面向违规导出风险的政务数据流通安全治理体系研究

王跃，莫莉娟，苏娜
中国信息通信研究院政务服务中心，北京 100036

摘要
违规导出是政务数据流通过程中面临的重大数据安全风险。从中观实践视角出发，梳理政务数据在政府信息系统中的存储分布情况，归纳了实践中政务数据前台、后台、共享、开放、运营、攻击6种数据导出流通通道，理清应重点关注的前台功能导出、前台接口导出、后台同步导出、后台操作导出、共享数据导出、运营数据导出6种典型的数据流通方式。其次，系统分析了安全合规要求及外部攻击、内部威胁、系统漏洞、合作方泄露等主要威胁的具体表现，进而围绕数据分类分级管控、外包管理与数据使用管理、精细化权限管理、导出规模与异常管控、泄露阻断与溯源管控、数据导出安全审计6个方面给出应对策略。在此基础上，提出一种面向违规导出风险涵盖管理落实、技术防护、运行实施三要素的政务数据流通安全治理体系方案，以高效应对违规导出这一重大风险，为政务数据流通安全治理提供参考。

关键词
违规导出；政务数据；数据流通；安全治理

中图分类号：G203 文献标志码：A doi：10.11959/j.issn.2096–0271.2024062

Research on the security governance system for the circulation of government data facing the risk of illegal export

WANG Yue, Mo Lijuan, SU Na
Government Service Center, China Academy of Information and Communications Technology, Beijing 100036, China

Abstract
Unauthorized data export is a significant data security risk in the circulation of government data. From a meso-level practical perspective, this study examines the storage and distribution of government data within government information systems. It identifies six data export and circulation channels in practice: front-end, back-end, sharing, openness, operation, and attack. Furthermore, it clarifies six typical data circulation methods that require special attention: front-end functional export, front-end interface export, back-end synchronized export, back-end operational export, shared data export, and operational data export. In addition, the study systematically analyzes security compliance requirements and the specific manifestations of major threats, including external attacks, internal threats, system vulnerabilities, and data breaches by partners. Based on this analysis, it proposes countermeasures focusing on six aspects: data classification and grading control, outsourcing and data usage management, granular permission

management, control over export scale and anomaly detection, leakage prevention and traceback control, and security audits for data exports. Building on these findings, the study introduces a security governance framework for government data circulation, which encompasses three key elements: management implementation, technical protection, and operational execution. The framework effectively mitigates the significant risk posed by unauthorized data exports and provide reference for the security governance of the circulation of government data.

Key words
illegal export, government data, data circulation, security governance

0 引言

2021年6月，《中华人民共和国数据安全法》正式发布，数据安全成为继网络安全、信息安全之后的又一焦点。2022年9月，国务院办公厅印发《全国一体化政务大数据体系建设指南》，围绕政务数据共享、政务数据开放提出一系列数据安全要求。2022年12月，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”）明确要求“强化数据安全保障体系建设，把安全贯穿数据供给、流通、使用全过程”。2024年，中央网络安全和信息化委员会办公室等四部门发布《互联网政务应用安全管理规定》，对政务应用的数据安全作出进一步规定。根据中国信息通信研究院发布的《数据要素白皮书（2022年）》，数据要素市场存在开放、共享、交易3种数据流通形式。从整体上看，在各类数据要素中，政务数据是政府部门及法律法规授权具有管理公共事务职能的机构和组织在依法履职过程中收集和产生的各类数据，也是公共数据的核心组成部分，其数据流通过程覆盖上述3种形式且具体方式多样。同时，政务数据包括大量的政府决策信息、行业运行信息、个人隐私信息与企业商业秘密，价值极大且高度敏感，因此强化面向政务数据的数据流通安全治理极为关键。

