

公共数据授权运营中数据安全问题研究

李若冰¹, 张 慧²

¹长春理工大学法学院, 吉林 长春

²图们市人民法院, 吉林 图们

收稿日期: 2025年6月5日; 录用日期: 2025年6月16日; 发布日期: 2025年7月23日

摘 要

社会主义核心国家“十四五”规划在“提高数字政府建设水平”一章, 提出要“加强公共数据开放共享”并指出要“探索将公共数据服务纳入公共服务体系, 构建统一的国家公共数据开放平台和开发利用端口”“开展公共数据授权运营试点, 鼓励第三方深化对公共数据的挖掘利用”。党的十九届四中全会将数据列为新型生产要素之一, 充分彰显了数据资源的极端重要性。数据日益成为国家战略性资源, 大量基础性、关键性的公共数据掌握在政府手中, 公共数据是数字经济时代的重要性基础资源之一, 这些数据是巨大的“创新财富”。

关键词

公共数据, 授权运营, 数据安全

Research on Data Security Issues in Public Data Authorization Operations

Ruobing Li¹, Hui Zhang²

¹College of Law, Changchun University of Science and Technology, Changchun Jilin

²Tumen City People's Court, Tumen Jilin

Received: Jun. 5th, 2025; accepted: Jun. 16th, 2025; published: Jul. 23rd, 2025

Abstract

In the chapter of “Enhancing the Construction of Digital Government” of the 14th Five-Year Plan of the socialist core country, it is proposed to “strengthen the opening and sharing of public data” and it is pointed out that “exploration should be made to incorporate public data services into the public service system, and a unified national public data opening platform and development and utilization port should be constructed”. “Pilot projects for the authorized operation of public data should be carried out, and third parties should be encouraged to deepen the mining and utilization of public data”. The

文章引用: 李若冰, 张慧. 公共数据授权运营中数据安全问题研究[J]. 法学, 2025, 13(7): 1463-1467.

DOI: 10.12677/ojls.2025.137205

Fourth Plenary Session of the 19th Central Committee of the Communist Party of China listed data as one of the new types of production factors, fully demonstrating the extreme importance of data resources. Data is increasingly becoming a strategic resource for the country. A large amount of basic and key public data is in the hands of the government. Public data is one of the important basic resources in the era of digital economy, and these data are huge “innovation wealth”.

Keywords

Public Data, Authorized Operation, Data Security

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 公共数据授权运营中数据安全的基础理论

1.1. 公共数据授权运营中数据安全概念

公共数据授权运营的提出实际上就是公共数据开放的一种渠道[1], 讨论公共数据授权运营的相关问题, 首先要明确的就是何为公共数据授权运营, 在 2025 年 1 月, 国家发展改革委、国家数据局关于印发《公共数据资源授权运营实施规范(试行)》的通知中, 明确规定, 授权运营, 是指将县级以上地方各级人民政府、国家行业主管部门持有的公共数据资源, 按照法律法规和相关要求, 授权符合条件的运营机构进行治理、开发, 并面向市场公平提供数据产品和技术服务的活动。

1.2. 公共数据授权运营中数据安全的重要性

信息时代数据影响着方方面面, 近年来, 中共中央、国务院都高度重视培育数据要素市场, 并将数据发展提升到国家顶层战略高度, 不仅仅先后印发了《关于构建更加完善的要素市场化配置体制机制的意见》(2020)、《“十四五”数字经济发展规划》(2021)、《关于构建数据基础制度更好发挥数据要素作用的意见》(2022)等政策文件, 还提出要协调发展与安全的关系, 在数据流通、使用全过程贯彻安全理念。2022 年党的二十大报告强调, 要加强个人信息保护, 提高公共安全治理水平, 健全国家安全体系, 捍卫国家数据主权。由此可见国家层面对于数据安全的重视程度, 同时, 随着法律的普及, 群众对于自己的个人信息的保障也逐渐重视起来, 因此数据安全问题成为了授权运营的首要任务, 只有有能力保障了公共数据的安全, 才有后续的使用与运营。

