生成式AI嵌入数字政府建设的审思与展望

——基于强人工智能视域

张　娟

（中国政法大学 商学院，北京　100088）

摘　要：生成式AI的引入与新时期我国数字政府建设的协同高效需求高度契合，这使数字政府建设脱离了对强人工智能时代的想象，走向全面的初级场景构建阶段。生成式AI嵌入数字政府建设能够大幅增强数字政府结构的协同性、提升数字政务服务的亲民性、提高公共治理的科学性。通过价值上的审思可以发现，生成式AI嵌入数字政府建设也伴随着国家数据主权安全风险、个人信息安全风险、资本侵蚀风险和资本同化风险。因此，为了推动技术理性与价值理性相合，应加强技术合规建设以维护国家数据主权安全，引入多部门协同配合以增强个人信息安全，规制资本行为以提高公共治理福祉，从而对生成式AI嵌入数字政府建设进行智能补强。

关键词：生成式AI；数字政府；数据主权；技术理性；价值理性

中图分类号：F49；TP18；D63　　**文献标识码：**A　　**文章编号：**1000-176X（2024）07-0036-12

一、问题的提出

随着数字技术的不断发展，我国已经逐步进入强人工智能时代。相比弱人工智能，强人工智能的自主学习能力、人机交互能力和数据处理能力大幅增强，技术赋能的效果也实现了质的提升。目前，生成式AI作为一种新技术，它具有GPT所要求的广泛适用性、发展性和生成开创性等特征[1]，从而被认为是强人工智能的初级形态。依靠其自身强大的技术逻辑和算力算法，生成式AI能够为数字政府建设的输入和输出过程提供数字化、信息化和协同化等方面的工具助力，从而形成协同高效的数字政府智能形式。《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》就目前如何进一步提升数字政府建设水平指出了三个重要方向，即推动政务信息化共建共用、提高数字化政务服务效能和加强公共数据开放共享。上述三个重要方向分别体现了数字政府建设的三个重要领域，即政府内部之间的决策支持、政府向公众提供的政务服务和政府为增进公众福祉进行的公共治理。因此，从生成式AI嵌入数字政府建设的应用场景、现实效能等角度展开，分析数字政府的强人工智能雏形及其可能产生的风险，是研究我国数字政府建设推进的必要命题。

收稿日期：2024-05-06

作者简介：张　娟（1986–），女，河北石家庄人，博士研究生，主要从事创业就业和创新经济研究。E-mail：zhangjuan2024@126.com

从现有研究来看，我国学者在研究生成式AI嵌入数字政府建设时，相应的讨论范式和研究进路较为单一，大多尝试通过实践、风险和规制的思路（或类似思路），从生成式AI在数字政府领域的探索应用出发，提出生成式AI对数字政府的内生性优化效能，分析存在的数据安全、虚假信息和隐私侵犯等风险，从而期望通过技术完善、数据监管和权利保障等形成全面的完善路径[2-6]。一部分研究以生成式AI为基础构建GovGPT，形成政府服务的无人化、自动化和虚拟化等特征[7]；通过以“大数据分析+可视化展示”为特点的生成式AI技术，以交互式的可视化平台展示成果，为政府决策提供科学依据[8]；建议通过以人民为中心的基础、以效率为优化的要点，建设聚焦自动决策与智慧决策的数字政府[9]。另一部分研究分析了生成式AI嵌入数字政府建设的利弊。就优势而言，生成式AI不仅可以提升数字政府的内部性能，而且能够优化外部行政行为，最终促成行政机关与公民的紧密互动。相关的风险包括数字政府建设存在的数据主权安全风险、技术资本异化风险和信息秩序失稳风险[10]。目前，鲜有研究从技术性质视角出发，结合数字政府建设的重点领域进行透视，或基于我国目前数字政府建设新时期的新需求展开分析和论证。

不同于现有研究，本文从数字政府建设的三个重要领域（即决策支持、政务服务和公共治理）出发，首先，分析生成式AI嵌入数字政府建设后所形成的强人工智能雏形的具体形态，从而说明生成式AI嵌入数字政府建设的功能价值。其次，根据数字政府建设新时期的协同高效目标进行价值审思，分析生成式AI嵌入数字政府建设时，由于人文理性尚未完全融入而导致的“高效”已成但“协同”目标尚未达到的现状所蕴含的风险。最后，基于价值审思分析得出的多角度技术限制问题，提出针对性的智能补强方案，从而真正实现强人工智能与数字政府的良性互动。

二、技术赋能：生成式AI嵌入数字政府建设的功能价值

作为强人工智能的典型代表，生成式AI嵌入数字政府建设能够大幅增强数字政府结构的协同性、提升数字政务服务的亲民性、提高公共治理的科学性，在提升政府自身管理水平的同时，加强政府与公众的良性互动，为优化数字政府建设生态提供契机。

（一）增强数字政府结构的协同性

在信息技术嵌入某一系统的过程中，若追求其正向效用则一般需要经历“技术联结—信息驱动—结构再造”的流程[11]，这一技术应用流程同时适用于信息技术嵌入政府治理的过程中，在政府的治理结构、治理方式和治理效能等方面推动政府的信息化和数字化转型。

第一，生成式AI强化了数字政府的信息协同。在数字政府运行中，信息和数据是其中的枢纽，也是联结政府各部门、实现各部门之间有效沟通协商的桥梁。在以往的政府运行中，由于科层体制和信息化建设的不足，政府各部门之间的沟通协商存在信息壁垒，导致各部门在诸多治理问题上无法达成一致。生成式AI的应用有助于打破繁复体制和信息壁垒的掣肘，促进信息和数据在智能系统之间的相互流动。此外，政府各部门还可以通过智能系统实时分享治理信息，向生成式AI输入部门的诉求和意见，借助其深度交互系统的特点整合分散的治理资源，实现数字政府的信息协同。

