开放群岛开源社区
Open Islands Community

2025

跨境数据流通

合规与技术应用白皮书

The White Paper on Cross-border Data Transfer
Compliance and Technology Applications

开放群岛开源社区跨境数据流通小组
2025年11月

参编单位

(排名不分先后)

开放群岛开源社区跨境数据流通小组

深圳数据交易所有限公司

中国科学院深圳先进技术研究院

粤港澳大湾区大数据研究院

深圳市网络数据合规与流通促进会

深圳市城市交通规划设计研究中心

野村综合研究所

中国移动通信有限公司研究院

粤港澳大湾区大数据中心

广东广和律师事务所

深圳市尚数网科技有限公司

OORTech Inc.

上海同态信息技术有限责任公司

同态信息科技（西安）有限公司

云基华海信息技术股份有限公司

福建新世通律师事务所

中部数据服务（湖北）有限公司

广东卓建律师事务所

参编人员

(排名不分先后)

丁振赣、张巍、古亮、岑芳缘、潘菲、易宥光、王冠、李智慧、李东阳、董宁、赵阳、胡雪晖、张宝龙、陈承正、谢文立、赵亮、李兰兰、高增、史凯、王青兰、刘晨璐、周宏、鲁胜强、林泽坤、欧靖泓、李飞、毕克、倪平宇、方应彬、刘雷、周博宇、陈清、贾蒙、梁迎莹、庄春燕、韩语童、廖晓倩、杨慧娟、冯思鹤、周桓羽、喻炜、信伦、杜娟、孙奇正、金洁华、黄雅君、王蒙、吴桂荣、周冬宝、陈世彪

前言

在数字经济全球化纵深发展的今天，数据作为核心生产要素，其跨境流动已成为连接全球产业链、激活创新动能、推动国际经贸协同的关键纽带。然而，数据跨境流动始终面临“安全与效率”的动态平衡难题——各国数据主权诉求、监管规则差异、技术标准壁垒、隐私保护要求等多重因素交织，既为全球数字经济发展带来挑战，也催生了制度创新与技术突破的迫切需求。

《跨境数据流通合规与技术应用白皮书（2025）》立足全球数据治理新格局与中国数字化转型实践，相较于以往版本，实现了两大核心升级：其一，前瞻性研究维度更深，突破过往以规则解读和案例复盘为主的模式，聚焦 AI+数据跨境、加密资产跨境应用等未来趋势，预判监管政策演进方向；其二，专题研究范围更广，新增数据跨境与货币结算、稳定币监管两大核心专题，填补以往版本在“数据流与资金流协同”领域的研究空白。本书整体聚焦“技术落地、合规实践、产业应用、政策演进”四大核心维度，构建起系统、可落地、前瞻性的理论与实践体系，兼具三大鲜明特点：一是逻辑闭环，以“前瞻探索—技术支撑—产业落地—政策优化”为主线，打通从顶层设计到底层执行的全链路；二是实践导向，整合粤港澳大湾区、金融、汽车、医疗等五大领域标杆案例，提炼可复制的技术路径与合规方案；三是国际视野，对比全球主要司法辖区监管框架差异，为中国参与全球数据治理提供实践参考。

本书内容基于编写时的法律法规、行业实践及技术发展现状整理而成，仅为数据跨境相关领域的研究参考与经验分享，不构成任何法律意见、合规建议或投资决策依据。数据跨境流动涉及的监管政策、技术标准、行业实践处于动态变化中，不同主体的业务场景、合规需求存在差异，读者在实际应用时，应结合自身具体情况，咨询专业法律、合规及技术顾问，自主判断并承担相应责任。本书编写过程中已尽力确保信息的准确性与完整性，但不对内容的绝对准确性、及时性或适用性作出任何明示或暗示的保证，因使用本书内容所产生的任何直接或间接损失，本书编写方不承担相关责任。

全书共分为四章，核心要点如下：

第一章数据跨境新场景、新技术及跨域监管带来的挑战

本章相较于以往版本的规则梳理，更侧重“趋势预判+场景前瞻”，系统梳理全球主要司法辖区（中、美、欧、日）数据跨境监管最新动态，重点解析中国“分级分类、多轨并行”合规框架与美欧治理逻辑差异。新增对 AI 数据跨境、加密资产跨境流动等未来趋势的预判，聚焦来数加工、智能网联汽车、跨境医疗等十大新兴场景，为企业应对监管变化、布局跨境业务提供前瞻性指引，弥补过往版本对新兴领域覆盖不足的短板。

第二章跨境数据流通基础设施构建与技术实践

作为全书技术核心，本章延续技术落地导向，构建“基础安全层－治理合规层－互联互通层－业务应用层”四层总体架构，详解身份认证、数字合约、隐私计算、加密传输等关键模块的技术原理与落地路径。通过深港数据跨境验证平台、汽车行业跨境数据空间等典型案例，具象化展示隐私计算、区块链存证等技术如何破解“数据可用不可见”难题，相较于以往版本，新增技术与行业场景的深度融合分析，提升技术落地的实操参考价值。

第三章稳定币及货币结算体系变革引发的数据跨境规则变化

本章为 2025 版新增核心专题，填补过往版本在数据跨境与资金流协同领域的研究空白。聚焦全球稳定币监管框架成型趋势，对比美欧新中四国稳定币监管规则与实践案例（含 2025 年 Finastra 与 Circle 的 USDC 跨境结算合作等最新案例），重点阐述中国“数字人民币+香港合规稳定币”双轨模式，探讨区块链、智能合约技术如何重构跨境结算逻辑，实现“数据流—资金流—合规流”三流融合，为数据要素市场化配置提供结算解决方案。

第四章数据跨境流动规则与技术演进预测及政策体系优化

本章在以往政策分析的基础上，强化国际协同与产业落地视角，系统分析数据跨境产业生态图谱与技术路线，提出“规范性政策优化+产业性政策引导”的双轮驱动政策体系。新增对 RCEP、CPTPP 等区域协定数据规则的解读，探索与国际规则对接的实操路径；从完善数据分类分级、加强政企沟通、技术驱动监管等维度给出落地建议，同时构建国际合作与外部协同机制，为政策制定者、企业管理者、行业从业者提供兼具实操性与前瞻性的决策参考。

本书期望为政府监管部门、跨国企业、技术服务商、科研机构等相关方提供全景式参考，推动形成“规则清晰、技术先进、产业协同、国际互认”的数

据跨境流动生态，助力中国在全球数字经济竞争中抢占制度性话语权，为全球数据治理贡献中国方案。

目录

第一章 面向未来：数据跨境的政策及新技术、新场景

1.1 数据跨境监管政策现状

欲迎接数据跨境的新一轮挑战，须先看清“脚下的地形”。过去三年，《跨境数据流通合规与技术应用白皮书（2022）》《2023》及《2024》三卷已替读者把全球主要司法辖区关于数据跨境和 AI 监管的立法沿革、监管框架与执法动态测绘成图；若您需要任一国家或地区的完整成文法脉络、历史修订轨迹或更细颗粒度的合规指引，仍可回到过去三年的白皮书进行查阅。然而，规则从未停步——2024 年以来，部分地区“充分性认定”再洗牌、敏感数据“负面清单”扩容、模型权重出境首被纳入许可范围，人工智能跨境算力调度、隐私计算监管认定及大模型训练语料来源合规亦成为执法新焦点。为了让企业在“已知地形”上迅速标出新增暗礁，本章以“政策快照”形式，聚焦重点司法辖区最新立法、执法与标准动态：若规则较白皮书发布之日已有实质性变化，则独立成段详述并给出新合规要点；若仅有微调或尚未落地，则以“更新提示”一笔带过，避免冗余。本节既承接过去三年白皮书的旧地图，又为您实时补上 2024 后的新坐标，使后续的技术方案、落地实践与产业案例拥有清晰且可检索的语境，帮助读者在快速比对中锁定关键差异，踏实迎接下一程跨境合规的新挑战。

1.1.1 国际条约中对数据跨境政策的规定

数据跨境流动的国际条约图景，呈现出“主权让渡”与“规则竞合”并存的独特景观。世界贸易组织（WTO）框架下的《服务贸易总协定》（GATS）率先将“数据”纳入服务贸易范畴，以“隐私例外”“安全例外”为各国预留监管切口：只要措施“必要”“非歧视”，即可对跨境传输设限。这一“原则放行、例外设卡”的思路，成为后续所有区域协定的底层代码。1997 年的《信息技术产品协议》（ITA）则通过零关税为数据载体扫清物理障碍，却将“非关税壁垒”留给成员自行解释，为数据本地化埋下伏笔。2019 年 76 个成员签署的《关于电子商务的联合声明》试图在 WTO 内再升级，却因发达成员与发展中成员对“数据自由流动”与“公共政策例外”的立场泾渭而陷入停滞，凸显多

边层面“共识赤字”的僵局。

当多边列车减速，区域轨道反而提速。《区域全面经济伙伴关系协定》（RCEP）在电子商务章复制了 GATS 的“原则+例外”结构，却首次以负面清单方式禁止将数据本地存储作为市场准入条件，同时为金融、电信等敏感行业单开“合法公共政策”后门，形成“大体自由、重点设防”的亚洲模板。《全面与进步跨太平洋伙伴关系协定》（CPTPP）则把门槛进一步拉高：数字产品非歧视、禁止强制开放源代码、永久免征电子传输关税，例外条款却被压缩到“不构成任意或不合理歧视”且“不超过实现目标所需限度”，实质上将“自由优先”锁定为高标准范式。更具信号意义的是《数字经济伙伴关系协定》（DEPA）——全球首部专司数字议题的专项条约，它将个人信息保护兼容机制、数据监管沙盒、可信任标志互认等柔性工具成文化，为中小经济体提供“菜单式”合规选项，也标志着数据规则从“边境措施”走向“边境后治理”的纵深。

在双边层面，条约功能转向“信任背书”。欧盟通过《通用数据保护条例》（GDPR）搭建的“充分性认定”机制，将自身权利本位标准输出为事实上的全球基准：截至 2025 年，仅 15 个国家被列入白名单，日本、韩国、英国等获准数据自由流入欧盟，而印度、巴西、土耳其仍在评估队列。美国则借《澄清海外合法使用数据法案》（CLOUD Act）确立“数据主权属人主义”，无论数据存储于何处，只要服务提供者受美国管辖即可被强制调取；作为对冲，欧盟与美国三度更迭的《跨大西洋数据隐私框架》以行政协议方式复活“充分性”，通过新增双层救济与独立仲裁庭，为欧美间万亿美元数字贸易提供“绿色通道”。日欧经济伙伴关系协定中的“数据自由流动与隐私保护并存”条款，首次在双边层面实现 GDPR 标准与亚太自由模式的嫁接，为后续中日、中韩谈判提供可复制文本。

纵览主要条约，监管方向已出现三重位移：其一，合法性基础从“同意”单点走向“多元正当性”，合同履行、法定义务、公共利益与数据主体利益平衡共同构成传输依据；其二，工具箱从“安全评估”一元扩展至标准合同、约束性公司规则、认证、行为准则等多轨并行，企业可依据业务场景“拼插”合规路径；其三，话语权争夺从“规则制定”下沉到“标准互认”，谁先输出技术规范、认证体系与执法先例，谁就能在对方市场获得“监管通行证”。当

CPTPP 的源代码条款、DEPA 的监管沙盒、GDPR 的权利清单被不同组合地吸纳进各国国内法，数据跨境治理已不再是“是否流动”之争，而是“以谁的标准流动”之辩。条约文本背后，实质是数字产业竞争优势与制度性话语权的双重博弈。

1.1.2 中国关于数据跨境政策的规定

近年来，中国跨境数据流通监管政策日臻完善，以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》为基石，陆续出台《网络数据安全管理条例》《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》及《个人信息出境认证办法》等配套文件，逐步搭起一套系统而清晰的合规框架，既为企业“出海”数据提供了可操作的指引，也为后续制度迭代预留了接口。

纵观既有安排，监管思路已呈现出四条主线：一是“分级分类、多轨并行”，不同敏感度的数据对应差异化的出境路径；二是“自贸试验区先行先试”，用负面清单、备案制等创新工具降低合规门槛；三是条款颗粒度持续细化，评估流程、合同模板、认证规则一应俱全，拿来即用；四是标准与政策同步升级，把抽象的法条转译为可量化、可验证的技术指标。

面向未来，这套体系仍将沿着“安全可控、流动有序”的方向演进，并呈现出五个鲜明特质：政策持续微调、安全底线加厚、流通环节减负、国际规则对接、技术深度嵌入。

具体来看，监管部门会进一步把“出境”拆成更多场景，对每一类数据“量体裁衣”，让标准追着业务跑；同时，全流程数据安全管理制度将被硬性嵌入企业内控，确保数据出境后的每一跳都可追溯、可召回。便利度方面，负面清单、白名单、沙盒监管等工具会在更大范围复制推广，让企业“花更少时间填表，把更多时间做业务”。

在国际舞台，中国将积极参与跨境数据流动、数字贸易、隐私认证等议题的多边磋商，把本土实践转化为全球规则，争取更大的话语权。技术层面，区块链存证、AI 风险扫描、隐私计算等工具会与审批、评估、执法环节深度耦合，让“事后罚”转为“事前防”，既提升监管精度，也降低合规成本。

总体而言，中国的跨境数据流通监管正步入“安全红利”与“开放红利”

同步释放的新阶段。随着政策工具箱不断丰富、技术底座持续加固，中国有望在保障数据主权和个人隐私的前提下，为全球数字经济提供更高效、更可信的跨境通道，也为自身数字产业的高水平开放注入持久动能。

1.1.3 美国关于数据跨境政策的规定

美国的数据跨境监管哲学，可以用一句话概括：以国家安全为最高准绳，以技术霸权为支点，用“长臂”与“高墙”组合成一套进攻型数据治理范式。与欧盟“权利优先”的逻辑不同，华盛顿把数据视为战略资产，其政策主线始终围绕“数据必须为我所用，且不被对手所用”展开，由此形成内外有别的双层结构：对外筑墙、对内松绑，对外长臂、对内短链。

1.立法基调：安全例外高于市场效率

从 2018 年《云法案》到 2024 年《防止关注国家获取美国人敏感个人数据最终规则》，美国历次修法都在重复同一句话——“数据跨境不得损害国家安全”。这一理念被写入《出口管理条例》第 744.23 条、14117 号行政命令第 3 节以及《国际紧急经济权力法》备忘录，形成“安全例外”的宪法级地位：只要总统认定存在“非常规威胁”，即可跳过国会听证、WTO 审议或隐私影响评估，直接对特定国家、特定数据类别实施零流量封锁。换言之，在美国法语境里，国家安全不是“免责事由”，而是“启动条件”，数据自由流动反而成为需要额外论证的例外。

2.规则骨架：三把“剃刀”同时下落第一把剃刀是“控制者标准”

《云法案》率先确立“谁控制数据，谁就受美国法管辖”，把属地原则改为属人原则，全球云服务商被一体纳入；14117 号令进一步把“控制”细化为“密钥持有、模型训练、算法调试”任一环节，确保数据、算力、模型一个都跑不了。第二把剃刀是“敏感数据负面清单”。不同于欧盟的“充分性认定”白名单，美国直接列黑：genomic（基因）、biometric（生物特征）、geolocation（地理位置）、financial（金融）、government-related（政府相关）五大类数据，只要接收方位于“关注国家”，即推定禁止；量级门槛从万人级一路降到百人级，基因数据甚至单人即触发许可。

第三把剃刀是“技术穿透”。2024 年《最终规则》把“远程访问”视同出口，加密备份、联邦学习、隐私计算统统不算“安全港”，必须走 EAR 或

ITAR 逐项审批；同时要求企业保存境外接收方的服务器日志、运维人员国籍、密钥托管地址，供 BIS“穿透式审计”，实质上将境外数据中心纳入美国长臂监管。

监管工具：许可证 + 刑事威慑 + 金融制裁许可证体系采用“默认禁止 + 个案豁免”：所有涉及敏感数据的跨境传输必须先申请出口许可，审批周期 6—9 个月，且可附带“随时撤销”条款；未经许可即构成“视同出口”，最高可处交易金额两倍或 300 万美元罚款。司法部同步启动《经济间谍法》《计算机欺诈与滥用法》等刑事条款，个人最高 20 年监禁；财政部 OFAC 可追加 SDN 清单制裁，导致企业瞬间失去美元清算通道。三重威慑叠加，使“合规成本”直接转化为“生存成本”，迫使跨国公司在数据流向问题上自动“选边站”。

3.对内政策：数据自由流动 + 弱隐私管制

与对外“筑墙”形成鲜明对比，美国国内并无统一联邦隐私法，CCPA/CPRA 等州法采用 opt-out 机制，企业默认可以收集、出售、共享个人数据，除非用户主动点击“Do Not Sell”。联邦层面仅 FTC 第 5 条“欺骗性贸易行为”作为兜底，执法以事后和解为主，罕见高额罚款。由此形成“对内宽松、对外严苛”的剪刀差：本土巨头可以低成本汇聚全球数据，再通过“白名单 + 安全港”机制把清洗后的数据输往盟友国家，实现“数据虹吸—价值增值—规则输出”的闭环。

4.战略指向：把国内法做成国际法

美国并不追求像 GDPR 那样的全球“模板”，而是通过“规则捆绑 + 市场杠杆”输出标准：

贸易协定嵌入：USMCA、IPEF、美日数字贸易协定均写入“禁止数据本地化”“禁止源代码披露”条款，锁定伙伴国不得自设壁垒；

技术标准锁定：NIST 框架、FIPS 加密、FedRAMP 云认证成为进入美国云生态的“通行证”，倒逼各国企业按美方参数改造系统；

金融杠杆放大：美元清算、IPO 通道、风险投资把“合规差异”转化为“融资成本”，使美国规则在境外实现“市场自执行”。

其结果不是全球照搬美国文本，而是全球必须在美国划定的“安全走廊”内运行：数据可以流动，但不得流向对手；算法可以开源，但不得屏蔽美国后

门；云可以全球部署，但密钥必须让华盛顿可及。

1.1.4 欧盟关于数据跨境政策的规定

欧盟奉行在保障个人数据权利的前提下，有条件实施数据跨境流通的理念。因受自身文化影响，欧盟在数据跨境流通中秉承着优先保障个人数据权利的理念，将数据权利作为公民的基本权利，将个人数据安全保障置于数据流通中的优先地位，并在数据跨境流通中通过一系列法律条文予以落实。

例如，1981 年，欧盟通过《有关个人数据自动化处理的个人保护公约》中，明确提出保护欧洲公民隐私权，以保障欧洲公民基本人权。2000 年，《欧盟基本权利宪章》出台，前两章着重提出要充分尊重自由、民主、平等和人权，赋予个人具有保护个人数据的基本权利。2016 年，欧盟通过《通用数据保护条例》以赋予数据主体更正权、被遗忘权等新权利，同样为保护人权的目标。

为保证法律的权威性，欧盟采取了统一立法的模式，将个人数据纳入调整范围，陆续出台规则建立起以个人数据权利保护为基础的防守型数据监管模式。一方面，该系列行为举措促进了欧盟内部的数据自由流动。另一方面，为实现强化隐私保护的目的，欧盟严格限制本地数据向欧盟区域以外区域传输，以此保障数据安全可控。

面向境内，欧盟建立统一数据立法，以促进数据内部自由流通。面向欧盟境外，根据充分性认定原则构建一套白名单制度，欧盟对数据的接收国进行数据保护认定。认定只有数据保护水平与欧盟相当的国家才获准数据流入，对未能获取充分性认定的国家只能采取适当性保障措施和按例外情况接收数据。

截至 2025 年 6 月，已经有 15 个国家与地区获得欧盟充分性认定，包括安道尔、阿根廷、加拿大、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、大韩民国、瑞士、英国、美国和乌拉圭。

欧盟数据监管政策并非仅为构建内部市场或单纯保护欧盟公民数据权益，基于基本权利保护与构建内部市场的双重目标，是欧盟对外输出数据监管模式的政策动机。在欧盟以外的国家中，约有 67 个国家遵循了《通用数据保护条例》，《通用数据保护条例》俨然成为个人信息保护的全球范式。由此可见，欧盟在数据流动监管政策上采取的发展路径是从欧盟严格立法开始，向全世界推广其价值理念，输出己方标准，最终实现在数据全球数据监管中的欧盟标准

与话语权，完成国内法向国际法的转变。

1.1.5 日本关于数据跨境政策的规定

日本秉持“技术信任先于权利限制”的本土文化基因，在数据跨境与人工智能治理中走出一条“先流动、后治理”的柔性道路。与欧盟将个人数据权利上升为“基本人权”的防御型模式不同，日本把数据视为“基础战略资源”，把算法创新视为国家竞争力的核心引擎，因而将“保障产业先行、补足风险底线”作为立法基调，并通过三层递进机制把这一理念转化为可操作的制度安排。

第一层面，以“软法”确立信任框架。2025 年 5 月生效的《人工智能相关技术研究开发及应用推进法》虽是日本首部 AI 专门法，却通篇不设罚则，而是用“AI 战略本部—白皮书—指导建议”的链条，先为市场划出弹性空间。战略本部每年发布《AI 技术动向与风险清单》，把“高风险场景”动态化、公开化；企业据此开展自我评估，评估报告向主管省厅备案即可。备案信息不对外公开，但可作为政府采购、补贴评审的“加分项”，形成“政府让渡声誉、企业换取市场”的隐性激励。该法第 16 条保留“调查—指导—公开”的兜底工具：若出现严重侵权或偏见事件，政府可要求开发者提交算法逻辑、训练数据来源及风险缓解措施；拒不配合或整改不力者，战略本部可公开其名称，借助资本市场与舆论完成“二次惩戒”。

第二层面，以“同等保护”撬动数据跨境。2023 年修订的《个人信息保护法》第 28 条沿用“相当保护水平”原则，却未设置“事前审批”硬门槛，而是把判断权交给市场：企业只要择一采用白名单、约束性企业规则（BCR）或标准合同条款（SCC），即可出境。日本个人情报保护委员会（PPC）2024 年 4 月发布的《跨境转移实务指引》将“相当”标准细化为“功能等效”——不要求接收国法律文本与日本逐条对应，只要能达到“同等风险缓释效果”即可。这种“结果导向”的认定逻辑，大幅降低了日企出海合规成本。

第三层面，以“国际互认”输出日式标准。日本把多边舞台视为放大“软法”影响力的最佳场域。2023 年 G7 广岛峰会启动的“广岛 AI 进程”已迭代至 2.0 版，核心文件《国际行为准则》提出“红队测试公开、合成内容标注、跨境漏洞共享”十项原则，均无法律约束力，却与 OECD、ISO/IEC JTC 1/SC 42 实现技术对接，成为日企海外“自证合规”的通行证。2025 年 11 月，经产省

宣布将与东盟共享“广岛准则”日英双语工具包，并协助建立“东盟—日本 AI 安全沙盒”，通过“技术援助+规则嵌入”方式，把柔性治理经验转化为区域公共产品。与此同时，ISMAP 认证作为进入日本公共部门的“硬门槛”，也在反向输出：2025 年 10 月更新的 3.0 版标准新增“AI 模型供应链”条款，要求训练数据须在日境内完成最小必要清洗、模型权重须支持“可验证删除”。目前仅 AWS、Azure、GCP 三家美系云通过“AI 增强级”认证，中国厂商需借“可信日本法人”模式间接申请，客观上把日式安全要求传导至全球供应链。

对内，日本用“软法”留足创新空间；对外，用“互认”放大标准影响力。两条路径交汇，形成“先予后取”的政策逻辑：先以低门槛吸引全球数据与算法流入，再通过市场优势与联盟外交把“日式规则”升级为国际规则。对于计划进入日本市场的企业而言，把握“柔性合规”节奏是关键：数据跨境优先采用 PPC 2025 版 SCC 并同步搭建 BCR，AI 服务提前对照《AI 运营商指南 1.1》完成“偏差测试+数据溯源+透明披露”三件套，政府采购则尽早启动 ISMAP“AI 增强级”认证。能在“软法”框架下交出一份可信的“技术答卷”，便可在日本市场获得数据与算法的双重通行证，进而借助“广岛 AI 进程”把日式合规转化为全球竞争力。

1.1.6 国际形式对数据跨境流通带来的挑战

各国因利益诉求、政治环境及安全考量不同，正在频繁调整数据跨境规则，使全球监管图景呈现高度不确定性。欧盟以《通用数据保护条例》（GDPR）为“权利本位”核心，通过“充分性认定”、标准合同条款（SCCs）和具有约束力的公司规则（BCRs）对外输出隐私标准，将第三国数据保护水平与欧盟标准强制绑定，形成高门槛合规壁垒。美国则在《美墨加协定》（USMCA）、《美日数字贸易协定》等谈判中力推“禁止数据本地化”条款，主张数据自由流动，但同时通过《出口管理条例》（EAR）和《澄清境外数据合法使用法》（CLOUD Act）对关键技术与涉密数据实施严格出境管制，形成“外松内紧”的反差结构。美欧两大体系对“数据主权”与“安全例外”的认知差异，已导致 WTO 电子商务谈判在“非本地化”条款上陷入长期僵局，凸显多边层面协调之难。

规则碎片化直接推高了企业的合规成本。同一笔跨境业务往往需同时满足

欧盟 GDPR 的“高保护”要求、美国出口管制对技术数据的“许可先出境”限制，以及部分新兴经济体设定的本地化留存义务。例如，印度《数字个人数据保护法》强制“关键个人数据”只能境内存储；俄罗斯第 149-FZ 号联邦法要求公民数据必须在俄境内处理，并对未落实的跨国平台处以封锁或罚款。当不同司法辖区对同一类数据采取截然相反的出境立场时，企业不得不为同一数据集建立多条隔离流程，显著增加运营复杂度和费用。

在地缘政治层面，数据跨境问题被进一步“武器化”。2023 年 10 月，美国贸易代表在 WTO 正式撤回 2019 年关于禁止数据本地化的提案，为未来实施更严格的出境审查预留政策空间；欧美虽于 2023 年 7 月重建《欧盟-美国数据隐私框架》，但欧盟法院在“Schrems Ⅱ”案中的严格审查标准仍让美企面临被随时叫停的风险。缺乏稳定的多边争议解决机制，使得跨境数据传输随时可能因单边制裁、技术封锁或“长臂管辖”而中断，全球数据要素的优化配置受到明显阻碍。

综上，监管政策的多线演进、地缘政治的叠加冲突以及多边协调的迟滞，共同构成了数据跨境流动的高不确定性环境；企业唯有在“政策快照”基础上建立动态合规矩阵，才能降低突发规则变动带来的断链风险。

1.2 数据跨境的新挑战

在了解了各国家与地区现行的数据跨境监管政策后，本节将在此基础上，进一步介绍当前数据跨境领域中出现的新兴场景与技术，并分析这些新场景、新技术在数据跨境流通过程中可能带来的监管与实践层面的挑战。鉴于这些技术与场景尚处于发展初期，受篇幅与认知所限，我们难以在本白皮书中对所有挑战一一给出对应的解决方案。后续章节中，我们会对部分挑战尝试提出可行的解决思路，供读者参考，希望能为您带来启发；对于暂未涉及的场景，也期待您能结合实际情况，探索并提出契合自身的解决方案。

1.2.1 新场景，新变革

1.2.1.1 来数加工

来数加工场景是数据跨境流通中侧重于数据要素初级增值的基础性模式。其核心特征为原始数据从境外传输至境内，在严格隔离的环境中进行清洗、标

注、分析等增值处理后，以非原始数据的形式（如数据分析结果、模型参数等）出境。该模式的关键在于通过技术手段实现“数据不出境，价值可跨境”，在满足境外数据本地化监管要求的同时，发挥境内数据处理能力优势。在技术架构上，该场景通常依托于跨境数据专用通道、数据保税区等基础设施，并综合运用数据脱敏、特征提取、区块链存证等技术，确保数据处理过程的可控、可溯与安全。

在行业应用方面。例如，在智能驾驶技术研发中，境外采集的原始道路影像数据可加密传输至境内处理平台，在物理隔离的环境中进行车辆、行人、交通标志等关键目标的标注与轨迹分析，最终输出高度结构化的标注数据集或训练好的感知模型参数至境外，用于提升自动驾驶系统的环境识别能力。整个过程，原始数据不落地、不与境内数据交互，仅输出经深度加工后的衍生数据产品。在生物信息学领域，境外科研机构可将基因测序原始数据传入境内符合安全标准的计算环境，利用境内高性能计算资源进行变异位点识别、功能注释等分析，最终生成符合国际规范的、经匿名化处理的基因变异图谱或分析报告传输回境外，显著加速全球范围内的联合科研进程。这些实践表明，**来数加工模式有效平衡了数据跨境流动的合规风险与价值挖掘需求。**

1.2.1.2 模型出境场景

模型出境场景的核心是将在境内训练成熟的机器学习模型或人工智能算法，通过安全合规的方式输出至境外部署应用，实现技术能力而非原始数据的跨境流动。此场景不涉及原始数据的跨境传输，而是将数据价值凝结而成的模型作为最终产品，其技术重点在于模型的轻量化封装、知识产权保护以及对境外应用环境的适应性调优。模型压缩、知识蒸馏、数字水印以及同态加密等技术是该场景得以实现的关键保障，确保模型在出境后能高效、安全地运行。

该场景在多个行业已有广泛实践。以工业智能制造为例，一家在境内研发了高精度视觉质检算法的服务商，可以将训练完成的模型进行轻量化处理，并将其封装为标准化软件模块。该模块通过合规评估后，可部署于境外合作工厂的边缘计算设备上，直接对生产线上的产品进行实时质量检测与分拣。整个过程中，境外工厂的生产线数据无需传回境内，仅需定期将模型的性能反馈日志（不包含原始图片）加密传回，用于模型的迭代优化。又如，在跨境数字内容

服务领域，境内企业开发的多语言大模型或内容生成模型，可以以 API 服务的形式提供给境外用户。境外用户通过接口调用获得智能化的内容创作、翻译或摘要生成服务，而所有的用户交互数据均存储在境外的服务器上，仅有个别不涉及个人隐私的模型优化参数被允许在加密后传回境内，用于服务质量的整体提升。**模型出境模式极大地降低了因原始数据跨境可能引发的合规风险，是人工智能技术全球化应用的重要路径。**

1.2.1.3 模型融合场景

模型融合场景代表了数据跨境应用的高级形态，其本质是在不移动原始数据的前提下，通过隐私计算技术实现分布在不同司法管辖区的数据协同计算，共同训练出一个更加强大和通用的融合模型。该模式旨在破解数据孤岛难题，实现“数据可用不可见”，在充分保障数据主权和安全的前提下，释放跨境数据元素的融合价值。其技术实现高度依赖于联邦学习、安全多方计算、可信执行环境等前沿隐私计算技术，通过在各方数据本地进行特征提取和中间计算，仅交换加密后的中间结果（如梯度、参数），最终汇聚成一个优化的全局模型。

在具体应用中，跨境金融风控是典型领域。境内金融机构与境外合作伙伴可以共建一个联邦学习系统。境内方利用本地的用户信贷数据，境外方利用本地的商户交易数据，分别在本地训练模型组件，然后仅交换加密后的模型参数更新值，而非任何原始数据。通过多次迭代，最终形成一个能够更准确识别跨区域欺诈行为的联合风控模型，该模型的性能优于任何一方仅用本地数据训练的模型。在全球公共卫生与医药研发领域，多个国家的医疗研究机构可以在不共享各自临床病患原始数据的情况下，利用模型融合技术协同训练疾病预测模型或药物疗效分析模型。每个参与方在本地数据中心计算模型更新，仅向协调方发送加密的参数更新，从而在保护患者隐私和遵守各国数据法规的同时，加速对全球性疾病的科学研究进程。**模型融合场景是构建可信数据流通生态、推动全球数字协作的关键技术方向。**

