大数据与决策研究

2024 年第 47 期（总第 267 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　　2024 年 9 月 27 日

隐私计算助力广西公共数据安全可信流通路径研究

国家数据局会同有关部门制定《“数据要素×”三年行动计划（2024—2026 年）》，强调深化隐私计算相关技术应用，为数据要素打造安全可信流通环境。基于隐私计算进行合规与数据开放的探索成为当前技术应用的主要方向。通过研究国内隐私计算在公共数据流通领域相关应用，分析广西公共数据流通存在的安全风险与挑战，为形成有效的广西模式机制和技术实施路径提供对策建议。

一、国内隐私计算应用进程加速推进

（一）多元技术融合发展特点呈现

隐私计算[1]作为一种综合的技术体系，目前主要有两大发展方向，**一是与区块链、人工智能等其他技术协同推进落地应用。**如隐私计算+区块链方面，浙江省统计局利用多方安全计算、联邦学习和区块链等技术，实现多个政府部门内外部千万级数据安全共享和融合计算，提高了政府部门的治理能力和治理水平。隐私计算+AI+大数据方面，“隐语”可信隐私计算框架融合 AI、大数据等技术，打造车险联合定价精算平台，可在安全合规环境下进行联合数据建模，实现新能源车险精算能力突破。**二是隐私计算体系内多种技术融合应用。**如多方安全计算+联邦学习+差分隐私。阿里妈妈营销隐私计算平台利用多方安全计算、联邦学习、差分隐私等隐私计算技术，在广告投放全流程中严格保障多方数据的隐私安全和数据合规，解决广告营销场景中数据孤岛和跨域数据流通问题。

（二）隐私计算应用涌现三种模式

一是平台服务模式。通过构建隐私计算平台，根据自身需求进行定制化数据分析和挖掘。如深圳福田通过搭建公共数据隐私计算平台构建多方数据安全融合计算环境，促进“政政”“政企”之间的数据价值共享互惠。**二是嵌入式应用模式。**在已有应用系统中嵌入隐私计算服务功能，为用户提供无缝的数据隐私保护体验。如翼支付融合安全多方计算

[1] 隐私计算是指在保护数据本身不对外泄露的前提下实现数据分析计算的技术集合，达到对数据“可用不可见”的目的。实施路线包括多方安全计算、联邦学习、可信执行环境、同态加密、零知识证明等。

技术，基于 PrivTorrent 密流安全计算平台研发部署“新冠疫情密切接触隐私查询”系统应用，在不泄露用户行程位置以及疾控中心病例数据的基础上判断是否有密切接触，从而构建分布式环境下用户与疾控中心双向隐私安全的多级疫情状态匹配机制[2]。**三是云服务模式。**通过云平台快速部署和使用隐私计算服务，在云端开展安全的数据分析和共享。如腾讯云采用云原生架构和容器化的交付方式，支持用户通过软件开发工具包或应用程序编程接口快速构建隐私计算应用。

（三）隐私计算发展生态逐步构建

一是技术标准和规范逐步建立。2021 年以来，隐私计算互联互通系列标准及规范发布，为隐私计算产品的研发、测试等提供统一的规范指导，提升隐私计算产品的质量和安全性，推动隐私计算技术的规范化、标准化发展。**二是市场规模持续扩大。**根据 IDC 发布的《中国隐私计算平台市场份额，2023》报告，2023 年中国隐私计算平台市场规模达到 8.9 亿元人民币，同比增长 12.8%。根据专业机构预测显示，2025 年中国隐私计算市场规模将达到 145.1 亿元[3]。**三是领域开源趋势愈加明显。**2022 年下半年以来，隐私计算开源平台、隐私计算开源协同计划[4]相继推出，推动隐私计算技术迭代和应用。开源平台降低了隐私计算技术门槛，促进隐私计算产品的多样化和竞争，加速了隐私计算应用发展。

[2] 案例来源:《国内隐私计算行业十大案例》
[3] 数据来源:《隐私计算应用研究报告（2022 年）》
[4] 案例来源:《数字安全专刊》No.007（总第 218 期）

二、隐私计算应用于广西公共数据流通的支撑要素

（一）算网协同能力增强

隐私计算应用需要强有力的算力及网络运力支撑，广西算力网络建设近年取得显著进展。广西 2023 年底已建成数据中心 38 个，机架数突破 4.4 万架，全区算力总规模达 668PFlops[5]，满足隐私计算初步应用阶段运算任务处理需求。2024 年上半年，五象云谷云计算中心项目竣工实现可承载 40000PFlops 算力，算力设施的持续升级，支撑隐私计算实现广泛应用。此外，广西已建成 5G 基站总数达 10.7 万个，实现全区行政村 5G 网络全覆盖，高速、稳定的网络连接可有力支撑隐私计算实时数据处理。

（二）技术应用取得突破

广西发挥重点实验室及高校技术攻关优势，积极推进隐私计算领域成果及专利取得新成效。如广西可信软件重点实验室的“不需要可信机构的面向数据发布的隐私计算”项目被授予中国电子学会自然科学奖二等奖[6]。广西大学提出基于边缘的物联网中异构数据的隐私保护拆分联邦学习方法防止原始数据信息泄漏并推进实际应用[7]。截止 2024 年 9 月 5 日，广西隐私计算领域专利总数 14 件[8]，同比增长约 56%，为隐私计算技术创新与产业发展奠定良好基础。

