E-Commerce Letters 电子商务评论, 2025, 14(11), 3240-3244
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14113802

Hans汉斯

电子商务中消费者个人信息保护问题研究

梁婉倩

贵州大学法学院，贵州 贵阳

收稿日期：2025年10月14日；录用日期：2025年10月28日；发布日期：2025年11月28日

摘 要

数字经济时代，电子商务在驱动消费增长的同时，其高度依赖个人信息的商业模式也引发了严峻的隐私保护挑战。本文通过梳理电商平台责任缺失、法律规制不足及消费者维权无力等现实困境，提出应从立法细化、平台责任强化、维权机制优化、协同治理构建与技术赋能五个方面进行系统性规制，以构建一个法律规范、技术保障与多元治理的有机结合的保护框架，有效平衡信息利用与隐私保护之间的关系，建立起公平、透明、安全的电子商务信息保护体系，为保障消费者权益与促进数字经济健康发展提供理论参考与实践路径。

关键词

电子商务，个人信息保护，数据合规

Research on the Protection of Consumers' Personal Information in E-Commerce

Wanqian Liang

School of Law, Guizhou University, Guiyang Guizhou

Received: October 14, 2025; accepted: October 28, 2025; published: November 28, 2025

Abstract

In the era of the digital economy, while e-commerce drives consumption growth, its business model—highly reliant on personal information—has raised serious privacy protection challenges. By examining practical dilemmas such as the lack of accountability of e-commerce platforms, insufficient legal regulations, and consumers' difficulties in safeguarding their rights, this paper proposes a systematic regulatory approach from five perspectives: refining legislation, strengthening platform accountability, optimizing rights protection mechanisms, establishing collaborative governance, and leveraging technological empowerment. The aim is to construct a protection

文章引用: 梁婉倩. 电子商务中消费者个人信息保护问题研究[J]. 电子商务评论, 2025, 14(11): 3240-3244.
DOI: 10.12677/ecl.2025.14113802

framework that integrates legal norms, technical safeguards, and multi-stakeholder governance, effectively balancing the relationship between information utilization and privacy protection. This framework seeks to establish a fair, transparent, and secure e-commerce information protection system, providing theoretical reference and practical pathways for safeguarding consumer rights and promoting the healthy development of the digital economy.

Keywords

E-Commerce, Personal Information Protection, Data Compliance

1. 引言

随着数字经济的蓬勃发展，电子商务毋庸置疑已成为我国消费的极为重要的组成部分。根据中国互联网络信息中心(CNNIC)最新发布的第 56 次《中国互联网络发展状况统计报告》显示，截至 2025 年 6 月，我国网络购物用户规模达 9.76 亿人，占网民整体的 86.9% [1]，电子商务交易额连续多年保持高速增长，交易规模持续扩大。

然而，电子商务的繁荣背后，消费者个人信息保护问题日益凸显。消费者在电商平台的注册、交易、支付、物流乃至售后环节都需要被收集大量信息，涵盖的信息包括但不限于姓名、联系方式、地理定位等基础数据，还广泛涉及浏览历史、搜索记录、购物偏好等行为数据。这些数据不仅是完成交易的必要条件，更成为平台通过大数据和算法分析实现精准营销、绘制用户画像乃至于进行差别定价的核心资源。一方面，电商平台收集的庞大数量的消费者个人信息为其带来了具有巨大的经济价值，另一方面，也伴生出信息泄露、“大数据杀熟”、“算法歧视”等乱象，加之跨境数据流动带来的合规挑战，使得消费者个人信息保护成为数字治理中的重要议题。

2. 电子商务中消费者个人信息保护的现实困境

(一) 电商平台责任缺失

1、强制性授权与形式化统一

在互联网时代，消费者几乎难以避免使用主流电商平台完成购物、支付和售后服务。然而，在注册与登录过程中，平台普遍采取“默认勾选”“捆绑授权”等方式，使用户在尚未充分理解隐私政策的情况下即被迫同意全部条款。这种做法实际上剥夺了消费者的自由选择权，导致“同意”机制流于形式。《个人信息保护法》第 14 条明确规定，处理个人信息须建立在“充分知情、自愿、明确同意”的基础上，但在实践中，消费者处于强势平台与必需服务的结构性依赖之下，只能无奈接受，从而使法律条款的保障效果大打折扣。