1.2.1.4 智能网联汽车

在车路协同道路建设及云控平台构建方面，临港新片区做出了积极示范。该区域推动了长达 86 公里的车路协同道路建设，并同步构建云控平台。在此基础上，形成了丰富的常态示范应用场景，涵盖无人重卡、无人公交、无人出

租和无人作业等领域。同时，该地区智能网联汽车领域的一般数据清单也颇具规模，涉及 4 个数据跨境场景和 23 个数据类别，为智能网联汽车的发展提供了数据支撑和应用基础。

在全球研发测试领域，特定装备制造企业为了实现全球协同研发，采取了数据跨境共享的策略。这些企业将研发测试、设备运行日志等数据与海外分部及合作伙伴进行合规共享。通过这种方式，企业能够整合全球资源，加快产品迭代速度，提升自身在全球市场的竞争力。

1.2.1.5 跨境医疗合作

在跨境就医场景中，跨境医疗有了创新性的突破。以某港资医院为例，其在市数据跨境流动服务平台的辅导下，成功实现了港人来粤跨境就医。经授权后，在港医生可以直接访问内地居民或港人在内地的电子病历、CT 和 MRI 影像记录等数据。这一举措极大地减少了重复检查，既为患者节省了时间和费用，也提高了医疗资源的利用效率。

在远程会诊、国际多中心临床试验等场景方面，北京积极推动生物医药领域的数据流通。为了让医疗机构、跨国药企、研究机构等主体之间的数据流动更加顺畅，北京畅通了“数据出境合规+行业业务合规”的双协同便利化路径。这有助于整合各方资源，加速生物医药领域的研究和创新，推动跨境医疗在更广泛的领域取得进展。

1.2.1.6 跨境金融服务

在银行资信业务方面，实现了“跨境通办”的创新突破。珠海搭建了粤澳跨境数据验证平台，该平台为金融机构构建了数字互信通道。凭借这一通道，银行资信业务能够顺利实现跨境通办。而且，这种模式的应用范围并不局限于金融领域，还拓展到了产权交易、民生服务等更多场景，为跨境业务的开展提供了更广泛的便利。

在跨境征信领域，深港两地开展了积极合作。当地的征信机构和银行机构携手，实现了跨境查阅征信数据。这一合作成果具有重要意义，银行在进行信贷评估时，可以更全面、准确地获取相关信息，从而有效提升信贷评估效率，降低信贷风险。

1.2.1.7 跨境电商

在跨境电商场景方面，佛山取得了重要突破，成为全国首个获批开展跨境电商资金收付业务的地级市。与此同时，惠州和肇庆也积极推动跨境电商的发展，分别建成了跨境电商公共服务平台，并成功引进龙头企业，这些举措有力地促进了当地跨境电商进出口业务的增长。

在智能调度系统与大数据应用领域，亦有不少成功案例。例如，美国的C.H.Robinson 公司借助生成式 AI 处理业务邮件，能够自动识别海关新规条款的变更，大大提高了业务处理的效率和准确性；国内的京东零售供应链则运用智能诊断系统，精准定位仓储瓶颈，并提前将库存下沉至海外仓，优化了供应链管理。

1.2.1.8 国际学术合作

以某香港高校为例，其河套分院在河套深圳园区开展药理学试验。在试验过程中，通过人工智能训练、验证、测试等环节产生了大量学术合作数据。由于双方构建的数据共享机制，这些数据能够无障碍地传输至香港高校本部。

得益于此，两地实验室可以同步开展学术研究，不仅提高了研究效率，还能集合双方的优势资源，实现科研成果的共享，推动学术研究取得更丰硕的成果。

1.2.1.9 跨国生产制造

跨国制造企业在生产制造过程中，非常重视数据的流通与整合。它们会传输生产管理、零部件及物料采购、库存管理、质量管理和物流供应链等多方面的数据，目的是实现全球生产制造数据的汇集。通过这种方式，企业能够对生产过程进行全面、精准的把控，从而更好地服务生产管理，优化生产流程。

以某大型跨国制造业企业为例，其分支机构与国内的制造工厂以及企业总部之间，开展了生产管理的数据协同。在这个过程中，各方能够实时共享生产相关数据，及时调整生产策略。比如，当总部获取到市场需求变化的数据后，可以迅速将信息传递给分支机构和国内制造工厂，调整生产计划；国内制造工厂在生产过程中遇到质量问题或库存短缺等情况，也能及时反馈给总部和分支机构，共同协商解决方案。这种顺畅的跨国场景协作，带来了显著的效益，不仅提升了生产效率和产品质量，还降低了生产成本。

1.2.1.10 全球售后服务

在装备制造业领域，企业在提供售后服务时积极推动售后服务数据的跨境流动。这些数据涵盖了产品运行日志、故障分析、售后服务报表等多个方面。通过跨境流动这些数据，企业能够更全面地了解产品在不同地区的使用状况，及时发现潜在问题并采取相应措施，进而有效提高产品服务的质量。

以某大型无人叉车制造企业为例，该企业为美国、日本等地客户的制造工厂提供无人叉车。在售后服务过程中，企业通过合规的方式进行产品运行日志、故障分析等数据的传输与共享。基于这些数据，企业可以精准地对无人叉车进行检查和维保作业。比如，根据产品运行日志，企业能了解叉车的使用频率、工作时长等信息，提前安排维护计划；通过故障分析数据，能快速定位问题根源，及时派遣技术人员进行维修，减少设备停机时间，保障客户工厂的正常生产。这充分体现了售后服务数据跨境流动在提升产品服务质量方面的重要作用。

场景类型	核心特征	核心挑战	对应解决方案章节参考
来数加工	**侧重于数据要素初级增值的基础性模式。**其核心特征为原始数据从境外传输至境内，在严格隔离的环境中进行清洗、标注、分析等增值处理后，以非原始数据的形式（如数据分析结果、模型参数等）出境。**来数加工模式在需要大规模数据标注与处理的领域作用显著。**	加工过程隔离防护、衍生数据合规边界界定、跨境传输效率平衡。	2.2.4 隐私计算、2.4.5 跨境电商案例
模型出境	将在境内训练成熟的机器学习模型或人工智能算法，通过安全合规的方式输出至境外部署应用，实现技术能力而非原始数据的跨境流动。**模型出境模式极大地降低了因原始数据跨境可能引发的合规风险，是人工智能技术全球化应用的重要路径。**	模型知识产权保护、境外部署环境适配、模型迭代数据回传合规。	2.1.1.3 互联互通层、2.4.3 汽车行业案例
模型融合	代表了数据跨境应用的高级形态，其本质是在不移动原始数据的前提下，通过隐私计算技术实现分布在不同司法管辖区的数据协同计算，共同训练出一个更加强大和通用的融合模型。	多司法管辖区技术互认、计算结果准确性保障、合规审计追溯。	2.2.4 隐私计算、2.4.4 医疗行业案例
智能网联汽车	车路协同数据、研发测试数据跨境共享，涉及多数据类别与场景。	地理信息安全保护、实时数据传输延迟、多主体数据权责划分。	2.4.3 汽车行业案例、4.2.1.1 政策优化
跨境医疗合作	电子病历、影像数据跨境共享，涉及敏感个人信息。	患者隐私保护、医疗数据标准化、跨境诊疗合规衔接。	2.4.4 医疗行业案例、2.1.1.2 治理合规层

跨境金融服务	征信数据、交易数据跨境验证，需实时性与安全性平衡。	金融数据主权保护、反洗钱合规、跨境风控模型协同。	2.4.2 金融行业案例、3.3 稳定币实践
跨境电商	订单、物流、支付数据高频跨境流动，数据量庞大。	多币种结算适配、跨境数据合规筛查、供应链数据协同效率。	2.4.5 跨境电商案例、3.4 结算协同
国际学术合作	科研数据跨境共享，涉及联合研究与成果转化。	科研数据权属界定、知识产权保护、多机构合规协同	2.4.1 大湾区案例、4.3 国际合作政策
跨国生产制造	生产管理、供应链数据全球汇聚，支撑协同生产。	工业数据安全防护、跨境数据同步效率、多工厂合规标准统一。	2.4.3 汽车行业案例、2.1.1.4 业务应用层
全球售后服务	产品运行日志、故障数据跨境传输，支撑远程维保。	设备数据隐私保护、跨境传输稳定性、故障数据合规使用。	2.4.3 汽车行业案例、2.2.5 传输加密体系

1.2.2 新技术，新挑战

1.2.2.1 智能合规治理

智能合规治理是保障跨境数据安全、合法流动的重要手段。它借助人工智能、大数据、规则引擎等先进技术，贯穿跨境数据流动的全过程，实现了从数据出境前的评估，到传输过程中的监测，再到事后审计追溯的全链条管理。

1.全流程合规审查与风险预警

出境前自动化评估：在数据准备出境时，智能合规治理系统运用预设的规则和算法，对数据进行全面扫描和分析。例如，判断数据是否包含敏感信息、是否符合目标国家或地区的法规要求等，提前识别潜在的合规风险，为数据出境提供安全保障。

传输中动态监测：在数据传输过程中，系统实时跟踪数据的流向和状态，监测是否存在异常的数据访问或传输行为。一旦发现异常，立即发出风险预警，以便及时采取措施，防止数据泄露或违规使用。

事后审计追溯：数据传输完成后，系统会对整个过程进行审计，记录所有相关操作和事件。这不仅有助于在出现问题时进行追溯和调查，还可以为企业提供合规性证明，应对监管检查。

2.跨境贸易合规平台的应用实例

跨境贸易合规平台是智能合规治理的典型应用。它集成了海关、税务、物流等多源数据，利用 AI 算法对数据进行深度挖掘和分析。一方面，自动识别数据中的敏感信息，如个人身份信息、商业机密等；另一方面，结合各国法规进行合规性评估，判断数据是否符合不同国家和地区的贸易政策、数据保护法规等要求。最后，平台会生成详细的合规报告，为企业提供清晰的合规指引。

3.跨境电商的显著成效

以某跨境电商为例，接入智能合规系统后，取得了显著的成效。在支付结算方面，时间从原来的 T+3 缩短至实时到账，大大提高了资金流转效率，增强了企业的资金流动性。同时，在合规风险识别方面，准确率达到了 98%，有效降低了企业面临的合规风险，避免了因违规行为可能带来的巨额罚款和声誉损失。这充分证明了智能合规治理在跨境数据流动中的重要价值和实际效果。

1.2.2.2 跨域可信交付

1.跨域可信交付的技术基础

跨域可信交付是保障数据在不同国家或地区之间安全、有效传输的重要方式，它依赖于一系列先进技术。区块链具有去中心化、不可篡改的特性，就像一个公正无私的“账本”，记录着数据传输过程中的每一个环节；隐私计算能在不泄露原始数据的前提下进行计算分析，好比给数据加上了一层“保护罩”；数字签名如同数据的“专属印章”，确保数据的发送方身份真实可靠；时间戳则为数据的传输时间提供精确记录，如同给数据的流动加上了“时间刻度”。

2.跨域可信交付达成的目标

这些技术共同作用，使得数据在传输过程中能够保证完整性，即数据在传输前后不被篡改，就像一件珍贵的艺术品在运输过程中不能有任何损坏；保证真实性，确保数据来源真实可靠，如同要确认一幅名画是出自哪位真正的画家之手；实现可控性，能够对数据的访问和使用进行精准管理，好比给数据的使用加上了一把“智能锁”；具备可追溯性，能随时查询数据的传输路径和使用情况，就像可以追踪一件商品的物流信息一样。最终实现“数据可用不可见”，让数据在发挥作用的同时，其核心内容得到严格保护。

3.医疗数据跨境共享应用实例

在医疗数据跨境共享领域，跨域可信交付有着典型的应用。例如某医疗体系搭建了个人授权病历跨境分享平台。在这个平台上，患者的病历数据采用加密上传的方式，就像把病历装进了一个“加密保险箱”再进行传输，防止数据在传输途中被窃取。在展示病历时采用脱敏展示，只呈现必要的、不涉及患者隐私的信息，如同给患者的隐私信息“打了码”。同时设置了授权机制，只有经过患者明确授权的医疗机构才能访问相关病历数据，就像只有拿到特定钥匙的人才能打开“保险箱”。通过这些措施，在充分保障患者隐私的基础上，实现了 A 市与 B 市医疗机构间病历数据的可信流通，让医生能够获取更全面的患者信息，为患者提供更精准的治疗方案。

1.2.2.3 算网协同保障

1.算网协同技术基础

算网协同保障是数据跨境过程中的关键安全架构。在全球化数据交互日益

频繁的当下，数据跨境面临着数据主权和合规性等诸多挑战。算网协同保障依托分布式计算资源、边缘节点、隐私计算框架与网络调度机制，构建起一套安全且高效的数据处理与传输体系。通过上述技术的协同作用，算网协同保障实现了数据本地处理、跨境结果传输、任务协同计算的安全架构。数据在本地进行处理，既满足了数据主权的要求，确保数据不出境，又减少了跨境数据传输带来的风险。跨境结果传输则是将处理后的结果进行安全传输，满足不同地区之间的数据交互需求。任务协同计算使得各个节点能够协同完成复杂的计算任务，提高整体计算能力。这种架构能够有效满足数据主权与合规要求，为数据跨境提供了可靠的保障。

2.智慧交通跨境协同应用案例

在智慧交通跨境协同应用中，算网协同保障发挥了重要作用。以深圳港“海铁联运智能闸口”系统为例，通过部署边缘计算节点与隐私计算引擎，实现了港口、铁路、物流商之间的跨境运输数据协同分析。

边缘计算节点：在港口和铁路站点等数据源头附近部署边缘计算节点，对运输数据进行实时采集和初步处理。例如，对集装箱的进出信息、货物状态等数据进行本地分析，只将关键的汇总信息传输到其他节点，减少了数据传输量和延迟。

隐私计算引擎：确保运输数据的隐私安全。不同参与方（港口、铁路、物流商）可以在不共享原始数据的情况下，通过隐私计算引擎进行联合分析。例如，在分析货物运输效率时，各方可以在保护自身数据隐私的前提下，共同计算运输时间、货物周转率等指标。

通过这种方式，实现了跨境运输数据的协同分析，提升了通关效率与物流透明度。海关可以更快速准确地获取货物信息，加快通关流程；物流商可以实时掌握货物运输状态，优化运输路线和调度安排。

1.2.2.4 隐私计算技术

在数据跨境服务场景下，为保障数据隐私安全并提升服务质量，采用了一系列前沿技术手段。

首先，运用隐私计算、同态加密等前沿技术，确保数据在跨境过程中不被泄露，实现数据服务的可运营、可管理与可评估。这使得数据服务能够有序开

展，便于管控服务流程并衡量服务效果。

其次，引入区块链技术，完整记录各方的数据交互流程与计算操作，达成可信多方隐私计算。此举极大地提升了数据跨境服务的可信度、安全性和可追溯性，让数据跨境服务更加可靠、透明。

1.2.2.5 智能路由技术

在跨境数据传输中，为保障业务连续性，提升传输稳定性与效率，可借助实时链路质量监测和动态路径切换等手段。实时链路质量监测就像一位敏锐的“侦察兵”，持续关注各条传输路径的状态，包括带宽、延迟、丢包率等关键指标。而动态路径切换则如同一位灵活的“调度员”，依据监测结果，在发现高风险传输路径（如拥堵、存在安全隐患）时，及时自动选择最优传输路径，避开拥堵或高风险节点。

电商平台应用案例：某电商平台采用了部署分布式节点的方式来优化跨境数据传输。通过这种方式，该电商平台成功将跨境数据传输延迟降低了 40%。这意味着用户在浏览商品、下单支付等操作时，等待时间大幅缩短，购物体验得到显著提升，同时也有助于电商平台提高业务处理效率，增强竞争力。

跨境支付系统应用案例：在跨境支付系统领域，某金融科技公司部署了智能路由系统。该系统具备实时监测链路状态的能力，当监测到“中国→日本”链路拥堵时，能迅速自动切换至“中国→新加坡→美国”路径。这一操作带来了显著的效果，传输延迟降低了 20-30ms，支付成功率提升至 99.5%。对于跨境支付业务而言，延迟的降低使得资金能够更快到账，支付成功率的提高则减少了交易失败的情况，保障了用户和商家的利益，促进了跨境贸易的顺利开展。

1.2.2.6 统一管控技术

企业在跨境数据管理中，面临多系统分散管理的难题，构建统一管控体系成为解决之道。该体系整合了数据分类分级、加密传输、合规审查权限管理、审计日志等多项功能。数据分类分级如同给数据贴上不同的“标签”，根据数据的敏感程度和重要性进行区分；加密传输就像给数据穿上“铠甲”，保护其在传输过程中不被窃取或篡改；合规审查权限管理则是把控数据访问和使用的“关卡”，确保只有符合规定的人员和操作才能进行；审计日志则记录下所有的数据操作，如同“黑匣子”，便于后续的审查和追溯。

通过这种整合，企业解决了多系统分散管理导致的效率低下问题，实现了自动化合规检查和跨境数据流动的一站式集中管理。这就好比将原本分散在各地的“小作坊”整合为一个高效的“大工厂”，让数据管理更加有序、高效。

跨国制造企业的应用实例：某跨国制造企业在亚太区部署了统一数据出境平台，这是统一管控体系的一个典型应用。该平台对采购、库存、售后等数据进行分级分类，根据不同的级别自动触发相应的合规审查与加密策略。例如，对于高度敏感的采购数据，会采取更严格的加密措施和合规审查流程。

在实际操作中，该企业实现了数据出境“一键申请、自动评估、全程留痕”。员工只需通过平台一键提交数据出境申请，系统会自动进行评估，判断是否符合合规要求。同时，整个过程的所有操作都会被记录下来，便于后续的审计和监管。这大大提高了数据出境的效率，降低了因多系统分散管理带来的合规风险。

1.2.2.7 数据智能诊断技术

数据智能诊断通过整合 AI 模型与大数据可视化两项关键技术，致力于对跨境数据开展全面且深入的分析。AI 模型如同一个“智能大脑”，具备强大的学习和分析能力，能够从海量的数据中挖掘出有价值的信息和规律。大数据可视化则将这些复杂的数据以直观的图表、图形等形式展现出来，就像为数据穿上了一件“易读外衣”，让人们更轻松地理解数据背后的含义。

借助这两种技术，数据智能诊断实现了对跨境数据链路、访问行为和传输异常的实时诊断与预测。在跨境数据链路方面，它能够监测链路是否畅通，是否存在带宽不足等问题；针对访问行为，可分析是否存在异常的访问模式，如频繁的恶意扫描等；对于传输异常，能及时发现丢包、延迟等情况。这一功能有助于快速定位故障根源，就像给数据系统配备了一个精准的“故障探测器”。同时，还能对系统性能进行优化，通过分析数据找出性能瓶颈并加以改进，以及提前发出风险预警，避免潜在问题演变成严重事故。

京东智能诊断系统的应用实例：京东零售供应链的智能诊断系统是数据智能诊断的一个成功应用典范。该系统运用蒙特卡洛树搜索算法，这是一种高效的搜索算法，如同一个“超级侦探”，能够从 200 多个维度对仓储情况进行全面排查。在众多的数据维度中，它可以精准地定位仓储瓶颈，比如发现某个仓

库的特定区域货物积压严重，或者某种商品的补货流程存在延误。

基于这些诊断结果，系统能够提前将爆款商品库存下沉至海外仓。通过这种方式，大大提高了订单满足率，让消费者能够更快地收到心仪的商品，提升了客户体验，同时也增强了京东在跨境零售市场的竞争力。

1.2.2.8 生成式 AI 技术

生成式 AI 在跨境数据治理领域具有广泛且重要的应用价值，能够显著提升治理的自动化与智能化水平，例如自动识别法规变更、生成合规报告、翻译与摘要跨境文档、模拟数据脱敏样本等。

美国 C.H.Robinson 公司的成功实践：美国 C.H.Robinson 公司在实际运营中充分利用了生成式 AI 的优势。该公司每天需要处理超过 1 万封业务邮件，其中包含大量与海关申报、运输安排等相关的重要信息。借助生成式 AI，它能够高效处理这些邮件，犹如拥有一支强大的“邮件处理军团”。

更重要的是，生成式 AI 助力该公司自动识别墨西哥海关新规中关于锂电池运输的条款变更。在货物启运前，系统就能迅速完成申报文件的适配工作，确保货物申报符合最新法规要求。这一举措避免了平均每票 2.3 天的清关滞留，大大提高了物流运输效率，降低了企业的运营成本，也增强了企业在跨境物流市场的竞争力。

1.3 面向“全球数据协作”的跨境流通新范式

在前一节，我们梳理了新兴场景与技术给数据跨境合规带来的多重变量，其中，生成式 AI、大模型训练与推理无疑是最具“破壁”潜力的一条鲶鱼：它同时放大了数据体量、流速和敏感度，也让传统“先分类、再出境”的合规节奏显得捉襟见肘。本节即以 AI 为切入口，畅想 AI 可能带来的变化。

1.3.1 AI 三要素，数据成为决定性要素

过去十年，算力与算法效率的叠加推进了人工智能的跃迁。特别是以中国企业深度求索旗下 Deepseek 为代表的“算法效率”的进步带来的收益，甚至超过“纯硬件”效率的改进；据统计，2024-2025 年间 AI 模型的 token（输入/输出基本单位）成本急剧下降 75%，这一趋势由开源模型（如 DeepSeek）和硬件创新驱动，例如 NVIDIA Blackwell 芯片在 AI 任务上速度提升 30 倍，

显著降低了训练和推理的单位成本。

伴随推理及调用成本的持续下降与硬件生态的多元化，更多瓶颈正在从“把模型做大”转向“把数据做对”：可合法获取、可追溯、可验证质量、覆盖多语多域且长期可更新的 AI 训练数据集，已成为影响模型可持续迭代的关键变量。

未来一段时间，算力价格与算法效率仍会改善，但约束 AI 发展的第一性变量将转向数据要素：从“有无”到“真假”、从“可用”到“可证”。这直接牵引数据跨境流通的路径与规则设计。

1.3.2 新场景：AI+加密资产，激活“全民数据协作”的全球市场

我们预测，以稳定币等加密资产为支付底座的全球数据协作市场将加速形成并发展。稳定币等加密资产具有即时、低额、跨境的特点，与模型对齐、合成数据校准、长尾场景采集等数据领域需求相互促进，形成正反馈循环。随着稳定币在全球跨境支付中的规模和渗透率快速增长，其为全球数据协作提供了有力的支付支撑。

1.稳定币在跨境支付中的合规基础

在合规层面，香港稳定币条例于 2025 年 8 月 1 日生效，这为小额高频跨境支付提供了合规底座。合规的稳定币制度构建了“低费率、近实时、可赎回”的结算层，对于按任务计酬的微型数据劳动，如数据采集和标注等工作，提供了稳定且透明的资金出入口，保障了数据工作者的权益，也促进了数据市场的健康发展。

2.数据领域新场景的出现

(1) 数据任务即资产

个人可以基于任务合约贡献链上可验证的数据，并获得稳定币等加密资产结算。这意味着数据贡献者的劳动成果能够以资产的形式得到体现和回报，激励更多人参与到数据贡献中来，丰富数据的来源和多样性。例如，一位数据爱好者可以通过完成特定的数据采集任务，获得相应的稳定币报酬，这些数据将被用于各类数据应用场景。

(2) 社区化数据工坊

围绕垂直场景，如医疗影像质检、工业缺陷图像、方言语音等，形成兴趣

社区。在这些社区中，参与者根据“质量、数量、信誉”等指标分配收入。这种模式促进了专业数据社区的形成，提高了数据的质量和专业性。例如，医疗影像质检社区中的专业人员可以共同对医疗影像数据进行审核和标注，根据各自的贡献获得相应的收益。

3.实际案例：OORT 公司的创新实践

据经济日报新闻，2025 年 3 月去中心化 AI 技术公司 OORT 以全球外包模式向深圳某人工智能企业提供高质量标准化工业数据集。OORT 采用了创新的 AI 数据采集和标注方式，允许全球贡献者收集、分类和预处理 AI 应用程序的数据，并获得加密资产报酬。通过利用区块链技术，OORT 解决了传统数据采集方式中数据来源单一和采集标注效率低下的问题，提高了数据的安全性，确保了数据透明性和用户隐私保护。这一案例推动了全球范围内的数据流通协作，以更高效和更低成本的方式助力构建公平、多样、安全、透明及可信的 AI 生态系统，为稳定币驱动下的全球数据协作市场提供了成功的实践范例。

1.3.3 直面 AI 变量：市场验证与可信数据双轨并行

1.3.3.1 市场与制度（合规）的双重验证

未来一段时期，任何新技术、新模式、新方案的扩散都必须先闯过两道关：第一道是市场需求关——看其是否真正解决痛点、能否跑通可持续的商业模式；第二道是制度合规关——看其是否在数据确权、隐私保护、跨境流通、支付结算等红线上“持证驾驶”。闯关路径有一条：把规则清单化、把流程做成可审计的“底账”，在国家和地方/园区政策给出的可预期边界内快速迭代、规模落地。市场验证为合规标尺提供鲜活案例，合规边界又为市场创新划出安全跑道，两者双向反馈、螺旋升级，新方案才能既活得下去、也活得长久。

1.3.3.2 质量与可信的技术要求

以区块链与可验证算法为底座，搭建数据要素“标准—采集—质检—验收—追溯”闭环治理框架，把质量控制拆成三道可执行、可度量的工程化动作：

质量达标：用任务化规范一次性锁定样本规模、字段精度、标注一致率等验收指标；流水线内置去重、污染检测、偏倚评估脚本，每一步跑出量化分值，不达阈值自动回炉，确保成品数据符合行业或场景基线。

可信留痕：采集、清洗、标注、移交等关键节点实时生成哈希摘要并写入链上，叠加时间戳与多方数字签名，形成不可篡改的“区块-批次”对应关系；任何后期改动都会触发哈希失效，从而第一时间暴露篡改行为。

全程可追、责任可界：链上记录与链外元数据共同组装成完整数据谱系：谁采集、谁标注、谁授权、谁传输、谁使用，一键生成可视化血缘图；监管部门或交易对手可在权限内溯源自证，实现“数据可信、来源可证、过程可审、结果可追责”，为后续定价、结算、合规抽查提供即取即用的技术凭据。

第二章 跨境数据流通基础设施构建与技术实践

数据跨境流动已成为全球数字经济发展的关键支撑。本章系统梳理跨境数据流通基础设施的架构设计、技术实现与实践经验，为后续章节的技术对比、场景推演和合规研判提供共同语境。

2.1 总体架构与技术体系

2.1.1 四层总体架构

跨境数据流通基础设施采用四层纵向架构，自下而上依次为基础安全层、治理合规层、互联互通层、业务应用层。四层架构遵循安全为基、合规为纲、互联为桥、应用为本的设计原则，通过标准化接口实现层间协同。

2.1.1.1 基础安全层

基础安全层作为数据跨境安全保障体系的基石，发挥着至关重要的作用。它凭借密码学、隐私计算、可信执行环境等一系列先进的底层安全能力，构建起一道坚固的数据安全防线，并且这道防线全面覆盖了数据跨境前、跨境中、跨境后这一完整的全流程，为数据的安全跨境保驾护航，确保数据在整个生命周期内都能得到妥善的保护。

1.核心技术

基础安全层核心技术包括：

- 数据脱敏包括静态脱敏和动态脱敏，静态脱敏是出境前的字段级处理，动态脱敏是访问时的实时遮蔽；
- 传输加密涵盖 TLS 1.3 端到端加密、国密 SM2/SM4 算法、IPsec VPN 专线；
- 隐私计算包含安全多方计算、联邦学习、同态加密、可信执行环境；
- 访问控制采用基于角色的权限管理、属性访问控制、零信任架构；
- 区块链存证实现数据操作日志上链、智能合约自动执行、分布式审计账本。

2.典型案例

案例专栏一：粤港澳大湾区的“跨境理财通”业务监管
粤港澳大湾区的“跨境理财通”业务监管就充分体现了基础安全与可信技术的价值。该业务需要内地和港澳多家银行共享个人投资数据用于监管统计。为保护客户隐私，华控清交构建了基于隐私计算的跨境数据匹配平台：内地银行和港澳银行分别在本地保存客户和投资数据，通过安全多方计算平台对加密后的关键信息进行匹配计算，原始敏感数据全程不出本地。最终平台将各银行的投资总额统计结果提供给监管部门，生成监管报告，同时确保个人敏感信息零泄露。该方案满足了法规对个人金融信息出境的严格要求（依据《促进和规范数据跨境流动规定》相关条款，详见 4.2.1.1），增强了客户对跨境金融服务的信任。在业务效果上，不仅提高了跨境数据统计的效率和准确性，也降低了各银行人工汇总数据的工作量，实现了“数据可用不见、监管高效透明”的目标。此案例已被纳入人民银行跨境金融创新试点，表明基础安全与可信技术在跨境金融应用中达到了实用可行的成熟度。
案例专栏二：跨国企业 HRMS 本地化与“最小必要”出境改造
某跨国企业在华运营需要与全球人力系统对接，涉及员工与应聘者个人信息的跨境流动。在近年来的申报实践中，监管对员工与应聘者信息采取差异化态度：对员工个人信息相对包容，但对应聘者及部分敏感个人信息更为严格。这迫使企业将 HRMS 进行本地化改造：明确允许出境的数据项并设置传输规则与日志留存；对禁止出境字段调整采集与录入流程；将应聘者模块剥离，采用境内替代方案以降低跨境必要性。实施后，企业实现了出境边界清晰化与可审计化，跨境体量与敏感暴露面显著收缩，符合“最小必要”与分场景差异化监管的趋势。 技术亮点与启示：以“制度—流程—系统”三联动将清单化、白/黑名单与日志审计固化到 HRMS 工程；在前置环节做“必要性/最小化”与“角色/场景”拆分，可显著降低评估难度与整改成本，特别适用于人力、财务共享等总部型系统的出境治理。
案例专栏三：跨境电商平台通过数据出境安全评估
某大型 B2B 跨境电商平台（中国制造网）覆盖交易、营销、支付与物流

多环节，业务跨域广、数据类型多。平台在北京相关机构指导下完成数据资产盘点、出境路径识别、制度与平台化改造，并通过国家网信办组织的数据出境安全评估，建立起“跨境前评估—跨境中执行—跨境后审计”的长期机制。工程推进中，同步完善标准合同与个保评估资料与备案，形成“评估+备案”的组合拳。

技术亮点与启示：电商典型的高并发与多接口特征，要求在 API 侧叠加频次与敏感访问监测、在数据侧叠加静/动态脱敏与最小化字段集设计，并以集中平台实现跨境资产可视与策略下发，能显著提升评估过程的可解释性与可验证性。

2.1.1.2 治理合规层

治理合规层将法律要求转化为可执行规则，实现数据出境全生命周期管理。

1.核心机制

治理合规层的核心机制包括：

- **三识别**：涵盖数据资产识别、跨境路径识别、合规风险识别。数据资产识别涉及盘点清单与字段级分类，跨境路径识别聚焦流向追踪，合规风险识别涉及开展影响评估；
- **三配套**：包含合规策略配套、数字合约配套、证据链配套，合规策略配套遵循最小化原则与脱敏规则，数字合约配套明确权限定义并实现自动执行，证据链配套包含用户同意、审批文档、审计日志等可供审计的踪迹；
- **三闭环**：包括事前闭环、事中闭环、事后闭环，事前闭环涉及评估、审批、备案，事中闭环开展传输、访问、处理监控，事后闭环涵盖审计、应急、改进。

