E-Commerce Letters 电子商务评论, 2026, 15(5), 891-897
Published Online May 2026 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2026.155590

Hans汉斯

我国电商平台数据安全风险治理：现状及对策研究

赖荣辉

江苏大学管理学院，江苏 镇江

收稿日期：2026年3月10日；录用日期：2026年3月25日；发布日期：2026年5月29日

摘　要

电子商务已深度融入我国经济社会生活的方方面面，平台在运营中积累的海量用户敏感数据，潜藏着泄露、滥用等安全风险，数据安全问题日益受到社会各界关注。本文深入探讨了我国电商平台数据安全风险治理的现状并提出了相应的治理对策。尽管我国已从法律与监管规制、行业管理和技术防护三大治理途径搭建起了多维度治理框架，但现有的治理途径仍然存在问题。基于此，本文针对目前治理途径存在的问题从三个方面提出了针对性对策，旨在为电商平台筑牢数据安全防线、推动行业高质量发展提供有益参考。

关键词

电商平台，数据安全，风险治理

Research on the Current Situation and Countermeasures of Data Security Risk Governance in E-Commerce Platforms in China

Ronghui Lai

School of Management, Jiangsu University, Zhenjiang Jiangsu

Received: March 10, 2026; accepted: March 25, 2026; published: May 29, 2026

Abstract

E-commerce has been deeply integrated into all aspects of China's economic and social life. The

文章引用: 赖荣辉. 我国电商平台数据安全风险治理：现状及对策研究[J]. 电子商务评论, 2026, 15(5): 891-897.
DOI: 10.12677/ecl.2026.155590

massive volume of sensitive user data accumulated by platforms during operation entails potential security risks such as data leakage and abuse, and data security issues have attracted growing attention from all sectors of society. This paper conducts an in-depth analysis of the current status of data security risk governance in China's e-commerce platforms and proposes corresponding governance strategies. Although a multi-dimensional governance framework has been established in China through three major approaches: legal and regulatory governance, industry administration, and technical protection, deficiencies still exist in the current governance practice. Accordingly, this paper proposes targeted countermeasures from three aspects in response to the existing problems of such approaches, aiming to provide useful references for e-commerce platforms to consolidate data security defenses and promote the high-quality development of the industry.

Keywords

E-Commerce Platforms, Data Security, Risk Governance

1. 引言

中国第一个电子商务平台最早可追溯到 1997 年夏天，2008 年之后电商行业开始迅猛发展，市场规模不断扩大且模式持续创新；在 2020 年，电商行业更是迎来新一轮爆发，线上消费习惯进一步普及，数字化零售格局也由此加速成型。截至 2025 年 6 月，我国网络购物用户规模达 9.76 亿人，电子商务已深度普及并已成为居民生活的重要组成部分[1]。同时，电商平台在为用户提供便捷购物体验的同时，会收集海量敏感数据，包括个人身份信息、交易记录和行为轨迹等，这些数据虽是平台精准营销、优化服务、提升竞争力的核心要素，但同时也极易产生数据安全风险，如数据泄露。一旦此类风险演变为数据安全事件可能会给用户造成直接经济损失，还可能引发用户对平台的信任危机[2]。

基于此，国家出台了数据安全相关的法律法规，规定了电商平台及其经营者应该对保护电商交易过程中产生的大量行为及信息数据所承担的责任，行业整体的数据安全意识慢慢提高。另外，部分电商平台为扩大用户规模、维护消费者合法权益、提升平台信誉与用户粘性，主动就数据保护达成一致意见，并积极运用新技术保护电商环境中流通的各类数据安全，这改善了电商平台数据安全状况。但现阶段电商平台面临的数据安全风险日益呈现出类型多元、隐蔽性凸显、波及范围广的复杂态势。一方面，黑客攻击手段持续迭代升级，网络攻击的精准度与破坏力不断提升；另一方面，平台内部管理疏漏频发，加之部分平台秉持“重盈利、轻安全”的发展理念，数据安全防护体系建设滞后，致使数据泄露、滥用等数据安全事件仍不时发生。在此背景下，探讨电商平台数据安全风险治理现状，剖析现存问题，提出有效的治理对策，不仅是电商平台应对数据安全挑战与筑牢安全运营底线的内在需求，更是维护数字经济安全稳定运行的关键举措。

