

电子商务平台数据安全困境及优化路径

蒋中婷

贵州大学法学院, 贵州 贵阳

收稿日期: 2026年8月6日; 录用日期: 2026年8月20日; 发布日期: 2026年10月22日

摘要

数字经济常态化发展背景下, 电子商务平台汇聚海量个人信息、交易数据与商业数据, 数据已然成为电商行业核心生产要素。平台数据的高效利用推动商业模式升级, 但数据泄露、过度采集、违规共享、算法滥用等安全问题持续频发, 既侵害用户信息权益, 也扰乱电商行业运行秩序。以电商平台数据安全监管为研究对象, 结合行业运行实际, 梳理当前电商领域数据安全现存现实隐患, 分析监管层面的困境与局限, 从制度完善、平台治理、技术赋能、协同监管等维度提出针对性优化对策, 以期强化电商数据全流程防护, 完善行业监管体系, 助力电商产业规范化、长效化健康发展。

关键词

电商平台, 数据安全, 智慧监管, 法律规制

The Dilemma and Optimization Path of E-Commerce Platform Data Security

Zhongting Jiang

Law School of Guizhou University, Guiyang Guizhou

Received: August 6, 2026; accepted: August 20, 2026; published: October 22, 2026

Abstract

Against the background of the normalized development of the digital economy, e-commerce platforms gather massive personal information, transaction data and commercial data. Data has become a core production factor in the e-commerce industry. The efficient utilization of platform data promotes the upgrading of business models, while security problems such as data leakage, excessive collection, illegal sharing and algorithm abuse occur frequently. These problems not only infringe on users' information rights and interests, but also disrupt the operation order of the e-commerce industry. Taking e-commerce platform data security supervision as the research object, this

paper combines the actual operation of the industry, sorts out the existing hidden dangers of data security in the current e-commerce field, and analyzes the shortcomings and limitations of supervision. Targeted optimization countermeasures are proposed from the dimensions of system improvement, platform governance, technical empowerment and collaborative supervision, so as to strengthen the whole-process protection of e-commerce data, improve the industry supervision system, and support the standardized and long-term healthy development of the e-commerce industry.

Keywords

E-Commerce Platform, Data Security, Smart Supervision, Legal Regulation

Copyright © 2026 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

互联网技术的普及与线上消费习惯的养成,推动电子商务行业进入高速扩张阶段。据国家统计局显示,2025年全国网上零售额159,722亿元,同比增长8.6%¹。从综合电商、直播带货到社交电商、跨境电商,多元业态融合发展的同时,电商平台的数据体量呈现爆发式增长。日常运营中,平台需要持续收集用户手机号、收货地址、支付信息、消费偏好等敏感内容,依托大数据分析实现精准推送、商品运营与商业决策,数据已成为电商行业核心生产要素。海量异构数据的快速沉淀与跨界流转,进一步放大了数据管理的难度与潜在隐患。

数据价值的不断攀升,使得数据安全风险随之加剧。近年来,电商平台用户信息批量泄露、黑灰产倒卖交易数据、平台私自共享商户信息、不合理算法采集隐私等事件屡见不鲜^[1],凸显了数据安全管控的紧迫性。数据安全不仅关乎普通消费者的个人隐私与财产安全,也影响中小电商经营者的商业信息安全,更关乎数字产业整体的安全稳定。各类数据隐患的持续滋生,极易破坏市场信任基础,制约电商产业的长效健康发展。

现阶段,国内已逐步搭建起数据治理相关法律框架,出台一系列针对性管理要求,对网络平台的数据处理行为作出基础性约束。但电商行业更新速度快、数据流转复杂、平台层级差异较大,传统监管模式难以适配当下的数据治理需求。监管规则落地弱化、企业安全意识薄弱、技术防护能力不足、跨部门监管衔接不畅等问题,共同造成电商数据法律安全漏洞。当前,学界围绕电商经济发展、数据营销应用、平台治理路径已形成一定研究成果,但针对电商全流程数据安全风险溯源、隐私计算技术落地适配、分层分类监管机制构建等方面仍存在研究空白,系统性、可落地的治理方案相对欠缺。聚焦电商平台数据安全现实痛点,健全常态化法律监管架构、搭建全链条数据安全防护体系,既能弥补现有研究不足,也具备较强的现实参考价值与边际贡献。

2. 电子商务平台现存数据安全问题

数字化运营背景下,电商数据流转范围持续扩大,采集、存储、应用各环节普遍存在安全隐患。当前电商数据风险隐蔽性强、类型复杂,主要集中在信息采集失序、存储防护不足、算法应用失范三方面,

¹国家统计局. 中华人民共和国 2025 年国民经济和社会发展统计公报[EB/OL].

https://www.stats.gov.cn/sj/zxfb/202602/t20260228_1962662.html, 2026-05-11.

