工程与管理科学
Engineering and Management Science
第 7 卷◆第 10 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

# 生成式人工智能赋能龙江数据跨境高质量发展路径研究

王熠　曲家兴（通讯作者）　白瑞　杨霄璇　肖鸿江
黑龙江省网络空间研究中心　黑龙江哈尔滨　150090

DOI：10.12238/ems.v7i10.15766

［摘　要］随着数据成为“五大生产要素”，黑龙江省数据跨境以“数据合同出境”为主导，但面临管理标准碎片化、合同合规不足、审核效率低等问题。本文以 DeepseekR1-14B、豆包 1.6 为测试模型，探索生成式 AI 的赋能路径，构建“制度-技术-管理”风险防控机制，并提出专项管理办法、专用 AI 模型等对策。研究表明，AI 可高效解决人工审核痛点，助力龙江深化对俄数据合作，打造东北亚数据要素流通枢纽。

## 引言

2020 年数据被纳入“五大生产要素”，2024 年“数据要素乘”计划进一步释放其价值，数据跨境需求激增。黑龙江省作为对俄合作核心与“一带一路”节点，数据跨境服务国企海外项目及自贸区贸易，却受标准碎片化、效率低等制约。生成式 AI 具备文本比对、合规校验能力，本地部署兼顾安全与效率。本文旨在探索 AI 赋能路径与风险防控，为龙江数据跨境高质量发展提供支撑。

## 1.相关理论与技术基础

### 1.1 数据要素化理论

数据要素属性随技术演进持续升级，2020 年《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》将其与土地、劳动等并列为“五大生产要素”，标志着数据从“辅助决策工具”正式升级为“核心生产要素”。其核心价值在于与其他要素融合产生乘数效应，而数据跨境是实现这一效应的关键载体。我国参考欧盟二元保护模式，通过《个人信息保护法》细化姓名、生物识别信息等个人信息范畴，平衡隐私保护与数据流动；同时，欧盟侧重隐私、美国侧重自由流动、俄罗斯强调本地化存储的监管差异，要求龙江对俄跨境数据流程在合规框架下适配调整[1]。

### 1.2 生成式 AI 技术原理与政务应用特性

生成式 AI 以大模型为核心架构，本文测试选用本地部署的 DeepseekR1-14B 与豆包 1.6，具备文本比对（快速识别多省备案指引异同）、合规性校验（定位合同“敏感信息未授权”条款）、结构化处理（规范评估报告格式）三大能力。本地部署依托龙江政务云物理隔离实现数据“不出网”，既规避云端泄露风险，又符合《数据安全法》中政务数据保密要求。在政务应用中，其可解决人工审核痛点：通过多省指引比对破解标准碎片化，10 分钟内完成万字文档审核提升效率（远超人工 5 个工作日 / 件），依据固定模板生成结论减少主观偏差，精准适配跨境备案需求[2]。

### 1.3 我国数据跨境管理框架与龙江适配性

我国依《促进和规范数据跨境流动规定》设三种出境模式（如表 1）：数据评估出境适配性低（龙江超百万个人信息出境场景极少）；白名单出境适配性中等（自贸区对俄贸易数据多豁免，但产业限制导致需求小）；数据合同出境适配性高（占备案总量 80%，适配国企“一带一路”项目）。此适配特征决定生成式 AI 需重点聚焦数据合同出境的审核流程优化。

表 1　我国数据跨境管理模式对比及龙江适配性分析表

| 管理模式 | 核心适用场景 | 关键要求 | 法律依据 | 龙江适配性分析 |
|---|---|---|---|---|
| 数据评估出境 | 关键信息基础设施运营者出境、超百万个人信息出境 | 向省级网信部门申报安全评估材料 | 《促进和规范数据跨境流动规定》第七条 | 适配性低：超百万个人信息出境场景极少 |
| 白名单出境 | 自贸区数据处理者提供负面清单外数据 | 免评估备案，需省级网信部门批准 | 《促进和规范数据跨境流动规定》第六条 | 适配性中等：对俄贸易数据多豁免，需求规模小 |
| 数据合同出境 | 非关键运营者累计出境 10 万—100 万个人信息 | 签订标准合同并上传省级网信办 | 《促进和规范数据跨境流动规定》第八条 | 适配性高：占备案 80%，适配国企海外项目 |