2.典型案例

案例专栏四：“COLOR IV 国际多中心临床研究”项目
“COLOR IV 国际多中心临床研究”项目是国内数据跨境合规治理的典型实践。该项目由北京友谊医院牵头，与荷兰阿姆斯特丹医学中心等多个中欧医疗机构合作开展临床研究，需要大量患者敏感数据在中欧之间共享。作为《数据出境安全评估办法》实施后的首个申报项目，友谊医院搭建了医疗数据跨境研究平台及配套的数据合规管理平台。在项目实施中，医院严格按照法规要求进行了个人信息出境的安全评估申报，评估内容涵盖数据出境的合法性（如是否为法律未禁止出境的数据、是否取得个人单独同意、境外接收方是否达到同等数据保护水平等）、正当性和必要性，以及双方安全保障能力和合同义务等。技术上，平台采取了 VPN 加密通讯连接境内外节点，设置仅授权 IP 可访问，并在系统中实现了数据下载传输控制、存储加密、动态脱敏、用户权限管理、操作留痕审计、数据备份等一系列安全措施。通过事前－事中－事后三个环节的合规监控：事前评估跨境数据最小必要原则和合法授权；事中实时监测传输过程并违规报警；事后对全流程留证审计，确保了研究数据跨境共享的每个步骤都有据可查。最终，该项目成功获得国家网信办的安全评估批准，顺利开展了数据出境合作。这一案例表明，借助完善的治理与合规体系，敏感医疗数据也能在合法合规的框架下实现跨境流动，为生命科学领域的国际合作提供了范例。
案例专栏五：某大型跨国制造企业的数据跨境合规实践
该企业是一家全球领先的跨国制造企业，业务遍及全球多个国家和地区，涉及大量研发数据、生产数据、客户数据和员工个人信息在全球范围内的流转。 **1.技术应用场景** （1）构建全球数据资产目录：利用数据发现与分类工具，对全球范围内的 IT 系统和数据库进行扫描，自动识别并分类分级敏感数据（如个人身份信息、商业秘密、核心技术数据），形成统一的数据资产目录。 （2）实施数据流转路径可视化：通过部署数据流转监控系统，实时追踪数据在不同国家、部门和系统间的传输路径，识别潜在的跨境数据流动风险点。

(3) 自动化合规风险评估：开发内部合规风险评估平台，集成各国数据保护法规知识库，对每次数据跨境传输请求进行自动化风险评估，包括合法性、必要性、最小化原则等，并生成风险报告。

(4) 强化数据安全技术：对所有跨境传输的敏感数据强制实施端到端加密和动态脱敏处理。同时，建立严格的访问控制策略，确保只有授权人员才能在特定场景下访问脱敏后的数据。

(5) 建立数据主体权利响应机制：设立统一的全球数据隐私门户，方便数据主体行使其访问、更正、删除等权利，并确保响应流程符合 GDPR 等法规要求。

2.实施效果

一是显著降低了因数据跨境流动不合规而导致的法律风险和罚款，确保了企业在全球范围内的业务连续性。二是提升了数据安全防护能力，有效防范了数据泄露事件的发生。三是优化了数据跨境审批流程，将审批时间从数周缩短至数天，提高了业务效率。四是增强了客户和合作伙伴对企业数据保护能力的信任。

3.核心技术亮点

(1) AI 驱动的数据发现与分类：利用机器学习算法自动识别和分类海量非结构化数据中的敏感信息。

(2) 联邦学习与隐私计算：在某些场景下，探索使用联邦学习等隐私计算技术，在不传输原始数据的情况下进行协同分析，进一步降低数据跨境风险。

(3) 区块链技术：利用区块链的不可篡改性，记录数据流转和访问日志，为数据审计提供可信证据。

4.经验启示

一是数据跨境合规是一个持续演进的过程，需要企业建立动态的合规管理体系，并定期更新技术和策略以适应法规变化。二是技术工具的引入是提升合规效率和准确性的关键，但仍需结合完善的组织管理制度和人员培训。三是将合规要求融入业务流程早期，实现“合规左移”，能够有效降低后期整改成本。

案例专栏六：某金融科技公司的数据跨境合规解决方案

某专注于国际支付和跨境金融服务的金融科技公司，处理大量用户的个人身份信息、交易数据和财务数据，面临严格的金融监管和数据保护要求。

1.技术应用场景

(1) 构建多法域合规知识图谱：整合全球主要金融监管机构和数据保护机构的法规要求，构建智能知识图谱，为数据跨境决策提供实时合规指引。

(2) 实施数据本地化与区域化部署：根据不同国家的数据本地化要求，采用多区域数据中心部署策略，确保敏感数据在符合要求的司法辖区内存储和处理。对于必须跨境传输的数据，严格遵循最小化原则。

(3) 基于零信任架构的访问控制：实施零信任安全模型，对所有数据访问请求进行严格的身份验证和授权，无论请求来源是内部还是外部网络。结合行为分析技术，实时监测异常访问行为。

(4) 数据沙箱与安全计算环境：为需要进行跨境分析的数据提供安全沙箱环境，确保数据在受控环境中进行处理，并限制数据外泄。对于高度敏感的统计分析，采用差分隐私等技术，在保护个体隐私的前提下发布聚合数据。

(5) 自动生成合规报告：系统能够根据预设模板自动生成数据跨境传输记录、风险评估报告和数据处理活动记录，以满足监管机构的审计要求。

2.实施效果

一是成功通过了多个国家金融监管机构的数据跨境合规审计，获得了业务运营许可。二是有效平衡了业务创新与合规风险，支持了公司在全球范围内的快速扩张。三是提升了数据处理的透明度和可追溯性，增强了用户对金融服务的信任。四是显著降低了人工合规审查的工作量和出错率。

3.核心技术亮点

(1) 智能合规引擎：利用自然语言处理（NLP）和知识图谱技术，将法律法规转化为可执行的合规规则，并集成到数据处理流程中。

(2) 多云/混合云合规管理：针对多区域部署和混合云环境，提供统一的数据合规管理平台，实现跨云环境的数据安全策略一致性。

(3) 加密数据库与同态加密：在某些极端敏感场景下，探索使用同态加密技术，实现数据在加密状态下的计算，进一步提升数据隐私保护水平。

4.经验启示

一是金融行业的数据跨境合规需要高度重视数据本地化和区域化部署策略，以满足严格的监管要求。二是将合规技术与业务流程深度融合，实现“合规即服务”，是提升效率和降低风险的有效途径。三是持续投入研发，探索前沿隐私计算技术，是构建差异化竞争优势的关键。

2.1.1.3 互联互通层

互联互通层构建跨域数据交换通道，实现数据可达、可识别、可交互。

1.核心组件

互联互通层核心组件包括：

- 网络互联包含跨境专线、SD-WAN 智能路由、IPv6-SRv6 路径优化，跨境专线采用 VPN 或 MPLS 技术；
- 数据集成涵盖 API 网关、IDS 连接器、数据传输协议，API 网关负责流量管控与格式转换，IDS 连接器实现异构系统对接，数据传输协议采用 DDTP；
- 目录服务包括元数据管理、数据资产编目、标识解析，元数据管理遵循 DCAT 标准，标识解析采用 DID 或 Handle 方案；
- 分布式身份包含去中心化标识符、可验证凭证、跨域信任传递。

2.典型案例

案例专栏七：CU DataHub 可信跨境数据流动平台

粤港澳大湾区的“CU DataHub 可信跨境数据流动平台”是互联互通层的代表性实践。该平台由深圳数据交易所、中国信通院等联合开发，旨在成为连接数据提供方、需求方和监管方的桥梁，为大湾区乃至全球提供安全、合规、高效的跨境数据流动服务。核心功能方面，CU DataHub 建立了跨境数据资产管理的一站式流程，涵盖数据资产的合规管理、应用管理、价值管理和运营管理，实现从数据登记、交换交易到跨境传输全流程的打通。技术亮点包括：全面遵循国内外数据流动标准和法律，内置高级加密和差分隐私、同态加密等隐私保护技术确保传输中的数据安全与隐私；采用分布式架构和区块链智能合约，实现数据流转自动化和过程可追溯，减少人工介入并提高准确性；提供实时监控与分析工具以及丰富的 API 接口，方便企业系统对接，实时掌握数据流动状态并优化策略。通过这些措施，平台兼顾了高速传输（如引入香港中文大学的网

络编码专利技术提高跨境传输效率和完整性）、严格合规（依据法规建立数据处理流程，避免法律风险）和行业便利（针对医疗、金融等提供定制化的一站式支持，提高服务效率并降低成本）。在实际应用中，CU DataHub 已经支持了多个场景的数据互通：例如会计审计场景中，香港的会计师事务所通过部署 nEdge 数据连接器对接深圳企业的数据，在平台支持下将处理后的结果回传香港，为客户提供便捷服务；又如平台已服务跨境医疗、保险、交通等行业，实现多领域数据自由流动。该平台的建设表明，通过采用国际通用架构（如 IDS）并融合自主创新技术，能够有效解决跨境数据流动中的技术、法律、标准差异问题，搭建出一个区域性的可信数据空间。CU DataHub 的成功经验也为其他地区构建跨境数据交换网络提供了范例，其技术模式具有可复制推广价值，有望在更多跨境场景中应用。

案例专栏八：某跨境数据安全流通平台

某头部数据要素流通交易创新型企业，致力于为企业提供安全合规的数据流通解决方案。

1.技术应用场景

（1）多方安全计算（MPC）平台：为某跨国金融机构提供多方安全计算平台，使其在不共享客户原始交易数据的情况下，与境外合作伙伴共同进行反洗钱（AML）和反欺诈分析。平台利用 MPC 技术，确保各方输入数据的隐私性，仅输出联合分析结果。

（2）区块链存证与审计：在跨境贸易融资场景中，利用区块链技术对贸易合同、物流信息、支付凭证等数据进行存证，确保数据来源可信、流转过程透明且不可篡改。监管机构和审计方可以通过区块链浏览器追溯数据全生命周期，满足合规要求。

（3）数据脱敏与匿名化服务：为某跨国汽车制造商提供数据脱敏服务，对其在不同国家收集的车辆传感器数据和用户行为数据进行处理，生成匿名化数据集，用于跨境的自动驾驶算法研发和城市交通优化分析，同时符合 GDPR 等隐私法规。

2.实施效果

一是成功实现了跨境敏感数据的“可用不可见”，有效规避了数据直接出

境的合规风险。二是提升了金融机构间跨境合作的效率和信任度，加速了反洗钱和反欺诈模型的迭代。三是为汽车制造商的全球研发提供了合规的数据基础，加速了产品创新。四是通过技术手段满足了多国监管机构对数据安全和隐私保护的严格要求。

3.核心技术亮点

(1) 高性能多方安全计算框架。优化 MPC 算法，提升计算效率，支持大规模数据集的联合分析。

(2) 联盟区块链技术：构建许可链网络，确保参与方的身份可信，并提供灵活的治理机制。

(3) 差分隐私与 K-匿名算法：结合多种脱敏技术，在保证数据可用性的同时，最大化隐私保护水平。

4.经验启示

一是将前沿隐私计算技术与实际业务场景深度结合，是解决跨境数据流通难题的有效途径。二是技术解决方案需要与法律合规框架紧密配合，才能真正落地并发挥作用。三是构建开放的生态系统，吸引更多合作伙伴共同参与，是推动可信数据空间发展的关键。

案例专栏九：城市交通数据可信共享与跨境协同

某城市交通领域的领先企业，在智慧城市建设和交通数据管理方面拥有丰富经验，积极探索城市交通数据的跨境应用。

1.技术应用场景

(1) 城市交通数据联邦分析：深城交与香港、澳门等地的交通研究机构合作，利用联邦学习技术，在不交换原始交通流量、出行 OD（Origin-Destination）数据的情况下，共同分析区域交通拥堵模式、预测未来交通需求，为大湾区跨境交通规划提供决策支持。

(2) 数字孪生城市数据可信映射：在构建粤港澳大湾区数字孪生城市的过程中，深城交利用可信数据空间技术，将深圳的交通基础设施、实时运行数据等，在确保数据主权和安全的前提下，与香港、澳门的数字孪生平台进行可信映射和互联互通，实现跨境交通态势的实时感知和协同管理。

(3) 跨境出行服务数据协同：与跨境出行服务提供商合作，通过 API 网

关和标准化接口，在用户授权的前提下，安全地共享部分匿名化出行数据（如公共交通班次、口岸通关时间等），为大湾区居民提供无缝的跨境出行信息服务。

2.实施效果

一是成功实现了粤港澳大湾区城市交通数据的安全跨境协同，为区域一体化发展提供了数据支撑。二是在保护城市数据隐私和安全的前提下，提升了跨境交通规划和管理的科学性与效率。三是促进了跨境出行服务的创新，提升了居民的出行体验。四是为城市级数据可信流通和跨境合作提供了示范案例。

3.核心技术亮点

(1) 城市级数据联邦学习平台：针对大规模、多源异构的城市交通数据，设计高效的联邦学习算法和分布式架构。

(2) 地理空间数据隐私保护：结合差分隐私和地理混淆技术，对包含位置信息的交通数据进行隐私保护处理。

(3) 高并发 API 网关与数据交换平台：支持海量交通数据的实时交换和查询，确保跨境服务的响应速度和稳定性。

4.经验启示

一是城市级数据跨境协同需要政府、企业、研究机构等多方共同参与，形成合力。二是将可信数据空间技术应用于智慧城市建设，能够有效解决城市数据共享和隐私保护的矛盾。三是标准化和开放性是推动城市数据互联互通的关键，有助于构建可持续的数字生态系统。

2.1.1.4 业务与应用层

业务与应用层面向行业提供数据协同、联合建模、跨境交易等应用服务。

1.典型应用

业务与应用层的典型应用场景包括：

- 金融服务：跨境支付清算、反洗钱联合风控、跨境征信互认；
- 医疗健康：国际多中心临床研究、远程医疗会诊、病历数据共享；
- 智能制造：全球供应链协同、车联网跨境数据分析、工业互联网平台；
- 数字贸易：跨境电商数据流通、国际物流追踪、贸易单证电子化。

2.典型案例

案例专栏十：“龙数贸”跨境数据服务
深圳市龙华区打造的“龙数贸”跨境数据服务是业务层应用的经典案例。该服务由九鑫智能公司建设，在区政数局指导下，利用其安全数据平台和数据加工技术，将邓白氏等海外合规授权的商业数据引入本地，为产业带企业提供全球市场情报分析。具体而言，“龙数贸”服务整合了来自全球 200 多个国家、超 5.6 亿家企业的高质量商业数据，通过 RPA 机器人和 API 接口从全球电商平台、B2B 网站、行业报告等获取多维信息（产品、客户、订单、评价等），并进行清洗和标准化处理。然后运用自然语言处理（NLP）和机器学习模型对市场行情、客户反馈进行深度挖掘，结合企业内部数据形成智能决策建议。在龙华区一家医疗器械企业的应用中，该平台帮助其匹配了欧洲市场的需求：企业利用平台获取了详尽的目标市场经济态势、行业趋势、主要竞争对手和潜在合作伙伴信息，以及潜在客户联系渠道。基于这些数据洞察，企业迅速调整营销策略并优化供应链布局，在不到半年时间里成功渗透多个欧洲细分市场，大幅提升了品牌知名度和市场份额。据测算，通过“龙数贸”数据服务，预计未来 3 年该行业有望新增 10 多个海外市场准入机会，国际市场收入增长 10%～30%，市场分析时间缩短 30%～40%，供应链效率提高 20%～40%且成本降低 5%～15%以上。该案例还荣获 2024 全球电子商务创业创新大赛跨境电商组一等奖，充分证明了跨境数据应用对传统产业的巨大赋能。“龙数贸”案例表明，在政府合规指导和国际数据授权的前提下，跨境数据的深度应用可以显著降低企业出海的难度和风险，成为企业数字化转型和全球布局的关键驱动力。类似地，在跨境金融领域，邓白氏的跨境企业征信服务帮助外向型企业在香港获得融资也是成功实践：通过共享境内企业的信用数据给境外金融机构，在保障合规的同时解决了信息不对称，促成中小企业跨境贷款。这些案例覆盖贸易、制造、金融等多个领域，展现了跨境可信数据空间在业务层的广阔前景——未来将有更多行业涌现出基于数据要素流通的创新应用，推动数字经济在全球范围的繁荣发展。
案例专栏十一：金融行业跨境风控协作平台

某大型商业银行与东南亚合作银行共同建设的“跨境风控协作平台”，是这一模式的典型代表。平台的建设目标是实现跨境信用风险联合评估，在确保境内客户数据不出境的前提下，共享风险特征与模型参数。

项目采用了双节点架构：一端位于上海，另一端位于新加坡。双方首先通过国家数据局备案的数据目录系统完成资产登记与分级，并签署经安全评估通过的数字合约。合约条款以机器可读的形式固化在系统中，对数据类型、使用范围、调用频率和再转移权限作出明确限定。

随后，双方基于联邦学习框架在本地完成模型训练，仅以加密参数的形式交换中间结果。整个训练过程运行在可信执行环境（TEE）中，传输链路采用国密算法进行端到端加密。所有调用和参数交互的记录自动写入区块链账本，实现全过程可追溯与可审计。

项目上线后，模型训练周期较以往缩短了约 40%，风险识别准确率提升了 12%。更重要的是，该平台成为首批通过国家网信办数据出境安全评估的金融项目之一。

其成功的关键在于“模型出境而非数据出境”的思路创新，以及数字合约对合规与业务目标的双重绑定。这一案例证明，通过可信计算与策略执行机制，可以在不牺牲安全与合规性的前提下，实现跨境数据的价值共创。它为金融业大规模国际协作提供了可复制的模板，也为监管部门探索评估结果互认与动态备案机制提供了技术依据。

案例专栏十二：汽车行业跨境智能运维中心

2024 年，一家日系主机厂在华设立的全球数据枢纽率先引入“跨境智能运维中心”模式。

该模式以可信数据空间为底座，通过“安全沙箱+数字合约+再转移控制”三项机制，实现了境内车辆数据的合规出境与受控使用。

在数据采集端，系统自动根据车型与场景执行分类分级策略，将含有个人信息的影像与语音数据即时脱敏并本地存储，仅允许技术参数和设备状态数据进入跨境目录。所有跨境数据产品都在国家级数据空间平台完成注册和标签标注，确保每一项数据流动都可被发现与追踪。

当总部需要进行算法优化或质量分析时，可通过合约授权访问沙箱环境。

所有分析计算均在境内完成，仅结果文件（如优化参数、统计报告）出境。

数字合约规定了结果文件的用途、保存期限及再转移限制，一旦超出范围即触发自动封禁或告警。同时，沙箱环境生成详尽的操作日志和算法调用记录，并通过区块链进行存证，确保整个过程符合法规要求。

项目运行一年后，车辆远程诊断的精度提升了 25%，OTA 升级周期由季度缩短至月度。企业内部的合规成本下降约三分之一，系统通过了工信部和网信办的联合评估。

该案例的核心价值在于确立了“结果出境替代原始出境”的原则，技术上实现了数据可用但不可见的状态，治理上实现了责任可界定、行为可审计。这一模式被多家跨国 OEM 借鉴，逐步形成智能汽车行业的数据跨境治理标准雏形。

案例专栏十三：医疗 AI 协同创新平台

2023 年底，国内某三甲医院与欧洲研究机构共同启动了“国际医学影像 AI 协同创新平台”。项目的目标是在不出境原始影像数据的前提下，联合开发脑部疾病诊断模型。双方选择了“标准合同+安全认证+伦理双备案”的路径。

在平台架构上，境内医院的数据中心部署了隐私计算节点，节点采用 TEE 和多方安全计算（SMPC）技术，支持本地模型训练与加密参数交换。欧洲研究机构在境外节点运行聚合算法，对上传的参数进行加权融合生成全局模型。整个过程在数字合约控制下运行，合约条款定义了数据种类、算法用途、保留期限和再转移限制。所有训练活动均被写入合约账本，并由第三方审计机构进行验证。此外，平台还与医院伦理委员会系统打通，自动同步研究备案信息，实现了伦理与技术双重闭环。

该项目的实施使模型训练效率提升一倍，数据出境审批周期缩短 40%，并成功获得欧盟 GDPR 与中国安全评估的双重合规认证。医院与研究机构均能在可控环境下共享算法成果，推动了跨境医学 AI 的产业化应用。

从技术角度看，该案例展示了隐私计算、伦理审批与数字合约三者的深度融合；从治理角度看，它为跨国科研合作提供了“合规即服务”的基础设施模式。这种模式未来有望推广至药物研发、国际远程诊疗及跨国公共卫生监测等更广泛的场景。

2.1.2 核心技术组件

基础设施的技术实现依托六大核心组件，各组件在不同架构层次协同工作，支撑数据全生命周期安全流转。

组件	核心功能	关键技术	部署层次
身份认证	跨域身份互认与权限管理	分布式身份（DID/VC）、PKI 数字证书、多因子认证（MFA）、生物识别	基础安全层
目录管理	数据资产发现与元数据治理	DCAT 元数据标准、Handle 标识解析、语义检索引擎	互联互通层
数字合约	规则自动化执行与履约追踪	区块链智能合约、ODRL 权限语言、策略引擎	治理合规层
隐私计算	密态数据协同分析	MPC/联邦学习/同态加密/TEE、差分隐私	基础安全层
加密传输	链路安全与数据保护	TLS 1.3、国密 SM2/SM4、IPsec VPN、完整性校验	基础安全层
审计追溯	全流程行为记录与溯源	区块链存证、日志审计系统、数字水印、数据库审计	治理合规层

2.1.2.1 身份认证

身份认证是数据跨境流通的第一道安全关口。传统的用户名密码方式难以满足跨域场景的安全需求，需引入多因子认证和基于密码学的强身份认证机制，多因子认证包括密码、动态令牌和生物识别。

分布式身份（DID/VC）：去中心化标识符（Decentralized Identifiers，DID），基于区块链技术，为数据主体、机构、数据资产分配全局唯一标识，无需依赖中心化身份提供商。可验证凭证（Verifiable Credentials，VC），将身份属性比如资质证明、授权许可以加密签名形式发放，接收方可独立验证凭证真实性而无需联系发放方。

PKI 数字证书：公钥基础设施（PKI），通过数字证书绑定实体身份与公

钥，支持数字签名和加密通信。在跨境场景中，需建立跨域信任锚（Trust Anchor）或采用联邦身份管理模式，实现不同国家颁发的证书互认。

跨域信任传递：通过建立国际信任列表（如欧盟 eIDAS 信任服务列表）、双边互认协议（如中新两国电子签名互认）、联邦身份协议（如 SAML/OAuth 2.0），实现“一次认证、多域互认”。

2.1.2.2 目录管理

目录管理解决“数据在哪里”和“数据是什么”的问题。在跨境场景中，数据来源多样、分布广泛、格式各异，需要统一的元数据标准和目录服务。

元数据标准：采用 DCAT（Data Catalog Vocabulary）国际标准描述数据集的基本属性，具体包括技术元数据、业务元数据和治理元数据三类。技术元数据涵盖名称、格式包括 JSON、CSV、Parquet、字段定义、数据量、更新频率；业务元数据包含所属领域、应用场景、数据质量评分、使用限制；治理元数据涉及所有者、分类分级标签包括一般、重要、核心、敏感字段标识、出境合规状态。

标识解析体系：为每个数据资产分配全球唯一标识符比如 Handle System、DOI，支持跨系统链接和精准定位，标识解析服务提供“标识→元数据→访问接口”的完整映射。

跨域发现机制：提供多维度检索能力、语义检索、智能推荐，多维度检索能力支持按名称、分类、标签、行业、跨境属性检索，语义检索基于本体的概念匹配，智能推荐根据用户画像推荐相关数据集，对于敏感数据，检索结果附加合规提示和风险预警。

2.1.2.3 数字合约

数字合约即智能合约，将数据共享协议以代码形式固化在区块链上，实现条款自动执行、不可篡改、可追溯验证。

权限定义语言：采用 ODRL（Open Digital Rights Language）标准，核心是通过结构化规则明确授权主体、授权操作、授权对象、约束条件及禁止行为。

自动化执行：智能合约监听数据访问事件，当触发条件满足比如接收方完成支付、提供合规证明时自动授予访问权限；当检测到违约行为比如超范围使用、未经授权再转移时自动终止权限并触发惩罚机制比如扣除保证金、发送监管预警。

跨链互操作：遵循 ERC-7683 跨链意图标准、IEEE 3221.01-2025 跨链交易标准，实现不同区块链平台间的合约互操作，通过跨链桥（如 LayerZero、Chainlink CCIP）传递合约调用消息，采用“三阶段提交”协议保障跨链交易原子性。

2.1.2.4 隐私计算

隐私计算是实现“数据可用不可见”的核心技术，允许多方在不共享原始数据的前提下进行协同计算。

安全多方计算（MPC）：将计算任务拆解至多个参与方，各方基于本地数据完成子任务计算并交换加密中间结果，最终合成计算结果，适用于对计算精度要求高、参与方互信程度较低的场景，比如联合统计、隐私集合求交。

同态加密：支持在加密状态下对数据进行运算，计算结果解密后与明文运算结果一致，适用于需将加密数据委托给不可信云环境进行计算的场景。

联邦学习：让各参与方在本地用自己的数据训练模型，仅交换加密的模型参数即梯度到中心服务器进行聚合，迭代优化成全局模型，原始数据始终保留本地。

可信执行环境（TEE）：在处理器内部创建隔离的安全区域，敏感数据在该区域内被解密和处理，外部系统包括操作系统、虚拟化层均无法访问，适用于需要在云端处理明文数据但又要防止云服务商窥探的场景。

差分隐私：在数据统计结果中加入精心设计的随机噪声，使得单个数据主体的信息无法被精准识别，同时保证统计特性基本不变，适用于公开发布统计报告、开放数据集的场景。

2.1.2.5 加密传输

加密传输保障数据在跨境流动过程中的机密性和完整性，防止网络窃听、篡改、重放攻击。

传输层加密：包括 TLS 1.3、国密 SM2/SM4、IPsec VPN，其中 TLS 1.3 是最新传输层安全协议，支持前向保密即 Forward Secrecy、0-RTT 握手、强制加密套件；国密 SM2/SM4 符合中国商用密码标准，用于政务、金融等强监管领域；IPsec VPN 在网络层建立加密隧道，实现点到点或网到网安全通信。

端到端加密：确保数据从发送方加密到接收方解密的全过程中，任何中间节点包括路由器、代理服务器、云服务商均无法解密数据内容。

完整性保护：通过数字签名、消息认证码、哈希校验验证数据在传输过程中未被篡改。

2.1.2.6 审计追溯

审计追溯实现数据流转全流程可记录、可查询、可验证，是事后追责和合规证明的关键。

区块链存证：将数据操作日志的哈希值定期写入区块链，利用区块链不可篡改特性确保日志真实性，日志内容包括操作主体即 DID、操作时间即可信时间戳、操作类型包括访问、下载、计算、操作对象即数据集标识、操作结果包括成功、失败。

日志审计系统：跨层采集数据库日志、应用日志、网络流量日志，进行语义解析和行为识别，输出可解释审计报告，支持多维度查询和异常检测，多维度查询支持按用户、时间、数据集、操作类型检索，异常检测识别越权访问、批量下载等风险行为。

数字水印：向高价值非结构化数据包括文档、图片、视频嵌入不可见水印，记录数据来源和使用者信息，数据泄露后可通过水印提取快速定位责任主体。

合规留存：日志保存期限根据数据敏感等级遵循对应法规规定的留存要求，存储环节采用加密、冗余备份、异地容灾等安全措施，确保日志存储的安全性、完整性与合规性。

2.1.3 技术成熟度评估

跨境数据流通基础设施各项技术的成熟度呈现梯度分布，部分技术已进入大规模商用阶段，部分技术仍处于试点探索期，具体分布如下：

传统安全领域：其代表技术包括 TLS/IPsec、防火墙/DLP、数据库审计，成熟度处于高度成熟水平，商用化程度极高，可实现标准化部署，当前面临的核心挑战集中在性能优化与国密适配方面。

数据治理领域：涵盖分类分级、脱敏、访问控制技术，成熟度为成熟应用水平，已形成完善的工具体系并广泛应用，仍需在自动化程度提升与跨域协同能力上持续优化。

区块链领域：联盟链、智能合约、存证溯源技术成熟度同样为成熟应用水平，在金融贸易领域已实现成熟落地，跨链互操作与性能扩展是其主要改进方

向。

隐私计算领域：包含 MPC、联邦学习、同态加密、TEE 等技术，成熟度处于快速发展阶段，目前处于从试点向商用过渡的关键阶段，计算性能、标准化建设与互操作性是当前面临的主要课题。

分布式身份领域：以 DID/VC 为核心技术，成熟度同为快速发展阶段，已在部分区域开展试点并逐步推广，全球互认机制建立与信任列表完善是其推广过程中的核心挑战。

量子安全领域：包括后量子密码（PQC）、量子密钥分发（QKD）技术成熟度处于探索阶段，目前处于从实验室研究向试点应用推进的阶段，面临成本控制、系统兼容性与标准化建设等多重挑战。

技术成熟度等级说明如下：

- 高度成熟：技术体系稳定可靠，配套产品丰富多样，行业标准完善健全，已实现大规模商业化应用；
- 成熟应用：技术方案具备较高可靠性，拥有成熟的商业化产品，行业应用覆盖广泛，在特定场景下仍有优化空间；
- 快速发展：技术可行性已通过验证，试点应用案例丰富，商业化进程加速推进，相关标准正在逐步完善；
- 探索阶段：技术原型已具备使用条件，仅开展小范围试点验证，商业化落地路径仍需进一步明确；
- 前沿研究：目前处于理论验证阶段，技术实用化过程中面临较大挑战，短期内难以规模化应用。

技术选型建议方面，核心业务场景需优先选用高度成熟或成熟应用等级的技术方案，以保障系统运行的稳定性与可维护性；创新试点场景可适度尝试快速发展阶段的技术，同时需提前做好技术风险评估，制定完善的应急预案；前瞻性布局场景应持续关注探索阶段及以下等级的技术发展趋势，结合业务需求适时开展技术储备与研发投入，为未来业务拓展奠定基础。

案例专栏十四：欧数中算平台
同态科技基于高效的隐私增强技术底座，建设了“欧数中算”平台，面向“一带一路”沿线国家，创新性内置了“密文计算引擎”，具备以高性能同态

加密为核心的数据封装、云数据托管、多维数据权限管控、数据安全融合计算、全流程监管等关键技术能力，保障数据在跨境计算时，数据的可用性、安全性和保密性，以便中俄科技企业、研究院校等能够灵活、快速、便捷地接入平台，增强自身的差异化竞争能力和数字经济创新能力。

其建设核心为“基于同态加密的标准化数据安全共享架构”，该框架具备高性能、轻改造的优点，对于数据安全共享等复杂场景可以进行有效标准化覆盖，满足在密文上完成后续的相关业务的数据计算应用。在相关部门的指导下，平台满足科研数据的跨境使用合规要求，在安全高效、灵活可控的基础上，解决了大规模数据资源计算问题，提高了数据可复用性、科研成功率，降低了单一用户的建设成本。

