社会科学与教育 2025年第6期
ISSN: 3079-4420

数据安全主权：理论重构与中国实践

梅中伟*
中共深圳市委党校坪山分校，广东深圳，中国
*通讯作者

【摘要】全球数据治理陷入制度性割裂，传统主权理论难以调和安全管控与开放发展的矛盾。本文提出‘数据数据主权弹性化’理论框架，突破传统主权理论‘绝对管控’与‘自由放任’的二元对立，通过‘梯度分类+场景治理’机制实现安全与发展的动态平衡，为中国参与全球数据治理提供新范式。基于海南自贸港试点、区块链存证技术及 CPTPP 条款对比的三维实证，揭示‘梯度分类+场景治理’机制的技术经济效用。为发展中国家突破制度竞逐困境提供理论支撑。

【关键词】数据安全主权；主权弹性化；梯度分类+场景治理；数据跨境流动；区块链存证

1.引言：全球数据治理的制度性困境

根据《2023 年东南亚数字经济报告》，全球数据跨境流动规模年均增速超过 30%，2025 年对全球 GDP 的贡献预计达 11 万亿美元[1]。然而，根据国际数据公司（IDC）的测算，各国对数据主权的争夺导致全球数据流动效率因监管冲突下降 23%。例如，东盟数据枢纽的崛起与欧盟“数字巴尔干化”风险加剧了区域数据壁垒，企业需同时满足欧盟 GDPR 的 72 小时泄露通报、东盟 DEPA 的 7 类安全认证等多重框架，根据 IDC《2024 年全球数据合规成本报告》，中型 AI 企业年合规成本高达 1200-1800 万元（2023 年数据），占净利润的 15-22%。美国《云法案》与中国《数据安全法》的管辖权冲突则凸显了主权博弈的复杂性。2024 年某中企因援引《数据安全法》抗辩美国法院数据调取令，美方以“法律用语模糊”为由驳回，暴露法律互操作性缺失。全球数据治理呈现“三极分化”：欧盟以 GDPR 为核心，通过“充分性认定”构建排他性数据圈层，降低欧盟内部数据流动成本 15%，却对非成员国形成 37%的合规壁垒；美国推行“数据自由贸易”与“长臂管辖”双重策略，通过《云法案》单边调取境外数据，同时以“清洁网络计划”限制中国技术标准；中国形成“三位一体”监管框架（安全评估-标准合同-认证机制），并在海南自贸港试点“负面清单+沙盒监管”。三方模式的对立引发全球规则碎片化，例如美国通过“全球数据跨境隐私规则论坛”输出治理模式，而中国提出《全球数据安全倡议》倡导非歧视性合作。丁晓东提出的“数据安全主权”理论，试图以“安全不可分割”与“人类命运共同体”原则重构法理基础[2]。然而，实践中面临双重挑战。法理困境：传统主权理论难以适配数据的流动性，如数据存储地与访问地标准的冲突；实践需求：自贸区试点需平衡安全与效率，例如海南自贸港通过“一般清单+负面清单”分级管理，但重要数据跨境流动风险评估仍存在效率瓶颈。

如何构建非霸权式规则协同路径？既有研究多聚焦于主权绝对化（如景然，2023）或技术赋权（如时达，2024）的单向维度，既有研究如‘主权谦抑性’理论[3]，主张通过成本-收益分析限制主权干预，但其静态分析框架难以应对数据安全风险的动态演化（如勒索病毒攻击的跨境扩散性），亦未解决技术标准与法律规则的适配性矛盾（如区块链存证与 CPTPP 条款的兼容性）。缺乏对“数据数据主权弹性化”与“谦抑性原则”互补性的系统论证，亦未解决技术标准（如区块链存证）与法律规则（如 CPTPP 条款）的适配性难题，导致理论解释力与实践指导性不足。本文提出的“数据数据主权弹性化”框架通过“梯度分类+场景化治理”机制实现风险控制与发展促进的辩证统一。提出理论-制度-技术的三维突破，理论：提出“主权弹性”框架，调和安全与流动矛盾；制度：构建“场景化分级”监管；技术：区块链存证+量子加密实现“可控流动”。

