社会科学进展
2023 年 12 月第 5 卷第 6 期

政务数据共享背景下数据安全监管的法治化路径

贾　静

上海政法学院，上海

摘　要 | 在“新时代数字政府建设”的背景下，政务数据共享是推进数字政府建设的核心，数据共享的开发不仅能加快数字政府建设、提升国家治理能力，还能提高政府为人民服务的效率，解决人民群众现实需求，便捷人民生活。然而，由于政务数据涉及多方面，包括但不限于国家利益、公共安全、商业秘密、个人隐私等高度敏感性信息，故在采集、传输、存储、共享与应用中，很容易出现一系列数据安全隐患。因此，必须加强对政务数据的安全监管，规整监管路径，保证政务数据共享在法治道路上有序进行。但是，由于我国尚未形成政务数据共享相关立法，使得数据共享范围和方式不统一，造成了监管难度系数增高。政府层面政务数据安全监管机制不完善，导致一旦出现数据泄漏，没有明确的数据安全管理部门进行监管和问责。此外，政府数据共享项目依赖于项目委托，因第三方的涉入更是增加了数据泄漏的风险。因此，我们必须厘清政务数据安全监管现状，重视现阶段数据安全监管所面临的困境，落实政务数据共享有关立法，建立统一的政务数据分类分级制度，明确政务数据安全监管职能部门，完善政府在数据监管中的问责方式和问责程序，探索更加法治化的数据监管新路径，以期实现政务数据跨地区、跨部门之间的高效率共享。

关键词 | 政务数据；数据共享；数据安全；法治化监管

作者简介：贾静，上海政法学院法律学院2022级硕士研究生，研究方向：民商法、数据法。
文章引用：贾静．政务数据共享背景下数据安全监管的法治化路径［J］．社会科学进展，2023，5（6）：536–548.
https://doi.org/10.35534/pss.0506050

1 引言

为全面实现中国式现代化，要加快促进政务数据共享以及进一步提升政府治理能力与服务水平。我国在政务数据共享建设方面已取得了初步建设成果，各级地方政府开始陆续建设本部门的政务大数据资源中心，政务数据相比过去分散的特点变得更加集中化，同时也暴露出许多数据安全隐患。例如，2016 年发生于浙江省松阳县的一例特大侵犯公民个人信息案，在这个案件中多达 7 亿条公民信息被泄露，8000 余万条公民信息被贩卖。这起公民信息侵权案在当时引起了极大轰动。该涉案团伙主要通过入侵一些政府单位数据系统的方式来窃取部分公民的个人信息，然后导出进行贩卖。从这个案件可以看出，如此巨大的公民数据系统，能够轻易被他人进入并窃取信息，是政务数据安全监管力度不够的显现。此类案件近几年也不在少数，政府和被侵权者往往充当一个后知者的角色，甚至到案发时才发现信息被泄露，以及被侵权的公民如何行使权利救济，当窃取信息者受到法律制裁后，受害人是否能对政府部门未能行使监管职责，请求其损害赔偿？诸如此类的问题都暴露在政务数据共享的过程中，但政务数据共享的相关理论研究却比较匮乏，政务数据共享中的数据安全监管的相关研究更是不足。因此，有必要深入分析政务数据共享中存在的安全隐患，探究数据监管困境，形成相应的法治保障，促进政务数据在法治轨道上实现共享，提高政府社会治理能力和公共服务水平。

2 我国政务数据共享的法治实践及隐患

2.1 政务数据共享发展状况

政务数据共享是发生在政务部门间，因政务部门履职需要，从其他政务部门获取数据资源或者在某些政务部门需要政务数据资源时进行提供的行为。目前，我国关于政务数据共享法律规制主要来源于国家和地方两个方面。国家层面上，2015 年，国务院发布了《促进大数据发展行动纲要》，明确提出建立政府数据统一共享交换平台。2016 年，国务院制定了《政务信息资源共享管理暂行办法》。2017 年实施的《政务信息资源目录编制指南》，并将政务信息分成