2. 国内电商平台数据安全研究综述

电商平台数据安全是指在电子商务交易全流程中所产生各类数据的安全性[3]。随着我国数字经济与电商行业的快速发展，国内不少数学者针对电商平台数据安全展开研究，研究的出发点基于以下几个层面。

技术层面。武浩婕指出，同态加密技术可有效保护电商平台数据安全，该技术支持对加密状态下的敏感数据直接计算，无需解密即可得到有效结果，让平台在业务操作中全程保持数据加密，从而降低处理环节的数据泄露与滥用风险；同时能实现隐私保护下的多方数据融合共享，兼顾数据安全与流通利用价值[4]。张卫斌等针对电商平台数据安全问题提出应对策略，提出应强化技术研发，推动政府与电商平台企业协同加大技术投入，研发大数据保密相关技术、搭建安全防火墙，从技术层面防范数据泄露风险[5]。闫宇飞指出通过 DSE (Data Security Encryption)算法构建私人密钥、RSA (Rivest-Shamir-Adleman)算法构建公开密钥，为不同类型数据设置针对性的加密保护，可以很好防止电商平台数据在传输、存储过程中被窃取，并实现数据的安全防护[6]。崔晓萌等提出运用入侵检测技术保障电商平台数据安全，通过旁路部署入侵检测系统，依托规则库检测网络异常攻击流量，结合事务生成器、分析器等模块完成入侵行为的识别、预警与记录，及时发现并响应非法网络入侵行为，从网络访问层面防范电商平台数据被恶意攻击、盗取，并守护数据安全[7]。

法律层面。杨熙针对电商平台数据泄露问题展开研究，发现电商平台法律责任不明确等问题，并强调应完善电商平台的信息泄露防范义务规定和明确电商平台的法律责任[8]。徐可行从法律层面提出，电商平台经营者的安全保障义务范畴还需明确包含平台信息安全保护，要求信息服务、撮合交易类电商平台分别履行对应的信息保护、交易全程信息安全保障等法定义务，以此强化电商平台数据安全的法律约束[9]。刘雪营等通过对比《中华人民共和国电子商务法》和《中华人民共和网络安全法》(后文简称《电子商务法》和《网络安全法》)关于个人信息保护发现，《电子商务法》细化了电商平台个人信息删除权的行使规则，取消了《网络安全法》中违法违约的前置条件，还明确了信息删除的程序与方式，以此强化电商平台个人数据安全的法律保护要求[10]。吴健强发现电商平台数据安全面临现行立法体系适配性不足的问题，《中华人民共和国个人信息保护法》实施后虽推动了电商领域个人信息保护，但相关法律规定未充分考量电子商务行业特征，立法间缺乏有效衔接与协调，致使电商平台消费者个人信息保护工作难以落地，亟需明确电商消费者个人信息法律地位，强化信息全流程法律规范，实现立法与电商行业特征、复杂性的适配[11]。

管理层面。孟曙艳提出，电商平台需构建多层级的电子商务安全体系结构保障数据安全，该体系融合加密技术层、安全认证层、交易协议层等核心层级，通过各层级协同配合、控制技术层层递增的管理逻辑，为电商信息管理系统的数据传输、存储和交易全流程筑牢安全防护屏障[12]。潘思谕等指出电商平台需由相关部门完善用户信息安全管理制度，将数据安全风险防范纳入平台顶层设计，明确各层级员工的数据访问权限范围，同时建立信息安全等级保护框架并定期开展风险评估，把数据安全维护纳入绩效考核，从制度层面筑牢跨境电商平台的数据安全防线[13]。

