政务数据开放共享中的安全治理困境与破解路径——基于数据确权与流通机制的分析

梁媛 张敏 姚雨秋

陕西省网络与信息安全测评中心，陕西西安，721000；

摘要：随着数字经济发展与国家治理现代化推进，政务数据开放共享成为提升政府治理效能、优化公共服务、激发社会创新活力的关键举措。然而，数据安全风险与安全治理困境同步凸显，核心症结在于数据确权模糊与流通机制不完善。本文从数据确权与流通机制双重视角，系统剖析政务数据开放共享中安全治理面临的确权争议、流通风险及治理体系缺陷，进而从制度构建、机制优化、技术支撑和协同治理等维度提出针对性破解路径，为构建安全可控的政务数据开放共享体系提供理论参考与实践指引。

关键词：政务数据；开放共享；安全治理；数据确权；流通机制

DOI：10.69979/3041-0673.26.02.077

1 引言

1.1 研究背景

数字时代，数据成为生产要素后，国家鼓励数据流通，政务数据开放共享、公共数据授权运营、企业数据的社会化开发利用等正打破平台的原有边界，政务、公共服务、科技、文化等领域的平台也开始向经济功能延伸，平台方主体增多，平台经济的范畴将进一步扩大[1]。国家通过《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》《政务数据共享条例》等构建政务数据开放共享制度框架。

由于政务数据开放共享的势态迅猛，传统的政务数据安全治理模式不足以支撑当前的数据安全合规需求[1]，一方面，政务数据涵盖个人隐私、商业秘密及国家安全信息，泄露、滥用或篡改将威胁个人权益、市场秩序与国家安全；另一方面，过度强调安全而限制数据流通，会阻碍数据价值释放。如何在安全前提下推动政务数据有序开放共享，成为当前亟待解决的重大课题。

1.2 研究意义

（1）理论意义：数据确权的难点源于数据自身特性，数据的概念需依赖具体场景和语境才能明确[2]。梳理数据确权、流通机制与安全治理的内在关联，深入剖析安全治理核心困境，丰富数据安全治理理论体系，为后续研究提供理论基础与分析框架。

（2）实践意义：针对安全治理困境，提出基于确权与流通机制优化的破解路径，为政府部门制定政策、完善制度、提升治理能力提供参考，推动政务数据在安全可控前提下实现价值最大化。

1.3 国内外研究现状

（1）国外研究：起步较早，积累了数据开放理念、模式与实践经验。例如，欧盟通过《通用数据保护条例》（GDPR）构建严格数据保护框架，明确数据确权与流通安全规则；美国侧重市场化导向，通过数据信托等机制探索流通与安全的平衡。但国外研究多聚焦个人数据保护与市场驱动的数据流通，对政务数据这一特殊类型数据的安全治理关注不足。

（2）国内研究：围绕政务数据开放共享的意义、模式、障碍等展开广泛探讨，安全治理领域侧重技术防护、法规建设与监管机制，但缺乏从数据确权与流通机制视角的系统性研究，尚未形成基于这两大核心要素的整体性破解方案。

2 政务数据开放共享安全治理的理论基础

2.1 核心概念界定

（1）政务数据：政务数据是指政府在履行其职能过程中产生、收集、存储、处理和使用的数据，这些数据通常涉及政府决策、公共服务、社会管理、经济调控等多个方面[3]。

（2）数据确权：明确数据所有权、使用权、收益权、处分权等权利的归属与内容，以及权利行使与保护规则，是数据流通与安全治理的基础，直接影响数据利用效率与安全保障水平。

（3）政务数据流通机制：政务数据在政府部门间、政府与企业间、政府与公众间传输、共享、交换和利用的规则、流程与方式总和，完善的机制可保障数据有序流动、提升利用价值并防范安全风险。

（4）安全治理：通过法律法规、政策制度、技术手段、组织管理等综合方式，保障政务数据开放共享中的完整性、保密性、可用性与真实性，目标是在促进数

据开放的同时，有效化解安全风险。

2.2 数据确权与政务数据流通的内在关联

数据确权是政务数据流通的前提，只有明确权利归属，数据主体才愿参与流通，使用者才能明晰权责，避免因权利模糊引发纠纷与风险。同时，政务数据流通反作用于数据确权，数据流通过程中，数据形态与价值不断变化，可能产生新的权利主体与内容。