https://doi.org/10.35534/pss.0506050

无条件共享目录、有条件共享目录、不予共享目录。2019 年，全国一体化在线政务服务平台建设和管理协调小组办公室印发了《全国一体化在线政务服务平台数据共享服务管理暂行办法》，国家政务服务平台正式在线上开展试运行。2021 年实施的《中华人民共和国数据安全法》，其中第 5 章对政务数据安全与开放进行了规定，从法律层面对于政务数据的开放与共享提出了具体的要求。2022 年 6 月，《国务院关于加强数字政府建设的指导意见》进一步提出“深化数据高效共享”的要求。地方层面上，各地也陆续出台了相应的政策，例如，贵阳市的《贵阳市政府数据共享开放条例》、上海市的《上海市公共数据和一网通办管理办法》、安徽省人民政府颁布了《安徽省政务数据资源管理办法》，广东省人民政府颁布了《广东省公共数据管理办法》等。但总体上看都是对中央立法的简单重复，并没有对政务数据性质进行细致划分，对于数据共享过程中的政府部门如何履行监管职能保障数据安全，以及一旦发生数据安全问题政府部门承担何种责任、被侵权人权利救济程序等关键制度还缺乏明确的规定。

2.2 政务数据共享存在的安全隐患

（1）数据泄漏风险

政务数据共享涉及多个不同部门之间政务数据信息的交换，在这个复杂的交换流程中容易出现信息泄漏风险。此外，政务数据共享建设往往是公私合营模式，政府依赖于委托第三方机制，由第三方提供技术支持完成数据共享项目的搭建，因此，第三方更容易获取到政务数据，很有可能进行不当披露或者违法使用，进而威胁到国家安全和个人隐私安全。实践表明，数据安全泄漏事件已经在陆续发生。目前为止全国范围内，有关政务数据泄漏个人隐私事件不在少数。例如，在 2017 年江西的黎川县，在年度建档立卡贫困户名单的公示附件中，披露出近 1 万条该县贫困户个人信息；安徽省《阳光社区 2017 孕前优生健康检查人员名单》中泄露了 40 对夫妻个人信息；河北省辛集市政府官网颁布的《辛集市 2021 年 10 月城乡特困公示》泄漏 2001 名特困群众身份信息等事件。诸如此类的数据泄露事件已经成为政务数据共享的主要安全隐患。[1]

（2）技术风险与黑客攻击

政务数据往往具有范围广泛、价值高等特点，不仅涉及国家或地方政府的

内部重要信息，还包括企业的商业秘密、公民的个人隐私信息等。[2] 这些数据如果处于分散状态，可能不具有太高的价值，但在数据共享过程中被集中在一起，将能够通过数据精确地刻画出某一个人的特征或者推测出某一政府的内部动态。[3] 对于那些违反犯罪分子或者犯罪集团，这些数据是获得非法财产的一个路径，因此政务数据很容易成为黑客攻击的目标。此外，我国正处于数字政府建设的初步阶段，很多方面尚未形成完备的技术规范，在技术层面尚未成熟，导致信息系统老化，政务数据管理系统的更新迭代速度相对较慢，造成系统漏洞，给黑客带来利用系统漏洞来攻击被保护对象的机会。

（3）数据不当使用风险

在政务数据过程中，涉及多个部门之间的合作，因地区发展水平不同，各政府部门数据政府建设水平处于不同阶段，发达地区有关数字政府立法或政策可能相对完善、人才培养体系相对规范，这就造成政府部门间技术人员专业技能相差过大，以及对数据安全监管规范的力度参差不齐。如果数据安全监管技术人员不具有相应的专业素质，数据安全意识不够，很容易在数据共享过程中，个别政府部门不按照规范或者未经授权进行数据共享，造成数据的不正当使用，甚至带来数据泄漏的风险。此外，数据日常的维修还需要一些专业管理员，对该类型人员并没有较系统的监管，导致其进入数据库以及进行操作时没有明确的限制，容易出现滥用或者窃取数据的风险操作等问题。[4]

2.3 数据安全监管法治化的必要性

大数据安全已成为数字政府建设中关注的焦点问题。数据安全监管决定了政务大数据共享建设的成败。实务中政务数据具有范围广、容量大、类型多、价值高等特点，政府部门储存的数据包括很多种，不单单只是一些企业数据，还有大量公民的户籍数据、住宿登记数据、车辆管理数据、纳税情况数据等各种与个人生活息息相关的数据。[5] 政府在发展大数据业务，提供大数据共享服务的同时，均面临着诸多安全隐患，尤其是个人数据与信息安全的问题，如果政府对政务数据监管不严，就会导致个人数据的泄露和数据安全隐患。因此，加强对政务共享数据的安全监管将会加强数据安全和个人隐私的有效保护。对政务数据安全的监管工作应贯穿于政务数据共享的全过程，应更加系统规范，

https://doi.org/10.35534/pss.0506050

不应流于表面。此外，考虑到政府数据开放中的安全和隐私的保护问题比传统的电子政务环境更为复杂，传统监管模式已经不足以防范数据风险漏洞、隐私信息泄露、数据库自身安全等问题，数据监管模式应更加规范化、法治化。

