数字政务背景下政务数据安全与隐私保护机制研究

周贞杏　杨　洋
数字广西集团有限公司　广西　南宁　530003

摘　要：数字政务已成为提升国家治理能力现代化水平的核心引擎。然而，在数据要素价值被空前释放的同时，海量、高敏的政务数据也面临着前所未有的安全威胁与隐私泄露风险。本文旨在系统性地剖析数字政务发展进程中政务数据安全与个人隐私保护所面临的严峻挑战，深入探究其成因，并在此基础上，从制度、技术、管理三个维度构建一个多层次、立体化的协同治理框架。研究认为，应通过完善法律法规体系、强化技术防护能力、优化组织管理模式，并引入多方共治理念，方能有效平衡数据利用与安全保护之间的张力，为数字政府的健康、可持续发展筑牢安全基石。

关键词：数字政务；数据安全；隐私保护；协同治理；数据生命周期

引言

当今世界正经历深刻数字化变革，数字政务建设成为全球战略重点。我国顶层设计文件明确提出加强数字政府建设、推动政务数据共享开放。在此背景下，各级政府依托一体化政务服务平台汇聚海量涵盖多领域的数据资源，这些数据是政府精准施策、科学决策的基础，也是驱动经济社会创新发展的关键要素。但“数据是新时代的石油”背后，潜藏巨大安全与伦理风险。政务数据权威、完整且关联性强，一旦泄露、篡改、滥用或非法交易，会侵犯公民权益、动摇公众信任，甚至危及国家安全和社会稳定。所以，如何在释放政务数据价值的同时，构建有效的安全与隐私保护机制，是数字时代政府治理亟待解决的核心问题，本文将深入探讨。

1 数字政务背景下数据安全与隐私保护的严峻挑战

1.1 数据全生命周期的安全风险加剧

在采集端，源头数据质量不一，过度采集、强制授权等问题频发，为隐私泄露埋下隐患。传输过程中，跨域、跨层级的高频数据共享使网络通道成为攻击焦点，易遭截获或篡改。存储环节高度集中，一旦数据中心或云平台被攻破，后果不堪设想，而混合云架构更增加了管理复杂度。处理与共享阶段风险尤为突出，数据在融合分析时，可能因算法缺陷或内部违规操作，导致通过关联分析实现“去匿名化”，间接暴露个人隐私；同时，共享边界模糊、权责不清，极易引发“共享即泄露”的困局[1]。最后，数据资产化后，其销毁常被忽视，残留信息构成潜在的安全后门。

1.2 隐私泄露的“涟漪效应”与复合风险

政务数据中的个人信息具有极强的敏感性与关联性。单一数据点的泄露，通过与其他公开或半公开数据的交叉比对，足以构建出完整的“数字画像”，揭示个人的行为轨迹、社会关系乃至思想倾向。这种“涟漪效应”使危害呈指数级放大。例如，医疗记录结合位置信息可暴露健康状况，社保数据与消费记录交叉则能推断经济能力与家庭结构。此类复合风险远超传统信息泄露范畴，对个人的人格尊严、财产乃至人身安全构成直接且深远的威胁。

1.3 新兴技术带来的“双刃剑”效应

人工智能、区块链等新技术在赋能政务的同时，也引入了新的悖论。AI模型依赖海量数据训练，但其本身可能成为隐私泄露渠道（如模型反演攻击），且“黑箱”决策难以解释追责。区块链的不可篡改特性虽利于可信，但其透明性与隐私保护存在天然冲突。此外，在推动公共数据授权运营、探索数据资产化的过程中，如何界定权属、防止垄断、确保公平，并遏制商业机构对个人数据的过度商业化利用，构成了复杂的法律与伦理挑战。

1.4 制度体系不健全与执行机制缺失

相较于技术的飞速迭代，法规标准与管理体系明显滞后。现有法律虽已搭建框架，但在数据分类分级细则、跨境流动监管、应急响应流程等操作层面仍存空白。同时，政府部门普遍缺乏专业的数据安全治理团队，安全责任未能有效压实，“有制度无执行”的现象普遍存在，使得技术防护缺乏坚实的制度支撑与组织保障。

2 挑战成因的深层次剖析

2.1 “重利用、轻保护”的发展理念偏差

在数字政务建设初期，为了快速展现成效、提升服务效率，各级政府往往将重心放在数据的汇聚、共享与应用上，而对伴随而来的安全与隐私风险重视不足。这

种“先发展、后治理”的路径依赖，导致安全防护措施常常作为事后补救，而非内生于系统设计之中（即缺乏“Privacy by Design”和“Security by Default”理念）。