围绕数据流通安全领域，学术界已开展了一系列研究，宏观研究聚焦于探讨强化数据流通安全的着力方向与整体视图、架构、新技术应用等，微观研究则聚焦于细化讨论保障数据流通安全的具体举措与技术方案。在宏观方面，马乐存等人[1]基于顶层宏观视角，从数据主权、数据市场、数据流通3个层面，提出涵盖数据资产合规、交易机构合规、交易行为合规、交易安全合规、数据跨境合规的广义数据流通安全体系架构；刘业政等人[2]、高亚楠[3]从整体视角分别提出数据交易流通的总体角色视图与安全保障框架；李伟[4]则提出以确定数据权责为起点、以数据审计为依据进行数据体系设计，并从制度、技术、行业3个层面加强数据安全治理；张凤娜等人[5]、林宏峥等人[6]聚焦金融领域的数据流通特点，提出法规制度、安全技术等具体方向，讨论基于访问控制、半监督联邦学习等数据安全技术的应用，保障金融数据安全共享流通；Somma等人[7]聚焦数字孪生领域，提出采用分布式账本技术来解决物理世界和虚拟世界的数据流通安全问题；Shrivastava等人[8]聚焦医疗数据安全流通共享，提出统一电子病历系统类型和数据防护技术，从而提升患者数据的互操作性，并实现隐私保护。在微观方面，何安珣等人[9]、栾国春[10]、欧阳日辉[11]、付少雄等人[12]分别从隐私计算技术、区块链技术、

数据基础设施、标准与保障4个方面研究保障数据流通安全的举措。聚焦政务数据流通安全领域，周群等人[13]、李博等人[14]、陈静等人[15]、郑文阳[16]研究数据共享与开放专用通道的安全保障体系；孙杨等人[17]提出一种基于数据沙箱、区块链、安全计算的分布式数据交换系统技术方案；Jana[18]聚焦敏感信息泄露，提出通过计算数据流通路径来监测敏感信息泄露的框架。上述研究较系统地梳理了保障数据流通安全的主要着力方向，并对涉及的技术领域、专用流通通道等进行了详细讨论，但从整体上看，已有研究成果缺乏基于中观视角的实践落地，即面向政府、企业等的数据流通体系，从实施角度提出科学化、系统化的高效策略，探讨面向真实环境的数据流通安全体系化方案。由此可知，亟须聚焦政务数据领域，研究面向实践的政务数据多样化流通体系，全面分析安全治理框架的设计，以指导政府部门快速建立高效完备的政务数据流通安全治理体系。

高效的安全治理体系通常以重大风险挑战为驱动快速建立，并向目标安全体系持续演进、完善，数据安全与网络安全、信息安全紧密关联，各有侧重。从数据安全视角切入，违规导出数据是指在未经授权或违反相关法律法规、安全要求的情况下，将内部或受保护的数据以任何形式（如复制、传输、下载等）转移到外部环境或提供给未经授权的个人或组织的行为，而防范违规导出数据风险引发的数据泄露、数据滥用等事件，应是保障数据流通安全的首要目标，以确保数据在流通过程中被合规受控地转移到外部环境，并被授权主体合规利用。本文以重大风险为驱动，开展基于中观视角的实践研究，全面梳理政务数据流通通道，理清政务数据在政府信息系统中的分布与流向，明确政务数据的多样化导出流通方式。在此基础上，聚焦基于各数据通道的政务数据违规导出这一重大风险，分析国家相关合规要求及外部攻击、内部威胁、系统漏洞、合作方泄露等具体威胁，从而提出具有针对性的强化安全治理的策略，以提升政务数据流通安全保障能力，指导政府部门快速建立较完备的政务数据流通安全治理体系。

1 政务数据对外流通通道与导出流通方式

在部委及省、市级政府中，政务数据主要分布于政府实时生产类应用系统、政府大数据分析应用系统、政府专用流通类应用系统、政务中台及云平台设施四大类政府信息系统。政务数据在政府信息系统中的分布与流向如**图1**所示。政务数据通常产生于政府实时生产类应用系统，支撑政务服务、监管执法、统计监测等日常履职需求。部分政务数据被处理后进入政府大数据分析应用系统，支撑政府内部的决策，满足大数据分析与展示的需求。上述政务数据面向不同流通场景，基于不同规则流入政府专用流通类应用系统，包括政务数据共享系统（承载无条件共享数据及有条件共享数据）、公共数据开放系统（主要承载无条件开放数据）、公共数据授权运营系统（主要承载有条件开放数据），专门服务于政府内外（包括全国各地方各部门的政府单位、社会中的企事业单位）的数据流通。其中，政务数据共享系统用于支撑政务数据在全国各地方各部门政府之间的共享导出流通；公共数据开放系统用于支撑政务数据面向社会的开放导出流通；公共数据授权运营系统用于支撑较敏感的、以政务数据为核心的公共数据，以数据产品或数据服务形式的运营导出流通，进而