第二，生成式AI重塑了数字政府的组织协同。在长期的政府治理实践探索下，我国形成了政府治理的“条块”模式，这种上下有序、部门分工的行政治理模式不仅有利于发挥各部门的专长，也有利于上下级之间的事权划分。但是，“条块”模式也逐渐暴露出各部门之间信息沟通不足、部门利益冲突严重等问题。在数字时代，政府治理事项的“非条块”特性愈发明显，仅靠单一部门的专业性治理已经无法满足目前的社会治理需求，因而需要改变以往“专业化—部门化—利益化”的格局，提升政府治理效能。生成式AI在数据收集、处理和共享等方面将助力改进科

层体制下高度分工的部门主义，增强政府各部门之间的协同性和联动性。

第三，生成式AI增强了数字政府的技术协同。在技术应用与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[5]。相较于目前运用于数字政府建设的人工智能系统，生成式AI更多地整合了云计算、大数据和物联网等技术，依托“云+网+端”的基础设施、互联互通的数据资源和高效协同的业务应用[12]，显著增强了数字政府的技术联结能力。此外，生成式AI强大的自主学习能力和自主生成能力，能够将此种联结以文字、视频和图片等多模态形式生动展现。以往的AI技术无法通过高度交互的场景给予行政相对人具身化的参与感受，其运行路径相对固定、机械，行政相对人对于人工智能系统的数据、资源和知识整合能力整体体验感不强。就生成式AI而言，从内部结构来看，其作为强人工智能的初级形态拥有强大的技术算法基础；从外部表现来看，其拥有强大的交互式沟通对话能力，内外两方面互相成就的技术系统能够极大程度地匹配数字政府的运行逻辑。

（二）提升数字政务服务的亲民性

人机交互系统的建设和完善是强化行政机关与行政相对人之间交互性的重要保障，对政务服务协同高效的实现具有重要意义。在人机交互方式的完善过程中，便于公众理解和感知是技术得以应用于数字政府建设的前提条件。尽管我国数字政府建设目前已经实现了从“对话智能体”（Conversational Intelligently Agent）到“涉身对话智能”（Embodied Conversational Agent）的技术转型，但距离实现人机流畅对话的终极目标仍存在一定距离。从表面来看，物联网、人工智能算法等新兴技术的出现革新了社会公众的生产方式和生活方式；但从实质来看，新兴技术的应用效能是否完全符合社会公众的实际需求有待商榷。根据《2020下半年中国地方政府数据开放报告》，数字政府的平台亲民性不足，只有22%的数字平台具有无障碍浏览、语言翻译和沟通对话等包容性功能。这尤其体现在政府向公众提供公共服务的智能系统的应用上，当行政相对人寻求诸如户籍、税务等公共服务时，智能系统多数情况下采取由行政机关向行政相对人的单向信息传输方式，智能系统只能在接收到预设关键词后才能作出相应反馈，人机交互的对话内容仅限于程式性语言，既有的智能系统无法有针对性地、具象化地解决行政相对人的全部实际需求，仍需要政府工作人员具体解决。

基于生成式AI的深度交互性和强大的自主学习能力，生成式AI能有效提升人机交互的亲民性，具体体现为：首先，强化智能系统的沟通交流。生成式AI与传统的AI设计体系相比，能够基于预训练数据库，依据标注数据自动生成并处理包括语言翻译、沟通对话和文本摘要等在内的任务类型，生成拟人化的文本数据并以对话形式呈现给用户，并依托强大的上下文关联能力，增强行政相对人的具身化体验。生成式AI采用的模型使用了“人类反馈强化学习（Reinforcement Learning from Human Feedback，简称RLHF）”的训练方式，能够通过预设的打分模型对原始模型进行反复训练，根据提示词内容生成标准模型，输出符合用户需求的智能化内容。其次，提高沟通语言的艺术性。相比于冰冷的信息传达，生成式AI能够充分考虑行政相对人的需要，模拟人类语言行为，与用户进行自然交互，其语言组织能力、文本水平和逻辑能力可以让人获得极大的满足感。生成式AI在算法生成和运行过程中可以结合情景学习方法，在保证数据的有用性、真实性和无害性的同时，最大程度地强调人类情感的拟合，促进生成式AI技术表现的“拟人化”。最后，加强沟通对话的对称性。在传统行政行为语境下，政府与公众之间面对面的物理交互往往使得政府工作人员和行政相对人感到力不从心，尤其是对行政相对人而言，在寻求行政服务时难免需要面对责任推诿、程序繁杂和服务敷衍等问题。生成式AI作为智能对话系统，有助于打破僵硬的传统行政模式，将政府与公众保持在“安全社交距离”中从而进行平等对话，具体体现为信息的公开透明、对话的平等亲和，以期实现行政信息的公开，并遵循公正、公平原则，提升政府的服务效能和治理水平。

（三）提高公共治理的科学性

生成式AI嵌入数字政府建设不仅深刻改变了政府的治理结构和治理方式，还在具体的公共治理活动中对政府行为产生深远影响。

第一，生成式AI有助于增强公共治理的公正性。无论是政府的具体行政行为还是抽象行政行为，在作出行政决策时都可能被相关利益主体所“俘获”[3]，从而影响公共治理的公正性。在行政治理中，这些不公平现象又有可能被各种表象掩盖，从而阻碍公众和利益相关方提出异议。生成式AI对于数据的收集和分析能力有助于增强公共治理的公正性，通过对数据的客观分析，排除可能影响公共治理公正性的人情、关系和偏见等因素，最大程度规避行政决策的主观性和随意性。这种客观性和数据驱动的决策过程，有助于确保政府在政策制定中尽量考虑到所有利益相关方的需求，从而增强公共治理的公正性。在各种行政决策中，与公共治理公正性密切相关的主要是与资源分配相关的行政决策。例如，在与资源分配相关的政策制定过程中，生成式AI可以通过分析大数据，提供客观的建议和预测，减少人为因素的介入。通过保证分配的公正进一步保证公共治理的公正性和决策过程的透明性。