1.数据服务平台

整体自主搭建私有云模式，自主搭建私有云服务和系统服务平台。充分利用自身机房的硬件安全防护能力，以及 7*24 的响应能力来应对系统的突发情况。基于业务场景化、模块化的设计方法，将实现数据交易平台中技术基础架构模块与业务运营模块松耦合，保障数据交易平台业务的动态扩展，新的数据业务与数据产品能够快速上线，且不影响原有运营。

在医疗健康领域，针对三类病例数据，总计药品 9 种，药物风险 214 种，整体病例 11345301 列，俄方通过租用同态隐私计算设备和按月、按功能订阅平台密文服务，首先完成原始数据的加密后传输至中国西北部的超算中心，再调用服务对加密数据实现密文计算与核验等功能。在此过程中，一方面，跨境企业可以利用中国高性能计算资源针对加密状态下的数据完成药物风险性与治愈率的差异性研究，仅对最终检验和分析结果进行解密确认，实现跨境联合科研中对照性实验的广泛、快速、有效和安全的结果共享。另一方面，平台能够提供隐私数据托管、数据安全交易和安全审计等服务，实现基于国产密码技术的安全存储及密文操作、数据确权，完善数据交易体系亟需解决的隐私化、安全化问题。

平台引入态势感知等主动防御策略，采用横向到边、纵向到底的方式建立应用隐私计算技术的数据交易平台安全防护体系，在传统安全支撑服务体系的基础上，采用商用密码算法和隐私计算应用技术建立密码应用支撑平台，面向

应用业务系统输出身份鉴别、传输保护、数据加密、可信时间、电子签章、访问控制等安全服务能力，对身份认证、支付结算等重要应用场景和关键环节开展全流程监控，对数据制定严格的权限控制机制、数据加密机制、开放脱敏机制，提升面向数据交易服务应用安全支撑能力。筑牢平台的安全基座，打造安全可信的运行环境。

在数据交付方面，平台使用自主可控的同态加密及隐私计算赋能数据交易，在确保数据交付过程全流程“可用不可见”的基础上，具备以下优势：

(1) **不改变原有业务模式，集成更轻松**：同态加密让数据在加密后依旧保有原有的计算能力，能够在数据层面实现数据可用不可见。因此基于同态加密构建的隐私计算平台确保原有业务模式的数据流向、数据使用方式等关键环节都不受影响，用户能够在不改变业务模式的情况下，享受隐私计算的赋能。

(2) **数据资产可复用，共享更省心**：原始数据经过平台处理后，生成的数据资产保有了数据的计算能力与可复用性。因此，数据源在接入平台后，仅需要对数据进行加密后共享，无需对接烦琐的协议或是进行复杂的系统改造。另一方面，当数据源的数据共享业务规模化扩大后，借助数据资产的可复用性，一份数据资产支持给到多个需求方进行使用。因此数据源无需为数据共享业务的拓展而投入大量成本。

(3) **新业务无需定制化开发，适配更轻便**：基于同态加密的能力，平台在数据层实现了隐私计算，隐私计算能力不受应用层的限制。因此，无需对数据交换共享过程中的不同业务应用进行定制化开发，有效降低了适配成本。

(4) **超高速算法核心，运算更高效**：平台的算法核心可采用国产自主可控同态加密算法，能够有效支持大数据场景下的数据交换共享应用场景。

(5) **核心模块国产，应用更合规**：平台的核心模块可实现全部国产自研，保证核心技术安全可控。实现充分的数据安全和隐私安全，对于国家、社会、公民绝对负责。

2.**业务创新性**

(1) **数据融合层面**，确保工业大数据、企业经营数据、装备数据、制造数据进行全生命周期的密态数据融合应用，降低工业信息化及各行业数据在密态流转过程中，尤其是使用过程中的风险。

(2) 数据交付层面，运用商用密码技术对数据源以密文形式完成数据的汇总、加工、分析，有效解决了企业在数据交付环节的不信任问题，有效保护双方的数据资产。

(3) 数据管控层面，通过商用密码设定数据的使用权限控制，形成数据源对于数据应用的直接授权细粒度管理，实现商用密码对数据应用的全流程可控制、可监控、可审计。

(4) 应用拓展层面，应用同态加密技术对原有商用密码系统进行优化与升级，对原有业务流程和 IT 基础设施的改造较小，并且填补了商用密码技术在数据交易领域的空白，对于未来推动我国商用密码在更多领域、更大范围的应用扩展起到了一定的先行示范作用。

3.标准符合

(1) 方案按照 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》，对数字丝绸之路数据密态流通与跨境数据交易平台密码应用需求进行了分析，在此基础上对数据交易平台进行了密码应用的总体设计，同时根据业务特点结合新型商用密码技术进行相关业务创新，实现商用密码在工业和信息化领域的推广应用。

(2) 方案明确了密码应用技术框架、密钥管理等内容，通过部署具有商用密码产品认证证书的相关产品，采用基于国产商用密码算法、技术、产品和服务，实现包括身份的真实性、数据的机密性和完整性保护等密码应用功能。方案内容完整、设计合理、技术路线可行，可用于相关密码应用实施建设。

4.行业推广

本方案实现了基于密文的多源数据融合，让数据在加密后依旧保有原有的计算能力，能够在数据层面实现数据可用不可见。因此融合同态隐私计算应用服务后的多源数据融合场景能够复用原有业务模式，数据流向、数据使用方式等关键环节都不受影响。不但保护了数据源的数据价值，支撑了数据融合方的数据应用，还无需定制化开发，有效降低了适配成本，因此在政务、工业互联网、金融等涉及重要关键数据的行业内进行推广具有天然优势。

5.经济效益

本方案在中后期有较高的经济效益和较好的抗风险能力，推动地区高科技

企业集聚、促进招商引资、提高税收。在社会效益方面，本方案有利于我国商密行业的持续发展与产业链生态壮大，协助各省市构建行业性数据资源平台，提升城市的差异化竞争能力和数字经济创新能力。

平台未来将持续面向科技型中小企业、具有跨境业务的国际型公司，以及政府部门、高校、研究机构等，提供隐私数据托管、交易、计算服务，通过参与构建全国数字交易流程与规则制定，最终将数据平台建设成面向“一带一路”沿线国家，具备差异化竞争能力和数字经济创新能力的跨境数据服务中心，从更多维度、更多行业、更大体量的打通数据孤岛，使数据价值在某地区得到最大程度地释放，从而推动地区数字经济高质量发展。同时，扩大我国商用密码产品和服务的影响力，增强我国密码产业的国际竞争力。

2.2 关键能力建设

数据基础设施的关键能力建设围绕身份管理、目录服务、合约执行、隐私计算、安全传输五大模块展开。各模块既相对独立又协同工作，共同支撑数据跨境流通的安全、合规与高效。

2.2.1 数据身份与信任管理

2.2.1.1 建设目标

建立统一、兼容、互认的身份管理体系，确保参与方身份的真实性、唯一性、可验证性与可追溯性，实现身份信息全生命周期可控管理。

2.2.1.2 核心建设内容

提供标准化的身份注册入口，支持不同主权领域、不同技术体系的实体完成身份信息初始登记，采用实名核验与资质审核双验证机制，通过区块链锚定确保身份源头的真实性和合法性。基于分布式身份架构，为注册主体生成全局唯一的 DID，签发过程采用加密签名技术，确保身份凭证防篡改、可验证，同时支持多格式输出，兼容国际标准与区域规范。验证方通过公开可查的分布式账本或解析服务，快速验证对方身份凭证的有效性和发行方签名，完成无中心化依赖的信任建立。建立实时的身份状态机制，当实体资质过期、权限变更或出现安全风险时，发行方可及时更新或撤销其凭证，并实时同步至跨域信任网络。

2.2.1.3 技术要求

- 身份标识格式遵循 W3C DID Core 规范
- 加密算法支持国密 SM2/SM3、RSA 2048、ECDSA P-256
- 互操作性兼容欧盟 eIDAS 与中国电子认证服务体系
- 隐私保护支持零知识证明实现选择性披露

2.2.2 数据目录与资产编目

2.2.2.1 建设目标

构建统一、智能的数据资源管理体系，实现跨境数据资产的标准化管理、精准发现与描述、规范化流转。

2.2.2.2 核心建设内容

建立覆盖数据资产全生命周期的元数据模型，涵盖基础元数据、业务元数据、治理元数据、溯源元数据。基础元数据包括名称、描述、格式、字段定义、数据量、创建及更新时间；业务元数据包含所属行业、应用场景、质量评分、使用限制；治理元数据涉及所有者、分类分级标签、敏感字段标识、出境合规状态、数字合约 ID；溯源元数据涵盖数据血缘、处理历史，整体兼容国际标准，确保跨系统互操作。

采用分层联邦式编码结构，编码格式为基础设施前缀、主权代码、数据空间标识、产品标识。其中基础设施前缀标识数据产品归属的顶层命名空间，主权代码明确数据产品的原始注册地和司法管辖锚点，数据空间标识是数据所在空间的唯一标识，产品标识是空间分配的本地唯一编码，基于相关技术提供全球解析服务，支持“标识→元数据→访问接口”的完整映射。

提供多维度精准检索能力，包括关键词检索、分类导航、高级筛选、语义检索。关键词检索支持按名称、标签、描述全文检索；分类导航可按行业、场景、分级筛选；高级筛选支持按数据格式、更新频率、质量评分、地理覆盖范围组合筛选；语义检索基于本体的概念匹配，检索结果附加合规提示和访问方式。

2.2.2.3 技术要求

- 元数据采集自动扫描数据库、数据湖、文件系统，提取 schema 和统计信息
- 质量审核自动校验元数据完整性，人工审核业务描述准确性
- 检索性能满足大规模数据集快速响应，支持模糊查询和联想推荐
- 敏感数据目录仅对授权用户可见

2.2.3 数字合约与策略管控

2.2.3.1 建设目标

提供合约模板管理、策略配置与执行引擎，将跨境数据合规要求、业务合作约定转化为可执行、可监控的数字化合约，实现数据流转全流程自动化管控。

2.2.3.2 核心建设内容

内置覆盖多场景、多行业的标准化合约模板，包括通用模板、行业模板、合规模板。模板内置通用法律条款、合规基线和业务逻辑，企业可在标准模板基础上自定义条款，定制化模板需经平台合规审核。

将合约规则转化为机器可读的策略集，采用 Open Digital Rights Language 描述权限，明确授权对象、授权主体、允许执行的操作，限定使用目的和有效期，禁止转分发、商业化等行为。策略执行引擎实时拦截数据访问请求，判断是否符合策略条件，决定允许、拒绝或告警，策略冲突时按“属地优先、约定优先”原则自动裁决。

履约管理与计量计费方面，记录合约关键节点，生成可信存证；自动识别越界行为，触发合约暂停、告警或罚金扣除；支持多种定价模型，自动生成账单和结算指令；按贡献度自动分配收益。

2.2.3.3 技术要求

- 合约部署在联盟链或公链
- 跨链互操作支持主流跨链协议
- 合约代码需通过第三方安全审计
- 满足跨境数据合规相关技术规范

2.2.4 隐私计算与安全沙箱

2.2.4.1 建设目标

综合运用安全多方计算、联邦学习、同态加密、可信执行环境等技术，构建技术先进、兼容适配、安全可控的隐私计算平台与沙箱环境，支持数据“可用不可见”的跨境协同分析。

2.2.4.2 核心建设内容

提供统一计算框架，支持多种隐私计算技术组合应用。MPC 引擎基于秘密共享、混淆电路实现通用计算，支持基础运算；联邦学习框架支持横向联邦、纵向联邦、联邦迁移学习；同态加密库集成开源库，支持多种加密方案；TEE 运行时兼容主流硬件，提供硬件级内存加密和远程证明。计算任务自动选择最优技术组合，按场景适配不同技术方案。

为跨境数据协作提供物理隔离、逻辑隔离、权限可控的计算环境。网络隔离方面，沙箱与外部网络严格隔离，仅允许经审核的 API 调用；数据隔离方面，不同用户的沙箱环境资源独立，数据不交叉；权限管理遵循最小权限原则，用户仅可访问授权数据集和工具库；结果审核要求计算结果需经脱敏审核方可导出。沙箱提供预装工具和预置数据接口。

全流程安全监控包括准入审核、行为监控、异常检测、审计日志。准入审核需完成用户身份认证、资质审核；行为监控记录用户关键操作；异常检测识别可疑行为；审计日志采用加密存储且不可篡改，支持合规审计和事后溯源。

2.2.4.3 技术要求

- 满足隐私计算相关技术标准，支持多技术融合应用
- 联邦学习模型精度接近集中式训练水平，保障隐私保护强度
- 遵循相关行业标准，确保跨平台互操作性
- 沙箱提供多样化访问方式，支持常用编程语言

2.2.5 传输加密与审计追溯

2.2.5.1 建设目标

提供端到端加密传输、实时流量监测、全流程审计追溯能力，确保数据在传输过程中的机密性、完整性，并实现事后可追溯、可审计。

2.2.5.2 核心建设内容

端到端加密传输涵盖传输层加密、应用层加密、完整性保护、前向保密。传输层加密采用高安全等级协议，禁用低版本协议，支持国密算法套件以满足国内合规要求；应用层加密在传输层加密基础上再对敏感数据加密，密钥由数据控制方管理；完整性保护采用消息认证技术，防止中间人篡改；前向保密采用密钥交换技术，保障历史通信安全。国际传输优先使用跨境专线，公网传输需建立加密隧道。

全流程审计追溯会捕获每次跨境传输的关键信息，包括发起方、接收方、数据资产标识、传输时间、数据量、加密算法、传输状态。日志采用加密存储，通过哈希技术保障完整性；关键日志的哈希值定期上链，确保不可篡改；支持多维度溯源查询；日志留存符合《数据出境安全评估办法》要求。

实时监控与异常检测会实时监控跨境数据流量、并发连接数、传输速率，建立异常检测规则库；检测到高危异常时自动阻断传输、告警管理员、生成事件报告；可视化展示跨境数据流向、热点传输路径、风险态势。

2.2.5.3 技术要求

- 加密传输满足等保 2.0 三级及以上要求，通过商用密码应用安全性评估
- 日志系统支持大规模日志存储与快速查询
- 异常检测具备高准确率，降低误报率
- 符合跨境数据传输相关安全规范

2.3 技术标准与互操作

技术标准是实现跨境数据流通互操作的基础。本节梳理国内外数据跨境标准体系的最新进展，阐述数字合约、隐私计算、元数据、标识解析等关键领域的互操作规范，并分析国际互认机制的实践路径。

2.3.1 国内外标准体系进展

2.3.1.1 中国标准体系 2024 至 2025 年最新进展

标准编号	标准名称	生效时间	核心内容	强制性
GB/T 43697-2024	《数据安全技术数据分类分级规则》	2024 年 3 月	规定数据分类分级的原则、框架、方法和流程，为重要数据识别提供依据	推荐性
GB/T 46068-2025	《数据安全技术个人信息跨境处理活动安全认证要求》	2026 年 3 月	我国首个数据跨境国标，细化认证路径技术要求，包括组织管理、制度流程、技术措施等	推荐性
T/CCSA 540-2025	《隐私计算安全接口规范》	2025 年 1 月	定义任务创建、算法容器、结果返回等 12 个原子接口，要求双向 mTLS 1.3、国密 SM2、会话密钥一次一密	团体标准
T/IDSA 001-2024	《跨境数据流通技术指南》	2024 年 6 月	北京国际大数据交易所发布，量化最小可用数据集即≤原始字段 5%、重识别风险即 $\varepsilon \leq 1$	团体标准

GB/T 46068-2025 是里程碑式标准，与《个人信息出境认证办法》形成配套，将认证从法律概念落地为可执行的技术规范。标准对个人信息处理者和境外接收方提出硬性要求：签订具有法律约束力的文件、建立组织管理体系、明确处理规则、开展影响评估、配备技术措施包括加密、脱敏、访问控制、建立应急响应机制。

2.3.1.2 国际标准最新进展

标准组织	标准编号/项目	发布/立项时间	新增内容
ISO/IEC	27701:2019 2024 更新	2024 年修订	隐私信息管理扩展要求，新增跨境数据处理者合规检查清单
IEEE	P3158 可信数据空间系统架构	2024 年立项	中国专家主导，定义 TDS 参考架构、互操作接口、安全要求，预计 2026 年发布
IEEE	P1988 集成隐私技术的数据空间架构框架	2023 年立项	聚焦隐私计算在数据空间中的集成应用，预计 2025 年发布
APEC	CBPR 2.0 跨境隐私规则	2024 年扩容	菲律宾、墨西哥加入，成员经济体扩至 8 个，新增 AI 数据跨境专项规则
ITU-T	X.1458 数据跨境流动安全框架	2025 年预研	由中国主导提案，定义数据出境安全评估技术要求和互操作协议

2.3.1.3 差异对比与实践建议

标准体系	核心理念	适用场景	企业策略
中国 GB/T 46068	国家安全优先，强调认证路径和第三方评估	中国企业数据出境或外企向中国传输数据	强制遵守，作为合规基线
ISO/IEC 27701	风险管理导向，体系化 ISMS 即信息安全管理体系	跨国公司全球合规，提升整体数据治理水平	建议采纳，建立统一管理框架
APEC CBPR	企业自评认证，促进贸易便利化，互信机制	APEC 经济体间跨境业务，降低重复认证成本	可选补充，尤其在亚太区域

实践建议：中国企业以 GB/T 46068 为基线要求，叠加 ISO 27701 体系化管理包括建立 ISMS、定期风险评估、持续改进，有条件的可申请 CBPR 认证以简化在 APEC 区域内的合规流程；跨国企业建立全球框架加本地化适配策略，全球层面采用 ISO 27701，中国区域满足 GB/T 46068，亚太区域可获取 CBPR 认证；中小企业优先满足强制性要求比如中国企业必须符合 GB/T 46068，借助第三方合规服务平台降低技术门槛。

2.3.2 数字合约与策略互操作

数字合约和策略管理是实现数据流通规则自动化执行的关键，互操作性依赖于权限语言、身份体系、智能合约的标准化。

2.3.2.1 ODRL：机器可读权限语言

ODRL（Open Digital Rights Language）是 W3C 推荐标准，用于描述数据使用权限、限制条件、义务责任。

技术规范：遵循 W3C ODRL 2.2 信息模型，统一权限三要素即主体、动作、约束；支持 JSON-LD 和 RDF Turtle 双序列化格式，确保跨平台解析；权限规则包含唯一标识符、签名验证字段、生效及失效时间戳。

互操作要求：资源绑定通过 CID 即 Content Identifier 实现 ODRL 策略与数据资源精准绑定；系统适配提供标准 REST API 供外部访问控制系统比如 XACML、OPA 调用；冲突检测提供策略兼容性校验接口，检测多源数据聚合场景下的规则冲突并输出解决方案。

2.3.2.2 DID：统一身份标识

DID（Decentralized Identifier），提供全球唯一、自主控制、可验证的身份标识，打破传统中心化身份系统的孤岛。

技术规范：遵循 W3C DID Core 规范，采用 did:method:specific-id 格式；DID 方法针对跨境数据流通场景定义专属方法，身份标识由区块链地址、机构编码、随机字符串组成；DID 文档包含公钥信息用于签名验证、可验证凭证包括学历、资质、授权证明、服务端点包括数据存储指针、API 入口；隐私保护支持零知识证明实现选择性披露比如证明年龄>18 而不透露具体年龄。

跨链互通：分布式解析网络集成多链轻客户端包括以太坊、联盟链 Fabric、FISCO BCOS，实现不同链上 DID 实时验证；VC 跨链背书可验证凭证经源链签名后，通过中继节点在目标链验证有效性；身份可移植用户可修改 DID 文档的服务端点，实现身份资产跨平台迁移。

2.3.2.3 智能合约：自动化执行载体

智能合约将数据使用规则即 ODRL 策略部署在区块链上，基于 DID 身份验证结果自动触发权限执行。

互操作标准：接口标准遵循 ERC-7683 跨链意图标准，定义统一跨链交互接口比如 crossChainCall、intentVerify；多语言兼容合约代码兼容 Solidity 即以太坊系、Rust 即 Polkadot、Solana、Go 即 Hyperledger Fabric；跨链协议支持哈希时间锁、中继链模式、公证人机制三种互操作架构；模块化设计拆分业务逻辑与跨链通信模块，通信模块兼容 Chainlink CCIP、LayerZero 等主流协议。

交易一致性：采用三阶段提交协议保障跨链交易原子性：1.准备阶段，锁定各链资源比如冻结代币、锁定数据访问权限；2.提交阶段，并行执行各链合约，收集执行结果；3.回滚阶段，若任一链执行失败，所有链回滚至初始状态。

2.3.2.4 信任闭环：ODRL+DID+智能合约

三者通过分层协同实现端到端互操作：基础层 DID 提供身份底座，为 ODRL 策略的主体和智能合约调用方提供可信标识；规则层 ODRL 将数据流通规则转化为机器可读策略，作为智能合约的执行依据；执行层智能合约自动解析 ODRL 策略，基于 DID 身份验证结果触发权限执行，通过跨链协议同步状态。

应用示例：跨境隐私计算场景

1.数据提供方即中国医院用 ODRL 定义使用权限：仅允许欧盟研究机构 A 用于癌症研究，计算期限至 2025 年底，禁止商业化

2.数据需求方即欧盟机构以 DID 身份发起隐私计算请求

3.智能合约验证：①身份合法性即 DID 解析确认机构 A 的研究资质②权限匹配度即请求的计算任务符合 ODRL 策略

4.验证通过后，合约自动授权访问加密数据，启动联邦学习任务

5.计算完成后，合约记录使用日志上链，扣除数据使用费，分配收益给数据提供方

全程可追溯、不可篡改，实现数据可用不可见、权限自动执行、收益公平分配。

2.3.3 隐私计算接口标准

隐私计算从可选技术演变为跨境数据合规的硬门槛，标准化是推动技术互操作和规模化应用的关键。

2.3.3.1 国家标准

GB/T 43697-2024 将隐私计算列为高敏感数据出境的必经环节。全国信安标委正在制定《隐私计算跨平台互通要求》，首次提出统一 API 语义，实现一次集成、多平台调用。

2.3.3.2 团体标准

T/CCSA 540-2025《隐私计算安全接口规范》由中国通信标准化协会发布，定义了 12 个原子接口：

接口类别	接口名称	功能描述	安全要求
任务管理	taskCreate	创建隐私计算任务	双向 mTLS 1.3 认证
任务管理	taskQuery	查询任务状态	国密 SM2 数字签名
任务管理	taskCancel	取消任务	会话密钥一次一密
数据管理	dataUpload	上传加密数据	端到端加密即 AES-256-GCM
数据管理	dataAuthorize	数据授权	ODRL 策略绑定
算法管理	algorithmRegister	注册计算算法	算法容器签名验证
算法管理	algorithmInvoke	调用算法	TEE 远程证明
结果管理	resultQuery	查询计算结果	差分隐私审核
结果管理	resultDownload	下载结果	访问控制+审计日志
安全审计	auditLog	获取审计日志	区块链存证
安全审计	complianceCheck	合规性检查	自动化规则引擎
性能监控	performanceMetric	获取性能指标	实时监控仪表板

安全要求：传输层强制双向 TLS 1.3，服务端和客户端均需提供数字证书；加密算法支持国密 SM2、SM3、SM4，满足商用密码应用要求；密钥管理会话密钥采用 ECDHE 生成，一次一密，用完即销毁；完整性所有请求、响应消息采用 HMAC-SHA256 或 SM3 进行签名；镜像安全算法容器镜像需签名即 Docker Content Trust，运行前验证签名；内存保护敏感计算在 TEE 包括 Intel SGX、AMD SEV、ARM TrustZone 中执行；可验证计算关键计算步骤提供零知识证明即 zk-SNARK，证明计算正确性而不泄露输入。

2.3.3.3 行业指南

北京国际大数据交易所《数据跨境隐私计算技术指南》量化最小可用数据集和重识别风险：最小可用数据集出境数据字段数≤原始字段总数的 5%，仅保留业务必需字段；重识别风险差分隐私参数 $\varepsilon \leqslant 1$ 即高隐私保护级别，确保单个数据主体信息无法被推断。

2.3.3.4 国际对接

中国隐私计算联盟与欧盟 GAIA-X、国际数据空间协会完成跨境数据空间互认白皮书，双方同意：技术互认接受 MPC 加区块链日志作为审计证据；标准对齐中国 T/CCSA 540 与欧盟 IDSA-RAM 即参考架构模型建立映射关系；试点先行深港跨境数据验证平台作为首个试点，验证互认机制可行性。

2.3.3.5 应用成效与挑战

成效：主流厂商包括蚂蚁链、微众银行、华控清交全面支持 T/CCSA 540 接口；深港征信互认平台日均 1200 次调用，零越权事件；北京、深圳数据交易所要求接入方必须通过接口合规认证；全链路加密加区块链存证，数据传输延迟增加<8%。

挑战：协议碎片化同态加密密文格式包括 CKKS、BGV、BFV 不互通，不同厂商产品无法直接对接；成本高中小企业一次性投入超 80 万元包括硬件设备、软件授权、技术集成，性能损耗 15-30%；标准滞后隐私计算技术快速迭代，标准更新周期慢国标 2-3 年，团标 1-2 年；监管时差国内合规评估周期 3-6 个月，欧盟 GDPR 充分性认定平均 18 个月，造成技术就绪、规则滞后。

2.3.3.6 发展趋势

统一认证信通院正牵头建立隐私计算 API 认证标志，目标 2026 年 Q2 将接入周期从 4 周缩至 1 周；量子安全金融与跨境结算场景将优先部署 QKD 即量子密钥分发加 PQC 即后量子密码混合加密，2027 年全面切换到 NIST 后量子标准；AI 自动化 2027 年推出 AI 合规引擎 SaaS 服务，提供 GDPR 到 PIPL 的实时条款映射，自动生成合规报告。

2.3.4 元数据与标识解析标准

元数据和标识解析是实现数据资源可发现、可理解、可定位的基础，是打破数据孤岛、建立跨境信任的前提。

2.3.4.1 元数据标准

元数据不仅是技术描述，更是承载法律、合规、安全、权属和溯源信息的核心载体。统一的元数据标准体系包括：

治理元数据涵盖主权与管辖、分类与分级、合规与授权、流通策略、安全基线等维度。主权与管辖明确数据原始属地、适用法律法规包括 GDPR、PIPL、CSL、控制者与处理者的法律实体归属；分类与分级界定敏感度定义为公开、内部、敏感、核心，明确个人信息标识符类型与级别；合规与授权标注数据收集的法律依据包括同意、合同必要、合法利益，说明同意的版本与范围、数据主体权利包括访问权、删除权的实现状态；流通策略规定允许的流通目的、可信接收方范围、数据出境审批状态、数据本地化要求、再传输限制，可指向数字合约标识符；安全基线明确访问或处理此数据所需的最低安全要求，比如必须在 TEE 中处理、必须采用 MPC。

描述元数据包含数据结构与模式、数据字典与词表、数据质量。数据结构与模式涵盖表名、字段定义、数据类型包括 JSON、XML、Parquet、关系约束；数据字典与词表建立跨行业、跨语言的公共词汇表和本体，解决语义鸿沟；数据质量包含完整性、准确性、时效性、一致性评分。

溯源与权属元数据涉及权属发布方和数据血缘。权属发布方为注册该数据产品的合法实体 DID；数据血缘包括依赖关系即数据集之间的衍生关系、处理历史即标准化记录数据从产生、采集、清洗、加工、隐私计算到跨境传输的每一步操作者、时间、算法和地点。

标准化要求明确：采用 DCAT 2.0 即 Data Catalog Vocabulary 描述数据集核心属性，该标准新增数据服务、关系、资源等类，以及访问服务、空间分辨率、时间分辨率等属性，进一步完善元数据描述维度；使用 Schema.org 提供 Web 友好的结构化元数据；支持多语言包括中文、英文、法语等和多编码包括 UTF-8。

2.3.4.2 标识解析体系

为每个数据产品分配全球唯一标识符，实现跨系统寻址和精准定位。

编码结构采用分层联邦式编码，格式为基础设施前缀、主权代码、数据空间标识、产品标识。其中基础设施前缀标识数据产品归属的顶层命名空间，是

国际互认的技术基础；主权代码明确原始注册地和司法管辖锚点，为联邦式解析提供路由依据；数据空间标识是数据所在空间的唯一标识；产品标识是空间分配的本地唯一编码，由数字、字母、连字符组成。

联邦式解析服务为保护数据主权采用联邦式架构：根解析即 Root Resolver 维护全球主权代码到解析节点的映射表，将解析请求路由至对应国家或地区的本地解析服务；本地解析即 Local Resolver 由各国家或地区自主运维，管理本辖区内的数据产品标识及元数据；跨域解析时，A 国节点需解析 B 国标识，根解析将请求路由至 B 国节点，B 国节点返回元数据或拒绝访问。

标准化接口包含注册、解析、检索三类，各类接口均需遵循统一的技术规范，确保跨系统调用的一致性和稳定性。

安全与合规要求：传输安全方面，所有 API 调用必须通过 TLS 1.3 与客户端证书认证；策略预检环节，解析服务在返回元数据前，检查请求方是否有权限访问，基于数字合约验证；审计日志方面，所有解析请求记录上链，包括请求方 DID、请求时间、标识符、响应状态。

2.3.4.3 互操作实践

Handle System 是国际通用的标识解析系统，支持 10^38 规模的标识空间，已用于 DOI 即数字对象标识符，能低成本实现与原有系统的无缝对接及不同应用系统间的互操作。与 DID 集成时，数据产品标识可绑定到 DID Document 的 service 端点，实现“身份→资产→元数据→访问接口”的完整链路。与区块链集成后，标识与元数据的绑定关系上链，确保不可篡改。此外，ISO/IEC 19941 标准定义的元数据映射矩阵，解决了不同司法管辖区确权要素的对应问题，提升跨境数据确权信息的转换准确率。

2.3.5 国际互认机制

国际互认机制通过技术手段建立跨境信任，使数据在不出境的前提下仍可被境外验证和调用，降低跨境数据流通的制度性交易成本。

2.3.5.1“数据桥”概念与实践

数据桥即 Data Bridge，是以区块链与分布式身份为底座、将各国监管规则转译成可自动执行的技术协议，实现“规则即代码、合规内嵌、可验证不可见”的跨境数据流通方案。

典型案例包括：英美数据桥于 2023 年 10 月生效，允许组织通过“欧盟-美国隐私框架的英国扩展”进行英美间数据自由流动，无需额外传输风险评估；中新海运电子提单试点在 2025 年完成，新加坡参与其中，基于区块链与 DID 技术，将纸质提单转为可验证凭证，全程无纸化，单据处理效率提升 60%，成本降低 30%；深港跨境数据验证平台基于国产区块链，将个人征信报告等敏感信息留在境内，仅向香港银行出示零知识证明即是否满足贷款资格，全程约 2 分钟；粤澳跨境数据验证平台在 2024 年建成，5 分钟内合规验证澳门居民在澳门的资产信息，用于境内银行快速审批信贷业务。

2.3.5.2 技术架构

数据桥采用五层架构：

1.数据准备层：在本地完成数据分级分类、脱敏、数字签名和时间戳，生成数据指纹即哈希值；

2.规则执行层：使用联盟链与公链混合平台，将监管规则写成智能合约，实现规则自动执行，规则需符合 GB/T 46068—2025 中“同等保护”原则，确保境外接收方保护水平不低于国内标准；

