E-Commerce Letters 电子商务评论, 2025, 14(11), 2251-2256
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14113683

Hans汉斯

跨境电商企业的数据信息保障体系构建

张　旭

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29日；发布日期：2025年11月26日

摘　要

在全球数字化浪潮与国际贸易格局重塑的双重驱动下，跨境电商已从一种新兴贸易业态演变为推动全球经济增长的核心引擎之一。然而，其业务模式所固有的无边界、虚拟化和数据驱动特性，在创造巨大商业价值的同时，也使其面临着前所未有的数据安全与信息保障挑战。数据，作为贯穿跨境电商营销、交易、支付、物流与客服全链路的生命线，其安全性、完整性、可用性和隐私保护水平，直接决定了企业的合规生存能力、市场竞争力与品牌公信力。本文旨在系统性地解构跨境电商企业在数据生命周期各环节所面临的多维、复合型安全威胁，并在此基础上，创新性地提出一个融合了技术防护、管理运营、法律合规及生态协同四位一体的数据信息保障综合治理框架。该框架不仅关注静态的防御措施，更强调动态的、适应性的风险治理能力。本文还将结合典型案例进行深入剖析，并前瞻性地探讨了在人工智能、物联网等新技术背景下，跨境电商数据安全的发展趋势与应对策略，以期为相关企业在全球数字市场中构建韧性、实现可持续发展提供兼具理论高度与实践指导意义的参考。

关键词

跨境电商，跨境数据流动，数据治理，隐私保护

Construction of Data Information Security System for Cross-Border E-Commerce Enterprises

Xu Zhang

Law School of Guizhou University, Guiyang Guizhou

Received: October 14, 2025; accepted: October 29, 2025; published: November 26, 2025

Abstract

Driven by the global digital wave and the reshaping of international trade patterns, cross-border e-

文章引用: 张旭. 跨境电商企业的数据信息保障体系构建[J]. 电子商务评论, 2025, 14(11): 2251-2256.
DOI: 10.12677/ecl.2025.14113683

commerce has evolved from an emerging trade format to one of the core engines driving global economic growth. However, the inherent borderless, virtualized, and data-driven characteristics of its business model not only create enormous commercial value but also expose it to unprecedented data security and information protection challenges. As the lifeline running through the entire chain of cross-border e-commerce marketing, transactions, payments, logistics, and customer service, data—with its security, integrity, availability, and privacy protection level—directly determines an enterprise's compliance survival ability, market competitiveness, and brand credibility. This paper aims to systematically deconstruct the multi-dimensional and complex security threats faced by cross-border e-commerce enterprises in each link of the data life cycle. On this basis, it innovatively proposes a four-in-one comprehensive data information security governance framework integrating technical protection, management operations, legal compliance, and ecological collaboration. This framework not only focuses on static defense measures but also emphasizes dynamic and adaptive risk governance capabilities. The paper also conducts in-depth analysis combined with typical cases and prospectively discusses the development trends and response strategies of cross-border e-commerce data security under the background of new technologies such as artificial intelligence and the Internet of Things, aiming to provide a reference with both theoretical height and practical guiding significance for relevant enterprises to build resilience and achieve sustainable development in the volatile global digital market.

Keywords

Data Security, Information Protection, Data Governance, Privacy Protection

1. 引言

21 世纪以来，跨境电商凭借突破时空限制、缩短贸易链路、满足个性化需求的优势实现快速增长，成为连接全球生产与消费的重要纽带。在这一商业模式中，数据已从业务附属要素转变为驱动运营的核心资源——通过大数据分析构建用户画像、依托算法实现智能推荐与动态定价、借助 API 接口完成跨境通关与物流追踪、基于云架构支撑全球交易平台弹性扩展，数据已深度融入跨境电商全价值链环节。

与此同时，数据资源的价值属性也使其成为风险集中领域。跨境电商运营涉及多司法管辖区、多网络环境与多合作主体的数据流转，传统基于物理边界的安全防护体系难以适配这一开放场景。数据泄露、篡改等安全事件不仅会导致企业经济损失，还可能引发合规风险与品牌信任危机，构建全面、适配的数据信息保障体系已成为跨境电商企业的核心运营需求，而非单纯的技术管理问题。从通过大数据分析精准描绘用户画像，到利用算法进行智能推荐和动态定价；从集成多方 API 接口实现一键通关与实时物流追踪，到依托云原生架构支撑弹性可扩展的全球交易平台——数据要素已深度融入并主导着每一个价值创造环节。

