数字政府建设面临的多重风险及其规避策略

王广辉 郭文博[1]

【摘 要】:数字政府建设是数字中国建设的重要内容,是推动政府治理体系和治理能力现代化的重要支撑,也是推动高质量发展、全面建成社会主义现代化强国的必然要求。在数字政府建设中,面临着技术风险、管理风险、数据风险、安全风险。这些风险的成因主要包括:关键核心技术发展滞后、体制革新不能适应发展需要、数据供给能力有限、相关法律法规与管理制度不完善、数字政府建设生态环境欠佳。规避数字政府建设风险,应加强原创性、引领性科技攻关,提高关键核心技术创新能力;推动数字政府体制革新,更好地适应数字政府建设需要;提升数据安全防护水平,提高数据供给能力;完善数字政府建设相关法律法规和管理制度,提升数字政府服务能力;优化数字政府生态环境,提升数字政府建设主体素养。

【关键词】:数字政府建设 数字政府治理 治理体系现代化

【中图分类号】:D63**【文献标识码】**:A**【文章编号】**:1003-7543(2022)03-0146-10

党的十九届四中全会提出,要“建立健全运用互联网、大数据、人工智能等技术手段进行行政管理的制度规则,推进数字政府建设”;党的十九届五中全会提出,要“加强数字社会、数字政府建设,提高公共服务、社会治理等数字化智能化水平”。数字政府建设是数字中国建设的重要内容,是推动政府治理体系和治理能力现代化的重要支撑,也是推动高质量发展、全面建成社会主义现代化强国的必然要求[1]。

数字政府建设是指政府充分利用计算机、大数据、人工智能、云计算、区块链、5G 等新一代信息通信技术,以政务数据治理为抓手,通过重组政府组织框架、再造政府业务流程、优化政府政务服务的方式,全面提高政府公共服务、社会治理、市场经济调节、市场监督、环境保护的能力,有效促进政府治理体系和治理能力现代化。

随着我国数字经济的迅猛发展及其在经济社会各领域的广泛应用,各地数字政府建设步伐明显加快,一些地方还制定出台了关于数字政府建设的纲要和专门性政策文件,为数字政府建设实践提供了具体的行动依据和建设指南。然而,现阶段无论是学术界还是政策层面,对数字政府建设可能面临的风险还缺乏全面而系统的分析,这对我国推进数字政府建设、提高公共服务的数字化智能化水平是不利的。基于此,本文将研究的重点聚焦于数字政府建设面临的多重风险,剖析其形成的原因,并提出规避风险的针对性建议。

一、数字政府建设面临的多重风险

“凡事预则立,不预则废”,只有充分考虑到数字政府建设可能面临的风险,并积极予以防范,才能更好地推动数字政府建设。这里认为,数字政府建设中可能面临技术风险、管理风险、数据风险、安全风险。

(一)技术风险

技术风险指的是支撑政府数据有效设计、开发建设、平台稳定运行的相关技术,在助推数字政府建设过程中存在一定的风

[1]**作者简介**:王广辉,中南财经政法大学法学院教授、博士生导师;郭文博,中南财经政法大学法学院博士研究生。

险，主要体现在技术标准规范风险、技术支持风险、技术防护风险、技术法律法规风险等方面。

一是技术标准规范风险。在推进数字政府建设中，可能因管理体系、关键核心技术不符合应用系统设计、建设和运行标准规范，而出现数字政府基础设施建设、运行平台、服务业务等层面技术不达标的现象，致使数字政府系统难以有效运行，从而引致风险。

二是技术支持风险。技术支持风险指的是因关键核心技术发展滞后，在技术支持数字政府平台运行过程中出现技术漏洞，不能有效保证政府数据平台稳定运行。例如，当关键核心技术发展滞后时，身份识别认证、接口访问链接、下载格式模式等技术出现漏洞，难以维持数字政府平台顺利运作。如果身份识别认证技术出现漏洞，就会导致用户不能通过提交用户信息身份进行快速注册与认证，进而不能及时有效获取政府平台数据；如果接口访问链接技术出现漏洞，就会导致用户平台接口访问的约束性增强，政府数据平台连接跳转的有效性降低；如果下载格式模式技术出现漏洞，就会导致政府数据下载的可用性与稳定性大为减弱。