风险治理层面。陈晓钰指出电商平台兼具商业属性与公共属性，其数据安全风险治理涉及政府监管部门、平台企业等多方主体，各主体在数据安全治理中的诉求、权责与行为逻辑存在显著差异，形成了复杂的权责交织关系，导致主体间协同难度大，难以形成治理合力[3]。数据安全风险治理也需要考虑电商平台自身的网络属性带来的挑战，王红指出，电商平台依托网络空间实现运营与数据流转，其跨地域、开放性、互联互通的网络本质成为数据安全风险滋生的天然载体，数字技术的快速迭代下，网络攻击手段从传统的代码注入向供应链攻击等新型手段演变[14]。另外，电商平台数据安全风险治理面临安全防护与流通利用的平衡难题，数据需在多主体间流通以释放价值，但流转环节增多、管控链条延长，且不同主体安全能力不一，极易造成数据泄露与滥用[15]。

杨昌慧发现，当前电商平台内部数据安全风险内控治理存在短板，核心体现在内部审查制度的建设与执行层面，平台未针对数据流转全流程建立精细化审查机制，也缺乏专人开展实时的合规检测与风险把控，这成为数据安全风险的重要诱因[16]。何玉华发现，电商平台内部数据安全管理体系中，业务部门

与安全管理部门的职责划分较为模糊，业务部门侧重运营效率与用户体验，安全部门聚焦数据风险治理与合规管控，二者目标导向的本质冲突，使得数据安全管理措施落地执行受阻，难以形成数据风险协同治理的有效合力。另外，他还指出当前大部分电商平台既未配备专职的数据合规岗、隐私保护岗与数据审计岗，也未明确各岗位在风险治理中的核心职责，仅由技术部门人员兼职承担相关工作，这大幅增加了数据泄露、滥用的安全风险[17]。

基于上述综述，可以得知现有研究有从单一角度出发针对电商平台数据安全展开研究，也有从更加宏观的风险治理层面展开研究。回顾相关研究一定程度上为下文探讨电商平台数据安全风险治理现状、剖析现存问题和提出有效的治理对策提供有益的参考框架。

3. 我国电商平台数据安全核心风险类型

电商平台的交易流程长且涉及合作方多，数据流转的每一个环节都可能蕴含安全风险。在探讨我国电商平台数据安全风险治理现状之前，需先行厘清我国电商平台数据安全核心风险类型。

3.1. 外部黑客攻击导致的数据盗取风险

这是我国电商平台最常遇到的外部安全问题，黑客和不法团伙常会用代码注入、网络瘫痪攻击、钓鱼链接、恶意爬取等手段，入侵平台的安全防线，窃取用户手机号、住址、支付信息等隐私数据，甚至会锁住平台核心数据，要挟平台支付赎金。现在针对电商平台的网络攻击日益呈现规模化、精准化特征，攻击者专门针对平台系统漏洞与应用接口漏洞实施入侵，一旦成功入侵，不仅海量数据会泄露和被篡改，导致用户财产受损，还会让平台系统崩溃，无法正常运营。值得注意的是，由于跨境电商及中小型电商企业的安全防护体系建设相对薄弱，它们更易成为此类攻击的对象。

3.2. 电商平台内部管理不严导致的数据滥用与泄露风险

电商平台因内部管理不严所引发的数据滥用与泄露风险，具有较强的隐蔽性，已成为当前数据安全领域的高发隐患。这类风险本质上源于平台内部数据安全管控体系存在缺陷，其具体表现为：数据权限管控较为粗放，未建立精细化分级分类管理机制，电商平台内部员工与运营人员存在越权调取敏感数据的可能，部分人员受利益驱动违规滥用数据，或因操作疏忽造成数据泄露；电商平台内部制度执行缺位，常态化数据安全培训与责任追究机制不健全，数据操作全程留痕、可追溯和可审计的监管体系不够完善，进一步加剧了因内部管理不严带来的数据泄露与滥用风险。

3.3. 第三方合作方数据泄露风险

电商平台业务运营高度依赖支付结算、物流配送、技术服务和营销推广等第三方合作主体，核心数据跨主体流转频次较高且范围较广，第三方合作方已成为数据泄露风险的重要传导节点，此类风险兼具跨主体和难管控的双重特性，是我国电商平台数据安全治理的重点与难点。从平台管控层面来看，部分电商平台未建立健全数据共享审核与全流程安全管控机制，且合作双方数据安全权责、使用边界及保密义务界定相对模糊，仅通过简易协议约束权责。同时，平台缺乏对合作方安全资质、防护能力的前置审核与动态监管。上述管控问题可能导致数据跨主体流转时防护缺位，进而导致泄露风险升高。从合作方自身层面来看，多数中小服务商数据安全防护体系不完善、防护技术薄弱且内部管理松散，很难落实数据加密、权限管控、安全审计等防护要求，易成为黑客攻击目标从而更易引发数据泄露。