第二，生成式AI有助于提升公共治理的精准度。提升政府治理效能，让公众在每一个政府行政决策中都感受到公平正义是我国政府职能转型的总体目标，以往由于信息收集的能力不足，导致政府行政决策往往只能顾及大多数人的利益，而这个大多数人又集中于城市和经济发达地区，忽略了农村和经济欠发达地区的公众诉求。生成式AI嵌入数字政府建设有助于提升公共治理的精准度，可以通过信息的收集和分析，形成个性化的“用户画像”，这个“用户画像”的主体不仅包括公众，还包括政府主体，通过预测相关主体的行为提升公共治理的精确度，提高相关主体对公共治理实用功能的期待。除此之外，生成式AI还可以在政府与公众之间搭建起沟通的桥梁。例如，智能客服系统可以利用生成式AI技术处理公众的咨询和投诉，接收农村和经济欠发达地区的公众诉求，快速响应关于类型化的公众意见，并及时记录公众反映的意见，由此为行政决策提供参考依据。在此过程中，生成式AI还可以通过自然语言处理和大数据分析，识别和分析社交媒体和其他在线平台上的公众舆论和反馈。这些分析结果可以帮助政府更好地理解公众的期望和需求，确保政策和决策能够更好地反映社会整体利益，重视农村和经济欠发达地区的公众诉求。

第三，生成式AI有助于提高政府治理效率。信息化建设程度深刻影响了政府治理效率，在政府行政决策中，往往在需要作出决策时才进行信息的收集行为，可能因为信息收集不及时、收集范围过窄等对具体行政相对人的切实利益造成影响。生成式AI嵌入数字政府建设有助于提升政府治理效率，如税务办理、市场监管和环境治理等政府行为，能够在持续不断的收集和分析数据过程中提升治理效率。当存在作出新决策的需求时，生成式AI不仅可以基于历史数据检索分析相关主体的偏好、行为，还能够基于数据分析预测其未来行为，为提升政府治理效率提供助力。除此之外，通过分析政府日常运行的人员需求和工作负载，生成式AI可以优化人员配置，进一步提高政府工作人员的工作效率和满意度。通过生成式AI的应用，相应的人力资源管理更加智能化，这不仅能够减少相关人力资源的浪费，还可以提升政府部门的整体执行能力和服务水平。

三、风险审思：生成式AI嵌入数字政府建设的多维挑战

从本质来看，生成式AI作为一项技术，在尚未通过规范的方式进行价值理性塑造的前提下，仍可能对数字政府建设造成诸多负外部性问题，如技术嵌入容易引发国家数据主权安全风险、技术依赖容易诱发个人信息安全风险、资本逐利易导致资本侵蚀风险和资本同化风险。

（一）技术嵌入容易引发国家数据主权安全风险

伴随着大数据与人工智能的快速发展，数据对于人类社会的重要性越来越大。不管是经济层面、社会层面，还是人们的日常生活，数据的参与度越来越高。对数据的占有和利用也成为各国之间博弈的关键，数据主权的概念也基于国家安全而产生。从主动的角度来看，国家掌握数据主权就能在网络秩序中掌握主动权，增强参与国际数据活动的活力，从而能够创造更大的经济价值、提供更加优质的网络服务。从被动的角度来看，国家若不能维护数据主权，其受到网络攻击的风险就越大，重要数据极有可能被泄露或滥用从而对国家安全产生巨大危害，这集中表现为三个维度：首先，数据滥用。生成式AI具有获取大量数据的能力，而这些数据可能被用于商业或其他目的，如果这些数据未经妥善保护而被滥用，数据主权将受到侵犯，数据主体对数据的控制权将被削弱，甚至威胁国家数据主权。其次，安全漏洞。生成式AI的敏感信息抓取特性可能导致安全漏洞的出现。如果安全措施不完善，黑客或恶意用户可能利用这些漏洞获取用户的敏感信息，造成数据泄露。针对生成式AI的敏感信息抓取特性，有关部门必须借助一定的技术手段进行制约。目前，已有数据脱敏、数据加密和用户自主性控制等技术机制，但面对生成式AI这一不断自我更新与学习的智能技术而言，对应的机制也需要不断强化才能够有效应对安全漏洞。最后，技术垄断。就技术垄断而言，其本质上是对技术壁垒的描述，但技术垄断上升为国家意志就会成为技术霸权[13]。如前所述，数据是重要的生产要素，美国等西方国家基于其掌握的先进计算机技术对相关领域实行了技术霸权。由于生成式AI的底层技术和训练数据受到特定实体或公司的控制和垄断，这些实体或公司在获取大量数据的同时也掌握和控制着这些数据的使用和流动。这将导致数据集中于少数实体，从而削弱其他国家或组织的数据主权。在技术垄断和技术霸权的壁垒下，不仅数据控制权会受到影响，对技术的依赖、竞争和创新的削弱也会限制数字政府建设的多样性和进步性。因此，在生成式AI嵌入数字政府建设中，需要认识到技术垄断和技术霸权的风险，通过自主掌握核心技术等强化自身的数据主权。