2、隐私条款的不透明性

隐私政策是电商平台制定的处理用户个人信息行为的基本准则，其内容必须清晰、具体。然而，现实中大量隐私条款存在表述模糊和信息不透明的问题[2]。例如，当平台申请使用麦克风或相机权限时，往往仅以“提供更好服务”为由，而未明确告知具体的收集场景、使用情形、数据采集范围以及保存期限。这种“模糊授权”既增加了消费者个人信息被过度收集的风险，也使消费者难以判断数据处理的合

法性与必要性。这些“模糊地带”往往可能成为企业不当处理用户数据的灰色地带，导致用户在不知情下被纳入精准画像、广告推荐乃至差别定价的系统之中。

3、外部独立监督机构的缺位

为强化互联网平台关于个人信息处理的监督管理，《个人信息保护法》第 52 条要求平台设立个人信息保护负责人，第 58 条更规定用户规模巨大的互联网平台需成立由外部成员构成的独立监督机构。但从部分学者的研究中，可以发现在实践中，尽管电商平台在隐私政策中说明了个人信息保护负责人的设立，但是在例如某淘这类非常大型的电商平台均并未出现关于外部独立监督机构的相关内容[3]。也就是说，《个人信息保护法》中关于“成立主要由外部成员组成的独立机构”进行监督的规定在大型电商平台运营的实施中落空。相较于欧盟 GDPR 所强调的“数据保护官”制度，我国在制度设计上虽已迈出重要一步，但执行层面的不完善，使监管缺位问题依旧突出。

4、数据共享与跨境流转风险外溢

消费者个人信息在电商平台内部各业务环节之间流转，并在平台与广告商、第三方服务提供商等多方主体间共享，其范围与用途常常超出用户的合理预期。数据一旦进入二级乃至多级合作链条，便更可能被用于广告定向投放、市场交易甚至未经授权的转售。更为复杂的是，在跨境数据流动方面，由于各国立法标准差异较大，存在管辖权冲突与监管真空问题。部分跨境平台利用“数据灰区”进行数据转移，既可能规避本地的法律要求，也增加了信息泄露与滥用的风险。这种情况不仅侵蚀了消费者对电子商务平台的信任，也对构建协调有效的国际数据治理体系提出了更为迫切的要求。

(二) 现有法律规制的不足

1、可操作性标准缺失

我国现行法律法规，如《个人信息保护法》《网络安全法》《数据安全法》等，均明确提出个人信息处理应遵循“合法、正当、必要、最小化”的基本原则。这些原则为个人信息保护奠定了制度框架，但在具体执行层面往往缺乏统一的操作标准。例如，“必要性”应如何界定？平台是否有权收集与交易无直接关系的浏览记录？执法机关与司法机关在案件处理过程中缺少统一尺度，导致同类案件可能出现不同的裁判结果。这种不确定性不仅削弱了法律的权威性和可预期性，也增加了企业的合规成本。

2、法律规范间衔接不畅

近年来，我国在个人信息保护领域已取得突破性进展，《个人信息保护法》作为专门立法填补了长期以来的制度空白。然而，在电商场景中仍然存在多头监管与规则不一致的问题。如《消费者权益保护法》与《个人信息保护法》两部法律在平台责任认定、罚则设计方面存在差异，消保法更强调消费者权益的整体保护，而个保法则突出信息处理过程的合法性，两者在具体适用时可能造成交叉与冲突。例如同一数据泄露事件究竟适用哪部法律优先？又该如何界定“消费者权益侵害”与“个人信息侵权”的关系？这类不衔接问题易导致执法混乱，甚至被不法企业利用法律空隙规避责任。

