Modern Management 现代管理, 2026, 16(2), 36-44
Published Online February 2026 in Hans. https://www.hanspub.org/journal/mm
https://doi.org/10.12677/mm.2026.162033

Hans汉斯

生成式人工智能驱动下跨境贸易安全管理的机遇、挑战与治理路径

王雪珂

云南财经大学物流与管理工程学院，云南 昆明

收稿日期：2026年1月9日；录用日期：2026年1月21日；发布日期：2026年2月6日

摘　要

生成式人工智能的快速发展正在推动跨境数字贸易的技术升级，其在提升贸易效率和优化数据管理的同时，也带来了复杂的安全与治理挑战。本文系统分析了生成式人工智能在跨境贸易中的智能数据分类、匿名化处理和动态访问控制等技术优势，揭示其在提升数据安全性与贸易效率方面的作用。同时，从用户权益、伦理规范、监管合规和技术治理等多维视角深入探讨了生成式人工智能带来的潜在风险。研究进一步提出“技术－规则－治理”协同框架，包括算法审计机制的建立、技术标准适应性设计、开发者责任与信用体系完善，以及动态风险应对机制的创新。研究结论为企业和平台在推进数字贸易应用过程中提供了可行的技术与治理参考，有助于实现安全、可控与高效的数据流通环境。

关键词

生成式人工智能，跨境贸易，数据安全，安全风险，治理路径

Generative AI-Driven Cross-Border Trade Security Management: Opportunities, Challenges, and Governance Pathways

Xueke Wang

School of Logistics and Management Engineering, Yunnan University of Finance and Economics, Kunming Yunnan

Received: January 9, 2026; accepted: January 21, 2026; published: February 6, 2026

Abstract

Generative Artificial Intelligence is reshaping the global landscape of cross-border trade. While

文章引用: 王雪珂. 生成式人工智能驱动下跨境贸易安全管理的机遇、挑战与治理路径[J]. 现代管理, 2026, 16(2): 36-44. DOI: 10.12677/mm.2026.162033

enhancing trade efficiency and optimizing data management, it also brings complex security and ethical challenges. This paper systematically analyzes the technical advantages of Generative Artificial Intelligence in cross-border trade, including intelligent data classification, anonymization, and dynamic access control, revealing its central role in improving data security and trade performance. At the same time, from multiple perspectives—including user rights, ethical standards, regulatory frameworks, and technical governance—it explores the security risks posed by Generative Artificial Intelligence. The study further proposes a "technology-regulation-ethics" collaborative governance framework, encompassing the establishment of a global algorithm audit alliance, the formulation of sovereignty-adaptive technical standards, the improvement of developer ethical credit systems, and the innovation of dynamic risk response mechanisms. The findings provide policymakers and enterprises with practical pathways to balance technological innovation with risk management, contributing to the construction of an open, secure, and fair global digital trade ecosystem.

Keywords

Generative Artificial Intelligence, Cross-Border Trade, Data Security, Security Risks, Governance Pathways

1. 引言

近年来，生成式人工智能(Generative Artificial Intelligence, GAI)的快速发展正深刻重塑全球经济格局，并成为推动数字经济增长的重要驱动力[1]。据估算，GAI 每年可为全球经济贡献约 4.4 万亿美元，2024 年上半年，全球 GAI 服务市场规模已达到 181 亿美元，较 2023 年增长 32.7%，凸显该领域的快速扩张趋势[2]。在全球数字化浪潮的推动下，GAI 正以前所未有的方式赋能产业发展，为全球贸易体系带来深远影响。

在跨境贸易领域，GAI 的因其强大的数据分析与自动化能力使企业能够精准洞察市场需求，从而优化产品研发、市场推广及供应链管理[3]。同时，GAI 在智能合同、风险控制等方面的创新应用，促进贸易流程的数字化与智能化发展，实现了自动化处理，增强交易的安全性与可靠性。此外，GAI 还能够优化国际贸易中的法律合规分析等关键环节，提高全球市场的竞争力。

