智慧城市数据安全治理标准：突出问题与改进对策

智慧城市的核心底座是数据，即类型、格式和来源多样的数字信息集合，包括政务数据、商业数据和个人数据等。这些数据具有独特性，时刻面临安全风险，而当前智慧城市数据安全治理标准不完善，仍存在一些突出问题，亟须采取措施改进，以更好地提高数据安全治理效能，服务新时代智慧城市建设。

文 | **温演驰** 资本市场学院办公室执行主任　**谭帅帅** 国家（深圳·前海）新型互联网交换中心技术部部长

一、智慧城市数据安全治理的法规分析

自2016年《网络安全法》实施后，我国已形成以《网络安全法》《数据安全法》《个人信息保护法》和《民法典》四部法律为基础，配套行政法规、部门规章和政策文件的网络安全法律法规体系框架（图1）。其中涉及智慧城市数据安全治理的法规与要求如下：

（一）法规。一是《网络安全法》。第十五条提出“国家建立和完善网络安全标准体系”“支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定”，第二十一条规定“采取数据分类、重要数据备份和加密等措施”，第四十条规定“网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度”。二是《数据安全法》。第四条规定“建立健全数据安全治理体系，提高数据安全保障能力”；第五章规定电子政务对收集的个人隐私、个人信息、商业秘

来源：根据网络公开资料整理

图1 网络安全法律法规体系

密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供；第二十一条要求“对数据实行分类分级保护”“关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度”。三是《个人信息保护法》。第二十四条提出“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正”；第五十一条要求个人信息处理者“制定内部管理制度和操作流程”“对个人信息实行分类管理”“采取相应的加密、去标识化等安全技术措施”及“制定并组织实施个人信息安全事件应急预案”。四是《民法典》。第一千零三十四条明确“自然人的个人信息受法律保护”“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息”；第一千零三十五条则规定处理个人信息“应当遵循合法、正当、必要原则，不得过度处理”。五是《网络数据安全管理条例（征求意见稿）》。由中央网信办于2021年11月发布征求意见，其中指出要建立“数据分类分级保护制度，不同级别的数据采取不同的保护措施”“国家支持数据开发利用与安全保护相关的技术、产品、服务创新和人才培养”“数据处理者应当采取备份、加密、访问控制等必要措施”“维护数据的完整性、保密性、可用性”并“建立数据安全应急处置机制”。六是《关于加强国家网络安全标准化工作的若干意见》。其中指出“网络安全标准化是网络安全保障体系建设的重要组成部分，在构建安全的网络空间、推动网络治理体系变革方面发挥着基础性、规范性、引领性作用。”在优化完善各级标准方面，“视情在行业特殊需求的领域制定推荐性行业标准”，重点推进“大数据安全、个人信息保护”等领域的标准研究和制定工作。七是《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》。由工信部2022年2月发布征求意见，其

中提出应推进“工信领域数据开发利用和数据安全标准体系建设”，应实行“数据全生命周期安全管理”，并建立了数据安全评估、安全预警和应急管理机制。

（二）要求。智慧城市数据是个人安全、公共安全和网络空间安全的基础。因此，其数据安全治理适用《网络安全法》《民法典》《个人信息保护法》《数据安全法》及配套规定。根据前述法规，智慧城市数据安全治理：一是应构筑全生命周期安全管理框架。《网络安全法》《数据安全法》和《个人信息保护法》均配套规定细化数据安全管理全过程要求。这就要求智慧城市数据安全治理应覆盖数据全生命周期所有阶段，还应建立识别规范、制定分类分级标准、设计数据安全风险评估框架，建立数据安全事件预警和应急处置流程，形成制度、流程、技术和人“四位一体”的智慧城市全生命周期安全管理框架。二是应建立包含创新技术的数据安全技术架构。《网络安全法》明确规定实行网络安全等级保护制度，《个人信息保护法》特别强调依据个人信息进行自动化决策应保持透明、公平和公正；《网络数据安全管理条例（征求意见稿）》支持数据开发利用与安全保护相关的技术、产品和服务创新。这就要求建立智慧城市数据安全技术框架时不仅要包含传统的网络空间安全技术，还应重点研究创新技术支撑数据保护的方法及防范由此引入的风险。三是应制定智慧城市数据安全治理标准体系。《网络安全法》要求建立和完善网络安全标准体系；《关于加强国家网络安全标准化工作的若干意见》明确推进“大数据安全、个人信息保护”等领域的标准研究和制定工作。这就要求智慧城市数据安全治理要建立安全防护和数据保护的标准化体系，以承载安全管理框架和安全技术架构。

二、智慧城市数据安全治理标准存在的突出问题

我国网络空间和数据安全治理经过多年发展已逐步迈入法治轨道，除前述各项法律法规和配套规定外，网络安全领域已发布数百项国家标准，智慧城市数据安全治理标准化工作也在有序推进，但从实践看，还存在以下突出问题：