（二）技术依赖容易诱发个人信息安全风险

1.生成式AI过度收集数据

在数字政府建设中，生成式AI这一重大技术的嵌入对现代政府的治理具有重大意义，但生成式AI嵌入数字政府建设离不开对治理对象数据的收集。生成式AI作为大语言模型主要依靠对数据的学习提炼信息、预测趋势[14]，离开海量数据的支撑，生成式AI生成新内容的能力将会大打折扣。据报道，生成式AI与其他网络平台一样，在收集用户个人信息（包括个人隐私和敏感数据）时并未获得用户的同意。此外，由于自身的先进性，生成式AI还可以不受时间限制跨平台收集注册用户在其他网络平台的信息，依靠该公司收集的大量数据进行转型、升级和创新。资源积聚到一定程度就是权力集聚[15]，生成式AI嵌入数字政府建设将会辅助政府治理，导致政府掌握的治理对象数据的大幅增长。

2.生成式AI过度整合数据

数据整合是指通过特定的数据转换、数据推理和数据模拟技术，将收集到的零散海量数据资源转换为具有一定内在规律和逻辑的数据的处理机制[16]。由此可见，数据整合是为后续的信息存储和使用工作进行准备的处理机制。生成式AI内嵌的算法技术对数据整合的处理极其专业，这从生成式AI生成的内容就可以看出，具有针对性和逻辑性的文本内容体现了生成式AI能够准确、高效地处理海量数据资源。因此，在近端策略优化（Proximal Policy Optimization，简称PPO）算法的强力支撑下，生成式AI的数据整合优势能够有效提升数字政府的智慧性[16]。与此同时，生成式AI无法避免的算法黑箱会导致在数字政府建设中，该模型背后的控制者为了经济利益而违背数字政府建设的公共管理目标，在数字政府和治理对象缺乏相关算法知识的情况下，控制者将数据整合转作他用——毕竟生成式AI是由资本控制，而资本的本质在于追逐利益最大化。算

法黑箱的存在使得作为治理对象的个人和数字政府在表面上可以感知模型算法的客观运行，但对其根本的运行机理和内部程序不甚了解[17]。在这种情况下，数字政府偏离了原本的建设初衷，而治理对象数据被过度加工、得不到有效保护。

3.生成式AI过度存储数据

经过对治理对象数据的生产和加工后，便进入了存储治理对象数据的环节。在这一环节中，会产生两个方面的数据持有或存储风险。首先，未经治理对象知情同意存储信息。目前，从生成式AI所属公司和用户签署的使用政策或隐私保护政策来看，并未有政策条款明确用户个人具备检查其留存于模型上的个人信息，更不用说将生成式AI用来保存用户个人信息的数据库公开以供社会检查。此外，为绝对保护生成式AI所存储的治理对象数据，相关公司拟定了对自身具有优势的信息使用条款——对用户个人信息存储保护和修复未作出任何说明。其次，治理对象数据无限期存储风险。根据《中华人民共和国个人信息保护法》第19条，除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。因此，数据存储行为存在着限制之说[18]。从生成式AI用户使用条款来看，未有关于数据存储的期限规定，这就表明开发公司可以借助政策的漏洞，即类似于“法无禁止即可为”，进而永久地保存用户留存于模型上的信息，查看、保存用户在其他网络平台上的信息。借助于技术优势，生成式AI在信息存储成本低廉的情况下，将会无限期地存储用户个人信息。生成式AI作为由外国资本控制的技术，我国数字政府建设借助其进行现代化治理时，必须对其无限期存储治理对象数据的行为进行监管。政府数据的管理属性和价值属性与国家数据主权安全密切相关[19]，因而必须警惕永久保存公民个人信息所引发的数据安全风险。

（三）资本逐利容易导致资本侵蚀风险和资本同化风险

1.生成式AI蕴含资本侵蚀风险

马克思认为，资本不是一种物，而是一种以物为中介的人和人之间的社会关系[20]。生成式AI是人工智能技术（也属于资本）的产物，其所具有的“类人”化特征正是资本入侵技术所期望看到的现象[21]。科学技术的发展带来了巨大的价值，但资本入驻技术所带来的科技伦理风险是人类所不能承受的。生成式AI在促进科技创新、经济增长的同时，也引发了技术异化带来的伦理问题。例如，生成式AI在文本生成上的优势吸引了大量的人群，这其中不乏学生群体。学生利用生成式AI最为准确的文本撰写功能进行论文写作，这显然与教育的理念相悖，许多学校和机构因此禁止使用其进行文本创作。但是，资本面对巨大的流量和广阔的发展前景必然会不断地侵蚀这一技术以获得更为巨大的利益。总之，生成式AI投入聊天时的低成本优势和商业公司不断追加的数十亿美元投资直接将生成式AI推进国内外各类资本的视线中，各类生成式AI的广阔商用前景不断推高资本侵蚀技术的风险。在生成式AI嵌入数字政府建设中，资本入驻技术与数字政府公共治理的理念相悖，将政府治理效果引导至资本利益想要发展的方向上。

2.生成式AI蕴含资本同化风险

生成式AI作为一项新技术，无论是企业、组织还是个人，都希望通过学习、引入、融合或创新等方式，将生成式AI这一外部技术资源转化为自身内部的生产力和竞争优势，由此产生了资本同化的现象。在资本同化的过程中，涉及知识产权保护，技术的转让、研发和应用等多方面。生成式AI作为大型聊天机器人可以提供多样的产品和服务，其文本生成服务深受广大用户的青睐。生成式AI所撰写的文本依托于海量数据资源，加之其特有的“类人”创造力，生成的文本内容富有文采且符合客观逻辑，因而实践中产生了生成式AI是否对其生成的文本内容具有所有权，是否受著作权保护等问题。有学者认为，生成式AI生成的内容具有独创性，应受著作权保护[22]。这是生成式AI资本同化导致的知识产权风险：用户应用生成式AI生成文本的本意是服务于自身的使用，但资本的介入使得知识产权的保护和合规性成为了难点，从而加大了资本同

