

论电子商务平台的数据安全保障义务

郭 洋

贵州大学法学院, 贵州 贵阳

收稿日期: 2024年12月2日; 录用日期: 2024年12月13日; 发布日期: 2025年1月21日

摘 要

随着电商经济的蓬勃发展, 电子商务平台积累了大量的用户数据和交易信息, 这些数据的安全性和隐私保护成为亟待解决的问题。电子商务平台作为数据的收集、存储和处理主体, 承担着重要的数据安全保障义务。为确保用户数据的安全与隐私, 电商平台需构建健全的数据安全管理体系, 强化数据加密、访问控制及应急响应等关键措施, 以应对日益复杂的数据安全挑战, 为电商经济的稳健发展奠定坚实基础。

关键词

电商经济, 电商平台, 数据安全, 安全保障义务

On the Data Security Assurance Obligations of E-Commerce Platforms

Yang Guo

Law School of Guizhou University, Guiyang Guizhou

Received: Dec. 2nd, 2024; accepted: Dec. 13th, 2024; published: Jan. 21st, 2025

Abstract

With the vigorous development of the e-commerce economy, e-commerce platforms have accumulated a large amount of user data and transaction information, and the security and privacy protection of these data have become an urgent problem to be solved. As the main body of data collection, storage and processing, e-commerce platforms bear important data security obligations. In order to ensure the security and privacy of user data, e-commerce platforms need to build a sound data security management system and strengthen key measures such as data encryption, access control and emergency response to cope with increasingly complex data security challenges and lay a solid foundation for the steady development of the e-commerce economy.

Keywords

E-Commerce Economy, E-Commerce Platform, Data Security, Security Obligations

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 21 世纪的数字时代，电商经济成为国民经济的新兴力量，电子商务平台也成为现代经济体系中不可或缺的重要部分。电子商务凭借其规模大、覆盖范围广、创新创业活跃等优势，不仅改变了传统的商业模式，还对国内外市场及社会经济产生了深远的影响。星图数据发布的《2024 年双十一全网销售数据报告》中显示，2024 年双十一期间，综合电商平台与直播电商平台累计销售额达到了 14,418 亿元，同比增长 26.6%。从销售份额来看，天猫淘宝占比为 38%，京东为 20%，抖音为 13%，拼多多为 10%，16 载双 11，由最初的天猫一枝独秀，发展到目前的群雄逐鹿。¹从近年来的数据可以看出，电商交易持续火热，在扩大内需、促进数实融合等方面发挥了积极作用，为促消费、稳增长提供了重要动力。

然而，随着电子商务的迅猛发展，数据安全问题也日益凸显。电子商务平台掌握着大量的用户信息和交易数据，这些数据的安全不仅关系到消费者的个人隐私和财产安全，还直接影响到电子商务平台的信誉和可持续发展。因此，电子商务平台的数据安全保障义务显得尤为重要。电子商务平台在履行数据安全保障义务方面，面临着诸多挑战。一方面，随着技术的不断发展，黑客攻击、病毒传播等网络安全威胁日益复杂多变，电子商务平台需要不断更新和完善其安全防护措施。另一方面，电子商务平台在保障数据安全的同时，还需要兼顾用户体验和运营效率，确保在保障安全的前提下，不影响用户的正常使用和交易的顺利进行。

因此，探讨电子商务平台的数据安全保障义务，不仅具有重要的理论意义，还具有深远的实践意义。本文将从法律法规、技术保障、挑战与应对等多个方面，深入剖析电子商务平台的数据安全保障义务，以为电子商务平台的可持续发展提供有益的参考和借鉴。