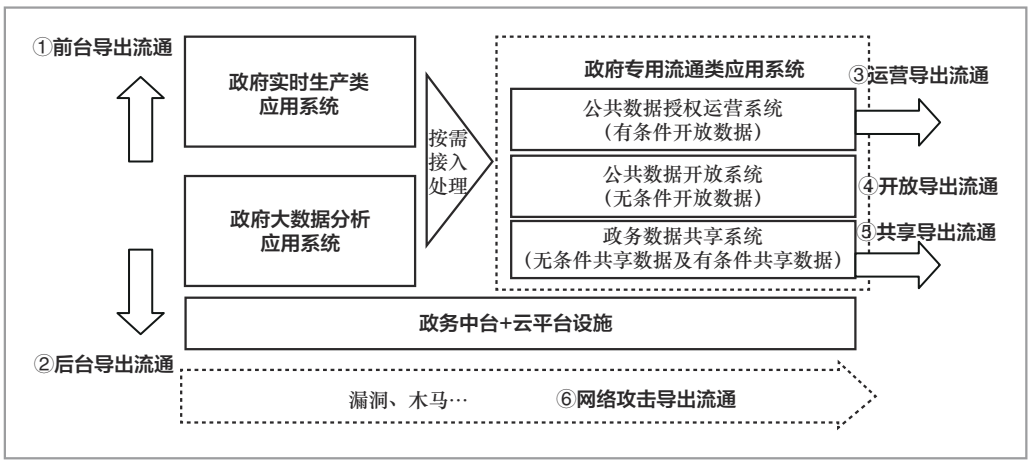

图1 政务数据在政府信息系统中的分布与流向

运营数据进入数据交易市场进行自由流通。最后的交易流通阶段脱离了政府直接管控或者不属于政府信息系统运行的边界范畴，因此，本文不对此进行讨论。底层支撑的云平台设施及相关运维系统、中间供调用的共性政务中台组件分别承载政府信息系统的运维与安全数据、部分业务数据，支撑上述应用系统的高效运行。

从政务数据对外流通的视角分析，可进一步梳理政务数据的对外流通通道。除基于政府专用流通类应用系统外，各地方各部门出于离线分析、业务协同、数据合作等履职需要，在实践中面向外包合作方、外部政府部门、企事业单位（如下属事业单位、管理服务的企事业对象等），可能同时构建了基于政府实时生产类应用系统、政府大数据分析应用系统、政务中台及云平台设施的导出流通通道。基于这些通道流通的政务数据在服务政府履职尽责方面发挥了重要作用，其基本属于政务数据在不同法人主体间的共享流通范畴。此外，政府信息系统中还可能存在因漏洞、病毒木马而产生的非法导出通道。整体上，根据数据源的分布及流向，可将导出流通通道划分为以下6种。

（1）基于政府实时生产类应用系统、政府大数据分析应用系统、政务中台及云平台设施的前台导出流通通道。一是基于数据离线分析、业务协同或数据合作等目的，面向系统外部用户（外部政府部门、企事业单位、专家、外包合作方等）设计开发的数据批量导出功能，外部用户登录系统后下载数据；二是基于业务协同需求，面向外部政府部门、企事业单位设计开发的专用数据接口，外部用户通过调用数据接口持续获取政务数据。

（2）基于政府实时生产类应用系统、政府大数据分析应用系统、政务中台及云平台设施的后台导出流通通道。一是基于业务协同、数据分析等目的，通过数据库同步等技术面向外部政府部门、外包合作方实现数据库选定范围（全部或部分）的库表导出，外部用户基于本地数据库进行分析应用；二是基于定期或临时业务需求，由外包合作方通过直接登录服务器后台、数据库后台来执行库表数据批量处理与导出操作。