对于任何有志于在全球市场中长期发展的跨境电商企业而言，构建一个全面、有效、敏捷的数据信息保障体系，已从一个技术管理问题升维为关乎企业生死存亡的核心战略命题。这要求企业管理者必须具备前瞻性的视野，不再将数据安全视为纯粹的成本中心或 IT 部门的职责，而是将其作为企业核心竞争力的基石进行投资和建设。本论文将围绕这一战略命题，从风险剖析、体系构建到未来展望，展开全面而深入地论述。

2. 跨境电商企业面临的核心数据安全风险剖析

2.1. 数据流转环节的技术性风险

2.1.1. 传输通道上面临的窃听与篡改威胁

跨境电商数据传输需跨越公共互联网、跨境通信链路等多场景，传输通道的开放性使其面临显著安全威胁。当用户通过公共 Wi-Fi (如机场、商圈网络)访问跨境电商平台时，攻击者可通过信息传输中介截获通信数据；即使在加密传输场景中，风险仍未完全消除：若平台未强制启用 TLS 1.3 及以上版本加密协议，或存在证书配置错误(如证书过期、域名不匹配)，攻击者可通过“降级攻击”将加密通信转为明文传输；部分地区跨境网络链路存在数据劫持风险，攻击者可篡改传输中的交易数据(如修改收款账户、调整订单金额)，此类事件在东南亚、中东等跨境电商新兴市场发生率较高。

2.1.2. 在存储与访问上面临的泄露与滥用威胁

数据存储阶段的风险主要集中于云环境安全与内部权限管理两方面。当前 85%的跨境电商企业采用公有云存储数据(AWS, 2024)，但云配置不当已成为数据泄露的首要诱因——AWS 2024 年安全报告显示，38%的跨境电商云存储泄露事件源于安全组配置错误(如开放不必要的端口)，27%源于未加密的存储卷。此外，数据库漏洞(如未修复的 SQL 注入漏洞)也为攻击者提供了可乘之机，2023 年 Shopify 平台某第三方卖家因数据库漏洞导致 12 万条用户支付信息泄露，最终面临 120 万美元罚款。

内部访问风险同样不容忽视。跨境电商企业客服、运营等岗位员工需接触用户数据，但部分企业未严格执行“最小权限原则”与“权限分离原则”。此外，数据融合分析场景中存在“去匿名化”风险。即使企业对用户直接标识符(如姓名、手机号)进行脱敏处理，但通过交易数据、地理位置数据与第三方标签数据的关联分析，仍可能还原特定用户身份[1]。

2.2. 跨境业务特有的合规与法律风险

2.2.1. 全球隐私法规林立所带来的合规冲突

跨境电商企业实质上是在一个由数十种不同数据隐私法规构成的结构所组成。欧盟的《通用数据保护条例》(GDPR)无疑是其中影响最深远、要求最严格的法规之一[2]。它确立了“长臂管辖”原则，只要企业向欧盟境内的数据主体提供商品或服务或监控其行为，无论其自身是否在欧盟设立机构，都必须遵守 GDPR。其严苛的处罚力度(最高可达全球年营业额的 4%或 2000 万欧元，以高者为准)足以让任何企业望而生畏。与此同时，美国的《加州消费者隐私法案》(CCPA)及其升级版《加州隐私权利法案》(CPRA)赋予了消费者知情、退出、更正和删除其个人信息的广泛权利。而中国的《网络安全法》《数据安全法》和《个人信息保护法》共同构成了国内数据治理的三方主体，对数据出境、关键信息基础设施保护等提出了明确要求。这些法律在核心定义(如何界定“个人信息”)、合法性基础(如“同意”的形式要求)、数据主体权利范围以及执法风格上均存在显著差异。企业必须投入巨大的法律和技术资源，构建一个能够同时满足多重合规要求的、极其复杂的运营体系。

2.2.2. 生态合作链条衍生的第三方风险

现代跨境电商的卓越用户体验，高度依赖于一个由众多专业服务商构成的生态系统。这包括支付网关(如 PayPal、Stripe)、国际物流巨头(如 DHL、FedEx)、云服务商、数字营销与广告平台(如 Google、Facebook)、客户关系管理(CRM)及企业资源规划(ERP)系统供应商等。然而，每一个接入的第三方都意味着企业安全边界的一次延伸和一个新的潜在攻击面[3]。第三方风险的核心在于“安全水平不取决于最强的环节，而取决于最弱的一环”。即使电商平台自身的安全体系坚不可摧，但其合作的某个小型营销分析工具供应商如果存在安全漏洞并被攻破，攻击者同样可以借此为跳板，窃取到平台共享过去的用户数