[5] 数据来源：2023 年度《广西互联网发展报告》
[6] 案例来源：广西可信软件重点实验室网站新闻动态：《“不需要可信机构的面向数据发布的隐私计算” 被授予中国电子学会自然科学奖二等奖》
[7] 案例来源：论轮智能科学信息平台《广西大学郑嘉利、陈一心等最新成果：PPSFL：基于边缘的物联网中异构数据的隐私保护拆分联邦学习》
[8] 数据来源：中国专利之星检索系统

（三）应用实践逐步拓展

广西积极探索隐私计算技术在银行、电网等重点领域的创新应用。兴业银行南宁分行利用隐私求交、隐匿查询等多方安全计算技术，依托隐私计算平台，合规共享反洗钱客户名单。广西电网有限责任公司采购基于区块链与隐私计算融合的电力数据安全协同技术研究项目推动电力行业隐私计算技术应用。广西北部湾银行实施采购隐私计算平台保护客户数据隐私和安全。

三、广西公共数据流通存在的安全风险与挑战

（一）数据安全防护能力不足

当前，广西公共数据资源主要存储在各部门本地系统。在推进数据共享与开放的过程中，由于地方部门技术实力不均衡，数据安全人才配备不足，数据在收集、管理与处理过程中仍然存在受损、丢失或被盗用的风险隐患。调研发现，部分地市数据部门超过60%的关键业务系统运行在超过5年以上的老旧服务器上，高达35%的人表示从未参加过任何形式的数据安全培训，数据安全基本防护措施能力不足。

（二）数据利用面临合规风险

在当前广西公共数据共享开放流程中，仍缺乏对数据利用场景的监测，数据提供部门将数据提供至申请部门后无法对数据利用过程及结果进行追踪，难以确保数据应用的合规性与正当性，且现行脱敏技术手段并不能解决所有的隐私问题，在数据利用过程中仍有通过数据拼凑还原个体数据的可能，使个人信息面临泄露和违规利用的风险。

（三）安全监管体系亟待完善

广西虽已出台相关政策明确数据保护要求，但在监管执行层面，仍存在覆盖不全、执行不力的问题。如广西北海一网站服务器未遵守数据安全与网络安全法规定使用数据加密技术保护个人信息，致 22 万个人隐私数据遭泄露，被境外论坛售卖[9]。这不仅严重侵犯了公民个人隐私权，也暴露出广西在数据安全监管方面的短板。

四、隐私计算助力广西公共数据安全可信流通路径建议

（一）运用隐私计算增强技术安全防护能力

一是加固数据流通平台安全防线。通过嵌入隐私计算技术，迭代升级现有自治区公共数据资源平台。通过对开放数据进行管控授权，区分用户权限提供不同颗粒度数据，对数据用法、使用时间、使用次数、并发限制等内容进行设定，实现对公共数据的精细化治理。**二是**提升地方部门数据安全防护水平。通过系统性宣传培训、引进高级技术人才以及提供持续技术支持等方式，增强地方部门安全意识及技术防护水平。升级优化地方数据基础设施，提升设备安全等级，确保数据基础设施满足数据安全防护需求。**三是**拓宽隐私计算应用场景。挖掘隐私计算在广西不同行业及同行业细分场景的需求价值，探索隐私计算技术多种应用模式，大幅度提升广西隐私计算应用规模，通过技术创新不断提升其在各场景的实用性、可用性和兼容性，为广西公共数据流通安全防护提供强有力支撑。

[9] 案例来源：界面新闻《约 22 万个人信息被挂卖，广西北海一公司涉数据泄露被罚款 20 万》https://new.qq.com/rain/a/20230811A03NCF00

（二）利用隐私计算强化数据利用合规管理

一是建立数据利用场景监测机制。对数据使用场景进行全过程跟踪和监管，协同使用隐私计算及区块链，利用区块链可追溯、隐私计算“可控可计量”技术特性，监测数据开放利用全周期的主体行为，为数据利用提供明确的指导和约束。**二是**构建数据安全管控能力。通过隐私计算的加密和脱敏技术，明确数据利用的范围、方式、目的等要求，借助隐私计算“数据可用不可见”模式，确保数据利用方仅获取结果，无法推理原始数据，以释放数据价值并降低泄露风险。**三是**加强数据合规性检查。通过隐私计算及区块链确保数据可信和不可篡改，通过同态加密技术验证数据完整性和真实性，确保数据合规、准确。

（三）依托隐私计算完善数据安全监管体系

一是构建基于隐私计算技术的智能化监管平台。使监管机构能在不接触原始数据的前提下，实现网站系统运作实时监控，及时检测和响应网站数据系统异常活动。以隐私计算作为技术支撑，助力加强对数据流通全链条的严密监管。**二是**推动数据跨部门协同监管。对于涉及多个部门的数据流通项目或活动，通过隐私计算技术加强跨部门之间的协同合作和信息共享，明确监管职责和分工协作，形成合力共同推进数据安全监管工作。**三是**建立数据安全应急响应机制。制定完善的数据安全应急预案，明确应急处置流程和责任分工，确保在发生数据安全事件时能够迅速响应、有效处置，减少损失和影响。

（执笔人：梁颖）

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