人工智能背景下政府数据安全治理的现实困境与应对策略研究

彭海艳 何振[1]

【摘 要】：政府数据安全是事关国家安全和经济发展的重大问题，随着人工智能的迅速发展，运用人工智能加强政府数据安全治理是当前备受学术界关注的一项重要课题，有利于落实国家总体安全观、保障政府数据安全、推动政府治理创新以及促进国家安全体系现代化建设。人工智能作为一项引领未来的战略技术，在给政府数据安全治理带来新机遇的同时，也给政府数据安全保障、数据安全风险防范、个人隐私数据防护等方面提出新挑战。现阶段，人工智能背景下的政府数据安全治理面临权责关系不明、标准规范缺位、安全审查不当、智能监控不足、技术应用不力等方面的现实困境。为了解决这些困境，须重点从深化数据安全顶层设计、共筑数据安全标准规范、完善数据管理保障机制、搭建数据综合治理平台、强化核心技术自主创新等方面进行治理。

【关键词】：人工智能 数据安全 数据风险防控 政府治理 安全治理 综合治理平台

【中图分类号】：N031**【文献标识码】**：A**【文章编号】**：1000-8691（2022）03-0029-09

数据是数字经济时代的基础性战略资源，是中国经济转型和社会发展的新引擎。运用数据进行政府治理已经成为社会共识，有利于提升政府决策质量、促进政府职能转变、优化行政流程以及改善政府绩效等。随着人工智能技术的蓬勃发展和在政府领域应用的不断深入，政府数据安全问题日益凸显，譬如隐私数据泄露、数据过度采集、数据非法使用等，给人民的生命财产安全和经济社会的快速发展带来不利影响。近年来，党和政府对数据安全问题高度重视。2016 年，国家“十三五”规划明确提出：“要强化信息安全保障，加快数据资源安全保护布局。”2017 年，习近平总书记在中共中央政治局第二次集体学习时指出：“要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”[1]2018 年，习近平总书记在中共中央政治局第九次集体学习时强调：“要加强人工智能发展的潜在风险研判和防范，维护人民利益和国家安全，确保人工智能安全、可靠、可控。”[2]2020 年，党的十九届五中全会明确提出：“保障国家数据安全，加强个人信息保护。”[3]可见，政府数据安全问题已然成为事关国家安全和经济发展的重大问题，加强政府数据安全治理是当前各级党政机关和政府职能部门必须面对的一个时代课题。

一、人工智能发展给政府数据安全治理带来的冲击

（一）人工智能发展对政府数据安全治理带来的机遇

人工智能技术的更新迭代为人工智能赋能政府数据安全治理提供了可能，其智能决策、精准感知、数据挖掘功能给政府数据安全策略制定、数据安全风险监测、数据安全隐患防范等方面提供新的机遇。

[1]**作者简介**：彭海艳，女，湘潭大学公共管理学院讲师，主要从事数据治理研究。何振，男，湘潭大学公共管理学院二级教授，博士生导师，主要从事数据治理研究。

基金项目：国家社会科学基金项目“改革开放以来湘江流域灾害档案文献整理与研究”（项目号：20BTQ098）、国家社会科学基金青年项目“污染源视角下流域生态环境协同治理及责任追究机制研究”（项目号：17CZZ022）;湖南省社会科学基金重大智库项目“加强应急体系、应急预案、应急力量、应急指挥建设，提升应急能力研究”（项目号：20ZWA14）的阶段性成果

一是智能决策为政府数据安全策略制定提供有力支持。制定数据安全策略（包括数据流转管控策略、数据分级分类策略、数据安全稽查策略等）是开展数据安全治理的重要基础工作，也是保障数据安全的指导方针，可有效维护政府数据的完整性、保密性和可用性。随着人工智能技术的快速发展，智能决策能力也随之提升，机器可基于高度数据集成，自动化编排方案并进行比选，从而辅助决策者选出最优策略。因此，政府可依托智能决策，运用深度学习等相关数据分析技术，帮助掌握数据全生命周期各个环节中的数据加密状态、数据脱敏状态、应用通道、数据使用行为等更多细节信息，尽可能排除相关因素的干扰，并根据不同的决策环境进行模拟计算，帮助解决决策复杂性，制定和寻找最优数据安全策略，持续优化，确保它们安全可用，从而减少重大决策失误。[4]