多重问题叠加，进一步加大了数据安全治理压力。

2.1. 过度收集普遍

数据采集是电商数据治理的首要环节，也是问题高发环节。为最大化挖掘商业价值，多数电商平台存在超范围采集的现象。在用户注册、下单、授权使用功能过程中，平台通过捆绑授权、默认勾选、强制同意等方式，索取与服务无关的定位、通讯录、相册等隐私信息。部分中小电商店铺、第三方小程序电商，缺乏规范的信息采集标准，对用户敏感信息无边界收集。

同时，平台对信息采集的告知义务履行不到位，隐私政策冗长，普通用户难以清晰知晓个人数据的使用范围与去向，被动完成隐私授权，为后续数据滥用埋下隐患。平台普遍以功能升级、个性化服务为噱头，不断拓展信息收集边界，将非必要数据纳入采集范畴。很多基础购物服务仅需手机号、收货地址等基础信息即可完成，却被平台附加多项隐私权限要求[2]。普通用户在使用服务时往往缺乏仔细阅读协议的意识，为正常使用功能只能选择全盘授权。长期无差别、无节制的信息采集，使得用户隐私边界不断压缩，从源头放大了数据滥用与信息泄露的潜在风险。

2.2. 信息泄露频发

电商平台掌握海量消费者个人信息与交易数据，负有网络安全保障与信息保密义务，若安全防护缺位、技术保障不足，将直接导致用户数据被窃取、泄露，严重侵害消费者安全保障权[3]。多数中小电商经营主体片面侧重业务扩张与营收增长，对数据安全建设重视程度不足，网络防护设施配置简陋，数据加密、风险拦截、灾害备份等基础防护体系存在明显空白。日常运营中缺少常态化安全巡检，系统漏洞修复不及时，整体防御能力薄弱，外部入侵、病毒渗透引发的数据泄露事件时有发生。

电商产业链条复杂多元，平台、入驻商户、第三方服务机构联系紧密，用户数据在多方主体间频繁流动、交叉共用。行业内部尚未形成统一的数据管理标准，合作环节缺少规范约束，敏感信息随意转发、私自留存的现象普遍存在。企业内部权限管理松散，工作人员越权查阅、私自拷贝用户资料的行为难以管控，大量隐私信息经由内部渠道外流倒卖，逐步形成隐蔽化、规模化的数据灰色交易链条，持续放大整体数据安全风险。

2.3. 合规约束不足

大数据与智能算法全面融入电商运营，深度赋能精准推广、流量调配与差异化运营模式的同时，也催生诸多新型数据隐患。平台长期采集整合用户浏览轨迹、消费层级、地域特征等多维信息，依托后台模型完成用户画像搭建，借此实施差异化定价与定向营销，在无形之中侵害消费公平。部分经营主体还会借助非法爬虫工具，恶意抓取同行商品参数、定价策略及经营动态，以不正当方式抢占市场优势，扰乱行业良性竞争秩序[4]。

当前行业对于算法运行与自动化数据处理的管控力度仍有不足，现有治理要求偏向宏观笼统，未能针对数据使用范围、算法运行逻辑设置清晰边界。平台多以封闭化模式运行算法体系，运作规则不对外公开，原始数据的二次加工、跨界复用缺少合理限制。技术迭代速度较快，治理节奏难以同步跟进，各类隐蔽化的算法滥用、数据违规开发行为难以被及时发现与约束，各类新型安全隐患不断滋生蔓延。