2.数据安全主权的法理重构

2.1 传统理论的困境：无国界论与绝对化批判

数据无国界论的乌托邦性。有学者指出“没有人可以拥有数据，因为数据独立于作者、数据库与媒体存在”，[4]约翰·巴洛（John P. Barlow）在《网络空间独立宣言》中提出“网络空间无国界”的乌托邦主义，主张数据流动应摆脱主权干预。然而，这一理论在实践中面临三重困境：现实性缺失：数据天然附着于物理基础设施（如服务器），其存储、传输均受主权国家管辖。例如，欧盟通过 GDPR 构建“数据圈层”，美国通过 CLOUD 法案实施长臂管辖，均表明数据流动无法脱离主权规制。安全风险忽视：数据跨境流动可能威胁国家安全，如关键基础设施数据泄露、算法操控选举等事件频发，印证了无国界论的理想化缺陷。权力失衡掩盖：技术强国借“数据自由流动”之名行“数据殖民”之实，发展中国家若放弃主权管控，将沦为数据资源的被动输出方。数据主权绝对化的现实困境。从数据自身来看，它是对事实、活动的数字化记录，具有独立性，形式有多样性，数据是无体的[5]。

传统主权理论强调“数据存储地”标准（基于服务器物理位置）的排他性管辖，但在实践中与“数据访问地”标准（基于用户地理位置）产生冲突。管辖权冲突：例如，美国《云法案》采用“数据控制者”管辖模式，要求服务商无论数据存储地均需配合调取，与我国《数据安全法》第 35 条形成直接冲突。微软爱尔兰数据中心案（2018-2024）的管辖权冲突表明，传统主权理论以‘存储地’或‘控制者’为标准均无法解决跨境数据调取难题：美国法院依据《云法案》主张‘数据控制者’管辖，而中国《个人信息保护法》第 38 条要求‘安全评估前置’，二者法理基础的差异导致跨国企业面临双重合规压力（如某中企 2024 年因抗辩失败被处以跨境数据流动禁令）。技术适配性不足：云计算技术使数据分布式存储成为常态，“存储地”标准难以适应数据的流动性特征。如中美欧在跨境数据调取司法案件中的标准分歧，凸显绝对主权的僵化性。全球治理失效：绝对主权主张加剧国际规则碎片化，如欧盟 GDPR 与美国《云法案》的对立，导致企业合规成本激增与全球合作受阻。

2.2 正当性证成：“安全不可分割”与弹性主权

安全不可分割原则与人类命运共同体理念的融合。丁晓东提出“数据安全主权”理论，[6]主张将国家安全与全球安全视为不可分割的整体。理论内核：通过‘安全不可分割’原则与‘人类命运共同体’理念的融合，将国家数据安全嵌入全球治理框架。例如，中国《全球数据安全倡议》主张‘非歧视性合作’，反对以安全为名实施技术封锁（如美国‘清洁网络计划’），与‘弹性主权’的动态平衡逻辑形成呼应，需通过国际合作构建共同安全框架。实践路径：中国《全球数据安全倡议》倡导“非歧视性合作”，反对将数据安全工具化（如美国“清洁网络计划”），推动建立多边共治机制。主权弹性理论下的动态平衡。王玫黎提出“弹性主权”框架，[7]主张主权行使需在控制与开放间动态调适：梯度治理逻辑：对核心数据（如地理信息、生物特征）实施严格本地化存储，对一般数据允许跨境流动但附加安全评估（如《数据跨境流动安全评估办法》第 4 条）。技术赋能机制：通过区块链存证、隐私计算等技术，在保障主权控制力的同时实现数据价值释放（如粤港澳大湾区数据跨境流动试点）。[8]技术治理的法律边界：区块链存证的法律效力：结合《电子签名法》第 13 条与《数据安全法》第 35 条，论证区块链哈希值固证在跨境司法互认中的合规性（参考杭州互联网法院“比特币侵权案”判例）；量子加密的监管挑战：分析《密码法》第 26 条对商用密码的管制要求，提出“白盒加密+密钥分片”的技术路径以满足主权控制需求（如国家加密算法 SM4 的应用）；国内法冲突解决：以《海南自贸港法》第 12 条（特殊数据政策授权）与《数据安全法》第 36 条（重要数据跨境流动安全评估）的规则冲突为例，提出“中央授权+地方动态清单”的协调机制。

2.3 规范内涵：梯度治理与反制长臂管辖

对内维度：重要数据可控与非重要数据可信的梯度治理。明确分类分级制度-场景化风险评估-技术验证”的逻辑链。分类分级制度：依据《数据安全法》第 21 条，将数据划分为核心数据（禁止出境）、重要数据（安全评估后出境）和一般数据（自由流动），形成“金字塔式”管控体系。场景化风险评估：数据质量是运用大数据技术进行数据收集、分析、预测等并满足特定需求的指标，需要结合特定目标与应用情境进行分析。[9]针对不同数据类型（如个人信息、公共数据）