3、事前预防与动态监管机制不健全

目前，我国在个人信息保护领域的监管模式仍以“事后处罚”为主，强调对违法行为的发现与追责，而缺少主动预防与实时监控的制度安排。监管部门通常依赖消费者举报或重大事件曝光后才介入调查，导致违法成本偏低、违法收益偏高。平台往往抱有“边违法、边纠正”的心态，缺乏主动合规的动力。与之相比，GDPR、美国《加州消费者隐私法案》(CCPA)等制度不仅重视事后处罚，还建立了数据保护影响评估(DPIA)、合规备案、数据传输审查等事前审查机制，以防患于未然。

(三) 消费者维权困境

1、举证困难与维权成本高

在用户个人信息泄露或滥用事件中，消费者常因证据获取困难而陷入维权被动。在刘某与某公司网

络侵权责任纠纷案中，刘某主张网络跨境电商平台泄露其购物交易订单及其个人信息，使其遭受诈骗电话骚扰，侵犯了个人信息权益和隐私权，但是法院认为，电商平台仅为网购过程中会接触刘某个人信息的多方主体之一，物流企业等均可能接触上述信息，且电商平台提供了其经营中已经采取的保护用户个人信息的做法和措施，在案证据尚不足以证明被告泄露了原告个人信息的事实达到民事证明标准高度盖然性的程度，故驳回了刘某的全部诉讼请求[4]。可见，电商后台的数据流转路径复杂且不透明，用户难以追踪并证明信息泄露的具体环节与平台责任。即便进入司法程序，由于举证责任倒置原则在实践中未能充分落实，消费者仍面临举证门槛高、诉讼周期长、经济与时间成本巨大的现实困境，导致维权意愿受挫。

2、侵权惩戒力度不足

当前法律对平台信息违法行为的处罚力度，与其可能获得的经济收益相比往往不成比例。实践中，即便平台泄露数百万条用户数据，也仅被处以数十万元罚款，难以形成有效震慑。根据北京市网信办的通报，2025 年北京某两家公司因未履行数据安全保护义务，导致系统存在未授权访问漏洞，大量个人信息被境外 IP 窃取。然而，最终的行政处罚结果仅为警告并处五万元罚款。这与数据泄露可能造成的巨大社会危害和企业的潜在收益相比，惩戒力度明显偏轻[5]。这种“违法成本低、收益高”的格局，客观上降低了平台主动加强数据合规的内在动力，也削弱了消费者通过赔偿获得实质救济的可能性。

3、消费者权利意识与认知有限

多数消费者对自身个人信息权益的认知仍较为有限，维权意识普遍不强。例如，平台利用算法进行差别定价、信息茧房构建、群体性标签化推荐等隐蔽性较强的行为，虽实质损害了用户的知情权与公平交易权，却常因认知门槛高、侵害感知弱而被消费者忽视或无奈接受。这种认知差距进一步加剧了消费者在数据关系中的结构性弱势。

3. 完善消费者个人信息保护的规制路径

(一) 压实平台主体责任与合规义务

电商平台作为个人信息处理的直接主体，应承担更高程度的合规责任。首先，平台应当简化隐私条款，将冗长、复杂的“法律术语”转化为通俗易懂的说明，确保用户真正理解其个人信息的使用范围。其次，应坚决禁止“默认勾选”“捆绑授权”等损害用户自主选择权的做法。在技术治理方面，应建立算法备案与透明度审查制度。平台在使用推荐算法、差别定价算法时，应定期向监管机构提交算法说明与合规性报告，避免形成“算法黑箱”。同时，应要求平台对信息安全事故承担严格的安全保障义务和赔偿责任，推动其主动建立健全内部合规审查机制。

(二) 强化技术赋能与算法审计

技术既构成潜在风险源，亦为治理提供重要路径。应积极推动隐私计算、差分隐私、联邦学习、区块链溯源等新兴技术在电商领域的落地，在保障数据流通效率的同时强化个人信息保护。例如，借助隐私计算实现“数据可用不可见”，使多方能够在不出域的前提下完成联合建模与分析；利用区块链不可篡改、全程可溯的特性，加强对数据处理行为的记录与监控，防范违规转移与恶意篡改。此外，应探索构建基于人工智能的合规预警平台，对数据操作与算法运行过程进行实时监测，及早识别异常行为并实施动态干预，增强治理的主动性和精准度。

