文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

大模型智能体背景下数据跨境交易安全分析：风险谱系、制度约束与治理框架综述

林飞
山东大学继续教育学院
DOI:10.32629/acair.v4i2.20505

[摘　要] 随着数据要素市场化配置持续推进以及跨境数据流成为数字贸易、全球研发和平台协同的重要基础,数据跨境交易已由静态的数据包转移和接口授权,扩展为面向模型训练、智能决策与跨域协同的数据服务交易。大模型智能体借助任务规划、工具调用、检索增强生成、长期记忆和多智能体协作等能力,显著提升了跨境数据利用效率,但也同步放大了提示注入、工具越权、记忆污染、交易后用途失控、跨法域责任不清等复合风险。本文在梳理数据跨境流动制度演进和智能体技术特征的基础上,从概念边界、作用机制、风险谱系、制度约束和安全技术五个层面综述相关研究,并提出涵盖Data、Agent、Compliance、Transaction的DACT全生命周期治理框架。研究认为,在大模型智能体背景下,数据跨境交易安全的分析对象已经由“数据是否出境”扩展为“数据、模型、工具、记忆与衍生结果能否被分类识别、最小化调用、持续审计并实现跨境可追责治理”。
[关键词] 大模型智能体；数据跨境交易；数据出境；数据安全；提示注入；隐私增强技术；合规治理；数据要素
中图分类号：TV149.2　文献标识码：A

Security Analysis of Cross-Border Data Transactions in the Context of Large Model Agents: A Review of Risk Spectrum, Institutional Constraints, and Governance Framework

Fei Lin
School of Continuing Education, Shandong University

[Abstract] With the market-oriented allocation of data factors and the increasing importance of cross-border data flows, cross-border data transactions have expanded from static data transfer to data-service transactions for model training, intelligent decision-making, and cross-domain collaboration. Large model agents improve the efficiency of cross-border data use through planning, tool invocation, retrieval-augmented generation, long-term memory, and multi-agent cooperation, but also amplify risks such as prompt injection, tool overreach, memory contamination, post-transaction loss of purpose control, and unclear responsibility across jurisdictions. This paper reviews related research from conceptual boundaries, mechanisms, risk spectrum, institutional constraints, and security technologies, and proposes a DACT full-lifecycle governance framework covering Data, Agent, Compliance, and Transaction. The study argues that cross-border data transaction security in agent scenarios should focus on whether data, models, tools, memory, and derivative results can be classified, minimized, continuously audited, and governed with accountability.
[Key words] large model agents; cross-border data transactions; data export; data security; prompt injection; privacy-enhancing technologies; compliance governance; data factors

1 引言

数据作为兼具非竞争性、可复制性和规模报酬递增特征的新型生产要素，正在重塑国际贸易与数字产业分工。中国“数据二十条”从数据产权、流通交易、收益分配和安全治理四个方面部署数据基础制度建设，“数据要素×”三年行动计划则进一步强调通过多场景融合释放数据要素的放大、叠加和倍增

效应[1-2]。在此背景下,数据交易已从单纯的数据资源转让,拓展为数据产品、数据接口、数据服务和模型能力交易的复合形态。

与此同时,跨境数据流已经成为国际贸易协同、跨国研发、跨境电商、金融服务和人工智能训练的重要基础,但其也伴随着隐私保护、商业秘密、知识产权、国家安全与监管触达等问题。OECD将“可信数据自由流动”(Data Free Flow with Trust,DFFT)概括为在促进跨境数据流动的同时维护必要监管和保护的制度平衡[11]。因此,数据跨境交易的核心矛盾并非单纯的“流动”或“限制”,而是如何在价值实现与风险控制之间建立可信中介。

近年来,以大语言模型为核心的大模型智能体快速演进。相较于传统模型调用,智能体不仅能够理解目标、分解任务、调用工具、访问外部知识和执行动作,还能够形成长期记忆并与其他智能体协同[13-17]。在这种技术条件下,数据跨境交易不再只是一次性“出境传输”,而可能演变为由智能体持续检索、调用、推理、加工、再分发和记录的动态过程。现有研究往往分别讨论数据出境合规、大模型安全或数据交易制度,对三者交叉场景下的系统性治理关注不足。基于此,本文围绕概念边界、机制变化、风险谱系、制度约束及治理框架展开综述,重点回答大模型智能体如何重构数据跨境交易安全问题。

