ChatGPT模型引入我国数字政府建设：功能、风险及其规制

周智博

摘要：数字政府建设关涉国家治理体系与治理能力现代化，面对ChatGPT模型这一重大技术性突破，切实发挥其在我国数字政府建设之中的作用具有重要意义。在数字政府建设中植入ChatGPT模型，必须厘清技术赋能、技术风险以及技术规制之间的逻辑关联。ChatGPT模型能够推动数字政府的亲民化、高效化和智能化发展，但同时也可能引发国家层面的数据主权安全风险、政府层面的行政公共性解构风险以及个人层面的数据权利侵犯风险。规范ChatGPT模型的技术应用，需要推动ChatGPT数据的分类分级，完善ChatGPT模型的责任链条，明确国家对公民数据权利的保护义务，强化国家对ChatGPT技术的引导与研发。

关键词：数字政府；ChatGPT模型；技术赋能；数据权

DOI：10.19836/j.cnki.37-1100/c.2023.03.013

一、引言

数字政府建设是新时代建设服务型政府，实现国家治理体系和治理能力现代化的重要举措。党的十九大以来，党和国家多次提出要推进和加强数字政府建设①，党的二十大更是明确提出要加快建设数字中国②。数字政府建设作为利用信息技术优化行政履职系统的智能化过程，离不开与时俱进的技术赋能体系，惟其如此，才能跟上时代潮流，满足行政履职的基本需要。

时下，ChatGPT的“爆火”为我国建设更高水平的数字政府提供了一个契机。作为一个深度交互的人工智能系统，ChatGPT仅仅发布2个月，月活跃用户就超过了1亿，创造了AI软件应用的新纪录。凭借其独特的语言交互能力，ChatGPT已经被广泛应用于金融、教育、科技、医疗等各个领域，可谓“一石激起千层浪”。面对ChatGPT的“爆火”，不少人认为这是人工智能技术的一次重大突破，如比尔·盖茨(Bill Gates)直言：“ChatGPT的影响不亚于互联网和个人电脑的诞生！”③但也有不少人表示担忧，如科技巨头马斯克(Elon Musk)认为：“ChatGPT让我们距离危险而强大的AI不远了。”④截至目前，尽管由美国OpenAI公司开发的ChatGPT模型尚未正式引入我国，但国内诸如百度、阿里、腾讯等科技巨头竞相决定推出类似产品，以此为ChatGPT模型画上中国印记。

在此情况下，未来数字政府建设与ChatGPT模型之间的互动就成为我们无法回避的问题。毕

基金项目：天津市教委一般项目“京津冀府际协同应急法律机制研究”(2022SK185)。

作者简介：周智博，天津财经大学法学院讲师(天津 300221；408819572@qq.com)。

① 参见耿亚东：《数字中国建设背景下政府数字化转型路径探析》，《治理现代化研究》2023年第1期。

② 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》，《人民日报》2022年10月26日，第1版。

③ 《比尔·盖茨：ChatGPT表明人工智能历史意义不亚于“PC或互联网诞生”》，https://baijiahao.baidu.com/s?id=1756921369033985165&wfr=spider&for=pc，访问日期：2023年2月25日。

④ 《马斯克：ChatGPT展示了AI已变得多先进，AI对人类是更大安全隐患》，https://www.thepaper.cn/newsDetail_forward_21929731，访问日期：2023年2月25日。

竞,不同于传统AI算法,ChatGPT模型能够给数字政府建设带来诸多“意外之喜”。依托于生成式人工智能(GAI)以及大型语言处理模型(LLM),ChatGPT模型不仅可以深度学习各类知识,将复杂的人机互动智能化,同时还可以模拟各种场景,帮助人类处理各类语言和文字工作。正因如此,有学者指出,ChatGPT模型作为人工智能技术发展至今的一次质变,其应用是今后各国推行数字治理、建设数字政府、开展数字竞争所无法回避的议题①。当前,美国、英国、日本和新加坡等国家的政府部门已明确发出了与ChatGPT合作的信号②。我国作为人工智能技术较为领先的国家之一,在将ChatGPT模型植入我国数字政府建设的过程中同样应该作出自己的判断,即:ChatGPT技术模型对于我国数字政府建设具有哪些功效?其植入数字政府可能会诱发哪些安全风险?未来又该如何进行引导和规范?有鉴于此,本文将尝试对上述问题进行系统回应,从而为今后相关的理论探讨、技术应用以及制度规范提供些许启示。