（3）基于政府专用流通类应用系统的共享导出流通通道。基于国家数据共享体系，面向全国各级政府部门，经过分权分

层审批，跨部门、跨层级、跨场景提供无条件共享、有条件共享的政务数据资源。

（4）基于政府专用流通类应用系统的开放导出流通通道。面向社会公众，主要提供无条件开放的数据资源，因为该类数据资源敏感度较低，不是面向数据违规导出风险的数据流通安全治理的重点，但需要对个人敏感信息、企业商业秘密信息等进行前置的脱敏处理。

（5）基于政府专用流通类应用系统的运营导出流通通道。面向授权运营单位主要提供有条件开放的数据资源，并以公共数据授权运营方式，按照“数据二十条”提出的“原始数据不出域、数据可用不可见”要求，向社会提供数据产品与服务。

（6）基于系统漏洞、病毒木马的网络攻击导出流通通道。政府信息系统中可能存在系统漏洞、病毒木马等安全威胁，可能导致数据泄露，但其仍属于本身技术缺陷及外部攻击导致的传统网络安全治理应对范畴，因此不作为本文讨论的重点。

综上分析，面向违规导出风险的政务数据流通安全治理，应重点关注前台导出、后台导出、共享导出、运营导出4种流通通道，并需要针对前台功能导出、前台接口导出、后台同步导出、后台操作导出、共享数据导出、运营数据导出6种典型数据导出流通方式（见**表1**）的合规要求及安全威胁，提出针对性的应对策略与体系设计。

2 面向违规数据导出的合规要求与安全威胁

《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》《互联网政务应用安全管理规定》对政务数据处理活动作出一系列规定，其中面向数据导出这一关键操作主要提出3个方面的合规要求：一是关注导出的重要数据，即对政务数据实施分类分级管控，对重要数据、个人敏感信息、商业秘密进行重点保护；二是关注导出的重点对象，明确政府部门委托外包合作方建设和维护电子政务系统以及存储和加工政务数据，应当经过严格的批准程序，按照最小必要原则对外包合作方人员进行精细化授权，并应当监督外包合作

表1 政务数据流通安全治理应重点关注的典型导出流通方式

导出流通方式	数据源位置	导出对象	业务逻辑	导出特点
前台功能导出	政府实时生产类应用系统、政府大数据分析应用系统、政务中台及云平台设施	系统外部用户（政府、企事业单位、专家、外包合作方）	数据离线分析、业务协同、数据合作	按需批量导出
前台接口导出		外部政府部门、企事业单位	业务协同	持续导出获取
后台同步导出		外部政府部门、外包合作方	业务协同、数据分析	实时全量导出
后台操作导出		外包合作方	定期或临时业务需求（如数据分析等）	按需批量处理与导出
共享数据导出	政府专用流通类应用系统	全国各级政府部门	数据共享	按照审批方式导出
运营数据导出		授权运营单位	公共数据授权运营	原始数据不出域

方履行相应的数据安全保护义务；三是关注导出的操作权限，政府部门应当建立严格的授权访问机制，操作系统、数据库、机房等最高管理员权限必须由政府部门在编人员专人负责。

聚焦前台功能导出、前台接口导出、后台同步导出、后台操作导出、共享数据导出、运营数据导出6种典型的数据导出流通方式，进一步梳理其面临的外部攻击、内部威胁、系统漏洞、合作方泄露等主要威胁（见**表2**）。

（1）前台功能导出：一是系统前台用户与权限分配失控的风险；二是授权前台用户滥用导出权限，导致较大的数据流出风险；三是导出数据在用户终端发生本地泄露的风险。

（2）前台接口导出：一是数据接口未经政府部门充分审批与授权使用的风险；二是拥有接口调用权限的对象，超出约定使用范围调用、超量使用、二次转发数据等滥用风险；三是调用对象在本地泄露数据的风险。