2.3 安全治理在政务数据开放共享中的价值定位

安全治理是政务数据开放共享的重要保障，为数据流通提供稳定的环境与技术支撑，防范政务数据泄露、滥用等风险，保护数据主体权益与国家、社会公共利益，若缺乏安全保障，数据开放共享难以持续推进。同时，安全治理需与开放需求平衡，过度管控会限制数据流通、降低利用价值，缺乏有效治理可能会导致风险积聚，损害数据开放公信力。因此，安全治理的核心是找到“安全”与“开放”的平衡点，实现政务数据高效、可持续共享。

3 政务数据开放共享中安全治理的现实困境

3.1 数据确权困境：权属界定模糊与权利行使冲突

（1）权属界定模糊不清

所有权争议：政务数据多由政府履职产生或收集，所有权归属存在分歧——部分观点认为其属国家，另一部分观点认为数据主体贡献了核心信息，应享有部分所有权。权属模糊导致数据开放中缺乏明确责任主体，难以有效管理与保护。

权利内容划分不明：即便明确所有权，使用权、收益权、处分权的边界仍不清晰。例如，政府作为数据管理者，使用权范围如何界定？数据开放产生的收益如何分配？这些问题未解决，易引发权利滥用与利益冲突。

（2）多元主体权利冲突凸显

个人权利与公共利益冲突：政务数据含大量个人信息，个人享有隐私权、知情权等，而数据开放旨在提升治理效能、实现公共利益，二者易产生矛盾。

政府部门间权利冲突：各部门积累的政务数据存在交叉关联，但因缺乏统一确权机制，部门常将数据视为“私有财产”，不愿共享，形成“数据壁垒”，降低整体利用效率。

使用方与数据主体冲突：数据使用方利用政务数据创新时，可能超出授权范围。

3.2 数据流通机制障碍：安全风险积聚与管控不足

（1）隐私泄露风险突出

脱敏技术应用不规范：数据开放前需对敏感信息脱敏，但部分地区、部门存在“脱敏不足”或“过度脱敏”的问题。

聚合分析引发隐私威胁：单一数据集脱敏后风险较低，但多源数据聚合分析，可还原个人生活轨迹、消费习惯等隐私信息，形成“数据画像”式泄露。

（2）数据跨境流动隐患显著

全球化背景下，政务数据跨境流动日益频繁，但各国数据安全法规、标准差异较大。部分国家要求境外企业将本地收集的政务数据存储于境内，或对跨境流动设置严格审批，影响国际合作与数据共享，同时，数据跨境可能被境外滥用、窃取，威胁国家数据安全。

（3）标准与技术支撑薄弱

格式与接口不统一：不同地区、部门的政务数据格式、接口标准差异大，导致数据流通中难以兼容整合，增加处理成本，且数据转换中易出现误差，引发安全风险。

安全技术能力不足：部分地区、部门缺乏数据加密、访问控制、安全审计等核心技术，难以防范传输、存储、使用中的风险；同时，数据安全监测与应急响应能力弱，无法及时发现、处置安全事件。

3.3 安全治理体系与能力不足：制度方式与协同乏力

（1）监管机制不健全

数据安全监管涉及多部门，但职责划分模糊，存在“多头监管”，事故发生后难以明确责任，影响监管效率。依赖人工检查、事后处罚等传统手段，缺乏对数据全生命周期的动态监管与实时监测，监管手段单一，风险预警与主动防范能力不足。

（2）责任划分与追溯困难

数据开放涉及产生者、收集者、管理者、使用者等多主体，因缺乏明确的责任划分机制，事故发生后难以确定责任方，导致“追责难”；同时，数据流转经过多环节，修改、传输轨迹难以全程追溯，进一步增加责任认定难度。

4 政务数据开放共享安全治理困境的破解路径

4.1 健全政务数据确权制度体系

（1）明确权属划分规则

确立国家所有权主导原则：明确政务数据所有权归国家，政府部门作为受托人履行管理、利用职责，避免数据“部门化”“私有化”，保障公共属性与国家利益。

差异化划分数据权属：按数据类型制定规则——个人信息数据所有权归个人，政府享有有限使用权；商业秘密数据所有权归企业，政府仅可在法定范围内使用；公共数据所有权归国家，免费向社会开放。

