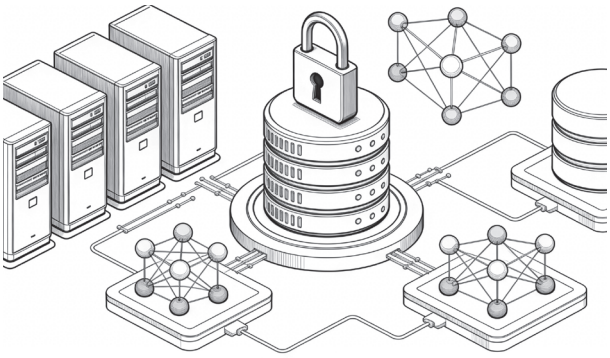
可信数据空间建设的法律规制研究

文丨 吴纪树

可信数据空间作为数据要素市场化配置的核心基础设施，已成为破解“数据孤岛”与“信任赤字”的关键路径，但数据流通伴随着安全风险，必须加强可信数据空间建设的法律规制，为我国 2028 年建成 100 个以上可信数据空间的建设目标提供制度支撑。



（配图由 AI 生成）

问题的提出

在数字经济时代，数据成为了社会的核心生产要素，其流通效率直接决定要素价值的释放程度。但大部分企业数据“沉睡”在本地服务器中，没有发挥其应有的价值，反而数据泄露、非法利用、隐私侵犯等数据安全事件却屡有发生。为应对此困境，中共中央、国务院于 2022 年 12 月印发《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”），明确指出要“建立数据可信流通体系，增强数据的可用、可信、可流通、可追溯水平”。于是，可信数据空间应时而生，其通过融合区块链、隐私计算等技术与共识规则，构建起“数据可用不可见、可控可计量”的流通生态，故而被纳入国家数据要素市场化配置改革的核心布局之中。2024 年 11 月，国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》[以下简称《行动计划（2024—2028）》]，明确提出到 2028 年建成 100 个以上可信数据空间的目标。但这一战略的落地落实需要法律给予支持与回应，理论上亟待厘清可信数据空间各方主体的权利义务关系，实践上亟待解决数据权属界定、跨境流动合规、算法公平保障等现实难题。

我国可信数据空间法律规制困境

数据权属界定不清

现有法律规定在应对可信数据空间权属争议时尚显乏力。一是原始数据与衍生数据权属划分不清。尽管最高人民法院指导性案例 264 号确认了数据处理者对衍生数据产品的合理利用权，但对企业基于公共数据加工形成的衍生数据的经营权归属与报酬支付标准仍缺乏明确规定。二是“三权分置”原则落地困难。持有权与经营权的权利边界模糊，导致收益分配纠纷频发，虽然一些企业的数据空间通过智能合约实现了分成，但缺乏全国统一的规则支撑。三是个人数据授权难题。用户在可信数据空间中难以有效控制数据的使用范围，且授权撤回机制不完善。最高人民法院指导性案例 265 号虽否定“一揽子授权”的合法性，但未明确动态授权实现的具体路径。

责任划分体系模糊

由于可信数据空间涉及数据运营方、数据提供方、技术服务方等多方主体，而当前相关法律规则并未明确主体责任的边界，导致现实中很多纠纷难以得到解决。数据运营方作为核心主体，其安全保障义务的范围与标准也不清晰，如国内一些可信数据空间产品，虽建立了安全防护体系，但立法未明确其对第三方数据泄露的责任承担标准；数据提供方的源头责任与运营方的管理责任划分模糊，发生数据泄露时，难以区分是提供方的数据质量问题，还是运营方的技术防护缺陷；技术服务方的责任认定缺乏依据，隐私计算技术提供商是否承担连带责任存在争议。

算法治理机制缺乏

当前我国可信数据空间中的算法风险缺乏有效规制。一是技术标准碎片化与适配困境。尽管国家标准委员会制定的《可信数据空间技术架构》为我国可信数据空间标准化建设做出了一定的努力，但全国统一的技术与管理标准尚未形成。二是权责划分模糊与协同障碍。“三权分置”失效，

数据提供方、使用方及运营方角色重叠，各方权责未明确，当算法错误引发风险时，数据质量与技术漏洞的责任归属无法界定。三是透明度缺失与审计失效。算法黑箱的比较问题突出，沙箱内隐私计算过程难以追溯，企业往往以“商业秘密”为由规避算法披露义务，司法与监管机构缺乏获取技术细节的有效手段。