在算法审计方面，应建立具备约束力的算法备案与透明度审查机制。审查主体可由国家网信部门牵头，联合行业协会、专家委员会及第三方技术机构共同组成。审计标准应涵盖算法的公平性、可解释性、隐私影响及用户权益影响等多个方面，并识别、纠正基于用户画像实施不合理歧视或操纵性推荐；审计程序则应包括算法功能备案、技术文档提交、模型可解释性评估、合规性评议及结论公示等环节，确保

重点算法从设计、部署到更新全周期接受监督，构建可信、可控、可审的算法应用环境。

(三) 完善立法与细化制度设计

在电商高度发展的背景下，仅依靠原则性法律条文已难以应对日益复杂的个人信息保护需求。应针对电商具体业务场景制定更具操作性的实施细则，重点对“必要性原则”的适用标准作出细化。

具体而言，可从业务功能、用户体验与安全需求等多个维度构建判断标准——在业务功能方面，仅允许收集与实现该功能直接相关且不可或缺的数据；在用户体验方面，需评估数据是否真正用于提升服务的便捷性与个性化水平，避免以“优化服务”为名过度收集信息；在安全需求方面，应识别保障交易安全所必需的数据类型，并严格限制其使用范围。

同时，应建立个人信息分类分级保护机制，对一般信息与敏感个人信息(如金融账户、健康数据、行踪轨迹等)实施差异化保护措施，对后者执行更严格的加密存储、访问权限控制与合规审计要求。

此外，跨境数据流动已成为电商的重要组成部分。我国应在《个人信息保护法》的基础上，进一步完善数据跨境流动规则，既要保障数据安全与国家利益，也要推动与欧盟 GDPR、美国 CCPA 等国际标准接轨，形成兼顾开放与安全的国际合作机制。

(四) 构建完善高效的消费者维权体系

消费者个人信息保护不仅依赖外部监管，还需要强化消费者自身的权利意识与能力。首先，应加大法律普及力度，通过多渠道宣传《个人信息保护法》《消费者权益保护法》，让消费者理解自身在信息处理中的权利与救济途径。同时，应完善公益诉讼与集体诉讼机制，降低消费者个体维权成本，形成与平台对话的组织化能力。探索建立针对个人信息侵权的行政投诉快速处理通道，构建“行政 + 司法”双轨并行的救济路径。

(五) 建立“政府–企业–社会”协同治理机制

个人信息保护涉及多方主体，单一力量难以实现有效治理。因此，应当构建政府、企业、社会三位一体的协同治理体系。政府部门应承担监管与执法职责，建立跨部门协调机制，避免监管碎片化。企业应强化行业自律，形成统一的行业标准与合规认证体系。社会组织与媒体应发挥监督与舆论引导作用，推动形成透明的公共讨论环境。同时，可试点设立用户代表参与的平台治理委员会，建立消费者直接参与监督的常设机制，增强治理过程的公开性与回应性。

参考文献

[1] 中国互联网络信息中心. 第 56 次中国互联网络发展状况统计报告[EB/OL]. 2025-07-21. https://cnnic.cn/NMediaFile/2025/0730/MAIN1753846666507QEK67ZS9DH.pdf, 2025-09-20.

[2] 刘璐. 电商平台用户隐私保护策略与路径设计研究[J]. 企业经济, 2025, 44(4): 89-97.

[3] 梁栋. 电子商务消费者个人信息保护的规范路径——基于 6 类 12 家电商平台隐私政策的实证研究[J]. 大连理工大学学报(社会科学版), 2022, 43(3): 102-112.

[4] 北京市第四中级人民法院. 刘某与某公司网络侵权责任纠纷案[EB/OL]. 2024-04-22. https://bj4zy.bjcourt.gov.cn/article/detail/2024/04/id/7907522.shtml, 2025-09-21.

[5] 央广网. 北京部分企业因未依法履行数据安全保护义务被查处[EB/OL]. 2025-06-15. https://news.cnr.cn/native/gd/kx/20250615/t20250615_527211932.shtml, 2025-09-21.