二、技术赋能:ChatGPT模型应用于数字政府的功效

ChatGPT模型作为人工智能领域的一次重大技术性突破,本身带有很强的赋能特征,其突出的语言交互能力、高效的信息驱动能力以及精密的算法运行能力,对于政府从事公共服务大有裨益。通过将ChatGPT模型引入我国数字政府建设,至少能够产生以下三方面积极作用:

(一)深度对话,增强数字政府的亲民性

友好的人机交互系统是数字政府建设的必然要求。易于理解、便于感知,是任何一项技术应用于数字政府的前提条件。尽管我国数字政府已经实现了从“对话智能体”(conversational agent)到“涉身对话智能”(embodied conversational agent)的技术转型,但距离人机双方实现流畅对话的终极目标始终存在一定距离③。当前,在数字政府建设过程中,各级政府很少从民众视角来检视一项技术的感知性与可接受性。其结果是,诸如物联网、区块链、人工智能等新型技术虽然从表面上赋予了数字政府以高度的便捷性和自动性,但由于内在“供需链条”的不匹配,使得这些技术始终无法真正深入人心,亦无法为人民提供满意的公共服务。根据《中国地方政府数据开放报告(2020下半年)》统计,数字政府的平台亲民性严重不足,只有22%的数字平台提供了无障碍浏览、语言翻译、沟通对话等包容性功能④。

ChatGPT模型内置了科学化和人性化的人工智能语言系统,能够通过学习和理解人类的语言来进行对话,还能根据聊天的上下文进行互动,其出人意料的语言“理解”和表达能力,已经超过90%的人⑤。因此,在数字政府建设过程中,ChatGPT技术的引入可以显著提升人机交互的友好程度,这集中表现为以下三点。其一,增强了沟通与对话的智能性。相比于传统的AI对话系统,ChatGPT在智能性上实现了重大突破。基于对行政公共服务数据的模拟训练,ChatGPT能够仿照人类语言互动模式,根据公众指令完成包括行政登记、行政审批、行政许可、行政确认以及政府信息公开等在内的各项行政公共服务事宜,这将极大提升民众对行政服务的满意度。其二,增强了沟通与对话的艺术性。相比于冷冰冰的信息传达,ChatGPT在运行过程中始终注重情境式表达,即在保证行政公共服务数据真实性、准确性和有用性的同时,最大程度上满足行政相对人的情感需求,从而在真正意义上实现沟

① 张佳欣、刘园园、陈曦等:《ChatGPT掀起技术狂潮“顶流”之下,看人工智能喜与忧》,《科技日报》2023年2月16日,第5版。

② 新加坡政府近日推行一个实验性项目,主题是利用ChatGPT模型辅助公务员草拟报告和演讲稿。参见《新加坡政府开发类ChatGPT系统帮公务员写报告,涉密信息除外》, https://www.thepaper.cn/newsDetail_forward_22108839, 访问日期:2023年2月26日。

③ 张帆:《人机对话系统的困境与解决》,《哲学分析》2022年第6期。

④ 冉连、张曦、张海霞:《政府数据开放中的公众参与行为:生成机理与促进策略》,《现代情报》2022年第2期。

⑤ 孙伟平:《人机之间的工作竞争:挑战与出路——从风靡全球的ChatGPT谈起》,《思想理论教育》2023年第3期。

通与对话的“以人为本”。其三,增强了沟通与对话的对称性。在传统行政行为语境下,政府与公民之间并无缓冲地带,“人人交互”的行为模式使得相对人时常感到力不从心。作为一种对话系统,ChatGPT能够在一定程度上突破传统行政模式下的对话失衡局面,使政府与公众在对话结构上始终具有平等的地位。这种平等不仅表现为信息本身的透明,更在于其能够在对话过程中,以一种十分亲和的方式,将行政行为的法律依据、组织程序、救济机制等以对话的形式呈现在人们的视野当中,从而将行政服务中的“官民摩擦”风险降到最低。

(二)技术嵌入,提高数字政府的效能性

技术赋能本身内含着组织、技术和流程再造的制度逻辑,一项新型技术嵌入数字政府一般会经历“技术联结—信息驱动—结构再造”三个阶段,这三个环节环环相扣,共同推动了数字政府在治理结构、治理方式和治理效能上的深层次变革①。