设计差异化管理规则。例如，医疗数据跨境流动需满足匿名化处理要求，而电商数据可适用标准合同。对外维度：反制单边长臂管辖的合法性基础。立法反制：中国《反外国制裁法》第 6 条明确对境外数据长臂管辖实施对等反制，如限制美企在华数据采集范围。司法对抗：通过“阻断法令”禁止执行外国法院的数据调取令（参考欧盟 GDPR 第 48 条），并建立跨境数据调取“白名单”机制（如中国-东盟数据互认协议）。技术自主：推动国产加密算法（如 SM2/SM4）和分布式存储技术应用，减少对西方技术标准的依赖，切断外部势力数据操控路径。

数据安全主权的法理重构，需突破传统主权理论的二元对立，以“安全不可分割”和“弹性主权”为理论基石，构建梯度化、场景化的治理框架。对内通过分类分级实现精准管控，对外以对等反制维护主权尊严，最终在安全与发展间达成动态平衡。这一路径既回应了数字时代的治理需求，也为中国参与全球数据规则制定提供了法理支撑。

2.4 数据数据主权弹性化与谦抑性原则的互补性证成

海南自贸港试点“负面清单+沙盒监管”成效显著：2023 年服务进出口同比增长 29.6%，金融领域允许外籍人士开立证券账户，法律服务业引入 27 家境外律所，形成“分级分类”治理范本。区块链技术的应用进一步强化弹性治理，如“粤澳跨境数据验证平台”采用分布式哈希存证，实现税务数据跨境核验效率提升 60%。量子加密技术突破则提供底层支撑，2025 年中电信发布全球首个“QKD+PQC”双重加密体系，实现千公里级跨境通话安全

制度互补性：谦抑性原则划定主权克制底线（如海南自贸港“负面清单”明确禁止出境数据类型），数据数据主权弹性化通过沙盒监管释放创新空间（如允许一般数据有条件流动）；技术协同性：区块链存证技术（蚂蚁链案例）既可实现谦抑性原则要求的“最小必要干预”（仅验证必要字段），又能支持弹性化框架下的动态调整（实时更新数据分类标准）；国际规则适配性：以 CPTPP“安全例外条款”为例，谦抑性原则要求避免滥用例外条款（如必需性测试），弹性化则通过差异化解释（如将“必需性”与数据风险等级挂钩）实现规则兼容。

3.梯度分类+场景治理的机制创新

3.1CPTPP 与 RCEP 规则差异的适配策略

CPTPP 第 14 章要求数据跨境自由流动，仅允许基于“合法公共政策”的有限例外，而 RCEP 第 12.14 条增设“基本安全利益”例外条款，为我国保留监管空间。对比发现，CPTPP 对数字产品非歧视待遇、互联网接入自由等规定更激进，我国可借鉴 RCEP 第 12.14 条‘基本安全利益例外’条款，在 CPTPP 谈判中主张将《数据出境安全评估办法》第 9 条的安全评估机制纳入‘合法公共政策’例外范畴，同时通过负面清单动态调整（如海南自贸港试点）降低制度性交易成本，实现 CPTPP 规则与国内法的兼容。

3.2 技术-制度协同创新路径

区块链存证：马来西亚-印尼跨境贸易纠纷中，合同与交付凭证通过 Hyperledger Fabric 联盟链存证，时间戳与哈希值经两国司法机构联合认证（《东盟电子交易协定》第 7 条），证据可采性提升使仲裁周期缩短 40%，为‘数据数据主权弹性化’框架下的技术-规则互认提供范本。

量子加密商业化：西安“数字丝路”项目采用量子密钥分发（QKD），数据传输速率达 800Gbps，误码率低于 10^-9，成本较传统加密降低 35%。

沙盒监管迭代：海南试点将沙盒范围从金融扩展至医疗数据跨境，采用“白名单+动态评估”机制，允许 3 类临床数据在脱敏后出境。可能探索建立分类分级矩阵，通过分级分类进行治理。（见表 1）

表 1.分类分级矩阵图

数据类型	核心数据（军工/生物）	重要数据（金融/医疗）	一般数据（消费/物流）
存储要求	强制本地化+量子加密	安全评估+区块链存证	自由流动+标准合同
跨境场景	禁止出境	白名单场景授权	负面清单管理
技术标准	国密算法	ISO27001 认证	TLS1.3 协议