三是技术防护风险。技术防护风险指的是技术在防护黑客攻击、防止数据泄露、阻止信息窃取等方面面临的不确定性。比如，因核心技术不成熟，或数据脱敏、数据沙箱、数据加密、数据屏蔽等技术的运用、标准及操作方式不成熟，而难以防止外界对平台的攻击和数据的泄露、被窃取。

四是技术法律法规风险。新一代信息通信技术的广泛应用对现有法律法规构成了较大的冲击。比如，区块链技术具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等重要特征[2]，对现有的网络安全法律法规、合同法、物权法、金融法律法规等提出了新的要求。人工智能容易引发失业和歧视、技术责任认定和履行等问题，对数据隐私和安全相关法律法规也形成了冲击。

（二）管理风险

管理风险指的是在数字政府建设中管理主体、管理组织、用户管理、运营管理等方面可能产生的风险。

一是管理主体的风险。数字政府建设运用新一代信息通信技术提升了政府治理能力，推动了政府治理体系现代化，同时也增加了政府治理的复杂性和多样性。由于政府规模的限制，在推进数字政府建设过程中，政府部门需要通过外包服务等多种方式引入新的参与主体，运用市场化的力量来处理“非关键性”技术或基于技术系统之上的部分业务，使政府部门从技术性、技能性的烦琐工作中解放出来，从而致力于战略制定、宏观协调和制度建设等工作，提升政府治理效率[3]。但是，新的市场化力量的参与，引致原有的治理主体结构、机制发生变化，对政府部门、新的治理主体的协调性提出了更高的要求。

实践中，政府部门与新的参与主体之间的管理制度、管理机制在较短时间内难以有效整合，这就会导致数据在跨部门的生产、使用、共享过程中引发矛盾冲突[3]。更为重要的是，市场主体的首要原则仍然是追逐利润，因而可能出现新的参与主体利用自己在数据和技术方面的优势争夺话语权和相关权力、侵蚀公共利益的问题。如何在“大胆放手”与“严格监管”之间找到平衡点，是摆在政府部门面前的难题。

二是管理组织的风险。数字政府建设将新一代信息通信技术引入政府组织，对原有的组织架构、治理方式、组织功能等造成了冲击。一方面，存在组织与技术的整合风险。新一代信息通信技术需要与政府组织进行较长时期的磨合，在磨合过程中，新技术变更与组织整合可能出现不一致性，容易造成技术体系与组织体系的不匹配[3]。

另一方面，存在与传统政府组织结构的冲突风险。数字政府要求政府体系拥有统一的信息数据平台，实现信息共享、数据共管，减少组织的中间层级以实现政府组织结构在纵向和横向上的互动、协同。而传统的政府组织按照级别和职责划分成多个层次

[4]，且各层次部门之间的职能边界较为清晰，导致地方政府部门在信息系统中的数据资源“断裂”，制约了政府数据的共建共管、共享共用。

三是用户管理的风险。数字政府建设可能会对政府数据平台管理用户造成冲击。数字政府建设会打破原有的与用户互动交流的模式，利用数据平台征集用户信息、及时反馈纠错信息、有效回复用户，强化数据平台与用户之间的互动联系。同时，数据平台对开发者提供的应用申请进行安全测试，收集开发者身份信息、数据等，这势必会增加数据平台运营成本。

四是运营管理的风险。运用新一代信息通信技术对政府数字平台运行的规范与约束存在一定冲击，如果不能有效设立平台安全保障机构，定期开展平台风险评估，及时制定应急预案，就可能出现数字平台运行脱离原来轨道的风险，增加数据平台管理成本。

（三）数据风险

数字政府的基础性资源是数据。数字政府的数据既包括了政府内部事件、活动、流程、制度等信息，又包括了公共管理及服务相关的外部环境与对象等信息。数字政府的数据风险是指在处理政府内部事件、活动、流程、制度等信息，以及处理公共管理及服务相关的外部环境与对象等信息过程中面临的不确定性。具体来看，主要包括数据采集和采集质量风险，数据供给质量和效率风险，数据处理、整合、共享、交换、运营风险等。

一是数据采集和采集质量风险。它是指将政府所关注的内外部信息数据化的不确定性。一方面，将政府内外部信息数据化面临一定的成本，同时也存在一定的滞后性；另一方面，可以数据化的政府内外部信息所占比例较小，依据这些有限的信息进行决策、从事公共管理和公共服务供给可能出现较大偏差。

