重庆大学学报(社会科学版) 2026年第32卷第2期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 32 No. 2 2026

Doi:10. 11835/j. issn. 1008-5831. zs. 2024. 01. 002

欢迎按以下格式引用:张楚凡,张佳琳. 数字政府建设与人工智能模型的互动研究——基于问题、法治与规制视角分析[J]. 重庆大学学报(社会科学版),2026(2):308-324. Doi:10. 11835/j. issn. 1008-5831. zs. 2024. 01. 002.

Citation Format:Zhang Chufan, Zhang Jialin. Interaction research between digital government construction and artificial intelligence models: An analysis based on the perspectives of issues, rule of law, and regulations[J]. Journal of Chongqing University (Social Science Edition),2026(2):308-324. Doi:10. 11835/j. issn. 1008-5831. zs. 2024. 01. 002.

数字政府建设与人工智能模型的互动研究
——基于问题、法治与规制视角分析

张楚凡[1],张佳琳[2]

(1. 武汉大学 法学院,湖北 武汉 430072;2. 辽宁大学 马克思主义学院,辽宁 沈阳 110036)

摘要:数字政府建设是数字中国战略的重要构成,人工智能模型的引入具有重大意义。从技术本身看,人工智能模型对数字政府建设具有层级性互动:结构层,人工智能模型延伸了数字政府的多维功能;决策层,人工智能模型提升了数字政府的运行效率;行为层,人工智能模型增强了数字政府的执法精度。从风险维度看,人工智能模型也对数字政府建设产生多方面影响:首先是从技术霸权、垄断以及人工智能模型基于技术本身对信息的自动获取看,数据主权受到动摇并进一步影响国家安全;其次是人工智能模型带入信息后引发的资本异化,将产生社会性的影响,进而冲击我国社会主义现代化建设成果;最后是无法响应人工智能模型冲击的信息秩序面临失范风险,个人权利等安全边界遭受侵犯。有鉴于此,迫切需要夯实法治基础:第一,运用法律激励手段,推进并完善自主创新的生成式人工智能系统;第二,结合数据分级制度,实现和升级合规生产的生成式人工智能系统;第三,实现关系适法样态,构建权责分配的生成式人工智能系统;第四,寻求原则统摄,设计伦理遵循的生成式人工智能系统。此外,还要完成配套的规制方案:事前立法机关应当履行风险预防义务,事中执法机关应当负担侵害排除义务,事后司法机关应当承接权利救济义务。

关键词:数字政府;人工智能模型;数据主权;权责分配;数字中国

中图分类号:TP18;D63 **文献标志码**:A **文章编号**:1008-5831(2026)02-0308-17

基金项目:2022年度国家社会科学基金后期资助项目(22FZXB083)

作者简介:张楚凡,武汉大学法学院博士研究生,Email:zhangchufanjx1994@126.com;张佳琳,博士,辽宁大学马克思主义学院副教授。

一、问题提出

2022年，习近平总书记在党的二十大报告中提出，要“加快建设数字中国”[1]。2024年3月5日，李强总理在第十四届全国人民代表大会第二次会议上所作《政府工作报告》再次强调，“加快数字政府建设。以推进‘高效办成一件事’为牵引，提高政务服务水平”[2]。2025年，《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》指出，要“全面实施‘人工智能+’行动，以人工智能引领科研范式变革，加强人工智能同产业发展、文化建设、民生保障、社会治理相结合，抢占人工智能产业应用制高点”[3]。显然，数字政府建设不仅是数字中国建设的题中应有之义，更是实现我国治理体系和治理能力现代化的重要举措，为打造服务型政府，提升治理效能提供了新的动力。数字政府建设离不开科技的支撑，随着智能化科技体系的发展，新技术赋能数字政府建设的路径更加多样化，同时也使政府治理更加直接地享受到科技发展的红利。

在全面发展新一代人工智能技术的背景下，如DeepSeek、ChatGPT等人工智能交互软件①，更加广泛地被用户所接受的基础在于其多进程多模式的自主学习能力。在拟人化、智能化的语言交互系统下，这种学习以及运算能力的进步使其应用的场合更加广阔，如在医疗、金融、教育等领域，其“改变人类工作方式，将人类从繁复的劳动中解放出来”的发明初衷已经初步显现。例如，当AI用于辅助教学，可以通过将机器学习与检查表相结合用以形成教学、科研与人才评价和反馈[4]，乃至定制教育方案、进行个性化的辅导反馈[5]。当然，在我们享受人工智能技术所带来便利的同时，也应当具有危机意识，如科技巨头马斯克（Elon Musk）提出，ChatGPT的出现使人类面临的危险而强大的AI风险更进一步。我国作为数字技术开发与应用的先行国家，同样需要思考DeepSeek、ChatGPT这一类具有强大自我学习能力的人工智能交互软件是否能够参与或是以何种方式参与我国的数字政府建设。国外有学者研究认为，人工智能在政府和政治领域的应用可分为以下几类：在政治方面，可帮助改善选民外联、增效竞选活动和加强政策分析；在公共安全方面，可帮助减少响应时间和优化资源配置；在税收方面，可以方便个人报税；在法律方面，可协助提起诉讼、提高法律效率、加强合同分析、简化文件审查；在军事方面，可帮助改进情报分析、优化后勤和提升训练[6]。新加坡政府推行利用ChatGPT模型辅助公务员草拟报告和演讲稿的实验性项目；美国国防部已经在创建人工智能合同编写解决方案，称为“AcqBot”，以简化复杂采购流程[7]。有学者直言，DeepSeek、ChatGPT模型是当前AI技术发展的一次“质变”，其未来的作用不亚于互联网的发明[8-9]。因此，作为人工智能技术较为领先的国家，我国要在科技变革中占得先机并保持优势技术地位，也应当积极开发与利用相应技术。具体到政府治理能力提升与职能转变，必须认真思考人工智能模型与数字政府的关系，在综合权衡人工智能模型对数字政府建设可能带来的功效和风险基础上，及时作出决策并提前采取措施，对其进行有效引导和规范。

二、技术全景：数字政府与人工智能模型的三重交互

人工智能模型在数字政府的建设上具有强大的正外部性，其最大优势在于构造了一种双重偶联的“间性”治理模式，这种模式的直接观测点在微观，它通过优化每一个治理问题点上的交往结

① DeepSeek、ChatGPT只是生成式人工智能的典型代表，类似的还有Google LaMDA、Chatsonic、Sparrow等，它们都致力于通过收集和分析大量的数据，从而简化人类的基础工作。

构,实现技术善治的联结目标。这意味着,人工智能模型辅助数字政府建设的行动逻辑,是从微观着手实现问题点的治理,进而将治理点扩散链接为最具效率的全局治理路线[10]。同时,人工智能模型对数字政府建设的宏观影响,并不仅仅体现在制度运行及其治理实践上,这种影响往往还通过治理行为反向渗透至各类静态组织要素本身,包括治理观念、治理工具、治理信息链乃至权力递导架构等。不过,出于对认知效率的考量,本部分并未沿着上述发生学的路径展开,而采用了从宏观到微观、从静态(制度安排)到动态(治理实践)的倒叙策略。

(一)结构层:人工智能模型与数字政府的功能互动

技术赋能意涵了组织、技术和流程梳理的制度逻辑,而新技术要想成功嵌入政府行政体系,则必须经历"技术连接—信息驱动—结构再造"的过程,这三个环节的环环相扣将直接推动数字政府在治理结构、方式和效能上的深层变革[11]。