首先,ChatGPT模型增强了数字政府的技术联结能力。技术联结能力是人工智能技术成功赋能的关键所在②。ChatGPT模型作为高度智能化的AI交互系统,本身内含了十分先进的算法体系。依托于云计算、大数据、物联网、移动终端等构建的“云+网+端”生态③,ChatGPT模型能够充分满足数字政府的运行需要,且随着技术联结性不断加深,数字政府的治理效能也势必会有一个质的突破。

其次,ChatGPT模型完善了数字政府的信息驱动系统。长期以来,信息驱动能力不足一直都是数字政府建设的一大掣肘,受制于科层体制、信息技术和信息人才的局限,各地政府往往心有余而力不足。ChatGPT模型作为大型数据处理系统,着重强调信息驱动能力建设,主张通过信息共享、信息交互以及信息协同机制来充分整合数据资源。因此,将ChatGPT模型引入数字政府建设,能够有效克服行政机关的技术短板,推动公共信息资源的融会贯通。

最后,ChatGPT模型优化了数字政府的结构再造体系。数字政府建设作为一个系统工程,时下“专业化—部门化—利益化”的治理模式严重影响了数字政府效能的提升。为此,如何打破这种“碎片化”治理格局就尤为重要④。ChatGPT模型作为一种新型AI技术,凭借其信息收集、数据分析以及语言重塑能力,能够有效整合政府治理资源,改善政府治理结构,打破政府组织壁垒,实现跨部门、跨层级的协同治理。

(三)算法融入,推动数字政府的智慧性

当今,在政府从事公共管理过程中,借助人工智能算法实现科技赋能,已经成为各国提升行政服务水平的基本经验。ChatGPT模型内含高度发达的算法系统,在近端策略优化(PPO)算法的强力支撑下,ChatGPT模型能够有效提升数字政府的智慧性。

首先,ChatGPT模型提升了行政决策的科学性。在人工智能时代,行政决策在一定程度上已经转变为“信息输入—数据分析—决策输出”的自动化公式。高度成熟的算法系统凭借其自主学习能力,往往能够妥善应对各类治理难题⑤。同样,ChatGPT模型通过自动抓取、精确识别、自动分类和高度模拟系统,能够对海量信息进行归类和整理,使基于大数据的政府智能决策成为可能。不仅如此,ChatGPT还可以将决策议题转换为算法能够理解的数据模型,并结合行政主体、行政权限、行政程序、相对人请求等特定语境,帮助行政机关作出一个最优决策。

其次,ChatGPT模型提升了行政程序的规范性。当前,随着科学技术的发展,人工智能算法已在

① 胡重明:《“政府即平台”是可能的吗? ——一个协同治理数字化实践的案例研究》,《治理研究》2020年第3期。

② 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》,《中国行政管理》2021年第2期。

③ 逯峰:《整体政府理念下的“数字政府”》,《中国领导科学》2019年第6期。

④ 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》,孙迎春译,北京:北京大学出版社,2008年,第17页。

⑤ 陈鹏:《算法的权力:应用与规制》,《浙江社会科学》2019年第4期。

无形中内嵌于政府的行政程序之中,悄无声息地完成了对行政程序的技术化改造。ChatGPT模型作为一个智慧化的神经网络系统,始终强调对现实情境的模拟与重塑。通过将ChatGPT模型融入数字政府,特定行政方式、行政步骤、行政时限和行政顺序就能更加有迹可循,与之相关的行政审批程序、行政处罚程序、政府信息公开程序以及行政自由裁量程序等,也可以在无形中变得更加标准化和规范化。

最后,ChatGPT模型增强了数字政务的公平性。数字政府建设在给个人带来便利的同时,也伴随着新型的伦理挑战,算法歧视便是其中之一。作为新型的科技伦理风险,算法歧视是指人工智能算法应用中不合理的区别对待。时至今日,如何通过算法提供更加公平合理的公共服务,始终是数字政府建设的重要诉求。ChatGPT模型引入数字政府能够在很大程度上降低行政算法歧视风险。众所周知,低门槛、多元化、智能化始终是ChatGPT模型的最大优势,强大的语言算法系统,能够让ChatGPT模型全方位了解不同学历背景、不同年龄阶段、不同专业能力的行政相对人需求。不仅如此,基于简单的问答和指令系统,ChatGPT模型还能一改此前"政府智能服务不智能"的窘境。从这个意义上讲,ChatGPT模型在一定程度上顺应了人工智能时代行政相对人的"期待转移"[①],极大地降低了算法对不同人群的歧视风险。