二是数据供给质量和效率风险。能否准确地将政府内外部信息数据化，会直接影响到数据供给质量和效率。例如，不少数据存在更新不及时、不完整、不准确、不一致等问题，这会直接影响到公共数据的开放利用进程。

三是数据处理、整合、共享、交换、运营风险。主要体现在数据流动风险上，数据流动风险很可能出现在数字政府组织与业务的应用系统内，也可能出现在底层的算法与技术系统内，还可能出现不同的数据应用系统之间。当前，我国公共数据的编目、归类、采集、汇集等方面均存在指标口径差异、技术标准不一等问题，导致数据难共享、难整合、难流动。因缺少统一元数据标准，不同系统、部门间数据兼容性欠缺，数据流通性和共通性弱，造成数据封闭现象。

（四）安全风险

数字政府建设面临的安全风险总体可以归纳为公民个体安全、社会安全、国家安全三个层面。安全风险是数字政府建设必须考虑的重要内容，在某种意义上说，能否有效防范安全风险，将安全风险控制在合理的范围内，直接决定了数字政府建设的成败。

一是公民个人隐私与信息安全保护风险。云计算、大数据、物联网、移动互联、区块链等新一代信息通信技术的发展，在提升生产生活便利性的同时，对公民个人隐私与信息安全保护构成了严重威胁与挑战。依托更为先进的信息通信技术，能够获得更好的信息技术服务，但也会在信息系统中留下更多的信息数据，这也就会更容易导致公民个人隐私与信息的泄露[5]。

一方面，新一代信息通信技术应用很可能模糊非隐私信息与隐私信息的界限，造成公民个人隐私保密性程度下降，增加公民个人保护其隐私的难度。另一方面，新一代信息通信技术更新迭代速度较快，保护公民个人隐私与信息安全的手段和技术难以及时跟进，这就增加了公民个人隐私泄露或被非法利用的风险。

二是社会风险。推进数字政府建设有助于扩大政务服务范围、提供更为便捷的政务服务、提供更为透明的政务服务信息，但也可能出现“不平衡”“不充分”的问题[6]。就“不平衡”而言，在数字政府建设中，存在地区或省份、城乡、收入三大差距问题。

从地区或省份差距来看，清华大学数据治理研究中心发布的《2020 数字政府发展指数报告》将 31 个省级政府按照数字政府发展指数差异划分为“引领型、优质型、特色型、发展型、追赶型”五种不同发展程度的类型[7]，其中，“引领型”省份有 4 个，分别是上海、浙江、北京、广东，得分均在 70 分以上；“追赶型”省份有 9 个，分别是陕西、辽宁、黑龙江、河北、甘肃、西藏、云南、新疆、青海，得分均在 50 分以下。

按地区来看，东部地区的数字政府发展指数总体水平明显高于西部地区和东北地区。由此可见，在不同地区或省份之间，数字政府建设水平还存在较大的差异，不同地区或省份的民众在享受数字政府建设所带来的便利和服务上还存在较大的差距。

从城乡差距、收入差距来看，城镇居民、收入水平较高的人群在使用信息技术以及数字政府提供的数据信息上处于优势地位，明显高于农村居民、收入水平较低的人群。这三大差距的存在，必然会导致“数字鸿沟”的出现。从某种程度上说，数字政府建设水平的差异，体现了各地数字经济、数字社会发展水平的差异，因为数字经济、数字社会发展程度越高，越会对政府提出更高的要求，推动政府的自我变革，倒逼地方加快数字政府建设[6]。

“数字鸿沟”的出现和不断拉大，可能会引发社会风险。就“不充分”而言，当前地方数字政府建设中还存在诸多乱象，既有因缺乏顶层设计、各部门各自为政而出现的“数据孤岛”“数据烟囱”问题，又有地方政府只重视网络回应诉求、忽视线下实际问题解决和推进制度化公民有序参与而出现的“尾巴主义”问题，还有地方政府重视与数字、数据相关的会议、商展而轻视落地机制方法的新“形式主义”问题，地方政府将数字技术使用偏向于某一领域或方面而出现的“选择性执行”问题，地方政府重视与数字经济和数字社会相关的新部门设置、忽视流程机制重构而出现的“叠床架屋”问题[6]。这些都是数字政府建设“不充分”的表现，表明当前不少地方的数字政府建设与国家治理体系和治理能力现代化的要求还存在较大的差距。这些问题也会直接影响到社会公众对数字政府建设的支持度，若长期得不到纠偏，也会引发社会风险。