跨境流动规制不足

从实践来看，粤港澳大湾区等跨境可信数据空间面临着制度性冲突。一是管辖权确定困难，数据存储地、处理地、主体所在地等连接点分散，广州互联网法院探索性地提出了综合多因素认定管辖权的思路，但仍未形成明确的标准。二是规则适用冲突。我国《数据出境安全评估办法》与欧盟《一般数据保护条例》（GDPR）、美国《云法案》（CLOUD Act）的要求存在不小的差异，跨境电商数据空间需通过数据元件化处理才能满足双重合规要求。三是互操作性不足。不同法域的数据标准与安全协议存在不兼容的问题，欧盟通过《欧洲健康数据空间条例》（EHDS）对电子健康记录格式进行了统一，而我国尚未形成类似的统一标准。四是数据的分类分级差异。我国重要数据目录与欧盟受限数据范围存在重叠，但并不完全一致，导致跨境数据在分类认定方面存在困难。

我国可信数据空间法律规制的完善路径

构建分层分类的权属确权体系

1. 完善立法确权规则

在修订《数据安全法》或者制定可信数据空间专门立法中，明确可信数据空间权属规则，细化“数据二十条”关于“三权分置”原则的适用标准规定。一是公共数据方面，确立“政府持有－授权运营－社会使用”的权属模式，明确授权运营的条件、程序及收益分配规则，对用于公共治理的数据实行有条件无偿使用，用于产业发展的数据则实行有条件有偿使用；二是企业数据方面，区分原始数据与衍生数据，原始数据归提供方持有，衍生数据的经营权归加工方所有，但需向原始数据提供方支付合理报酬，报酬计算应参考数据贡献度、使用频率等因素；三是个人数据，赋予用户“授权－撤回－删除”的完整控制权，建立基于智能合约的动态授权机制，用户可实时查看数据使用情况并调整授权范围，可参考《欧盟健康数据空间条例》的端口迁移权设定经验，允许用户将个人数据在不同数据空间进行迁移。

2. 建立权属登记制度

依托全国数据交易场所建立统一的数据权属登记平台，对可信数据空间中的数据资产进行登记。登记内容应包括数据类型、权属主体、使用范围、期限、技术加密方式等，登记结果作为权属认定的重要证据。如具体到数据信托登记方面，我们可以总结、提炼上海的实践经验，引入信托财产独立登记制度，要求受托机构必须将数据资产纳入独立的存管账户中，实现权属登记与风险隔离的法定化，确保其独立性与可追溯性。建立登记异议处理机制，当事人可向登记机构申请复核或提起行政诉讼。推动登记平台与可信数据空间技术架构对接，实现权属信息的自动更新与验证，如数据授权使用时自动同步登记信息。

3. 规范收益分配机制

确立“市场评价贡献、贡献决定报酬”的分配原则，可在立法中明确收益分配的考量因素（资源数量、使用频率、技术投入等）。鼓励通过智能合约实现自动分配，如在企业数据空间中，原始数据提供方可按使用次数获得实时报酬。关于公共数据衍生收益，可实行“政府统筹＋社会共享”模式，部分收益用于数据空间建设与维护，另一部分用于公共服务提升。关于个人数据收益，要建立“用户主导＋平台代持”机制，用户可通过授权使用获得相应报酬。

建立清晰可辨的责任划分机制

1. 明确多主体责任边界

今后立法要明确不同主体的责任类型与归责原则。一是数据运营方须承担核心责任，包括数据安全保障、算法合规、交易监管、权属登记协助等，要建立“架构内生、预防前置”的数据安全责任体系。二是数据提供方承担源头责任，确保数据来源合法、质量合格，对提供虚假数据或侵权数据造成的损害承担全额赔偿责任。三是技术服务方在未尽到合理注意义务时承担过错责任，如隐私计算技术提供商未按标准提供服务导致数据泄露的情形。四是数据监管方承担监督责任，未履行监管职责导致重大数据安全事件的，要追究相关人员行政责任。

2. 建立过错推定责任原则

对数据运营方实行过错推定责任，当发生数据泄露、算法偏见、权属纠纷等损害时，由运营方举证说明自己履行了法定义务，无法举证的要承担责任。这一规则既强化了运营方的责任意识，又降低了受害方的举证难度，恰好符合可信数据空间技术的复杂性特点。与此同时，还必须明确运营方法定义务的具体内容，包括定期安全评估、算法公平性测试、数据访问日志留存（建议至少6个月）、应急响应机制建设等。特别注意的是，对医疗、金融、应急等高风险行业的数据空间，则必须严格实行责任原则，只要发生重大安全事件，无论运营方是否有过错，均需承担惩罚性赔偿责任。