4. 我国电商平台数据安全风险治理的现状及存在的问题

在数字经济发展与数据安全监管趋严的双重背景下，我国电商平台数据安全风险治理依托法律和监

管规制、行业管理和技术防护三大治理途径搭建起多维度治理框架，为降低电商平台数据安全风险提供了有力支撑。但基于法律和监管规制、行业管理和技术防护三大治理途径仍然存在问题。

4.1. 法律与监管规制的治理现状及存在的问题

法律途径是电商平台数据安全风险治理的重要制度保障，依托法治建设筑牢行业合规治理根基。近年来，我国数据安全领域立法进程持续加快，逐步构建起以《电子商务法》和《中华人民共和国数据安全法》(后文简称《数据安全法》)为核心、且以配套细则与规章为补充的立体化法治体系。这一体系清晰界定了电商平台在数据全生命周期各环节的法定义务，明确了平台的数据安全主体责任、权责划分标准与违法惩戒机制，有效完善了电商行业数据安全治理的法律规制体系。与此同时，网信、市场监管和公安等多部门建立协同监管机制，开展电商数据安全专项整治行动，聚焦非法泄露或滥用数据等违法行为并依法查处与追责，以监管约束促使平台严守合规底线，推动行业数据安全治理逐步迈向法治化、规范化轨道。

问题导向的治理逻辑贯穿各领域发展进程，均以发现问题为先导，再针对性完善，与电商平台数据安全相关的法律也是如此。尽管我国已相继出台《电子商务法》和《数据安全法》等法律法规，为电商平台数据处理提供了明确的制度框架，但在实际执行过程中，仍然存在着问题。其一，针对数据收集、存储、使用及共享等各个环节的规范缺乏足够的细致性，导致电商平台在实际操作中拥有较大的自由裁量空间[18]。其二，在发生数据隐私侵权事件时，责任认定及处罚标准不明确，致使违法违规成本较低，无法对电商平台形成有效约束[19] [20]。其三，法律规制对第三方合作方的风险覆盖明显不足，例如《电子商务法》未明确第三方合作方的数据安全防护义务，也未细化平台与第三方在数据流转中的权责划分，这极易引发第三方合作方数据泄露风险。另外，当前我国电商平台数据安全监管存在执行性短板，主要体现在监管体制层面尚未设立独立的数据安全保护行政机构，数据安全保护监管职能分散于网信、市场监管和公安等多个部门导致监管职能分散、权责边界模糊[21]。

4.2. 行业内部管理的治理现状及存在的问题

行业内部管理是落实数据安全治理责任的重要支撑，通过行业自律与平台内控双向发力以提高治理效能。行业层面，电商行业协会及相关联盟组织发挥引导协调作用，通过制定行业数据安全自律公约与合规操作指引、统一行业数据处理行为规范和规范第三方合作方的数据处理行为等，以营造行业共治的良好治理氛围。早在2002年，中国互联网协会就已发布自律公约，明确倡议全行业企业应自觉维护用户权益、严格保护用户信息安全，不得擅自使用所收集数据，更不得利用行业优势地位损害消费者权益，这为行业数据合规自律提供了早期实践范例。平台层面，头部电商平台主动落实其主体责任。通过建立专业的数据安全管理架构，并完善数据权限管控、操作规范及合作方准入审核以细化对数据全生命周期的管理。

当前行业内部管理仍存在着问题。一方面，体现在行业自律规则体系失范上，行业数据安全自律公约与合规操作指引的制定往往缺乏法律所需的严谨程序，如公开征集意见和多部门协调等，其形成过程通常由少数企业代表闭门协商完成，内容更倾向于维护行业利益，对用户权益的考量明显不足。潘煜萌发现某电商行业协会制定的“个人信息处理自律规范”中，对“必要信息”的界定标准模糊，仅笼统提及“基于业务必需”，未明确具体范围和判定依据，且未规定企业违规的内部惩戒措施，导致所制定的规范沦为形式化的宣言[19]。另一方面，体现在电商平台管理执行疏漏上，部分电商平台虽搭建了数据安全管理架构，但实际内控执行流于形式，数据权限审批等关键环节管控不严，容易引发内部人员违规调取、泄露用户数据等问题，进而引发数据滥用、信息泄露等安全风险。