化的风险。

四、进路展望：生成式AI嵌入数字政府建设的智能补强

如上所述，生成式AI嵌入数字政府建设能够实现理论上的强人工智能雏形，但由于技术理性尚未附加价值理性，此种理论上的强人工智能雏形在实践中受到各方面的掣肘。若将理论形态转化成实践效能，需要针对上述局限进行不同程度的智能补强。

（一）加强技术合规建设以维护国家数据主权安全

1.通过规范构建遏制霸权倾向

数字技术已经成为国家数据主权竞争秩序和数据安全维护效果的基本保障。在数字政府建设中，国家不仅是生成式AI的技术应用者，还是生成式AI的技术监管者，且后者往往直接决定了国家数据主权的安全性。鉴于生成式AI的应用前景和数字治理的发展进程，有必要完善生成式AI的应用体系从而为其规范发展制定合理的制度边界。

其一，应保证既有规范的体系性、协调性。为规范生成式AI的开发应用，保护国家数据主权安全、个人信息安全，2022年11月25日，国家互联网信息办公室、工业和信息化部、公安部联合发布了《互联网信息服务深度合成管理规定》，从概括性规定、数据和技术管理规范、监督检查与法律责任等维度对深度合成服务提供者的义务和责任进行了明确规定。2023年7月13日，国家互联网信息办公室等七部门联合发布了《生成式人工智能服务管理暂行办法》，从内涵界定、主体责任和应用程序等方面对生成式AI的应用体系进行了具体界定。同时，还应注意上述规范内容与已经公布实施的规范文件的衔接与贯通。在上述规范的具体落实过程中，对于规范漏洞和规范空白可以参考适用《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《数据出境安全评估办法》《互联网信息服务算法推荐管理规定》等相关规定；对于规范冲突可以依照法的效力层级理论进行具体分析。

其二，应探索制定新的规范文件和条例细则。系统化的法律文件要求法律规范内容具有相对完备性和高度适用性。为保证既有的规范性文件得以完全贯彻落实，应完善《生成式人工智能服务管理暂行办法》《互联网信息服务深度合成管理规定》等规范文件适用的程序机制和内容解释细则，从实体内容和程序方法等角度完善生成式AI的应用规则，以免上述规范性文件陷入难以落实的窘境。

2.通过分类分级限制信息处理

在信息时代，数据既是数字技术作用的主要对象，又是数字政府建设的基础资源，也是生成式AI嵌入数字政府建设要运用的关键要素。为了充分发挥生成式AI在数字政府建设中的积极作用，需要界定其发挥作用的空间或领域——数据对象的类型、多少、大小和内容范围。数据的分类分级管理是对数据全流程、全过程进行保障的基础[21]。在科学、合理、有效的分类分级管理基础上，才能够以最低的数据风险成本达到最高的数据建设成效。2022年12月出台的《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》强调，探索建立数据产权制度，推进公共数据、企业数据和个人数据的分类分级确权授权使用，这不仅对于数据经济效益发掘具有重要意义，也说明数据可运用于其他领域。当然，从数据本身来看，不同类型的数据，其权益主体、权益内容和权益保护等方面均呈现出特殊性[22]。只有对数据形成一种体系化的分类分级利用标准才能节约成本、提高效率。

作为顶层设计，对于生成式AI数据的分类分级应坚持一些基本原则。可参考基础电信企业的数据分类分级原则，如安全性原则、稳定性原则、可执行原则和时效性原则等[22]，还要结合数字政府政务运行的实际情况确定相应的原则。首先，安全性原则。并非所有数据都能利用生成式AI进行处理，涉及国家安全、重要行业和重点产业的敏感数据应被排除在外，并根据敏感程

度、安全程度进行分级。相关的原则还有就高不就低原则，涉及多层级的数据应该归为高敏感层级；关联叠加效应原则，虽然刚开始层级较低，但处理之后层级变高的数据应重新归类。其次，可执行原则。为保障可操作性，分类分级原则应贴近政府实际情况，不应过于复杂或过于粗犷。例如，可根据政府级别划分数据管理权限，有技术、有条件的政府可处理多类别多层级的数据；还可根据行政机关主管业务划分数据类别。最后，完整性原则。数据在数字政府的运行过程中呈现不同的状态，可从输入、处理和输出这三个阶段确定数据状态，并进行不同的类别划分。最关键的是，这些基本原则应体现在相关规范的内容之中，应体现在落实生成式AI嵌入数字政府建设的实践之中。例如，各地区、各部门可以根据数据分类分级原则进行政策或法律、法规的制定，确定本地区、本部门和相关行业、领域的数据分类分级实施细则或具体目录[23]，方便进行实务操作。

（二）多部门协同配合以增强个人信息安全

生成式AI嵌入数字政府建设的制度架构侧重于从抽象性、方向性和原则性维度对生成式AI参与行政治理活动进行规制。在此基础上，若要在“知情同意—类别划分”的规范性框架内完善生成式AI处理数据的制度约束，在“他律—自律”的逻辑闭环内建构个人信息保障机制，则有必要在异质化的治理空间中通过明确不同主体的保障义务进行具体展开。如前所述，生成式AI嵌入数字政府建设时会对数据主权、数据安全和信息秩序产生负向影响，政府公共权力行使与公民个人信息权利保护之间的关系陷入失调状态。从宪法基本权利的教义学角度来看，将个人信息受保护权视为基本权利的观点，具有坚实的宪法规范基础；从主观权利和客观法维度来看，国家对其具有消极和积极保护义务[24]。因此，需要立法机关、执法机关与司法机关协调配合，以完善生成式AI嵌入数字政府建设的保障机制。