2. 电商平台的数据安全保障义务的理论基础

2.1. 信赖保护理论

电商平台与用户之间存在一种基于信赖的契约关系。用户选择在该平台进行交易，是基于对平台安全性的信赖。因此，电商平台有责任维护这种信赖关系，确保用户数据的安全。安全保障义务是我国民法上一项相对比较成熟的制度，主要源于法律法规的直接规定以及合同中的明确约定。它是指经营者在经营场所对消费者、潜在的消费者或其他进入服务场所的人之人身、财产安全依法承担的安全保障义务。该义务要求经营者采取合理措施，预防和控制可能发生的危险，以保护他人的人身和财产安全。如果经营者未尽到安全保障义务，造成他人损害，则需承担相应的法律责任^[1]。随着互联网的迅速发展，网络空间已成为人们日常生活的重要组成部分，其社会性和公共性日益显著。因此，将安全保障义务扩展到网络空间，不仅是理论发展的需要，也是实务发展的迫切需要。网络空间与现实空间一样，具有公共性、群众性和开放性，是网民互联、互通、共享的场所，也存在对公众的财产与人身造成侵害的可能性。网

¹ 来源于复旦大学消费大数据实验室发布《2024 年“双 11”线上消费数据观察》。

络平台经营者通过技术手段可以精准掌握进入平台空间的用户情况，并对其在网络空间的行为予以控制，因此有必要承担相应的安全保障义务。网络空间虽是虚拟空间，但使用网络空间的主体是现实存在的人们，网络秩序同样是社会公共秩序的重要组成部分，其影响范围可能比现实空间更广泛，影响程度亦可能比现实空间更大[2]。

2.2. 法律法规要求

除了理论基础外，电商平台的数据安全保障义务还受到法律法规的明确约束。电子商务平台的数据安全保障义务主要源于相关法律法规的规定。例如《电子商务法》第三十八条明确规定，对于关系消费者生命健康的商品或者服务，电子商务平台经营者负有安全保障义务。这一规定将安全保障义务由线下物理空间过渡到线上虚拟空间，扩大了平台义务与责任，有助于维护消费者切身利益，保障网络交易秩序。²此外，《消费者权益保护法》等相关法律法规也对电子商务平台的数据安全保障义务提出了明确要求。电子商务平台的数据安全保障义务包括多个方面。第一，电子商务平台应保障其提供的网络服务的安全性，采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动，有效应对网络安全事件，保障电子商务交易安全。第二，电子商务平台应制定网络安全事件应急预案，在发生网络安全事件时立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。第三，电子商务平台还应保障交易系统安全，采用技术确认用户的真实身份和有效授权，保障数据传输真实、完整，防范因黑客攻击、病毒、网络中断等导致的交易信息错误、迟延、丢失或不能辨认的风险[3]。“乐清女孩搭乘滴滴遇害案”2018年8月24日，在浙江乐清市，一名19岁的少女赵培辰在搭乘滴滴顺风车后失去联系。次日上午，犯罪嫌疑人钟元，即该滴滴司机，在乐清市的一座山上被捕。他供认了对赵培辰实施强奸并杀害的罪行，随后受害者的遗体也被发现。8月25日，滴滴公司发表道歉及声明，承认自身负有不可推卸的责任，并承诺将全力配合警方，妥善处理受害者家属的相关事宜。同时，犯罪嫌疑人钟元已被警方依法刑事拘留，案件正在深入调查中。8月26日，最高人民检察院发布消息，乐清市人民检察院迅速响应，立即派员前往乐清市公安局，对该案进行提前介入，并对公安机关提出了全面研判案件性质、依法规范取证等建议。钟元继续被依法刑事拘留。8月27日，乐清市人民检察院以涉嫌抢劫罪、强奸罪、故意杀人罪，依法对“女孩滴滴顺风车遇害案”的犯罪嫌疑人钟元实施逮捕。8月28日，滴滴公司再次发表郑重道歉声明，并宣布将对顺风车业务模式进行全面评估，在安全保障措施未获得用户广泛认可之前，将无限期暂停该业务。³说明法律对电商平台数据安全保障的迫切需求。

在司法实践中，已有多个判例认定网络空间属于公共场所，并判决网络服务提供者未尽到安全保障义务时需承担相应的法律责任。例如，北京互联网法院在“何小飞诉北京密境和风科技有限公司网络侵权责任纠纷案”中，就将安全保障义务扩张至网络空间。虽然《民法典》第一千一百九十八条所列举的场所类型主要指向现实空间，但随着社会的发展和技术的进步，将安全保障义务扩展到网络空间已逐渐成为趋势。最高人民法院、最高人民检察院的相关司法解释也将信息网络空间纳入公共场所的范围[4]。