1. 人工智能模型推动数字政府技术联结

在技术和数字政府效能的关系中,技术成功赋能的关键在于组织结构自身对技术的吸收[12]。人工智能模型能够成功赋能数字政府建设的关键不在于其AI技术的运用,而在于其具有强大的系统规划性与技术兼容性,更多地整合了云计算、大数据、物联网、移动终端等构建的"云+网+端"的基础设施、互联互通的数据资源以及高效协同的业务应用[13],在多重技术的共同作用下,实现了数字政府的整体技术联结。同时,多重交互系统的应用使技术联结能够在统一的系统中运用自然语言系统表达出来。相较于以往的AI技术,虽然其技术水平也可以实现但却需要专业人才长期调试,或是出现交互系统词不达意的情况时,人工智能模型可以通过其逻辑的学习以及对问题精准的应对,更加直观地满足行政相对人的行政需求。从目前人工智能模型的应用情况看,其先进的人工智能算法体系,在一定程度上与数字政府的需求不谋而合。例如,美国国土安全部的美国公民和移民服务局开发的聊天机器人EMMA,每月可受理一百万人的申请,并能够处理英语和西班牙语的请求,具有包括回答有关移民服务、绿卡获取流程、护照和USCIS提供的其他服务功能[14]。当然,随着人工智能模型技术运用的加深,数字政府建设的功能必然会呈现更加多样化的趋势。

2. 人工智能模型强化数字政府信息驱动

在现有的数字政府建设模型上,其整体系统基本是以大数据和人工智能机制为枢纽,以信息技术为支撑,以行政需求为外观的逻辑架构。在数字政府建设的过程中,为满足其提升整体治理效能的目的,更多的需求在于实现各个环节相互协调,并最终形成一个整体性的行政作业流程。"信息技术有助于推倒组织之间的壁垒,赋予政府及其合作伙伴各种工具,以跨越组织界限进行有效的合作"[15]。但在科层制体制之下,囿于信息技术、信息人才和治理视野等方面的局限,信息处理能力与需求的不匹配严重影响了数字政府的治理效果和运行速率。实证研究证明,数字政府建设主要通过提升财政透明度和缓解信息不对称两条路径赋能地方政府治理[16]。人工智能模型的优势在于其对信息驱动的重视,在模型建立时本身就已经涵盖了上千亿的数据参数,这种庞大的信息数据库是解决数字政府技术系统中信息数据长期冗杂、信息提取能力受限、信息处理能力较弱的可行方法。人工智能模型将包括政府数据、社会数据、互联网数据在内的信息资源加以融会贯通,通过信息共享机制以及一站式服务机制整合分散的治理资源,实现不同系统主体的数据汇集,并借助"深度交互系统"实现政府服务系统的智能化。

3. 人工智能模型实现数字政府治理结构转变

在向服务型政府转型的过程中,数字政府建设的系统性要求政府必须从单向度管理向多元主

体协同治理转型。但转型过程中实际仍然面临政府的专门职能、部门团体、既有制度不协调,以及参与主体范围窄、利益导向倾向严重的情况,极大困扰了数字政府的效能提升。因此,实现数字政府治理结构转变需要解决目前“割裂”的局面,实现跨部门、跨层级的综合治理尤为重要。人工智能模型的优势在于凭借其信息搜集、数据处理和语言组织等方面的技术优势可以打通科层制体制下高度分工的部门服务主义,形成“去中心化”的治理结构,增强部门之间的协同性与联动性。正如清华大学教授周伯文所言,建基于“人+环境+AI”相互交互的ChatGPT,本身即是一个跨时间、跨区域、跨层级的协同系统[17]。

(二)决策层:人工智能模型与数字政府的运行互动

随着中国特色社会主义进入新时代,“算法”和“智能”正在以前所未有的深度和广度形塑政府治理,逐渐形成政府政务服务的数字化、智能化转型,以全新的运作模式和智能生态向人民群众提供智能化政府服务。

1. 人工智能模型提升政府服务自动化水平

生成式人工智能技术赋能的算法模型将政务办公服务场景升级到更加智能的层级。生成式人工智能技术特有的机器学习和自动交互生成等特征在繁杂的政务服务面前具有智能优势。这一路径的支撑逻辑是,以数据赋能打破信息壁垒,以技术创新提升服务效率,让数字技术成为政务服务质效跃升的“加速器”[18]。人工智能模型能够有效克服政务服务和办事群众的“在场性”弊端,结合办事需求提供线上和线下相结合的服务生态,能够有效克服政府服务的时间空间限制,延伸政府服务的触角至服务一线,最终形成线上线下、虚实交互的扁平化政府组织结构,从而实现政府政务服务的提质增效。同时,人工智能模型形成的政务服务智能生态建立于人工智能的精准感知、准确理解和快速响应的基础之上,能够对政府治理过程中所需的资源要素进行深度整合应用,最终形成自动化的、兼具科学高效特征的应用型方案,从而有力回应构建数字政府的时代诉求。

2. 人工智能模型提高政务管理无人化程度

最为常见的现代政府组织形式是科层制,科层制下的行政效率与行政主体的理性程度息息相关。也即,只有行政主体在理性规范下才能避免实施人格化的、情绪化的非理性行政行为,才能实现对行政行为效率和质量的期待。因此,非理性的行政行为也通常被认为是科层制组织形式的弊端。人工智能模型的应用,能够有效克服科层制带来的弊端——交互式人工智能的非感性保证了行政行为的理性前提。也即,人工智能模型能够帮助行政主体从机械重复的政务服务工作中解脱出来,克服行政主体群体中常见的疲劳倦怠和操作失误等问题,从而更好实现生成式人工智能在理性方面的承诺。在政府政务服务中,人工智能模型可以同时有序地处理多项工作任务,依靠政务大数据资源和智能人机交互模式及时作出行政决策,有效提高行政效率并降低行政成本,为政府数字化转型创造价值,为政务智能化管理提供方向。

3. 人工智能模型推动电子政务公平化

生成式人工智能依托大数据技术而具有“类人”的学习认知能力,其离不开人工智能模型的支撑。同人类从经验教训中获得知识一样,人工智能模型作出行政决策的依据是以往典型的行政决策案例构成的资料检索库。在政务服务中,由于行政主体的认识差异和模型学习的机械性和固定性,大数据模型作出的行政决策不可避免地带有一定的算法歧视。随着人工智能技术的迭代更新,人工智能模型通过对话方式,以更高水平的价值创造和更精细的公众联结,能够根据群众诉求进行政府政务服务的识别匹配,最终以更加精准细腻的政务服务供给回应群众需求。数字政府可以增

进公众对政府透明度和回应性的感知[19]。在政务服务实践中,人工智能模型重构政务服务运作模式,通过问答式算法设计有效提升政务服务的智能性,在“一问一答”式对话中增强使用者的体验感。以人工智能模型为代表的智能技术融入我国数字政府建设中,是建设以人民为中心的服务型政府的应有之义,以生成式人工智能的高智能性和高便利性回应人民对美好生活的需求。

(三)行为层:人工智能模型与数字政府的执法互动

DeepSeek、ChatGPT模型均是弱人工智能向强人工智能过渡的产物,同其他人工智能技术的发展历程相似,DeepSeek、ChatGPT的发展也是机遇与风险并存。人与人工智能模型的交互对数字政府建设产生了具有革命性的重大影响,形成了人与人工智能模型交互的新型政府政务服务模式。纵观当前数字政府建设中的人机交互模式,其出发点更多地集中在政府端的技术革新,而非从群众需求出发,探索能够确保人民群众深度参与的人机交互模式。现实生活中,在民众、企业、社会组织同政府部门工作人员交流沟通的过程中,经常遭遇无效行政和低效行政的状况,让民众倍感无奈。即便通过政府互联网线上办事端口,或者通过政务热线寻求解决问题的方案,抑或通过政府部门网站获取所需信息,民众也经常遭遇政务服务困难。

