规制[J]. 法商研究, 2019, 36(2): 16-27.
- [7] Solove, D.J. and Hartzog, W. (2014) The FTC and the New Common Law of Privacy. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2312913>
- [8] 江必新, 郭峰. 《中华人民共和国个人信息保护法》条文理解与适用[M]. 北京: 人民法院出版社, 2021: 140-142.
- [9] 唐林垚. 公共卫生领域算法治理的实现途径及法律保障[J]. 法学评论, 2021, 39(3): 95-107.
- [10] 褚婧一. “用户-平台”关系中告知同意规则修正的路径选择[J]. 苏州大学学报(法学版), 2023, 10(2): 61-74.
- [11] 郑佳宁. 知情同意原则在信息采集中的适用与规则构建[J]. 东方法学, 2020(2): 198-208.
- [12] 李小玲. 电子商务平台规范商家自律行为的策略研究: 基于制度理论的视角[M]. 武汉: 武汉大学出版社, 2016: 34.
- [13] Deotale, R., Rawat, S., Vijayarajan, V. and Surya Prasath, V.B. (2021) POCASUM: Policy Categorizer and Summarizer Based on Text Mining and Machine Learning. *Soft Computing*, **25**, 9365-9375. <https://doi.org/10.1007/s00500-021-05916-w>
- [14] 钟瑞栋, 张道鹏. 数字人权视阈下隐私政策的双重规制——基于隐私基准理论的公私法协同路径[J]. 江汉学术, 2025, 44(5): 5-15.
- [15] 马骋宇, 刘乾坤. 移动健康应用程序的隐私政策评价及实证研究[J]. 图书情报工作, 2020, 64(7): 46-55.
- [16] 米铁男. 中国电子商务领域隐私数据保护研究[J]. 学术交流, 2013(7): 38-41.
- [17] 王乐, 王璐瑶, 孙早. 隐私侵犯经历对网络用户自我披露的影响机制[J]. 理论与实践, 2020, 40(1): 79-89.
- [18] 许可, 刘畅. 论算法备案制度[J]. 人工智能, 2022(1): 64-70.
- [19] 郑晓剑. 比例原则在现代民法体系中的地位[J]. 法律科学(西北政法大学学报), 2017, 35(6): 101-109.
- [20] 工业和信息化部. 关于侵害用户权益行为的 APP (SDK)通报(2023 年第 4 批, 总第 30 批)[J]. 互联网天地, 2023(7): 53-56.