3. 电商平台数据安全保障义务的问题

3.1. 电商平台存在技术漏洞

随着大数据、人工智能等技术的广泛应用，黑客攻击、数据泄露等事件频发，严重威胁到用户隐私和财产安全。例如DDoS攻击、SQL注入等网络攻击手段可能导致平台服务中断、用户信息被窃取。尽

²《电子商务法》第三十八条：电子商务平台经营者知道或者应当知道平台内经营者销售的商品或者提供的服务不符合保障人身、财产安全的要求，或者有其他侵害消费者合法权益行为，未采取必要措施的，依法与该平台内经营者承担连带责任。

³来源于：8·24乐清女孩乘车遇害案——百度百科。

管电商平台在数据安全保障方面面临着诸多挑战，但同时也在不断探索和实践有效的保障措施。字节跳动公司通过制定数据安全政策和标准，明确数据收集、存储、使用等环节的安全要求。其还设立专门的数据安全管理机构，负责数据安全管理的日常工作，包括数据分类分级、风险评估、安全审计等[5]。天猫淘宝则通过部署防火墙、入侵检测系统、安全信息和事件管理系统等安全技术工具，实时监测和防御潜在的安全威胁。并采用数据加密技术，对敏感数据进行加密存储和传输，确保数据在存储和传输过程中的安全性。定期进行漏洞扫描和安全评估，及时发现和修复系统中的安全漏洞。在各大电商平台中，均做到对员工进行背景调查和安全培训，提高员工的数据安全意识和防范能力。实施严格的访问控制策略，确保只有授权人员才能访问敏感数据。建立数据安全事件的应急预案，明确在发生数据安全事件时的应对步骤和责任分工。电商平台需要遵守多个国家和地区的法律法规，包括《电子商务法》《消费者权益保护法》《知识产权保护法》等。建立专门的合规团队，跟踪和研究相关法律法规的变化，确保平台的数据处理活动符合法律要求[6]。但仍存在着技术漏洞，在 2024 年以色列网络安全公司 Hudson Rock 发现一个据称包含 3.5 亿条 Hot Topic 顾客个人和支付数据的庞大数据库在暗网上被公开出售。名为 Satanic 的威胁组织发布了该订单，并声称数据库包括用户详细的个人信息，如姓名、电子邮件地址、邮寄地址、出生日期、交易信息、信用卡信息、发票信息等。Hudson Rock 的研究人员对威胁组织提供的数据样本进行分析，发现主要来源于 Hot Topic、Torrid 和 BoxLunch 三家零售企业，他们都由快时尚集团 Hot Topic 创立并运营。Hot Topic 在 2023 年和 2024 年分别披露了多起网络攻击事件，安全分析人员表示，此次在暗网上售卖的数据可能来源于此。⁴

3.2. 有关电商经济法律法规有待完善

随着网络技术的快速发展和新型网络威胁的不断涌现，现有的法律体系在应对这些新威胁时可能存在一定的滞后性。在网络安全领域，违法行为的法律责任和处罚力度是维护网络安全的重要手段。然而，目前一些网络安全法律法规在对违法行为的处罚方面可能存在力度不足的问题，导致违法成本相对较低，难以有效遏制违法行为的发生。我国电子商务立法明显滞后于行业发展，相关法律法规分散、层级较低且内容不全[7]。例如，网络支付、税收征管等方面的法律法规尚不完善，导致电商平台在运营过程中面临诸多法律风险和合规挑战。此外，监管体制的不完善也加剧了这一问题。政府管理缺乏协调机制，导致监管或政出多门或职能缺位。电商平台数据安全保障的监管涉及多个部门，如何确保各部门之间的有效协作和信息共享是一个难题。目前，我国在网络安全监管方面可能还存在一定的分散性和不协同性，需要加强跨部门、跨地区的协调合作机制建设[8]。同时，随着网络技术的不断发展，网络安全威胁也日益隐蔽和复杂，这给监管部门的执行工作带来了极大的挑战。虽然《电子商务法》等法律法规对电商平台的安全保障义务进行了一定的规定，但具体条款可能还存在一些模糊和不明确的地方。例如，对于电商平台在数据安全保障方面的具体责任和义务、数据泄露后的应急响应和处置措施等方面可能缺乏详细的规定。这可能导致电商平台在执行数据安全保障义务时存在困惑和不确定性。