1.通过立法规制实现风险预防

在基本权利的功能体系中，主观防御权以排除国家的不当限制、防御国家的侵害为内容，个人可以据此请求排除国家对其基本权利的不当侵害[25]。但是，随着风险社会的到来，由此增加的人为风险不同于自然风险，其与人类的实践活动和决策行为相伴而生，包含技术风险和制度风险[26]。在此视域下，基本权利的主观防御权功能无法全方位地保障个人基本权利的充分实现，因而应引入国家保护义务理论，从而延伸基本权利作为“请求权体系”的内涵与外延，为国家以积极的方式保障个人基本权利的充分实现提供坚实的理论支撑。风险预防义务是对国家保护义务的拓展和延伸[27]。申言之，生成式AI自身的技术逻辑和算法构造加剧了数字政府建设的算法风险和制度风险，对数据主权、数据治理和数据安全造成极大挑战。同时，国家保护义务的实现离不开完备的法律规范体系，需要立法机关从立法层面落实风险预防责任。

其一，立法机关要将风险预防义务予以具体化展开。在生成式AI嵌入数字政府建设中，要着重强调构建个人信息受保护权的国家保护义务体系。一方面，立法机关要注重对于法益侵害风险源的规范规制。在个人信息受保护权的功能体系建构过程中，立法机关要不断完善以《中华人民共和国个人信息保护法》为中心，以《中华人民共和国数据安全法》《中华人民共和国网络安全法》等法律规范为补充的法律法规体系，从源头切断生成式AI侵害个人数据权利的运行路径。另一方面，立法机关要注重对于权利主体的规范保护。“知情—同意”原则是个人数据权利得以规范化利用的合法性基础[28]。在告知程序上，要实现“知情—同意”原则的明示化，避免以默示方式或行为推定模糊个人信息收集使用的权限，有效防止该原则陷入僵尸条款的窘境；在告知内容上，要在前述数据分类分级保护的基础上，对数据收集主体、数据收集方式和目的、信息内容、第三方参与等进行规范化、明确化设定，不得强制公民、个人对数据收集和使用等表达同意。

其二，立法机关要完善风险预防义务的合宪性论证。虽然风险预防义务是国家保护义务的概

念性拓展，在其落实过程中，国家机关不得以任何方式增加公民的义务或减损公民的权利。在生成式AI嵌入数字政府建设中，对于数字政府基于法定职责和公共利益应对突发公共卫生事件等处理个人信息的行为，立法机关应严格论证其合宪性，对上述行为进行严格限制以保护个人数据权利的规范性使用。

2.通过执法监督落实保护职责

在个人信息受保护权的基本权利体系中，国家防御权的功能体现为行政机关的排除侵害请求权功能。在生成式AI嵌入数字政府建设中，行政机关由于自身的技术弱势地位，往往采取政企合作的方式构建算法行政治理体系。又由于行政机关的公权力属性，其在数字政府建设中便兼具参与者和监管者的双重角色。在排除侵害请求权功能实现的过程中，行政机关更多的是以监管者的角色对生成式AI的应用场域和运行路径进行全方位动态监管。在生成式AI嵌入数字政府建设中，要从行政责任和合规监管对生成式AI衍生的算法风险和伦理风险进行规制。一方面，行政机关要科学化、规范化地启用行政处罚机制，有效惩戒生成式AI嵌入数字政府建设中的侵犯行为。《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《互联网信息服务算法推荐管理规定》等法律法规在法律责任章节规定，主管行政机关可以采取停业整顿、吊销营业执照或许可证、没收违法所得等行政处罚措施，保护国家数据主权和个人信息安全。另一方面，行政机关要加强对生成式AI的算法提供主体的合规管理体系的行政监管。行政机关应依据依法行政原则、比例原则和程序正当原则展开对算法服务提供主体的合规监管，以期有效排除对个人数据权利的不当侵害。同时，应探索建立相对完善的行政内部和外部救济路径，防止因行政权力的过度干预而制约算法服务提供主体发展的系统性风险[29]。

3.通过司法供给兜底权利救济

在数字社会中，自由、平等、民主，以及法律、秩序和正义都将被重新定义，数字正义将是更高的正义[30]。在数字时代，个人数据权利的实现和保障是司法机关的重要时代议题，司法救济是保障个人数据权利的强有力机制和最后防线。因此，要从司法环节强化对个人数据权利的公力救济。一方面，要强化保障个人数据权利的司法供给。在生成式AI侵害行政相对人数据权利的案件中，司法机关要适当向处于技术弱势地位的公民倾斜。在生成式AI嵌入数字政府建设中，数字平台技术服务提供者拥有强大的技术优势和人才资源，行政机关基于其公权力属性也属于拥有便利数字技术资源的主体，部分公众由于数字素养差异在个人数据权利被侵害的案件中时常处于弱势地位。此时，司法机关应在立案、法庭调查和证据交换等环节强化对数字弱势群体的保护，基于释明权保障数字弱势群体的诉讼权利，适用举证责任倒置或严格责任原则等内容平衡诉讼主体的责任。另一方面，可以尝试建立惩罚性赔偿机制。在数据类别划分的规范框架下，对于高度涉密的数据应采取更为严格的保护策略。在生成式AI嵌入数字政府建设中，对于严重侵害国家数据主权和个人信息安全的行为，可以适当采取惩罚性赔偿机制加大对于相关侵害行为的惩戒力度，以发挥司法的警示性作用。