三是国家安全风险。2014 年 4 月习近平总书记在中央国家安全委员会第一次会议上提出要“坚持总体国家安全观”，明确了国家安全体系的主要内容，其中就包括了科技安全、网络安全。与数字政府建设密切相关的国家安全风险主要表现为两大方面：

一是国家安全系统遭受攻击的风险。在数字政府建设中，信息系统的漏洞缺陷是难以避免的，具体包括信息系统设计的漏洞缺陷、信息系统软硬件中隐藏的漏洞、系统集成的配置漏洞、信息系统的管理漏洞等。在国家之间的竞争中，这些漏洞的存在，可能给外部敌对势力的攻击留下缺口。外部敌对势力可能蓄意利用各种手段对政务信息系统的组件、结构和信息进行篡改和销毁等，直接危及数字政府的运行，甚至引致整个系统的瘫痪和不可恢复[3]。例如，数字政府大数据平台的网络环境无法确保永久安全，当计算机与云服务器的信息内容存在安全漏洞时，云服务商与运营商受到黑客攻击的可能性增加，可能导致数字政府大数据平台的云政务信息丢失。此外，数字政府大数据平台还面临因恶意篡改而引致的云信息内容被更改或删除的风险，面临因黑客恶意拦截或盗取而引致的云信息内容被拦截或盗取的风险。

二是国家安全信息遭受泄露的风险。数字政府不仅要为社会提供高质量的公共服务，而且要为国家提供高质量的信息机密保障。同时，政府处在治理体系的中心位置，通过各种信息技术汇聚大量的政府职能部门信息、社会信息、城市信息、市场信息等数据资源，这其中就包括一些涉及国家安全的信息。但在数字政府建设中，更多的信息被公开、共享，与国家安全有关的信息变得更容易检索，在各种数据挖掘、处理、分析技术和软件的加持下，国家安全信息被泄露的风险也大大增加。

二、数字政府建设风险探源

深度解析我国数字政府建设面临的多重风险及其成因，有助于采取更具针对性的策略。总体而言，我国数字政府建设的风险成因主要包括：关键核心技术发展滞后、体制革新不能适应发展需要、数据供给能力有限、相关法律法规与管理制度不完善、数字政府建设生态环境欠佳。

（一）关键核心技术发展滞后

数字政府建设的重要前提条件是拥有并依赖先进的关键核心技术。关键核心技术是提高数字政府治理效率和安全水平的基本保障。当前，我国还面临着原创性和引领性科技攻关能力不足、关键零部件和核心技术受制于人的窘境。按照《科技日报》梳理的“卡脖子”技术清单，我国至少有 35 项技术与国外先进水平还存在较大的差距。如我国的高端芯片制造工艺落后国际先进水平 2 代以上，95%的高端专用芯片依赖进口[8]。

关键核心技术发展的滞后，大大增加了我国推进数字政府建设的风险，也是技术标准规范风险、技术支持风险、技术防护风险产生的最主要原因。突破原创性、引领性科技攻关和关键核心技术需要长期的技术与行业经验积累，需要依靠长周期、系统性的研发投入以及整个创新链与产业链的高度融合，需要高素质的研发人员队伍支撑。这些都注定了突破原创性、引领性科技攻关和关键核心技术之路并非坦途。

（二）体制革新不能适应发展需要

体制革新理念滞后、体制革新内容不完善、体制革新方式不恰当是造成现阶段数字政府建设管理风险的主要诱因。加快推进数字政府建设，要求革新政府治理理念，以更好地适应政府数据治理的需要。一方面，受传统的政府治理理念和治理思维惯性影响，部分政府管理者倾向于过度集中权力而对政府治理理念革新的重视程度不足；另一方面，因数字政府建设明显提速，一些地方政府和管理者的管理理念更新速度赶不上快速变化了的要求。体制革新相关制度不完善、权力结构设置不合理、权责关系不明晰是跨地区、跨部门、跨层级难以实现数据信息共享共用的主要原因。