二是精准感知为全面监控政府数据风险提供条件。当前的政府数据安全风险监测存在着效率低、风险识别周期长、风险防控滞后性强等不足。据 IBM 发布的《2020 年数据泄露成本报告》数据显示，识别数据风险需要一定时间，如金融行业识别风险所需时间为 177 天，医疗保健行业识别风险所需时间为 236 天。[5]而时间越长，数据风险所造成的危害就越大。人工智能技术的超强计算和智能感知可实现对数据的全域精准感知、对异常数据智能识别与智能警报，打造动态监测、精准防控、提前预警的智慧监控模式。在该模式下，可帮助政府有效计量、监测和控制各类风险，实时识别、标记并上报政府数据异常行为，大大缩减风险识别的时间成本，大幅提升数据安全风险感知的真实度、精确度、全面度与及时度。

三是数据挖掘为消除政府数据安全隐患提供可能。随着人工智能技术的发展，数据挖掘能力得到显著提升。数据挖掘具备基于大量数据、隐含性、价值性等多重特性，可对庞大的、不完整的、有干扰的数据集开展智能分析，通过关联分析、分类、聚类或偏差检测等方法，自动搜索隐藏于其中有着特殊关系性的数据和信息，快速、准确地检测异常数据、预测安全风险，进而帮助应体快速采取应对措施。基于此，将智能挖掘技术应用于政府数据安全治理领域，可建立起具备快速运算能力、精准风险识别的数据安全预测模型，通过对海量数据进行多维度、长周期的深度挖掘分析和计算，精准考察政府数据利用行为是否合理、数据是否真实可信、是否存在隐私数据滥用行为等，快速识别并提前预警政府数据安全治理中的漏洞和不足，为政府工作人员提供重点监管方向，推动政府数据安全风险“主动防御”，为消除政府数据安全隐患提供可能。

（二）人工智能发展对政府数据安全治理提出的挑战

技术是一把双刃剑。人工智能在政府数据安全治理领域，同样存在着“安全赋能”和“安全伴生”效应[6]，既加剧了传统的数据安全风险，如数据过度采集、数据窃取；也催生出新的数据安全问题，如数据投毒、样本偏差问题，给政府数据安全保障、数据安全风险防范、个人隐私数据防护等方面提出新的挑战。

一是技术自身发展给政府数据安全保障提出更高要求。首先，要求完善数据安全标准体系。人工智能技术自身面临的数据安全、算法安全、隐私泄露风险，极易引发政府数据安全问题，亟待加强人工智能数据安全标准建设，保障人工智能背景下的数据安全与开发利用。其次，要求加强数据安全风险监控。人工智能背景下政府数据安全风险更加多发频发、更加隐蔽，传统的数据安全风险监控技术已经难以满足政府数据安全治理的需要。因此，有必要对政府数据安全风险进行全方位的监控。再次，要求构建多元化的数据安全治理人才队伍。从安全产品的简单堆砌到数据安全的全流程治理，从提供产品到提供服务，不仅需要技术手段创新，更离不开专业化技术人才队伍。因此，构建多元化的政府数据安全治理人才队伍势在必行。

二是技术恶意或不当应用导致政府数据安全风险增多。人工智能的滥用或不当应用，加剧了个人隐私数据泄露、数据投毒、逆向攻击、模型窃取等风险，严重者可导致政府数据分级分类、数据安全决策发生错误。2018 年，世界上最大的国营生物识别数据库 Aadhaar 数据泄露，根据印度《论坛报》(Tribune)的调查显示，超过 10 亿印度公民的个人资料（包括用户的姓名、家庭住址、Aadhaar 号码、指纹和虹膜等生物识别信息）被在线出售。此外，人工智能可增强数据挖掘能力、快速发现系统漏洞，当其被不法分子恶意应用时，可以让行动者执行原本不可行的攻击，如深度造假、破解验证码、蜂拥式攻击等，进而窃取机密数据，造成政府数据泄露。

三是技术偏见或算法黑箱导致个人隐私数据泄露严重。政府掌握大量隐私数据，这些数据在存储、复制、传播的过程中，容易产生隐私泄露等伦理风险，尤其是人工智能存在的技术偏见和算法黑箱更容易导致个人隐私数据泄露严重。当前，私人技术公司因负责算法设计与运行而掌控算法，政府公共部门仅仅明确算法输出端的信息即算法目标或算法结果，而社会公众则几乎完全被排除在算法“黑箱”之外[7]。这意味着，在数据产业链中的安全能力薄弱主体可能会使整个数据链面临风险，产生数据泄露或数据盗取的危害。2015 年，重庆、上海、山西、沈阳、贵州、河南等超过 30 个省市卫生和社保系统出现大量高危漏洞，数千万用户的社保信息可能因此被泄露，其中包括社保参保信息、财务、薪酬、房屋等敏感信息。[8]同时，“算法黑箱”或算法不透明性可能成为“隐形”恶意武器，操控决策致使算法权力诱导个人行为，窃取或贩卖隐私数据。