然而，尽管 GAI 为跨境贸易带来了诸多机遇，其发展仍然面临一系列挑战，包括监管障碍、数据隐私保护、算法偏见、市场垄断以及技术伦理问题等[4]。首先，由于 GAI 依赖于海量数据进行训练和推理，其在跨境贸易中的应用不可避免地涉及数据跨境流动与合规性问题。其次，GAI 算法可能存在偏见，影响贸易公平性，进而导致市场的不均衡发展。此外，GAI 在跨境贸易中的广泛应用还可能导致某些行业因技术壁垒而被边缘化，加剧市场集中度，提高行业垄断风险。

因此，本文将系统梳理 GAI 在跨境贸易中的应用现状，分析其对贸易流程、市场结构及监管环境的影响，探讨其潜在的安全风险，并构建 GAI 赋能跨境贸易的影响机制，为中国加快发展开放型数字服务贸易提供科学合理的治理路径。

2. GAI 驱动跨境贸易数据安全管理的优化

GAI 依托深度学习、自然语言处理(NLP)和计算机视觉等技术，能够在数据分类、隐私保护、访问控制和合规管理等方面发挥重要作用，为跨境贸易的安全性和效率带来深远影响[5]。如图 1 所示，GAI 尤

其是在跨境数据安全管理中的智能数据分类、隐私保护、访问控制、合规审查等方面有着积极的影响。

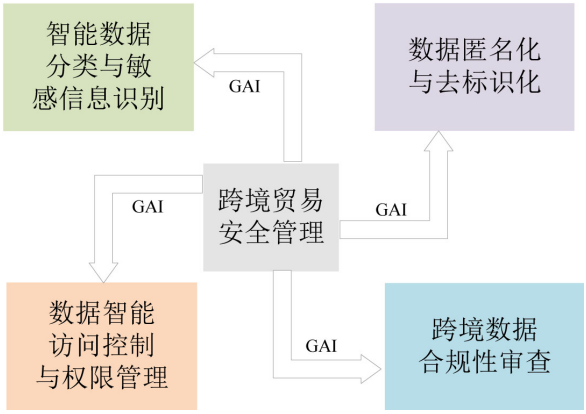

Figure 1. Impact mechanism of GAI-driven cross-border trade data security management
图 1. GAI 驱动下跨境贸易数据安全管理的影响机制

2.1. 智能数据分类与敏感信息识别

跨境贸易涉及大量结构化和非结构化数据，传统数据分类方法依赖于人工或规则的方式，效率较低且易受主观因素影响。而 GAI 可通过 NLP 和深度学习模型，实现数据的自动分类与敏感信息识别，提高数据安全管理的精度和效率[6]。

在跨境贸易中 GAI 通过训练大规模跨境贸易数据集，自动区分普通交易数据与敏感信息，并依据不同的安全等级采取相应的保护措施。同时，GAI 可实时标记数据传输过程中的敏感信息，并结合数据加密技术确保信息安全。研究表明，采用 GAI 进行数据分类的跨境企业，其敏感数据识别准确率可达 99%以上，有效降低数据泄露风险[4]。

2.2. 数据匿名化与去标识化

数据匿名化和去标识化是保障数据跨境流通安全的重要技术手段。GAI 可基于差分隐私和同态加密等技术，对数据进行匿名化处理，在确保数据分析价值的同时避免个人或企业隐私信息泄露。

GAI 通过生成与原始数据分布一致但不包含敏感信息的虚拟数据集，使数据能够在不同国家和地区间安全流通。此外，GAI 可结合去标识化技术，在数据传输前移除直接或间接可识别的信息，同时保持数据的完整性与可用性[7]。

2.3. 数据智能访问控制与权限管理

传统的访问控制机制往往采用静态权限分配方式，难以满足跨境贸易中动态且复杂的访问需求。GAI 结合基于属性的访问控制和零信任架构，可实现动态权限管理，提高数据访问的安全性与灵活性。

GAI 可根据用户行为模式、数据敏感性和访问环境，智能化地调整权限设置，并通过深度学习技术识别异常访问行为。GAI 可分析访问者的地理位置以及访问设备等信息，在检测到异常情况，自动触发安全警报或阻断访问权限。现有国际供应链管理公司采用 GAI 赋能的访问控制系统后，其跨境数据访问违规率降低了 30%以上，同时提高了数据合规性和安全性[8]。