2 概念界定与研究脉络

2.1大模型智能体的技术内涵

大模型智能体可被理解为以大语言模型为认知中枢,结合规划、记忆、工具调用、检索增强生成、多智能体通信和外部执行环境的复合软件系统。其风险单元不只是模型本身,还包括提示上下文、向量库、插件、API、身份权限与执行链路[13-17]。因此,智能体安全并不等同于传统模型安全,而更接近“模型—工具—数据—权限”的系统安全。

2.2数据跨境交易的范围重构

数据跨境交易不应被狭义理解为数据库整体迁移或文件出境,它至少包括四类形态：一是数据资源或数据产品的跨境许可、订阅与转让；二是API、SaaS、云数据库和数据空间带来的跨境调用；三是模型训练、微调、评测与推理过程中的数据输入、输出和衍生参数流动；四是分析报告、知识图谱、嵌入向量、标签结果和合成数据等加工结果的跨境交付。由此,即便原始数据未整体离境,其片段、特征、日志、记忆和推理结果仍可能构成实质性跨境流动。

2.3研究脉络与不足

现有研究大致沿四条路径展开：其一是围绕数据要素市场、数据确权、数据资产化和数据交易制度的研究[1-2]；其二是围绕个人信息保护、重要数据识别、标准合同、认证和充分性机制的跨境合规研究[3-10]；其三是围绕LLM智能体架构、提示注入、工具滥用、记忆污染和多智能体可信协作的安全研究[13-17]；其四是围绕差分隐私、联邦学习、安全多方计算、同态加密和可信执行环境等隐私增强技术的可信数据共享研究[12][18-23]。不足之处在于,相关文献多将“数据跨境”“智能体安全”“数据交易”分别讨论,尚未充分解释智能体自治能力如何将数据跨境交易的风险从传输风险扩展为执行风险。

2.4安全分析边界的扩展

传统数据安全通常将关注点放在机密性、完整性、可用性和越权访问控制上,而智能体场景下还必须纳入交易安全、行为安全和责任安全。所谓交易安全,是指数据标的、授权范围、使用期限和收益分配是否清晰；行为安全,是指智能体是否按预定权限和目标执行；责任安全,则是指跨境过程中谁应负责举证、通知、补救和赔偿。只有将三类安全与个人信息保护、国家安全和行业监管要求统合,才能形成真正适配智能体场景的分析边界。

3 大模型智能体重构数据跨境交易的机制

大模型智能体至少通过三种机制改变数据跨境交易。首先,交易对象从静态交付转向动态调用。传统交易更多表现为离线数据包交付、数据库访问授权或固定接口订阅；而智能体能够依据任务目标自动检索境内外数据库、调用跨境SaaS和MCP/工具接口、读取文件并触发外部工作流。交易行为由“交付时点”拓展为“检索—调用—推理—输出—记录”的全过程,风险也随之分布到各个环节。

其次,交易关系从单次传输转向持续交互。长期记忆和上下文缓存使一次授权可能演化为持续查询、持续训练和持续推理。数据被写入向量库、日志系统或会话记忆后,可能在原始目的结束后继续被引用,甚至被纳入后续模型微调和再销售流程。删除原始文件并不等于消除所有出境痕迹,嵌入向量、缓存结果、审计日志和衍生知识都可能形成新的存留点。

再次,责任结构从单一处理者转向复合责任链。智能体场景中通常同时存在数据提供方、模型服务商、云平台、工具提供商、插件开发者、向量数据库服务商、跨境接收方和终端用户。若低权限智能体通过提示注入诱导高权限智能体调用外部接口并导出敏感数据,单纯按照“谁接收数据谁负责”的传统思路已难以充分覆盖[15-17]。责任配置需要延伸到代理关系、权限配置、供应链审查和日志可追踪性上。

进一步看,智能体还可能把原本分散的跨境环节内嵌到自动化业务流程中。例如,在跨境采购、全球客服或研发协同场景中,智能体可根据任务自动比价、验真、生成合同草案、触发审批、下单并回传结果；当数据调用、合同执行和支付指令被同一工作流串联时,任何局部失控都可能迅速演变为跨境合规违约。这也是为什么智能体交易治理需要同时面向数据、行为和业务流程设计控制点。