二、人工智能背景下政府数据安全治理面临的现实困境

当前，中国政府数据安全治理尚处于初步探索阶段，人工智能背景下的政府数据安全治理在权责关系、法律法规、安全审查、智能监控、技术应用等方面还存在一些亟待解决的问题，政府数据安全治理任重道远。

（一）权责关系不明、主体协同不畅

加强组织制度建设，是政府数据安全治理的根本保障。但是，当前中国政府数据安全治理在组织建设方面仍面临一些困境。主要表现在：

一是责任边界模糊。省级行政单位设有大数据管理机构承担数据安全治理责任，但市、县政府却无此类机构衔接，数据安全责任散落于网信、通信管理等部门，导致数据安全治理责任边界模糊。一旦发生政府数据安全事件，则难以溯源，各级政府、部门之间容易出现互相扯皮、推诿的现象。尤其是在人工智能场域中，人与机器的界限越来越不明显，与技术本身相关各方的行为失当、责任界定不清[9]等问题，使得政府数据安全责任更难认定、责任边界更加模糊。

二是权力归属不明晰。受传统科层制和“权力本位”观念影响，中国治理相关权力在多层级政府体系中呈现出层层上收的特点。[10]上级政府对下级政府没有进行明确的授权，或虽进行明确授权却又掌握着任意干预权，这就使得下级政府的治理权变得非制度化、残缺或薄弱[11]，这种不明确、有“卸责”意味的数据安全治理权力配置使得层级政府间的数据安全治理难以协同，降低了数据安全治理效能。此外，中国行政体系中的条块分割，也容易导致同级政府部门间数据安全治理权力归属的混乱，例如，数据安全监管政出多门，既有数据管理部门也有网信部门行使监管权力，在信息不对称的情况下，容易形成数据安全监管真空，难以全面防护政府数据安全风险。

三是职能划分不合理。当前，中国尚未构建全国统一的政府数据安全治理行政机构，各级政府内部也没有设立专门的政府数据安全管理部门，虽然部分地区设置了数据管理机构，但其对数据安全方面的职能要求尚不完善[12]，数据安全治理的决策、组织、协调、控制、监督等职能缺乏有效的顶层设计和统筹规划，对网信、公安、数据管理部门等安全责任主体的职能划分不太合理。对于数据安全治理由谁来牵头、谁来负责、谁来落实、谁来监督以及谁来考核等问题均缺乏详细的规定。

（二）法律法规滞后、标准规范缺位

政府数据安全治理需要法律法规和标准规范的指导与约束，这是政府数据安全治理有效实施的前提和基础。但是，当前中国政府数据安全治理在法治建设方面相对滞后，已经不能满足人工智能发展的需求。

一是有关法律法规的系统性有所欠缺。目前，现有的数据安全治理法律法规仍未形成完整的体系，首先，数据安全治理相关法律法规之间缺乏衔接性与一致性。譬如，《个人信息保护法》规定了个人信息收集使用的“明确同意”规则；《民法总则》则对其采取更为宽松的立法理念，收集、转让或者使用个人信息，既可以通过书面等其他明示形式做出，也可以以默示的方式做出[13]；

《民法典》对隐私权和个人信息处理进行了界定，承认隐私权是一种人格权，但没有规定自然人对个人信息享有人格权，仅规定自然人的个人信息受法律保护。此外，《民法典》所定义的隐私和个人信息的范围存在重叠[14]，相关法律条文仍不够细化，可操作性和可执行性略显不足。如有关数产权的规定目前仍为原则性规定，数据产权规则不清晰，可能会导致多方数据主体之间的利益冲突。[15]

二是配套政策缺乏系统性。虽然中国人工智能和数据治理政策体系已初见雏形，但是专门针对人工智能背景下的政府数据安全治理的规定非常少见，散见于人工智能和数据治理的顶层设计和战略规划等相关文件中，缺乏统一和协调。另外，虽然现有数据安全顶层设计和宏观政策比较多，但是其颗粒度大，针对性和系统性不强，实施效果大打折扣。以地方政府为例，当前地方政府数据安全政策文件内容主要集中于安全体系、安全技术、安全审查机制、安全监测等方面的宏观论述，有的政策文件论述过于精简，有关数据安全内容甚至不足 100 字符。[16]