（3）后台同步导出：一是数据库同步未经政府部门充分审批与授权使用的风险；二是授权后台同步导出对象在本地泄露数据的风险。

（4）后台操作导出：一是对后台操作人员的粗放授权风险，给过多人员赋权或赋予过高权限；二是授权外包合作方在建设与运维政府信息系统过程中误操作或恶意操作，引发数据泄露风险；三是外包合作方基于运维终端，通过拍照录屏、软件工具访问等方式在本地泄露数据的风险。

（5）共享数据导出：一是后台操作人员的粗放授权风险，给过多人员赋权或赋予过高权限；二是数据被共享接收方超出约定使用范围调用、超量使用、二次转发等滥用风险；三是共享接收方在本地泄露数据的风险。

（6）运营数据导出：一是没有满足公共数据授权运营“原始数据不出域、数据可用不可见”的要求，直接导出原始数据的风险；二是对授权开发者的粗放授权风险，给过多人员赋权或赋予过高权限；三是授权运营者在授权运营过程中误操作或恶意操作，导致原始数据、产品和服务数据被泄露。

3 政务数据流通安全治理策略研究与体系设计

3.1 治理策略研究

针对上述面向导出风险的合规要求及安全威胁，政务数据流通安全治理应从数据分类分级管控、外包管理与数据使用管理、精细化权限管理、导出规模与异常管控、泄露阻断与溯源管控、数据导出安全

表2 6种典型的导出流通方式面临的主要数据安全威胁

导出流通方式	主要数据安全威胁
前台功能导出	前台用户与权限失控、导出功能被滥用、用户终端本地泄露数据
前台接口导出	未经充分审批与授权使用、数据接口被滥用、调用对象本地泄露数据
后台同步导出	未经充分审批与授权使用、导出对象本地泄露数据
后台操作导出	后台用户粗放授权、授权外包合作方失控、运维终端本地泄露数据
共享数据导出	后台用户粗放授权、共享数据被接收方滥用、共享接收方本地泄露数据
运营数据导出	原始数据导出、开发者粗放授权、开发者行为失控

审计6个数据流通安全治理领域切入，采取以下针对性治理策略，以全面覆盖应对上述合规要求及安全威胁。

（1）数据分类分级管控：一是核心数据、重要数据、个人敏感数据、商业秘密进行加密存储，并在数据开发及数据导出前进行脱敏处理；二是限制重要数据、个人敏感数据、商业秘密每次导出的数量与导出频率，并应经政府部门充分审批与授权使用；三是核心数据不允许导出。

（2）外包管理与数据使用管理：一是充分评估外包合作方数据安全治理支撑保障能力，签订委托协议，明确并监督落实外包合作方的数据安全治理责任和义务；二是面向导出数据的各类用户，签订授权使用政务数据协议，明确并监督落实使用方的数据安全治理责任和义务。

（3）精细化权限管理安全：一是操作系统、数据库等最高管理权限由政府部门在编人员专人管控；二是政府信息系统前台导出功能，应基于不同角色进行最小化授权；三是面向操作系统、数据库、应用系统、政务中台及云平台设施等后台各类用户，实施最小化授权；四是面向授权运营的应用开发者，实施精细化授权。

（4）导出规模与异常管控：一是政府信息系统前台导出功能应对批量导出的范围、数量与频率进行限制；二是外包合作方必须通过堡垒机或管理平台等统一工具访问管理数据库、服务器等后台，并严格设置数据导出的安全策略；三是建立API安全管控设施，自动发现数据接口，并进行流量监测与分析，识别流量激增、二次代理等异常；四是推进后台同步导出方式向前台接口方式转变，严格监管通过后台同步导出的本地数据。

（5）泄露阻断与溯源管控：一是面向政府信息系统各类API及政务环境内本地终端网络出口部署数据泄露防护设施，阻断数据泄露；二是推进云桌面环境的部署，实现用户终端的集中统一管控，强化基于云桌面的数据开发行为、数据导出操作的安全监测与风险阻断；三是面向政府信息系统运维物理环境，强化智能视频监控，发现并阻断拍照录屏、物理介质转移等数据泄露路径；四是在各通道中广泛应用数据水印技术，面向各类数据导出行为、数据开发行为强化数据溯源能力；五是基于数据沙箱、可信数据空间、隐私计算等技术建立公共数据授权运营开发平台，确保原始数据不出域，支撑授权运营者导出数据产品和服务。