3. 完善追责与追偿机制

可信数据空间的法制建设，必须明确责任追究的流程与方式，监管

部门可对违法运营方处以罚款、吊销资质、责令停业等处罚，对构成犯罪的，要依法追究刑事责任。建立内部追偿机制，运营方承担责任后，可向存在过错的数据提供方、技术服务方追偿，追偿比例根据过错程度确定。鼓励通过商业保险转移风险，开发数据安全责任保险产品，强制高风险数据空间运营方投保，降低赔付压力。建立责任纠纷快速处理机制，设立数据纠纷仲裁委员会，可优先通过仲裁解决责任争议，为纠纷解决提供更多救济渠道。

完善算法公平的治理制度

1. 建立算法透明制度

要求可信数据空间的运营方承担公开算法基本信息的法律义务，包括但不限于算法名称、用途、决策逻辑、训练数据来源、可能的偏见风险等。对高风险算法，如信用评估、权限分配、数据匹配算法，实行事前审查与事后披露制度，需向监管部门提交算法说明书与公平性评估报告，通过审查后方可上线。运营方运用算法技术需要可视化，为用户提供算法决策的解释服务，如用户对数据授权结果有异议，运营方需以通俗方式说明决策依据。此外，还要建立算法透明度分级机制，根据风险等级确定公开范围与详细程度，平衡透明度与商业秘密保护。

2. 规范算法开发使用

可信数据空间立法需要明确算法开发的合规要求，禁止设置歧视性参数，训练数据需符合多样性要求，避免单一来源导致的偏见。数据运营方要建立算法测试机制，在上线前进行公平性测试、安全性测试、稳定性测试，并邀请第三方机构参与评估。与此同时，需要建立算法审计制度，定期由第三方机构对算法进行合规审计。审计结果向监管部门备案，建议对高风险算法每季度审计一次，普通算法每年审计一次。

3. 明确算法责任划分

完善算法公平治理规则，还需要构建“开发者－运营者－审计者”的责任链条。算法开发者承担设计责任，以确保算法符合公平原则与安全标准。运营方承担使用责任，以确保对算法运行过程进行监控，及时发现并纠正偏见。第三方审计机构承担审计责任，以确保如实出具审计报告，对虚假审计承担连带责任。当算法偏见侵权发生时，我们可直接根据各方过错程度划分责任。开发者设计存在缺陷的承担主要责任，运营方未履行监控义务的承担次要责任，审计机构未发现问题的承担补充责任。

构建安全便利的跨境流动规制体系

1. 制定专门跨境规则

针对粤港澳大湾区等跨境场景，制定有针对性的《跨境可信数据空间管理办法》，明确具体规制规则：一是管辖权方面，要采用“主要利益中心”标准，综合考虑数据空间运营中心所在地、主要数据处理地、当事人合意等因素，合理认定管辖权，避免管辖权冲突；二是准入管理方面，要建立“白名单”制度，符合安全标准、技术规范的跨境数据空间可免于安全评估，进一步简化合规流程；三是数据标准方面，要制定粤港澳三地统一的数据分类分级标准、安全评估标准、接口标准，实现三地数据互认，建议先在医疗、金融等领域试点统一数据格式；四是争议解决方面，要建立跨境数据纠纷协同解决机制，因法域有别，建议由三地法院、仲裁机构组成联合委员会，负责协调裁判尺度与执行协助。

2. 加强国际规则协调

积极参与全球数据治理规则制定，要在亚太经合组织（APEC）跨境隐私规则（CBPR）体系中发挥更大作用，积极推动将我国可信数据空间标准纳入国际规则体系之中。与欧盟、美国等建立规则互认机制，探索“安全港”模式的适用，对符合我国安全标准的外国数据空间，应当减少不必要的重复评估。在科研、物流等领域建立区域跨境数据空间，实行“数据本地存储＋授权访问”模式，敏感数据本地存储，经安全评估后授权境外访问。要依托“一带一路”倡议，推动与东盟国家建立跨境数据空间合作网络，构建统一的数据安全合作框架。

3. 强化技术保障措施

在跨境可信数据空间建设规制实践中，要全面采用量子密钥分发、同态加密等高级安全技术，筑牢数据跨境传输与交互的安全防线。创新推行“数据元件化处理”机制，将需要跨境流通的完整数据拆解为互不关联、不具备独立敏感价值的基础元件，严格按照监管要求完成跨境传输，再于境外遵循预设规则精准重组使用，从源头降低数据跨境流通的合规风险。此外，还要加快跨境数据安全评估自动化平台建设，依托智能算法实现评估流程的全线上化、智能化运作，自动完成数据敏感程度筛查、风险等级判定等关键环节，大幅缩短数据评估周期，切实减轻企业的数据安全合规成本负担。

作者简介：吴纪树 中共重庆市万州区委党校副教授

责任编辑：杨佳宇
投稿邮箱：zhouhl@staff.ccidnet.com