三、技术风险:ChatGPT模型应用于数字政府的安全隐患

人工智能技术本身是一把双刃剑,在ChatGPT模型服务于数字政府建设的同时,也伴随着来自国家层面、政府层面以及个人层面的数字安全风险,相关风险认知对于我国数字政府建设具有重要意义。

(一)国家层面:国家数据主权之安全风险

在大数据时代下,数据作为政府从事智能化管理的重要战略资源,不仅关乎数字政府的运行状态,同时还涉及国家数据主权安全问题[②]。作为一个舶来品,ChatGPT模型在应用于我国数字政府建设的过程中,很可能会给国家数据主权带来如下两方面风险:

其一,国家数据情报安全风险。在大数据时代,国家情报安全无疑被提上了新的高度,一旦相关数据被他国情报部门入侵,就很可能引发"数据污染""数据窃取"以及"数据攻击"等安全隐患[③]。众所周知,数字政府的持续运行须始终以政治、经济、文化、社会等各个领域的"关键信息基础设施"[④]作为支撑。如果直接将ChatGPT模型应用到我国数字政府平台中,则意味着将与"关键信息基础设施"直接相关的"关键性基础信息"的收集权、使用权、分析权、存储权交由ChatGPT数据平台处置,稍有不慎,就可能引发超大规模敏感性信息的泄漏。不仅如此,ChatGPT模型的语言交互行为带有很强的价值传输属性,在服务于数字政府的过程中,很可能因为安全立场分歧对我国主流安全价值观造成负面影响,进而引发数据情报安全风险。

其二,数据主权技术安全隐患。自主、安全、可靠的技术是维护国家数据主权安全的重要保障,在将ChatGPT模型引入数字政府建设的过程中,我国极有可能面临因自主技术不足而产生的安全隐

① 梅立润:《人工智能时代国家治理的算法依赖及其衍生难题》,《中南大学学报(社会科学版)》2022年第6期。

② 国家数据主权安全作为国家主权在网络空间领域的延伸,是国家对数据、软件、标准、服务和其他数字基础设施享有的合法控制权、最高管辖权以及独立自主权。参见孙南翔、张晓君:《论数据主权——基于虚拟空间博弈与合作的考察》,《太平洋学报》2015年第2期。

③ 吴承义、唐笑虹:《大数据时代国家安全情报面临的变革与挑战》,《情报杂志》2020年第6期。

④ 根据国务院公布的《关键信息基础设施安全保护条例》可知,关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

患。据悉,早在2015年,OpenAI公司就基于自主研发的近端策略优化算法推出了语言模型GPT-1。时至今日,该公司又围绕这一模型开发出了神经网络(Jukebox)、图像神经网络(CLIP)、人工智能系统(DALL·E)等多项前沿技术,并初步将模型从第一代发展到了第四代。然而相较于OpenAI公司,我国对于类ChatGPT模型的研发起步相对较晚,诸如百度、腾讯、阿里等公司于2019年才开始涉入这一领域。因此,如何在克服芯片研发困难的同时,开发出大型神经网络和语言交互系统,进而实现技术的补强与赶超,无疑是今后我国数字政府建设过程中面临的重大挑战。不仅如此,除了自身研发能力不足外,我国同时还面临OpenAI公司的直接技术性封锁。截至目前,OpenAI的应用程序编程接口(API)尚未向我国正式开放,这种技术性垄断也在一定程度上阻滞了ChatGPT模型在我国数字政府中的应用。

(二)政府层面:行政权公共性之解构风险

根据我国宪法,国家一切权力属于人民,因此,无论数字政府如何发展,公共行政始终都是其主色调[①]。但随着ChatGPT模型的融入,数字政府将会或多或少面临一些公共性伦理挑战,稍有不慎,就会引发行政权力公共性的解构风险。