2.4. 跨境数据合规性审查

全球各国对跨境数据流动的监管政策存在较大差异，企业需确保数据传输符合不同国家的法律法规

要求。GAI 可用于自动化法规解析与合规性审查，减少人工审查成本，提高合规性管理效率。

GAI 通过 NLP 解析各国数据保护法规，并将其转化为可执行的合规标准。此外，GAI 可结合区块链技术，实现数据跨境流通过程的全流程监测，确保每个环节均符合国际合规要求。研究表明，GAI 赋能的合规性审查系统可减少 60%以上的人工审核成本，同时提高合规管理的准确性与时效性[9]。

GAI 在跨境数据安全管理中的应用，不仅有效提升了数据安全性、隐私保护和合规管理水平，还推动了跨境贸易的高效运作。

3. GAI 背景下数据跨境流动的安全风险

随着全球数字化转型的不断推进，数据的跨境流动伴随而来的是一系列复杂的安全风险，尤其在 GAI 技术的广泛应用背景下，数据的处理、存储和流动方式发生了深刻的变化，为跨境数据的流动带来了新的安全挑战。

本节，通过对 Deepfake 技术(DT)进行分析、对各国的数据保护法律进行对比、对不同技术计算和通信成本的比较，从用户、道德、监管和法律、技术这 4 个不同的角度讨论生成人工智能的跨境贸易数据流动构成的安全威胁[10]。

3.1. 用户视角

GAI 的快速发展催生了 DT，这对个人和全球机构提出了重大挑战。DT 是一种人工智能驱动的创新，它操纵视觉，听觉和视频内容来制造从未发生过的事件。图 2 显示了 DT 如何操纵经过编码器和解码器的输入内容，以输出所需的结果。从用户权益保障视角审视，GAI 技术驱动的 DT 对跨境贸易数据流动构成三重安全悖论，其风险传导机制在跨国场景中呈现显著放大效应。

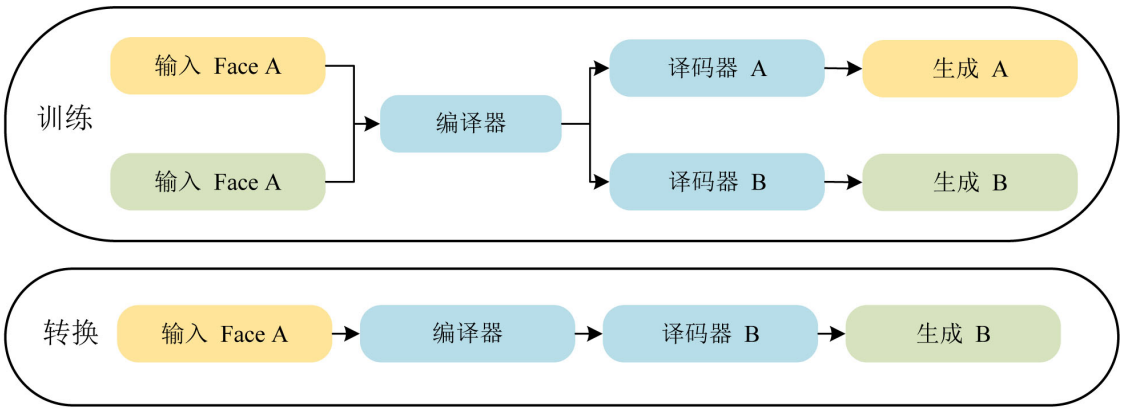

Figure 2. Deepfake generation
图 2. Deepfake 生成图

3.1.1. 多主体数据治理框架下的权益保障

在跨境贸易场景中，DT 通过伪造面部、声纹等生物特征数据突破地理边界限制，导致用户授权机制的全球性失效。欧洲一化妆品企业高管的面部数据在亚洲供应链审计过程中被恶意截取，攻击者利用联邦学习框架下的分布式数据处理漏洞，生成动态深度伪造视频，冒充其向中东分销商下达虚假订单指令。此类事件更因涉事方分属不同司法管辖区，造成用户撤销侵权内容的法律救济成本激增。

3.1.2. 身份控制权的系统性瓦解

跨境支付系统普遍采用的多因子认证正面临 DT 解构，会导致生物认证体系失效。印尼某进出口商

的案例显示，攻击者通过分析其跨国视频会议中的 2.7 秒面部微表情样本，生成可通过 3D 活体检测的深度伪造模型，成功突破瑞士银行跨境结算系统的虹膜认证。国际清算银行模拟实验证实，当前主流生物识别技术在跨境场景中的误识率因 Deepfake 攻击提升至 0.47%，已超过金融安全阈值[11]。