根据数据统计,当前我国数字政府建设过程中,存在亲民性不足的情况,严重阻滞了民众与政府的数字化沟通[20]。有学者指出,人与人工智能模型的交互,能够在数字政府建设过程中增强政府的民主性和回应性以更好地体现民意,从而有助于建设回应型民主政府[21]。人工智能模型在各领域都具有强大的适用性,通过对各领域信息数据的整合,以及高水平的人机交互对话,极大地提高政务服务的响应性,在此过程中人工智能模型扮演着政府与民众进行有效沟通的智能平台的角色。不同于对话式人工智能的种种局限,人工智能模型实现了两方面的完善:一方面,人工智能模型的人机交互是一种学习方式,而非以往单纯的机械式应用。以往人工智能人机互动仅是重复式的机械性的问答,只是为了完成任务而非能动的学习与提高,也无法准确理解人的意图反馈。而人工智能模型的人机互动具有较强的协同性,在数字政府建设场域中,人民群众的反馈能够帮助人工智能模型快速定位所需知识,并及时更新数据库,作出精准回答。另一方面,在人工智能模型训练过程中,模型数据的样本量和参数规模达到一定程度之后,民众反馈信息的价值远远高于数据规模和运算结果。也即,人工智能模型借助民众反馈的信息,运用其强大的学习能力,从人的视角出发,完善其与人交互对话的能力,在这个过程中让人获得互动感和获得感。总的来说,人工智能模型本身具备的强大学习能力和语言生成能力,能够为数字政府建设中破解“政府—民众”互动难题产生实质帮助,能够有效解决传统交互模式下的“老大难”问题,同时极大降低民众同政府沟通过程中的各类成本,提高人们与政府沟通的体验感。

三、风险检视:数字政府与人工智能模型的三重问题

人工智能模型强大的运算和语言组织能力,已经让人望而生畏。与其他领域类似,在政治领域使用人工智能模型也存在各种威胁,包括隐私和安全问题、道德问题、错误或误解的可能性,以及给出带有偏见性建议的可能性。那么如何发挥人工智能模型的正向作用,尤其是在算法行政中的应用,成为本次探讨的主要内容。

(一)国家安全风险:数据主权的动摇

数据主权安全风险是指在处理、存储和传输数据过程中,可能导致数据的机密性、完整性和可用性受到威胁或侵犯的风险。这种风险涉及对数据的控制权和保护的问题,以及可能对数据的安全性

和隐私性产生负面影响。在当今社会,数据已经成为一种重要的生产要素,不仅如此,它也是政府实现智能化建设的战略资源之一。随着数字化的快速发展,数据安全已经成为数字政府建设中不可或缺的重要组成部分。从微观层面看,数据安全涉及数字政府的建设基础和运行秩序。这意味着保护数据的安全性和完整性对于数字政府的正常运转至关重要。而从宏观角度看,数据安全与国家的数据主权安全密切相关。《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》强调,要"加强网络、数据、人工智能……新兴领域国家安全能力建设"[3]。国家数据主权安全是国家主权在网络空间领域的延伸,它代表着国家对数据、软件、标准、服务和其他数字基础设施享有的合法控制权、最高管辖权,以及国家在全球数据治理中独立自主参与和合作的权利[23]。保护国家数据主权安全意味着确保国家对自身数据的控制和管理,以及抵御来自外部的威胁和干扰。这需要国家采取相应的措施,包括制定和执行相关法律和政策,建立安全的数据存储和传输基础设施,加强网络安全和防御能力,以及积极参与国际合作,推动数据治理的规则制定和落实。

1. 数据主权风险的"基础动因":数据流动及其存储困境

数据的运行本身就意味着自由流动,而基于数据自由的原则,各国会进行相关内容的分享,并由此展开文化和商业层面的交流。在全球化的背景下,这一趋势不可阻挡。然而,随之而来的是无法忽视的数据风险,它包含了两个方面。其一是数据源头的不确定。在电子化时代之前,各种经由书面传播的信息都可以得到较为有效的官方审查,只有通过审查的刊物,才能获取正式刊号并印刷。这种模式的信息传递更易于溯源到传播源头,一旦出现不当的言论或颠覆性的观点,政府都能够及时加以管控和处理。但是在数据化时代,对信息起始之处的追溯俨然变得十分艰难,毕竟任何一个人只要拥有智能手机,就可能成为信息端。同时,因为牵涉数据的跨境传播,许多危害信息对本国的入侵会由于属地原则的限制而无法予以合法制裁。此类危害信息中,最为突出的莫过于意识形态层面的渗透[23],②,其主要通过各种视频的形式宣传资本主义的价值观念,由于其中往往并不含有暴力或色情的元素,所以在信息审核的过程中,很难被察觉,特别是基于数据源的不明确,即使最终被排查出来,也难以做到治标治本。其二是数据存放地的风险。一方面,虽然近年来我国的电子信息技术已经获得了长足的发展,但是相较于西方国家,仍然有着不小的差距,所以不少重要信息都可能依赖国外的技术甚至存储设施,而一旦信息被备份在国外的应用设备上,难免会对我国的信息安全构成巨大威胁,尤其是可能发生敏感信息的泄露。另一方面,即使存储地在我国境内,由于技术的后发等因素,加之政府信息存储较为集中,极易成为网络攻击的对象,被一些发达国家的人员非法窃取相关信息[24],③。

2. 数据主权风险的"加重情节":人工智能模型的敏感信息抓取特性

在大数据时代,国家情报安全的内涵与外延都被扩展了。传统安全和新型安全之间的界限变得模糊,这导致国家情报安全体系从线下转移到线上。而技术算法对国家主权安全的影响主要在于技术算法在无形中拓展了国家主权安全的边界。国家数据安全、信息安全均与国家主权安全密切相关,同时也会对国家政治安全和经济安全等其他领域产生影响,这可以被称为"蝴蝶效应"。此外,根据国家立场和利益的不同,涉及国家安全和国家利益的敏感数据,如国防建设信息、军事建设信息和国家外交数据等,容易成为网络攻击的主要目标。因此,将人工智能模型直接应用于我国数

② 在当今全球各种思潮、文化和价值观念相互碰撞的背景下,人工智能技术面临着被政治操纵、用作意识形态宣传的风险,应当对此始终持谨慎态度。

③ 政府的数据存储系统受到攻击时可能会造成数据意外泄露,数据的聚合处理也会威胁到公民的隐私权。

字政府平台可能会引发大规模敏感信息泄露的风险。

数字政府建设依赖于关键信息,涉及政治、经济、文化、社会和生态等领域。如果将这些关键信息直接作为人工智能模型的信息基础,那么涉及国家安全和国家利益的敏感信息也会暴露在技术算法的视野之下,严重破坏重要敏感信息的保密性和完整性。同时,作为一个语言模型,人工智能模型在语义分析中可能会抓取涉及国家情报安全的信息。稍不留神,这些信息就可能被国外情报机构利用,从而引发国家数据主权安全隐患。此外,在数据出境和数据入境的情境中,作为一种人工智能生成式内容的工具,人工智能模型生成并传输的信息数据很容易受到错误文化思潮和西方价值观的恶意渗透,这可能会影响我国的主流安全价值观建设体系,阻碍我国主流意识形态的传播,并导致数据跨境流通的安全隐患[25]。

总的来说,引入人工智能模型到数字政府平台时可能存在的国家安全和数据安全隐患,以及与国家情报安全和主权安全相关的问题,可能阻碍我国主流思想意识形态的传播并造成数据跨境流通安全隐患。

(二)社会安全风险:资本运作的异化

大型语言模型(Large Language Models,简称LLM)快速产生大量文本的能力可以前所未有的规模传播错误信息,这可能会产生"人工智能驱动的信息疫情"——信息疫情成为一种新的公共安全威胁[26]。而当这种人工智能传播的技术掌握在资本的手中时,通过传播乃至编造虚假、错误信息影响社会思潮的形成,进而解构和威胁主流思想的权威性便成为可能。