2.2 数据权属与利益分配机制不明晰

政务数据的所有权、管理权、使用权、收益权等权属关系尚未在法律上得到清晰界定。政府作为数据的管理者，其权利边界在哪里？公民作为数据的主体，其权利如何有效行使？企业在参与数据开发运营时，其行为边界又该如何划定？权属不清直接导致了责任主体模糊，各方在数据安全与隐私保护上的投入意愿和动力不足。

2.3 技术防护体系协同不足与纵深防御能力薄弱

尽管政务信息系统已逐步实现集约化、一体化建设，安全基础设施如政务云、统一身份认证平台等广泛应用，但在实际运行中，安全防护仍存在“重平台建设、轻安全协同”的倾向。部分单位在依托统一平台的同时，未能有效落实分层防护责任，安全策略配置不一致、监测响应机制割裂，导致整体防御体系缺乏纵深与联动。同时，面对日益专业化、组织化的网络攻击（如APT攻击），传统的边界防御、病毒查杀等手段已显乏力，亟需在集约化架构下深化零信任理念，融合威胁情报、主动免疫、动态访问控制等新一代安全能力，构建覆盖“云—网—端—数”的一体化主动防御体系。

3 构建多层次协同的政务数据安全与隐私保护机制

3.1 制度维度：筑牢法治根基，明晰权责边界

3.1.1 健全精细化法规标准体系

在《网络安全法》《数据安全法》《个人信息保护法》等基础法律框架下，亟需构建覆盖全生命周期、贯穿全业务场景的精细化政务数据法规标准体系。该体系应以“分类分级”为基础、“权限可控”为核心、“行为可溯”为保障，推动数据安全管理从原则性要求向可量化、可配置、可审计的细粒度规则演进。具体而言，应在国家统一标准指引下，细化政务数据的分类分级目录，并据此建立基于角色、场景和风险的动态访问控制机制，明确不同主体对特定数据的访问权限、操作范围、调用频次及使用目的限制。同时，法规应强制要求对高敏感数据的访问行为实施日志留存、异常监测与定期审计，确保“谁访问、为何访问、访问了什么”全程留痕、责任可追。在此基础上，同步完善数据共享、开放与跨境流动的精细化规则，包括：共享前的安全影响评估、开放清单的负面/正面双向管理、出境数据的风险分级审批等，形成“制度—标准—技术”三位一体的精细化治理闭环。

3.1.2 确立以数据主体为中心的权利保障机制

在制度设计上，必须确立“以数据主体为中心”的权利保障机制，从根本上扭转政府与公民在数据关系中的不对等地位。政府部门在采集和使用公民数据前，必须履行充分、清晰、易懂的告知义务，并获得公民清晰、自愿、具体的同意，除非法律明确规定无需同意的情形。这种同意应当是可撤回的，并且不能因拒绝授权非必要数据而影响公民获取基本政务服务的权利。在此基础上，应着力降低公民行权成本，建立便捷、高效的个人数据权利行使通道。例如，可以依托全国一体化政务服务平台，为公民提供统一的“数据门户”，支持其在线查询自身数据被哪些部门使用、用于何种目的，并能方便地行使查阅、复制、更正、删除以及撤回授权等法定权利，真正将纸面上的权利转化为可触达、可操作的现实保障[2]。

3.2 技术维度：打造内生安全，赋能隐私计算

3.2.1 推行全生命周期的内生安全设计理念

应全面推行“安全左移”与“Privacy by Design”（隐私设计）理念，将安全与隐私保护要求深度嵌入政务信息系统规划、设计、开发、测试、部署及运维的全生命周期各环节。内生安全并非依赖某类特定技术，而是通过在系统架构设计阶段即融入安全原则——如最小权限、数据最小化、默认安全配置、端到端加密、身份强认证等——从源头控制风险暴露面。为此，需建立覆盖需求分析、架构评审、代码开发、上线前检测等关键节点的安全管控流程，强制实施威胁建模、安全编码规范、第三方组件风险评估等实践。同时，应制定统一的安全设计指南与审查标准，确保无论采用何种技术路线（单体、微服务或云原生架构），均能遵循一致的安全基线。

3.2.2 构建纵深防御与隐私增强计算融合的技术体系

在面向政务数据高敏感、多主体、跨域流通的典型场景，亟需构建以纵深防御为基础、隐私增强计算（PEC）为核心支撑的融合型技术体系。该体系应打破传统“分层堆叠”的安全思维，转而围绕数据全生命周期的使用与流动，实现“防泄露、控使用、保隐私”的一体化防护。在基础设施与网络层面，应全面推行零信任架构，实施“永不信任、持续验证”的动态访问控制，并优先部署自主可控的软硬件底座，夯实安全根基。在应用与行为监控层面，依托用户与实体行为分析（UEBA）、安全信息与事件管理（SIEM）等系统，对异常操作与潜在攻击进行智能感知与快速响应，形成外层防线。关键突破在于数据层的安全范式升级：不仅要延续静态/动态脱敏、全链路加密、数据水印等传统防护