据，或者获取访问平台内部系统的凭证。此外，第三方服务的 API 接口如果设计不安全或配置错误，也可能成为数据泄露的直接通道。因此，对第三方合作伙伴的安全资质审查、持续的监控以及通过具有法律约束力的数据处理协议(DPA)明确其安全责任，构成了一个庞大而艰巨的管理挑战[4]。

3. 构建跨境电商数据信息保障的多维治理体系

3.1. 构筑纵深防御的技术保障体系

本文中所指的保障体系，依据《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》定义，是围绕数据保护目标，整合技术工具、管理流程、制度规范与组织架构，覆盖数据存储、传输、计算全生命周期的系统性防护框架，具备风险识别、威胁阻断、应急响应与持续优化能力。基于此，本文系统性解构跨境电商企业在数据生命周期各环节面临的多维安全威胁，创新性提出融合技术防护、管理运营、法律合规及生态协同四位一体的数据信息保障综合治理框架[5]。该框架既关注静态防御措施，也强调动态、适应性的风险治理能力。本文结合典型案例展开深入剖析，并前瞻性探讨人工智能、物联网等新技术背景下跨境电商数据安全的发展趋势与应对策略，为相关企业在复杂的全球数字市场中构建韧性、实现可持续发展提供兼具理论高度与实践指导意义的参考。在高级持续性威胁(APTs)面前，没有绝对的防御，因此“检测与响应”能力变得至关重要。部署安全信息和事件管理(SIEM)系统或更现代化的安全编排、自动化与响应(SOAR)平台，是构建这一能力的核心。它们能够聚合来自防火墙、入侵检测系统、终端防护软件、数据库审计系统及云平台日志等全源数据，通过预定义的关联规则和用户与实体行为分析(UEBA)技术[6]，发现诸如“一个账户在短时间内从两个不同国家登录”“内部员工在离职前大量下载客户数据”等异常行为。数据防泄露(DLP)系统则应在网络网关、出口通道以及员工终端上部署内容识别策略，一旦检测到试图外传的信用卡号、身份证号等敏感信息，即可进行实时阻断、隔离并告警。当安全事件被确认后，一个经过精心设计并定期演练的应急响应计划是减少损失的关键。该计划应明确宣布事件的指挥链、沟通流程(包括何时及如何通知监管机构和受影响的用户)、证据保全方法以及业务恢复步骤[7]。

3.2. 完善严谨规范的管理体系

管理信息机构应当部署安全信息与事件管理(SIEM)系统，整合防火墙、入侵检测系统(IDS)、终端防护软件(EDR)等多源日志数据，通过用户与实体行为分析(UEBA)技术识别异常行为；在数据防泄露(DLP)层面，采用“内容识别 + 行为阻断”模式：在网络出口部署 DLP 网关，识别并阻断信用卡号、身份证号等敏感数据外传；在员工终端安装 DLP 客户端，限制未授权数据拷贝；同时建立标准化应急响应机制，参考 NIST 应急响应框架(Preparation, Detection, Containment, Eradication, Recovery)制定流程：明确应急指挥链(如由 CTO 牵头，联合法务、公关团队)、证据保全方法(如数据镜像备份)、合规通知时限(如 GDPR 要求 72 小时内上报数据泄露事件) [8]。

4. 新技术背景下跨境电商数据安全的发展趋势与应对

4.1. 遵循全球视野的法律合规体系

面对日益复杂的全球监管环境，被动响应式的合规模式成本高昂且风险巨大。最根本的解决方案是将隐私与数据保护要求前置于产品和业务的设计阶段，即“设计即合规”与“默认即合规”[9]。这意味着，在产品经理构思新功能时，就需要与法务、DPO 和安全团队合作，进行隐私影响评估(PIA)，识别并规避潜在的合规风险。在系统开发过程中，遵循安全开发生命周期(SDL)，将威胁建模、代码安全扫描、渗透测试作为必经环节。在面向用户的界面设计上，应采用“隐私友好型”的默认设置，例如，默认不勾