1. 人工智能模型推高技术资本侵蚀风险

马克思将工业定义为"人的本质力量的公开展示"[27]。在此观念下,无疑应当将技术进行"主体行为客体化"理解,即在人类进行对象化活动的过程中,技术居于客体地位。人工智能模型作为辅助数字政府建设的技术性工具,能够在技术赋能的视域下革新政府行政权力的实现方式,提升其实际效用。此时,如何把握"技术"与"权力"的平衡是将技术嵌入数字政府建设过程中的重点问题。然而,人工智能模型的引入强化了技术资本的话语控制权,可能会引发因"技术"一端加码而导致"技术"与"权力"失衡的难题,政府等公权力机关在行政活动中的主体地位受到威胁。我国数字政府建设的实践深刻反映了数字资本对社会治理的双面性,资本促进了技术创新及应用,同时也限制了技术更好地向服务社会方向的发展[28]。在数字政府建设过程中,行政机关由于技术基础较为薄弱,专业人才较为缺乏,极易受到技术与资本的双向侵蚀。过度依赖人工智能模型,甚至可能颠覆行政机关在行政治理活动中的主体地位。在此情形下,与行政相对人进行交互式对话的主体会由行政机关变为人工智能模型支持下的智能算法。由于对技术与资本的双重依赖,国家行政机关行政权力的公共性特征受到挑战,政府公权力中蕴含的权威出现分化甚至流失。在政府主体地位受到威胁和政府公信力受到挑战的情形下,行政机关的行政治理能力势必会被削弱,行政公权力也将面临解构困境。

如果技术的进步与使用始终无法脱离资本主义的干预,技术的"自律"极易衍变为侵犯人类主体性地位的"他律"[29]。当前,人工智能技术迅速发展并扩张应用至医疗、教育、执法等多领域,但相应的制度规范与价值逻辑尚未实现同步更新。同时,由于技术赋能视域下算法歧视、算法偏见等隐形风险的存在,数字政府建设的实然状态并未达到预设目标。在此状况下,若盲目引入并过度依赖人工智能模型,极易颠覆行政机关在行政治理活动中的主体性地位。换言之,数字技术应用与数字行政治理之间尚未建立平衡稳定的关系,技术资本的话语权相对较强,极易消解行政权力的公共性

特征。

2. 人工智能模型推高技术资本同化风险

在数字政府建设过程中,行政机关对技术资本具有天然依赖。但是,基于成本考量和技术劣势等原因,行政机关往往选择技术相对成熟的市场主体作为外力,为数字政府建设提供技术支持。但是,在此过程中,技术资本的逐利属性难免会在无形中对数字政府治理逻辑产生同化影响,行政机关的公共属性最终被技术资本的功利主义价值观同化,产生“大数据功利主义”[30]。依据行政法中权责一致的基本逻辑,传统行政治理活动中的决策主体应当为自己的决策结果承担不利后果。但是,在人工智能模型引入数字政府建设过程中,决策程序和决策依据很大程度上依赖于人工智能模型的算法设计和训练数据,若由于算法歧视、算法黑箱因素引发决策失误,追责链条就会受到负向影响进而产生断裂风险。

以比例原则规约算法行政的逻辑出发点为权力制约与损益均衡。基于人工智能模型的算法化、自动化、程序化表征,在算法行政视域下,能够有效减少主观情绪、价值选择、人情关系等因素对行政决策主体的主观影响,从而促使行政治理活动趋于客观化、标准化。但是,在此过程中,政府与市场的权力边界出现交叉,行政机关与技术公司甚至中介机构的责任归属和责任比例难以界定。一旦出现决策失误,多元主体的耦合行为难以自证主观过错,归责方式的意向性要件缺失。人工智能模型嵌入数字政府建设过程不同于以往的政府采购服务,而是以行政治理的参与者甚至是主导者的身份角色存在于行政治理活动中[31],公共责任的承担出现分化甚至转移。例如,印度在疫情管控活动中应用的智能工具(Aarogya Setu),虽然能够有效追踪病毒传播链条,但其严重影响了健康公民的出行活动,目的与手段存在不当联结[32]。此时,技术资本难以针对个性化的社会公共需求作出具体行政行为,社会公民的权益可能出现增加和减损,进而脱离比例原则的实施初衷,压缩行政裁量行为的生存空间,损害行政相对人的合法权益。

(三)个人安全风险:信息秩序的紊乱

人工智能模型背后强大的训练数据库和主体信息库能够提升行政治理的精准性和高效性。但是,从人工智能模型的基础隐私保护声明及其运作机制看,在行政机关的行政治理活动与个人信息保护活动中依然存在明显张力,行政治理活动前端和终端环节均可能衍生出数据安全风险。并且,政务数据涉及的群体向度广泛、价值密度较高、安全保护传统,在数字政府建设过程中极易产生数据收集失当、数据运行失序、数据监管缺位等风险,危害政治安全与社会公共安全。

1. 信息生产秩序失稳:人工智能模型过度收集治理对象信息

数字政府建设的基石是政务数据的收集、整合、分析、服务和应用[33]。人工智能模型的算法设计和运行依托于强大的训练数据库,基础训练数据的规模与行政治理活动的准确性基本呈正相关。而人工智能模型中训练数据库的建立和完善,离不开行政治理活动前端的信息收集程序。但是,从ChatGPT模型公开的隐私保护文本内容看,OpenAI公司的数据收集规则模糊,对于个人基本信息和敏感隐私数据的收集程序和使用场景并未进行具象化操作,数据权利主体的“知情—同意”权未得到充分保护。在数据收集规则尚未得到完善的前提下,将人工智能模型引入数字政府建设,无疑会加速个人基本信息和敏感隐私数据被不当收集的进程,政务数据安全风险程度也随之升高。

在数据供给阶段,将人工智能模型引入数字政府建设,会为其训练数据库的扩张披上“政府公权力”的外衣。在社会契约论的理论架构中,行政机关是公共权力行使的“代理人”。政府信任是政治合法性和政策有效性的重要基础[34]。但是,由于技术资本的裹挟,算法公司的技术优势极易演变

为技术权力,颠覆数字政府建设的治理逻辑。若以行政治理为名,加快人工智能模型训练数据库的扩张,基于行政机关的公信力,无疑会降低社会公众的警惕性,使“知情—同意原则”陷入形式主义泥潭,加剧个人数据收集和使用的道德伦理风险。

2. 信息加工秩序失稳:人工智能模型过度整合和支配治理对象信息

在数据运行过程中,数据壁垒和数据垄断等现象加剧数据运维风险。数据整合过程就是在完成前端数据收集的基础上,以数据抽取、数据转换、数据加载等方式,以可利用程度为价值选择标准,将大量散乱的数据系统化、类别化的过程[35]。由于资源分布状况、部门协同建设等差异的存在,政务数据的协同共享机制尚不完善,数据壁垒、数据垄断等问题依然存在。无纸化办公和数字化流程使程序越发难以用特定的制度节点进行界分,可能重返“算法黑箱”时代[36]。鉴于算法黑箱等问题的存在,人工智能模型在数字政府建设运行过程中,极易因算法漏洞等问题在侵犯政府和公民知情权的情况下,变更数据分析结果和具体用途。加之技术门槛的存在,政府和公民仅能从宏观角度把握政务数据的整合过程,却无法探知整合结果与预设目标的细微差异。在国家互联网信息办公室发布的《生成式人工智能服务管理办法(征求意见稿)》中,虽然规定生成式人工智能在向社会提供公开服务前,应向国家网信部门申报安全评估,履行算法备案和变更、注销备案手续,但是并未设立算法向社会公众公开的规范内容,社会公众对算法设计的知情权和监督权仍未得到有效保证。同时,人工智能模型还有可能面临因数据收集偏差、数据样本欠缺、分析标准错位等原因降低政务信息的有效性和可利用程度,进而增加或减损公民权益,影响政府公信力,威胁公民人身财产安全。

在数据流动过程中,数据共享程度的加深会拓展政务数据的可攻击面。在人工智能模型应用至数字政府建设的过程中,政务数据对社会公众的开放程度进一步加深,行政机关内部的安全防护和数据管理呈现出应用上的局限性,政务数据的非法传播、复制、篡改风险加剧,个人基本信息与敏感隐私信息以及国家安全数据的安全性面临新的挑战。概言之,人工智能模型的技术优势和逐利属性极易受到个别行为人的不当利用,基于算法的潜在性、隐藏性等特征,对数字政府行政治理活动产生公共性、安全性、政治性威胁,加剧技术资本对个人信息和国家安全的侵蚀力度。