因此,数据跨境交易安全分析应从“数据有没有出境”升级为“智能体如何决定出境、调用什么数据、能否被限制、调用后如何审计以及结果是否继续扩散”的连续治理问题。

4 风险谱系及典型场景

在大模型智能体场景下,数据跨境交易风险呈现出技术风险、数据风险、交易风险和合规风险相互耦合的特点。其中,

最值得警惕的并非单一攻击点,而是“提示注入—工具滥用—数据外泄—记忆残留—二次扩散”的链式失控。表1概括了当前较具代表性的风险类型及其治理要点。

表1 大模型智能体场景下数据跨境交易的主要风险谱系

风险类别	典型表现	治理要点
提示注入与目标劫持	外部网页、邮件、文档或 API 返回中嵌入恶意指令,诱导智能体泄露数据或改变任务目标	外部输入消毒,指令/数据隔离,高风险动作人工确认
工具滥用与权限提升	智能体自动调用数据库、云盘、邮件、支付或命令执行工具,触发未授权跨境传输	最小权限,工具白名单,操作分级与显式授权
记忆与 RAG 污染	恶意内容写入长期记忆或向量库,导致后续检索与决策持续偏移	记忆隔离,来源校验,索引审计,过期与删除机制
数据外泄与再识别	通过输出、日志、参数或拼接外部数据造成个人信息、商业秘密和匿名数据重识别	DLP、脱敏、差分隐私、合成数据与再识别测试
供应链与模型污染	模型、插件、MCP 工具、数据集或中间件被污染,成为跨境泄露通道	供应商审查,签名校验,SBOM/AI-BOM 与持续监测
交易后用途失控	境外接收方超范围使用、再训练、再销售或向第三方转移,原授权边界失效	用途限制条款,删除/撤回机制,用途审计与可追踪授权

上述风险并非彼此孤立。例如,提示注入可能诱导智能体错误调用外部工具,进而造成合同文本、客户画像或实验数据的跨境泄露;泄露出的数据若被写入智能体记忆,又会在后续会话中转化为更隐蔽、更持久的风险源。这种链式耦合使得传统基于“传输时点”或“单次接口”的安全控制显得不足。

典型场景至少包括三类:其一是跨境客户服务与营销场景,智能体可能同时访问境内CRM、境外工单系统和第三方广告平台,导致用户画像在多法域间自动扩散;其二是跨国研发与供应链协同场景,智能体可能调用境内生产数据与境外实验平台、云算力和模型服务,实现高效协同的同时放大商业秘密和重要数据暴露风险;其三是数据经纪和数据交易平台场景,智能体在撮合、定价、验真和交付过程中会生成大量衍生信息,这些信息本身也可能构成新的交易对象或新的泄露点。

从风险传导路径看,智能体风险具有明显的“低门槛触发—高权限放大—跨系统扩散”特征。攻击者往往只需控制一个看似低风险的输入入口,例如公开网页、第三方知识库或工单文本,即可能通过间接提示注入影响具有高权限的企业智能体。由于智能体常与邮件、代码仓库、ERP、CRM和云盘等系统联动,风险会迅速穿透技术边界,从信息安全事件升级为合同违约、个人信息侵权甚至行业监管处罚。

5 跨境制度约束与治理工具

5.1中国路径：从严格审批走向分类分级和便利化流动

中国已逐步形成“安全评估—标准合同—认证—豁免—负面清单”的数据出境制度框架。《数据出境安全评估办法》确立了事前评估与持续监督相结合的基本逻辑[3];《促进和规范数据跨境流动规定》进一步明确,对国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等场景中不包含个人信息或重要数据的数据出境,可以免予安全评估、标准合同或认证,并引入自贸试验区负面清单机制[4][24];《网络数据安全管理条例》自2025年1月1日起施行,明确了网络数据处理活动和个人信息出境的基本条件[5];《个人信息出境标准合同办法》和《个人信息出境认证办法》分别完善了标准合同与认证路径,其中认证办法于2025年公布、自2026年1月1日起施行[6-7]。总体看,中国制度正在由“一般性严格控制”转向“分类分级、风险导向、便利与安全并重”,但对于日志、嵌入向量、长期记忆和衍生输出等智能体特有对象,仍需更细化的识别与规则衔接。