（2）建立权利登记与流转制度

搭建全国统一的政务数据权利登记平台，记录数据所有权、使用权、收益权等权利主体与内容，实现“权

利可查”；规范权利流转程序，明确数据转让、许可使用的条件与流程，保障合法流转。

（3）完善权益保护机制

明确个人、企业在数据开放中的权利，如知情权、同意权、更正权、删除权等；建立侵权赔偿制度，对泄露、滥用数据的行为严厉处罚，维护数据主体合法权益。

4.2 优化政务数据流通全流程安全管控机制

（1）构建分级分类流通规则

按数据敏感程度与重要性分级：数据分级则应根据数据的敏感性、重要性和潜在风险进行划分，如一般数据、重要数据、核心数据等。

（2）强化技术安全防护

制定数据脱敏、加密技术标准，规范技术应用——明确脱敏范围，采用国密算法等先进技术对数据传输、存储加密，防止非法窃取与篡改。

（3）建立安全评估与预警机制

定期开展数据流通安全评估，排查隐患；利用大数据、人工智能构建风险预警平台，实时监测数据流转，发现问题及时预警并处置。

（4）规范跨境流动管理

制定政务数据跨境流动管理办法，明确流动条件、审批程序；建立跨境安全评估机制，对涉及国家利益、个人隐私的数据严格审核；加强国际合作，推动形成数据跨境流动通用规则。

4.3 构建协同联动的安全治理保障体系

（1）完善法规与标准规范

提升法律层级与执行力，协调《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》《政务数据共享条例》等法规的衔接；制定数据确权、流通安全、技术防护等标准，形成统一规范的体系。

（2）健全跨部门协同监管机制

明确各部门监管职责，避免权责交叉；搭建跨部门、跨地区协同监管平台，共享监管信息，开展联合执法，形成监管合力。

（3）强化责任落实与追溯能力

建立数据安全责任制，明确各主体的安全责任，将其纳入绩效考核，对违规行为严肃问责；研发数据溯源技术，记录数据全生命周期流转轨迹，为责任认定提供依据。

（4）提升技术与应急能力

加大安全技术研发投入，支持加密、隐私计算、访问控制等技术创新；建立技术保障体系，为数据开放共享提供全流程技术支撑；制定数据安全应急预案，定期开展演练，提升事件处置能力。

（5）加强安全意识教育

面向政府工作人员、企业、公众开展数据安全培训与法规宣传，解读数据开放政策与安全要求，提升全社会数据安全素养，引导各方依法参与数据共享。

5 结论与展望

5.1 研究结论

（1）政务数据开放共享安全治理面临多重交织困境：数据确权模糊导致权利冲突，流通机制不完善引发安全风险，治理体系不健全削弱管控能力，三者共同制约数据开放共享的进程与效果。

（2）数据确权是安全治理的基础，明确权属可减少权利纠纷与风险；优化流通全流程管控是防范风险的关键，通过分级分类、技术防护等措施保障数据安全；构建协同治理体系是重要支撑，需依托法规、监管、技术等多维度形成合力。

5.2 研究展望

（1）深化新技术应用研究：探索区块链在数据确权、溯源中的作用，人工智能在风险预警、动态监管中的实践，提升治理智能化水平。

（2）聚焦跨境流动治理：结合全球化与数据主权需求，研究适配国际合作的政务数据跨境流动规则，平衡“开放共享”与“安全可控”。

（3）开展比较研究：总结不同地区、不同领域的数据安全治理经验，提炼可复制的模式。

（4）关注新兴风险治理：针对数据滥用、算法歧视等新型安全问题，研究治理策略，完善安全治理体系。

政务数据开放共享安全治理是系统工程，需政府、企业、公众等多方协同，通过制度完善、机制优化、技术创新、协同联动，实现“安全”与“开放”的良性互动，为数字经济发展与国家治理现代化提供有力支撑。

参考文献

[1]张晓,程建润,鲁汇智.平台经济：时空演进路径与增长机制[J].数据与计算发展前沿(中英文),2025,7(04):196-207.

[2]王瑞.“十四五”背景下地方政府政务数据安全治理研究[D].贵州财经大学,2024.DOI:10.27731/d.cnki.ggzcj.2024.000559.

[3]沈劼,刘晋名,姚迁.法律和经济学视野下的数据确权研究[C]//《信息安全研究》杂志社.2025 网络安全创新发展大会论文集.公安部第三研究所;,2025:46-49.DOI:10.26914/c.cnkihy.2025.017924.

[4]吴建南,权一章,王亚星.破解政务数据共享的“三不”难题——来自上海市 C 区的实践分析.公共管理与政策评论,2025,14(5):4-17.