3. 人工智能模型对信息的不当存储易产生数据泄露风险

部分西方国家已经开始注意到广泛运用人工智能所引发的不当后果。例如2023年3月,意大利数据保护局(DPA)主席对Open AI实施了临时禁令,原因是该公司严重违反了欧盟关于个人数据处理和保护的立法,未能向其用户提供足够的隐私信息,并且缺乏适当的数据收集法律依据[37]。这表明,人工智能模型嵌入数字政府建设中的确存在许多法律风险,尤其是人工智能模型对数据信息的不当存储容易导致数据泄露,这对政府的公信力将造成严重的负面影响。

首先,人工智能模型的服务提供者没有明确是否存在对使用者的信息进行删除的程序或规则,甚至使用者对于人工智能模型是否存储了个人数据也毫不知情。当人工智能模型嵌入数字政府治理中时,由于处理的个人数据基数更为庞大、类型更为多样以及信息更为敏感,一旦在公民不知情的情况下擅自存储,不仅涉嫌对公民个人数据处分权的侵犯,还将对国家数据安全构成威胁。其次,人工智能模型在对公民信息不当存储的同时也未明晰存储的时间期限。诸如Open AI、谷歌、百度、阿里巴巴等人工智能或互联网公司,都未直接规定人工智能模型收集数据的存储期限。面对无期限的存储状况,公民个人信息保护将受到严峻挑战,人工智能模型无限期存储公民信息的行为将令公民个人数据长时间暴露在泄露的风险之中。最后,由于对信息数据的不当存储和无限期存储,公民个人数据泄露成为可能或必然。数据泄露具有不可逆的特征,政府处理的个人数据具有高度

的敏感性,此类型数据泄露将伴随终身的风险。并且,根据数据泄露后的不同流向,也将对数据权利主体产生不同程度的伤害。人工智能模型不当存储公民信息数据已经构成对公民知情权和处分权的侵犯,如果由于操作不当或非法盗取等因素导致数据的大面积泄露,则不但侵犯了公民的数据隐私权,更令数字政府建设陷入信任危机。总之,人工智能模型嵌入数字政府治理后,能够精准记录公民的一切隐私数据,经过简单的数据整理与智能算法,便会轻松推测出个人偏好等隐私信息,这无疑会加剧个人隐私信息泄露及被滥用的风险[38]。

四、法治保障:数字政府与人工智能模型的交互根基

面对新一代数字技术的普及与深度运用,数字政府建设也将不断迎来未知风险,这是创新价值导致的必然结果。因此,需要以制度的刚性力量防范人工智能模型涌现出的法律风险,并通过法治化的约束体系进一步强化制度保障的效果。

(一)法律激励:推进自主创新的生成式人工智能系统

尽管DeepSeek曾经一度引领了当今世界生成式人工智能的发展路向,并且在技术成熟度和语料资源丰富度上都一枝独秀[39],然而必须意识到,人工智能模型的技术开发者大多是外国人工智能企业,一般的跨国商业行为是值得支持的,但将其嵌入我国数字政府建设后,如不做好防范措施,则极有可能产生国家数据安全风险,侵犯国家数据主权。ChatGPT的核心技术是InstructGPT,即采用基于人类反馈的强化学习(Reinforcement Learning with Human Feedback,RLHF),让人工智能模型的产出和人类的常识、认知、需求、价值观保持一致[40]。这一技术依赖由语料体系、预训练算法和微调算法组建起来的主体架构。首先必须提供千亿以上级别参数量的文本数据,以此为基础建立具有文本向量表示能力的预训练模型,再加上微调模型赋予预训练模型修改生成内容和生成更合理内容的能力,才能够令人工智能模型生成的语言更加贴合人类表达习惯。无论是基于海量数据的语料库学习,还是通过各种算法程序的辅助训练,都有可能产生数据安全风险,甚至意识形态安全风险[41]。因此,为了保障数字政府建设,必须构建自主的生成式人工智能系统。

当前国内一些技术团队也在展开对生成式人工智能系统的研发,例如DeepSeek(深度求索)、百度"文心一言系统"和复旦大学"Moss系统",但仍然处于民间资本或学术研究层面上。要想使生成式人工智能真正有效融入数字政府建设中,就必须借助国家层面的力量,运用具有鲜明优势的举国体制,加大对生成式人工智能的技术投入,组建专门科研团队集中攻关核心技术。一方面能够有效弥补民间力量开展语料库训练时资金不足的缺陷,促进自主生成式人工智能技术的有效突破;另一方面也能够确保语料库中数据流通的安全性,从而将国家数据主权牢牢掌握在自己手里。

(二)数据分级:实现合规生产的生成式人工智能系统

人工智能模型与数字政府建设相结合既需要利用好人工智能系统的信息技术优势,同时也要遵守国家安全、数据安全底线,防范信息时代可能产生的数据安全问题;尤其是在"数字政府建设"这一议题项下,又涉及政府层面的财政、税收以及公民层面的商业、医疗、交通等各个方面的数据,因此做好底层制度建设甚为关键。数据确权、数据分级分类制度可以说是整个数字时代的"基础设施"[42],前者涉及对数据内人身及财产权益的分配,后者则与数据安全问题紧密相关。从当前的制度实践以及学理探讨看,关于数据分级分类已经形成了一些共识,但同时亦有分歧。要推进人工智能模型与数字政府建设深度融合,就需要在共识的基础上努力化解分歧,以提升服务型政府效率为总体目标,建设好数字政府效率与人工智能相结合的基础工程。

关于必须建立数据分级分类制度已经达成了共识,并写入法律。《中华人民共和国网络安全法》第21条明确规定“国家实行网络安全等级保护制度”,《中华人民共和国数据安全法》(以下简称《数据安全法》)第21条也规定“国家建立数据分类分级保护制度”,为数据分级分类奠定了制度框架。在此基础之上,接下来的工作应当是探索如何进行具体的数据分级分类,以能够同时满足促进数据流通以及保障数据安全的双重目标。在《数据安全法》按行业划分进行数据安全监管赋责的要求下④,当前已有部分主管部门出台了数据分级分类的相关指南,如工业和信息化部印发《工业数据分类分级指南(试行)》,科技部向国家标准化管理委员会申报的《科学数据安全分级分类指南》获批立项。此外,还有各个地区根据数字产业发展情况、产业数据使用情况等制定了本地区适用的行业数据分类分级制度。可见,数据分级分类已经走向了制度建构与具体实施的阶段,但也正是由于各行业分散监管的格局,造成了当前我国数据分类分级制度的实践分歧。主要体现在行业分散监管的法律赋责导致数据分级分类存在分歧,工业数据、科学数据、金融数据并非泾渭分明,各类数据之间存在交叉,而不同的数据分级分类制度导致某些数据在不同规范内的级别、分类不同,在一定程度上阻碍了数据效用的最大化发挥。

基于此,必须依照《数据安全法》第6条的规定,发挥国家网信部门统筹协调的作用,在与其他行业数据分级分类对标的基础上,尽快推进政务数据分级分类制度的出台。因政务数据与行业数据的交叉更为明显,因此应当以政务数据为基础,统筹协调各行业的数据分级分类框架,由国家网信主管部门主导建立“自上而下”的数据分级分类总体性框架和目录,进而根据强制性适配规则,再由不同行业和层级的政府主管部门加以具体细化,改进当前行业分散进行数据安全监管的弊端,为人工智能模型与数字政府建设的融合提供一个安全可靠的数据资源处理库。

与此同时,建构政务数据分级分类还需具备国际视野,与其他国家进行沟通交流,努力促进数据分类分级的标准一致。其原因就在于,基于数据本身的性质,促进其流通才是发挥数据效用最大化的合理途径。在制定政务数据分级分类规则时,我国应该秉持安全、动态、合作以及可持续的发展原则,把握好数据分类分级与数据治理效能之间的张力,积极与他国沟通协商,努力形成类似于知识产权保护领域中的国际条约、国际协议,从而实现数据治理主权、安全和效能的最大化。