5.2欧盟路径：数据保护、数据共享与AI风险治理叠加

欧盟以GDPR第五章的国际传输规则为基础,强调向EEA以外转移个人数据时仍应维持与EEA内部相当的保护水平,常见机制包括充分性认定、标准合同条款和其他适当保障[8]。在此之上,Data Act自2025年9月起适用,强化了公平访问和使用数据、用户权利、数据共享和云服务切换等制度安排[10];AI Act则自2024年生效并分阶段适用,已对禁止性实践、AI素养义务和GPAI模型治理提出要求[9]。因此,欧盟场景下的数据跨境交易并非仅受“能否传输”约束,还要接受“数据共享是否公平”“模型是否透明可控”“高风险AI是否满足风险管理要求”的复合审查。

5.3国际框架与技术治理工具

OECD将DFFT概括为在促进跨境数据流动的同时,确保数据跨境后仍获得必要监督和保护的国际协调思路[11]。围绕这一目标,隐私增强技术逐渐成为连接“流动”与“保护”的关键工具。OECD 2025年报告指出,可信执行环境、联邦学习、安全多方计算、差分隐私和同态加密等PETs能够在降低原始数据暴露的同时支持AI模型协同开发,但其效果仍受效能、成本和适用场景限制[12]。与此同时,OWASP、NIST和ISO分别从智能体安全、AI风险管理和管理体系角度提供了可操作的治理基线[16-22]。表2对主要制度与治理框架作简要比较。

表2 主要制度与治理框架比较

维度	中国	欧盟/国际
核心逻辑	安全与有序流动并重,强调分类分级、重要数据识别与持续监管	以基本权利保护为底层逻辑,并叠加数据共享公平与可信 AI 风险治理
跨境路径	安全评估、标准合同、认证、豁免和自贸试验区负面清单并行	充分性认定、SCC/BCR、例外机制,以及 Data Act、AI Act 的复合约束
智能体治理启示	应将日志、向量、记忆和衍生输出纳入识别与审计范围	应关注 onward transfer、透明度、高风险系统义务和 GPAI 模型责任
通用技术工具	数据分类分级、脱敏、水印、审计日志和访问控制	DFFT、PETs、NIST AI RMF、ISO/IEC 42001 与 OWASP 控制基线

从制度协调角度看,中国与欧盟并不存在简单的“宽”与“严”二分,而是在风险识别对象和治理重心上存在显著差异。中国更强调重要数据、国家安全和分类分级基础上的可控流动,欧盟更强调个人数据跨境后的等同保护、数据共享公平以及高风险AI的基本权利影响。这种差异意味着跨国企业仅完成单一法域的合规清单远远不够,还需要构建可以映射不同规则体系的统一数据台账、传输影响评估与证据留存机制。

6 面向智能体的数据跨境交易全生命周期治理框架

为避免治理停留在静态合规审查层面,本文提出DACT(Data

-Agent-Compliance-Transaction)全生命周期治理框架,其核心是将数据对象、智能体行为、合规路径和交易合同纳入同一控制闭环。

第一,Data维度强调交易前治理。组织应建立数据资产目录和元数据说明,对个人信息、敏感个人信息、重要数据、商业秘密和行业敏感数据进行分类分级,并依据GB/T 43697-2024等标准识别是否确有出境必要[23]。在不具备必要性的场景下,应优先采用境内处理、最小化字段出境、脱敏、匿名化、合成数据或结果替代等路径,而不是默认输出原始数据。

将DACT落实到操作层面,还需要按照“交易前—交易中—交易后”划分控制要求：交易前重点核验数据来源、权属和合法基础,完成分类分级、最小必要判断及影响评估；交易中重点控制智能体的身份、工具、上下文和输出,避免越权检索、批量导出和隐蔽外发；交易后则应围绕用途追踪、删除撤回、日志留存、模型记忆清理和争议举证建立可验证机制。