三是标准规范仍需完善。人工智能数据安全通用标准缺乏，术语定义、参考架构、分级分类等基础类指标不太明确，导致不同组织制定出来的数据标准各不相同，难成体系；人工智能数据安全采集、流通、使用和共享等关键技术标准还未建立，覆盖政府数据全生命周期安全的技术标准亟待制定，包括分类分级、去标识化、数据跨境、风险评估等内容；人工智能数据安全的部分重点领域相关标准仍存在空白，政府数据安全评估、重要数据保护以及人工智能背景下的跨境数据流动、政府数据合规使用等相关的标准规范尚需建立。

（三）安全审查乏力、数据风险频发

从当前的情况来看，中国政府数据安全审查乏力的情况时常发生，数据安全风险仍然频发。其主要表现在：

一是数据安全审查不规范。根据已有的法规政策文本，虽然明确要求建立数据安全审查制度，但相关内容尚不具体、未细化。例如，对数据安全审查制度的实施主体、实施机制、审查内容和覆盖范围等方面还不明确，可执行性不强，易导致政府具体实践中的无所适从。此外，绝大多数政府数据安全审查集中在数据开放阶段，以保密审查、脱敏审查为主，而随着人工智能技术在政府领域的嵌入，数据采集、数据流转、数据销毁等阶段都有可能存在着数据泄露、隐私侵权等安全风险，政府应当对数据全生命周期开展安全审查。

二是数据安全审查方式较陈旧。现阶段，政府数据安全审查以传统的方式为主，而传统的数据安全审查方式，对工作人员的专业知识和经验具有很强的依赖性，且在非自动化审查和大量人工干预下，审查周期长、成本高。网络安全审查通常在 45 个工作日内完成，情况复杂的会延长 15 个工作日；对于进入特别程序的审查，审查周期为 90 个工作日或者更长。此外，传统的数据安全审查方式容易受主观因素的影响从而忽略某些审查内容，导致一些数据安全问题产生。比如，2015 年，由于政府数据开放安全审查不到位，北方某省一住房和城乡建设局在公示人员名单时，公布了公民完整的身份证号码等个人信息，侵犯了公民个人隐私。

三是数据安全审查非常态化。中国数据安全审查一般在开展数据活动（如数据共享、数据开放）前进行，暂未形成常态化、规律性的制度化工作。但在日常工作中，也需要定期开展数据安全审查。这是因为，在人工智能背景之下，数据安全风险变得更为隐蔽，政府数据采集环节中可能存在隐私侵犯问题、数据质量问题，在数据存储、使用等阶段都有可能存在数据泄露、数据遭篡改等安全问题。例如，2018 年某公务员利用职务之便非法获取出售、提供 82 万条包含居民身份证号码、手机号码、固定电话等在内的个人信息。

（四）平台兼容性差、智能监控不足

当前，围绕数据安全治理平台建设的议题，政府面向市场上多家企业寻求解决思路，并取得一定进展。然而，在人工智能背

景下，政府数据安全治理平台支撑体系仍未建立，尚存在着平台兼容性差、风险智能监控不足的问题。具体而言：

一是人工智能系统平台兼容性差。将人工智能系统嵌入数据安全治理平台可以大大提升政府数据安全风险监控的自动化与智能水平。但从实践情况来看，由于系统设备智能化的关键处理器和操作系统绝大部分并非由中国研发与生产，这就意味着人工智能从算法到芯片、从软件到硬件都有可能存在差异和信息安全风险。

二是数据安全治理平台兼容性差。政府数据安全风险监控需要基于数据全生命周期构建一条完整坚实的数据安全监控链。然而，现阶段政府数据安全平台体系大多缺乏自上而下的顶层规划，数据接口标准、技术标准等缺乏统一规范，致使各平台多为封闭生态，平台与平台之间兼容性差，智能水平也各不相同。在此情况下，“各自为战”的数据安全平台容易阻滞风险分析数据的汇集，导致全域风险分析和研判难以开展，数据安全风险难以溯源。厦门市建立的大数据安全开放平台，通过采用“数据安全屋”技术开展政务大数据安全开放，重点监控政务数据开放共享中的数据安全风险，难以形成覆盖全流程的数据安全智能监控平台体系。

三是跨部门政务数据平台兼容性差。当前政府各部门之间的政务平台兼容性差，数据壁垒问题突出。江苏无锡市公共数据中的人口数据、历年排污企业目录、排污量等数据分别保存在无锡统计官方网站、无锡市生态管理局官网中，政府各部门数据平台间数据流通不畅、整合困难[17]。然而，实现政府数据安全风险智能监控离不开数据支持，政府部门数据垄断问题阻滞了政府全量数据资产的数据状况梳理、敏感数据流转路径和动态流向感知，无法实现对政府数据安全风险发展与变化情况全程监督，以及多维度、全方位智能风险核验、实时预警与拦截操作，智能监控稍显不足。