(三)关系适法:构建权责分配的生成式人工智能系统

无论人工智能模型的智能化发展程度如何,至少在数字政府建设这一重要领域当中,仍然应当始终明确其辅助性职责[43],即人工智能模型与数字政府相结合不能也无法代替政府职责,政府永远是作出、实行决策的真正主体。基于此,为防范人工智能模型引入数字政府所可能对行政相对人造成的权益损害,应当对引入前、引入后进行不同的阶段划分,明确政府与人工智能模型这两个主体的法律责任,防范对行政相对人权益造成侵害的风险。

1. 在政府引入人工智能模型前负有安全审查义务

在美国的Open AI公司发布ChatGPT的同时,我国的一些科技创新型企业也同时宣布要开发人工智能模型,部分公司如DeepSeek和百度的“文心一言”亦已经投入市场使用。因此,出于对外合作的安全风险考虑,未来真正与数字政府建设融合的应当是科技公司或科研机构研发的人工智能模

④《数据安全法》第6条规定,“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。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。公安机关、国家安全机关等依照本法和有关法律、行政法规的规定,在各自职责范围内承担数据安全监管职责。国家网信部门依照本法和有关法律、行政法规的规定,负责统筹协调网络数据安全和相关监管工作”。

型。但无论其研发主体是谁,政府都需要在将其引入数字建设之前做好安全审查义务。具体而言,行政机关在人工智能模型引入阶段的审查义务,由审慎选择服务提供方、充分考察服务方技术水平、对服务提供全过程的日常管理等多元义务组成。既要充分考虑到服务提供方的技术能力,同时也要对其数据存储、数据备份以及数据安全中心的建设情况进行全面考察,审慎选择合作对象。如果因政府疏于审查而造成在具体的智能程序运行中产生数据泄露或者对相对人人身、财产权益造成损害,应当由政府作为主体对外承担行政责任,并可由上级政府在行政体制内部追究主管部门及其责任人员的责任。

2. 在政府引入人工智能模型后负有结果审查义务

算法的自动化运行、算法黑箱的存在等不能成为政府对智能模型输出结果不予审查的理由。在秉持人工智能模型辅助性原则的基础上,政府仍然需要对其算法输出结果进行审查,尤其是对于涉及不特定多数人权益以及相对人社会基本权益的事项,更需要对算法结果进行最终的论证与审查,才能将其运用于行政决策当中。换言之,人工智能模型与数字政府建设应当始终警惕"算法至上"陷阱。当行政决策造成相对人权益损害时,在行政法律规范体系下,政府仍应作为主体承担赔礼道歉、恢复原状、赔偿损失等行政责任。

与此同时,人工智能模型或者其服务提供者也并不能因为所谓的"技术中立"而规避责任,模型服务提供者的民事责任是对算法价值中立性观点矫正[44]。具体而言,应当将人工智能模型看作是一种产品或技术服务的提供,因产品或服务质量存在缺陷或瑕疵,作为购买服务一方的政府主体,有权依据民事法律规范要求服务提供者承担民事责任。在因该模型的数据收集或数据分析等非技术中立问题而造成对政府或行政相对人权益损害时,政府可以要求模型提供者承担经济赔偿等责任,并可将其纳入政府采购黑名单,行政机关由此获得的经济赔偿可以作为向行政相对人予以赔偿或补偿的经济来源。

基于以上,以法律方式分配人工智能模型与数字政府融合当中各方主体的权利义务以及责任,才能够约束各主体行为,防范技术应用风险,最大化发挥人工智能模型辅助数字政府建设的功能效用。

(四)原则统摄:设计伦理遵循的生成式人工智能系统

"科学技术的发展究竟是给人类带来幸福还是灾难,完全取决于人类自己而非工具"[45]。人工智能模型可以说是当前人类新兴技术的"集大成者",其能够自主学习的强大技术优势使人工智能系统第一次真正地拥有了类人化的能力。但无论如何,该模型的研发和运用还是需要具体现实的人进行操作,虽然无法对人工智能模型进行科技伦理规训,但是可以对其背后的研发者、应用者进行数字时代的科学技术伦理教育,切实发挥伦理调节器、伦理评估工具以及伦理督导的功能作用 ,使科技创造更多的价值。

算法并非完全中立且客观,在研发与使用过程当中,极容易因为运用人员自身价值观的偏狭而导致技术中立的美好理念被破坏。因此在数字经济时代,还需要通过制度化、规范化的方式加强对人工智能模型研发与运用人员进行科学技术伦理教育,防范其运用风险,促进科学技术效用的最大化发挥。对于研发人员而言,不仅需要其所属机构对其研发产品进行伦理审查,行政监管部门也需要切实履行职责,当发现算法或者其他人工智能产品存在技术伦理问题时,应适时追究法律责任,及时扭转科学研发方向。对于技术运用人员而言,在数字政府建设当中则是指具体的政府工作人员,虽然不要求其知悉人工智能模型的技术原理,但是在运用算法及算法结果时,也需要政府部门加强科学技术伦理教育,以社会主义核心价值观为指导,防止人工智能模型背后技术资本对我国行

政系统的价值腐蚀[46]。

五、规制机制:数字政府与人工智能模型的全程对接

人工智能模型可以成为数字政府建设的重要工具,但是需要建立一套完善的制度体系以管理其数据和信息,促进其辅助数字政府建设的标准化和规范化。当然,制度设计需要符合分级分类的框架,同时需要在公私合作情形中明确数字政府职责,建立科技伦理相关规范和标准,以指导政府部门和数据机构的运作。这些机制和柔性工具的建立可以有效提高数字政府的安全性,避免出现数据滥用、泄露等问题。实际上,引导人工智能模型的理性回归目的是平衡公权力与私主体之间的关系,将保障安全、维护公共信任与保护个人信息和隐私安全有机结合起来,实现信息化和人权保障的有机衔接。数字化建设过程中,国家和政府需要强化对数字技术的监管和规范,制定相关法规和标准,完善事前、事中和事后全链条治理。

(一)事前保障机制:立法机关风险预防义务

现代社会的风险是"被制造出来的风险",是由于我们不断发展的知识对世界产生影响而产生的风险[47]。立法机关制定的法律不仅要符合公众利益和社会道德规范,还要考虑到各种风险和潜在风险的防范。因此,立法机关应当承担风险预防义务。在人工智能模型辅助数字政府的应用中存在个人数据泄露的问题,人工智能模型可能包含用户敏感信息,例如个人身份信息、财务信息和健康信息等。这些信息如果泄露,可能会对用户造成极大损害,导致个人隐私遭受侵犯、虚假诈骗或身份盗窃等问题。数据时代下,单纯地依靠惩戒第三人以达到保护公民数据的作用收效甚微。国家层面的风险预防义务可以从事前预防危害的发生着手,立法机关可以制定和修改与数据保护相关的法律规定,以确保数据和隐私得到适当的保护。例如,通过立法规定数据安全和隐私保护标准。目前大多数人智能模型的训练与测试都在美国服务器上部署,训练过程及测试过程均会收集使用者的信息,甚至会记录使用者的反馈和使用习惯,这存在严重的信息泄露与用户隐私保护风险[48]。《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)中的"知情—同意"规则要求采集个人信息时必须经过个人同意,并清楚告知个人信息采集的目的、范围、方式和用途等内容,通过严格的规定和监管保护个人信息的安全。比如规定数据处理方必须明确告知个人信息收集的目的和方式,以此通过事前风险预防使人工智能模型更好地辅助数字政府建设。

人工智能模型在数字政府建设的应用中,会对公民的个人信息进行收集、处理、分析、存储,以更好地完善政府部门的建设。公民个人数据权利的保障问题是人工智能模型适用的重要问题,人工智能模型需要遵守《个人信息保护法》中"明确告知—充分知情—自主自愿—明确同意",以法律形式有效应对人工智能模型的算法黑箱问题,避免数据收集处理行为背离数字政府建设初衷。然而目前我国个人信息保护的立法存在很多不足,特别是个人信息范围的不确定性和抽象性很难为个人提供明确的行为预期[49]。人工智能模型在辅助数字政府建设中有碍于个人权益的保护,难以发挥其最大价值,同时《个人信息保护法》第14条中关于个人信息处理同意的一般有效条件也存在诸多争议,因而未能充分发挥作用[50]。