3.1.3. 风险全球化与保险机制失配

现行跨境贸易保险产品尚未建立针对 Deepfake 风险的动态精算模型。伦敦劳合社的承保数据显示，2022 年涉及数字身份欺诈的贸易索赔中，87%的案件存在 DT 痕迹，但仅有 12%成功获得理赔——核心争议在于：侵权行为发生地与数据存储地的司法管辖权冲突，生物特征数据泄露的因果链难以跨境追溯以及伪造内容传播速度超越保险公司的风险响应周期[12]。

GAI 驱动的深度伪造技术在提升生成能力的同时，可能削弱传统身份认证机制的有效性并增加跨系统风险传递。为平衡技术创新与风险管理，有必要构建动态治理框架，以提升系统韧性和可控性。

3.2. 道德视角

从道德伦理维度来看，GAI 驱动的深度伪造 DT 对跨境贸易数据流动的安全风险构建多层次的道德困境，其伦理失范在跨国商业场景中呈现结构性扩散特征。

3.2.1. 算法偏差与跨境贸易决策一致性问题

GAI 模型在训练阶段对数据来源结构高度敏感。当训练数据长期集中于特定区域或平台生态时，模型在处理来自其他地区或业务环境的数据时，容易产生系统性性能偏差。已有研究表明，基于单一数据分布训练的身份识别与风险评估模型，在跨境贸易支付与风控场景中，对部分出口主体的识别准确率显著下降，进而影响交易决策的一致性与可靠性[12]。在联邦学习等多主体协同建模框架下，这类隐性偏差还可能被持续放大并固化于全局模型之中，削弱算法决策的技术中立性。

3.2.2. 多主体协作开发中的责任可追溯性缺失

在跨平台、跨团队协作开发生成式模型的过程中，算法结构复杂化与可解释性不足，使得系统在发生数据泄露或模型滥用事件时，难以准确定位责任环节。以 Deepfake 防护模型为例，当模型组件由多个开发主体共同维护且基于开源框架快速迭代时，现有的软件许可与使用规范在约束模型二次利用和滥用方面的效力明显下降[13]。这一现象凸显出 GAI 在工程实践中对责任划分机制与技术可追责性设计的迫切需求。

3.2.3. 规则差异下的伦理约束碎片化问题

在跨境贸易数字化应用中，不同平台与行业组织对生物特征数据、合成内容标识及自动化决策的规范侧重点存在差异。当生成式模型被嵌入智能合约或自动执行系统时，规则解释不一致可能导致同一数据在不同系统环境中触发不同的合规与伦理约束，从而增加系统治理复杂度[14]。这种规则碎片化状态在实际运行中削弱了伦理约束的可执行性，也为跨系统协同带来额外不确定性。

GAI 在跨境贸易场景中的应用伴随着算法偏差累积、工程责任模糊以及规则不一致等治理难题。这些问题在多主体协作与自动化决策环境中相互叠加，增加了跨境数据应用的风险复杂度。

3.3. 监管和法律视角

从监管与法律视角来看，如表 1 所示，通过对比各国的数据保护法律《通用数据保护条例》(GDPR)、《加州消费者隐私法案》(CCPA)、《巴西通用数据保护法》(LGPD)、《阿根廷个人数据保护法》(PDPA)、《个人信息保护法》(POPIA)，发现 GAI 对跨境贸易数据流动的安全风险聚焦于三大矛盾[7]。

Table 1. Comparison of data protection laws
表 1. 数据保护法的对比

数据保护法	原则	权利	数据传输	执行
GDPR	合法性、目的限制、准确性、完整性、保密性	访问权、更正权、反对权、数据可移植权	主体充分性决定、标准合同条款、有约束力的规则	数据保护权、罚款
CCPA	知情权、不歧视权、删除权、安全	知情权、删除权、选择权	限制性	加州总检察长、私人侵权诉讼权
LGPD	目的限制、数据最小化、透明度、安全性、非歧视权	访问权、删除权、纠正权、数据可移植权	主体充分性决定	巴西数据保护局、罚款
PDPA	同意、限制、通知、准确性、保护	访问权、更正权、撤回权	主体充分性决定、示范合同条款	个人数据保护委员会、罚款
POPIA	问责制、合法性、目的限制、透明度	访问权、更正权、时代权	限制性	信息监管机构、罚款