（五）技术应用不力、安全漏洞凸显

近年来，中国在人工智能数据安全技术攻坚方面虽然取得了一些成绩，清华大学创业公司的瑞莱智慧团队开发了“珠算”概率编程库，对数据标准和数据模型安全提供了可靠技术。但是，从总体上看，仍存在一些亟待解决的问题。主要体现在：

一是智能技术应用保守、网络攻击防范不力。部分政府部门在应用智能技术时仍然比较保守，“不想用”“不敢用”“不会用”等现象普遍存在。与此同时，网络攻击防范也不力，当人工智能技术被不法分子利用时，其超强算力与自适应能力，也能够帮助网络黑客实现政府平台自动化漏洞检测与攻击。根据英国网络安全公司 Darktrace 分析显示，集成人工智能技术的勒索软件可自动瞄准更具吸引力的目标，如政府数据库文件等。

二是智能技术过度应用、隐私泄露风险加剧。人工智能技术在大幅度提升数据安全管理效率的同时，也让人产生了对技术的依赖，从而容易引发技术过度应用问题（过度采集、过度挖掘、过度利用等）。随着各类智能设备和智能系统的应用普及，公民活动的任何痕迹以及人脸、指纹等具有强个人属性的生物特征信息都可能会被智能终端自动采集，一旦这些数据被泄露或者滥用，将会对公民权益造成严重危害。在数据采集中，2019 年中国人民大学 WAMDM 实验室发布的《中国隐私风险指数分析报告》显示，约 10%的数据收集者获取了 99%的权限数据，公民个人隐私信息被严重侵犯。

三是智能技术缺乏监管、数据安全存在不可控。2021 年 4 月，欧盟委员会提出了一项旨在加强人工智能（AI）技术监管的法规草案，该法案致力于解决人工智能技术在实际应用中给人类及社会发展带来的风险。相比之下，中国人工智能技术缺乏有效监管，安全漏洞日益凸显。360、腾讯等企业安全团队就曾多次发现 Tensor Flow、Caffe、Torch 等深度学习框架及其依赖库的安全漏洞，攻击者可利用相关漏洞篡改或窃取人工智能系统数据[18]，如果将未经监管的人工智能技术应用于数据安全治理，很大程度会导致数据安全不可控。

三、人工智能背景下政府数据安全治理的应对策略

当前，为了应对人工智能发展给政府数据安全治理带来的冲击以及解决人工智能背景下政府数据安全治理面临的一些困境，须重点从深化数据安全顶层设计、共筑数据安全标准规范、完善数据管理保障机制、搭建数据综合治理平台、强化核心技术自主创新等方面进行。

（一）深化数据安全顶层设计、建立权责明晰的多元共治组织结构

人工智能背景下的政府数据安全治理是一个系统工程，为此，应重点加强顶层设计、完善政府数据安全组织建设，形成权责明晰的组织结构。

一是加强政府数据安全顶层设计。政府数据安全治理离不开国家战略规划的指引，如英国发布的《数据安全战略》中提供了国家层面的数据安全治理方案。中国应根据人工智能数据安全特点、业务模式、组织架构等因素进行战略规划，力争将其上升为国家战略，以实现国家层面的统筹协调。明确人工智能背景下的政府数据安全治理目标，旨在降低数据安全风险、保障数据合法合规，从而使数据使用更加安全；确定政府数据安全治理的重点领域，主要包括数据分级分类管理、数据安全风险防范与监测预警、数据安全事件应急处置与动态跟踪等；制定政府数据安全治理总体策略和行动纲领，明确政府数据安全治理的主体、内容、工具、方式、方法、流程等，为政府数据安全治理提供实践指南。

二是建立政府数据安全治理机构。建议由中共中央网络安全和信息化委员会办公室和国家互联网信息办公室牵头，联合各级政府部门的大数据管理机构和数据治理机构共同组建统一的政府数据安全行政管理机构。各级政府部门设立相应的数据安全保护部门，专门负责政府数据安全治理工作。此外，成立由各级党委、政府主要领导牵头的数据安全治理工作领导小组，加强集中统一领导。设立政府数据安全治理委员会、政府首席数据保护官、数据安全管理专员等，负责相关政府数据安全保护措施的监督和落实。