4.3. 技术防护手段的治理现状及存在的问题

技术途径是抵御数据安全风险有效途径[6]。当前电商平台通过部署针对性技术手段以识别、防范与应对数据安全风险。目前常见的技术路径包括：借助防火墙、入侵检测等工具加强网络边界的监控与防护；通过数据加密、访问控制及数据库安全机制，在关键环节设置风险管控点；利用生物识别、多因素认证等方式提升身份验证的可靠性，防范越权操作；并结合安全审计、日志分析及定期备份等手段，增强操作可追溯性与系统可恢复性。这些技术从网络防护和数据保护等环节，为平台应对不同类型数据安全风险提供了工具支持。

与近些年平台数据被侵入的速度相比，现有的技术防护手段尚不能成为电商平台的“金钟罩”。这很大程度上是因为目前的技术防护手段存在以下问题。其一，各类防护手段碎片化部署且单独运行，且未形成协同联动的防护体系。现有防火墙和数据加密等治理技术，大多只能实现单一维度的防护功能，针对平台全流程数据流转的包容性和兼容性不足，各类技术之间难以互通联动。当各类治理技术配合效益有限，且技术之间难以关联，难以保证电子商务时代的数据安全[22]。其二，技术应用水平不均衡，头部电商平台技术投入充足，防护技术比较成熟完善，中小电商平台因资金不足、投入有限，存在技术能力薄弱、防护体系不完善等问题，这意味着在应对外部攻击时，中小电商平台更容易引发数据盗取风险。《2025 年上半年数据泄露风险态势报告》显示，中小电商平台因安全防护能力不足，往往更容易发生数据盗取等安全事件[23]。

5. 我国电商平台数据安全风险治理优化对策

结合我国电商平台数据安全风险治理存在的问题，针对性提出以下优化对策，以推动数据安全治理效能提升。

5.1. 完善法律规制并强化监管执行

针对法律层面上存在数据全环节规范不够细致等问题，以及监管层面上存在职能分散和权责边界模糊的问题，需从立法细化与监管优化双向发力。一方面，细化数据收集、存储、使用及共享全环节操作规范，明确用户授权方式、数据留存期限、共享脱敏要求等具体合规标准，压缩电商平台自由裁量空间；明确数据隐私侵权的责任认定细则与处罚标准，按泄露数据量级、敏感程度、主观过错设置阶梯式处罚，提高违法违规成本，强化对平台的法律约束效力；同时补齐第三方合作方的规制短板，明确其数据安全防护义务，细化平台与第三方在数据流转中的权责划分，建立合作方准入审查、全程审计与连带追责机制，防范合作环节数据泄露风险。另一方面，理顺监管体制，明晰网信、市场监管、公安等部门的监管权责边界，健全跨部门协同监管机制，填补监管职能分散带来的执行漏洞，提升监管规范化与执行力。

5.2. 规范行业自律并加强平台内控

针对行业自律规则体系失范与平台内控管理执行疏漏问题，需从自律约束与内部管控双向完善。一方面，规范行业自律规范制定流程，落实公开征集意见、多部门协调等严谨程序，平衡行业利益与用户权益；细化自律条款，明确“必要信息”具体范围和判定依据，增设企业违规内部惩戒措施，解决自律形式化、空心化问题，让行业自律真正发挥约束效力。另一方面，强化平台内部管理执行力度，严格落实数据权限审批等关键内控环节，防止内控执行流于形式，从源头上防范内部数据滥用与信息泄露风险，切实提升平台自身数据安全治理能力。