缺乏制度设计引领的体制革新，容易形成条块分割的管理体制[9]，使得各地区、各部门、各层级仅依靠自身的财力物力对本地区、本部门、本层级数据平台进行建设、运营、管理、维护，各地区、各部门、各层级信息系统相互独立，最终导致各地区政务服务平台建设发展不平衡，数据平台不能协调一致。权力结构设置不合理将会导致数字化政府在数据治理过程中决策机制不明确、决策目标不统一[10]。在数字政府建设过程中，数据信息的所有者、使用者、管理者之间权责不明晰，容易导致数字政府治理工作责任落实和执行不到位以及数据信息的利用、安全、保密等方面出现问题。体制革新方式不恰当，将导致体制革新效率下降，引起用户管理和运营管理风险。

（三）数据供给能力有限

在数字政府建设进程中，数据供给能力的限制可能引发数据采集和采集质量风险，数据供给质量和效率风险，数据处理、整合、共享、交换、运营风险。数据采集人员对数据采集对象的认知能力有限，将导致数据采集人员对数据理解的偏差，引致数据冗余和数据残缺，增加后续数据清洗、整合、解读、运用、维护的人力和财力成本，降低数据供给质量和效率，从而使得数字政府数据治理决策的科学性降低。不仅如此，数据造假和数据不符合规范均增加了数据的处理难度、整合成本，影响了数字政府信息共享、交换、运营效率。此外，数字政府的大数据平台管理者和操作者的管理和操作灵活度低、宏观认知能力差、预见性弱，很可能导致数据在处理、整合、共享、交换、运营过程中出现明显的失误或滞后，引致数据风险。

（四）相关法律法规与管理制度不完善

相关法律法规的不完善和管理制度的缺失，尤其是政府数字化监管体系的缺位，导致公民个人隐私与信息安全保护受到挑

战，存在“不平衡”“不充分”的社会风险隐患以及国家安全系统遭受攻击、国家安全信息遭受泄露的风险。一方面，在推进数字政府建设中，相关法律法规不健全且衔接度不够，可能导致数字政府在数据和信息开放运营中容易出现漏洞，致使信息安全遭受威胁。另一方面，相关管理制度还存在缺失和值得改进之处。

数字政府的数据和信息收集、加工、整合、运用标准和规范制度不完善，数字政府的数据和信息开放标准和流程不规范，数字政府的数据和信息保障标准、保障体系不完善，数字政府数据开发和信息挖掘准入许可等不规范，均是数字政府管理制度缺失的重要表现。各个管理制度之间缺乏有效衔接，也是诱发公民个人风险、社会风险、国家安全风险的重要原因。不仅如此，现阶段，数字政府监管体系尚不完善，对数字政府数据信息的开放进度、使用进度、维护进度等跟踪监控不足，容易导致信息系统遭受破坏、信息安全遭受挑战。尤其是网络安全等级保护制度的落实和执行难到位，职责划分不明确，技术防护方案未部署，网络等级测评、跟踪、监控、整改、监督不到位，导致网络安全等级保护对政务云安全防护的实效性大为削减。

（五）数字政府建设生态环境欠佳

数字政府建设生态环境是数字政府建设的助推器。如果数字政府建设生态环境不佳，就可能导致数字政府建设的初始成本、学习成本、适应性预期成本的增加，使路径依赖问题更加凸显。按照路径依赖理论，人类社会中的技术演进和制度变迁一旦进入某种路径，就可能对这种路径产生依赖。

数字政府建设既涉及技术演进，又涉及相关制度的变迁，因而也会产生路径依赖的问题，这就给数字政府建设带来了多重风险，如信息互联互通效应横纵失衡、“信息孤岛”效应严重、数据利用效率低下、大数据管控难度增加等[3]。缓解路径依赖引发的诸多问题，应不断优化数字政府建设生态环境，这就需要政府部门、企业、科研单位和人员、投资机构等众多参与主体共同参与数字政府生态环境建设和治理。

三、数字政府建设的风险规避策略

新时代加强数字政府建设，有利于释放数字经济发展潜能、应对数字经济发展带来的新挑战，也有利于加快推动社会治理精准化、公共服务高效化、社会互动信任化，更有利于对政府自身进行全方位、全领域、全时空系统性和数字化重塑[11]。规避数字政府建设风险，应从如下方面着手：加强原创性、引领性科技攻关，提高关键核心技术创新能力；推动数字政府体制革新，更好地适应数字政府建设需要；提升数据安全防护水平，提高数据供给能力；完善数字政府建设相关法律法规和管理制度，提升数字政府服务能力；优化数字政府生态环境，提升数字政府建设主体素养。