（6）数据导出安全审计：一是面向政府信息系统中具有批量导出的前台功能，对其操作日志进行全面记录，并定期开展审计；二是操作系统、数据库、应用系统、政务中台及云平台设施等开启后台操作审计日志记录，并定期进行审计，从而发现导出安全风险。

3.2 治理体系设计

基于上述安全治理策略，围绕政府实时生产类应用系统、政府大数据分析应用系统、政府专用流通类应用系统、政务中台及云平台设施，建立管理落实、技术防护、运行实施三位一体的面向违规导出风险的政务数据流通安全治理体系，如**图2**所示。

（1）管理落实

一是聚焦外包行为与数据提供行为，面向外包合作方与各类数据使用对象，审核签订委托与授权使用协议，并监督其落实安全责任；二是聚焦政府信息系统开发与运维管理，对系统批量导出前台功能的导出数量与导出频率进行限制，要求后台

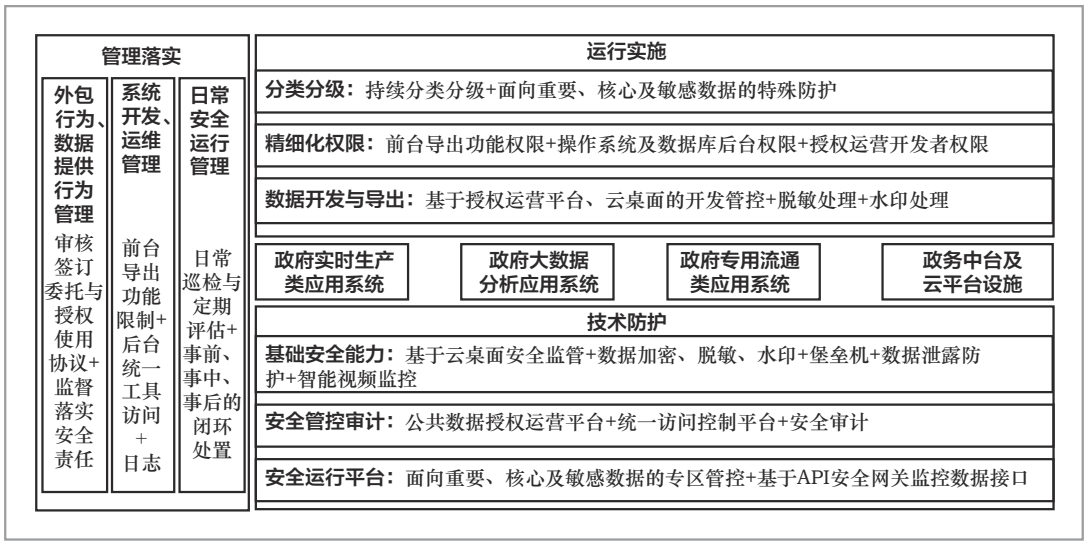

图2 面向违规导出风险的政务数据流通安全治理体系

访问通过堡垒机等统一工具进行访问管控，并保留数据导出的相关日志；三是聚焦日常安全运行管理，开展巡查与定期评估，实施事前、事中、事后的闭环处置管理。

（2）技术防护

一是聚焦基础安全能力，基于云桌面实现面向数据开发行为、数据导出操作的安全监测与风险阻断，构建数据加密、脱敏、水印的数据安全技术支撑组件，部署堡垒机、数据泄露防护与智能视频监测设施；二是聚焦安全管控审计，构建面向数据开发、保障“原始数据不出域”的公共数据授权运营平台，打造面向前台、后台、开发者的统一访问控制平台，强化安全审计能力；三是构建安全运行平台，实现面向重要、核心及敏感数据的专区管控，并基于API安全网关主动发现、全面监控数据接口。