3.身份验证层：基于 DID 与可验证凭证，实现数据主体自主授权，对方“只验证、不触碰”明文；

4.密码学证明层：使用零知识证明、同态加密等技术，将合规证明转化为“可验证不可见”的数学证据；

5.应用接口层：封装为轻量化 SDK 与 API，直接插入 ERP、银行系统、港口系统等现有应用。

2.3.5.3 互认机制与流程

采用“1 份规则互认清单+2 套技术底座+3 步评估流程”的架构：

规则层由两地监管部门与行业协会共同发布“最低可接受数据要素与格式清单”，将需要互认的字段、脱敏粒度、哈希算法、零知识证明方式写入联合白皮书，形成“规则即代码”的互认基准。

技术层分为境内侧与跨境侧：境内侧采用国产开源联盟链比如 FISCO BCOS、长安链，对原始数据进行脱敏、哈希后生成数据指纹，签发可验证凭证即 VC；跨境侧通过跨链桥将 VC 摘要同步到境外节点，境外机构调用智能合

约验证凭证真伪，无需触碰原文。

治理层引入第三方审计节点和合规沙箱，对智能合约、加密强度、权限模型进行穿透式测试，通过后方可接入数据桥。

评估流程包含三步：1.授权申请，数据主体在境内平台发起“跨境验证”申请，一次性授权本地节点使用指定数据生成 VC；2.指纹跨境，平台仅将 VC 及其哈希值经加密通道推送到境外验证节点，原始数据留在境内；3.结果回写，境外机构调用智能合约完成校验后，将“评估通过/不通过”结果回写链上，双方监管节点同步存证，实现 1 分钟级互认。

2.3.5.4 应用成效

深港平台已完成 341 笔信用报告互认，香港银行凭数据指纹即可给内地企业放款；中新海运电子提单试点完成，被世界互联网大会评为 12 大精品案例之一；跨境融资领域，蚂蚁数科提供的“境内资产链+境外交易链+可信跨链桥”组合，已支持新能源电站完成约 1 亿元人民币跨境融资；成本效益方面，中小企业跨境数据合规成本降低 50%以上，审批时间从数周缩短至数天。类似欧盟-美国数据隐私框架机制，使跨区域数据传输合规成本降低约 40%，业务响应速度提升 60%以上。

2.3.5.5 挑战与展望

挑战主要体现在四个方面：

1.法律效力：技术互认的法律地位尚未明确，需要国际条约或双边协定背书，而当前各国数据法律体系差异显著，管辖权冲突突出；

2.标准碎片化：不同国家或地区的数据桥技术标准不统一，互联互通困难，且 ISO/IEC 23053 等国际标准尚未覆盖跨境场景下的元数据互认问题；

3.安全风险：跨链桥成为攻击目标，2022 年全球跨链桥被盗金额超 20 亿美元；

4.隐私保护：零知识证明等密码学技术复杂度高，可解释性差，公众信任建立需要时间。

展望包括四项方向：

1.多边机制：从双边数据桥走向区域性与全球性多边互认框架，比如 APEC 数据桥、“一带一路”数据桥；

2.标准统一：推动 ISO、ITU-T 等国际组织制定统一的跨境数据互认技术

标准，缓解标准碎片化问题；

3.监管沙箱：建立国际性的跨境数据流通监管沙箱，允许创新试点在可控范围内先行先试；

4.技术升级：引入后量子密码、可验证计算、联邦学习等新技术，提升安全性和隐私保护水平。

2.4 典型应用场景与案例

本节精选六个代表性案例，覆盖区域协同、金融、汽车、医疗、电商、隐私计算等领域，展示基础设施在不同场景的适配性与成效。

2.4.1 粤港澳大湾区：跨法域数据协同标杆

维度	内容
核心挑战	“一国两制”三关税区背景下，内地个人信息保护法与香港个人资料（私隐）条例存在法律差异，金融、医疗等重点领域数据流通受到限制
技术方案	大湾区标准合同机制结合深港数据验证平台，集成 MPC 与区块链存证技术
关键创新	①全国首个区域性标准合同机制，大幅简化数据出境审批流程；②通过 API 与沙箱技术实现“数据不动身份验证”模式，原始数据无需跨境传输
量化成效	数据出境申报时间从 45 天缩短至 15 天，降低 67%；每年服务港澳居民超 50 万人次；银行开户时间从 5 天压缩至 30 分钟；客户满意度达 92%
可复制性	该模式已推广至长三角沪苏浙地区、京津冀区域开展试点

2.4.1.1 制度创新

2023 年 12 月，香港创新科技及工业局与国家互联网信息办公室联合发布《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》，这是我国首个区域性跨境数据流动标准合同。

2.4.1.2 技术架构

深港数据验证平台采用三层架构。

1.数据源层，内地与香港各自维护本地数据库，涵盖征信报告、医疗记录等数据，实现数据物理隔离；

2.验证计算层，部署 MPC 节点，专门执行加密数据匹配和验证计算；

3.应用服务层，向银行、医院等机构提供标准化 API 接口，支撑业务场景落地。

2.4.1.3 应用场景

1.跨境金融服务，港澳居民在内地银行开户时，通过 API 调用香港征信系统验证身份和资产信息，全程无需传输明文数据；

2.跨境医疗服务，港澳居民在内地就医产生的电子病历，通过医疗数据沙箱回传香港医疗机构，为后续治疗提供支持。

2.4.1.4 关键经验

1.制度先行，标准合同机制有效降低跨境数据流通的制度性交易成本；

2.技术赋能，MPC 等隐私计算技术破解“数据可用不可见”的核心难题；

3.平台支撑，一站式服务平台显著提升用户体验和业务办理效率；

4.协同治理：粤港澳三地监管部门建立常态化沟通机制，保障数据流通合规有序。

2.4.2 跨境金融：mBridge 多边央行数字货币桥

维度	内容
核心挑战	传统跨境支付存在结算周期长、手续费高、过度依赖 SWIFT 网络、外汇管制流程复杂等问题
技术方案	基于分布式账本技术、智能合约与多央行数字货币互联架构，依托 Corda 平台搭建
关键创新	实现支付即结算模式、去中介化交易、7×24 小时不间断运行、跨境汇兑自动化处理
量化成效	交易时间从 3-5 天缩短至秒级；交易成本降低 50%以上；截至 2024 年已完成跨境贸易结算 22 亿美元
产业影响	推动全球 30 余家央行加入央行数字货币研发；2024 年被国际清算银行创新中心列为最成功试点项目

2.4.2.1 项目背景

mBridge 由中国人民银行数字货币研究所、香港金融管理局、泰国中央银行、阿联酋中央银行联合发起，是全球领先的跨境央行数字货币平台。

2.4.2.2 技术特点

1.基于 R3 Corda 企业级区块链，同时支持 UTXO 模型和状态机模型；

2.采用拜占庭容错共识算法，交易确认时间小于 10 秒；

3.支持多币种智能合约，涵盖人民币、港币、泰铢、阿联酋迪拉姆，可自动完成汇兑操作；

4.隐私保护方面，采用选择性披露技术，交易方信息仅对相关节点可见。

2.4.2.3 应用场景

1.跨境贸易结算：出口商发货后，通过 mBridge 平台即时收款，无需等待传统银行汇款周期；

2.供应链金融：核心企业凭借电子仓单在平台申请融资，资金可实现秒级到账；

3.跨境投资：机构投资者通过平台直接购买海外资产，实现券款兑付。

2.4.2.4 成效数据

1.参与机构：4 家央行及 20 家商业银行；

2.交易规模：2023 年试运行期间完成 160 笔交易，累计金额 22 亿美元；

3.成本优势：传统跨境汇款手续费为 3-5%，mBridge 手续费低于 0.5%；

4.时间优势：传统电汇为 T+3 模式，mBridge 实现 T+0 实时到账。

2.4.3 智能汽车：中国汽车行业跨境数据空间

维度	内容
核心挑战	单辆车日均产生 4TB 数据，包含位置、影像等敏感信息；车企全球研发协同需求强烈，数据跨境流通合规压力大
技术方案	可信数据空间 TDS 结合联邦学习与本地化数据中心，由中汽科技与华为云联合共建
关键创新	①采用“可用不可见”联合建模模式，原始数据不出境；②搭建一站式合规申报平台，可自动生成数据出境评估报告
量化成效	研发周期缩短 40%；算法性能提升 15%；合规风险降至零；已服务 10 余家头部车企

维度	内容
行业地位	中国首个汽车行业跨境数据空间，入选工信部《车联网数据安全典型案例》

2.4.3.1 项目背景

2025 年 8 月，中汽科技上海与华为云签署战略合作协议，共同搭建中国汽车行业跨境数据空间，为车企提供合规、高效的跨境数据协同服务。

2.4.3.2 技术架构

1.数据本地化，在中国、德国、美国等地部署本地数据中心，车辆数据就近存储，满足数据本地化要求；

2.联邦学习平台：各地数据中心部署联邦学习节点，仅交换模型参数梯度，不传输原始数据；

3.合规管理平台：实现数据分类分级自动化、出境风险评估智能化、申报材料生成数字化；

4.API 网关：提供标准化接口，支持 ERP、PLM 等企业现有系统无缝对接。

2.4.3.3 应用案例

案例 1：全球协同研发某头部车企在中国、德国、美国设有研发中心，需共享自动驾驶算法训练数据。

传统方式：将中国路测数据传输至德国总部，面临 6 个月数据出境审批周期、数据泄露风险及高昂传输成本；

TDS 方式：采用联邦学习技术，各地数据留存本地，仅交换加密梯度参数，在 TDS 平台完成聚合训练；

成效：研发周期从 18 个月缩短至 11 个月，降低 40%；mAP 指标从 0.82 提升至 0.94，算法性能提升 15%；全程零合规风险。

案例 2：高精地图跨境协作境外采集的高精地图数据需回传境内处理。

技术方案：在境外部署边缘脱敏节点，对政府机关、军事设施等敏感地理信息自动进行模糊化处理，脱敏后数据通过专用通道回传，在 TDS 中完成地图构建；

成效：地图更新频率从季度更新提升至月度更新，效率提升 3 倍；敏感信息泄露风险为零；数据传输成本降低 50%。

2.4.4 医疗行业：COLOR IV 国际多中心临床研究

维度	内容
核心挑战	患者病历跨境共享需同时满足隐私保护与伦理审查要求，国际合作流程复杂、难度大
技术方案	医疗数据沙箱结合同态加密、VPN 专网与动态脱敏技术，由北京友谊医院牵头搭建
关键创新	首个通过《数据出境安全评估办法》的医疗项目，构建“事前评估-事中监控-事后审计”全流程闭环管理
量化成效	中欧 10 家机构实现协同研究；单据处理效率提升 60%；综合成本降低 30%；累计涉及患者数据超 1000 万例次
合规认证	通过国家网信办数据出境安全评估与医院伦理委员会双备案，全程零数据泄露事件

2.4.4.1 项目背景

“COLOR IV 国际多中心临床研究”由北京友谊医院牵头，联合荷兰阿姆斯特丹医学中心等多个中欧医疗机构共同开展，需跨境共享大量患者病历、影像、检验报告等数据。

2.4.4.2 技术架构

1.医疗数据沙箱：提供受控数据分析环境，境外研究人员可在沙箱内对脱敏数据进行统计分析和 AI 建模，但无法下载原始数据；

2.同态加密：基因序列、诊疗方案等敏感数据采用同态加密技术，在加密状态下完成联合分析；

3.VPN 专网：建立中欧医疗专用网络，采用 IPsec 加密技术，保障数据传输安全；

4.动态脱敏：数据在沙箱内访问时实时脱敏，例如将姓名替换为唯一 ID、出生日期仅显示年份。

2.4.4.3 合规流程

1.事前评估：完成个人信息出境安全评估申报，评估内容包括数据出境合法性、境外接收方安全能力、双方合同义务等；

2.事中监控：实时监测数据访问行为，对批量下载、越权访问等异常操作自动告警并阻断；

3.事后审计：全流程操作日志上链存证，定期向监管部门提交审计报告。

2.4.4.4 成效数据

1.研究规模：覆盖 10 家医疗机构，涉及 1000 万以上患者数据；

2.效率提升：病历数据处理时间从 2-3 天缩短至 1 天内，效率提升 60%；

3.成本降低：无需人工跨境邮寄纸质病历，综合成本节省 30%；

4.科研成果：联合发表 SCI 论文 15 篇，成功发现 3 个新的致病基因。

2.4.5 跨境电商：贸链智综综合服务平台

维度	内容
核心挑战	中小企业面临报关流程复杂、税费计算繁琐、物流信息碎片化、融资难度大等多重痛点
技术方案	数据湖结合 API 网关与 AI 智能决策系统，整合海关、税务、物流、金融等多源数据
关键创新	①一站式整合多源数据，智能报关准确率达 99%；②基于交易数据提供信用贷款服务，破解中小企业融资难题
量化成效	服务企业超 5000 家；报关效率提升 70%；通关时间控制在 4 小时以内；运营成本降低 30%；年交易额突破 500 亿元
生态价值	降低中小企业国际贸易门槛，助力“专精特新”企业出海拓展市场

2.4.5.1 平台定位

为中小跨境电商企业提供一站式数字化、智能化综合服务，降低国际贸易参与门槛，提升业务运营效率。

2.4.5.2 核心功能

1.多源数据整合

海关数据：涵盖进出口申报、通关状态、检验检疫等信息；

税务数据：包括出口退税、跨境税收、增值税发票等内容；

物流数据：覆盖国际运输、仓储配送、快递追踪等环节；

金融数据：包含跨境支付、外汇结算、信用评估等服务；

市场数据：提供需求分析、竞品情报、汇率走势等资讯。

2.智能服务能力

智能报关：自动生成商品编码、原产地证明、装箱清单等报关单据，人工审核时间从 2 小时缩短至 10 分钟；

税费计算：实时计算关税、增值税、消费税，支持 200 多个国家和地区税制；

物流优化：基于 AI 算法推荐最优物流方案，综合考量时效、成本、可靠性等因素；

风险预警：精准识别汇率波动、政策变化、合规风险等潜在贸易风险；

融资服务：基于交易数据提供信用贷款，包括出口订单融资、应收账款保理等产品。

2.4.5.3 技术架构

1.数据湖：汇聚海关、税务、物流、金融等多源异构数据，支持 PB 级数据存储；

2.API 网关：提供 200 多个标准化接口，支持 ERP、WMS 等企业系统对接；

3.AI 决策引擎：基于机器学习模型实现智能报关、物流优化、风险预警等功能；

4.区块链存证：交易记录、电子合同、物流凭证等信息上链存储，确保不可篡改。

2.4.5.4 成效数据

1.服务企业：5000 多家中小跨境电商企业；

2.报关效率：从人工操作 2 小时缩短至智能处理 10 分钟，效率提升 70%；

3.通关时间：从平均 2 天压缩至 4 小时内，缩短 75%；

4.运营成本：企业综合运营成本降低 30%；

5.交易规模：平台年交易额突破 500 亿元。

2.4.6 隐私计算：欧数中算跨境科研平台

维度	内容
核心挑战	中俄医疗数据跨境科研需满足双方数据主权要求，敏感病例数据无法直接共享
技术方案	同态加密结合密文计算引擎与超算中心，由同态科技提供技术支撑
关键创新	①数据加密后再跨境传输，全程开展密态计算，仅对最终结果进行解密；②集成国产密码算法与高性能同态加密技术，支持 PB 级数据处理
量化成效	完成 11345301 例病例分析；开展 214 种药物风险评估；结果共享效率提升 60%；全程零数据泄露
技术突破	成功攻克同态加密性能瓶颈，计算效率提升 10 倍以上

2.4.6.1 项目背景

“欧数中算”平台面向“一带一路”沿线国家，为中俄科技企业、研究院校提供跨境数据协同计算服务。平台内置“密文计算引擎”，基于高性能同态加密技术，保障数据在跨境计算过程中的可用性、安全性和保密性。

2.4.6.2 技术架构

1.密文计算引擎：基于 CKKS、BGV 等同态加密方案，支持加减乘运算和多项式近似计算；

2.超算中心：部署在中国西北部，配备 100 多个 GPU 节点，提供高性能计算资源；

3.数据托管服务：境外数据加密后托管在平台，密钥由数据所有方自主掌控；

4.订阅式服务：境外机构可按月份、按功能订阅平台密文计算服务。

2.4.6.3 应用案例：医疗健康领域

1.数据规模：

三类病例数据，总计 11345301 例；

涉及 9 种药品，开展 214 种药物风险评估。

2.协作流程：

俄方通过租用同态计算设备和订阅平台服务，完成原始数据加密处理；

加密数据传输至中国西北部超算中心；

平台调用密文计算服务，对加密数据开展药物风险性与治愈率的差异性研究；

仅对最终检验和分析结果进行解密确认，全程不触碰原始数据。

3.成效

计算效率：密文计算性能达到明文计算的 60%，处于业界领先水平；

结果共享：跨境对照性实验的结果共享效率提升 60%；

安全性：全程零数据泄露，满足中俄双方数据主权要求；

成本：计算成本仅为传统多方安全计算的三分之一。

4.技术亮点

轻改造：对原有业务流程和 IT 基础设施；

高性能：国产密码算法优化，同态加密计算效率提升 10 倍以上；

可复用：数据资产可复用，一份加密数据支持多个需求方使用；

国产化：核心模块全部国产自研，安全可控。

2.4.7 案例对比分析

场景	数据敏感度	合规复杂度	核心技术	成熟度	经济效益	适用行业
大湾区协同	高	极高	标准合同+MPC	试点推广	时间成本-67%	金融、医疗、政务
跨境金融	极高	极高	DLT+智能合约	成熟应用	交易成本-50%	金融、贸易结算
智能汽车	高	高	TDS+联邦学习	快速发展	研发周期-40%	汽车、制造、物联网
医疗科	极高	极高	沙箱+同态加	探索试点	处理效率	医疗、生命科

场景	数据敏感度	合规复杂度	核心技术	成熟度	经济效益	适用行业
研			密		+60%	学
跨境电商	中	中	数据湖+API	成熟应用	运营成本-30%	电商、物流、贸易
隐私计算	高	高	密态计算	技术突破	结果共享+60%	科研、金融、医疗

共性经验总结：

1.制度创新先行：所有成功案例都离不开制度层面的突破，例如大湾区标准合同、mBridge 央行协作机制、医疗数据出境评估；

2.技术赋能合规：隐私计算、区块链、可信数据空间等新技术是实现“数据可用不可见”的关键；

3.平台化降门槛：一站式服务平台显著降低企业合规成本和技术门槛，例如贸链智综、汽车数据空间；

4.标准化促互通：数据格式、接口协议、安全标准的统一至关重要，例如医疗 HL7 FHIR 标准、金融 ISO 20022 标准；

5.生态协同共建：需要政府、企业、技术服务商、行业组织多方协同，政府提供政策支持，企业积极实践，技术商提供解决方案，行业组织推动标准。

2.5 管理与运营体系

数据基础设施的长期稳定运行需要系统化、规范化、可持续化的管理与运营体系。本节从组织架构、运行保障、绩效评估三个维度阐述管理与运营的最佳实践。

2.5.1 组织管理架构

2.5.1.1 设计原则

1.集中决策与分散执行相结合：重大政策、技术标准、安全策略由高级别管理委员会集中决策，具体业务执行由业务单元分散负责；

2.合规优先原则贯穿始终：设立独立、专职的合规及法律事务部门，深度参与数据跨境传输的流程设计、合同审查、风险研判。

2.5.1.2 建议架构

组织层级	核心机构	主要职责	汇报关系
决策层	数据治理委员会	制定数据跨境流通总体战略、安全政策和技术标准；审批重大数据出境项目；协调跨部门资源	向董事会/CEO 汇报
管理层	数据合规办公室	日常合规管理，包括数据分类分级、安全评估申报、标准合同签订、隐私保护认证；对接监管机构	向数据治理委员会汇报
执行层	数据基础设施运营中心	跨境数据通道、可信数据空间、数据中心等基础设施的建设、运行和维护；实施安全技术措施	向 CTO/CIO 汇报
监督层	内部审计与风险控制部门	定期对数据跨境流通的流程、技术和合规性进行独立审计和风险评估；监督安全事件响应	向审计委员会汇报

2.5.1.3 跨部门协同机制

1.联席会议：每月召开数据治理委员会会议，讨论重大事项；

2.项目组：针对大型跨境数据项目，组建跨部门项目组，涵盖合规、技术、业务、法务相关人员；

3.应急响应：建立 7×24 小时应急响应机制，快速处置数据安全事件。

2.5.2 运行与安全保障

2.5.2.1 数据全生命周期安全管理

1.数据分类分级

依据 GB/T 43697-2024、行业标准和业务特点，对涉及出境的数据进行分类和定级，分类包括个人信息、重要数据、一般数据，定级分为核心、重要、一般；

不同级别实施差异化安全策略：核心数据原则上不出境，重要数据出境需安全评估，一般数据出境简化流程。

2.数据出境风险评估

建立制度化、常态化的评估流程，评估内容包括合法性、正当性、必要性、安全性；

合法性评估重点关注是否为法律未禁止出境的数据、是否取得个人单独同意、境外接收方是否达到同等保护水平；

正当性评估聚焦数据出境的业务目的是否正当、是否有替代方案；

必要性评估核查出境数据范围是否最小、出境频率是否合理；

安全性评估确认双方安全保障能力和合同义务是否充分。

3.数据本地化与脱敏策略

敏感或关键数据优先在境内存储和处理；

确需出境的数据采用脱敏处理，包括匿名化、假名化、数据聚合等方式，降低泄露风险。

2.5.2.2 技术保障机制

1.可信数据空间

应用隐私计算、联邦学习、安全多方计算等技术，实现“数据可用不可见”；

在沙箱环境中提供受控的数据分析能力，原始数据不导出。

2.安全通道与加密传输

采用高强度加密算法和专用网络通道，加密算法包括 TLS 1.3、国密 SM2、国密 SM4，专用网络通道涵盖跨境 VPN、SD-WAN；

确保数据在传输过程中的机密性、完整性、可用性。

3.安全监测与审计追踪

建立 7×24 小时安全运营中心 SOC，实时监控跨境数据流动状态、用户访问行为、异常事件；

全流程日志记录操作者、时间、数据集、操作类型、结果等信息并定期审计；

日志加密存储且不可篡改，采用区块链锚定方式，保存期限一般不低于 6 个月，敏感数据保存期限不低于 3 年。

2.5.3 绩效与评估体系

2.5.3.1 效率维度

估指标	衡量标准	目标导向
数据出境审批时长	从提交申请到获得批准的平均时间	缩短至 30 个工作日内，提升业务响应速度
数据传输成功率	跨境数据传输任务的成功比例	≥99.5%，确保基础设施可靠性
系统可用性	基础设施年度可用率	≥99.9%（三个九），支持 7×24 业务连续性
业务创新支持度	基于跨境数据流通实现的新业务或新产品数量 衡	衡量基础设施对业务增长的贡献

2.5.3.2 安全维度

评估指标	衡量标准	目标导向
安全事件发生率	每年发生的跨境数据安全事件数量和严重程度	零重大安全事件，包括数据泄露、篡改、丢失
安全漏洞修复时长	从发现安全漏洞到完成修复的平均时间	高危漏洞≤24 小时，中危≤7 天，低危≤30 天
合规审计通过率	内部和外部合规审计的通过情况	100%通过率，确保安全措施有效性
应急响应时效	从安全事件发生到启动应急响应的时间	≤30 分钟，快速处置降低影响

2.5.3.3 合规维度

1.法规政策遵循度

定期组织对国内外数据保护法律法规符合性评审，包括 PIPL、DSL、GDPR 等；确保基础设施及操作流程持续满足监管要求。

2.合规成本分析

全面统计为实现数据跨境合规所投入的成本，包括技术改造、专用设备、人员、罚款等方面；通过成本效益分析推动流程优化与资源合理配置。

3.员工培训与意识提升

确保参与跨境数据操作的全体员工接受定期且具针对性的合规与安全培训；通过考核检验培训成效，持续提升数据安全意识与操作规范水平。

2.5.3.4 评估方法

1.定期评估：每季度进行一次综合评估，生成绩效报告；

2.专项评估：针对重大项目或安全事件进行专项评估；

3.第三方评估：每年委托第三方机构进行独立评估，如审计公司、测评机构。

2.5.3.5 持续改进机制

1.建立 PDCA 闭环，即规划→执行→检查→改进；

2.对评估中发现的问题，制定整改计划并跟踪落实；

3.定期总结最佳实践，形成标准化流程和制度。

2.5.4 本章小结

本章系统阐述了跨境数据流通基础设施的构建理念、技术实现与实践经验，主要结论如下：

1.架构设计：四层架构基础安全、治理合规、互联互通、业务应用为跨境数据流通提供了系统化解决方案。各层职责明确、接口标准化，实现了技术能力与治理要求的深度融合。

2.核心技术：六大核心组件身份认证、目录管理、数字合约、隐私计算、加密传输、审计追溯协同工作，支撑数据全生命周期安全流转。其中，隐私计算技术是实现“数据可用不可见”的关键，区块链技术为审计追溯提供了可信支撑。

3.标准体系：国内外标准体系持续完善，GB/T 46068-2025 的发布标志着中国数据跨境标准进入新阶段。数字合约、隐私计算、元数据等领域的互操作规范逐步建立，为跨境数据流通提供了技术基础。

4.实践经验：六个典型案例展示了基础设施在不同场景的应用成效：

- 粤港澳大湾区：跨法域协同标杆，出境审批时间缩短 67%；

- mBridge：跨境支付变革，交易成本降低 50%以上；
- 汽车数据空间：智能制造协同，研发周期缩短 40%；
- 医疗科研：隐私保护典范，处理效率提升 60%；
- 跨境电商：为中小企业赋能，运营成本降低 30%；
- 隐私计算：技术突破，结果共享效率提升 60%。

5.管理运营：完善的管理与运营体系是基础设施长期稳定运行的保障。需建立“决策-管理-执行-监督”四层组织架构，实施数据全生命周期安全管理，建立“效率-安全-合规”三维绩效评估体系。

6.发展趋势：

- 技术融合：隐私计算、区块链、AI 等技术深度融合，提升数据流通效率与安全性；
- 标准统一：国际标准互认加速，降低跨境合规成本；
- 平台化：一站式服务平台降低技术门槛，促进中小企业数字化转型；
- 生态化：政府、企业、技术服务商、行业组织多方协同，共建数据要素市场。

第三章 稳定币及货币结算体系变革引发的数据跨境规则变化

在数据跨境流动从“能流”走向“好用”的临界点，技术底座与制度框架已基本就绪，但“价值如何结算、信任如何传递”的新命题随之浮出水面。第二章勾勒的“可信数据空间”解决了数据“可用不可见”，却仍未回答另一关键问题：当数据要素与加密资产、模型参数、算力凭证等新型资产在同一跨境链路中实时交换时，该用何种结算媒介才能兼顾效率、合规与主权？传统代理行网络的高成本、长链条与货币割裂，使得“数据流”与“资金流”始终难以同频。正是这一缺口，催生了稳定币的规模化应用与央行数字货币的加速试验——它们不仅重塑支付底层，更把“结算即合规、转账即审计”的可编程能力嵌入跨境数据生命周期。第三章将镜头对准这场“货币结算革命”，剖析美欧新港多极监管如何围绕储备资产、赎回权、反洗钱规则展开博弈，解读中国“数字人民币+香港合规稳定币”双轨模式如何为数据要素定价、结算、分账提供主权级信任底座，并探讨当智能合约把支付条款与数据交付状态实时绑定后，“数据流—资金流—合规流”三流合一的新范式将如何重新定义跨境数据生意的结算逻辑与风险边界。

3.1 货币结算规则的新趋势

3.1.1 全球稳定币监管框架成型，合规化成为核心共识

3.1.1.1 国际政策协同治理加速

1.全球主要经济体密集出台监管规则

美国总统特朗普于当地时间 2025 年 7 月 18 日，签署《指导与建立美国稳定币国家创新法案》（GENIUS 法案），标志着全球首个联邦层面的稳定币监管框架正式确立，成为稳定币发展史上里程碑的事件。与此同时，各国纷纷跟进，加密金融资产有望从“边缘性实验”迈入主流金融体系。GENIUS 法案要求美元稳定币发行商持有 100%美元或美国国债等储备资产，通过绑定私人稳定币强化“美元数字化”影响力[1]；欧盟《MiCA 法案》进入全面实施阶段，建立统一的稳定币准入与运营标准[2]；香港《稳定币条例》于 2025 年 8 月生

[1] 美国国会网：https://www.congress.gov/search?q=%7B%22search%22%3A%22GENIUS+Act%22%7D.

[2] LexisNexis Legal & Professional：https://www.lw.com/en/markets-in-crypto-assets-regulation-tracker/mica-all-

效，设立发牌制度，要求发行人实现客户资产隔离与合规赎回机制[3]；英国金融行为监管局（FCA）于 2025 年 5 月发布监管提案，明确稳定币储备资产披露与价值维持要求，将 KYC/AML 规则全面覆盖虚拟资产服务提供商（VASP），形成“相同风险相同监管”的国际共识。[4]

2.监管与创新的平衡探索

IMF 指出稳定币去中心化特性带来洗钱与制裁规避风险，各国普遍采用“监管沙盒”模式试点，如香港金管局“Ensemble 沙盒”、上海临港新片区封闭测试区；多边央行数字货币桥（mBridge）项目从 BIS 创新中心“毕业”，由中、港、泰、阿联酋四地央行自主推进，实现跨境数字货币结算效率提升 50%以上，成为监管协同与技术创新结合的典范。[5]

3.区域监管差异与协作

新加坡明确稳定币收益需缴纳资本利得税，而马来西亚尚未出台相关政策，导致跨境投资者面临税务合规风险，推动东盟国家签署《稳定币监管合作备忘录》，明确域外效力适用范围以降低合规成本。

3.1.1.2 市场结构呈现两极分化

1.稳定币成为跨境结算主力

2025 年全球稳定币总市值突破 2900 亿美元，2024 年年化交易额达 27.6 万亿美元，超过 Visa 与 Mastercard 之和，越南-迪拜-巴西等跨区域贸易中，稳定币实现秒级到账，摆脱 Swift 与结售汇限制6；国际清算银行（BIS）指出，稳定币在新兴市场成为美元获取渠道，在阿根廷、土耳其等通胀高企国家的跨境支付占比已达 15%-20%。[7]

2.美元稳定币主导与多极化突破

美元稳定币占全球 99%以上份额，但人民币稳定币也加速崛起，如京东通过“京链通”稳定币接入 CIPS 系统完成一笔跨境电商订单结算时，系统显示

---

texts.

[3] 香港政府新闻网：trae.com.cn/?utm_source=doubao&utm_medium=bookmark&_enter_from=new_home_page.

[4] Financial Stability Board：https://www.fsb.org/publications/.

[5] IMF：https://www.imf.org/en/Publications/GFSR.

[6] Chainalysis：https://www.chainalysis.com/blog/introducing-sentinel-token-compliance/.

[7] BIS：https://www.bis.org/publ/bppdf/bispap159.htm.