3. 电商平台数据安全现存困境

当前我国电商平台数据安全监管已初步建立基础框架，但随着电商业态创新和数据体量扩大，监管在规则、技术、协同等方面存在突出困境，难以应对行业数据安全风险。

3.1. 监管法规细化不足

我国电商数据治理已初步形成以《中华人民共和国电子商务法》《中华人民共和国数据安全法》为核心的制度框架，为数据合规划定了基本边界。但电商业态更新速度快，直播电商、社区团购、跨境电商等新模式不断出现，数据采集、流转、应用的场景也在不断变化，现有法律体系的滞后性逐渐显现，难以实现精准监管[5]。

现行法律规范多以原则性条款为主，侧重宏观层面的指引，没有结合电商行业交易频繁、主体多样、数据敏感的特点，制定针对性的细化规则和操作标准。比如“合法、正当、必要”等法律原则在电商实际运营中，很难真正落地。对于大数据杀熟、算法黑箱、爬虫盗数等电商领域常见的违规行为，法律没有明确界定行为边界、构成要件和豁免情形，导致执法过程中认定标准不一，自由裁量空间过大。同时，现有规范未区分不同规模平台的合规要求，头部平台与小微商户、个体店铺适用同一标准，既增加了中小企业的合规成本，也让部分合规要求因脱离实际而难以落实。

此外，数据权属界定不清、数据交易规则缺失、责任划分不明确等问题，使得数据泄露、滥用等违法违规行难以精准追责，现有规定的威慑力不足，不少灰色地带行为长期得不到有效管控。基层监管部门因缺乏细化指引，面对新型数据纠纷常常无从下手，平台也容易利用规则漏洞规避合规义务，进而导致行业合规秩序松散，治理效果不佳。

3.2. 监管技术滞后

当前电商数据监管仍以线下核查、事后处罚的传统模式为主，治理方式较为被动，往往是在数据泄露、信息倒卖、违规采集等问题发生后，才开展整改和追责，事前预防和事中管控能力薄弱[6]。

电商行业依托互联网全天候运转，用户数据、交易信息、经营数据实时产生、快速流转[7]，传统的人工巡查、定期抽查等监管方式，已经无法适应数字化治理的需求。监管部门的数字化建设进度较慢，智能化监管工具配置不足，缺乏大数据筛查、智能风险识别、全链路动态追踪、异常数据预警等现代化技术手段。面对海量、碎片化的电商数据，难以实现全覆盖、全天候的动态监测，无法及时发现平台超范围采集信息、数据私下流转、后台数据异常导出等隐蔽违规行为。

技术能力的不足，直接导致监管链条出现断层，无法构建起事前预警、事中拦截、事后溯源的全流程管控体系。算法隐蔽操作、后台暗箱处理、第三方隐性数据共享等新型违规行为，能够轻易规避常规检查，持续积累安全隐患。监管技术的滞后，进一步拉大了治理能力与行业发展的差距，降低了日常监管的精准度和实效性。

3.3. 多元监管协同不足

电商数据治理涉及市场监管、网信、公安、工信等多个职能部门，各部门职责不同，监管侧重点也不一样，日常工作中容易出现职能交叉和监管空白。比如市场监管部门侧重交易环节的数据合规，网信部门聚焦网络数据安全，公安部门负责打击数据违法犯罪，工信部门监管技术层面的安全防护，分工差异易导致衔接不畅。

部分数据安全问题涉及多个治理领域，单一部门难以独立完成全链条管控，而各部门各司其职、独立执法的模式，容易形成监管重叠或管控缺位的情况[8]。同时，各部门之间缺乏稳定的信息共享和数据互通机制，监管资源分散、执法信息割裂，无法实现线索互通、联合核查、结果共用。很多时候出现违规问题，各部门各自排查，重复投入人力物力，且难以掌握完整违规链条。不同部门的执法标准和管控尺度不统一，面对同类数据违规行为，整治力度和处置方式存在差异，容易出现重复治理或监管不到位的问题。

除此之外,行业自律体系不够完善,行业协会的引导和约束作用没有充分发挥,未能形成统一的行业自律规范。电商行业内部发展不均衡,大型平台合规体系相对完善、监管较为严格,而大量中小型平台、个体店铺、小众电商小程序长期处于监管边缘,合规意识薄弱。缺乏统一的协同治理考核机制,各主体履职积极性不足,加剧了监管协同不足的问题[9]。