3.3. 消费者保护意识有待提升

尽管电商平台在数据安全方面做出了诸多努力，但消费者数据保护意识不足仍然是一个严峻的问题。许多消费者对于个人数据在电商平台上的安全性和隐私保护缺乏足够的认知。他们可能不了解自己的数据是如何被收集、存储和使用的，也不清楚数据泄露可能带来的风险和后果。这种认知不足导致消费者在电商平台购物时，可能忽视对个人数据的保护，甚至在不安全的网络环境下进行交易，从而增加了数据泄露的风险。尽管一些消费者意识到数据安全性的重要性，但在实际操作中往往因为便利性或疏忽而忽

⁴ 来源于：数据安全每周观察 | 工业和信息化领域数据安全事件应急预案印发。

略了对数据安全的保护[9]。例如，他们可能为了方便记忆而使用简单的密码，或者在多个平台使用相同的密码，这些都增加了数据被破解的风险。即使消费者意识到自己的数据可能已经泄露，他们也可能不知道如何应对[10]。他们可能不清楚应该立即更改密码、联系电商平台或相关机构进行报告，或者采取其他必要的措施来减少损失。这种缺乏应对措施的了解可能导致消费者在数据泄露后无法及时有效地保护自己的权益。许多消费者对于数据保护的法律法规和维权途径缺乏了解。他们可能不知道自己的数据受到哪些法律法规的保护，也不知道在数据泄露后应该如何寻求法律救济。这种缺乏法律意识和维权意识可能导致消费者在数据泄露后无法有效地维护自己的合法权益。

3.4. 行业自律集约化程度不高

目前，电商平台在数据安全保障方面往往遵循各自的企业标准和内部规范，导致行业内部缺乏统一的数据安全保障标准。这种差异性和不统一性不仅增加了监管难度，也使得消费者在选择电商平台时难以判断其数据安全保障能力的强弱[11]。行业自律的有效性在很大程度上取决于监督机制的完善程度。然而，目前电商平台数据安全保障的行业自律监督机制尚不完善，缺乏有效的第三方独立监督机构来评估和监督电商平台的数据安全保障措施。这可能导致一些电商平台在数据安全保障方面存在侥幸心理，忽视对数据安全的投入和管理。虽然我国已经出台了一系列网络安全法律法规，但行业自律与法律法规之间的衔接仍存在不足。一方面，法律法规可能未能全面覆盖电商平台数据安全保障的各个方面[12]；另一方面，行业自律标准可能未能与法律法规保持一致，导致在数据安全保障方面存在法律空白或监管漏洞。此外，内部员工也可能成为数据泄露的风险源，目前电商平台及其从业人员在行业自律意识方面仍存在不足，对数据安全保障的重要性认识不足，缺乏主动遵守行业自律标准的自觉性和积极性，他们可能滥用权限或泄露用户数据[13]。

4. 电商平台数据安全保障义务的建议

4.1. 加强技术保障

电商平台应引入最新的加密技术，如量子加密、区块链等，作为下一代加密技术的代表，量子加密利用量子力学原理，如量子纠缠和量子密钥分发(QKD)，实现理论上无法被破解的数据加密。电商平台若采用量子加密技术，能在数据传输过程中构建一道坚不可摧的安全屏障，即使是最强大的计算机也无法破解，从而极大提升数据传输的安全性。对敏感数据进行加密存储和传输，确保数据在存储和传输过程中的安全性。建立定期的安全检查机制，利用自动化工具和专业团队对平台进行安全漏洞扫描和风险评估，及时发现并修复潜在的安全隐患。制定详尽的应急预案，包括应急响应流程、数据恢复措施、用户通知机制等，确保在发生网络安全事件时能够迅速响应，减少损失[14]。