3.3.1. 跨系统数据合规的协调挑战

GAI 在跨境数字贸易中的应用，由于训练数据来源多样且跨系统流动，可能导致单一合规措施在部分应用场景下无法完全适用。一些物流企业在 AI 报关系统中同时处理不同来源的数据时，可能触发各系统对数据使用规范的差异要求，形成合规协调难点。该类问题主要体现为数据处理流程中对数据访问、存储和共享规则的不一致性，从而增加系统管理的复杂性和风险。

3.3.2. 知识产权归属与使用权的不确定性

当 GAI 生成的工业设计、产品方案或算法成果在供应链环节流转时，其知识产权归属和使用权界定可能存在不确定性。这种不确定性增加了企业在跨系统部署和交易环节的合规风险，并可能对交易流程和资源分配造成影响。2023 年美墨汽车零部件因 AI 设计成果的专利归属和使用权分配存在模糊性产生争议，导致价值 12 亿美元的订单陷入法律僵局[15]。

3.3.3. 多轨合规体系与运营成本压力

为满足多样化的数据使用规范，企业通常需要建立多轨合规体系，以应对不同平台或系统的规则要求。这种做法虽然能够降低合规风险，但同时增加了运营成本，并可能对中小企业开展数字贸易造成一定门槛。世界银行测算显示，这种“监管套利成本”使中小企业跨境数字贸易门槛提升 40%，实质性构成新型技术性贸易壁垒[16]。

3.4. 技术视角

从技术治理视角观察，GAI 在跨境贸易数据流动中引发了新型安全悖论，如表 2 所示，当前跨境贸易场景中所采用的隐私计算技术在设计目标与适用假设上存在显著差异。具体而言，差分隐私侧重于统计发布阶段的数据匿名化，联邦学习主要服务于多主体协同建模，同态加密与多方安全计算则面向跨域计算过程中的数据不可见性保障。然而，当上述技术被直接引入跨境贸易数据流动场景时，其在实时性、安全性与合规性三个维度上逐渐显现出结构性能力断层[17]。

3.4.1. 联邦学习的合规性陷阱

在跨境供应链协同分析中，联邦学习被广泛视为满足数据本地化合规要求的重要技术路径。然而，该机制在贸易决策高度敏感的场景下，如关税策略、定价模型与产能布局仍面临梯度泄露与模型反推风

险。尤其是在参与方数量有限、模型结构相对稳定的跨国企业联盟中，梯度更新信息可能被用于推断隐含的贸易策略参数[10]。

Table 2. Comparison of privacy-preserving technologies
表 2. 隐私保护技术比较

隐私与安全功能	计算成本	通信消耗
差分隐私	高	正常
联邦学习	正常	高
同态加密	高	高
多方安全计算	稍高	稍高

3.4.2. 同态加密的效率瓶颈

在实时报关与跨境支付验证等高时效贸易场景中，基于全同态加密(FHE)的隐私计算方案虽然能够在理论上实现“数据可用不可见”，但其计算复杂度仍显著高于明文处理。现有研究表明，在典型跨境支付验证任务中，FHE 方案的处理时延可达明文方案的十余倍，从而在实际应用中迫使企业在数据安全性与贸易效率之间进行权衡[6]。

3.4.3. 差分隐私的效用衰减

差分隐私在跨境贸易统计分析与宏观趋势研判中具有较高适用性，但当其被直接用于港口调度、运力配置等高精度决策场景时，噪声注入可能显著削弱预测准确性。全球物流企业运用差分隐私进行货运数据聚合时，噪声注入导致港口吞吐量预测误差率突破 9.2%，引发集装箱空置率上升与碳排放量增加的双重负外部性。这种隐私保护与商业效能的量子纠缠状态，折射出技术方案在跨国场景中的适应局限[5]。

当前技术迭代已进入“隐私不可能三角”的深水区，在隐私计算技术尚难以同时满足跨境贸易对实时性、安全性与合规性的多重要求背景下，相关治理实践可优先从区域合作与行业自律机制入手。在 RCEP 框架下，成员国可围绕 GAI 驱动的贸易数据应用，探索数据标准、模型接口与合规评估机制的先行互认，为更大范围的跨境数据治理积累制度与技术经验。