4. 电子商务平台数据安全监管优化解决方法

当前电商平台数据安全监管在规则、技术、协同等方面的突出困境,需从规范完善、责任落实、技术升级三个维度,构建全链条监管优化体系,破解监管难题,筑牢数据安全防护线。

4.1. 细化行业规范

结合电商行业复杂特点,完善数据安全专项管理细则,清晰划定数据采集、储存使用、对外共享及后期销毁的完整管理边界。电商行业需建立覆盖数据采集、存储、处理、共享全流程的数据治理机制,强化数据安全与合规管理,遵循合规要求规范数据使用行为。

严格恪守最小必要与合法正当原则,坚决整治捆绑授权、强制索取无关隐私信息等乱象,精简隐私协议冗长晦涩条款,切实保障用户知情同意权与自主选择权[10]。按照平台体量、经营模式实行分层管理,区分大型电商、中小商户、直播小程序等不同主体,设置适配的合规要求。针对跨境经营场景,单独约束跨境数据传输行为,严防敏感信息外流,填补细分领域监管漏洞。

依托现有规定,贴合电商交易场景完善落地细则,细化日常数据处理的操作规范,划定违规收集、私自流转数据的监管底线。明确数据全生命周期各环节禁止性条款与合规准则,压实平台内控管理责任,形成可执行、可核查的常态化管控依据。电商平台应立足场景特征细化数据处理规范,强化数据隐私保护与合规管理,同步适应行业新业态、新模式迭代,持续完善合规体系[11]。紧跟直播电商、即时零售等新兴模式发展,及时补齐监管空白内容,常态化优化管理制度,保持规则适配行业变化,方便监管落地执行,也为平台日常合规管理提供清晰参照。

4.2. 强化平台主体责任

压实电商平台数据安全责任,督促企业健全内部数据安全管理机制,落实数据分级分类管理要求,对身份证、支付信息、收货地址等敏感数据,采取专项加密措施做好防护[12]。要求企业加大网络安全技术投入,升级服务器防护设备,建立数据实时备份和应急处置机制,有效防范黑客入侵、病毒攻击引发的数据泄露和丢失问题。

规范企业内部数据权限管控,严格限定员工数据访问范围,遵循最小权限原则实行分级授权。留存完整操作日志,实现行为可追溯、可审计,从源头杜绝内部人员违规导出、倒卖用户数据的行为。开展常态化合规培训和安全自查,定期组织学习与内部排查。引导平台规范算法使用,公开算法运行基本规则,明晰算法决策逻辑与应用边界,杜绝大数据杀熟、非法爬虫抓取等违规行为,强化行业自律。

明确平台对入驻商家、第三方服务机构的管理责任,建立严格的合作方准入审核机制,重点核验数据安全防护资质与合规能力。签订数据保密协议,全程监管合作方的数据使用行为。建立数据安全考核评价体系,将合规情况与平台资质、信用评级挂钩。细化考核指标、实行量化评分,对合规落实不到位的平台,采取约谈、限期整改、行政处罚等措施,倒逼平台主动履行主体责任,形成自我约束、自我规范的良性循环。

4.3. 升级智慧监管手段

推动监管数字化转型,搭建电商数据安全智能监测平台,运用大数据、人工智能技术,实时监测平

台数据采集、流转及异常访问情况,及时发出风险预警,实现监管从被动查处向事前防控、事中管控转变[13]。平台重点监测超范围采集、违规共享等高频问题,对异常数据操作快速识别、精准定位,打破传统监管的滞后性局限。

打通网信、市监、公安、工信等部门的信息共享渠道,建立联动执法机制,开展联合专项整治,集中打击数据泄露、信息倒卖、违规共享等违法行为。可引入联邦学习、差分隐私等隐私计算技术构建跨域协同监管体系。依托联邦学习分布式建模优势,各部门、各电商平台无需上传原始隐私数据,仅同步模型参数即可开展联合风险研判,规避数据集中归集带来的泄露风险。借助差分隐私算法对监测数据流添加合理噪声扰动,在保留数据统计特征、保障监管可用性的前提下,实现用户个人信息隐私有效保护[14]。两类技术存在算法研发、算力部署与专业运维的较高技术门槛,前期硬件集群、算法适配投入成本偏高,后期可通过财政专项拨款、行业共建共享算力、统一技术标准等方式摊薄应用成本。