一方面,可能产生数字技术资本入侵风险。与传统经济资本中的技术力量不同,数字技术资本在人工智能时代下掌握着更高的话语主导权以及资源配置权[②]。在逐利价值观的影响下,ChatGPT模型的数字技术资本属性在带来政府数字科技革新的同时,也在一定程度上加剧了行政权力公共属性的解构风险。随着技术、市场、资本等各方面资源的不断聚集,ChatGPT模型背后的技术资本很可能拥有比公权力机关更为强大的影响、控制与支配权,甚至将传统行政权力中蕴含的公益色彩排除在外。申言之,ChatGPT拥有的技术优势很可能会因为其逐利特质而对公民进行行为支配,并将"政府—相对人"的行政法律关系演变为"ChatGPT—公民"的支配性法律关系。正如有学者指出,资本的逐利本质将会进一步引发"数字方式"的异象,并导致政府公共秩序的强烈阵痛[③]。

另一方面,可能引发追责链条断裂风险。行政追责是强化行政权力公共属性的关键一环,在传统行政决策视域下,遵循"谁决策,谁负责"的理念,基本可以实现行政追责的逻辑闭环[④]。但随着ChatGPT模型的引入,权力、责任和算法的关系愈发紧密,一旦因ChatGPT模型内部算法黑箱、算法偏差等原因引发决策失误,相应的行政追责逻辑链条很可能会存在断裂风险。申言之,政府很可能会以ChatGPT模型运行失误为理由推诿责任。同样,除却民事责任之外,我们也很难对ChatGPT模型课以行政责任,否则很容易混淆行政行为与市场行为的责任边界[⑤]。更重要的是,ChatGPT模型在行政决策环节很可能会由辅助系统演变为事实上的决策系统,甚至在特定情形下直接取代政府公务人员自身的价值判断[⑥],这无疑将进一步加剧行政追责链条的断裂风险。总之,新型算法系统与传统行政主体在行政决策中的角色错位,使行政决策很可能会陷入一种无责可追的状态之中。在这一方面,英国女性在乳腺癌筛查中遭遇的追责窘境就是算法行政责任链条断裂的鲜明实例[⑦]。

① 李承、王运生:《当代公共行政的民主范式》,《政治学研究》2000年第4期。

② 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》,《东北大学学报(社会科学版)》2022年第4期。

③ 孟庆国、崔萌:《数字政府治理的伦理探寻——基于马克思政治哲学的视角》,《中国行政管理》2020年第6期。

④ 周叶中:《论重大行政决策问责机制的构建》,《广东社会科学》2015年第2期。

⑤ 王怀勇、邓若翰:《算法行政:现实挑战与法律应对》,《行政法学研究》2022年第4期。

⑥ 陈飏、裴亚楠:《论自动化行政中算法决策应用风险及其防范路径》,《西南民族大学学报(人文社会科学版)》2021年第1期。

⑦ 2018年,在英国女性乳腺癌筛查漏检丑闻中,关于"算法错误"究竟是怎么产生的,国家卫生医疗系统、公共卫生局以及负责软件维护的日立咨询公司三方互相踢皮球,至今仍然未有定论。参见汝绪华:《算法政治:风险、发生逻辑与治理》,《厦门大学学报(哲学社会科学版)》2018年第6期。

(三)个人层面:公民数据权利之侵犯风险

数字政府建设并不是一种静态的理论假想,而是一种动态、开放的阶段性过程①。ChatGPT模型并不能从根本上消解数字政府建设与公民数据权利保障之间的张力,公众在享受政府智能化服务的同时,也要时刻承担数据权利被侵犯的风险。

首先是个人信息过度收集风险。ChatGPT模型的高效运行离不开对信息数据的收集,脱离海量数据的支撑,ChatGPT模型的语言能力将会大打折扣。截至目前,OpenAI公司在未经数据权人同意的前提下,已经收集了大量个人敏感数据②。正所谓"资源集聚在一定程度上就是权力集聚"③,一旦ChatGPT模型被正式引入数字政府之中,那么其掌握的个人信息数据将会呈指数级增长。在这种情况下,ChatGPT模型基于信息数据的资源集聚效应,很可能会进一步对普通公民施以"数据权力支配"。更重要的是,有了"政府合作"这层合法外衣,ChatGPT模型对于个人信息数据的收集将会更加肆无忌惮,庞大的数据基数、多元的数据种类、高超的分析能力,将会给公民个人隐私权保障带来严重挑战。