3 政务数据安全监管困境的原因分析

政府开展政务数据共享时，由于政务数据种类的复杂性，均面临着大数据带来的数据安全隐患问题，对数据安全的监管有助于保护公民的个人信息、尊重公民的隐私权，促进政府信息公开透明，提高政府公共政策制定的高效性、科学性和针对性。目前我国部分省市已经陆续展开政务数据共享工作，但在数据安全监管方面还存在诸多问题，目前，结合各省政务数据共享平台的发展现状，总结当前政务数据安全监管面临的困境包括以下几点。

3.1 数据共享标准不统一

在有关政务数据共享的法律规范中，《政务信息资源共享管理暂行办法》作为指导性原则，明确了政务数据共享“以共享为原则，不共享为例外”，并将其分为无条件共享、有条件共享、不予共享三类，还指出对于不予共享类的政务信息资源，必须有法律、行政法规或党中央、国务院政策依据。但关于涉及个人信息领域的政务数据并未明确规定，哪些个人信息可以共享，哪些个人信息不能共享或有条件共享并没有统一的标准，对于可以共享的涉及个人信息的政务数据中，哪些政务数据共享必须遵循《个人信息保护法》第十三条规定的“取得个人的同意”，《个人信息保护法》第十七条规定的告知义务，哪些政务数据又可不遵循此条规定，这些问题都是含糊不清的。[6] 因此这就导致了各级政府在政务数据共享过程中裁量权过大，对数据共享的种类做出的限制也就不同，数据共享范围没有统一标准，加大了对数据监管的难度，使得数据安全监管范围不明确，不能明确对哪些信息是可以限制的，对哪些信息又是必须限制的。如果政务数据的产生仅仅来自同一个部门，且只有一个部门拥有，不用在其他部门之间进行交流，则数据责任毫无疑问由这个部门进行承担，该部门对其需要直接负责，但政务数据的共享涉及数据在多个部门之间进行交换共享，此时没有统一的共享标准，一旦产生敏感数据泄漏问题，相关的监管责任

很难进行确定。在部门数据共享过程只有对政务数据进行明确划分，根据数据不同的分类和不同的安全等级进行监管，如对敏感数据的监管力度应不同于一般数据，才能使得政务数据安全得到双重保障。

3.2 数据安全监管法律法规体系尚未完备

尽管《数据安全法》已经颁布，且从第六条明确规定：各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。从第六条规定来看，监管体系已明确，即国家网信部门负责统筹，国家安全机关和公安机关在各自职责范围内承担监管。但是，这些政务数据共享有关规定过于笼统，监管标准缺乏统一性和明确性，监管部门职责不明确导致监管效果参差不齐。例如，在具体的数据共享过程中，往往涉及两个以上政府部门，那么政务数据提供部门与数据使用部门之间究竟由哪一方承担监管职责？拥有哪方面监管权力？因数据共享产生的问责究竟由谁启动？采取哪种问责方式和问责程序？这些问题均未有明确的法律规定，导致各级政府在数据监管中各自为政，可能出现不同甚至相反的地方政策，一旦遇到政务数据泄露事件时，受害人不知道去通过哪一个部门寻求救济，权利很难得到保障。

3.3 监管技术手段和工具滞后

随着数据数量的快速增长，传统的数据安全技术手段已经无法满足复杂的需求，需要引入新兴技术和工具来应对数据安全威胁。一方面，在数据平台的建设中，开发人员可以直接拥有访问数据库的权限，不当的操作很容易造成数据的泄露。另一方面，由于数据库存储文件是明文，如果数据存储介质丢失、权限泄露、直接复制文件等情况容易造成数据泄密风险。[7] 对于以上安全漏洞，传统数据监管路径已经不能满足当前阶段对大数据安全的要求，需要不断完善数据加密技术。传统的数据安全监管手段包括但不限制以下几个方面：访问控制、加密技术、安全审计、防火墙系统、数据备份，以及物理安全措施等。传统技术在数据传输、存储等过程中，主要依靠加密等手段来防止数据的泄漏。[8] 但是，由于技术的不断发展和威胁的不断变化，单一的加密手段已经不能应对各式各样的数据安全隐患，应该综合运用以上数据安全监管手段。此外，传统

https://doi.org/10.35534/pss.0506050

安全监管技术多属于被动式防御，即当攻击发生后才会响应并进行处理。然而，随着网络威胁的日益复杂，尤其对于政务数据这种价值极高的信息，很容易成为犯罪分子攻击的对象，被动式防御无法适应现实所需。针对这些漏洞，需要结合新的技术及处理方式，以弥补传统数据安全监管技术的不足之处。