选“同意接收营销邮件”的选项，默认仅收集完成交易所需的最少数据，通过将合规要素深度融入业务流程，可以从源头最大程度地降低违规风险[10]。

4.2. 构建合作共赢的生态协同体系

单个企业的视野和能力总是有限的。积极参与跨境电商行业协会、数据安全联盟等组织，能够帮助企业获取最新的行业安全动态、最佳实践和法规解读。加入行业性的威胁情报共享平台(如 ISAC)更是提升主动防御能力的关键。通过匿名共享自身遇到的攻击指标(如恶意 IP、钓鱼域名、攻击手法)，并从同行处获取情报，企业能够提前布防，在攻击蔓延之前就将其扼杀，从而实现“一处受损，处处预警”的协同防御效果[11]。

面对人工智能、物联网等新技术浪潮，跨境电商数据安全的挑战与机遇并存。企业应秉持“持续演进、主动适应”的安全观：首先，加大在创新安全技术上的研发与投资，特别是 AI 安全(如利用 AI 提升威胁检测效率)、零信任(深化动态访问控制)和隐私增强技术(如联邦学习、同态加密) [12]；其次，提升组织的安全韧性，不仅注重预防，更要强化在遭受攻击后快速恢复业务和持续运营的能力；最后，积极参与行业对话与标准制定，通过与同行、监管机构的沟通，共同塑造一个更安全、更公平、更可持续的全球数字贸易环境[13]。

5. 结语

在数字经济席卷全球的宏大背景下，数据信息保障已然从跨境电商企业的辅助性支撑，蜕变为其核心竞争力的关键组成部分和业务连续性的生命线。本文系统地论证了，其所面临的挑战是一个由技术漏洞、管理盲点、法律冲突与生态风险相互交织构成的复杂系统性问题。因此，任何孤立的、片面的解决方案都难以奏效。

企业必须从根本上转变思维，构建一个动态的、深度融合的多维治理体系。这个体系以纵深防御的技术体系为坚实底座，以严谨规范的管理运营为运作框架，以前瞻全球的法律合规为航行规则，并以开放协同的生态合作为核心进行组织建构[14]。四者相互支撑，缺一不可。

展望前路，挑战与机遇并存。技术的飞速迭代与法规的持续演进，意味着数据安全保障是一场没有终点的马拉松。对于立志于全球市场的跨境电商企业而言，唯有将数据安全理念深植于企业文化基因，以战略性的眼光进行持续投入，以开放务实的态度进行内外协同，方能在汹涌的数字浪潮中稳健航行，不仅赢得当下的市场，更能驾驭未来的变局，实现基业长青。

参考文献

[1] 齐鹏. 中国与 DEPA 数据跨境流动: 规制差异及制度对接探究[J]. 法学评论, 2025, 43(3): 30-43.
[2] 杨猛. 企业数据治理的底层逻辑及法律体系构建——以欧盟立法比较研究为切入点[J]. 南京社会科学, 2025(5): 65-76.
[3] 杨军. 基于跨境电子商务环境下供应链风险体系研究[J]. 价值工程, 2019, 38(4): 82-84.
[4] 金莹璋. 基于模糊群决策的跨境电商企业供应链风险评估研究[J]. 全国流通经济, 2023(7): 16-19.
[5] 张晓东. 基于生态位视角的跨境电商产业竞争力实证研究[J]. 国际商务研究, 2022, 43(1): 26-36.
[6] 周辉, 闫文光. 美国数据跨境监管立场转向: 从自由流动到安全流动[J]. 国际法研究, 2025(3): 100-114.
[7] 顾华详, 顾红霞. 数字贸易强国: 健全战略决策法治支撑体系的路径研究[J]. 新疆社会科学, 2025(4): 55-71.
[8] 唐楠, 李静, 曹啸, 等. 跨境数据流动限制对全球价值链分工的影响研究[J]. 财经论丛, 2024(12): 26-35.
[9] 陈伟光, 刘芳蕊, 钟列炀. 跨境数据流动限制对全球价值链嵌入的影响[J]. 国际贸易问题, 2025(8): 55-71.
[10] 汤诤. 数据跨境流动国际规则碎片化与协调路径[J]. 江西社会科学, 2025, 45(6): 112-124+207+209.

[11] 张东冬. 数字外交强化与美国全球数字竞争的全新图景[J]. 国际关系研究, 2025(1): 35-56+156.

[12] 王子沛, 陈雯清, 常艳丽. 科技创新、供应链金融与跨境电子商务产业政策的耦合研究——以河南省为例[J]. 对外经贸, 2020(8): 44-48.

[13] 霍俊先. 数据跨境流动安全例外条款的适用困境与中国对策[J]. 国际贸易, 2025(8): 86-96.

[14] 蒲新蓉. 数字经济时代跨境电商生态系统建设与发展策略[J]. 质量与市场, 2022(8): 160-162.