三是明确政府数据安全治理相关方的权责关系。一方面，政府部门应基于人工智能背景制定权力清单。从宏观上对各级政府数据治理机构所拥有的权力边界和活动范围进行统一规定，明确各级政府数据安全治理机构的职责权限，从而防止各级政府数据安全治理机构“权责交叉”“多头执法”“相互推诿”等问题出现。另一方面，划定责任界限。按照“谁生产、谁拥有、谁负责”和“权责统一”的原则，明确责任主体，划清每个部门的职责边界，要明确相关方的法律责任，也要规定相关方人员的伦理责任。

四是构建政府数据安全多元协同治理机制。人工智能时代的政府数据安全问题日益突出，构建以政府为主导多元主体共同参与的协同治理机制，是人工智能背景下政府数据安全治理的内在需求。政府部门要加强“纵向大联动，横向大合作”工作，吸纳企业、行业组织以及社会公众等不同主体广泛参与到政府数据安全治理工作中来，发挥不同主体在政府数据安全治理中的作用，为人工智能背景下的政府数据安全治理营造良好的生态环境。

（二）共筑数据安全标准规范、形成结构完整的数据安全法治体系

加强政府数据安全治理，提升数据安全防护水平，推进国家治理体系和治理能力现代化，必须加强法治建设。

一是完善政府数据安全法律法规。一方面，继续推动数据安全治理法律法规体系建设，加强政府数据安全治理和人工智能领域的立法，明确政府数据安全治理不同参与主体所享有的数据权利与承担的安全责任，并对人工智能技术监管以及数据过度采集、偏见歧视、资源滥用、深度伪造等突出问题进行规制。另一方面，基于数据生命周期管理理论，围绕政府数据采集、存储、传输、开放、共享、交易、使用等方面，建立政府数据全生命周期安全管理专项法规，增强数据安全法律条文的可操作性以及数据安全重点领域的约束规范。

二是制定政府数据安全标准。2020 年的“人工智能与数据安全”分论坛已提出“人工智能和数据安全的治理需要世界各国和组织联合起来，构建统一的人工智能模型与系统的安全评估准则和标准。”因此，中国可通过与 IEEE、ISO/IEC/ITU 等国际化标准组织联合发声等方式，实质性参与人工智能数据安全相关国际标准制定工作，提出更多的人工智能政府数据安全相关提案，以开放协同的方式进行科学研究和技术交流，推动人工智能数据安全标准快速落地。同时，以中国人工智能安全标准框架为指引，重点加强对人工智能政府数据安全技术标准、安全管理标准、运行平台标准、安全评估标准、数据质量标准等方面的制定，完善中国人工智能背景下的政府数据安全标准体系。

三是推进政府数据安全执法。执法部门应严格按照人工智能政府数据安全相关法律法规的规定，依法开展政府数据安全治理工作，特别是要加强对政府数据收集、使用、共享等高风险环节的安全执法，加大对政府数据过度采集、数据滥用与违规使用、个人隐私侵犯、数据泄露等行为的处罚力度，创新和规范人工智能政府数据安全事件处置程序和方法，促进人工智能政府数据安全法律法规的有效实施。同时，还要进一步优化人工智能背景下政府数据安全执法体制，提升执法能力，规范执法行为，敢于追究违法行为，并能有针对性地提出整改建议，以提高人工智能背景下政府数据安全执法实效。

（三）完善数据管理保障机制、加强数据安全审查和分级分类管理

良好的安全制度是政府数据安全治理的前提和基础，人工智能背景下政府数据安全治理应建立专门针对人工智能发展需要的政府数据安全综合管理制度，从制度层面保障政府数据安全。

一是健全政府数据安全审查制度。现阶段，中国《数据安全法》明确规定要建立数据安全审查制度，《网络安全审查办法（修订草案征求意见稿）》将“数据安全”纳入审查范围。鉴于此，应进一步完善政府数据安全审查制度，明确数据安全审查主体，规范审查内容。建议由网络安全审查办公室统一负责数据安全审查工作，审查内容应当围绕政府数据采集、存储、加工、使用、交易、开放、共享等活动进行操作稽核、合规性检查、日志审计、例行安全检查以及风险评估等。此外，针对审查所发现的安全问题，网络安全审查办公室应当牵头协调各部门提出改进方案，要求相关部门落实解决且对其持续跟踪检查，防范化解重大政府数据安全风险。