公共数据公开的同时也面临着许多风险。因此, 有些公共部门甚至基于安全的考虑, 对公共数据采取“以不公开为原则, 以公开为例外”的态度, 导致公共数据的价值无法被挖掘和释放, 为了打破这一局面, 公共数据授权运营中的数据安全问题成为重中之重。

1.3. 公共数据授权运营中数据安全的范围

2025 年 1 月, 国家发展改革委联合国家数据局发布的《公共数据资源授权运营实施规范(试行)》明确要求, 县级以上地方政府及国家行业主管部门在满足数据分类分级保护要求、保障国家安全和公共利益、维护商业秘密及个人隐私权益的前提下, 可将其合法持有的公共数据资源纳入授权运营范畴。对于通过政务数据共享机制获取的其他地区或部门公共数据, 若需用于授权运营, 必须事先取得数据提供单位的正式许可。该规范同时强调, 公共数据资源授权运营需严格遵循依法合规、公平公正、公益优先、

收益合理、安全可控的指导原则。文件对数据安全范畴作出明确界定,具体涵盖三个层面,首要层面是保障国家安全与公共利益不受损害;其次需严格保护商业秘密不受侵犯;第三要全面维护个人隐私及个人信息相关合法权益。

2. 公共数据授权运营中的数据安全的问题

公共数据承载着涉及公民隐私与财产安全、社会公共秩序维护以及国家安全等领域的海量信息。随着数据持续开放和流通,公共数据规模呈现爆发式扩张态势,其风险显著增加。在交易实践过程中,数据窃取、非法篡改、不当利用等安全事件呈现高发趋势,这种安全防护压力持续升级的态势表明,公共数据的开放程度越高、流通范围越广,其面临的安全隐患就越严峻。

2.1. 公共数据流通中个人信息保护和隐私保护的问题

在推动公共数据要素价值最大化的过程中,政府部门将公共数据资源授权给符合资质要求的运营机构进行开发利用。由于公共数据包含海量个人信息,这种深度开发与利用行为可能突破个人信息处理的基本原则并引发数据安全隐患。我国《个人信息保护法》明确规定^[2],要求信息处理必须严格限定在达成目标所需的最低限度内,同时禁止过度采集。该法律通过约束信息处理行为实现权益保护的目标,与公共数据运营追求数据价值深度挖掘的诉求存在本质性矛盾,导致实践中难以避免出现超范围处理个人信息的情况。值得注意的是,公共数据运营会显著提升数据安全风险。尽管运营主体主要处理非敏感类基础信息,但海量数据汇聚后,存在通过关联分析揭示敏感属性的潜在风险。例如,如个人的姓名、性别、年龄等常规数据虽未被归类为敏感信息,但当这些离散信息经系统化整合形成数据集后,即可实现特定自然人的精准识别,甚至可能关联推演出其私密生活信息,进而威胁公民隐私权、人格尊严及财产权益。

2.2. 公共数据流通中政府安全管理水平不足

随着数字技术的快速演进,政府部门的追踪管控面临前所未有的挑战。公共数据的跨区域、跨行业流动已成为常态,但国际敏感信息与商业机密若遭整合分析及非正当使用,极有可能引发企业合法权益受侵犯,危害国家安全的重大隐患。值得注意的是,公共数据授权运营机制中,具备特定资质的私营机构取代了传统公权力机构成为运营主体。相较于以公共利益为导向的公共部门,私营机构在利益驱动下更易出现滥用公共数据谋取私利的情况。在公共数据处理过程中,运营主体必然涉及数据存储环节,这使得数据安全保障成为关键问题。相关统计显示,2022年度我国发生数据泄露事故逾5100万宗,位列全球第三位^[3],数据安全风险犹如悬顶之剑,随时可能引发严重后果。

传统认知普遍将数据安全风险视为私营领域的高发问题,然而随着公共部门数字化进程的深化,政府机关及事业单位的数据泄露事件已呈现常态化趋势。以2023年南昌某高校信息泄露案为例^[4],该事件造成逾3万条师生敏感信息遭非法交易,凸显公共数据防护的紧迫性。相较于商业机构,公共部门承载着国家基础数据、企业核心信息及公民隐私资料的三重安全责任,其数据外泄可能引发社会风险。究其根源,除内部人员蓄意泄密外,还涉及其他三个方面:其一,数据保管环节缺乏系统化的安全规范与加密技术应用;其二,责任主体未严格落实信息安全防护职责;其三,现行法律框架对公共数据存储期限缺乏明确规定,对数据销毁问题缺乏规范流程。值得注意的是,无限期数据存储模式客观上放大了安全风险,而依赖契约约束的数据管理模式因条款模糊、标准不一等缺陷,难以构建稳固的数据防护机制。