5.3. 整合技术资源均衡防护能力

针对技术防护碎片化部署、单独运行无协同联动体系、以及技术应用水平不均衡的问题，需构建有

效的防护体系。一方面，整合防火墙、入侵检测、数据加密、访问控制、安全审计等各类防护技术，避免单一孤立部署模式，搭建互通联动的一体化防护体系，提升技术兼容性与全流程防护能力。另一方面，通过政府、行业、市场等多方协同，缓解中小平台在数据安全投入方面的压力。例如，政府可通过财政补贴、税收优惠等措施提供支持，并开放部分公共技术检测与咨询服务；头部平台可适度开放成熟技术体系，输出适配性较强的定制化防护方案；市场可鼓励研发轻量化、模块化防护产品，具体包括云端安全服务、一体化在线防护系统等，以提升优质技术对中小平台的可用性，促进数据安全防护技术的普及应用。

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]. https://www.cnnic.net.cn/n4/2025/0721/c326-11327.html, 2025-07-21.

[2] 王丽娜, 尚明瑞. 电子商务时代数字化营销现状与路径研究[J]. 电子商务评论, 2025, 14(1): 2777-2781.

[3] 陈晓钰. 电商平台数据安全风险治理研究[D]: [硕士学位论文]. 哈尔滨: 黑龙江大学, 2023.

[4] 武浩婕. 电子商务领域消费者个人信息安全生态化保障机制研究[J]. 中国商论, 2025, 34(6): 121-124.

[5] 张卫彬, 陈计. 我国跨境电商中网络用户个人信息保护的困境与路径[J]. 河南理工大学学报(社会科学版), 2023, 24(6): 29-36.

[6] 闫宇飞. 电子商务时代信息安全保护技术探讨[J]. 电脑知识与技术, 2015, 11(6): 248-249.

[7] 崔晓萌, 田思雨. 计算机网络安全技术在电子商务中的应用[J]. 信息与电脑(理论版), 2024, 36(5): 221-223.

[8] 杨熙. 电商平台的信息泄露防范义务研究[J]. 商场现代化, 2020(8): 32-33.

[9] 徐可行. 试论电子商务平台经营者的安全保障义务[J]. 中国商论, 2022(13): 57-59.

[10] 刘雪营, 胡天琦. 《电子商务法》对个人信息保护及经营者风险防范研究[J]. 法制与经济, 2019(2): 90-91.

[11] 吴健强. 电子商务消费者个人信息法律保护问题研究[D]: [硕士学位论文]. 哈尔滨: 哈尔滨商业大学, 2024.

[12] 孟曙艳. 电子商务信息管理系统数据的安全性[J]. 电子商务, 2017(12): 51-52.

[13] 潘思谕, 黄紫华. 数字经济下跨境电商平台的用户信息安全风险防范策略[J]. 沿海企业与科技, 2022(3): 17-22.

[14] 王红. 大数据时代跨境电商网络安全风险及防范措施研究[J]. 科技经济市场, 2024(11): 131-133.

[15] 赵雅晴. 基于定制产品背景的电商平台信息共享与安全策略研究[D]: [硕士学位论文]. 天津: 天津大学, 2024.

[16] 杨昌慧. 大数据背景下电商平台的数据伦理问题及应对措施[J]. 老字号品牌营销, 2022(9): 54-56.

[17] 何玉华. K 钢铁集团电子商务系统数据安全管理研究[D]: [硕士学位论文]. 昆明: 云南大学, 2018.

[18] 段玉清. 电商平台消费者数据隐私保护的困境及应对策略研究[J]. 商业 2.0, 2025(13): 64-66.

[19] 潘煜萌. 电商平台中的个人信息保护研究[D]: [硕士学位论文]. 银川: 北方民族大学, 2025.

[20] 孙莹. 大规模侵害个人信息高额罚款研究[J]. 中国法学, 2020(5): 106-126.

[21] 张平. 大数据时代个人信息保护的立法选择[J]. 北京大学学报(哲学社会科学版), 2017, 54(3): 143-151.

[22] 刘璐. 电商平台用户隐私保护策略与路径设计研究——基于国内主流电商平台隐私条款的分析[J]. 企业经济, 2025, 44(4): 89-97.

[23] 威胁猎人. 2025 年上半年数据泄露风险态势报告[EB/OL]. https://www.threathunter.cn/blog/2025, 2026-05-26.