二是实施政府数据分级分类制度。政府数据分类分级是政府数据安全治理的前提，如美国颁布的《国家安全信息分类》《受控未分类信息》等就对联邦数据分级分类进行了统一规范。为此，中国应依据数据的来源、内容和用途对数据进行分类，根据政府数据的价值、敏感程度和影响程度等进行数据分级，并出台相应的政策文件对政府数据的分类、标记、评估、保护等诸多方面进行规制。同时，在数据分级分类过程中，针对海量的政府数据，可运用机器学习、模式聚类等技术，打造数据分级分类引擎，实现对数据进行基于内容的实时、自动、精准分类分级。

三是完善政府数据安全管理保障机制。主要指健全政府数据安全保密制度。在数据安全审查过程中，相关部门要严格承担保密责任，尤其是做好重要数据和重要储存介质的安全保密工作，未经批准和授权，任何人不得随意使用数据和泄露数据；推进政府数据容灾备份管理制度。政府部门应利用人工智能等新兴技术构建政府数据容灾系统，坚持数据级备份与应用级备份相结合，通过异地备灾、实时备份和在线备份等多种途径，防范各类政府数据安全风险；建立政府数据安全应急处置机制。在数据分级分类管理和安全审查过程中，应按照“谁主管谁负责、谁运行谁负责”的原则落实应急处置责任，及时做好数据安全应急处置工作。

（四）搭建数据综合治理平台、筑牢多元立体的数据安全防护网络

人工智能背景下，搭建运行有效的政府数据综合治理平台，实现数据安全监管、数据安全加固、数据安全应急，是确保政府数据保密性、完整性、可用性的重要保障。

一是组建围绕业务流程的数据安全监管平台。政府数据安全是一个动态变化的过程，政府部门需要关注数据的流动性特征，组建围绕业务流程的数据安全监管平台。利用物联网、人工智能、云计算等技术，针对各类设施设备、数据资产以及资源（如空间、带宽、端口、容量、IP 等），进行浸入式、全景式的数据资产、数据流动等自动化、可视化跟踪管理。并通过顶层设计与数据加密、数据授权、数据脱敏、安全审计等产品进行深度联动，突破传统的单点防护方案，实现政府业务平台数据在存储、使用、传输、共享等流转环节中的数据安全风险联防联控、实时动态监测、智能分析、态势评估和快速响应。

二是完善面向数据开放的数据安全加固平台。根据《2020 年中国互联网网络安全报告》的统计数据，中国境内被篡改的政府网站有 494 个；被植入后门的政府网站有 256 个。政务网站被“黑客”植入暗链或黑页等诸如此类的问题，很容易造成隐私数据泄露。为此，政府部门应着重面向数据开放开展数据安全加固，针对数据存储、数据流通、数据访问等环节中的敏感数据泄露、接口设计风险、数据流动风险等，利用数据识别算法、敏感接口识别策略以及智能识别引擎，对数据开放共享进行风险智能识别，并同时出具实时数据安全加固方案，对诸如账号安全、敏感信息、网络架构、安全产品配置以及安全漏洞方面进行针对性的加固，从而打造政府部门安全用数开放平台。

三是构建针对数据安全突发事件的应急平台。一方面可依托具备智能感知的风险监管平台和数据安全智能监测系统对政府数据采集风险、数据组织存储风险、数据流动传输风险、数据开发利用风险等进行精准识别，为精准防范数据风险提供基础。另一方面，应积极打造数据安全应急预案库、数据安全智能应急决策引擎，针对汇聚的数据安全风险数据开展高效研判，并及时对政府数据安全风险进行快速预警。与此同时，应急平台应依据预警信息分级响应，实时启动应急预案，协调政府各部门采取不同的处置措施，以最短时间，快速从事件中恢复、使影响降至最低，并避免再次发生。

（五）强化核心技术自主创新、推进数据安全技术研发和有效应用

人工智能背景下的政府数据安全治理需要严密有效的技术予以保障。因此，应着力研发人工智能和政府数据安全相关技术，为实现人工智能背景下的数据安全治理提供支撑。

一是完善政府数据安全技术。政府可联合社会组织和企业，通过成立联合实验室、共同投资等方式，开展人工智能背景下政府数据安全技术研究。首先，围绕政府数据全生命周期，加强对加密技术、入侵检测技术、访问控制技术、隐私保护技术、个人信息去标识、数据标签技术、数据交换技术、数据安全风险监测技术等相关政府数据安全技术研发。其次，加强对人工智能技术攻坚，增强对人工智能技术与物联网、区块链等其他信息技术融合研究，进一步解决人工智能技术的强数据依赖性、算法黑箱性等问题。

