大数据与决策研究

2023 年第 60 期（总第 216 期）

广西壮族自治区信息中心
广西壮族自治区大数据研究院　　2023 年 12 月 12 日

广西政务数据全生命周期安全治理存在问题与对策

近年来，国家对数据安全的重视程度不断提升，政务数据作为新时代数字政府的核心资产，不仅涉及公民个人信息数据，还涉及政府机构的相关的敏感信息等重要数据，如何降低政务数据流转过程中的不确定性、防范大数据风险造成的价值受损等负面影响，成为当前推进政务数据安全治理应着重考虑的问题。目前，我区信息资源共享开放工作的逐步

深入，政务数据安全治理成为各方关注的焦点，但在推进政务数据“聚通用”全生命周期安全治理上仍面临着安全标准规范、安全运营管理、安全防护水平等挑战，亟需加强由“内到外”安全管理、优化布局“聚到用”各环节安全技术体系、构建由“智到全”安全运营体系。

一、我区政务数据“聚通用”全生命周期安全治理存在问题

（一）政务数据“聚”的安全标准规范有待统一

一是数据采集缺少统一的标准规范。现有的法律法规主要针对网络安全或大数据发展工作制定，仅仅部分内容与数据安全相关，且内容主要集中在宏观层面，没有细化实施细则和标准，缺少适合数据安全保障工作规范和指引。数据采集无法确保数据的完整性和准确性，给共享应用带来不便。比如：在政务数据采集阶段，广西区直中直部门目前尚未完成政务服务事项标准化和系统一体化工作，申请表单字段没有实现全区统一。**二是数据分级分类不统一。**我国的《网络安全法》和《个人信息保护法》在提数据保护时，都是只提分类，没有提分级。《数据安全法》第 21 条规定了数据分类分级保护制度，但仅为原则性规定，尚未构建国家层面关于政务数据分类分级的具体规则和操作标准，地方性法规文件对于政务数据分类分级的原则与规定也并不统一。例如广西发布《公共数据分级分类指南》相比浙江的《数字化改革公共数据分类分级指南》，浙江的数据分级分类维度更加细

化，从安全保护维度将数据分为核心数据、重要数据和一般数据，便于后期对不同重要程度数据进行相对应的保护措施，广西相关规范有待完善。

（二）政务数据“通”的安全运营管理有待提高

一是数据流通过程面临较大攻击风险。我区在推进政务工作中容易产生并汇集大量涉及民生重要数据和个人敏感隐私政务数据，因其应用价值高容易招致攻击。根据《广西政务云网网络与数据安全态势监测月报》显示今年 6—9 月自治区政务云每月有超 40 万次攻击。**二是较难开展数据流通访问权限管控。**政务数据归集后，数据持有者或采集人对数据失去了控制权，不同部门基于特定使用目的进行数据二次使用，因政务数据来源复杂、流动性高、使用者广泛，容易造成访问者身份难辨、访问行为难以控制。**三是流通过程容易存在账户管理风险。**数据流通涉及到交换平台对接、部门之间各类政务事项产生，经调研发现，部分部门存在保密意识不足、账户管理不严、口令密码安全等级弱等情况，极易对政务数据造成安全泄漏隐患。例如，弱口令问题连续多年成为我区网络攻防演习中最突出安全问题，根据《广西政务云网网络与数据安全态势监测月报》显示，2023 年 7 月监测中发现存在 API 接口弱口令登录行为，部分业务系统的管理账号使用弱口令，攻击者可通过弱口令直接登录此类 API 窃取敏感信息，极易引发政务数据大规模泄露。