## 2.黑龙江省数据跨境发展现状与核心问题

### 2.1 龙江数据跨境发展现状

龙江数据跨境以“数据合同出境”为主导模式，占全省备案总量 80%，主要服务两类主体：一是大型国企“一带一路”海外电力、基建项目，需传输驻外员工身份与行程数据、工程进度与设备参数，符合“累计出境 10 万 —100 万个人信息”场景；二是自贸区对俄贸易企业，聚焦食品进口、木材加工、旅游合作，数据出境以经营数据为主，个人信息出境多不满 10 万人。从区域特色看，自贸区对俄数据呈“低敏感、小体量”特征，贸易数据无个人信息属性，个人信息出境符合白名单豁免条件，但因产业集中于一二产，白名单出境实际占比仅 15%。管理上，由省网信办负责备案审核，核心材料包括企业统一社会信用代码、法定代表人及经办人证件、授权委托书、标准合同、个人信息保护影响评估报告，审核分材料查验、合规性审查、结论反馈三环节，依据《黑龙江省个人信息出境标准合同备案指引》设 15 个工作日时限[3]。

### 2.2 龙江数据跨境现存核心问题

一是管理标准碎片化，各省依中央文件制定本地指引，黑龙江与江苏、上海、天津差异显著：非敏感个人信息总量统计起点，黑龙江为“当年 1 月 1 日”，江苏、上海为“上年 1 月 1 日”；备案方式上，天津要求附加电子版光盘，江苏需先线上注册，企业跨区域备案需重复适配，增加成本。二是出境合同合规性不足，待审合同常存敏感信息未获授权、境外接收方处置权超标问题，且境外接收方添加的隐蔽条款（如“数据可用于关联公司业务”）人工难识别。三是评估报告质量参差，编写主体无统一规定（第三方或企业自行编写），存在结构偏离模板（新增“评估原则”“释义”章节）、核心内容缺失（未说明数据向第三方流转情况、整改时限）、格式不规范（正文非四号仿宋、行距非固定 26 磅）问题。四是审核效率低下，人工审核单份材料需 5 个工作日，因材料标准不一、不合理内容隐蔽，实际周期常超 15 个工作日，部分国企海外项目因延迟受影响。

## 3.生成式 AI 赋能龙江数据跨境的风险防控机制

### 3.1 审批合法性风险防控

一是建立垂直领导体系，成立“龙江 AI 辅政工作领导小组”，厅局级领导任组长，副厅局级负责日常管理，正处级主抓具体工作，定期召开会议形成“问题反馈 — 责任落实 — 标准审批 — 流程决策”闭环：企业或审核人员遇 AI 问题可反馈，责任明确到个人，AI 应用标准逐级审批、集体决策，确保符合政策导向。二是推行“三审三校”制度，AI 审核结果经三级人工校验：初级审核员校验结论与法律条款一致性（如“敏感信息未授权”是否合《个人信息保护法》），中级复核问题定位准确性（如不合规条款位置描述），高级审定整改建议可行性（如“补充敏感信息授权程序”是否适配企业），避免 AI 替代行政审批[4]。三是设立举报受理机制，授权省网信办独立处室受理举报，明确“举报 — 核查 — 整改 — 反馈”流程：企业或公众可线上线下举报，受理处室 5 个工作日内核查，确认问题后责令整改，3 个工作日内反馈举报人 。

### 3.2 政务数据泄露风险防控

一是技术架构设计，采用“本地部署 + 物理隔离”模式，在龙江政务云部署 DeepseekR1-14B 专用模型，备案材料仅在政务云内流转，不上云、不联网，规避外部传输泄露；政务云与互联网、其他政务系统物理隔离，降低外部攻击风险。二是权限管控机制，建立“分级授权”体系：仅省网信办审核人员可访问，需“用户名 + 密码 + 动态口令”三重认证；依职责划分权限，初级审核员仅查看结果，中高级可二次操作 AI；操作日志实时记录“人员 — 时间 — 操作内容”，实现访问可追溯，符合《数据安全法》政务数据保密与可追溯要求[5]。

### 3.3 AI 时效性风险防控

一是建立更新机制，每月更新 AI 本地数据库，内容含最新数据跨境政策（如中央网信办指引修订、《个人信息保护法》修订条款）、行业新场景（如对俄数字贸易、跨境电商个人信息传输）、区域监管差异（如俄罗斯数据本地化政策调整）。二是时效性校验，设“AI 无法回答”触发条件，遇新增场景问题（如对俄数字贸易数据出境合规判断），自动触发“人工介入 + 数据库补录”流程：人工先依最新要求审核，再将政策、场景、标准录入数据库，避免信息滞后导致失误。