（3）运行实施

一是持续推进政务数据分类分级，基于技术防护能力，实现面向重要、核心及敏感数据的加密、脱敏等特殊防护；二是推进精细化授权，以最小化必要原则进行政府信息系统前台导出功能、操作系统及数据库等后台、授权运营开发者权限的授权；三是面向数据开发与导出操作，基于公共数据授权运营平台与云桌面，实施安全开发管控，避免原始数据泄露，并开展常态化脱敏处理、水印处理，确保流通数据安全合规、源头可溯。

4 结束语

本文聚焦违规导出数据风险的防范，基于中观视角的实践研究，全面梳理政务数据流通通道，理清政务数据在政府信息系统中的分布与流向，归纳实践中政务数据的多样化导出流通方式；在此基础上，聚焦政务数据违规导出这一重大风险，分析国家合规要求及外部攻击、内部威胁、系统漏洞、合作方泄露等具体威胁表现，提出针对性的强化安全治理的相关策略；进而围绕政府实时生产类应用系统、政府大数据分析应用系统、政府专用流通类应用系统、政务中台及云平台设施，建立涵

盖管理落实、技术防护、运行实施三位一体的政务数据流通安全治理体系。不同于学术界主要面向较理想化的理论框架模型的研究，本文从实践推进视角切入，聚焦真实运行环境中的政务数据流通通道，提出一种较为系统、科学的数据安全治理方案，为全国各地方各部门高效建立面向政务数据流通的安全治理体系提供参考。

未来研究可围绕两个方向展开：一是聚焦政府数据流通中的其他次要安全风险，开展针对性研究，进一步完善本文提出的政务数据流通安全治理策略与体系；二是随着政务数据相关管理与利用政策的发布与深化落实，当前多样化的政务数据导出流通方式也将进一步演化，面临的主要数据安全威胁表现也将发生变化，应持续关注政务领域的最新实践，提出新的数据流通安全治理策略与体系，从而保障政务数据流通安全。

参考文献：

[1] 马乐存, 裴雷, 李白杨. 数据要素流通安全治理: 体系架构与实践进路[J]. 农业图书情报学报, 2024, 36(3): 46-58.
MA L C, PEI L, LI B Y. Security governance of data element circulation: system architecture and practical approach[J]. Journal of Library and Information Science in Agriculture, 2024, 36(3): 46-58.

[2] 刘业政, 宗兰芳, 金斗, 等. 数据要素流通使用的安全风险分析及应对策略[J]. 大数据, 2023, 9(2): 79-98.
LIU Y Z, ZONG L F, JIN D, et al. Security risk analysis and countermeasures in the circulation and use of data factors[J]. Big Data Research, 2023, 9(2): 79-98.

[3] 高亚楠. 数据交易流通安全保障探索与研究[J]. 信息安全研究, 2023, 9(7): 662-666.
GAO Y N. Exploration and research on security guarantee of data transaction and circulation[J]. Journal of Information Security Research, 2023, 9(7): 662-666.

[4] 李伟. 数据交易流通安全保障探索[J]. 数字通信世界, 2024(3): 185-187.
LI W. Exploration of security protection for data transaction circulation[J]. Digital Communication World, 2024(3): 185-187.

[5] 张凤娜, 刘金波. 安全视角下金融数据要素流通共享研究[J]. 商业经济, 2023(3): 161-164.
ZHANG F N, LIU J B. Research on the circulation and sharing of financial data elements from the perspective of security[J]. Business & Economy, 2023(3): 161-164.

[6] 林宏峥, 金维国, 宋国英, 等. 基于金融场景数据流通的安全技术研究[J]. 网络安全技术与应用, 2024(3): 105-107.
LIN H Z, JIN W G, SONG G Y, et al. Research on security technology of data circulation based on financial scenario [J]. Network Security Technology & Application, 2024(3): 105-107.

[7] SOMMA A, DE BENEDICTIS A, ESPOSITO C, et al. The convergence of digital twins and distributed ledger technologies: a systematic literature review and an architectural proposal[J]. Journal of Network and Computer Applications, 2024, 225: 103857.