（一）加强原创性、引领性科技攻关，提高关键核心技术创新能力

准确把握原创性、引领性科技攻关和关键核心技术的内涵、特征、规律、趋向，科学谋划原创性、引领性科技攻关和关键核心技术的突破路径，是我国数字政府建设的基础性保障，已成为我国在百年未有之大变局中赢得竞争、推动经济社会高质量发展、实现第二个百年奋斗目标的必然要求和重要抓手。具体而言，要从如下方面着手：

第一，着力强化基础研究，实现从“中国制造”到“中国创造”。加强原创性、引领性科技攻关必须强化基础研究投入、加快基础研究平台建设、加强基础研究人才培育、增强基础研究设施布局，着力提升基础研究能力和水平。一是完善、优化、健全基础研究投入机制。持续优化中央和地方基础研究财政资金支出的规模、结构，由政府、社会和市场共同设立基础研究基金，加大全社会基础研究投入力度。

二是推动基础研究平台落地。通过规划和落实组织制度、经费管理制度、科研评价机制等方式加快“双一流”高校建设和科研院所建设的进程，推动形成重大科技突破的策源地。通过优化创新平台发展模式，实现创新资源由粗放分散到共享共用。

三是培育基础研究的主力军。升级学科专业体系，瞄准基础研究前沿和关键领域，加快培养基础研究紧缺人才，加强基础学科培养能力建设。

四是布局基础研究设施。通过加快 5G 技术、融合通信技术、物联网技术、云存储技术、区块链技术等的部署和应用，为攻克“卡脖子”的关键核心技术提供基础研究设施基础。

第二，推进科研成果转移转化，促成从资源禀赋到现实生产力的转化。从目前我国成果转移转化情况来看，还有很大的潜力可挖，加强成果转移转化已迫在眉睫。一方面，不少高校、科研院所的专利难以被发现、被应用；另一方面，不少中小企业难以获取所需的专利技术。

这些问题的出现，主要是因为科技创新成果产业化转化平台尚未完成系统布局，难以有效对接专利技术的需求与供给，尤其是高校、科研院所和中小企业的专利技术需求之间对接水平、对接能力、对接效率较低，这不仅导致高校、科研院所的大量专利技术被闲置，而且导致中小企业等市场主体获取所需要的专利技术难度增大。

发挥科技成果转化平台集聚新兴产业、培养和吸纳专业化转移机构和人才等方面的重要载体支撑功能，系统性布局科技创新成果转化平台，显得十分必要和紧迫。为此，需进一步系统性布局科技成果转化平台，为推动科技创新成果产业化顺利转化奠定基础，为国家技术转移体系建设搭建重要载体。坚持“成果产业化”的原则，是攻克“卡脖子”技术难题的关键。为了实现创新技术的产业化应用，应鼓励广大科技工作者到基础研究一线去，完成基础研究源头创新的使命和责任。持续加强科技管理改革，加强基础研究单位配套设施建设，提高专利部门技术保护力度，努力克服科技成果转化障碍。

（二）推动数字政府体制革新，更好地适应数字政府建设需要

第一，优化数字政府的管理职能与组织设置。首先，建立政府数据治理委员会，承担统筹协调管理、数据资源共享等工作，负责统筹规划、协调推进数字政府数据共享、信息共用、资源共建的重大事项。其次，数字政府建设的管理职能要突出向数字政府管理创新转变，充分发挥数字政府管理指挥中心的职能优势，进一步加强数字政府管理政策统筹协调，加强与发改、经信、教育、财政、人社、工商、金融、交通等部门的联络沟通协作，建立沟通紧密、制度完善、协调有力、覆盖广泛的沟通协作平台。最后，围绕职能转变需要，不断完善能体现数字政府管理创新，且有利于优化内部机构设置和数字政府治理的内部控制制度[12]。要围绕数字政府管理创新管理职能定位，打破传统政府管理工作部门内部机构设置模式，体现高效、充分、扎实的数字政府管理创新元素，着力优化内部机构设置，减少综合性数字政府管理处室，引导科研人员力量向业务处室倾斜。

第二，适当改进数字政府管理负责人选拔机制。通过优化和调整数字政府管理负责人结构，支持技术专家、科学家、工程师、企业家进入数字政府管理队伍，为传统的数字政府管理队伍注入新鲜血液。这样才能保证在面对专业领域或复杂局面时，负责人不会因专业能力或行业经验的缺失，造成决策上的重大失误和不必要的损失。