4.2. 完善法律法规

通过立法明确电商平台在数据安全方面的具体义务，如数据收集、存储、使用、传输等方面的规范要求，为电商平台提供明确的法律指导。电商平台在收集用户数据时，应遵循合法、正当、必要的原则，明确告知用户数据收集的目的、方式和范围，并获得用户的明确同意。电商平台应采取有效的技术手段和管理措施，确保用户数据的安全存储，防止数据丢失、损坏或被未经授权的访问、泄露、篡改。电商平台在使用用户数据时，应仅限于实现用户授权的目的，不得超范围使用，更不得将数据用于非法交易或泄露给第三方。电商平台在数据传输过程中，应采用加密技术，确保数据传输的安全性，防止数据在传输过程中被截获或篡改。提高对数据泄露等违法行为的罚款标准，增加违法成本，形成有效的法律威慑力。结合电商平台的实际情况，制定具体、可操作的数据安全保障标准，为电商平台提供明确的执行依据。

4.3. 提升消费者保护意识

通过线上线下的方式,开展数据安全知识宣传活动,提高消费者对数据安全的认识和重视程度。利用互联网和社交媒体平台,如微博、微信、抖音等,发布数据安全知识短视频、图文文章、互动问答等,以生动、直观的方式向消费者普及数据安全知识。同时,电商平台可以在其官方网站和 APP 上设置数据安全专区,提供数据安全政策、隐私保护指南、安全使用提示等信息,方便消费者随时查阅和学习。在社区、学校、商场等公共场所举办数据安全知识讲座、展览、咨询等活动,邀请专家、学者、律师等现场解答消费者关于数据安全的疑问,发放数据安全宣传手册、海报等宣传资料,提高消费者的数据安全意识 and 自我保护能力。建立专门的消费者投诉和维权平台,简化投诉流程,提高处理效率,保障消费者的合法权益。建立消费者数据安全监督机制,鼓励消费者积极参与数据安全监督,形成社会共治的良好氛围。

4.4. 加强行业自律合作

电商平台之间在数据处理、存储、传输等方面存在差异性,这可能导致数据安全管理的混乱和漏洞。通过建立数据安全联盟,各平台可以共同协商、制定统一的数据安全标准,明确数据收集、使用、保护等方面的具体要求,为电商平台提供明确的行为规范,降低数据安全风险。推动电商平台之间建立数据安全联盟,共同制定数据安全标准,分享数据安全技术和经验,提升整个行业的数据安全保障水平。定期组织数据安全交流会,邀请行业专家、学者和企业代表分享数据安全最佳实践和经验,促进数据安全技术的创新和应用。数据安全交流会是一个集思广益、互学互鉴的平台。通过定期举办此类活动,可以促进电商平台之间、企业与学术界、监管机构之间的沟通与合作,共同应对数据安全挑战。数据安全交流会不仅是经验分享的场所,更是技术创新和应用的催化剂。通过交流、碰撞思想,可以激发新的数据安全解决方案和创新应用的诞生,推动数据安全技术的持续进步。面对数据安全风险和挑战,电商平台应加强协作,共同制定应对策略,提高整体抗风险能力[15]。