的 10 秒到账时间与 90%的成本降幅，实现港元、数字人民币跨链兑换[8]，同时也标志着传统货币结算体系正在悄然发生变革[9]；中国正联合东盟国家共建区块链跨境支付基础设施，推动人民币稳定币在东南亚农产品贸易中试点应用。

3.1.2 中国政策双轨驱动，数据与结算基础设施深度融合

3.1.2.1 本币结算与稳定币试点双向发力

1.跨境人民币结算政策升级

中国通过银行激励机制推动国企、大宗商品贸易优先使用本币结算，2025 年一季度数字人民币跨境结算规模同比增长 120%；中伊石油贸易中，昆仑银行通过 CIPS 系统承接 90%人民币结算量，2025 年一季度能源结算同比增长 60%。[10]

2.区域试点形成协同效应

数字人民币国际运营中心落地上海，上海提出“稳定币实时结算+数币最终清算”双轨模式，在临港新片区探索离岸人民币稳定币，联动香港持牌机构发行合规稳定币；香港作为枢纽承接大陆试点延伸，京东币链科技进入香港金管局沙盒第二阶段测试，覆盖跨境支付、RWA 等场景；粤港澳大湾区试点“跨境结算税务协同机制”，实现稳定币交易涉税数据与海关、银行系统实时同步，合规审核效率提升 60%。

3.1.2.2“三流融合”的实践创新

1.数据流驱动结算效率革命

保税科技清算通平台通过联盟链绑定数字人民币钱包，将物联网设备采集的物流数据（如储罐液位）与资金流实时上链，根据行业分析及第三方平台信息，保税科技清算通平台 2024 年清算金额突破 2 万亿元，数字人民币结算占比超 60%，并通过联盟链与物联网技术实现秒级 DVP 结算；厦门国际银行联合澳门国际银行，依托香港 CMU 数字化债券平台，实现珠海华发集团 14 亿元人民币公募债券的全流程上链发行与结算，发行文件审核时间从 15 天压缩

[8] 网易新闻：https://c.m.163.com/news/a/K564CTDJ0511V6QH.html.
[9] https://finance.ifeng.com/c/8kLVVaDztt6#:~:text 刘强东宣布，京东将推出稳定币。
[10] 昆仑银行：https://www.klb.cn/eportal/fileDir/kunlbank/resource/cms/2025/04/2025041011021091306.pdf.

至 2 天[11]。

2.生态协同构建结算闭环

京东与天阳科技联合开发跨境 B2B 结算系统，依托香港《稳定币条例》合规框架及技术标准，实现京东“京链通”稳定币与数字人民币的跨链兑换，并接入人民币跨境支付系统（CIPS）。该系统采用天阳科技自主研发的 FINNOSafe 跨境支付底层技术——其已通过香港金管局“数字货币桥”沙盒测试，支持亚秒级交易确认与合规化清算，实际运营中可将跨境结算手续费较传统 SWIFT 模式降低 60%，到账时间从传统的 1-3 个工作日压缩至 30 秒以内。目前该系统已在东南亚跨境电商试点中落地，依托区块链的不可篡改性与智能合约自动化处理能力，有效适配跨境贸易中的实时清算需求[12]。

3.1.3 技术重构结算底层逻辑，跨境基础设施迭代升级

3.1.3.1 区块链与数字技术深度渗透

1.智能合约实现自动化合规

预授权冻结合约在交易达成后自动锁定资金，待物流数据确认后触发划转，如海南国际能源交易中心通过该技术实现原油跨境结算从 3 天到实时的突破；量子加密与 AI 风控结合，保税科技平台异常交易拦截率超 99%，交易成功率达 99.99%；厦门数字化债券项目通过智能合约自动执行付息兑付条款，避免传统债券结算中的延期风险[13]。

2.跨体系互联互通加速

FINNOSafe 跨境支付系统通过香港金管局测试，交易确认达亚秒级，实现 CIPS 与香港稳定币体系直连；华为与金融机构合作开发可信 ICT 底座，支撑中东银行接入数字人民币跨境系统；多边央行数字货币桥（mBridge）实现四种法定数字货币的原子互换，跨境清算成本降低 40%以上。

---

[11] 香港金融管理局：https://www.hkma.gov.hk/gb_chi/key-functions/international-financial-centre/financial-market-infrastructure/debt-securities-settlement-system/.
[12] 东方财富证券：https://guba.eastmoney.com/news,gssz,1568904652.html?jumph5=1.
[13] 东方财富网：https://caifuhao.eastmoney.com/news/1559014791.

3.1.3.2 数据要素赋能结算生态

1.数据资产化反哺风控

清算通平台沉淀 10 万+企业交易数据，开发“仓融通”模型评估偿债能力，坏账率控制在 0.3%以内，数据服务年收入达 5800 万元；香港金管局依托“商业数据通”系统，整合企业跨境交易流水与海关数据，为稳定币发行人提供动态准备金监测服务，储备资产透明度提升 80%[14]。

2.绿色金融场景创新

数字人民币与碳配额通证化结合，企业通过质押碳资产获取贷款，2024 年相关业务规模增长 37 倍[15]；广东能源集团在中泰光伏项目中，采用“数字人民币结算+碳足迹上链”模式，实现跨境能源交易与碳减排数据的同步验证，获得欧盟碳关税减免优惠。

3.技术局限与优化方向

国际清算银行（BIS）指出，稳定币在单一性、弹性和完整性测试中表现不足，如不同发行方的美元稳定币存在汇率差异，且缺乏央行最终结算保障。对此，中国正在研发基于统一账本的央行数字货币结算系统，计划 2026 年实现数字人民币与稳定币的底层账户互通。

3.2 境外司法辖区稳定币监管框架与典型实践探析

3.2.1 美国稳定币的监管框架与实施范例

美国对稳定币的监管经历了从法律定性模糊到逐步清晰的过程。学界和业界曾对其性质存在多种观点，包括将其归入货币市场基金、活期存款账户或证券进行监管。[16]《GENIUS 法案》的通过标志着美国在联邦层面为“支付型稳定币”确立了统一的法律地位和监管框架。

3.2.1.1 美国关于稳定币的法律界定与监管架构

《GENIUS 法案》将“支付型稳定币”界定为具备价值支撑、采用电子化转移方式、基于分布式账本技术、被公众接受为支付/偿债/投资工具，并能作为

[14] 香港金融管理局：https://www.hkma.gov.hk/gb_chi/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/.
[15] 广州市地方金融管理局：https://jrjgj.gz.gov.cn/gzdt/content/post_10017396.html.
[16] 参见张阳：《论稳定币本土发展的规范逻辑》，载《交大法学》2025 年第 5 期，第 124 页。

计算单位或价值存储载体的数字通证。[17]该法案确立了联邦与州的双轨制监管架构：对规模巨大或具有系统重要性的发行方，由联邦机构（如货币监理署 OCC）实施统一监管；同时允许各州在符合联邦底线标准的前提下，为规模较小的发行方提供灵活的监管路径，以鼓励创新并保持竞争力。

在核心监管要求方面，美国框架强调通过多重机制保障稳定币系统的稳健运行。其中最为关键的是储备资产刚性兑付要求，法案强制规定稳定币必须以 1:1 的比例由高质量流动性资产全额支撑，主要包括美元现金、短期美国国债及已投保的银行活期存款。[18]这种“链上货币市场基金”的模式形成了“美元-稳定币-美债”的资金循环。[19]同时，发行主体必须持牌经营，接受严格的资本充足率和流动性管理要求，并被限制业务范围以防演变为“影子银行”。为确保消费者权益，法律还明确规定持有人享有按面值随时赎回的法定权利，且在发行方破产时享有优先受偿权，这些规定共同构建了防范挤兑风险的制度防线。

3.2.1.2 美国稳定币的实施范例与在数据跨境结算中的应用

在明确的监管规则下，美国的稳定币市场形成了以 USDC、USDT 等为主导的格局，并在跨境支付与数据服务结算中展现出应用潜力。

1.典型实施范例：USDC 的运行机制

由 Circle 公司发行并受纽约州金融服务局监管的 USDC 是合规稳定币的典型代表。其采用 1:1 全额美元资产抵押发行模式，即每发行 1 枚 USDC，Circle 公司即在银行存入等额美元或购买等值短期美债作为储备。该公司每月公开由独立审计机构出具的储备报告，确保了较高的透明度。这种“链上货币市场基金”的模式，形成了“美元-稳定币-美债”的资金循环，不仅为美债市场引入了新的需求，也为稳定币本身提供了坚实的信用基础。

2.在数据跨境结算中的应用潜力

在数据跨境结算领域，稳定币的技术特性使其与数据流通场景高度契合。其基于区块链的交易记录具有公开可追溯、不可篡改的特点，使得资金流动可以与数据流、物流信息形成可信的映射关系。在跨境数据服务、软件即服务

[17] 参见张阳：《论稳定币本土发展的规范逻辑》，载《交大法学》2025 年第 5 期，第 123 页。
[18] 参见杨松、王雨婷、雷紫斌等：《美国稳定币化债机制、政策与影响》，载《福建金融》2025 年第 8 期，第 57 页。
[19] 参见杨松、王雨婷、雷紫斌等：《美国稳定币化债机制、政策与影响》，载《福建金融》2025 年第 8 期，第 58 页。

（SaaS）、数字内容贸易等场景中，稳定币能够实现“交易即结算”，大幅缩短支付周期，降低传统跨境支付平均高达 6.7%的成本。[20]更为重要的是，通过智能合约的可编程特性，可以将支付条款与数据交付状态自动绑定，实现“条件支付”。这种机制能够在数据接口调用达到特定次数或数据包成功传输验证后自动触发稳定币支付，从而将商流、数据流与资金流紧密耦合，实现结算流程的自动化与智能化。目前，部分提供跨国云服务与数据分析 API 的科技公司已开始接受 USDC 作为支付方式，利用其链上交易的透明性为双方提供清晰、不可抵赖的结算凭证，极大简化了高频、小额微服务结算的对账流程。

3.2.2 新加坡稳定币的监管制度与实践情况

新加坡作为全球 Web3.0 及虚拟货币发展最为活跃的国家之一，新加坡金融管理局（Monetary Authority of Singapore,MAS）率先出台针对性法规，并通过《支付服务法》与《稳定币监管框架》确立了清晰的合规路径，构建起针对单一法币挂钩稳定币（SCS）的监管体系。[21]该体系强调币值稳定、储备资产安全与投资者保护，为稳定币在跨境场景中的合规应用提供了制度保障。对新加坡现行规则及实施范例的研究，可为跨境数据流通中的货币结算机制提供有益参考。

3.2.2.1 新加坡稳定币监管框架：稳健创新下的分层准入与储备管理

新加坡稳定币体系的形成可追溯至《支付服务法》（Payment Services Act,2019），该法案首次明确数字支付代币的概念，并建立了基于风险分层的许可制度。这一机制为稳定币纳入金融体系提供了基础，使不同规模与功能的支付机构能够在明确定义的监管层次中运营。

在此基础上，新加坡金融管理局于 2023 年发布《稳定币监管框架》（Stablecoin Regulatory Framework）。《稳定币监管框架》明确了稳定币（Single-Currency Stablecoins,SCS）的概念，即稳定币（Stablecoin）被定义为一种数字货币，其价值与特定国家货币挂钩，并且限定在新加坡发行。值得注意的是，框架将稳定币分为两种类型，分别为单一货币稳定币与其他稳定币。《稳定币监管框架》要求稳定币与新加坡元或 G10 货币挂钩（即本次 MAS 监

[20] 参见周光友、杨洁萌：《<GENIUS 法案>下美元稳定币扩张与数字人民币战略应对》，载《发展研究》2025 年第 8 期，第 14 页。

[21] 《稳定币研究报告解读丨稳定币的分类与发展（第 2 期）》，载微信公众号“Web3.0 标准化”，2025 年 5 月 7 日上传。

管下的稳定币特指单一货币稳定币），并限定其发行活动须在新加坡境内进行，以确保可监管性与金融稳定。[22]储备资产需完全覆盖流通量，并以现金、短期国债及其他高流动性资产形式托管于受监管机构。发行方需保持充足信息披露与定期审计，确保市场透明度与兑付能力。

关于发行方，新加坡金融管理局（MAS）对稳定币发行方设定了准入门槛并实行差异化监管。在准入门槛方面，MAS 强调申请主体需同时满足多重审慎要求：①发行人必须维持不少于 100 万新元或年度运营费用 50%的资本金，以确保持续运营能力。②发行人必须持有充足的流动性资产，其规模需满足正常提现需求或高于年度运营费用的 50%。③为防范风险交叉传染，MAS 要求稳定币发行人不得从事交易、资产管理、质押借贷等高风险业务，也不得直接持有其他法人实体股份。在监管方面，MAS 根据稳定币发行方是否为银行机构设定了不同的准入条件：对于非银行发行主体，若其稳定币流通规模超过 500 万新元（即“重大发行人”），必须申请相应牌照。对于银行发行主体则豁免牌照要求，但其发行的稳定币必须由 100%的资产作为抵押。此外，MAS 还从基础资本、偿付能力、业务范围、储备资产、白皮书披露以及反洗钱与网络风险管理等多个维度，对发行主体提出了统一的审慎要求，以保障市场的稳定与安全。

关于币值稳定机制，新加坡金融管理局（MAS）通过严格的储备资产管理制度保障稳定币价值稳定。按《稳定币监管框架》规定，发行人的储备资产必须由风险极低、流动性充足的资产构成，具体包括现金、现金等价物及剩余到期日不超过三个月的短期债券。这些资产的发行主体限定为主权政府、中央银行或信用评级达到 AA-及以上的国际机构。[23]为确保资产安全，发行人必须设立基金并开设隔离账户，将自有资金与储备资产严格隔离。

这种设计体现出新加坡在数字金融治理中的“稳健创新”原则。MAS 在制度上强调功能中立与风险导向，不对技术路线作硬性限制，而聚焦于价值锚定与资金安全等核心要素。这种开放结构为金融科技企业预留了创新空间，使新加坡在数字资产监管中兼具灵活性与信任基础。

---

[22] 《[专题・政策]全球视角下稳定币行业创新及发展动态（政策篇）》，载微信公众号“工银亚洲研究”，2025 年 6 月 11 日上传。

[23] 《Web3 律师深度解读：一文详解欧盟、阿联酋、新加坡三地稳定币监管框架》，载微信公众号“盈科新视野”，2025 年 6 月 18 日上传。

3.2.2.2 新加坡稳定币制度的市场实践与发展趋势

新加坡的稳定币生态在监管确立后迅速发展，金融科技公司 StraitsX 发行的 XSGD 成为其中最具代表性的市场案例。XSGD 稳定币自 2020 年上线以来，以 1:1 比例锚定新加坡元，储备金由星展银行（DBS Bank）与渣打银行（Standard Chartered Bank）共同托管，具备高度透明的资金结构与兑付保障。XSGD 可在以太坊、Polygon 与 XRP Ledger 等多链环境中流通，实现跨平台支付与去中心化金融（DeFi）应用的兼容性。[24]

XSGD 稳定币在功能层面实现了传统支付网络与区块链支付系统的融合。用户可通过合规的支付通道以法币兑换链上资产，再经由本地银行体系完成结算，从而实现“链上交易—法币兑付”的闭环机制。多家交易平台和支付服务提供商（如 OKX Pay 与 Fazz）已将 XSGD 纳入支付与兑换流程，使新加坡元的链上结算成为日常商业支付的现实选项。

新加坡稳定币体系呈现出“监管明确—操作开放—功能融合”的特征，使得新加坡在全球数字金融竞争中始终保持着制度优势。在未来发展方向上，稳定币有望在跨境结算、供应链融资、数据交易及数字贸易领域发挥更大作用。凭借成熟的法律基础与国际化的金融环境，新加坡正逐步成为亚洲稳定币与数字货币治理的关键枢纽，为其他国家提供制度化、市场化与技术化并行的实践范式。

新加坡的稳定币体系已从政策实验阶段进入制度化运营阶段。依托清晰的监管逻辑、合规的资产托管机制与开放的技术架构，稳定币在新加坡实现了货币功能与创新价值的双重整合。其经验表明，稳定币的成功并不在于监管强度的高低，而在于能否在信任、透明与效率之间建立可持续的平衡。这一平衡正是新加坡稳定币模式的核心竞争力所在。

3.2.3 欧盟稳定币的监管规则与实际应用

为构建统一的加密资产市场监管格局，欧盟于 2023 年出台了 2023/1114 号法规，《加密资产市场监管法案》（Markets in Crypto-Assets regulation，MiCA），并于 2023 年 4 月 20 日欧洲议会会议上正式投票通过，构建了全球首个综合性稳定币监管框架，旨在平衡创新与风险，维护金融稳定与货币主

[24] 《全球稳定币监管的框架、理论与趋势研究》，载微信公众号“上海金融与发展实验室”，2025 年 5 月 2 日上传。

权。25欧盟《加密资产市场监管法案》为加密资产制定了统一的欧盟市场规则。该法规涵盖目前不受现有金融服务立法监管的加密资产。对于发行和交易加密资产（包括资产参考代币和电子货币代币）的人来说，关键条款包括交易的透明度、披露、授权和监督。新的法律框架将通过监管加密资产的公开发行并确保消费者更好地了解其相关风险来支持市场诚信和金融稳定。[26]

3.2.3.1 监管界定：分类与使用限制

依据加密资产是否通过锚定其他资产以实现价值稳定的核心特征，可将其划分为三类适用监管的加密资产：电子货币代币（Electronic Money Tokens,EMT）、资产参考代币（Asset-Referenced Tokens,ART），以及其他不符合前两类定义的加密资产（如主要用于访问特定服务或功能的“实用型代币”Utility Tokens,UTs）。值得注意的是，完全去中心化、缺乏明确发行人或运营主体的加密资产则不在《加密资产市场监管条例》（Markets in Crypto-Assets Regulation,MiCA）的监管框架覆盖范围内。

其中，EMT 是一种通过锚定单一法定货币（通常以 1:1 比例持有相应法币储备）来维持其价值稳定的加密资产（即法币支持型稳定币）。其主要功能是作为一种高效、便捷的支付手段，其法律属性与功能定位与欧盟现行《电子货币指令（EMD2）》所界定的电子货币高度相似。而 ART 则通过锚定一种或多种价值来源（可能包括其他价值、权利、商品、法定货币或加密资产等）或其组合来维持其价值的相对稳定（即资产支持型或混合支持型稳定币），其主要用途除了作为交易媒介外，更侧重于作为投资工具使用。因此，ART 的发行人和提供相关服务的实体在运营过程中需遵守 MiCA 设定的更为严格的特定要求。EMT 与同样锚定法定货币的 ART 之间存在一项关键区别，即赎回权的保障程度：EMT 持有人通常拥有法定的、可随时按面值全额赎回其代币的明确权利；相比之下，ART 持有人的赎回时间安排和实际赎回价值则缺乏同等程度的法定保障，可能受限于发行人的条款或市场条件。

在此监管分类基础上，MiCA 对 ART 和 EMT 的具体使用场景设定了明确的操作性要求：首先，单一代币的日交易量被限制在五百万欧元以内，以防

[25] https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng.
[26] https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

止市场过度集中或波动；其次，当某类代币的总市值超过五亿欧元这一重要门槛时，其发行人必须立即向欧盟监管机构（欧洲银行管理局 EBA 和欧洲证券与市场管理局 ESMA）进行报告，并实施额外的、更高级别的合规与风险管理措施。在支付应用方面，MiCA 允许市场参与者自由使用 EMT（稳定币）进行加密货币之间的交易结算以及参与去中心化金融（DeFi）协议活动，但对于将其用作购买商品和服务的支付工具则施加了差异化的限制：明确规定仅锚定欧元的稳定币（欧元 EMT）可用于日常的商品和服务支付结算。这一政策设计的主要目的是维护欧盟的货币主权，防范非欧元外币稳定币的广泛流通可能对欧元区货币体系稳定性和货币政策传导有效性造成的潜在冲击。同时，ART 在日常支付中的使用规模受到更为严格的限制：当某一 ART 在欧盟单一货币区内日均交易笔数超过一百万笔，或其日均交易额超过二亿欧元（此阈值基于季度平均值计算）时，监管机构将强制要求必须停止该 ART 的继续发行，以控制其系统重要性风险。此外，作为一项重要的金融稳定措施，ART 与 EMT 的发行人明确被禁止向代币持有人支付任何形式的利息，旨在防止其演变为具有信贷风险的无监管存款工具。[27]

此外，对于实用型代币（Utility Tokens,UTs），尽管被归类为其他加密资产，其监管处理取决于具体功能：如果 UTs 主要用于访问特定服务或平台功能（如去中心化应用或会员权益），则通常不直接受 MiCA 约束，但若其设计或市场行为使其具有投资属性（如二级市场交易活跃），可能触发证券法规或其他金融市场监管要求，需由发行人主动评估合规性。同时，完全去中心化的加密资产虽明确排除在 MiCA 框架外，但在实际应用中可能面临国家层面的反洗钱（AML）或消费者保护法规监管，确保其不会成为规避监管的漏洞。在使用限制方面，非欧元稳定币的支付限制进一步细化：例如，在跨境电子商务场景中，非欧元 EMT 或 ART 用于欧元区交易时，需事先向监管机构报备交易规模，并实施额外的风控机制（如实时监控交易量），以防止系统性风险积累。这些分类与使用规则的设定，旨在通过精细化的监管区分，促进加密资产市场的创新活力，同时维护欧盟金融体系的整体稳定性和消费者权益保护。

[27] 朱太辉.《全球稳定币监管的框架、理论与趋势研究》[J].金融监管研究,2025,(03):16-36.

3.2.3.2 发行人准入：分类持牌与资质要求

根据欧盟《加密资产市场监管框架》（MiCA）的规定，“加密资产发行人”（issuer of crypto-assets）特指向公众提供任何类型加密资产或寻求将此类资产引入加密资产交易平台的法人实体。MiCA 旨在确保市场透明度和投资者保护，因此基于加密资产的不同分类，对发行人的资质和许可要求进行了差异化设计。在加密资产分类的基础上，MiCA 将资产分为稳定币（如电子货币代币 EMT）和资产参考代币（ART）等类别，并对每类发行人提出了具体准入标准。

对于一般加密资产发行人，若未偿金额不超过 500 万欧元或由欧盟授权的信贷机构发行，则可豁免监管授权，但发行人必须持续、定期披露储备资产信息，以确保市场透明。MiCA 对稳定币发行人实施分类授权机制：EMT 发行人必须为欧盟授权的信贷机构或电子货币机构（例如银行或支付机构），并需严格遵守《电子货币指令》（EMD2）的资本充足要求。若 EMT 未偿金额低于 500 万欧元或仅面向合格投资者发行，发行人可豁免授权，但仍需向公众发布详细的白皮书，说明资产特性和风险。

MiCA 特别关注资产参考代币（ART），认为 ART 可能被持有者广泛用于价值转移或作为交换手段，为保护持有者（尤其是零售投资者）利益和维护市场完整性，对 ART 发行人施加了更严格的准入要求：ART 发行人必须在欧盟境内设立为法人实体，并首先获得其母国指定监管机构的正式授权；此外，此类资产必须通过加密资产交易平台进行交易，以增强流动性监管。然而，在特定情形下可豁免准入授权，例如 ART 发行人已是信贷机构、未偿 ART 总额低于 500 万欧元、或 ART 仅发行给合格投资者等。

除上述发行人准入外，MiCA 还针对加密资产服务（如稳定币相关活动）设定了加密资产服务提供商（CASP）的授权要求。CASP 必须满足资本、治理和运营标准，并获得欧盟监管机构批准，以确保服务的安全性和合规性。整体而言，MiCA 通过分类持牌制度，平衡了创新激励与风险控制，为加密资产市场建立了统一的监管框架。

3.2.3.3 经营监管：资本与风险管理

欧盟《加密资产市场监管条例》（MiCA）规范了 ART 发行人和 EMT 发行人两类加密资产发行实体，其监管框架聚焦于信息披露、公司治理、内部控

制、风险管理、储备资产管理及资本要求等核心领域。ART 发行人需遵守最低自有资金规定，该要求取以下金额中的较高者：35 万欧元、储备资产与发行代币平均值的 2%，或前一年固定间接费用的四分之一（若为信贷机构则适用相应监管）；此外，ART 发行人必须制定恢复计划，以应对资产储备失衡等问题，确保及时恢复合规。EMT 发行人则需满足电子货币与支付工具机构的标准，资本要求不低于流通规模的 2%，并遵从信贷机构或电子货币机构的资本监管。所有加密资产发行人（除非是小型或豁免类型）均需发布白皮书。MiCA 还引入“重要加密资产”概念，依据客户数量、市值规模、交易量及与传统金融系统的关联度进行评估，对大型或有系统影响的发行人施加额外风险管理与资本要求。

3.2.3.4 储备金管理：隔离托管与流动性保障

欧盟 MiCA 法规为 ART 和 EMT 的储备资产管理确立明确规则，提升透明度与投资者保障。MiCA 强制要求 ART 储备资产必须与发行人资产完全隔离，由持牌信贷机构、投资公司或加密服务商单独保管。储备资产严禁抵押，定期审计。若资产损失，托管人须返还同类资产（不可抗力等免责除外）。如 EMT 储备须遵循 EMD2 和 PSD2，要求与非用户资金分离、挂钩货币一致、资产独立。发行人破产时，ART/EMT 持有人享有优先受偿权。同时，MiCA 对储备资产配置实施严格管控：普通 ART/EMT 发行人需将 30%储备资产存放于信贷机构，增强资产流动性；重要发行人（通常指资产规模庞大或具有系统性风险的实体）将该比例上调至 60%，大幅强化风险抵御能力。此外，ART 须设流动性框架与赎回计划，市价偏离时持有人可强制赎回。EMT 须随时按面值兑付，披露赎回条件。30 日内未履约，持有人可向托管方/分销商主张权益。

3.2.3.5 反洗钱与反恐怖融资（AML/CFT）监管

MiCA 高度重视稳定币和加密市场的违法犯罪行为（如内幕交易、市场操纵），要求所有加密资产服务提供商执行全面的反洗钱和反恐融资措施，包括严格的 KYC 程序（如客户身份验证）、客户尽职调查（CDD）程序、实时监测可疑交易并报告监管当局。尽管 AART 和 EMT 允许匿名参与，但 MiCA 强调发行人利用区块链分析监控代币使用情况，如持有人行为、跨链交易量和涉及受制裁实体的交易，以防范非法活动。

同时，欧盟大幅提高“旅行规则”要求，《资金转移条例》规定加密资产服务提供商转移加密资产时须附带汇款人和收款人完整身份信息，否则禁止转移，覆盖所有金额交易，超越 FATF 的大额起点。此外，欧洲银行管理局（EBA）将《旅行规则指南》扩展至加密服务提供商及中介机构，要求收集报告交易信息（如时间、金额）、区分合法活动、监测可疑行为，并公开声明中介处理流程和跨境政策，以提升透明度和监管效率。

3.3 中国稳定币监管框架与典型实践探析

中国在稳定币及相关数字支付领域的监管与发展路径呈现出鲜明的“一国两制、双轨并行”特征。在内地，监管机构对私人加密资产和非主权背书的稳定币采取严格禁止态度，同时大力推动以数字人民币（e-CNY）为核心的央行数字货币体系建设；而在香港特别行政区，金融管理部门正积极探索建立全球接轨的稳定币监管框架，旨在打造国际化的数字资产中心。这一“内地审慎管控、香港开放试验”的格局，不仅反映了中国在金融创新与风险防范之间的平衡策略，更潜藏着为未来数据跨境流动构建安全、高效、合规结算基础设施的战略布局。

3.3.1 中国大陆地区虚拟货币监管规则与政策逻辑

中国内地对虚拟货币及稳定币的监管立场始终以防范金融风险、维护货币主权和保障经济安全为核心。自 2013 年起，中国人民银行等监管机构便陆续发布多项政策文件，逐步收紧对加密资产的管控。2017 年，央行等七部门联合发布《关于防范代币发行融资风险的公告》，明确将首次代币发行（ICO）定性为非法融资行为，全面叫停相关活动。此后监管持续加码，至 2021 年 9 月，中国人民银行、中央网信办、最高人民法院等十部门联合印发《关于进一步防范和处置虚拟货币交易炒作风险的通知》，标志着监管框架的全面成型。该文件明确指出，虚拟货币不具有与法定货币等同的法律地位，相关业务活动属于非法金融活动，严禁任何机构和个人从事虚拟货币兑换、交易、信息中介服务以及为境外交易所提供境内展业便利等行为。这一系列政策从根本上切断了私人稳定币在中国大陆的发行与流通路径，USDT、USDC 等主流稳定币无法通过正规金融渠道进入国内市场，本土企业亦不得开展类似业务。

尽管监管态度严格，但其深层逻辑并非否定技术本身，而是强调对金融秩

序与数据主权的统筹治理。在数据跨境流动日益频繁的背景下，支付结算已不仅是资金转移的工具，更承载着交易主体身份、资金用途、合规条件等关键信息。若允许境外主导的稳定币广泛使用，可能导致交易数据外流、资金流向不可控，甚至被用于规避外汇管理或数据出境监管。因此，内地的监管禁令实质上是在构建一个“安全可控”的结算环境，确保所有资金流动均处于监管可视范围之内。

在此背景下，数字人民币（e-CNY）作为唯一合法的法定数字货币，被赋予了战略使命。e-CNY 由中国人民银行发行，采用“双层运营”架构，具备可控匿名、离线支付和可编程性等技术特征。其中，可编程性允许通过智能合约设定资金的使用条件与流转规则，实现“规则内嵌于支付”的新型治理模式。例如，在数据服务交易中，可设定 e-CNY 仅用于特定数据产品购买，或在数据调用完成后自动触发分账结算，从而实现资金流与数据流的协同控制。这种机制不仅提升了交易效率，也为监管机构提供了更强的审计与追溯能力。

3.3.2 香港《稳定币条例》及其主要监管规则

香港特区《稳定币条例》于 2025 年 8 月 1 日起正式实施，标志着其在构建全球领先的数字资产监管框架方面迈出关键一步。该条例以“风险为本、透明稳健、国际兼容”为核心原则，首次明确将合规稳定币纳入金融基础设施监管体系，旨在吸引国际资本与技术参与，推动香港成为亚太地区数字支付与资产代币化的枢纽。条例确立三大核心监管要求：

一是发行准入严格化。仅允许持牌机构发行与法定货币挂钩的稳定币，申请人须具备健全治理、充足资本及独立审计能力，并提交技术架构、风控方案与应急计划。锚定资产限于美元、欧元等主要货币或一篮子货币，禁止与商品或其他加密资产挂钩，防范价值波动风险。

二是储备管理规范化。实行“全额储备+高流动性+第三方托管”机制，要求发行的每一单位稳定币均有等值的高质量短期资产（如国债、央行存款）支持，每日披露储备构成，由独立机构托管并接受定期审计，确保兑付能力。同时设立储备隔离机制，防止资金挪用。

三是持续监管制度化。香港金管局拥有直接监督权，可实施现场检查、数据报送和压力测试，并建立跨境监管协作机制。对虚假披露、储备不足等违规

行为，将处以高额罚款或吊销牌照。在保障安全前提下，鼓励试点智能合约驱动的自动兑付与跨链结算功能。

相较于内地全面禁止私人稳定币的审慎立场，香港《稳定币条例》展现出鲜明的开放性与功能性导向。这种差异并非对立，而是中央顶层设计下“一国两制”框架内的战略互补。内地通过数字人民币构建主权可控的底层支付结算体系，强调规则内嵌与数据主权保护；而香港则依托普通法传统和国际金融中心地位，探索国际兼容的合规稳定币制度，形成对外连接的“制度接口”。两地由此构成“内环安全、外环联通”的双层架构：数字人民币保障境内资金流的可溯可控，香港合规稳定币则作为对接国际市场、服务离岸人民币需求的重要工具，二者共同服务于国家金融安全与对外开放的平衡目标。