第二,Agent维度强调交易中的行为约束。智能体应采用最小权限原则,只允许访问完成当前任务所必需的数据和工具;对导出、批量查询、外发邮件、写入云盘、调用外部API等高风险动作设置显式授权和人类在环确认[16-17]。同时,应对提示词、网页、邮件、工具返回值等外部输入进行不可信处理,对长期记忆设置隔离、过期、删除和审计机制,并通过消息签名、身份校验和上下文边界控制保障多智能体通信安全。

第三,Compliance维度强调交易前后的合规连续性。对于涉及个人信息或重要数据的场景,应在数据出境安全评估、个人信息保护影响评估和接收方尽职调查基础上,动态判断是否适用安全评估、标准合同、认证或豁免规则[3-10]。在欧盟相关业务中,还需额外评估onward transfer、合同公平性以及AI Act下的透明度与GPAI义务[8-10]。

表3 交易前—交易中—交易后安全控制矩阵

阶段	主要风险	控制要点
交易前	权属不清、数据分类错误、出境必要性判断失准、合法基础不足	建立数据目录与元数据说明,完成PIA/DPIA或数据出境影响评估,执行最小必要原则
交易中	越权访问、提示注入、工具滥用、跨境批量导出、日志泄露	最小权限、工具白名单、上下文隔离、输出过滤、人类确认和实时审计
交易后	二次使用、再训练、再销售、记忆残留、删除不彻底、举证困难	用途追踪、删除/撤回、日志留存、模型记忆清理、水印和违约追责

第四,Transaction维度强调将技术控制写入交易规则。数据交易合同不应只描述标的和价格,还应明确授权范围、处理目的、保存期限、可否进入模型训练集、可否再销售或转许可、删除与撤回机制、日志留存方式、审计权和争议解决安排。对于智能体自动执行的交易,应特别约定代理权限边界、异常处置流程以及第三方工具和云服务商的责任分担。

上述四个维度需要通过技术工具和管理体系落地：在技术层,可引入联邦学习、安全多方计算、可信执行环境、同态加密、差分隐私和数据clean room以降低原始数据跨境暴露；在组织层,可结合NIST AI RMF、Generative AI Profile、ISO/IEC 42001与ISO/IEC 27001建立持续的风险识别、控制、审计和改进机制[12][18-22]。由此,数据跨境交易治理可以形成“交易前分类评估—交易中权限约束—交易后用途追踪与审计问责”的闭环。

除技术和合同控制外,组织还应把智能体所依赖的模型、插件、数据服务和云基础设施纳入供应链治理。对外部模型或工具的更新应建立版本备案、兼容性测试和风险复核机制；对关键供应商应要求安全承诺、审计接口和事件通报义务。只有把智能体治理嵌入采购、研发、法务和内控流程,才能避免安全控制停留在单一系统层面。

7 研究展望与结论

总体来看,大模型智能体使数据跨境交易从“数据转移”演化为“数据、模型、工具、记忆与行动链条的复合流动”。因此,交易安全已不再只是网络传输加密或静态合规审查问题,而是涉及数据对象识别、智能体权限控制、模型供应链可信、跨境法律责任分配与持续审计的系统性治理议题。

未来研究至少应关注五个方向:其一,智能体跨境调用行为的可解释、可验证与可审计机制；其二,嵌入向量、长期记忆、合成数据和模型衍生知识是否构成新的交易标的及其权属边界；其三,多智能体系统中的责任链和举证机制；其四,隐私增强技术在真实数据交易场景下的经济成本、性能损失与合规收益评估；其五,面向智能体的数据跨境交易标准体系、监管沙盒与可验证合规基础设施建设。

综上,在大模型智能体背景下,数据跨境交易安全的治理思路应由“以传输为中心”转向“以行为、用途和责任为中心”。只有把数据分类分级、智能体最小权限、跨境合法基础、合同用途限制、持续日志审计和组织级AI风险管理整合为统一框架,才能在促进数据高效流动与维护安全可信之间实现更稳健的平衡。

[参考文献]

[1]中共中央,国务院.中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见[EB/OL].(2022-12-19)[2026-05-20].https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm.

[2]国家数据局等17部门.“数据要素×”三年行动计划(2024—2026年)[EB/OL].(2023-12-31)[2026-05-20].https://www.cac.gov.cn/2024-01/05/c_1706119078060945.htm.