（三）政务数据“用”的安全防护水平有待提升

一是政务数据应用容易存在违规泄露风险。政务数据存在不合规的开放和共享，导致违规数据泄露，例如：广西柳州柳城县以及广西百色平果市卫生部门在公布执法人员信息时违规泄露执法人员的个人隐私信息，公布了完整的身份证号码以及手机号码；北海市某中心窗口人员利用工作便利，多批次筛选整理公民个人房产信息贩卖个人信息 50 万条。**二是数据共享开放运用意愿不强。**随着国家出台数据安全保护的法律法规，我区公共数据拥有部门因为担心在数据开放运用过程中存在敏感数据泄露风险而不敢共享开放数据，部分国垂系统至今尚未开展对接且部门人员存在畏难情绪，导致政务数据接入共享平台时存在对接不全、不完整、不闭环问题。**三是对政务数据有效溯源能力不足。**数据共享交换过程中存在大量人的主观性，数据在多个主体之间流动，存在主体的保密责任不清晰，在数据共享交换过程中发生的泄露，目前缺乏有效的数据标识能力，一旦发生数据泄露，无法有效进行溯源，定位相关责任人，无法对数据泄露形成有效的威慑。

二、对策建议

（一）构建由“内到外”的安全管理体系

在内部管理方面，明确具体的安全管理规则和策略，以规范化、流程化方法指导实际工作落实，避免“无规可依”，

建立基于风险管控的数据安全管理及内控体系。建立“审管用”分离的数据安全岗位职责，厘清各方主体安全责任；建立数据共享交换平台的安全管理规范，明确数据采集、共享、使用全过程的身份鉴别、授权管理等安全保障措施，加强内外部人员操作审计，确保数据安全。**在外部管理方面**，建立健全数据交易服务机构管理制度，建立数据安全使用承诺制度，制定数据分析和交易禁止清单，对运营主体规划的应用场景进行合规性和安全风险等评估。依法制定数据流通交易规则，完善数据交易监督管理制度。加强对第三方公司人员监管，建立外部第三方工作人监督管理机制。

（二）构建由“聚到用”的安全技术体系

在“聚”环节，重点从数据的分级分类、数据源鉴别、数据质量监控、数据水印等方面进行安全设计。通过存储加密、防泄漏、防勒索、数据备份、数据容灾、数据审计等技术手段，保障数据汇聚的安全。**在“通”环节**，通过传输加密、数字签名、安全认证等技术手段确保传输数据的真实性。利用敏感数据自动发现、动态脱敏、数据清洗以及数据转换等手段，保障数据安全可用性。**在“用”环节**，完善数据共享交换平台的用户授权、访问控制、入侵检测、日志记录等技术措施，建立完备的数据溯源系统，监控高风险数据交换操作，记录及报告重要敏感数据的分发和调用行为，对数据共享全流程进行监测预警分析，对异常数据交换操作的自动化识别和实时预警。

（三）构建由“智到全”的安全运营体系

构建“智到全”安全运营体系是指建立智能化全生命周期安全运营体系。**一是严格授权管理和身份认证。**通过智能运维管控实现大数据操作平台和数据库的统一账户管理、统一认证、统一鉴权、数据资产梳理和安全审计等功能。对数据进行操作的所有人员组织、设备等进行智能化身份鉴别，确保参与者身份安全可信，按照最小授权、权职分离的原则，对数据处理各方的访问权限进行控制，结合数据分级分类要求，对各类人员、设备访问的数据进行数据脱敏处理。**二是建立智能化事中的预警监测与异常分析工作。**主要包括：敏感信息数据流分析检测、数据访问与传输异常检测、用户操作行为异常分析等智能化分析功能。**三是做好安全审计与溯源工作。**使用人工智能审计工具，对政务数据的使用和访问进行审计，确保合规性，采用日志管理技术，确保数据流和用户行为的可追溯，有效执行安全事件调查和追责。

（执笔人：大数据发展研究课题组）

编辑部地址：南宁市体强路 18 号广西信息中心 1412 号房
联系电话：0771-6113592
电子邮箱：dsjyjs@gxi.gov.cn
网　　址：http：//gxxxzx.gxzf.gov.cn/

扫描二维码获取
更多决策参考信息