这一协同格局对数据跨境流动具有深远启示。基于合规稳定币的结算不仅提升效率，还可将身份认证、用途声明、审计轨迹等非财务信息编码至交易元数据中，实现“资金流—信息流—合规流”的三位一体。这正是未来数据要素全球化配置所需的关键支撑——一个兼具主权信用背书、市场广泛接受与监管互认能力的中间结算层。香港《稳定币条例》所建立的制度基础，正为此类创新提供了合法、可信、可扩展的试验场域，为中国参与全球数据治理规则制定开辟了新的战略通道。

3.3.3 典型实践与探索性案例分析

尽管中国尚未出现基于稳定币的大规模数据跨境结算应用，但在多个领域已涌现出具有示范意义的试点与探索项目。北京市部分政务服务系统已试点使用数字人民币支付企业信用报告查询、不动产登记信息调取等数据服务费用。该项目实现了从申请、身份验证到自动扣费的全流程线上化，验证了可编程货币在数据资源有偿使用中的可行性。虽然当前应用局限于境内，但其技术架构为未来在跨境数据交易平台中实现自动化结算提供了可复制的模板。

另一个更具战略意义的案例是多边央行数字货币桥（mBridge）项目。该项目由国际清算银行牵头，中国人民银行、香港金管局、泰国央行和阿联酋央行共同参与，旨在构建一个基于央行数字货币的跨境支付平台。截至 2024 年，mBridge 已完成首例基于真实交易场景的试点测试。其底层架构支持智能合约、实时清算和结构化信息传输，完全适用于数据服务的跨境交易。未来，mBridge

可扩展为“数据-资金”双流合一的基础设施，实现端到端的自动化执行。

尽管上述案例大多处于试点或规划阶段，尚未形成规模化应用，但它们共同指向一个清晰趋势：结算工具的数字化、可编程化与合规化，正在成为支撑数据要素高效、安全流动的关键基础设施。这些探索不仅验证了关键技术的可行性，也为中国构建自主可控、国际兼容的数据跨境结算体系积累了宝贵经验。

3.3.4 内地与香港协同发展的战略展望

中国在稳定币领域的“双轨制”探索，本质上是一种顶层设计下的功能互补。内地通过发展数字人民币，致力于构建一个主权可控、规则内嵌的底层结算底座；香港则通过制度创新，探索与国际规则兼容的合规稳定币发行路径。二者看似分立，实则协同，共同构成了中国应对未来数据跨境挑战的“双轮驱动”战略。

可以预见，随着 mBridge 等跨境基础设施的成熟，以及内地与香港在监管标准、技术协议上的逐步衔接，一种融合“主权信用+可编程支付+合规透明”的新型结算体系将逐步成型。这一体系不仅有助于提升中国在全球数据价值链中的地位，也将为构建更加公平、安全、高效的国际数据治理新秩序贡献中国方案。

3.4 未来稳定币对货币结算规则的影响

3.4.1 CBDC 与结算逻辑重塑

2025 年，国际清算银行（BIS）2025 年发布的《协同推进：2024 年 BIS 央行数字货币与加密资产调查报告》显示，全球 91%的中央银行已启动央行数字货币（CBDC）探索，其中 38%的发达经济体央行已进入批发型 CBDC 试点阶段。[28]

全球正在重塑国家间数据基础设施与货币结算规则的底层逻辑。未来十年，货币结算将不再是单纯的资金划转，而是通过复式记账向分布式记账的迭代升级，依托可信数据流实现商流、物流、资金流“三流合一”的系统性变革，其核心驱动力来自技术创新、全球监管协调、生态融合与风险防控的多维协同。

3.4.2 DLT 颠覆传统结算

分布式账本技术（DLT）正在颠覆传统结算的“层层代理”模式。香港金

[28] https://www.cebnet.com.cn/20250908/102994888.htmlBIS 央行数字货币与加密资产调查报告：协同推进的数字金融新图景。

管局数据显示，在《稳定币条例》框架下，京东“京链通”稳定币通过区块链实现跨境结算时间从 3 天压缩至 10 秒，这种“去中介化”的清算逻辑，本质是将结算过程从“异步批量处理”转变为“实时交易”。

数字人民币国际运营中心采用并推出三大业务平台——数字人民币跨境数字支付平台、数字人民币区块链服务平台及数字资产平台。数字人民币跨境数字支付平台探索运用法定数字货币解决传统跨境支付中存在的痛点；数字人民币区块链服务平台为各场景和行业类区块链提供标准化的跨链交易信息转接和链上数字人民币支付服务；数字资产平台可提供标准、即用的金融级数字资产服务，支持现有金融基础设施将业务拓展至链上。[29]

3.4.3 传统支付痛点与稳定币破局

传统的支付体系自 20 世纪中期以来基本是稳定的，其核心架构以中央银行主导的金融清算网络与银行间通信系统（如 SWIFT），并由商业银行、清算机构、支付网关等多层中介支撑。在保障交易安全方面，这种体系发挥了重要作用，但由于复杂的层级结构，导致了全球支付普遍存在三大“痛点”：高成本、低效率与存在准入障碍。信用卡支付的交易费用普遍在 2%～3%，国际电汇的费用往往高达 20-50 美元，实际到账的时间长达 3～5 个工作日，严重滞后于数字经济时代的节奏效率。[30]

稳定币作为区块链世界对法币的一种数字映射，正在挑战原有的架构、规则、体系。结合区块链去中介、高效、可编程的优势，与相对稳定的法币币值融合，货币结算规则将经历从“以法币为中心的层级体系”向“多极化网络体系”的转变，其核心特征可概括为“三化”：结算实时化（从 T+5 到实时）、资产数字化（从纸质凭证到链上代币）、监管智能化（从事后审计到实时穿透）。这一变革的底层驱动力，是数据基础设施与货币结算的深度融合，以零信任架构为代表的安全技术，构建可信数据传输通道，以分布式账本、AI 预测为代表的效率技术，提升结算速度与风险管理能力，实现全球协同与风险可控。

3.4.4 规模爆发与未来愿景

2025 年 USTD 与 USDC 的活跃用户数分别突破 2 亿与 1 亿，每日交易量分别达 500 亿美元与 200 亿美元，涵盖支付、投资、结算、借贷、理财、

[29] https://www.gov.cn/yaowen/liebiao/202509/content_7042292.htm 数字人民币国际运营中心正式运营。
[30] 《稳定币：数字金融的未来》高华声，林雅恒著。

抵押等多个维度[31]。2025 年数字人民币跨境支付场景将加速拓展，成为人民币国际化的重要抓手。预计跨境支付市场规模将突破 3.5 万亿元，占人民币跨境结算比例提升至 18%，覆盖大宗商品贸易、跨境电商、供应链金融等核心场景[32]，基于人民币为基础的稳定币在未来也具有极大的发展空间。

未来，稳定币不应只是加密世界的试验场，而是成为以跨链、低效、可编程为特征的全球支付基础设施，在全球数字经济繁荣发展的进程中，货币、账户、支付、合约逐步融合，在跨境结算、供应链金融、消费支付、储蓄理财中扮演重要角色。中国作为全球最大贸易国，在这一进程中的角色尤为关键：数字人民币的“双层运营”架构与香港稳定币的“合规创新”经验，为“主权货币+市场驱动”的协同模式提供了范例；京东“京链通”与数字人民币国际运营中心的实践，则验证了“技术赋能+生态融合”的商业可行性。正如国际清算银行所指出的，未来的货币结算体系将不再是“谁取代谁”的零和博弈，而是“传统与创新”“中心化与去中心化”“主权与市场”的共生共存。

3.4.5 风险挑战与战略临界点

稳定币的匿名性与跨境高效性已成为中国资本流动监管的主要挑战，典型案例显示其通过境内外钱包对敲+OTC 平台洗钱形成非法通道。2023 年上海 65 亿元 USDT 非法换汇案中，团伙操控 17 家空壳公司对公账户，将境内人民币通过 OTC 平台兑换为 USDT，再由境外团伙在链上划转后兑现为外汇，全程分割为两段独立操作以逃避监管。重庆何某案更揭示稳定币成为资产转移工具，通过低买高卖 USDT（收购价 6.85 元、出售价 7 元）实现 6.09 亿元资金跨境转移[33]。

美元稳定币通过公链渗透至非美国家，形成“数字殖民”效应，东南亚国家若被迫接受 USDT 作为跨境结算工具，其货币政策的独立性将受到冲击。中国若未能快速构建以数字人民币为核心的跨境支付体系，可能丧失对“一带一路”沿线贸易的定价权[34]。稳定币推动的 RWA（真实世界资产代币化）热潮可能催生新泡沫，美国国债代币化产品规模已超 1200 亿美元，若市场逆转引发

[31] 数据引用自《稳定币：数字金融的未来》高华声，林雅恒著。
[32] https://www.chinairn.com/news/20250307/153324712.shtml#:~:tex2025 年数字人民币跨境支付场景拓展与货币政策影响分析。
[33] https://finance.sina.com.cn/stock/wbstock/2025-07-17/doc-inffuzvh4873358.shtml 以稳定币为媒介非法换汇，上海公布 65 亿元跨境换汇大案。
[34] https://sof.sufe.edu.cn/cc/90/c18088a248976/page.htm 稳定币和加密资产立法可能加剧金融体系脆弱性。

抛售，将加剧美债流动性危机。更为危险的是，链上资产估值模型与传统金融脱节，可能掩盖系统性风险[35]。

3.4.6 终点即起点

站在 2025 年的变革临界点，我们可以预见：当可信数据流像“血液”一样贯穿商流、物流、资金流的每一个节点，货币结算将不再是贸易的“附属品”，而是驱动全球经济高效协同的“神经系统”。这不仅是技术的胜利，更是规则、生态与信任的重构——而那些能在这场重构中把握平衡、拥抱开放的国家与机构，将赢得未来十年的战略主动权。

[35] https://sof.sufe.edu.cn/cc/90/c18088a248976/page.htm 稳定币和加密资产立法可能加剧金融体系脆弱性。

第四章 数据跨境流动规则与技术演进预测与政策体系优化

前三章系统梳理了数据跨境流动的政策版图、技术架构与场景实践：从全球监管规则的“多轨并行”到 AI、加密资产带来的新变量，从“可用不可见”的隐私计算到稳定币重塑结算底座的制度突破。当前，数据要素正加速突破地理与主权边界，但规则差异、技术门槛与信任缺口依旧制约着数据跨境流动向“全球协作”新阶段迈进。

本章聚焦“规则-产业-生态”的整体跃迁：第一部分绘制数据跨境产业全景图谱，解析各赛道的企业分布与技术路线；第二部分提出“规范性政策+产业性政策+国际合作政策”三位一体的协同设计框架；第三部分展望规则演进与产业发展趋势，研判面临的核心挑战。通过微观层面降低合规摩擦、中观层面激活产业动能、宏观层面嵌入全球数字治理多边进程，为数据跨境流动提供可持续、可扩展的制度支撑。

4.1 数据跨境产业图谱

4.1.1 图谱整体架构

数据跨境产业图谱呈现六大核心层级，构建了从底层基础设施到上层应用的完整产业生态体系。该图谱涵盖基础设施层、数据资源与供给层、数据采集与加工层、数据安全与合规治理层、数据流通与交易层以及数据应用层，形成了支撑数据跨境安全有序流动的完整产业链条。各层级既相互独立又紧密协同，共同保障数据在跨境流动过程中的合规性、安全性和可用性。

数据跨境产业图谱

4.1.2 图谱分层架构

4.1.2.1 基础设施层

基础设施层是数据跨境流动的物理底座，提供全球化的计算、存储、网络传输能力，解决数据跨境流动中的连通性和承载能力问题。该层级主要包括跨境云服务、国际网络连接与传输、物理数据中心以及国际数据港与产业园区四大板块。

1.跨境云服务

跨境云服务商作为该层级的核心，通过全球分布的可用区实现“数据本地化存储、服务全球化访问”。亚马逊云科技(AWS)凭借全球覆盖优势，成为中国企业出海的首选云平台，其区域隔离架构帮助企业满足 GDPR 和 CCPA 的数据驻留要求；阿里云在东南亚市场建立了最完善的数据中心布局，是中资企业布局“一带一路”的首选底座；华为云在欧洲、中东地区优势明显，提供符合德国 C5 认证等严苛标准的合规云服务；微软 Azure 通过世纪互联运营，为外资企业在中国提供符合“数据不出境”要求的本地云环境；腾讯云专长于游戏和音视频领域，在全球部署了大量边缘节点支持跨境游戏加速；天翼云依托中国电信的全球网络，为央国企提供高安全等级的跨境政务云服务。

2.国际网络连接与传输

国际网络连接与传输板块聚焦解决跨境访问的延迟和稳定性问题。中国电信国际(CTG)的 CN2 网络提供质量最优的回国链路，是跨国金融机构的首选；中国移动国际(CMI)拥有极大的出海带宽储备，在中国香港、新加坡建有超大型核心枢纽节点；中国联通国际(CUG)在连接欧洲方向拥有独特的陆缆资源优势；南凌科技提供合规的跨境 SD-WAN 服务，帮助制造业企业实现国内外工厂互联；第一线(DYXnet)专注于大中华区的企业级网络互联；网宿科技通过全球 CDN 节点加速跨境电商的内容分发。

3.物理数据中心与硬件设施

物理数据中心与硬件设施提供核心物理承载空间。万国数据(GDS)在国内一线城市和东南亚拥有大规模高等级数据中心，支持客户“国内+海外”双部署；Equinix 的 IBX 数据中心是全球网络汇聚点，是中资企业接入全球生态的关键物理节点；世纪互联(VNET)作为外资云服务在华落地的物理载体，承载了微软和 IBM 等国际巨头的本地化部署；秦淮数据在马来西亚等地为字节跳动等客

户定制建设海外超算中心；亨通光电作为全球前三的海底光缆制造商，构建了数据跨境的“物理血管”。

4.国际数据港与产业园区

国际数据港与产业园区作为政策高地，提供特殊监管便利。上海临港国际数据港建设有独立的光缆登陆站和国际通信设施，探索“数据海关”模式，开展一般数据清单式出境；海南自由贸易港连接东南亚的海缆枢纽，允许开展“两头在外”的数据加工业务；北京数字贸易示范区探索建立离岸数据中心，支持企业开展离岸云服务；深圳前海和河套深港合作区通过深港跨境专线，实现科研数据的低时延互通；中新天津生态城与新加坡建立点对点数据连接，服务中新贸易。

4.1.2.2 数据资源与供给层

数据资源与供给层汇聚了拥有高价值、标准化全球数据资产的企业，其业务模式本质上就是数据的跨境许可、订阅或 API 调用。该层级企业根据数据类型和应用场景呈现明显的行业特征。

1.金融与资本市场数据

金融与资本市场数据领域标准化程度最高，跨境流动最为频繁。彭博(Bloomberg)提供全球实时行情、固定收益数据和大宗商品数据，是外资机构的核心数据源；伦敦证券交易所集团(LSEG)旗下的路孚特(Refinitiv)数据库涵盖全球外汇、ESG 数据和企业基本面；万得(Wind)作为中国 A 股、债券和宏观经济数据的权威提供商，是外资机构了解中国市场的核心窗口；同花顺(iFind)和东方财富(Choice)提供中国金融市场深度数据；标普全球(S&P Global)提供全球信用评级、指数数据和大宗商品价格。

2.企业征信与商业情报数据

企业征信与商业情报数据用于跨境供应链管理和商业尽职调查。邓白氏(Dun&Bradstreet)拥有全球数亿家企业的商业画像和 DUNS 编码；益博睿(Experian)提供个人与企业信用评分和反欺诈黑名单数据；中国出口信用保险公司(Sinosure)提供全球国别风险报告和海外买方信用数据；企查查国际版和天眼查提供中国全量工商注册数据，供海外合规审查使用；合合信息(IntSig)的启信宝支持全球企业征信查询。

3.知识产权与科研数据

知识产权与科研数据用于全球研发协同。科睿唯安(Clarivate)的 Web of Science、Derwent 专利数据库和 Cortellis 医药研发数据是科研机构的重要资源；爱思唯尔(Elsevier)的 ScienceDirect 和 Scopus 引文数据库覆盖全球学术文献；智慧芽(PatSnap)提供全球专利数据、生物序列数据和新药研发情报；中国知网(CNKI)是中国学术数据出海的主要通道，需通过安全评估。

4.国际贸易与物流数据

国际贸易与物流数据用于掌握全球货物流转。ImportGenius 和 Panjiva 提供全球海关提单数据和进出口贸易商名录；亿海蓝(Elane)提供全球船舶位置(AIS)数据和港口调度数据；上海航运交易所(SSE)发布出口集装箱运价指数(SCFI)等航运指数；Freightos 提供全球货运实时定价数据。

5.行业垂直数据

行业垂直数据涉及特定行业的专业数据。地理信息领域，四维图新(NavInfo)提供中国高精度地图数据和自动驾驶编译数据，HERE Technologies 提供全球位置数据；医疗医药领域，IQVIA（艾昆纬）提供全球药品销售数据和真实世界研究数据；时尚电商领域，WGSN 提供全球时尚趋势预测数据；航空旅游领域，中航信(TravelSky)提供中国航空客运订座数据，OAG 和 Cirium 提供全球航班时刻表数据。

6.公共与开源数据源

公共与开源数据源提供宏观数据基础。世界银行(World Bank)提供全球发展指标和营商环境数据；国际货币基金组织(IMF)提供国际收支平衡表和汇率数据；国家统计局(NBS China)提供中国 GDP、CPI、PMI 等宏观经济数据；Hugging Face 和 GitHub 托管开源 AI 数据集和代码库。

4.1.2.3 数据采集与加工层

数据采集与加工层是连接数据资源与数据应用的中间环节，在跨境场景下承担通过技术手段使数据满足跨境合规要求的核心任务，包括去标识化、标准化处理，从而降低数据出境风险。该层级主要包括综合数据治理平台、数据分类分级与资产盘点、数据脱敏与去标识化以及跨境语种与格式处理四大板块。

1.综合数据治理平台

综合数据治理平台建立全球统一的数据标准，确保跨国数据的一致性和可追溯性。Informatica 作为全球主数据管理(MDM)的领导者，被大量跨国公司用于统管全球分公司数据标准；SAP 依托 ERP 生态，提供跨国供应链和财务数据的统一治理工具；星环科技(Transwarp)提供全链路数据治理平台，支持多国部署下的数据资产目录构建与血缘追踪；华为云 DataArts 具备强大的数据集成与治理能力，支持“一处开发，全球部署”；亿信华辰(Esgrand)擅长元数据管理和数据标准建立，帮助企业梳理出境数据的“家底”；科杰科技(KeenData)提供数据虚拟化技术，支持不移动原始数据的情况下进行跨域逻辑管理；网易数帆强调数据开发与治理一体化，适合跨境电商和游戏等高频数据流动行业。

2.数据分类分级与资产盘点

数据分类分级与资产盘点自动识别“重要数据”和“个人敏感信息”，这是数据出境安全评估的第一步。全知科技(Gokuhs)专注于 API 数据暴露面监测，能实时发现通过 API 接口违规出境的敏感数据；阿里巴巴 Dataphin 内置行业分类分级模板，自动扫描并打标出境数据中的敏感字段；昂楷科技(Ankki)自动梳理数据库中的敏感资产分布，生成数据资产分布地图；极盾科技(Jidun)提供实时的数据资产测绘，动态监控敏感数据的访问行为；御数坊(DGWorkshop)结合咨询服务，提供符合监管要求的数据分类分级落地工具；BigID 作为全球领先的隐私发现工具，支持 GDPR、CCPA、PIPL 多法规下的敏感数据自动发现。

3.数据脱敏与去标识化

数据脱敏与去标识化对拟出境的敏感数据进行技术处理，使其达到“出境不违规”的标准。美创科技(Mchz)提供高性能数据库脱敏系统，支持仿真脱敏以便海外系统测试使用；安华金和(DBSEC)具备丰富的数据静态脱敏规则库，支持不可逆加密；炼石网络(CipherGateway)的“数据安全主服务”架构，在不修改业务代码的前提下对跨境传输数据进行透明加密和脱敏；闪捷信息(Secsmart)针对跨境访问场景，根据访问者 IP 动态展示不同脱敏程度的数据；Imperva 提供数据库防火墙及动态遮蔽功能，常用于外资企业在华数据的合规防护。

4.跨境语种与格式处理

跨境语种与格式处理解决中外数据格式、编码、语言不通的问题。合合信息(IntSig)智能识别多国票据和证照，将其结构化为可治理的数据资产；拓尔思(TRS)针对跨境舆情和多语言文本数据进行清洗、分类和摘要提取；科大讯飞(iFlytek)提供跨境会议数据和客服录音数据的转写与清洗服务。

4.1.2.4 数据安全与合规治理层

数据安全与合规治理层是数据跨境流动的核心保障，主要包括数据治理与合规以及互联互通与可信数据空间两大板块，旨在确保数据在全生命周期内符合法律法规要求，并构建多方参与、规则共识、技术保障的数据流通环境。

1.数据治理与合规

数据治理与合规板块通过技术工具和专业服务，帮助组织建立健全的数据合规管理体系，分为合规与政策服务层、数据治理平台层和数据安全工具层三个子层级。

合规与政策服务层提供顶层设计、法律咨询和专业评估服务。金杜、中伦、广和、卓建、新世通等律师事务所专注于《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》（PIPL）、GDPR 等国内外法规，提供数据出境安全评估和合规制度设计等高价值法律服务；这些企业具备跨国协作能力，能够协调不同国家和地区的法律要求，为跨国公司提供一站式合规解决方案；具有合规审计资质与认证资质的企业提供独立的第三方合规审计报告服务，协助企业获得 ISO、C-STAR 等安全合规认证。

数据治理平台层提供平台化、流程化的工具和系统，将法律要求转化为可执行的技术规范。华为、中科软联、星环科技、浪潮、华宇信息等企业提供从数据采集、存储、处理、使用到销毁的全流程治理能力，核心功能包括元数据管理、数据质量、数据标准和数据血缘追踪；华为、星环科技等具备大数据平台能力的企业提供自动化识别和标记敏感数据的能力，支持基于不同合规要求的精细化分类分级，这是跨境数据安全评估的基础；华为、阿里云、腾讯云等平台通常基于云原生架构，能够与主流云服务商和各类数据源进行深度集成，实现统一的数据视图和治理。

数据安全工具层提供底层技术手段，直接作用于数据本身和数据环境。启明星辰、深信服、奇安信、天融信、安恒信息等企业专注于数据防泄露

（DLP），监控和阻止敏感数据未经授权的传输和流出，是数据跨境安全的核心技术之一；提供加密服务的厂商以及数据治理平台企业提供高性能的数据加密、同态加密、数据脱敏等技术，确保数据在存储、传输和使用过程中的机密性；提供身份认证、访问控制和安全审计的厂商实施零信任、最小权限原则的精细化访问控制，并提供全面的审计日志记录；部分提供虚拟化、安全计算或安全隔离技术的厂商提供安全隔离的沙箱环境，用于处理敏感数据，确保数据不出域。

2.互联互通与可信数据空间

互联互通与可信数据空间旨在构建多方参与、规则共识、技术保障的数据流通环境，确保数据在跨境传输和利用过程中的可信、可控和合规，实现“可用不可见”或“可控可计量”的数据共享与协同。该板块包括运营方、技术提供方和数据服务方三个角色。

运营方主要由政府主导或政府与企业联合的实体构成，体现出强烈的区域政策驱动特征。中关村、临港等区域聚焦高新技术产业和贸易，运营模式强调“平台+网关”的双层合规机制，旨在服务特定产业的数据跨境需求；平潭枢纽则侧重于提供一站式合规服务，包括数据出境评估、脱敏和托管，旨在降低企业合规门槛。

技术提供方集中在保障数据“可用不可见”的核心技术上。安恒等企业代表了密态计算在跨境场景的深度应用，其低性能损耗的特点是实现大规模、高频次数据处理的关键；华为等基础设施提供商通过 TEE（可信执行环境）和区块链等技术，构建了可信的硬件和软件环境，是数据空间的基础底座；炼石则专注于数据安全与脱敏，为运营方的合规平台提供关键的安全工具。

数据服务方是连接技术与合规实践的桥梁，主要由法律服务和数据治理机构构成。国浩、金杜等顶级律所的参与，凸显了跨境数据流通中法律合规的极端重要性，它们为企业提供定制化的多国法规（如 GDPR、PIPL）合规设计与审计服务；实达集团则作为综合服务平台，将技术与合规咨询相结合，提供一站式数据出境服务。

3.隐私增强计算与协同智能

隐私增强计算与协同智能作为数据跨境流动技术体系的核心赋能板块，通过底层多种安全技术集群实现上层企业、行业数据跨境服务落地，支撑数据跨境“可用不可见”的核心需求。该板块企业呈现“技术研发+解决方案+行业落地”的多元化业务布局，可划分为技术壁垒型、资源整合型、场景应用型三大类别。

技术壁垒型企业聚焦底层技术攻坚，形成技术研发集群。华控清交、洞见科技、同态科技等垂直服务厂商依托高校与科研院所的学术资源，通过算法创新、协议优化、框架搭建，为数据建模提供高性能、高安全、高兼容的技术底座；这类企业以技术研发能力为核心壁垒，研发投入占比高、核心专利密集，为跨境场景的产业技术迭代提供底层的前沿技术研究和技术可行性论证。

资源整合型企业借助政策红利与区位优势，整合国内外技术供应商、行业客户、监管机构资源，构建跨境协同网络。各运营商、腾讯、阿里巴巴等大型互联网厂商，亚信安全、安恒信息等安全厂商以跨境资源协同与流程优化为核心能力，充分整合技术与方案，打破资源壁垒，搭建跨境合作生态，聚焦跨场景通用解决方案，覆盖多个行业或多个跨境环节。

场景应用型企业以跨境业务需求为导向，基于对垂直场景的深度理解与全生命周期运营能力，提供定制化数据协同服务。商汤科技、火山引擎、翼支付等企业的分布与垂直行业集群高度契合，如医疗领域聚焦上海、广州等医疗资源密集城市，金融领域集中于北京、上海、深圳等金融中心，汽车领域围绕长三角、珠三角汽车产业带布局，实现多主体、跨区域的联合建模落地，将技术能力转化为实际业务价值。

4.1.2.5 数据流通与交易层

数据流通与交易层通过提供合规的交易场所、可信流通技术和专业服务，解决数据“不敢出、不愿出”的问题，推动数据要素市场化配置。该层级主要包括跨境数据交易场所、可信流通技术服务商、跨境数据商以及跨境数据资产评估与服务四大板块。

1.跨境数据交易场所

跨境数据交易场所提供合规的挂牌、登记、撮合与结算服务。深圳数据交易所(SZDE)依托大湾区地缘优势，设立跨境数据专区，重点推动深港澳数据流通，在金融、科研数据跨境交易方面活跃；上海数据交易所(SDE)设立国际板，主要引入海外数据产品（如邓白氏、LSEG），并支持国内数据通过合规评估后挂牌出海；北京国际大数据交易所(IDEX)结合北京“两区”建设，设立数据跨境服务中心，重点探索数字贸易规则；贵阳大数据交易所探索气象与电力数据跨境交易产品；海南数据产品超市利用自贸港政策优势，探索游戏出海、跨境医疗等场景的数据产品交易；AWS 数据交换作为全球最大的云上数据交易市场，是国内企业出海获取第三方数据的重要渠道。

2.可信流通技术服务商

可信流通技术服务商利用隐私计算(MPC、FL、TEE)技术，实现数据在跨境场景下的“可用不可见”。华控清交(Tsingjiao)基于多方安全计算（MPC），支持境内外银行在不交换原始数据的前提下联合计算反洗钱模型；洞见科技(InsightOne)利用隐私计算技术，帮助保险公司与海外再保机构进行数据协作；蚂蚁集团的摩斯(Morse)支持 Alipay+全球支付网络中的风控协同；翼方健数(BaseBit)通过“数据沙箱”模式，让海外药企算法在沙箱内运行，原始医疗数据不出域；冲量在线(Impulses)利用 TEE（可信执行环境），解决跨国分支机构间的数据联合分析信任问题；富数科技(Fudata)通过联邦学习（FL），帮助中国品牌在海外利用本地数据进行联邦建模；微众银行的 FATE 开源社区提供的 FATE 框架是目前全球跨境数据合作中被采纳度最高的开源隐私计算标准之一。

3.跨境数据商/经纪商

跨境数据商/经纪商作为数据的“搬运工”和“加工厂”，发现海外需求，采购国内数据或反之，并进行产品化封装。上海钢联(Mysteel)将中国的大宗商品产能、库存数据销售给全球对冲基金和贸易商；卓朗科技协助企业将内部数据转化为可交易的标准产品；易华录(E-Hualu)提供海量冷数据的长期存储与跨境灾备服务；云赛智联(INESA)探索将上海的公共数据经过脱敏后开发成面向国际航运公司的产品；中远海科汇聚全球航运大数据，提供面向全球船东和货主的 SaaS 数据服务。

4.跨境数据资产评估与服务

跨境数据资产评估与服务为跨境流动的数据“定价”和“入表”，使其成为可被国际市场认可的资产。普华永道(PwC)和德勤(Deloitte)提供符合国际会计准则的数据资产估值服务（D-Score/数据估值），帮助跨国企业数据资产入表；中联资产评估是国内数据资产入表的领军机构，探索跨境数据交易定价模型；上海立信对跨境数据交易过程中的合规性、真实性进行第三方审计。

4.1.2.6 数据应用层

数据应用层代表了数据跨境流动的最终价值实现，涵盖金融支付、智能网联汽车、跨境电商、生物医药、数字娱乐以及企业服务等多个领域，呈现出显著的行业特征和差异化的合规需求。

1.跨境金融与支付

跨境金融与支付领域数据流向高频、实时，涉及核心敏感个人信息和资金信息。SWIFT（环球银行金融电信协会）作为国际基础设施，是全球银行间资金划拨信息的传输通道；银联国际(UnionPay Intl)处理中国持卡人海外消费数据的回传和海外发卡数据；蚂蚁国际(Ant International)通过 Alipay+和 WorldFirst 提供全球商户收单数据和跨境汇款 KYC 信息校验；PingPong 和连连数字提供亚马逊等平台卖家交易数据的归集与合规申报；Airwallex（空中云汇）提供企业全球虚拟账户的开户信息验证与资金流向分析；同盾科技和邦盛科技利用设备指纹和关联图谱，识别跨境支付中的欺诈团伙。

2.智能网联汽车

智能网联汽车是监管最严领域之一，涉及地理信息（GIS）、车外视频和车辆工况数据。特斯拉中国承诺中国数据存储在上海，仅脱敏统计数据出境向美国总部汇报；比亚迪、蔚来、小鹏等中国 OEM 的出口车辆行驶日志回传和远程 OTA 升级指令下发体现了数据出境特征；Momenta 和小马智行收集全球路测数据用于优化自动驾驶模型；四维图新(NavInfo)协助外资车企将中国地图数据进行合规编译后传输给海外系统；中远海科提供远洋货轮的实时位置、油耗、工况监控数据回传。