（三）规制资本行为以提高公共治理福祉

1.通过模型审查抵御资本侵蚀

要发挥生成式AI的积极作用，抑制其可能带来的风险，关键还在于对生成式AI本身的审查和追责。首先，应完善对生成式AI应用的审查机制。尤其是要严格审查生成式AI的数据源头，网络中虚假、编造、伪造数据的存在影响着生成式AI的输出结果，还可能被有心之人利用，通过将歪曲、伪造的虚假数据大规模地“喂给”生成式AI达到蛊惑人心的目的。为防止可能出现的侵害个人隐私、破坏社会伦理道德、制造政治偏见和种族主义混乱等现象，必须以严格的数据审查和清洗对数据源头进行把关，防止资本推手的过度发力[29]。其次，应完善对生成式AI应用的追责机制。责任和权力同时存在，这不仅适用于政府，更适用于生成式AI。当政府与生成式

AI结合在一起时，这其中的管理边界和管理措施，尤其是责任边界和追责机制就必须加以明确从而显示政府对公众的负责。关键在于要回答：政府部门及其工作人员在运用生成式AI的过程中是否能分清彼此的责任承担。例如，因学习机制强化而放大既有偏见，从而导致歧视问题[30]。由于政府只是名义上的法律主体，生成式AI缺乏法律主体资格，因而最终责任可能还是要归于个人——政府工作人员、企业负责人和其他相关人员。这就要求政府工作人员在运用生成式AI和企业人员在设计生成式AI的过程中应时刻注意履行自己的审查、纠错职责，尽到应尽的注意义务。最后，生成式AI审查和追责机制的建立要求政府具有更高的管理水平。就数据源头审查生成式AI应用和设计中的注意义务而言，不论是对生成式AI的算法审查，还是通过生成式AI的回答进行验证和判断，都要求政府工作人员需具备更高的专业知识和素养，以减少错误和偏差，降低简单、机械性应用可能带来的风险。企业的创新能力总会保持提升、生成式AI将会持续更新，政府工作人员的素养能力需要不断地与时俱进[31]。此外，政府必须注意数字化人才的培养，提高数字化管理水平。

2.通过主体责任防止资本同化

数字时代的到来、人工智能的兴起，叠加着快速发展的算力，生成式AI嵌入数字政府建设更是面临着严峻的科技伦理挑战。生成式AI嵌入数字政府建设可能存在数据安全和隐私保护、消费者权益和公平保障、数据深度合成治理等问题，都会影响政府治理效率。上文提出的规范体系、分类分级原则、审查和追责机制均是为了解决这些问题，并且属于政府应担负的责任。同时，作为生成式AI的提供者，部分管理义务和责任也最终将落实到企业层面。首先，企业作为提供者，其主体责任也应贯穿于数字政府治理全过程，应采取技术措施对数据进行分类分级利用和保护。例如，通过物理隔离、病毒防护、加密脱敏、身份甄别和数据备份等技术手段，辅之相应的数据管理制度和业务操作规范，防止相关风险的发生。此外，针对不同类型、不同级别的数据，相关主体也可采用不同等级的安全防护措施[2]。其次，在对于生成式AI数据的商业化利用过程中，应做好国家利益、社会公共利益和用户个人利益之间的平衡。在类别划分数据管理制度之下，根据个人信息权益保护、数据追溯和共享机制、数据管辖标准的法律框架开展企业数据业务[32]，达到数据合规要求。最后，促进算法责任分配标准的形成。由于以生成式AI为主导生成的内容和行为具有交互性，算法和源代码可能来自并非营利的开源提供者，这些开源提供者往往利用大规模互联网数据参与生成式AI运作，其运作结果便可能与多个设计者、多家企业发生牵连关系，一旦出现算法偏差或决策失误，责任分担就成为一个复杂的问题。对此，可通过区块链的技术方法追踪模型生成过程，也可通过市场化的运作方式让各方自愿平等协商达成责任分担的协议，以促进最终算法责任分配标准的形成。

五、结　语

在新兴技术极速发展的背景下，关于生产式AI如何积极介入社会治理的讨论日益增多。目前，相关的论争和尝试多因传统路径的桎梏而成效不明。具体到生成式AI，其在介入社会发展的过程中，需要始终沿着尝试与修正的循环而不断地进行有益实践。生成式AI相较于其他的人工智能技术来说，其可视化、交互性和可得性等方面均有所提升，对现实生活的影响超越了其他技术，也让社会看到数字政府建设步入强人工智能时代的可能。但是，在重视工具理性从而将技术运用到数字政府建设的同时，应强调价值理性的注入，一方面，通过法律持续输出安全优先的方案，将伦理原则落到实处，减少技术的无序发展和危险利用。另一方面，法律也应细化风险项，通过法律责任分配等措施将风险消解于各个主体的能力范围之内，从而保证技术发展流程在可控的范围内自由发展。通过上述途径，方能同时将技术理性和价值理性注入运用生成式AI的数字政府建设之中，从而真正将数字政府的建设嵌入我国社会主义现代化建设的实践之中。

参考文献：

[1] 陈永伟.作为GPT的GPT——新一代人工智能的机遇与挑战[J].财经问题研究,2023(6):41-58.

[2] 张洪雷.生成式人工智能参与数字政府建设的技术跃迁、目标导向与可行路径[J].南昌大学学报(人文社会科学版),2023(4):100-109.

[3] 刘玮.ChatGPT类生成式人工智能嵌入数字政府建设:可供、限制与优化——基于技术可供性视角[J].情报理论与实践,2023(10):69-76.

[4] 曾宇航,史军.政府治理中的生成式人工智能:逻辑理路与风险规制[J].中国行政管理,2023(9):90-95.

[5] 董超,王晓冬.生成式人工智能在数字政府建设中的探索、挑战及建议[J].数字经济,2023(11):36-39.

[6] 房娇娇,高天书.生成式人工智能辅助行政决策的算法隐患及其治理路径[J].湖湘论坛,2024(1):99-111.