二是建立中国人工智能开源开放平台。目前，较为流行的开源框架仍然由国外公司或机构开发。为了从根本上解决过度依赖国外开源代码的问题，中国应在核心技术上实现自主可控，可依托新一代人工智能产业技术创新战略联盟，建立自有的人工智能开源开放平台。同时，通过中国市场优势，加快培育自有人工智能开源平台共享应用生态圈和产业链，为人工智能行业的发展提供新动力，为人工智能背景下的政府数据安全技术研发提供基础平台。

三是研发人工智能相关技术。利用国家资金和社会资源引导社会各界联合研发以政府数据保护为前提的人工智能技术，突破小样本学习、迁移学习、联邦学习、差分隐私等人工智能数据安全保护核心关键技术。通过研发基于隐私的机器学习技术如同态加密、安全多方计算、差分隐私等，可以有效保护用户的数据安全。通过研发减少数据需求的技术如迁移学习、数据增强技术等，可以从根本上解决人工智能对海量数据需求带来的数据安全问题。通过完善数据偏见监测技术、数据攻击防御技术、对抗样本监测技术等，可以有效防止政府数据被恶意破坏和篡改。

综上所述，人工智能背景下保障政府数据安全是当前的重要议题。中国政府数据安全治理困境主要体现在治理主体权责不明、法规标准滞后、安全审查乏力、平台兼容性差、技术应用不力五个方面，亟须从组织架构、法规标准、保障机制、治理平台、

技术手段多个维度采取措施解决问题，从而促进人工智能在数据安全领域中的高效赋能，力求实现人工智能与数据安全的良性互动发展。不过，本文提供的只是理论层面的观点，人工智能背景下政府数据安全治理本身是一个异常复杂的系统问题，不仅需要实践来验证和完善，还需要学术界更进一步的关注和探索。

注释：

1 中华人民共和国中央人民政府网:《习近平主持中共中央政治局第二次集体学习并讲话》,http://www.gov.cn/xinwen/2017-12/09/content_5245520.htm。

2(1)中华人民共和国中央人民政府:《习近平主持中共中央政治局第九次集体学习并讲话》, http://www.gov.cn/xinwen/2018-10/31/content_5336251.htm。

3(2)光明网:《发展数字经济的新航向》, https://theory.gmw.cn/2020-12/19/content_34477163.htm。

4(3)唐新华:《智能决策在国家治理现代化中的应用探析》,《当代世界》2020 年第 3 期。

5(4)IBM:《2020 年数据泄露成本报告》, https://www.ibm.com/downloads/cas/BK0BB0V1,2020 年 7 月 24 日。

6(5)参见方滨兴主编:《人工智能安全》, 北京：电子工业出版社, 2020 年。

7(1)谭九生、范晓韵:《算法“黑箱”的成因、风险及其治理》,《湖南科技大学学报（社会科学版）》2020 年第 6 期。

8(2)腾讯网:《数千万人社保信息或遭泄露》, https://tech.qq.com/a/20150422/002390.htm,2015 年 4 月 10 日。

9(3)全国信息安全标准化技术委员会:《网络安全标准实践指南——人工智能伦理安全风险防范指引》,https://www.tc260.org.cn/upload/2021-01-05/1609818449720076535.pdf。

10(4)田玉麒:《职责优化与组织调适:政府治理体系现代化的双重进路》,《社会科学战线》2020 年第 4 期。

11(1)向静林、艾云:《政府治理创新的层级差异及其组织根源——以互联网金融治理为例》,《学海》2021 年第 3 期。

12(2)孟庆国、林彤等:《中国地方政府大数据管理机构建设与演变——基于第八次机构改革的对比分析》,《电子政务》2020 年第 10 期。

13(3)杨蕾:《数据安全治理研究》, 北京：知识产权出版社, 2020 年。

14(4)中国法制出版社编:《中华人民共和国民法典：实用版》, 北京：中国法制出版社, 2020 年。

15(5)利刃出鞘:《〈数据安全法〉下中国数据保护路径解读》, https://www.pkulaw.com/lawfirmarticles/8d31eb44ffda0aeda1f c5702b38eaf3fbdfb.html,2021 年 8 月 3 日。

16(6)冉连、张曦:《地方政府数据开放全生命周期安全管理政策研究——基于全国 17 个省级政府的政策文本分析》,《情报杂志》2021 年第 8 期。

17(1)周林兴、崔云萍：《智慧城市视域下政府数据开放共享机制研究》，《现代情报》2021 年第 8 期。

18(1)魏薇、景慧昀、牛金行：《人工智能数据安全风险及治理》，《中国信息安全》2020 年第 3 期。