3.4 政府内部监管部门职能不明确

关于对政务数据安全的监管问题，各地方政府机关也陆续出台了相应政策，例如，《山西省政务数据管理与应用办法》第二十一条规定：省网信部门负责统筹协调全省政务数据安全的监督和管理。另外指出，县级以上人民政府公安机关负责政务数据安全指导、监督、调查等工作。《贵州省政府数据共享开放条例》第三十六条规定：省和市、州人民政府大数据主管部门负责对本行政区域政府数据的开发利用实施统一监督管理。《浙江省公共数据条例》第三十八条对政务数据的监管工作也有相关规定。这些政策既规定了对政务数据进行统筹监管的部门，又赋予了各级地方政府一定的裁量权，即各级政府可以在这个指导性原则下去部署各自内部的数据监管部门。但数据监管毕竟是一个相对新兴领域，地方政务数据监管部门可能缺乏相应的经验和技能，此时给予地方政府在监管部署方面过大的裁量权，无法有效地落实这些政策和规范。在具体的监管过程中，大多数政府机构数据系统并没有进行严密的规划，领导层也缺乏相应的数据安全监管意识，[9] 导致部门内部数据管理系统的规划、建设可能分属于不同的部门完成，致使数据监管混乱，成为数据安全监管中的重要问题。

3.5 政府监管人员专业素质偏低

政务数据安全监管需要专业的技术人员和管理人员配合完成，但是当前相关人才相对匮乏，导致监管工作中出现不足。一方面，由于政务数据监管人员都是来自各级政府部门，不同地区教育水平的不同，导致一些政务数据监管人员可能并没有进行统一的相关技能培训，缺乏必要的教育背景，而政务数据监管人员又要求具备广泛的跨领域、运用新兴技术等方面的知识需求，因此，部分监管人员无法适应快速变化的技术和信息环境。[10] 另一方面，政务数据监管

工作的对象相对复杂和庞大，也使得监管工作不同于其他行政工作，过程相对艰辛，倘若政府部门缺乏相应的激励机制和晋升渠道以激发工作人员的责任心和使命感，这份监管工作很难吸引和留住优秀的监管人员，这也导致了监管队伍素质整体降低。因此，政府部门应该改变过去那种认为培训和学习是个人事项的态度，对于政务数据监管人员的选拔应该采取统一培养模式，定期对相关监管人员进行技术培训，提高监管人员数据安全意识，使他们真正了解数据安全的重要性，知道如何处理敏感数据，避免因为操作失误导致数据泄露的风险。实现了监管人员的专业水平提升和优化素质的培养。

4 完善我国政务数据共享监管法治化路径的对策

政务数据的监管既是一个技术问题，又是一个涉及法律制度和政府管理制度的问题。政府数据的监管需要从法律制度、行政部门和社会监督三方面共同去完善，不断探索符合我国国情的监管模式，加强对政务数据的质量、隐私、安全的管理，才能有效地发挥政务数据共享的作用，促进数据的循环利用。

4.1 法律监管

（1）完善政务数据共享相关立法

当前关于政府部门信息共享的主要法律规定有行政法规、部门规章等，但这些规定都过于笼统。因此，完善政务数据共享相关立法对数据安全十分有必要，具体建议如下：首先，我国应制定一部统一的政务数据共享法，对政务数据的“无条件共享、有条件共享、不予共享”三种分类再进一步进行列举，明确其具体范围。另外，对拒绝共享的理由在政务数据共享法中列出限制原因，同时对什么行为属于政务数据共享不当行为，以及不当行为的法律后果进行明确规定。其次，完善数据保护立法，对于政务数据涉及的个人数据主体，其权利虽然有《个人数据保护法》进行保障，但在数据共享中，一旦个人数据被泄漏时，受害人能否请求损害赔偿仍然需要专门法律来具体规定，例如《个人数据保护法》第六十九条规定，处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。[11] 单从此法条，并不能推断出个人信息侵权损害赔偿是否适用于行政机关，以及政府部门在何种

https://doi.org/10.35534/pss.0506050

情况下可以需要赔偿或者可以免责也并不明确。此外，政府部门在政务数据共享中如何保障个人数据主体的权利，在监管中承担何种责任、被侵权者权利保障的程序为何、救济措施为何等关键制度还缺乏明确的规定，故有必要完善数据保护立法，对政务数据中有关个人数据权利再进一步进行规范。