4. GAI 数据跨境流动的安全风险治理路径

针对上述 GAI 对跨境贸易数据流动的多维风险，构建“技术－规则－伦理”协同治理框架，如图 3 所示，通过以下路径实现风险管控与贸易效能的动态平衡。

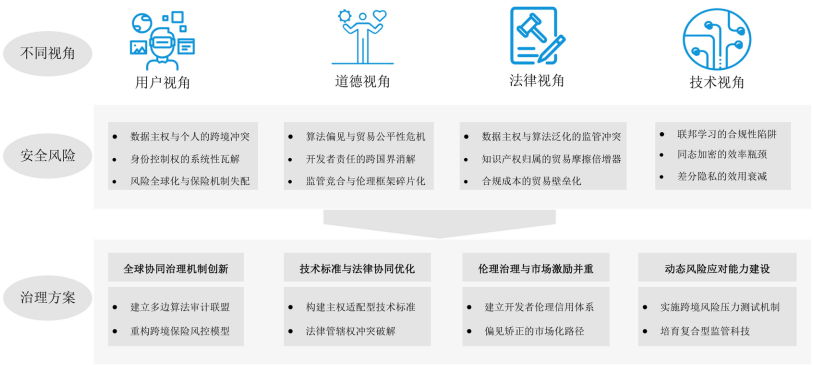

Figure 3. Governance framework for security risks in cross-border data flows
图 3. 数据跨境流动的安全风险治理框架

4.1. 全球协同治理机制创新

为提升算法透明度和跨系统数据治理的可控性，可建立协作型算法审计机制，并推动算法透明度认证标准的互认。针对敏感数据处理场景，可设计动态加密协议，使加密层级能够根据系统策略和使用场景灵活调整，从而降低合规风险。同时，可重构数字贸易和 AI 应用的风险管理模型，设计针对 Deepfake 或生成式内容的风险量化指标，并通过智能合约实现风险缓释和自动化管理，由数据平台和算法开发方按既定规则分担风险，实现技术化和可控的风险治理。

4.2. 技术标准与法律协同优化

构建适应多系统协作的技术标准，制定联邦学习梯度交换的合规白名单，以限制敏感参数的非授权流动。结合同态加密与安全多方计算方案，确保梯度数据在可用的同时保持不可见性。为增强责任可追溯性，可明确训练数据贡献方、算法开发者与应用方的权益分配。与此同时，引入数字身份异常检测机制，当发现生物特征使用异常时，可暂停相关交易流程并触发风险应对流程，实现数据安全、合规性与风险可控的协同治理。

4.3. 伦理治理与市场激励并重

建立开发者伦理信用体系，推行全球开发者道德护照制度，并在开源社区的 GAI 工具包中嵌入伦理影响标签。对于违规行为者，将纳入数字贸易黑名单，限制其算法的跨境部署权限。同时，探索偏见矫正的市场化机制，设立算法偏见对冲交易市场，允许企业购买“偏见矫正期权”，在因算法误判造成损失时获得相应补偿，从而形成技术约束与经济激励相结合的治理模式。

4.4. 动态风险应对能力建设

实施跨境风险压力测试机制，由国际货币基金组织主导建设 GAI 贸易冲击模拟系统，每季度评估包括 Deepfake 攻击、算法偏见等场景对全球供应链的传导效应，并生成供应链韧性提升指南。企业必须通过数字贸易安全成熟度认证，方可接入主要经济体的跨境数据通道。同时，推动复合型监管科技发展，开发监管沙盒的跨境镜像系统，允许企业在虚拟环境中测试 GAI 应用的合规性，从而实现风险预警、合规验证与治理创新的有机结合。