（三）提升数据安全防护水平，提高数据供给能力

第一，建立数据安全技术防护体系，为数据安全提供保障支持。要在提升关键核心技术的同时，加强数据安全风险管控核心技术联合攻关，包括数据安全风险预防防护、处理处置、安全监测、预警防范以及数据加密、数据访问、数据控制等重要数据安全技术，以此构筑数据安全风险管理技术支撑体系，促进数字政府数据安全开放、安全共享、安全运营。在政府数据使用、运营、维护的过程中，不仅要建立风险预警化解机制，而且要形成风险监控和管理制度，利用数据安全防范技术建立各地区、各层级、各部门可共享的数据安全防范数据库和数据安全防范技术清单。在数据采集和收集、整理和处理、发现和获取、储存和开放、利用和运营、维护和修补等环节出现安全漏洞时，可快速利用应对数据安全漏洞技术，并利用智能分析技术、信息采集和整合技术等新一代信息技术，识别数据库中存在的数据管理漏洞、数据管理薄弱点，并形成预警，以此监测、反馈、应对、防范相关数据

风险。

第二，建立数据质量保障体系，为数字政府数据供给提供有力支撑。首先，加强对数字政府基层数据采集人员的教育、培训力度，提高其对采集对象的认知能力、理解能力，与此同时，加大数据采集方面的宣传力度，提高公众和用户对采集对象、采集数据的认知和理解。其次，持续关注和整体跟踪数据的采集、处理、整合、共享、交换、运营全过程，并制定实施完备的政策和制度，保障政府数据采集、处理、整合、共享、交换、运营过程顺利进行[13]。再次，建立数据采集主体与采集对象定期双向互联模式，这对于提升数据中高质量、高需求的优质数据集比例具有重要作用，不仅有利于提升数据的采集效率，而且有利于提升数据的处理、整合、共享、交换、运营效率。最后，强化数据治理保障体系建设，通过建立数据质量高低筛选机制，定时剔除重复、无效数据集，定期清理碎片化、低容量的低质数据集，实时动态更新、引入大容量数据集，从而为数字政府数据供给提供有力支撑。

（四）完善数字政府建设相关法律法规和管理制度，提升数字政府服务能力

第一，提升信息安全保护技术水平。首先，在数字政府大数据平台中，注重网络访问、保密和使用技术水平的提升。如提升大数据平台账户注册、账户密保、账户验证、账户安全等技术水平，具体包含秘钥、验证码、保护等级、指纹识别、人脸识别等方面的技术。其次，为大数据平台接口提供详细的操作指南和具体的使用说明，从而降低接口难度，提高接口响应的精确度，减少操作失误几率，有效防止国家信息系统遭受破坏和国家信息泄露。再次，加强与高校、科研院所、企业等技术支持单位的合作，共同推进数据特征值提取、数据防泄漏以及数据加密等技术的研究，攻克数据风险管控关键核心技术难关，构筑数据开放技术防范体系，提高政府应对信息系统遭受破坏和国家信息泄露的技术支撑能力。最后，推广数据脱敏、数据沙箱等数据安全技术的应用，形成统一的数据标准，提升数据安全与个人信息保护技术水平。

第二，加强信息安全保护法制建设。一方面，加快出台与数字政府建设相关的法规和政策。尽可能出台、制定、实施与数字政府建设同步的地方性法规、地方政府规章或规范性文件，对数字政府的数据采集、整合、处理、整合、共享、交换、运营的方式、范围、标准、安全、保障等方面作出要求和规定，有效防止公众隐私泄露、信息窃取、用户攻击、数据盗用等现象发生。另一方面，可依托现有互联网行业自律组织，推动各利益相关方共同制定个人信息收集使用行为准则，对平台等信息收集者进行安全评估检测和认证，确定数据和信息公开与非公开边界的划分标准，确定政府数据开放、使用的等级，使之符合平台协议合规性。