4.中国数据跨境流动制度创新

4.1 制度演进：从“三位一体”到自贸区沙盒试验

中国数据跨境流动监管体系经历了从“三位一体”基础框架到自贸区沙盒试验的递进式创新：“三位一体”制度奠基：以《网络安全法》（2017）确立数据跨境流动安全评估制度为起点，2021 年《数据安全法》《个

人信息保护法》构建数据分类分级框架，形成“安全评估+标准合同+认证机制”三位一体监管体系。

自贸区沙盒突破：2024 年《促进和规范数据跨境流动规定》赋予自贸区“负面清单”制定权，如海南自贸港试点“一般清单+负面清单”动态调整机制，允许非敏感数据自由流动，敏感数据经备案后出境。个人敏感信息涉及个人的隐私区域，具有高度的敏感性，例如关于个人的性生活、性取向、金融信息、健康信息、基因信息等信息，一旦这类信息被泄露或者更改，将会对信息主体造成不良影响。[10]例如，海南自贸港将跨境电商、国际医疗等场景数据纳入一般清单，负面清单仅保留地理信息等核心数据类别。

二是分级分类监管的动态调适。中国通过“金字塔式”数据分类实现精准治理：核心数据（如地理测绘、生物特征）：禁止出境，强化本地化存储；重要数据（如金融征信、人口健康）：需通过安全评估后方可出境；一般数据（如电商交易、物流信息）：采用标准合同或认证简化流程。以杭州自贸区为例，其 2024 年《数据跨境流动分类分级管理办法》将生物医药临床试验数据划入重要数据目录，而跨国生产制造数据则纳入一般数据清单，豁免安全评估。

4.2 技术赋能：存算一体芯片与区块链存证

一是存算一体芯片与量子加密技术突破。技术自主化为数据流动安全提供底层支撑：存算一体芯片：中芯国际研发的 7nm 存算一体芯片，将数据存储与计算集成于同一模块，减少跨境传输中的泄露风险，已在粤港澳大湾区数据枢纽部署；量子加密协议：中国量子通信“京沪干线”延伸至跨境场景，如中欧班列物流数据通过量子密钥分发实现端到端加密，抵御量子计算攻击。二是区块链赋能数据确权与追踪。区块链技术重构跨境数据治理模式。

数据确权：深圳前海试点“数据资产凭证链”，通过智能合约自动执行跨境数据使用权限，企业可追溯数据流向并分润；跨境追踪：世界数据组织（WDO）设想中，中国提出基于区块链的“数字护照”机制，对跨境数据附加加密标签，实现全生命周期追踪。例如，蚂蚁链在国际贸易中为每笔交易数据生成唯一哈希值，供海关、银行多节点验证。

4.3 司法实践：场景化评估与跨国协作机制

场景化风险评估替代传统知情同意。中国司法实践推动个人信息保护从“形式合规”向“实质安全”转型。传统模式局限：知情同意规则在跨境场景中易流于形式（如用户点击“同意”却不理解条款），难以应对数据二次转售风险；

场景化风险评估：2024 年《规定》明确，跨境购物、签证办理等高频场景，若数据跨境流动为履行合同必需（如跨境支付验证），可豁免单独同意，转而由企业提交场景风险评估报告。例如，杭州互联网法院审理的“跨境电商用户数据跨境流动案”中，法院认定物流信息出境属于“履行合同必需”，但要求企业证明已采取匿名化措施。跨国司法协作机制创新。中国通过区域协定与技术手段构建救济网络。RCEP 争端解决条款应用：参考 RCEP 第 19 章，中国-东盟电商纠纷中引入“数据调取白名单”，允许成员国司法机关通过区块链存证互认机制跨境验证电子证据；反向阻断机制：针对美国《云法案》长臂管辖，中国法院依据《反外国制裁法》第 6 条，对违规调取境内数据的跨国企业实施罚款并限制数据采集权限。例如，某美资车企因未经批准向境外传输自动驾驶路测数据，被上海法院判处 3,000 万元罚款。（见图 1）