（一）对现实情况考虑不够。现与智慧城市数据安全治理相关的标准有三项：《智慧城市安全体系框架》针对智慧城市保护对象和安全目标，从安全角色和安全要素视角提出了由“保护对象、安全要素、安全角色和相关关系”四个要素组成的框架；《智慧城市建设信息安全保障指南》提供了智慧城市建设全过程的信息安全保障指导，包括从规划、设计、施工、运维、优化与持续改进的全过程信息安全保障的管理机制与技术规范；《大数据安全管理指南》提出了大数据管理的基本原则，规定了大数据安全需求、数据分类分级、大数据活动安全要求、评估大数据安全风险等。前述标准虽已构筑智慧城市数据安全治理的基本框架，但存在以下问题：一是主要防护对象是系统而非数据。现行标准侧重对智慧城市全局建设的安全概述和

设计，其防护目标是信息系统，措施是防御外部攻击者，未涉及智慧城市数据防护及全生命周期各阶段管理的策略机制。二是使用的安全模型不适合智慧城市数据安全管理。传统的数据安全模型建立在内部信任基础上，即在逻辑上划分数据安全边界，并向边界内的实体（人、设备、程序）分配数据访问和管理权限。但智慧城市按传统模型划分到边界内的实体数量巨大，包含部署在不安全环境中的传感器及计算设备和众多数据使用者和管理者。这一变化使得信任关系成为“时变不稳定”，即过去可信任不代表现在和未来可信任。按现行安全模型管理数据，易致数据被内部滥用或泄露。三是未全面涵盖基础资源。我国近年建设了一批新型信息基础设施，如新型互联网交换中心体系、数据交易中心体系和工业互联网标识解析体系，现有管理标准体系尚未涵盖。

（二）对发展趋势适应不足。现行或即将实施的安全技术相关标准有七项，包括：通用数据安全标准两项。《网络数据处理安全要求》规定网络运营者在数据全生命周期各阶段的管理和技术规范；《数据安全能力成熟度模型》按照组织建设、制度流程、技术工具和人员能力四个方面将数据安全能力成熟度划分为5个等级。个人信息保护标准三项。《个人信息安全影响评估指南》规定个人信息安全影响评估的基本原理和实施流程；《个人信息安全规范》旨在规范个人信息控制者在信息处理中的相关行为；《公有云中个人信息保护实践指南》则为公有云上存储和处理个人隐私信息的保护提供指引。特定行业数据安全标准两项。《健康医疗数据安全指南》要求健康医疗数据者应采取合理和适当的管理技术保障措施，给出针对医疗数据的分类体系、披露原则、管理指南和技术指南等；《政务信息共享数据安全技术要求》明确了共享数据准备、共享数据交换和共享数据使用阶段的数据安全技术要求及相关基础设施的安全技术要求。前述标准针对数据安全和个人信息安全明确了技术要求和控制措施，但在技术架构发展趋势上适应不足。一是从层次结构上看，现行标准将智慧城市分为“物联感知层、网络通信层、计算与存储层、数据及服务融合层、智慧应用层”五个层面。其中虽均涉及数据安全防护，但未将数据全生命周期视为整体考虑，无法适应形势建立以数据为中心的防护标准；同时，碎片化数据安全管理和防护可能造成数据运营漏洞，引发数据安全风险。二是从技术架构上看：数据安全和个人信息安全标准虽明确了技术措施框架，但均面向通用数据安全保护设计，未考虑智慧城市数据“面向智能、高度异构、相对开放”等独特性。

（三）对贯彻执行缺少抓手。当前智慧城市数据安全治理标准因缺强有力抓手而影响治理效果。一方面，管理标准落实效率不高。管理标准体系严重依赖于制度和流程，检验落实成效目前仍主要通过人工检查、核查、抽查等方式进行，存在主观性强、时效差等弊病。另一方面，技术标准落实易出偏差。技术标准体系

的落实不仅依赖于设备、软件，还与使用和配置技术的人高度相关，实践中存在不少因误配置或使用不当造成风险的情形；同时，智慧城市数据安全涉及的技术纷繁复杂、相互交织，更易出现兼容性和误配置问题。

三、智慧城市数据安全治理标准改进对策

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》发布，要求“统筹发展和安全，贯彻总体国家安全观，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，划定监管底线和红线。”综合前文法规分析和突出问题，建议遵循“严格依法依规”“优先复用现有标准”和“紧密结合智慧城市数据特性”原则，构建基于“两个标准一个平台”的智慧城市数据安全治理体系。