加大监管技术投入,升级监测工具,提升对算法隐蔽操作、数据异常流转等新型违规行为的识别能力,实现数据全链路动态追踪。依托监测平台建立预警机制,及时推送风险隐患并督促整改,同时加强监管人员数字化技能培训,确保智慧监管手段落地见效,提升监管精准度和效率。结合电商数据特点优化监测算法,定期更新监测指标,适配直播电商等新兴业态的监管需求,持续适配隐私计算模型应用场景,让智慧监管既贴合电商行业发展实际,又在技术合规、隐私保护层面具备长效性与前瞻性,让智慧监管真正贴合行业实际、发挥实效。

5. 结语

数据是电子商务行业持续发展的核心动力,数据安全更是行业稳定运行的底线要求。当前我国电商平台在数据处理全链条中,仍存在采集失范、防护薄弱、算法滥用等多重安全隐患,叠加监管规则滞后、技术手段不足、协同治理欠缺等现实问题,电商数据安全风险防控形势依旧严峻。数字经济快速发展背景下,电商数据规模持续扩张,数据应用场景愈发复杂,各类隐蔽化、常态化的数据风险不断滋生,进一步加大了安全治理的难度。

完善电商平台数据安全法律监管体系,既要依托制度建设补齐规则短板,贴合电商多元业态特点细化治理要求;也要依托技术升级实现智慧监管,压实企业内部安全防护责任。合理划分政府、平台、行业主体的治理职责,理顺监管权责,打通部门协作壁垒,构建衔接顺畅的治理格局。通过制度约束、技术防护、多元协同、社会监督的多重发力,平衡数据合理利用与安全防护的关系,既能充分释放数据要素的商业价值,又能全面保障用户与经营者的信息安全,有效化解各类数据安全隐患,维护网络交易秩序,最终推动电子商务行业在安全、规范的环境中实现长效高质量发展。

参考文献

- [1] 李增辉, 赵甜. 大数据背景下电子商务企业管理问题及对策[J]. 商场现代化, 2025(9): 39-41.
- [2] 孙晋, 万召宗. 滥用市场支配地位侵犯隐私行为的反垄断法规制[J]. 财经法学, 2021(5): 3-16.
- [3] 蓝寿荣. 消法视角下的电子商务平台安全保障义务[J]. 政法论丛, 2023(2): 37-46.
- [4] 熊浩, 张晨, 鄢慧丽. 监管与市场调节下大数据杀熟治理的演化博弈研究[J/OL]. 海南大学学报(社会科学版), 2025. <https://doi.org/10.15886/j.cnki.hnus.202410.0119>, 2026-04-28.
- [5] 张钦昱. 电子商务平台治理的理念转型与制度调适[J]. 法学评论, 2025, 43(6): 145-156.
- [6] 越嫫. 数字化背景下平台经济发展合规路径探索[J]. 金融客, 2024(3): 30-32+3.
- [7] 余成峰. 数字平台监管模式的系统论重构[J]. 中国法学, 2025(5): 84-103.
- [8] 王岭. 数字经济时代中国政府监管转型研究[J]. 管理世界, 2024, 40(3): 110-126+204+127.
- [9] 蒋敏娟, 汪睿. “共享性链接”: 平台经济跨部门协同监管何以可能——基于 B 市 S 区互联网经济协同监管平台

的案例研究[J]. 甘肃行政学院学报, 2026(1): 49-59.

- [10] 武腾. 最小必要原则在平台处理个人信息实践中的适用[J]. 法学研究, 2021, 43(6): 71-89.
- [11] 潘春会. 大数据驱动下的电商行业发展与应用研究[J]. 活力, 2024, 42(3): 28-30.
- [12] 李三希, 刘希, 张明圣. 数据网络外部性与垄断平台数据收集[J]. 经济研究, 2025, 60(10): 61-82.
- [13] 陆进宇, 赵花蕊, 马晓威, 等. 以智慧监管助推平台经济规范健康发展[J]. 中国信息化, 2023(7): 5-8.
- [14] 刘泽刚. 人工智能时代联邦学习隐私保护的局限及克服[J]. 中外法学, 2025, 37(1): 65-84.