（2）健全政务数据分级分类保护制度

政府数据的共享过程不仅仅是单一数据信息的披露，它还会涉及各种各样的信息，如个人隐私、商业秘密等，《政务资源共享管理暂行办法》并未对数据的种类做出明确的列举式区分，导致在共享过程中就会出现数据安全问题。首先，应对政务数据共享种类做出明确的法律规范，加快不同部门之间的数据互享。其次，在“以共享为原则，不共享为例外”的基础上，做好对政务数据的分级分类工作，进一步划分哪些个人信息可以共享，哪些个人信息不能共享或有条件共享。对于不同数据应采取不同程度的监管措施。对于最高等级的机密数据，必须采用最高的安全监管措施，并在数据的共享过程中由监管部门进行定期的审查和检查。此外，其他更低级别的政务数据可由数据监管部门采取相适当的安全措施，以避免数据发生泄露或损坏等情况。[12]

4.2 行政监管

（1）建立统一的数据监管职能部门

各级政府内部建立专门的数据安全职能部门是在制度和组织上保障政务数据安全管理的重要举措。统一的监管部门能够有效降低政务数据在多个部门之间流转的安全风险，可以实现规范化的监管流程和标准，同时将多个审批环节整合成一个，更加简化了管理程序，避免了重复投入和协调困难等问题，提高了监管效率。[13] 具体举措如下：第一，设置监管政务数据安全的专职部门，对数据共享的全过程进行负责，在共享前对数据进行安全风险分析、评估、预测，在共享中进行全程监督，在共享后对可能导致较大范围黑客攻击的敏感数据，及时发布预警信息，提出应对策略。[14] 第二，建立政务透明与行政问责机制，对于政务数据的监管要做到公开透明，从而及时发现和纠正数据监管方面存在的问题，对不按照规定进行监管、滥用监管权力、怠于履行监管义务的部门，要进行问责处罚，以提高政府部门在信息共享中的责任感。

（2）加强数据监管人员人才培养

政府部门工作人员对推动政务数据共享工作发挥着重要作用。要从多方面对数据工作人员进行人才培养，不仅要在技术层面进行指导，还要在思想方面进行教育。数据监管工作不同于其他行政部门，其专业性要求更加严格。目前，各级政府数字政府平台的搭建往往依赖于第三方机构，对于在数据监管工作中，一些安全检测问题往往也是由第三方来完成，即使是政府内部人员来进行监管，但由于其技术和专业的限制，很难达到预期的效果。为解决此类问题，政府可以与高等院校、职业学校等教育机构开展合作，开设符合行业需要的数据监管课程，进行定点人才培养，引进更加专业的监管人员。此外，对于监管工作人员的思想教育也不可忽视，政府可以定期对数据监管人员以及部门领导进行思想培训，增强其数据保护安全意识，激励其更好地履行职责。

4.3 社会监管

社会公众是监督政务数据安全的重要主体。公众参与数据安全监管不仅可以提高政务数据共享的质量，还可以提高政府服务公众和解决社会问题的能力。[15] 首先，政府部门应加强信息公开，及时公开与之相关的数据采集、处理、共享等各个环节的情况，为公众提供及时的参考资料和反馈渠道，让社会公众知道对于哪些信息政府可以行使查阅、复制权，以防止政府机关随意以查询、复制侵害公民的权利。[16] 其次，积极建立数据安全投诉举报奖励机制，设置便民的投诉方式，调动社会公众参与监督的积极性，从而防止数据遭到非法操作和滥用。此外，政府部门还要做好普法工作，对相关的法律责任和法规内容进行及时、准确、全面的宣传，让公众知晓如何在法律规范下保障自己的数据权益，增强公民数据安全防范意识。