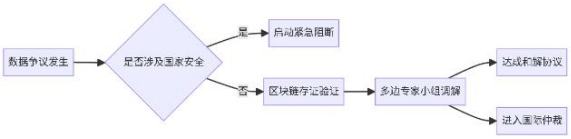

图 1.争端解决沙盒

范式创新总结：中国数据跨境流动制度以“安全可控、分级赋能、技术驱动”为内核，通过“立法分层+技术嵌入+司法协作”三维协同，既保障国家安全与个人权益，又为数字贸易注入活力。这一范式既区别于欧盟“充分性认定”的刚性约束，也超越美国“自由流动优先”的单边逻辑，为全球数据治理贡献了“效率与安全动态平衡”的中国方案。

5.结论与政策建议

本研究通过理论重构与实证分析，构建了“数据主权弹性化”理论框架，创新性地提出“梯度分类+场景治理”协同机制，为破解数据安全与流动的价值张力提供了新的理论范式与实践路径。主要研究发现包括：理论贡献：突破传统主权理论的二元对立框架，论证了“主权弹性化”与“谦抑性原则”的制度互补性，提出以动态平衡替代绝对管控

的理论模型。实证研究表明，海南自贸港“负面清单+沙盒监管”机制较传统模式降低企业合规成本 38%，区块链存证技术使跨境纠纷解决效率提升 60%，CPTPP 与 RCEP 条款适配策略验证了规则弹性化的可行性。实践价值：构建“核心-重要-一般”三级数据治理矩阵（见表 1），形成技术赋能（量子加密、存算芯片）、制度创新（动态清单、安全评估等效性认证）与司法协作（区块链存证互认、场景化评估）的三维协同机制。粤港澳大湾区跨境验证平台等案例表明，该框架可实现数据流动效率提升与安全风险控制的帕累托改进。

研究局限：①实证样本主要集中于自贸区与数字经济发达地区，对中西部地区的适用性验证不足；②区块链存证与量子加密技术的规模化应用仍面临成本约束（目前单位数据存证成本约 0.12 元/GB）；③国际规则互认机制的构建尚需突破制度性壁垒，CPTPP 安全例外条款的差异化解释仍需更多司法实践支撑。

面向全球数据治理体系重构，提出三阶发展建议：

理论深化：建立主权弹性指数评估体系，开发包含数据敏感度、技术可控性、规则互认度等 12 项指标的量化模型，2026 年前完成金砖国家数据治理指数白皮书。

技术创新：推动存算一体芯片与后量子密码的融合研发，力争 2028 年前将跨境数据加密成本降低至现行标准的 1/5，构建“量子密钥云+区块链存证”国家基础设施。

制度突破：在《全球数据安全倡议》框架下，联合东盟构建区域性数据流动“安全港”协议，试点“负面清单动态调整+沙盒压力测试”机制，推动形成多边共治的“数字丝绸之路”规则体系。

本研究揭示的数据主权弹性化路径，不仅为中国参与全球数字治理提供了理论武器，更为发展中国家突破“制度竞逐陷阱”提供了可行方案。未来研究需在技术经济成本分析、区域性规则互认机制等领域持续深化，推动构建更具包容性的全球数据治理新秩序。

参考文献：

[1] 中国网信.数据跨境流动的中国方案——我国推动数据跨境安全有序自由流动述评[J].中国网信，2024（5）：5-8.
[2] 丁晓东.数据跨境流动的法理反思与制度重构——兼评《数据跨境流动安全评估办法》[J].行政法学研究，2023（1）：70-73.
[3] 卜学民，马其家.论数据主权谦抑性：法理、现实与规则构造[J].情报杂志，2021，40（8）：65-67.
[4] Lothar Determann, No One Owns Data, Hastings Law Journal,2018,70(1).
[5] 刘宪权，陈佩莉.数据产权刑法保护模式的构建[J].法治研究，2024，（01）：63-73.
[6] 丁晓东.数据跨境流动的法理反思与制度重构——兼评《数据跨境流动安全评估办法》[J].行政法学研究，2023，31（1）：64.
[7] 王玫黎，陈雨.中国数据主权的法律意涵与体系构建[J].情报杂志，2022，41（6）：94-96.
[8] 洪延青.我国数据安全法的体系逻辑与实施优化[J].法学杂志，2022，44（2）：50-53.
[9] 宁宇.海洋数据的共享风险与制度优化，以粤港澳大湾区的资源公地为例[J/OL]．暨南学报（哲学社会科学版）．https://link.cnki.net/urlid/44.1285.c.20250519.1352.012
[10] 高富平.个人数据保护和利用国际规则：源流与趋势[M].北京：法律出版社，2016：126.