[3]国家互联网信息办公室.数据出境安全评估办法[EB/OL].(2022-07-07)[2026-05-20].https://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm.

[4]国家互联网信息办公室.促进和规范数据跨境流动规定[EB/OL].(2024-03-22)[2026-05-20].https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm.

[5]中华人民共和国国务院.网络数据安全管理条例[EB/OL].(2024-09-30)[2026-05-20].https://www.cac.gov.cn/2024-09/30/c_1729384452307680.htm.

[6]国家互联网信息办公室.个人信息出境标准合同办法[EB/OL].(2023-02-24)[2026-05-20].https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm.

[7]国家互联网信息办公室,国家市场监督管理总局.个人信息出境认证办法[EB/OL].(2025-10-17)[2026-05-20].https://www.cac.gov.cn/2025-10/17/c_1762449728720008.htm.

[8]European Union.Regulation(EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[EB/OL].(2016-04-27)[2026-05-20].https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[9]European Union.Regulation (EU)2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence[EB/OL].(2024-06-13)[2026-05-20].https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

[10]European Union. Regulation(EU)2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data[EB/OL].(2023-12-13)[2026-05-20].https://eur-lex.europa.eu/eli/reg/2023/2854/oj.

[11]OECD.Fostering Cross-Border Data Flows with Trust[R].Paris:OECD Publishing,2022:OECD Digital Economy Papers, No.343.https://doi.org/10.1787/139b32ad-en.

[12]OECD.Sharing Trustworthy AI Models with Privacy-Enhancing Technologies[R].Paris:OECD Publishing,2025:OECD Artificial Intelligence Papers,No.38.https://doi.org/10.1787/a266160b-en.

[13]WANG L,MA C,FENG X,et al.A Survey on Large Language Model based Autonomous Agents[J].Frontiers of Computer Science,2024,18(6):186345.https://doi.org/10.1007/s11704-024-40231-1.

[14]GUO T,CHEN X,WANG Y,et al.Large Language Model based Multi-Agents:A Survey of Progress and Challenges[C]//Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence.2024:8048-8057. https://doi.org/10.24963/ijcai.2024/890.

[15]GAN Y,YANG Y,MA Z,et al.Navigating the Risks: A Survey of Security, Privacy, and Ethics Threats in LLM-Based Agents[EB/OL].(2024-11-14)[2026-05-20].https://arxiv.org/abs/2411.09523.

[16]OWASP.AI Agent Security Cheat Sheet[EB/OL].[2026-05-20].https://cheatsheetseries.owasp.org/cheatsheets/AI_Agent_Security_Cheat_Sheet.html.

[17]OWASP. OWASP Top 10 for Agentic Applications for 2026[EB/OL].(2025-12-09)[2026-05-20].https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/.

[18]NIST.Artificial Intelligence Risk Management Framework(AI RMF 1.0)[R].Gaithersburg: National Institute of Standards and Technology,2023.https://doi.org/10.6028/NIST.AI.100-1.

[19]NIST.Artificial Intelligence Risk Management Framework:Generative Artificial Intelligence Profile[R].Gaithersburg: National Institute of Standards and Technology,2024.https://doi.org/10.6028/NIST.AI.600-1.

[20]NIST.Guidelines for Evaluating Differential Privacy Guarantees: NIST SP 800-226[R].Gaithersburg: National Institute of Standards and Technology,2025.https://doi.org/10.6028/NIST.SP.800-226.

[21]ISO.ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system[S/OL].2023[2026-05-20].https://www.iso.org/standard/81230.html.

[22]ISO.ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements[S/OL].2022[2026-05-20].https://www.iso.org/standard/27001.

[23]国家市场监督管理总局,国家标准化管理委员会.GB/T 43697-2024数据安全技术数据分类分级规则[S/OL].2024[2026-05-20].https://std.samr.gov.cn/gb/search/gbDetailed?id=14156507D2210337E06397BE0A0AE656.

[24]国家互联网信息办公室.数据出境安全管理政策法规问答(2026年1月)[EB/OL].(2026-01-30)[2026-05-20].https://www.cac.gov.cn/2026-01/30/c_1771505108953002.htm.

作者简介：

林飞(1974--),男,汉族,山东乳山人,大学本科,副研究员,研究方向为网络安全和信息化。