5. 结论

在电商经济中,消费者的个人信息和交易数据是电商平台运营的基础。然而,一旦这些数据发生泄露,将严重损害消费者对电商平台的信任。数据泄露可能导致消费者的个人隐私被曝光,甚至面临身份盗用、财产损失等风险。这不仅会让消费者感到不安和愤怒,还会让他们对电商平台的安全性产生怀疑,从而降低对平台的信任度和忠诚度。电商平台的数据安全保障义务对于电商经济的可持续发展具有深远的意义。在数字经济时代,数据已成为电商平台的核心资产,其安全性直接关系到平台的运营稳定、用户信任以及整个电商生态的健康发展。数据安全保障是电商平台赢得用户信任的关键。当用户确信自己的个人信息和交易数据在平台上得到妥善保护时,他们更愿意在平台上进行消费和交易,从而增强用户的忠诚度和黏性。这种信任关系的建立,为电商平台的长期发展奠定了坚实的基础。电商平台必须遵守相关法律法规,确保数据的安全和合规使用。研究数据安全保障义务,有助于平台了解并遵守相关法律法规,避免因违规行为而遭受法律制裁和声誉损失。同时,合规经营也有助于提升平台的品牌形象和市场竞争力。在数据安全保障的基础上,电商平台可以更加放心地探索新的业务模式和技术应用。例如,利用大数据和人工智能技术优化供应链管理、提升用户体验、实现精准营销等。这些创新举措将推动电商经济的持续发展和转型升级,为经济增长注入新的动力。

尽管电商平台的数据安全保障义务研究已经取得了一定的成果,但仍存在一些局限性和未来值得探索的方向。研究的局限性:现有研究大多侧重于技术层面的探讨,而对于法律、经济、社会等多维度的综合分析还较为缺乏。实证数据不足,导致研究结果的普适性和准确性受到一定限制。跨领域合作有待

加强,需要更多计算机科学、法学、经济学等领域的专家共同参与研究。未来研究方向:加强综合研究,构建包含法律、经济、社会等多维度的理论体系,全面分析数据安全保障义务的内涵和外延。加强实证研究,通过收集和分析大量的实证数据,评估电商平台数据安全保障义务的实施效果和影响因素。推动跨领域合作,加强计算机科学、法学、经济学等领域的合作和交流,共同探索电商平台数据安全保障的新技术和新方法。

参考文献

- [1] 赵精武. 论聚合平台的数据安全保障义务[J]. 法制与社会发展, 2024, 30(6): 111-128.
- [2] 张凯, 张旭. 大数据安全治理与防范[M]. 北京: 人民邮电出版社, 2023.
- [3] 王磊. 安全保障义务的解释论展开[J]. 现代法学, 2024, 46(3): 99-112.
- [4] 张莉, 中国电子信息产业发展研究院. 数据治理与数据安全[M]. 北京: 人民邮电出版社, 2019.
- [5] 张衡. 大数据时代个人信息安全规制研究[M]. 上海: 上海社会科学院出版社, 2020.
- [6] 雷玄. “羊毛党”肆虐电商生态受损[J]. 中国质量万里行, 2024(9): 14-15.
- [7] 杨异, 张武杰. 网络直播中安全保障义务规则的移植与再塑[J]. 大连理工大学学报(社会科学版), 2024, 45(6): 70-75.
- [8] 牟柯. 夯筑网络安全铜墙铁壁共建安全稳定网络空间[N]. 巴中日报, 2024-09-09(001).
- [9] 于润芝. 数据犯罪刑法规制的价值选择、法益定位及利益识别[J]. 河南财经政法大学学报, 2024, 39(6): 78-89, 100.
- [10] 吴宇飞. 互联网用户信息保护的路径优化——基于快递行业视角[J]. 现代管理科学, 2018(5): 103-105.
- [11] 曹凡. 电商平台经营者安全保障义务标准构建[J]. 学习与探索, 2024(2): 73-81.
- [12] 陈思静. 电商平台经营者民事责任设置基础: 逻辑构成与利益平衡[J]. 法学论坛, 2024, 39(5): 65-76.
- [13] 宋瑞, 隋福毅. “双十一”花式调价消费者遇假优惠陷阱[N]. 经济参考报, 2024-11-12(004).
- [14] 刘锦. 电商平台承担信息审查义务的困境与出路[J]. 大连理工大学学报(社会科学版), 2023, 44(5): 95-102.
- [15] 肖峰. 信息利益视野下电商平台消费者保护责任立法的完善[J]. 上海财经大学学报, 2022, 24(1): 137-152.