手段，更需将隐私增强计算深度融入数据使用与协作环节，实现从“数据不动算法动”到“数据可用不可见”的转变。例如：在跨部门联合建模场景中，采用联邦学习，使原始数据始终保留在本地，仅交换模型参数，避免敏感信息外泄；在多方联合统计或比对任务中，运用安全多方计算（MPC），确保各方输入数据不被泄露，仅输出合规结果；在高敏感数据处理环节，依托可信执行环境（TEE），在硬件级隔离环境中完成计算，保障数据在内存中的机密性与完整性。

3.2.3 建设统一智能的数据安全管控平台

为克服当前政务系统“烟囱林立”带来的管理难题，应着力建设一个统一的数据安全管控平台。该平台应作为政务数据安全的“神经中枢”，有机整合统一身份认证、精细化权限管理、全量操作日志审计、自动化风险评估、智能化应急响应等核心功能。通过这个平台，管理者能够对全域政务数据资产进行可视化盘点，实时监控数据流转状态，动态评估安全风险，并在发生安全事件时迅速启动预案、追溯源头、阻断影响，从而实现对政务数据安全的集中化、标准化、智能化管理。

3.3 管理维度：强化组织协同，培育安全文化

3.3.1 完善数据治理的组织架构与责任体系

应在中央到地方各级政府部门设立首席数据官（CDO）与数据安全官（DSO）等专职领导岗位，赋予其统筹协调数据战略、数据治理、数据安全与隐私保护工作的权威和资源。通过明确的岗位职责和考核机制，将数据安全责任层层压实，确保每一项安全要求都能找到具体的责任人，从根本上解决“九龙治水、无人负责”的困境。

3.3.2 建立跨部门协同与常态化演训机制

建议成立由网信、公安、大数据局、司法以及各主要业务部门共同参与的政务数据安全与隐私保护联席会议，定期研判风险、会商对策、协同处置重大安全事件。同时，安全能力的提升离不开实战检验，应将安全培训与应急演练常态化、制度化。针对不同岗位的工作人员，特别是直接接触敏感数据的一线人员，开展有针对性的安全意识教育和技能培训。并定期组织覆盖全链条的数据安全应急演练，模拟真实攻击场景，检验应急预案的有效性，持续提升整个组织的实战防御与应急响应能力。

3.3.3 引入多元共治的社会监督与评估机制

应积极引入第三方专业力量，鼓励独立的、具备资质的第三方机构对政务系统的数据安全与隐私保护水平进行定期的合规性审计和风险评估，其结果可作为改进工作的重要依据。同时，必须畅通社会监督渠道，通过官方媒体、政务平台等途径，及时公布数据安全政策与实践情况，并设立便捷的举报机制，鼓励媒体、公众、行业协会和专业研究机构对潜在的数据滥用或安全漏洞进行监督和曝光。通过构建政府主导、企业履责、社会监督、公众参与的多元共治格局，共同营造一个安全、可信、负责任的数字政务生态[3]。

4 结语

本文研究表明，应对数字政务背景下的安全与隐私挑战，不能寄希望于单一的技术突破或法规出台，而必须采取一种系统性的、协同治理的思路。通过构建“制度为纲、技术为器、管理为基”的三维联动机制，将安全与隐私内化为数字政务的基因，才能真正实现数据要素的安全、可信、高效流通。展望未来，随着量子计算等颠覆性技术的发展，现有的密码学体系可能面临重构，这将对数据安全提出更高要求。同时，全球数据治理规则的竞争与博弈也将日趋激烈。我国应在积极参与国际规则制定的同时，持续深化国内政务数据治理体系改革，不断探索符合国情、引领未来的数据安全与隐私保护新范式，为全球数字文明贡献中国智慧与中国方案。

参考文献

[1]李志飞.政务数据共享平台中的隐私保护与AI应用策略研究[J].中国战略新兴产业,2025,(35):26-28.

[2]沈博,杨军,王福喜,等.政务云环境下的数据共享隐私保护增强方案[J].沈阳师范大学学报(自然科学版),2025,43(01):28-36.

[3]王正超.数智时代政务大模型数据安全风险及治理机制研究[J].中国科技论坛,2025,(11):151-160.