数据权主体作出的同意行为的明确性是保障个人数据安全和隐私权利的基本要求。明确性意味着同意人应当对自己的同意行为有充分的理解和认识。只有同意人明确知晓自己同意了哪些内容,并在这些内容上作出非强制性的、自主的、充分知情的决定,才能够保障个人数据安全和隐私权利。数据权主体作出同意的过程应当充分保障同意人的知情权、自主权和选择权。对于数据收集、

使用的目的、方式、范围以及可能的风险和影响需要对同意人进行明确的告知,确保同意人充分理解同意的内容。需要注意的是,国家预防风险并不是一定会彻底消除数据风险,事实上某些数据风险可能是人工智能模型适用数字政府过程中不可避免的,但是国家应该采取预防措施,以确保这些风险不会给公民的数据和隐私权利带来更大的威胁。国家应该针对社会现实的变化不断地调整和完善基本数据权利保障的措施,以确保这些措施能够适应社会的发展。

(二)事中保障机制:执法机关侵害排除义务

在数字政府的建设过程中,政府始终对数字平台负有监管职责。相比立法机关,政府监管机构能够更加细致地执行相关法律和规定,监测和审核那些可能违反数据保护的行为,保护公众的隐私利益和个人数据安全。数字平台是大量个人数据的存储和交换场所,甚至一些数字平台运营商占据了垄断地位,利用数据形成垄断优势。政府需要监管其数据采集、处理、传输和存储等环节,以防止个人敏感信息被泄露、滥用或者遭到其他不法侵害。监管机构可以对数字平台和组织进行检查和评估,确保它们遵守相关法规和标准,将个人数据处理和管理的过程规范化,减少个人数据泄露等安全风险。政府监管还能够对数字平台提供咨询和指导,帮助它们制定更好的数据保护政策。人工智能模型在数字政府的运用中,大量的个人数据被用于训练和学习。政府监管促使人工智能模型制定更好的告知义务,贯彻"知情—同意"规则的实施,并加强人工智能模型履行这一义务的执行力。这样,企业和组织就不得不通过明确、清晰的方式告知个人其数据的使用和处理情况,进一步提高其知情同意的程度和质量,确保其合法性和真实性。通过政府监管强化知情同意规则的实效性,可以有效保障公众个人数据安全和隐私权益,同时也能够促使人工智能模型更加规范地运作和提高可信度。政府监管部门也可以加强对于数字平台上的开放数据的收集与利用,在保障数据安全的基础之上,政府部门同样可以利用数据爬虫、数据清洗等技术实时监控平台上的监管风险并反馈于最终监管决策的形成[50]。人工智能模型可以为监管科技的研发与应用提供决策和方案支持。

(三)事后保障机制:司法机关权利救济义务

司法救济是保护个人数据权益的重要途径,当个人数据被侵犯或滥用的时候,可以向法院提起民事诉讼或刑事诉讼,通过司法程序使自身的合法权益得到有效保护。

一方面可以完善数据权利举证规则,明确数据主体和数据控制者的举证责任。数据主体需要举证证明自己数据权利被侵犯的事实,而数据控制者需要举证证明他们有合法的数据处理基础和程序。考虑到数据主体在举证过程中可能面临难度,法律应该减轻数据主体的举证负担。同时,在数据权利案件举证中,需要建立更为科学、准确的证据标准,确保证据的真实性、可靠性,为法院作出公正、合理判断提供帮助。另一方面,数据权集体诉讼制度的完善也是事后保障的重要举措。数字平台和公权力在资源、信息等方面都优于公民,因此仅依靠被侵权个体难以对抗资源力量更大的数据侵权行为人。适格主体可以是与被告数据控制者的关系密切,并且受到其数据处理活动损害的个人或组织。集体诉讼有助于缓解数据侵权案件中双方法律地位失衡的问题。

有论者指出,算法侵权中的起诉主体不应限于算法运营商的客户或终端用户,只要因算法受到特定滋扰均可提起集体诉讼[51]。由此可以借鉴相关集体诉讼制度的探索,可以将集体诉讼代表扩大到科技协会,使力量微弱的个体能够对抗掌握个人数据信息的巨大的数字平台,实现社会公平。

六、研究总结

人工智能模型引发的讨论需要人文关怀的引入,相较于AlphaGO等人工智能模型,新一代人工

智能模型不仅在对话能力和信息获取方面有了显著的进步,也有了较多难以解释的现象,因而一定程度上代表着弱人工智能向强人工智能阶段转变的普及化。以往的人工智能系统更多的是仅运用于特定领域,但人工智能模型近乎可以适用于社会的各方面和各主体,这就对当下具体化的伦理生活产生了从个人到国家的全方位影响,因而人文关怀不应当仅侧重于某个问题,而应全方位地考察人工智能模型之影响。数字政府建设对新兴技术的利用是一把"双刃剑",经验的证据和价值的论证均表明,法治政府能够有效抵消技术中立引发的伦理风险和技术应用带来的全景风险,故采用从顶层设计到具体制度的法治保障方案是恰当的。未来,人工智能模型的成功已经证明生成式人工智能系统至少是一条可行的道路,制度性的探讨将会在立法、执法和司法的三重作用下逐步成熟,个案研究将会成为进一步值得思索的方向。

参考文献:

[1] 习近平. 高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告[N]. 人民日报,2022-10-26(01).

[2] 李强. 政府工作报告——2024年3月5日在第十四届全国人民代表大会第二次会议上[EB/OL]. (2024-03-12)[2025-08-12]. https://www.gov.cn/yaowen/liebiao/202403/content_6939153.htm.

[3] 中共中央关于制定国民经济和社会发展第十五个五年规划的建议[N]. 人民日报,2025-10-29(01).

[4] 蒋华林. 人工智能聊天机器人对科研成果与人才评价的影响研究:基于ChatGPT、Microsoft Bing视角分析[J]. 重庆大学学报(社会科学版),2025(2):97-110.

[5] Devi S, Sreedhar, Arulprakash P, et al. A path towards Child-Centric artificial intelligence based education [J]. International Journal of Early Childhood Special Education 2022, 14(3).

[6] Bahrini A, Khamoshifar M, Abbasimehr H, et al. ChatGPT: applications, opportunities, and threats [EB/OL]. 2023: arXiv: 2304.09103. http://arxiv.org/abs/2304.09103.pdf.

[7] Allen B. The impact of ChatGPT on the federal workforce [EB/OL]. (2023-04-06) [2023-04-07]. https://www.federaltimes.com/thought-leadership/2023/04/06/the-impact-of-chatgpt-on-the-federal-workforce/.

[8] 张佳欣,刘园园,陈曦,等."顶流"之下,看人工智能喜与忧[N]. 科技日报,2023-02-16(05).

[9] 蒲清平,向往. 生成式人工智能:ChatGPT的变革影响、风险挑战及应对策略[J]. 重庆大学学报(社会科学版),2025(3):102-114.

[10] 封海波. 迈向"数据治理":数据确权方案的本土争论与理论调和[J]. 法理——法哲学、法学方法论与人工智能,2024(2):180-199,371-372.

[11] 邓经超. 数字政府技术资本侵蚀的生成机理与法律规制[J]. 东北师大学报(哲学社会科学版),2023(2):135-148.

[12] 阙天舒,吕俊延. 智能时代下技术革新与政府治理的范式变革:计算式治理的效度与限度[J]. 中国行政管理,2021(2):21-30.

[13] 逯峰. 整体政府理念下的"数字政府"[J]. 中国领导科学,2019(6):56-59.

[14] Dilmegani C. Government Chatbots: top benefits & use cases in 2023[EB/OL]. (2023-10-12)[2023-11-16]. https://research.aimultiple.com/government-chatbot/.

[15] 斯蒂芬·戈德史密斯,威廉·D. 埃格斯. 网络化治理:公共部门的新形态[M]. 孙迎春,译. 北京:北京大学出版社,2008.