3.跨境电商与数字营销

跨境电商与数字营销领域数据量最大，涉及全球用户的浏览行为、订单信息、收货地址。SHEIN 和 Temu（拼多多）将全球用户订单回传至中国供应链

中心，进行生产排期和物流发货；阿里巴巴通过速卖通和 Lazada 实现中国卖家数据与海外买家数据的撮合匹配；汇量科技(Mobvista)基于海外用户画像进行程序化广告投放归因分析；易点天下(EasyTech)帮助中国品牌分析海外社交媒体数据，优化营销策略；店匠(Shoplazza)为商户提供全球站点的数据分析看板。

4.生物医药与大健康

生物医药与大健康领域涉及“人类遗传资源”（HGR）管理，合规门槛极高。药明康德(WuXi AppTec)作为 CXO 龙头，代表全球药企处理药物发现过程中的实验数据，需向委托方交付数据；泰格医药(Tigermed)同步中国与海外临床试验基地的患者数据，用于 FDA/EMA 新药申报；阿斯利康和辉瑞中国将中国患者的不良反应报告(PV)上报至全球安全数据库；华大基因(BGI)涉及全球基因测序数据的科研合作，受限于极严的 HGR 审批；医渡科技(Yidu Tech)利用脱敏医疗数据支持全球药企的药品上市后评估。

5.数字娱乐与游戏出海

数字娱乐与游戏出海领域涉及用户互动数据、聊天日志、账号资产数据。米哈游(HoYoverse)虽然多采取分区部署，但涉及跨区账号互通和全球运营数据统计；腾讯游戏的 Level Infinite 在新加坡或法兰克福节点处理海外用户行为数据，数据不回传国内；字节跳动的 TikTok 通过“数据本地化”（Project Texas/Clover），切断与中国的数据关联；昆仑万维和欢聚时代处理海外用户的 UGC 内容审核、语音/视频数据流。

6.企业服务与人力资源

企业服务与人力资源领域主要涉及跨国公司内部员工数据(HR Data)和客户关系数据（CRM）。Salesforce 作为 CRM 巨头，跨国企业中国分公司的销售数据同步至全球总部；Workday 和 ADP 提供跨国企业中国员工的薪酬、考勤、绩效数据跨境传输；SAP 和 Oracle 实现全球财务报表和供应链库存数据的统一视图；飞书(Lark)和钉钉支持中资出海企业的跨国文档协作和会议录制数据传输。

4.1.3 图谱特征与产业趋势

数据跨境产业图谱呈现出以下核心特征：一是分层协同，从基础设施到应用层形成完整的产业链条，各层级既相互依存又专业分工；二是合规导向，数

据安全与合规治理层贯穿各个环节，成为数据跨境流动的核心保障；三是技术驱动，隐私增强计算、数据脱敏、区块链等技术创新成为破解“数据不敢出、不愿出”难题的关键；四是生态化发展，“律所+技术”“平台+网关”等联合交付模式日益普遍；五是区域集聚，上海临港、深圳前海、海南自贸港等政策高地汇聚了大量跨境数据服务商，形成产业集群效应。

从产业趋势看，数据跨境正从“规则驱动”向“AI 驱动”演进，从“单点突破”向“生态协同”转变，从“被动合规”向“主动治理”升级。随着《数据出境安全评估办法》等法规体系的完善，以及隐私计算、联邦学习等技术的成熟，数据跨境产业将迎来规范化、规模化发展的新阶段，为全球数字经济合作提供坚实支撑。

4.2 数据跨境流动支持政策体系设计

4.2.1 数据跨境流动规范性政策优化与落地保障

4.2.1.1 政策演进背景

我国加入 WTO 后各产业深度融入全球产业链，数据随跨境业务流动全球，管控体系亟待建立。为维护国家安全与数据主权，我国接连发布《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》，形成以法律定框架、以行政法规和部门规章为支撑、以地方试点与国际共创作补充的多层次数据跨境流动规范体系。明确以安全评估、标准合同、个人信息保护认证为三大具体路径。

2024 年，国家互联网信息办公室发布《促进和规范数据跨境流动规定》，标志政策重大转向，其核心在于通过制度创新平衡安全与发展需求，采取“以安全促发展”模式。通过分级分类、有限豁免、区域试点等方法，规定共十四条，将促进措施前置：第三至第五条：规定数据跨境有限豁免情形，覆盖国际贸易、跨境运输、学术合作、跨国生产制造、市场营销、跨境购物等高频场景；第六条：赋予自由贸易试验区在国家数据分类分级保护制度框架下制定数据出境负面清单；第七至第十一条：规定数据处理者在数据跨境中应尽义务。

4.2.1.2 政策实施成效

政策实施一年多以来成效显著，数据来源：国家网信办，2024 年：

1.行业效率提升：全国 8 个自贸区针对 30 多个特色行业领域制定负面清单。

上海自贸区：金融、航运、商贸 3 个领域；

北京：汽车、医药、民航、人工智能等 5 个领域；

广西：地理信息与气象数据服务、企业信用信息服务、直播跨境电商、海外音视频制作与传播 4 个领域；

海南：深海、航天、旅游、免税商品零售等 5 个领域。

2.审批效率优化：

数据出境安全评估项目月均受理数量下降约 60%，个人信息出境标准合同月均备案数量下降约 50%。

3.企业正向反馈：

大众汽车集团（中国）认为简单且可落地的政策法规反映政府对促进数据跨境流动的重视；

乐高玩具（上海）认为规定为企业数据跨境传输提供清晰操作指南；

武汉某化妆品效果评价外资公司因上调申报数据规模阈值，人脸皮肤检测数据不再需要标准合同备案。

4.2.1.3 优化路径

尽管成效显著，数据分类分级标准不清晰、合规成本高昂、合规不确定性等问题仍待解决。

1.完善数据分类分级制度

主管部门应公开征集数据分类分级制度制定需求，综合考虑行业数据出境规模、紧迫度，结合已有负面清单、申报请求次数等因素，按需求程度研究出台分类分级标准。

行业标准制定：网信部门联合数据局与行业主管部门，参考《工业数据分类分级指南（试行）》《电信领域重要数据识别指南》，在各自贸区发布的行业数据跨境负面清单基础上研究制定相关细分规范；

基础方法整合：将 GB/T 43697-2024《数据安全技术数据分类分级规则》作为基础方法论，整合各地现有数据分类分级规范如江苏省《财政数据分类分级规范》，研究制定重要数据清单。

2.加强政企沟通

细化规则体系：基于自贸区分行业制定数据跨境负面清单的授权逻辑，探索推动标准合同从通用版向行业定制版升级；联合律师协会开展研究，在标准合同中补齐与他国签署的自由贸易协定中数据跨境相关内容；

主动理解场景：灵活使用政策激励机制，将数据跨境费用补贴作为了解业务实践与市场需求的窗口；以场景化方式明确不同场景下可跨境流动的一般数据及对应字段；邀请企业共同构建行业数据跨境流通标准规范。

3.开拓第三方公益咨询渠道

构建“政府引导、专业支撑、公益普惠”的第三方咨询体系：

线上渠道：依托数据交易机构官网或公众号开设“数据跨境公益咨询专区”；

线下窗口：联合本地律师协会、律师事务所等专业机构在主管部门、数据交易机构、自贸区或行业园区设立咨询窗口；

典型案例：江苏“苏数通”平台、上海临港新片区数据跨境服务中心。

4.以技术驱动监管创新

轻量化工具：研究上线本地部署的评估工具，企业导入需跨境传输的数据后，输入行业类型、数据量、应用场景等信息，工具自动判断是否符合豁免条件或匹配申报材料。工具不联网、不存储企业数据，避免数据泄露；

监测系统建设：将数据跨境监管设施融入我国数据基础设施框架；建立全国统一的跨境数据流动监测系统；基于数据跨境负面清单与已成型的数据分类分级办法，运用 AI 算法自动识别异常数据，对高风险传输触发实时预警；

通道基础设施：统计数据跨境主要流向国家；试点建设数据跨境传输专用通道；探索中国-新加坡、中国-欧盟、中国-非洲等跨境数据专线。

4.2.2 数据跨境产业性政策引导与生态培育

4.2.2.1 设立研发专项，突破核心技术瓶颈

1.政策背景

在国内大数据产业稳步发展、数据要素市场化配置加快推进的背景下，我国同态加密、多方安全计算、差分隐私、联邦学习等新兴技术的产业化仍处于发展阶段。欧美国家已设置严格的数据安全与使用规范，一旦技术完全落地并

通过商业体系和壁垒形成控制，在极限脱钩场景下可能出现严重的数据制裁和事实封锁，对跨境贸易、金融业务、科研应用、交通旅游、医疗健康产生极大影响。

中国的技术国际化与商业体系的全球化可以有效延缓甚至阻止这一情况出现。因此，新兴技术应在算法层面实现突破与领先，率先实现高安全、低功耗、标准化的技术攻关，是未来规模化推动数据流通应用的核心制高点。

2.专项设计

设立“数据跨境流动核心技术攻关专项”，重点支持：高性能隐私计算算法研发：提升技术计算效率与易用性；低功耗技术优化：针对边缘设备、移动终端等场景，研发低功耗隐私计算技术方案；技术标准化研究：联合产学研机构制定隐私增强计算技术接口标准、安全评估规范、数据合规治理指南等。

3.实施机制

产学研联合攻关模式：优先支持龙头企业牵头，联合高校、科研院所组建攻关团队；跨领域技术融合：鼓励密码学与人工智能、分布式计算与区块链技术的结合；成果转化机制：设立技术中试基地、举办成果对接会，缩短技术从实验室到市场的周期。

4.2.2.2 构建国家级跨境可信数据空间基础设施与试点示范

1.基础设施建设

跨境可信数据空间基础设施建设需重点强化三大能力：

- 安全互联能力：支持不同国家、不同机构的数据空间实现身份互认、策略互通、审计互信；
- 数据治理能力：内置数据分类分级、出境风险评估、合规证据链构建等功能模块；
- 协同计算能力：集成隐私增强计算引擎，支持企业在数据空间内开展“可用不可见”的联合建模与数据分析。

2.创新驱动与场景结合

以创新驱动、需求为引导，将隐私增强应用与数据场景有机结合：

- 结合云计算安全、大模型应用、数据跨境等需求；
- 为数据新业态遇到的实际困难落实解决方案；

- 快速推动跨境可信数据空间的国际化与规模化。

3.运营模式

政府引导、企业主导、市场化运作：鼓励社会资本参与基础设施建设运营；

产学研企联合：以核心技术骨干企业作为牵头单位，联合地方政府、央企、民企、高校团队；

场景打造：打通政务、大行业中结合数字经济与合规流通的典型场景，打造跨境数据可信流通案例与要素应用模式。

4.试点示范

选择汽车、金融、生物医药、跨境电商等数据价值高、跨境需求迫切的重点行业开展跨境流动试点，给予政策、资金、技术支持。试点结束后，由监管部门组织专家评估，提炼可复制、可推广的行业解决方案与实践指南，在全国范围内推广应用。

4.2.2.3 构建与国际接壤的合规服务生态

1.合规认证标准建设

研究借鉴欧盟充分性评估机制、日本数据保护互认经验，结合我国数据保护法规要求，明确中国数据出境合规认证标准的范围、流程、评估指标等，内容涵盖数据分类分级、出境风险评估、安全保障措施、合规审计等方面。

2.国际互认机制

推动国内合规认证与国际主流认证体系的互认：

与欧盟、美国、日本、新加坡等重要贸易伙伴的监管机构开展合规认证互认谈判；

建立互认清单，对通过我国合规认证的企业，在对方国家开展数据跨境业务时可享受简化的合规审核流程；

降低企业国际合规成本，提升我国企业在国际市场上的合规信誉与信任度。

3.专业服务机构培育

加强政策引导培育一批具有国际视野的专业数据合规服务机构：

为企业提供从数据分类分级、出境风险自评估、合规审计到国际互认的全链条服务；

支持国内合规服务机构“走出去”，鼓励其在海外设立分支机构开展本地

化合规服务；

推动我国合规标准与国际标准对接，提升我国在全球数据合规领域的话语权与影响力。

4.2.2.4 实施数据跨境产业人才专项培育计划

1.学科建设与课程优化

针对数据跨境产业对复合型人才的需求，推动高校优化学科设置：

- 开设数据合规、隐私计算、数据要素市场、国际数据治理等交叉学科课程；
- 将数据跨境相关知识纳入计算机科学与技术、法学、国际贸易、金融学等专业培养方案；
- 开展数据跨境领域研究生教育，培养高层次研究型人才。

2.校企合作育人机制

建立高校与企业的合作育人机制：

- 支持高校与龙头企业联合设立实训基地；
- 推动企业参与课程设计、实践教学、毕业设计等环节；
- 确保人才培养与产业需求无缝对接。

3.国际化人才引进

设立数据跨境产业国际化人才引进绿色通道，重点引进海外在隐私计算、国际数据治理、跨境数据合规等领域具有丰富经验的高层次人才。

通过上述政策引导落地，能够有效降低企业合规成本，激发市场主体参与数据跨境合作的积极性，最终形成技术先进、服务健全、人才充沛的良性产业生态，为我国深度参与全球数字治理与竞争奠定坚实基础。

4.3 数据跨境流动的国际合作性政策与外部协同

在全球数字经济蓬勃发展的背景下，数据跨境流动已成为驱动创新和贸易的关键要素。然而，各国间日益分化的监管框架和地缘政治因素，使得数据跨境流动面临严峻的合规挑战和不确定性。本节旨在阐述构建国际合作性政策和外部协同政策的必要性、核心原则与设计路径，以期在保障国家安全和个人隐私的前提下，促进数据安全、有序、高效地流动，实现全球数字治理的平衡与共赢。

4.3.1 国际合作性政策：构建全球数据治理的共同框架

国际合作性政策是解决数据跨境流动监管冲突、降低合规成本、促进数字贸易的根本途径。其核心在于通过多边和双边机制，建立一套被广泛接受的、兼顾发展与安全的共同规则。

4.3.1.1 核心原则与目标

核心原则	政策目标	论证严密性
主权与安全平衡	尊重各国数据主权和安全审查权，同时避免以安全为名设置不必要的贸易壁垒。	政策设计应明确界定“重要数据”和“核心数据”的范围，并建立透明、可预期的安全审查机制，以消除不确定性。
互操作性与兼容性	推动各国数据保护标准和认证机制的相互承认，降低企业在多法域下的重复合规成本。	借鉴 APEC CBPR（跨境隐私规则）等机制，探索建立区域性或行业性的数据保护认证体系，实现“一次认证，多国通用”。
发展与普惠	确保发展中国家和中小企业能够公平参与数字经济，避免合作机制成为少数发达国家的“排他性俱乐部”。	政策应鼓励数字公共产品和数字公共基础设施的建设，促进数据要素的共享和利用，赋能全球普惠增长。

4.3.1.2 政策设计路径

一是推动多边协议的务实进展。积极参与世界贸易组织（WTO）电子商务谈判，推动数据流动条款的达成。同时，支持联合国等国际组织在数字治理领域发挥更大作用，例如推动《全球数据跨境流动合作倡议》的落地实施，将其转化为具体的合作项目和双边协议。

二是深化双边和区域合作机制。通过与主要贸易伙伴签订数据跨境流动双边协议，明确数据传输的安全保障措施、监管协调机制和争议解决机制。例如，

在“一带一路”倡议框架下，推动沿线国家建立数据流动“绿色通道”，简化合规流程。

三是建立监管协调与对话机制。设立常态化的国际监管对话平台，由各国数据保护机构、行业监管机构和企业代表共同参与，定期交流监管实践、澄清模糊地带，并共同应对新兴技术（如 AI）带来的数据安全挑战。

4.3.2 外部协同政策：构建多方参与的治理生态

外部协同政策旨在将数据跨境流动的合规责任和治理能力从政府延伸至企业、行业组织和技术服务商，形成“政府引导、企业主体、社会参与”的协同治理格局。

4.3.2.1 政策设计要点

协同主体	政策设计要点	核心价值
企业主体	合规激励与豁免机制：对已建立完善数据治理体系、通过第三方合规认证的企业，提供数据出境“负面清单”或“白名单”的便利化措施，减少不必要的安全评估。	激发企业内生合规动力，将“要我合规”转变为“我要合规”。
行业组织	行业自律与标准制定：鼓励行业协会（如金融、医疗、互联网）根据行业特性，制定高于国家标准的自律规范和数据处理行为准则，并推动其国际互认。	提升行业整体合规水平，为政府监管提供专业支撑。
技术服务商	技术赋能与工具创新：政策应鼓励和支持技术企业（如数据治理平台、安全工具商）研发数据沙箱、隐私计算、联邦学习等技术，实现“数据可用不可见”，从技术层面解决跨境流动的安全顾虑。	以技术创新应对监管挑战，提供“合规即服务”的解决方案。
第三方机	专业评估与认证：赋予具备资质的第三方机	引入市场机制，提升

构	构（如律所、会计师事务所、专业评估机构）更大的合规评估和认证权力，减轻政府监管压力，提高评估效率。	合规评估的专业性和效率。

4.3.2.2 外部协同的实施路径

一是“监管沙箱”机制的推广。在特定区域（如自由贸易区、数据特区）设立数据跨境流动监管沙箱，允许企业在受控环境中测试新的数据跨境传输模式和技术方案，为政策制定提供实践经验。

二是数据分类分级标准的统一。推动企业、行业组织和监管机构在数据分类分级标准上的协同，特别是对“一般数据”和“重要数据”的界定，为实施差异化监管奠定基础。

三是国际法律服务协同。鼓励国内律所与国际律所建立数据合规联盟，共同为跨国企业提供涵盖多法域的法律服务，确保企业在不同司法管辖区都能获得一致且专业的合规指导。

4.4 总结和展望

4.4.1 规则趋势

4.4.1.1 监管精细化和场景化

当前，我国数据跨境监管体系正经历关键转型，从以往侧重原则性约束的模式，逐步迈向分级分类清晰、操作流程明确的制度化新阶段。近年来，国家网信办等部门持续迭代优化数据跨境的申报及备案机制，以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》三部上位法为框架，建立了数据出境安全评估、个人信息保护认证、个人信息出境标准合同 3 大合规路径。

2024 年 3 月，国家网信办发布《促进和规范数据跨境流动规定》，一方面适当放宽数据跨境流动条件，适度收窄数据出境安全评估范围，另一方面探

索建立自贸区负面清单、标准合同等便利化机制，为一般数据流动提供制度通道，分类分级安全有序推动数据跨境流通，有效推动跨境数据管理从“一刀切”的粗放式管控，转向“分类施策、精准监管”的精细化治理模式。监管层面始终对重要数据、涉及国家安全及关键信息基础设施相关的数据流动保持严格管控态势，筑牢数据安全底线；而在一般性商业场景的数据跨境场景中，已开始探索简化合规流程的实施路径，兼顾监管效能与市场活力。

4.4.1.2.重点行业率先推进

2025 年 4 月 9 日，国家网信办发布“数据出境安全管理政策问答（2025 年 4 月）”，明确指出国家网信办正会同相关行业主管部门，逐步细化明确具体行业领域的数据出境业务场景以及个人信息出境必要范围，为企业机构数据出境提供更为细化的政策指引。为落实国家数据跨境管理要求，各行业主管部门正结合自身特点加快制定细化的数据出境规则。当前，各行业主管部门在数据出境管理上，正从相对原则性的规定转向建立更为精细化和基于风险管理的合规体系，其核心是基于数据分类分级，对不同级别的数据实施差异化的出境管理措施，而非要求所有数据一概本地化存储。

1.金融行业

2025 年 4 月，中国人民银行、金融监管总局、中国证监会、国家外汇局、国家网信办、国家数据局联合印发《促进和规范金融业数据跨境流动合规指南》，首次提出“金融数据分级分类管理”体系，扩展形成了 47 项免于安全评估、标准合同或认证的高频金融业务场景及对应数据项清单，涵盖跨境支付、跨境汇款、跨境开户、跨境购物等活动，并且梳理了主管部门认可的、但无法免于数据跨境流动合规义务的其他 61 项常见金融业务场景。同时，该指南还创新性设立“数据跨境流动协议”机制，支持金融机构与境外合作方通过合同约定权责，并引入“数据出境风险自评估”工具包，强调“数据主权可控”与

“技术自主创新”的协同，为金融行业的数据跨境流动提供了明确的合规指引。2025 年 5 月，中国人民银行正式发布《中国人民银行业务领域数据安全管理办法》（简称“《人行数安新规》”），《人行数安新规》于 2025 年 6 月 30 日开始实施。《人行数安新规》第 24、25 条对于领域内业务数据跨境传输规则进行了规定，整体而言，衔接对齐了国家网信部门《评估办法》及 2024 年 3 月发布的《规定》相关规则。

2.汽车行业

汽车行业，作为数据安全管理的重点行业部门，其数据跨境流动的规模和复杂性不断增加，迫切需要统一的规则指引，以加强汽车数据的保护和出境管理。2025 年 6 月，工业和信息化部、国家网信办、国家发展改革委、国家数据局、公安部、自然资源部、交通运输部、市场监管总局联合起草的《汽车数据出境安全指引（2025 版）（征求意见稿）》公开发布并面向社会征询意见。该指引总体上整合了我国境内数据出境相关管理要求，并延续风险分级管理思路，主要对重要数据的出境活动进行了细化，包括各个场景下的重要数据范围、重要数据识别和备案、数据出境安全评估申报流程，以及汽车数据出境安全保护要求，一定程度上回应了汽车行业在数据出境实操中遇到的问题，反映了监管部门对各类汽车数据的认定标准。

4.1.1.3 国际数据治理规则林立

如何统筹发展与安全的关系，始终是各国构建数据跨境流动规则与管理体系时的核心考量。在当前全球数据治理领域，尚未形成一套被广泛认可的统一规则，各国基于自身的利益诉求和价值理念，逐渐形成了多元的治理模式，共同构成了复杂的全球治理格局。

具体而言，美国奉行“市场本位”的治理理念，在各类双边及区域贸易协定中大力推动数据的自由流动，明确反对设置数据本地化等限制性条款，试图

以市场力量主导全球数据流动秩序；欧盟则以《通用数据保护条例》为核心支柱，构建起一套严格的“权利本位”治理模式，将个人隐私保护置于优先地位，通过严格的准入审查和责任规制规范数据跨境行为；而众多发展中国家出于维护自身利益的需求，更加强调“数据主权”的核心地位，普遍通过数据本地化存储、跨境流动审批等针对性措施，为国家安全筑牢防线，同时为本土产业预留充足的发展空间。

RCEP、CPTPP、DEPA 等协定虽已成为全球数字贸易治理的重要制度载体。然而，由于各国在数据主权、安全标准与隐私保护上的立场差异，短期内难以形成统一的全球规则。因此，未来的跨境数据治理将更可能采取“区域模块化”与“规则互认”的方式推进。

4.4.2 产业发展趋势

4.4.2.1 数据跨境流动提质扩容，本地化规制持续收紧

在全球数字经济蓬勃发展的驱动下，跨境数据流动的规模正不断扩大，其蕴含的商业价值与社会价值也同步攀升。与此同时，数据本地化的发展态势愈发明显，已成为各国数据治理的重要方向。当前，多国针对个人征信数据、金融交易数据、医疗健康档案等敏感性数据，纷纷出台强制性本地化存储与处理要求。这一现象背后，反映出全球网络数据安全意识的普遍提升，各国在数据本地化管控措施的设计上，也更趋向于精细化与限制性，以强化对核心数据的主权管控。

4.4.2.2 数据跨境安全成核心关切，产业链安全投入显著增长

高水平安全的数据跨境流动，是数字贸易发展的重要前提。数据跨境流动为个人隐私安全、国家安全等带来前所未有的冲击，数据安全和隐私保护等成为全球数据治理的重点内容。数据流动所创造的价值使得个人信息、企业和行业数据等成为人们逐利的资本，数据泄露、黑客攻击等安全问题频发，跨境数据流动为个人隐私安全、国家安全等带来前所未有的冲击。随着网络空间国际

博弈的加剧以及全球局势的复杂多变，组织化程度高、实施计划缜密、攻击目标明确的网络攻击行为已呈现常态化特征，突发性、大范围的网络安全事件仍处于高发周期。这种严峻的安全形势直接催化了产业链各环节的安全保障需求，推动上下游企业持续加大数据安全技术研发、设备部署及服务采购等方面的投入。

4.4.2.3 数商服务生态加速成型，专业化分工体系逐步显现

跨境数据的高效流动正推动数据要素作为生产资料，在全球范围内实现重组与优化配置，并逐步构建起贯穿国际生产分工体系的全球数据价值链。在数据从基础资源向可量化资产的跨境转化进程中，需经历数据采集、存储备份、分析建模、交易撮合及流通复用等多个关键环节，这些环节通过跨境流转形成完整的价值创造与循环链条。在此过程中，以数据服务商为核心的生态体系加速崛起，涵盖数据合规咨询、脱敏处理、交易中介、价值评估等领域的专业化分工格局初步显现，为数据跨境价值转化提供了全方位支撑。

4.4.3 面临挑战

4.4.3.1 政策落地效果不佳

因数据存在虚拟性、场景依赖性等特性，兼之数据跨境流动的安全监管是一个复杂的系统工程，具有头绪繁、场景多、体量大、监管难等特点，政策在落地中也暴露一些问题。

一是数据分类分级标准不清晰。现有数据跨境流动规范性政策建立在数据分类分级基础上，数据出境审查主要覆盖重要数据与个人数据，个人数据相对而言界限清晰，重要数据则相对模糊。尽管配套的《数据出境安全评估办法》（国家互联网信息办公室令第 11 号）相比《中华人民共和国数据安全法》对重要数据做出进一步界定，确定为一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的

数据”，但该定义对数据跨境实践的指导意义相当有限。抑制正常商业需求下企业数据出境，或导致企业抱有侥幸心理不经判断直接向境外传输数据。

二是高昂的合规成本与巨大的不确定性。一方面企业担忧在咨询过程中划定更为严格的出境限制，不愿直接咨询数据跨境管理部门；另一方面咨询律师事务所成本较高，大型跨国公司（MNCs）和科技公司，仍然感受到巨大的合规压力。它们指出，理解复杂的法规、进行内部改造、准备申报材料等需要投入大量的人力、物力和财力。不确定性也导致中小企业承担不成比例的负担，对于同一套规范体系，中小企业往往较之大型企业缺乏足够的资金和专业人才来应对复杂的合规流程。企业咨询需求被抑制，表现为数据跨境需求少，数据跨境管理部门无法得到正确反馈，信息闭塞，从而无法根据实际行业需求调整配套落地保障，无法形成“市场反馈意见-政策调整-促进市场发展”的良性循环。此外，标准合同中对补充条款的要求隐形增加了企业的合规复杂度。《个人信息出境标准合同办法》第八条规定“境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的”，意味着若境外接收方所在国出台新的数据本地化要求，企业需重新评估合同条款是否符合中国标准，并可能触发重新备案流程。

三是我国数据跨境规则的理论基础不足且规则呈现出“碎片化”特征。数据跨境处于多学科交叉领域，既需要从国际关系层面考虑数据主权理论与国际法基础，也需要从经济学层面关照数据要素价值理论，还需要探讨数据权益保护理论下的个人数据隐私保护，防控风险的同时以发展为导向推动数据跨境规范体系的完善。当前学界虽以基本形成共识，从促进发展并保护国家主权和个人权利的角度，就数据跨境流动规范提出诸多建设性措施，但多以文本对比、社会调研的方式，并未深入论述共识背后的理论基础并进行举证，同时未形成贯通多领域的理论体系。同时规定分散于不同层级的法律法规中，尚未形成一

个系统性、逻辑自洽的完整体系，我国跨境数据流动规制体现于一系列分散性的法律规范之中。就单边规制而言，《民法典》第 127 条明确了数据保护的重要意义；《中华人民共和国网络安全法》第 37 条规定国家应对关键数据和信息出境开展安全评估，从而确保数据安全；《中华人民共和国数据安全法》第 10 条着重指出我国应积极参与国际数据安全规则和标准的制定工作，以推动数据安全、自由地流动。《中华人民共和国个人信息保护法》要求信息处理者在进行数据出境操作时，不能使用一揽子、模糊的授权协议，而必须就该项特定事宜向用户进行清晰、明确的告知，并获得用户主动、清晰的“单独同意”。这与欧盟 GDPR 中的“明确同意”要求相呼应。在实践中，如何设计符合要求的告知同意流程，特别是对于线下场景和复杂业务模式，成为企业普遍面临的挑战。

4.4.3.2 核心技术仍需攻关

在国内大数据产业稳步发展、数据要素市场化配置加快推进的背景下，我国同态加密、多方安全计算、差分隐私、联邦学习等新兴技术的产业化仍处于发展过程中，但欧美等国家已经设置了严格的数据安全与使用规范，一旦技术完全落地，在这一技术之上通过其原有的商业体系和壁垒，面对极限的脱钩场景，极有可能出现严重的数据制裁和事实上的封锁，对于跨境贸易、金融业务、科研应用、交通旅游、医疗健康都产生极大影响。

4.4.3.3 国际规则对接空缺

就双边协定而言，截至 2023 年 7 月，我国已同 26 个国家和地区达成了 19 个自由贸易协定，在电子商务章节对该行业领域的数据流动予以一定规范，但甚少涉及其他领域的数据跨境流动规制。

就多边协定而言，我国积极参与的涉及跨境数据流动的多边协定主要为《区域全面经济伙伴关系协定》（RCEP），也是基于商贸物流领域对数据跨境

做出一定规范，确定“禁止实施数据本地化”“确保电子信息跨境传输”以及“必要的措施由数据流出国判定，其他成员国不得对此持有任何异议”等框架性共识，因多边规则制定的复杂性也并未涉及具体规制措施，我国数据跨境规范政策仍需补齐空缺，加强国际协调性，畅通中国企业“走出去”的道路。

终章：构建安全、高效、可信的全球数据跨境新生态

在数字经济全球化纵深发展的今天，数据跨境流动已成为激活创新动能、推动国际经贸协同的关键纽带。然而，数据主权诉求、监管规则差异、技术标准壁垒与隐私保护要求等多重挑战，始终考验着全球治理的智慧与协作。

本白皮书立足全球数据治理新格局与中国数字化转型实践，系统梳理了数据跨境的新场景、新技术与跨域监管挑战，构建了“技术支撑—合规实践—产业应用—政策优化”的全链路体系。我们看到：

- 技术驱动正重塑跨境规则，隐私计算、区块链与 AI 技术的融合，“数据可用不可见”的安全流通在逐渐实现；
- 场景创新激活数据价值，从跨境金融、智能汽车到医疗科研，数据要素在协同中释放倍增效应；
- 政策协同破解安全与发展难题，中国“分级分类、多轨并行”的合规框架与自贸区试点，为全球提供“平衡术”范例；
- 产业生态加速成型，从基础设施到应用层，数据商、技术服务商与合规机构共同构筑可信协作网络。

未来，数据跨境流动将向**“精细化、场景化、生态化”**演进：监管需进一步穿透场景、适配行业需求；技术需突破性能瓶颈、实现“三流融合”（数据流、资金流、合规流）；国际合作需深化规则互认、弥合“碎片化”治理鸿沟。

我们呼吁政府、企业、技术社群与研究机构携手共建**“规则清晰、技术先进、产业协同、国际互认”**的数据跨境生态：

- 以技术筑牢安全底座，推动隐私计算、量子加密等前沿技术落地；
- 以合规赋能产业创新，降低中小企业跨境门槛，激发数据要素活力；
- 以协同拓展全球链接，积极参与多边规则制定，贡献“中国方案”智慧。

唯有如此，方能在保障数据主权与个人隐私的前提下，为全球数字经济注入持久动能，让数据跨境流动真正成为连接世界的“数字丝绸之路”。