2.3. 公共数据流通中数据安全法律规范不完备

当前我国公共数据授权运营领域的法律规范尚未形成系统化规范体系,覆盖范围存在明显局限性。

尽管这些基础性法律对数据流通环节有所涉及,但尚未形成层级分明、逻辑自洽的规范体系,导致不同法规间存在内容重叠、标准差异甚至规范冲突等现象,使得公共数据流通过程中难以建立统一的操作指引和监管标准。现有法律条文多聚焦于运营主体及监管机构在隐私保护与数据安全的原则性要求,而在具体实施细则层面,如如何授权运营的法律规定、数据处理流程的标准、隐私侵权追责机制等领域,尚未制定具有可操作性的专项条款。

《数据安全法》在“政务数据安全与开放”章节的第38条明确规定,国家机关在履职过程中获取的个人隐私、个人信息、商业秘密及保密商务信息等数据,必须严格履行保密责任,依法采取保密措施,禁止擅自披露或违规向第三方提供。然而该条款的适用范围主要限于政府机构,未能覆盖公共数据授权运营涉及的其他参与方。同时该法律对数据市场化运作的规制存在空白,导致公共数据授权运营过程中产生的诸多安全问题难以通过现行法律有效解决。《中华人民共和国网络安全法》特别强调,必须对履职过程中掌握的个人信息、隐私及商业秘密实施严格保护,禁止非法泄露、出售或违规转交他人。《数据安全管理办法》则详细规定了网络服务提供者的责任,要求当信息收集使用规则纳入隐私政策时,应当采用集中编排、显著标识等便于用户查阅的方式呈现。文中虽明确了特殊条款,即“需在用户充分了解数据使用规则并主动授权的前提下,网络服务提供方才能进行个人信息采集”,但针对公共数据授权运营机构是否具备《个人信息保护法》中规定的网络运营主体资格,现行法规体系尚未对此作出充分阐释,这一法律适用边界问题仍存在争议。

3. 公共数据授权运营中数据安全问题的解决办法

3.1. 明确公共数据授权运营的范围

当前政务数据及具备公共事务管理属性的信息已被普遍认定为公共数据开放管理的主要对象,这在多地政策文件中已得到明确。针对实践中存在争议的模糊性数据,亟需建立科学分类标准。以公安系统与交通管理部门所掌握的信息为例,需对公民出行轨迹、通勤方式偏好等数据信息进行讨论,明确其是否纳入公共数据共享范畴。对于医疗机构的诊疗档案、药品采购记录,教育机构的学生学业评估数据,以及企业的经营报表等数据,因其涉及个人隐私和商业机密且缺乏公共治理价值,应排除在政务数据共享体系之外。对于确因科研需求或统计工作需调取此类敏感数据的情形,应当进行规范化审批,要求申请机构在数据脱敏处理后通过加密传输渠道获取,并在使用周期结束后进行定期清理,严禁非公共性数据长期滞留于政府数据平台。在数据应用边界划分方面,国家层面可建立基础公共数据目录,允许跨区域自由流通以提升行政效能;省级行政单位则应细化应用场景分类,针对不同业务场景制定差异化的数据开放清单。这种分层管理模式既能有效平衡数据安全与使用效率,又可减轻政府部门在数据治理中的工作负荷。