第三，提高信息安全保护监督能力。首先，建立数字政府大数据监管体系，形成数据追溯、标识、监测、反馈、修正机制，减少不符合法律法规和政策规定的数据获取和交易行为，尽可能避免信息数据的泄露。其次，建立大数据使用行为规范协议。一旦出现不符合法律法规和政策规定的数据交易或交换行为，就应对大数据运营商、管理者予以必要的惩处。再次，联合公检法、社会公众、社会媒体等众多力量，组成第三方监督机构，打造协同监督机制，并对大数据平台展开定期与不定期检查，组织第三方评估机构开展风险评估。最后，建立政府公共数据安全预警机制，实时监控敏感数据可能泄露等异常情况，确保国家信息系统和国家信息数据安全有序运转。

（五）优化数字政府生态环境，提升数字政府建设主体素养

第一，重塑数字政府建设理念，实现从效率改善到价值创造。科学的数字政府建设理念是优化数字政府建设生态环境、提升数字政府建设主体素养的基本前提。优化数字政府建设生态环境、提升数字政府建设主体素养的目的，就是要提高政府数字化水平、加快数字政府政务服务效率，从而推动高质量发展，为构建新发展格局和开启全面建设社会主义现代化国家新征程提供助力。为达此目的，一方面，要坚持提升数字政府建设能力的理念，把提升数字政府建设能力摆在更加突出的位置，实现更大规模的数字政府价值创造。

另一方面，要以需求和问题为导向。坚持以公众和用户数据信息需求和重大社会问题为导向，加快数字政府资源配置整合优化，加强数字政府人才教育培养，加快数据安全人才队伍建设，提高数字政府建设主体的安全素养，培养全体公民的数据权利意识，实现更高水平的数字政府价值创造。

第二，健全数字政府建设的创新生态体系。优化数字政府建设生态环境，需要政府部门、企业、科研单位和人员、投资机构等主体共同参与，健全数字政府建设的创新生态体系。

首先，营造创新生态氛围，通过树立创新生态理念、完善科技金融模式、推进知识产权管理、拓展创新生态空间、构建“双创”体系、整合“双创”资源，形成更高服务水平、更高决策水平、更高创新水平的创新治理生态。

其次，充分发挥新一代信息通信技术的管理赋能作用。新一代信息通信技术驱动着创新生态管理模式从粗放式管理迈向精细化、智慧化管理[14]。

最后，积极激发创新人员的积极性。不仅要将基础研究理论成果、实践成果、应用成果、转化成果纳入科研人员绩效、职称、岗位考核体系，提高科研人员收入水平；而且要改革创新科研单位的人才评价体系，努力破除人才评价体系中的各种不良倾向，提高基础研究科研工作者尤其是青年科研工作者的积极性。

参考文献：

[1]李军鹏.面向基本现代化的数字政府建设方略[J].改革,2020(12):16-27.

[2]戚学祥.区块链技术在政府数据治理中的应用:优势、挑战与对策[J].北京理工大学学报(社会科学版),2018(5):105-111.

[3]王谦,曾瑞雪.社会技术系统框架下“数字政府”风险分析及治理[J].西南民族大学学报(人文社科版),2020(5):226-233.

[4]沈费伟,诸靖文.数据赋能:数字政府治理的运作机理与创新路径[J].政治学研究,2021(1):104-115.

[5]张丽,陈宇.基于公共价值的数字政府绩效评估:理论综述与概念框架[J].电子政务,2021(7):57-71.

[6]杨雪冬.地方数字政府建设的成绩与问题[N].环球时报,2021-05-14(015).

[7]清华大学数据治理研究中心.2020 年数字政府发展指数报告[EB/OL].(2020-11-06)[2021-09-15].http://ex.cssn.cn/zzx/zzxzt_zzx/126991/bg/202011/t20201106_5212396.shtml.

[8]盛朝迅.新发展格局下推动产业链供应链安全稳定发展的思路与策略[J].改革,2021(2):1-13.

[9]赵娟,孟天广.数字政府的纵向治理逻辑:分层体系与协同治理[J].学海,2021(2):90-99.

[10]张成福,谢侃侃.数字化时代的政府转型与数字政府[J].行政论坛,2020(6):34-41.

[11]王孟嘉.数字政府建设的价值、困境与出路[J].改革,2021(4):136-145.

[12]黄未,陈加友.创新行政管理和服务方式推进数字政府建设[J].贵州社会科学,2019(11):16-19.

[13]陈玲,段尧清,王冰清.数字政府建设和政府开放数据的耦合协调性分析[J].情报科学,2020(1):162-168.

[14]魏江,赵雨菡.数字创新生态系统的治理机制[J].科学学研究,2021(6):965-969.