[7] 郭少飞.通用人工智能语境下智能法律行为的定位与效力探析[J].东方法学,2023(5):82-93.

[8] 龙柯宇.生成式人工智能应用失范的法律规制研究——以ChatGPT和社交机器人为视角[J].东方法学,2023(4):44-55.

[9] 马亮.新一代人工智能技术赋能国家治理现代化的前景分析[J].国家治理,2024(1):29-33.

[10] 张佳琳.ChatGPT模型辅助数字政府建设的风险及其法律规制[J].内蒙古社会科学,2024(1):65-75.

[11] 汪波,牛朝文.从ChatGPT到GovGPT:生成式人工智能驱动的政务服务生态系统构建[J].电子政务,2023(9):25-38.

[12] 庞洋.生成式人工智能嵌入数字政府建设的系统性分析[J].学术交流,2023(8):148-162.

[13] 包帅.对ChatGPT的一个历史唯物主义反思[J].浙江学刊,2023(4):178-184.

[14] 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.

[15] 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.

[16] 李盛竹.跨国公司国际竞争背景中的技术霸权现象——理论回顾与展望[J].社会科学家,2011(9):106-108.

[17] 蔡翠红.大变局时代的技术霸权与"超级权力"悖论[J].学术前沿,2019(7):17-31.

[18] 姜英华.数字时代资本意向、技术加持与劳动异化的政治经济学分析[J].北京社会科学,2022(10):4-13.

[19] 陈永伟.超越ChatGPT:生成式AI的机遇、风险与挑战[J].山东大学学报(哲学社会科学版),2023(3):127-143.

[20] 马克思,恩格斯.马克思恩格斯文集:第5卷[M].北京:人民出版社,2009:877-878.

[21] 张峰,于乐,马禹昇,等.数据安全分类分级研究与实践[J].信息通信技术与政策,2021,47(8):45-50.

[22] 李健男,高宁宁.企业公开数据权益保护的复合路径——基于数据形态进化的可能选择[J].北京行政学院学报,2023(2):96-108.

[23] 程啸.论数据安全保护义务[J].比较法研究,2023(2):60-73.

[24] 王锡锌,彭錞.个人信息保护法律体系的宪法基础[J].清华法学,2021,15(3):6-24.

[25] 张翔.基本权利的体系思维[J].清华法学,2012(4):12-36.

[26] 刘水林.风险社会大规模损害责任法的范式重构——从侵权赔偿到成本分担[J].法学研究,2014(3):109-129.

[27] 田野.风险作为损害:大数据时代侵权"损害"概念的革新[J].政治与法律,2021(10):25-39.

[28] 郑佳宁.知情同意原则在信息采集中的适用与规则构建[J].东方法学,2020(2):198-208.

[29] 赵阳.行政合规整改嵌入监管体系的路径及制度保障[J].西南政法大学学报,2023,25(2):154-166.

[30] 周强.深入学习贯彻党的十九届四中全会精神 不断推进审判体系和审判能力现代化[J].人民司法,2020(1):4-8.

[31] 杜洁.生成式人工智能赋能基层政务服务:技术嵌入、角色重塑与实践路径[J].兰州文理学院学报(社会科学版),2024,40(2):113-118.

[32] 林伟,周耀铭.国内外数据治理研究述评[J].数字图书馆论坛,2022(6):65-72.

Review and Outlook on Generative AI Embedding Into Digital Government Construction: From the Perspective of Strong AI

ZHANG Juan

(Business School, China University of Political Science and Law, Beijing 100088, China)

Summary: With the development of digital technologies, China has gradually entered the era of strong AI. The emergence of a new generation of generative AI interactive software is considered as the primary form of strong AI. The introduction of generative AI is highly compatible with the demand for "synergy and efficiency" in the new period of China's digital government construction, which makes the digital government construction move towards the stage of comprehensive primary scene construction. From the perspectives of application scenarios and the actual effectiveness of generative AI embedded in digital government construction, this paper analyzes how to present the prototype of strong AI in digital government and the possible risks associated with it, which is a feasible and necessary proposition for the promotion of China's digital government construction.

This paper finds that embedding generative AI into digital government can significantly enhance the synergy of government structure, the scientificity of the public governance system, and the accessibility of government services. However, the value analysis shows that the embedding of generative AI into digital government construction comes with national data sovereignty security risks, personal information security risks, and capital erosion and assimilation risks. Therefore, to promote the convergence of technical rationality and value rationality, technical compliance should be strengthened to safeguard data sovereignty and security, including curbing hegemonic tendency through normative construction and restricting information processing through class classification; multi-sectoral coordination should be strengthened to enhance personal information security, including the risk prevention through legislation and regulation, the implementation of protection responsibilities through law enforcement supervision, and rights relief through judicial provision; and capital interests should be regulated to enhance public governance welfare, including resisting capital erosion through model review and preventing capital assimilation through subject responsibility, so as to intelligently complement the construction of generative AI embedded in the digital government.

This paper emphasizes that while attaching importance to instrumental rationality and thus applying technology to the construction of digital government, we should pay attention to the injection of value rationality. On the other hand, the law should also refine the risk items and eliminate risks within the ability of each subject through responsibility and other standardized tools, so as to ensure that the process of technological development develops freely within a controlled range. Only through the above ways can technical rationality and value rationality be injected into the construction of digital government using generative AI at the same time, thus truly embedding digital government into the practice of socialist modernization in China.

Key words: generative AI; digital government; data sovereignty; technical rationality; value rationality

（责任编辑：尚培培）

[DOI]10.19654/j.cnki.cjwtyj.2024.07.003

[引用格式]张娟. 生成式AI嵌入数字政府建设的审思与展望——基于强人工智能视域[J]. 财经问题研究，2024（7）：36-47.