[8] SHRIVASTAVA U, SONG J H, HAN B T, et al. Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation[J]. International Journal of Medical Informatics, 2021, 148: 104401.

[9] 何安珣, 李宏宇, 韦韬. 保障隐私安全 促进数

据流通: 隐私计算应用技术发展趋势综述[J]. 人工智能, 2023, 10(6): 35-42.
HE A X, LI H Y, WEI T. Ensuring privacy security and promoting data circulation: a summary of the development trend of privacy computing application technology[J]. Artificial Intelligence View, 2023, 10(6): 35-42.

[10] 栾国春. 基于区块链技术保障数据流通、交易和共享安全[J]. 中国经贸导刊, 2023(8): 64-66.
LUAN G C. Security of data circulation, transaction and sharing based on blockchain technology[J]. China Economic & Trade Herald, 2023(8): 64-66.

[11] 欧阳日辉. 数据基础设施保障数据安全及高效流通[J]. 人民论坛, 2024(7): 70-75.
OUYANG R H. Data infrastructure ensures data security and efficient circulation[J]. People's Tribune, 2024(7): 70-75.

[12] 付少雄, 孙建军. 数据流通与安全: 标准与保障体系[J]. 图书与情报, 2023(4): 20-28.
FU S X, SUN J J. Data circulation and security: standards and assurance systems[J]. Library & Information, 2023(4): 20-28.

[13] 周君, 王显强. 新型智慧城市下政务数据安全管理的研究[J]. 信息通信技术与政策, 2020(3): 29-33.
ZHOU J, WANG X Q. Research of government data security in the construction of new-type smart city[J]. Information and Communications Technology and Policy, 2020(3): 29-33.

[14] 李博, 郑华祥, 李绍宾. 基于隐私计算的政务数据开放技术平台设计与实践[J]. 信息安全研究, 2023, 9(12): 1203-1209.
LI B, ZHENG H X, LI S B. Design and practice of open government data platform based on privacy-preserving computation[J]. Journal of Information Security Research, 2023, 9(12): 1203-1209.

[15] 陈静, 白洁. 面向全国一体化政务服务平台的科技政务数据资源安全共享体系研究[C]//第38次全国计算机安全学术交流会论文集. [S.l.:s.n.], 2024.
CHENJ,BAIJ.Researchonthesecureshar-ing system of scientific and technological government data for the national integrated government service platform[C]//Proceedings of the 38th National Computer Security Academic Exchange Conference. [S.l.:s.n.], 2024.

[16] 郑文阳. 我国政务数据开放的价值面向及安全保障[J]. 行政管理改革, 2023(9): 70-80.
ZHENG W Y. The value orientation of China's governmental data openness and the construction of security guarantee mechanisms[J]. Administration Reform, 2023(9): 70-80.

[17] 孙杨, 陈晏鹏, 孙宗臣, 等. 面向政务领域的可信数据交换系统设计与实现[C]//2024世界智能产业博览会人工智能安全治理主题论坛论文集. 天津: [S.n.], 2024.
SUN Y, CHEN Y P, SUN Z C, et al. Design and implementation of a trustworthy data exchange system for government applications[C]//Proceedings of the Thematic Forum on Artificial Intelligence Security Governance at the 2024 World Intelligence Industry Expo. Tianjin: [s.n.], 2024.

[18] JANA A. Sensitive information leakage analysis of database code by abstract interpretation[J]. International Journal of Security and Networks, 2023, 18(2): 91-105.

作者简介

王跃（1983– ），男，中国信息通信研究院政务服务中心副主任、高级工程师，主要研究方向为数据资源体系治理与应用、数字化转型与数字政府建设。

莫莉娟（1990– ），女，中国信息通信研究院政务服务中心数据部副主任、高级工程师，主要研究方向为数据治理、数据运营。

苏娜（1976– ），女，中国信息通信研究院政务服务中心主任、高级工程师，主要研究方向为电子政务、数字政府建设运营。

收稿日期： 2024-08-13

通信作者： 苏娜，suna@caict.ac.cn