其次是个人数据深度整合风险。数据整合是指通过一定数据转化、数据推理和数据模拟技术,将规模庞大、排序散乱的数据转换为具有一定规律性和逻辑性数据的处理机制。深度、专业、高效且精准的数据整合系统赋予了ChatGPT模型以极大优势。但问题是,在建设数字政府的过程中,ChatGPT模型很可能会偏离公共行政目标,在政府和用户不知情的情况下,将数据整合系统转为他用。毕竟,算法黑箱的存在使得社会公众虽然能在表面上感知算法的宏观运行,却始终不能追根溯源,对其内部一窥究竟④。在这种情况下,公民数据权保障难免会陷入更加被动的局面。

再次是个人数据存储和泄漏风险。其一,未经允许的个人信息存储。当前,OpenAI公司并未提供任何方式供个人检查其数据存储库。不仅如此,OpenAI公司信息使用条款也并未包含任何数据存储的保护和救济内容。其二,无限期的个人数据存储。根据《个人信息保护法》⑤,信息存储是有时间限制的,并非可以无限期地保留。但在实践中,ChatGPT模型并未明确规定信息存储期限,这种"刻意"回避显然不利于公民数据权的保障。其三,个人数据泄露风险。在数字政府建设过程中,ChatGPT模型极有可能因为数据处理不当造成公民数据泄露,这不但会对公民的"数据人格"造成侵害,甚至会因公民的焦虑和抵触情绪,让数字政府建设陷入"寒蝉效应"⑥。

最后是个人数据支配风险。仅从表面看,服务于数字政府的ChatGPT技术是客观中立的产物,可一旦这种技术植入特定法律关系,其中立性便会经不起推敲。可以想象,随着数字政府建设的不断推进,在商业化需求的导向下,ChatGPT模型对政府的智能化服务极有可能转变为对公民个人的数据支配和统治。申言之,我们在利用算法提升数字政府效能的同时,ChatGPT模型很可能演变为"准数据权力"机关,在看似平等的数据法律关系中愈发占据主动性,并成为公民数据权利侵害的主要风险源。

---

① Attard J., Orlandi F., Scerri S., et al., "A Systematic Review of Open Government Data Initiatives", *Government Information Quarterly*, 2015,32(4), pp.399-418.

② 根据OpenAI的隐私政策,ChatGPT模型有权随时收集用户的IP地址、浏览器类型及设置、用户与网站互动的数据,包括用户所参与的内容类型和使用的功能,另外它还会收集用户在不同时间以及不同网站上的浏览活动信息。

③ 周旺生:《论作为支配性力量的权力资源》,《北京大学学报(哲学社会科学版)》2004年第4期。

④ 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。

⑤ 《个人信息保护法》第19条规定:"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。"

⑥ Solove D. J., Citron D. K., "Risk and Anxiety: A Theory of Data-Breach Harms", *Texas Law Review*, 2018,96(4), pp.737-786.

四、技术规制:ChatGPT模型应用于数字政府的路径规范

在数字政府建设过程中,风险与规制相生相随,唯有建立一个涵盖数据规范、责任导向、权利保障以及技术培育的完整体系,ChatGPT的技术应用才能被纳入一个安全可控的范围之内。