[16] 高玉胭,王立勇. 数字政府建设何以赋能地方政府治理:基于大数据管理机构改革的证据[J]. 经济问题探索,2025(12):18-36.

[17] 成都市战略决策咨询服务平台. AI与人和环境的协同与交互:多模态学习的新机遇[EB/OL]. (2023-02-17)[2023-02-27]. https://www.cdasp.org/p/d.php? id=2029.

[18] 汪玉凯. 政务服务变革赋能美好生活:“十五五”时期数字政府建设前瞻[J]. 人民论坛,2025(24):12-18.
[19] Mahmood M, Weerakkody V, Chen W. The Role of Information and Communications Technology in the Transformation of Government and Citizen Trust[J]. International Review of Administrative Sciences, 2020(4): 708-728.
[20] 李书宁,刘一鸣. ChatGPT类智能对话工具兴起对图书馆行业的机遇与挑战[J]. 图书馆论坛,2023(5):104-110.
[21] 张爱军. 人与ChatGPT交互政治的可能性质化:风险维度与规约路径[J]. 学术界,2023(4):61-71.
[22] 段荟,张海,王东波. 信息资源管理领域科研人员对ChatGPT态度、认知及应对策略研究[J]. 情报理论与实践,2023(7):17-24.
[23] 斜晓东. 论生成式人工智能的数据安全风险及回应型治理[J]. 东方法学,2023(5):106-116.
[24] 梅傲,陈子文. 政府数据开放中的数据安全隐忧及其纾解[J]. 情报杂志,2023(5):76-85.
[25] 代金平,覃杨杨. DeepSeek类生成式人工智能赋能中华文明发展传播研究[J]. 重庆大学学报(社会科学版),2026(1):164-176.
[26] Pian W J, Chi J X, Ma F C. The causes, impacts and countermeasures of COVID-19 “Infodemic”: a systematic review using narrative synthesis[J]. Information Processing & Management, 2021, 58(6): 102713.
[27] 马克思,恩格斯. 马克思恩格斯文集:第一卷[M]. 北京:人民出版社,2009:195.
[28] 李娟. 数字政府建设从制约走向融合的逻辑理路:以长三角地区为例[J]. 苏州大学学报(哲学社会科学版),2025(2):31-41.
[29] 孟飞,冯明宇. 数字资本主义的技术批判与当代技术运用的合理界域[J]. 东北大学学报(社会科学版),2022(4):1-8.
[30] 沈琪章. 大数据功利主义计算逻辑中的“道德囚徒”[J]. 太原学院学报(社会科学版),2023(1):9-15.
[31] 肖梦黎. 算法行政责任的分布式重建[J]. 国家检察官学院学报,2023(2):42-56.
[32] 谭九生,胡健雄. 比例原则规约算法行政的法理基础与路径[J]. 理论月刊,2023(3):123-134.
[33] 郭少青,谢明. 以数据治理为中心推进数字政府建设[J]. 中国社会科学报,2022-06-15(07).
[34] 聂爱云,陈林志,况雅琴. 数治增信:数字政府建设如何影响居民政府信任[J/OL]. 产业组织评论,1-16[2026-03-16]. https://link. cnki. net/urlid/CN. 20260312. 1603. 014.
[35] 庄乾龙. 刑事案件中大数据整合行为定性及其适用规则[J]. 法学杂志,2020(12):44-54.
[36] 蒋红珍. 数字政府建设面临的法治议题:以判例为观察视角[J]. 中国法律评论,2025(6):36-52.
[37] De Angelis L, Baglivo F, Arzilli G, et al. ChatGPT and the rise of large language models: the new AI-driven infodemic threat in public health[J]. Frontiers in Public Health, 2023, 11: 1166120.
[38] 张夏恒. 类ChatGPT人工智能技术嵌入数字政府治理:价值、风险及其防控[J]. 电子政务,2023(4):45-56.
[39] 杜振雷,刘金婷,史金鹏. ChatGPT及其核心技术在科技名词规范化中的应用潜力与挑战[J]. 中国科技术语,2023(4):45-54.
[40] 钱力,刘熠,张智雄,等. ChatGPT的技术基础分析[J]. 数据分析与知识发现,2023(3):6-15.
[41] 蓝江. 生成式人工智能与人文社会科学的历史使命:从ChatGPT智能革命谈起[J]. 思想理论教育,2023(4):12-18.
[42] 陈祥玲. 政府数据分类分级保护的理论逻辑、现实困境与实践路径[J]. 征信,2023(4):36-44.
[43] 汪太贤,唐祎. 人工智能嵌入政府治理:算法图景、价值问题与回归路径[J]. 中国科技论坛,2023(2):104-113.
[44] 朴毅,叶斌,徐飞. 从算法分析看人工智能的价值非中立性及其应对[J]. 科技管理研究,2020(24):245-251.
[45] 令小雄,王鼎民,袁健. ChatGPT爆火后关于科技伦理及学术伦理的冷思考[J]. 新疆师范大学学报(哲学社会科学版),2023(4):123-136.
[46] 许开轶,谢程远. 数字政府的技术资本侵蚀问题论析[J]. 政治学研究,2022(2):103-114,170-171.
[47] 安东尼·吉登斯. 失控的世界:全球化如何重塑我们的生活[M]. 周红云,译. 南昌:江西人民出版社,2000.
[48] 张华平,李林翰,李春锦. ChatGPT中文性能测评与风险应对[J]. 数据分析与知识发现,2023(3):16-25.
[49] 齐爱民,张哲. 识别与再识别:个人信息的概念界定与立法选择[J]. 重庆大学学报(社会科学版),2018(2):119-131.

[50] 唐林垚. 人工智能时代的算法规制:责任分层与义务合规[J]. 现代法学,2020(1):194-209.
[51] 陈少威,范梓腾. 数字平台监管研究:理论基础、发展演变与政策创新[J]. 中国行政管理,2019(6):30-35.

Interaction research between digital government construction and artificial intelligence models: An analysis based on the perspectives of issues, rule of law, and regulations

Zhang Chufan[1], Zhang Jialin[2]
(1. *Law School*, *Wuhan University*, *Wuhan 430072*, *P. R. China*;
2. *Department of Marxism*, *Liaoning University*, *Shenyang 110036*, *P. R. China*)

Abstract: The construction of a digital government is an important component of Digital China, and the introduction of artificial intelligence models is of great significance. From a technological perspective, artificial intelligence models provide hierarchical interactions for the construction of a digital government: at the structural level, artificial intelligence models expand the multidimensional functions of digital government; at the decision-making level, artificial intelligence models improve the operational efficiency of digital government; at the behavioral level, artificial intelligence models enhance the law enforcement accuracy of digital government. From a risk perspective, artificial intelligence models also have multifaceted impacts on digital government construction. Firstly, technological hegemony, monopoly, and the automatic information acquisition by artificial intelligence models have eroded data sovereignty and further endangered national security. Secondly, capital alienation caused by the application of artificial intelligence models will exert social impacts and undermine the achievements of China's social development. Lastly, the information order that cannot cope with the impact of artificial intelligence models faces the risk of disorder, and the security boundaries such as individual rights may be violated. In view of this, the first step is to solidify the foundation of the rule of law. First, legal incentives should be adopted to promote the development of generative artificial intelligence systems with independent innovation capabilities. Second, combined with a data classification system, generative artificial intelligence systems should be developed to ensure compliant production. Third, it is important to achieve a legally compliant relationship structure and construct generative artificial intelligence systems with a clear allocation of rights and responsibilities. Fourth, it is necessary to seek overarching principles and design generative artificial intelligence systems that adhere to ethical standards. Additionally, complementary regulatory frameworks need to be established. Legislative bodies should fulfill the duty of risk prevention in advance, law enforcement agencies should bear the responsibility of eliminating infringements during implementation, and judicial authorities should assume the obligation of providing remedies for rights violations.

Key words: digital government; artificial intelligence models; data sovereignty; allocation of rights and responsibilities; Digital China

(责任编辑 彭建国)