5. 结语

作为跨境贸易数字化转型的重要技术驱动力，GAI 在提升贸易流程智能化水平、优化业务决策效率的同时，也因技术滥用风险与治理机制滞后暴露出多层次安全隐患。已有研究表明，在用户层面，生物特征伪造与数字身份失真问题已对现有身份认证与风险分担机制提出挑战；在技术与伦理层面，算法偏差、模型决策不透明以及责任界定模糊，可能影响贸易参与主体之间的公平协作与信任基础；同时，合规要求差异与技术实现成本的叠加，进一步加重了跨主体数据共享与系统对接的复杂性。针对上述问题，本文从多主体协作视角出发，提出涵盖协同治理机制、技术与规则协同设计、责任约束与激励并重以及动态风险评估的综合治理路径，为相关平台与企业在推进智能化应用过程中实现风险可控提供参考。未来研究可进一步关注 GAI 与区块链、隐私计算等技术的融合应用，并探索跨系统、跨平台数据治理规则的互操作性设计，以适应数字贸易生态的持续演进。

基金项目

云南省教育厅科学研究基金项目“基于区块链的跨境贸易数据存储与流动安全研究(2025Y0820)”。

参考文献

[1] Liu, Y., Huang, J., Li, Y., Wang, D. and Xiao, B. (2024) Generative AI Model Privacy: A Survey. *Artificial Intelligence Review*, **58**, Article No. 33. https://doi.org/10.1007/s10462-024-11024-6

[2] Quintais, J.P. (2025) Generative AI, Copyright and the AI Act. *Computer Law & Security Review*, **56**, Article ID: 106107. https://doi.org/10.1016/j.clsr.2025.106107

[3] 唐岚敕, 袁中华. 信用数据跨境流动安全风险的全链条规制方案建构[J]. 征信, 2025, 43(3): 28-36.

[4] 马其家, 冯慧敏. 跨境生成式人工智能服务贸易的障碍与中国因应[J]. 亚太经济, 2024(5): 88-99.

[5] 张亮, 陈希聪. 生成式人工智能背景下的跨境数据安全规制——基于 DeepSeek、ChatGPT 等主流 AI 的思考[J]. 湖北大学学报, 2025, 52(2): 120-128, 199.

[6] 斜晓东. 论生成式人工智能推进应用中的能源数据安全“分类分级治理体系”建构——基于国家大安全的审视[J]. 法学论坛, 2025, 40(2): 114-127.

[7] 黄锫. 人工智能大模型训练数据的风险类型与法律规制[J]. 政法论丛, 2025(1): 23-37.

[8] 聂立泽, 王祯. 生成式人工智能对数据安全保护的挑战及刑法应对[J]. 河南社会科学, 2025, 33(1): 56-63.

[9] 李想. 生成式人工智能的数据安全风险与刑法应对[J]. 湖南社会科学, 2024(5): 98-107.

[10] Yang, Y., Zhang, B., Guo, D., Du, H., Xiong, Z., Niyato, D., *et al.* (2024) Generative AI for Secure and Privacy-Preserving Mobile Crowdsensing. *IEEE Wireless Communications*, **31**, 29-38. https://doi.org/10.1109/mwc.004.2400017

[11] 牛建国, 夏飞龙. AIGC 促进跨境电商高质量发展的机制研究[J]. 企业经济, 2023, 42(10): 85-94.

[12] Krakowski, S. (2025) Human-AI Agency in the Age of Generative AI. *Information and Organization*, **35**, Article ID: 100560. https://doi.org/10.1016/j.infoandorg.2025.100560

[13] Madaan, G., Asthana, S.K. and Kaur, J. (2024) Generative AI: Applications, Models, Challenges, Opportunities, and Future Directions. In: Sankar, J.G. and David, A., Eds., *Generative AI and Implications for Ethics, Security, and Data Management*, IGI Global, 88-121. https://doi.org/10.4018/979-8-3693-8557-9.ch004

[14] 李艳华. 国际贸易法下跨境数据流动模板条款的平衡: 核心、结构与适用[J]. 国际经济法学刊, 2025(1): 58-80.

[15] 姜玉妍, 刘学东, 徐沛原. 美墨经济一体化进程中的供应链转移与中国供应链安全[J]. 拉丁美洲研究, 2025, 47(4): 60-80, 163-164.

[16] Wang, N., Wang, X. and Su, Y. (2024) Critical Analysis of the Technological Affordances, Challenges and Future Directions of Generative AI in Education: A Systematic Review. *Asia Pacific Journal of Education*, **44**, 139-155. https://doi.org/10.1080/02188791.2024.2305156

[17] Chen, Y. and Esmaeilzadeh, P. (2024) Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges. *Journal of Medical Internet Research*, **26**, e53008. https://doi.org/10.2196/53008