(一)数据规范:推动ChatGPT数据的分类分级

当前,随着数据安全上升到国家主权安全层面,数据分类分级制度已经成为国家数据治理的必然选择①。所谓"数据分类分级",是指国家以数据敏感程度、运作方式、运行目的等信息为标准,将数据类型化为不同等级和类别的数据管理制度。从根本上讲,ChatGPT模型引发的数据安全风险源于其所依托和处理的数据,如果我们在源头上建立数据分类分级制度,就能实现对ChatGPT数据的有效规范。当前,我国以《中华人民共和国数据安全法》《工业数据分类分级指南(试行)》《科学数据管理办法》为代表的法律和规范性文件,已经围绕数据分类分级提出了初步的战略构想,如《中华人民共和国数据安全法》明确国家要建立数据分类分级保护制度②。因此,为了降低ChatGPT模型处理数据所产生的风险,今后我国应该围绕《中华人民共和国数据安全法》,以数据内含的价值、利益和公共属性为标准,在中央主导下建立"自上而下"的数据分类分级制度。在中央层面,应该建立国家数据安全工作协调机制,根据数据对国家、社会和个人的重要程度,建立数据分类分级的总体性框架和目录。之后,再根据强制性适配规则,由不同层级的政府主管部门加以具体细化,从而为ChatGPT模型应用于数字政府提供一个安全准确、可供操作的数据处理规则。具体而言:首先,就高等级涉密数据而言,事关国家主权安全和有关个人隐私的信息,ChatGPT模型背后的数据处理系统无权涉及,政府在与ChatGPT模型合作的过程中也应保持这类数据的绝对安全。其次,就中等级涉密数据而言,对于部分涉及企业商业秘密的数据,政府经数据所有者同意,可以适度向ChatGPT模型开放。如此,就能在公共利益与个人利益之间形成一个良性平衡。另外,基于"协商"这一前置要件,政府的裁量权也能够得到适度规范。最后,就低等级无涉密数据而言,对于不涉及国家安全、个人隐私和商业安全的数据,政府有权将其完全交由ChatGPT模型,从而在最大程度上提升政府的公共服务效能。需要注意的是,无论是哪一等级和类别的数据,ChatGPT模型在数据收集、处理和应用过程中都必须始终依照法律进行。与此同时,数据分类分级并不等同于绝对意义上的"闭关锁国"。在全球化视野下,全球数据流通与数据治理已经是大势所趋,为了避免因为数据过度分类分级而降低数据治理价值,今后我国应该秉持安全、动态、合作以及可持续的发展原则③,把握好数据分类分级与数据治理效能之间的关系,科学制定数据分类分级目录,从而实现数据治理效能的最大化。

(二)责任导向:完善ChatGPT模型的责任链条

诚如上文所言,尽管ChatGPT模型在一定程度上提升了行政决策的自动化效能,但为避免ChatGPT模型植入行政决策所导致的"无责可追",必须完善配套的追责链条。需要明确的是,无论是行政机关还是ChatGPT模型的服务提供者,都不能基于算法而免责。此前有学者一度认为,算法作为一种技术,基于其价值中立性,相应的算法决策也是客观的,"可以有效避免传统政府治理模式下

① 崔爽:《国家网信办:拟建立数据分类分级保护制度》,《科技日报》2021年11月15日,第3版。

② 《中华人民共和国数据安全法》第21条规定:"国家建立数据分类分级保护制度,根据数据在经济社会发展中的重要程度,以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用,对国家安全、公共利益或者个人、组织合法权益造成的危害程度,对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录,加强对重要数据的保护。"

③ 洪延青:《国家安全视野中的数据分类分级保护》,《中国法律评论》2021年第5期。

行政裁量的偏向性问题”[①]。本文认为这种算法责任虚无主义明显违背了人工智能时代下的算法价值伦理,我们必须予以抵制。申言之,即便ChatGPT模型具有很强的技术性,运行原理和过程不易被普通公众理解和把握,但行政机关和ChatGPT模型的服务提供者并不因此享有豁免权利,其与传统模式的区别仅在于责任承担形式有所不同而已。

一方面,就政府而言,其应该就ChatGPT模型的决策失误承担行政责任。行政机关是算法决策过程中唯一“出场”的行政主体,一旦特定行政决策对行政相对人的权益造成了不利影响,行政机关理应被视为第一责任人。究其原因,作为ChatGPT模型的实际应用者,行政机关始终负有审慎依赖的义务,具体而言:(1)ChatGPT模型引入阶段的安全审查责任。在ChatGPT模型植入阶段,政府有义务基于公共性审慎选择数字合作平台。当前,考虑到政府自身研发能力不足,各地在建设数字政府过程中更多采用“政企合作”模式,但这种合作并非简单的“拿来主义”。相反,在数字政府建设过程中,政府对于特定算法技术应用必须保持审慎态度,即基于“利之所在,损之所归”的基本理念,政府理应审慎考察合作平台资质、充分了解合作平台技术、妥善签订平台合作协议,从而将ChatGPT模型应用的负外部效应降到最低。否则,一旦因为前期审查不当造成不利影响,那么政府必须承担相应的行政责任。(2)ChatGPT模型应用阶段的结果甄别责任。尽管算法决策具有很强的自动化特征,但政府在基于算法作出行政决策的过程中,仍然能够在一定程度上控制算法的运用。ChatGPT模型作为一种语言系统,尽管其结果输出往往取决于问题输入,但政府对数据筛选、数据输入以及结果采用等始终应承担一定的谨慎处理义务。政府有义务意识到“算法至上”和“算法代表”的陷阱,进而决定如何采用算法决策方案,一旦因为过分依赖而诱发行政决策失误,就必须承担相应的行政责任。