### 3.4 AI 局限性风险防控

一是数据格式规范，出台《龙江数据跨境备案材料格式要求》，明确备案材料为“结构化文本”，禁图片、扫描件：评估报告按“出境方情况 — 拟出境信息 — 境外接收方 —

影响评估”分章，合同用“条款编号 + 内容”格式，数据统计用表格替代饼图、柱状图。二是技术升级方向，联合哈尔滨工业大学研发“AI 图像识别插件”，通过图像分割提取图形数值与图例，语义分析关联含义（如“蓝色区域 80%”关联“数据合同出境占比 80%”），实现图形结构化转换，弥补图片处理短板。

**4.推动生成式 AI 赋能龙江数据跨境高质量发展的对策建议**

4.1 出台龙江专项管理办法

制定《黑龙江省生成式 AI 辅助数据跨境备案管理办法》，将 AI 辅政纳入法治化轨道。明确 AI 仅为“辅助审核工具”，不可替代人工最终审批，审核结果需经“三审三校”生效，禁止 AI 直接出具“通过”或“不通过”结论；划定审核边界，AI 仅处理合同、评估报告等结构化文本，暂不审核图片、扫描件，待图像识别插件研发后再扩范围；划分责任主体，省网信办负责 AI 模型运维更新，审核人员复核 AI 结果并审定结论，企业保障备案材料真实合规，解决 AI 应用的“权利来源”与“约束力”问题。

4.2 打造龙江专用 AI 模型

联合 Deepseek、字节跳动定制“龙江政务 AI 模型”，提升场景适配性。优化对俄数据跨境适配，添加俄语条款合规校验功能，可识别俄文合同中违反俄罗斯数据本地化的内容，翻译后标注风险点；融入龙江产业特色数据，在数据库中添加对俄食品进口、木材加工、旅游合作的典型跨境案例，如木材贸易订单合规要点、旅游团信息传输授权流程，提升审核精准度；针对国企海外工程合同、自贸区贸易报告等常见材料，预设审核规则与模板，将 AI 深度思考时间从 21 秒缩短至 15 秒内，提升效率。

4.3 开展自贸区试点

在哈尔滨、黑河、绥芬河自贸区开展“AI 审核试点”，验证效果并总结经验。筛选 20 家对俄贸易企业为样本，覆盖食品进口、木材加工、旅游合作领域；重点测试 AI 在“木材进口数据出境”“旅游服务个人信息出境”“食品贸易订单数据出境”场景的准确率、效率与企业满意度；试点周期 3 个月，每月评估一次，针对场景适配不足、结论偏差等问题优化模型与制度，形成“模型优化 — 制度调整 — 效率提升”闭环，试点后向全省推广。

4.4 加强审核人员培训

定期组织省网信办审核人员参加“AI 技术应用培训”，实现“人机协同”。培训含三部分：AI 模型操作培训，讲解材料上传、指令下达、结果查看流程及格式错误修正方法；AI 问题定位解读培训，教授理解“不合规条款”“报告缺失内容”，如分析“敏感信息未授权”条款的法律依据与整改方向；AI 风险防控培训，讲解识别政策更新导致的时效偏差、图形识别失误等问题，掌握“人工介入”触发条件与流程，培训每季度一次，确保人员适配 AI 辅政模式。

**结束语：**

生成式 AI 技术为解决龙江数据跨境现存问题提供了有效路径，通过“标准统一 — 合同校验 — 报告优化 — 效率提升 — 客观保障”五大技术路径，可显著提升龙江数据跨境备案的合规性与效率，将审核周期控制在 15 个工作日内，同时降低人工主观偏差。通过“制度 — 技术 — 管理”三维风险防控机制，可有效规避审批合法性、政务数据泄露、AI 时效性与局限性风险，确保 AI 应用安全合规，为我国边疆地区数据跨境发展提供“龙江方案”。

**[参考文献]**

[1]郭海威，胡正荣.生成式人工智能赋能数字内容创作：逻辑耦合、实践偏差与规范进路[J].传媒观察，2024，(11)：24-35.

[2]董秀萍.新质生产力推动物流业高质量发展的机制与路径研究[J].中国商论，2024，33（18）：98-101.

[3]李猛.“人工智能+”赋能新质生产力发展——内在机理与路径探索[J].北京航空航天大学学报（社会科学版），2024，37（04）：127-137.

[4]卢荣婕.ChatGPT 赋能智慧法院建设：机遇、挑战和规制[J].重庆邮电大学学报(社会科学版)，2024，36(03)：83-93.

[5]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.

通讯作者：曲家兴（1979 年 8 月-），男，汉族，黑龙江省哈尔滨人，研究生，研究员级高级工程师，研究方向：网络安全和信息化。

基金项目：黑龙江省自然科学基金资助项目《数据跨境合规检测与隐私保护技术》（项目编号：JQ2024F001）。