5 结语

21 世纪以来，世界范围内掀起了以数字化推动政府运行模式的变革浪潮，我国也不例外，2017 年 10 月，习近平总书记在党的十九大报告也提出“加快建设数字中国”。数字政府背景下，政务信息化系统在为公民提供公共服务方面发挥着重要作用。目前，数据结构日趋复杂，给政府数据收集使用、共享开放

https://doi.org/10.35534/pss.0506050

及监管带来了前所未有的挑战，政务数据安全监管已成为当下政务数据共享发展的一项重要任务。[17] 本文阐述了我国政务数据共享现状，着重分析了存在的数据安全隐患，以及数据安全监管面临的问题，紧紧围绕数字政府治理和公共服务的改革需要，贯彻共享发展理念。从法律制度、政府部门、社会公众三个角度探索了数据安全监管的法治化路径，以期实现更符合我国国情，更符合中国式现代化理念的政务数据共享策略。

参考文献

[1] 铁德铭．数字政府建设的法治困境及其因应［J］．西北民族大学学报（哲学社会科学版），2023（3）．

[2] 朱海涛．政务大数据开放及共享安全问题研究［J］．网络安全技术与应用，2022（6）．

[3] 郭泽炎．大数据环境下的数据安全研究［J］．电子世界，2017（2）．

[4] 唐宏波，张宁．公安数据开放风险评估模型与管理措施［J］．网络安全技术与应用，2023（4）．

[5] 潘文静．构建数字化智能化的政府运行新形态［EB/OL］．［2023-11-22］．https://baijiahao.baidu.com/s?id=1767541489884320512&wfr=spider&for=pc．

[6] 邢会强．政府数据开放的法律责任与救济机制［J］．行政法学研究，2021（4）．

[7] 达钰鹏，陈艳春．基于零信任模型的电子政务信息共享研究［J］．信息安全研究，2021，7（8）．

[8] 王征，朱光．政务数据治理中的弱隐私信息追踪监测模型研究［J］．情报杂志，2022，41（11）．

[9] 迪莉娅．政府开放数据的监管模式研究［J］．情报理论与实践，2018，41（5）．

[10] 王宇航，王西．论大数据在政府监管应用中的法律障碍与完善［J］．河南社会科学，2020，28（5）．

［11］邢会强．政务数据共享与个人信息保护［J］．行政法学研究，2023（2）．
［12］倪千淼．政府数据开放共享的法治难题与化解之策［J］．西南民族大学学报（人文社会科学版），2021，42（1）．
［13］黄璜．中国“数字政府”的政策演变——兼论“数字政府”与“电子政务”的关系［J］．行政论坛，2020，27（3）．
［14］沈汝发．“数字政府”如何赋能中国式现代化新实践［N］．新华每日电讯，2023（1）．
［15］王娟，杨现民，高振，等．大数据时代教育政务数据开放共享的监管机制［J］．现代远程教育研究，2022，34（3）．
［16］张珊．打造智慧高效的数字政府［N］．联合日报，2023．
［17］张茂月．大数据时代个人信息数据安全的新威胁及其保护［J］．中国科技论坛，2015（7）．

The Legalization Path of Data Security Supervision under the Background of Government Data Sharing

Jia Jing

Shanghai University of Political Science and Law, Shanghai

Abstract: Under the background of “construction of digital government in the new era”, government data sharing is the core of promoting the construction of digital government. The development of data sharing can not only accelerate the construction of digital government, improve the national governance capacity, but also improve the efficiency of government to serve the people,

https://doi.org/10.35534/pss.0506050

solve the practical needs of the people, and facilitate people's lives. However, since government data involves many aspects, including but not limited to national interests, public security, trade secrets, personal privacy and other highly sensitive information, it is easy to appear in the collection, transmission, storage, sharing and application, a series of data security risks. Therefore, it is necessary to strengthen the security supervision of government data, regulate the supervision path, and ensure the orderly sharing of government data on the road of rule of law. However, because China has not yet formed the relevant legislation of government data sharing, the scope and method of data sharing are not uniform, resulting in an increase in the difficulty coefficient of supervision. The government data security supervision mechanism is not perfect, resulting in the absence of a clear data security management department for supervision and accountability in the event of data leakage. In addition, government data sharing projects rely on project mandates, and the involvement of third parties increases the risk of data security leaks. Therefore, we must clarify the current situation of government data security supervision, pay attention to the difficulties faced by data security supervision at this stage, implement relevant legislation on government data sharing, establish a unified government data classification and classification system, clarify the functional departments of government data security supervision, improve the government's accountability method and accountability procedure in data supervision, and explore a new path of more legalized data supervision. In order to realize the efficient sharing of government data across regions and departments.

Key words: Government data; Data sharing; Data security; Law-based