3.2. 健全公共数据授权运营安全政府管理监督机制

在推动数据价值利用的过程中,公共数据授权管理必须以安全防护为根本前提。数据安全保障并非阶段性工作,而是持续性要求,需要构建覆盖各环节的监管机制。在数据生成环节,必须严格审查数据来源的合规性,防范非法数据采集及公共数据边界的不当扩展。针对运营环节的安全管控,可采取行政监管与行业自治相结合的模式。同时通过实施罚款、行政督导、司法追责等手段,形成强有力的约束机制,切实提升运营机构的安全责任意识。在数据储存层面,需构建可信赖的数据存管体系,既要采用分布式存储、区块链存证等先进技术,也要通过信息公开机制保障公民的知情权,形成社会监督与技术防护的双重保障。对于数据存续期限的规范,应当突破传统合同约定的局限性,避免因协议条款的任意性导致数据滞留风险。在数据开放应用阶段,应对数据敏感程度、涉密层级、社会价值等分类,实施差异

化的开放策略。对于涉及个人隐私或国家安全的数据资源,可采用去标识化处理、特征模糊化等技术手段,在确保数据效用的前提下实现安全开放。建立政府主导、第三方机构协同、社会公众参与的监管网络。清晰划分参与各方的权责边界。

3.3. 完善公共数据授权运营中数据安全法律制度

公共数据指公共机构在履职过程中生成、收集、处理及管理的各类信息资源,此类信息资产涵盖诸多敏感内容,包括个人身份资料、政府运作数据、核心基础设施信息等。因此,在授权运营环节中,必须对相关公共数据进行脱敏技术处理。但实际操作中,部分授权运营的公共数据存在未实施脱敏或处理不规范的现象。若在此类情形下发生数据泄露、非法篡改或恶意利用事件,将直接威胁社会秩序稳定并危及国家安全。随着公共数据存储日趋集中化,其与国家安全领域的界限逐渐模糊化,对政治治理、经济运行、国防建设、科研创新等关键领域产生深远影响。即便完成全面脱敏的授权运营数据,若被不法分子获取大规模、高价值的数据资源,仍可依托人工智能、大数据分析等前沿技术手段,对国家的政治体制、经济结构及文化领域构成潜在威胁。

因此,需要通过专项立法对各参与方在数据采集、存储、加工及共享等全流程中的安全义务进行明确规定。一方面,特别要强化授权运营平台在实施数据加密技术、制定访问权限策略以及开展风险预警监测等方面的责任。另一个方面,在于优化数据分类管理方法。可依据《数据安全法》确立的基础理论,结合公共数据实际应用场景的具体特点,制定具有针对性的安全防护方案。针对包含个人隐私信息或商业机密的关键数据,必须进行严格的脱敏[5];对于高敏感的数据,则需采取加密存储措施并实施最小化权限管理,同时着力打造“数据可应用不可获取”的技术防护系统。健全公共数据授权运营领域的安全治理体系,重点强化监管机制、隐私保护与信息安全保障等环节的制度化建设。政府部门应当建立覆盖中央与地方的多层次法规体系。在地方性法规制定过程中,应结合区域发展特征与中央政策导向,形成兼具地方特色与全局视野的数据安全规范体系。

4. 结语

公共数据授权运营中的数据安全问题成为重中之重,但现如今公共数据授权运营相关法律规定仍不完善,数据安全面临着个人信息保护和隐私保护、公共数据流通中政府安全管理水平不足、数据安全法律规范不完备等挑战。对此我们应明确公共数据授权运营的范围,健全公共数据授权运营安全政府管理监督机制、完善公共数据授权运营中数据安全法律制度,以此来解决我国公共数据授权运营中安全保障所面临的问题。防止数据信息被滥用、片面解读,避免数据信息被不法集团进行信息买卖并以此进行诈骗行动,维护数据信息秩序和安全。

参考文献

- [1] 宋烁. 构建以授权运营为主渠道的公共数据开放利用机制[J]. 法律科学(西北政法学报), 2023(1): 83-94.
- [2] 刘权. 论个人信息处理的合法、正当、必要原则[J]. 法学家, 2021(5): 1-15+191.
- [3] 尹建国, 周采擎. 公共数据授权运营的困境与法治出路[J]. 海南大学学报(人文社会科学版), 2025(43): 226-234.
- [4] 廖嘉林. 公共数据要素市场化配置的主要困境与法治保障[J]. 宏观经济研究, 2025(3): 50-57.
- [5] 钟晓雯. 公共数据授权运营的授权制度研究[J]. 电子政务, 2025(2): 85-96.