（一）制定智慧城市数据安全管理域标准。在智慧城市设计、建设和运营过程中提供关于数据安全管理方面的基本原则、管理组织和机制、安全规范和流程等，以指导智慧城市数据全生命周期处理规范，控制人为因素造成的数据安全风险。一是基本原则。除传统的“最小化收集”“最小化授权”和“谁管理谁负责、谁使用谁负责、谁运维谁负责”原则外，智慧城市数据安全治理还应遵循“零信任原则”。零信任是一种以资源保护为核心的网络安全范式，其前提是信任从来不是隐式授权的，而必须进行评估。通俗而言，在智慧城市场景下，数据的访问和管理权限是动态分配、用后即销的，而非长期信任一个账号或个人。该原则对需要访问的多样化数据实体不建立任何前置信任关系，只在确定需要访问数据时才分配权限，且用后随即取消，可最大化实现数据安全保护效果。二是管理组织和机制。智慧城市数据安全保护的管理组织除常规的“建设者、运营者、使用者、行业主管部门和信息安全监管部门”外，可设立城市级智慧城市数据安全委员会，负责建立跨部门、城市之间的协调联动机制，统筹数据安全方面资源分配，联合响应和处置安全事件；制定基于新型网络基础设施的数据保护机制。三是安全规范和流程。至少应包含智慧城市数据识别规范、分级和分类规范、智慧城市数据风险评估标准、智慧城市数据安全保护要求、智慧城市网络安全保护要求。当前智慧城市数据安全的标准已基本涵括以上标准规范，但应根据零信任原则作适当的修改。

（二）建立智慧城市数据安全技术域标准。《网络数据安全管理条例》指出数据安全的目标是保证数据的机密性、完整性和可用性。机密性是指不允许未授权访问，完整性是指不允许未授权篡改，可用性是指数据随时可访问、可应用的能力。智慧城市数据安全技术可分为：基础安全防护技术，主要保护承载智慧城市业务的设施、设备和信息系统不受外部攻击影响，例如防火墙、入侵检测、主机安全等；传统数据安全技术，

按照现有等级保护要求的技术标准规范执行即可实现；新型数据安全技术，包括人工智能技术、隐私计算技术、区块链技术和供应链安全技术等，主要是解决传统技术在智能度、效率和普适性等方面的不足，目前尚未启动新型数据安全技术标准化工作。

因此，建议针对智慧城市数据安全新型技术研究制定相应标准：一是人工智能技术。重点研究机器学习算法可解释性标准，解决人工智能黑盒模型造成的不透明和伦理问题，响应个人信息法等关于数据处理透明度和结果公平、公正的要求。二是隐私计算技术。注重国产加密算法在安全多方计算、同态加密等方面的嵌入和应用标准，保证关系数据底层安全的关键加密算法的控制权，防止因政治因素导致的灾难性数据安全事件。三是区块链技术。重点研究如何将区块链应用于智慧城市分布式数据收集和验证的指南性标准，利用区块链独特的信任模型使能智慧城市信任关系的建立。四是供应链安全技术。关注智慧城市数据安全产品和服务的供应标准，保证智慧城市的正常供给和自给自足，防范极端情况下智慧城市被“卡脖子”的风险。

（三）建设智慧城市数据安全治理平台。推进智慧城市数据安全管理体系和技术标准体系落地，不仅需要行政管理和自律监管，还需构建统一高效的治理平台，实现管理流程自动化和技术规范可控化。建议构建一个承载“数据快递单”“策略编排器”和“合规可视化”三个面向法律合规关键组件的智慧城市数据安全治理平台。其中：一是数据快递单。是指为智慧城市数据单元绑定数据属性和流转审计的记录，类似物流快递单，用以响应法律法规中对数据分类分级保护和全生命周期控制的要求。数据快递单应充分利用国家统一社会信用代码系统和互联网标识解析系统，建立智慧城市数据标识体系，叠加智慧城市分类分级标准，作为每个智慧城市数据单元收集时的数据属性。数据单元每个步骤都添加信息至流转审计记录，实现生命周期中的异常流转、安全事件发生后可溯源审计。二是策略编排器。智慧城市场景多变，每个场景均需根据具体需求进行安全技术措施选择。策略编排器可通过建立场景和标准体系技术措施，根据需求作出自动化技术策略选择和编排，高效响应法律法规对数据加密和安全保护等的要求。三是合规可视化。将网络空间和数据安全法律法规框架的抽象描述映射为智慧城市具体场景中的可视化展示。例如，针对“数据处理者应当采取备份、加密、访问控制等必要措施”，可通过在数据处理者信息系统中部署数据探针，持续检测智慧城市数据的备份数量、加密算法强度和访问控制状态，并以图形化或指标化方式呈现给决策者，支持智慧城市数据安全治理过程中的高级别行政决策。

责任编辑：杜玢翰 dubh@staff.ccidnet.com