另一方面,就服务提供者而言,其应该就ChatGPT模型的决策失误承担民事责任。算法的提供者在某种程度上直接决定了ChatGPT模型的运行过程和结果,即其不仅能够在算法开发阶段控制算法的实际运行状态,还能在算法的运营中实时监测算法的运行公式、算法的训练模型以及语言操作系统。按照此种观点,算法从根本上属于“产品”[②],如果ChatGPT模型存在缺陷或瑕疵,政府有权依据委托开发合同以及民事法律法规来对服务提供者进行追责,责任承担内容可以包括经济赔偿、合同单方解除权利、纳入政府采购黑名单等[③]。

(三)权利保障:强化公民数据权的国家保护义务

面对来自ChatGPT模型的数据权利侵害,传统基本权利功能视域下针对国家的防御权模式难免力有不逮,此时,引入国家保护义务理论就尤为必要。所谓国家保护义务,是指基于宪法基本权利的辐射效力,要求国家对来自私法主体的基本权利侵害行为采取积极的国家保护措施,从而保障弱势一方基本权利实现的义务。

首先,就事前阶段而言,应强化立法机关的风险预防义务。在人工智能时代,为减少公民基本权利的不确定性,国家必须事先履行风险预防义务[④]。风险预防义务是国家保护义务在数据权领域的体现,要求国家必须积极完善立法,从而有效防止第三人对数据权的不当侵犯。诚如欧盟工业主管蒂埃里·布雷顿(Thierry Breton)所言,ChatGPT带来的权利侵害风险,凸显了制定预防性规则的迫切需要[⑤]。在此,为了有效防止ChatGPT模型在数字政府建设过程中对公民数据权的侵犯,必须围绕

① 王文玉:《算法嵌入政府治理的优势、挑战与法律规制》,《华中科技大学学报(社会科学版)》2021年第4期。

② 王叶刚:《个人信息处理者算法自动化决策致害的民事责任——以〈个人信息保护法〉第24条为中心》,《中国人民大学学报》2022年第6期。

③ 王怀勇、邓若翰:《算法行政:现实挑战与法律应对》,《行政法学研究》2022年第4期。

④ 王旭:《论国家在宪法上的风险预防义务》,《法商研究》2019年第5期。

⑤ 《ChatGPT爆火 伦理安全拷问现行治理体系》, https://baijiahao.baidu.com/s?id=1758391383708671496&wfr=spider&for=pc, 访问日期:2023年2月25日。

《个人信息保护法》优化“知情—同意”规则。有效的“知情—同意”规则应遵循“明确告知—充分知情—自主自愿—明确同意”的逻辑路径。当前,鉴于“明确告知”环节仍存在一定不足,今后法律必须细化ChatGPT模型的告知义务,强调其以一种简洁、透明、通俗、易懂的方式向数据权主体作出解释和说明,且数据处理的风险程度越高,告知规则就要越明确。惟其如此,数据权主体的“数据同意”才更为真实可靠①。需要注意的是,国家的风险预防并不同于风险消除,这意味着基本权利保障必须是动态和包容的,一旦主客观条件发生了变化,相应的预防方式、预防程度和预防内容也应该进行配套变更。申言之,国家保护义务并非一蹴而就,而是一个长期、动态且持续的过程,一旦法律的适用环境发生了变化,立法者必须进行配套修改和补充,否则同样违反了国家保护义务的要求②。

其次,就事中阶段而言,应明确行政机关的侵害排除义务。在数字政府建设过程中,政府不仅是数字平台的合作者,同时也是数字平台的监管者,其对ChatGPT模型与数据权主体之间的关系始终负有平衡义务。具体而言,通过政府监管,“知情—同意”规则的实效性将会大大增强,促使ChatGPT模型更加合理地提供数字服务。同时,面对ChatGPT模型对公民数据权的侵犯,行政机关应适时启动行政处罚机制,通过没收违法所得、停业整顿、吊销营业执照等制裁措施,为数据权主体提供一种实时性、机制性的保障。此外,面对数据平台的数据违规处理,国家网信办还可以根据群众举报启动行政约谈,强制ChatGPT数据平台限期完成整改。事实证明,“行政约谈+行政处罚”的监管模式往往事半功倍,可以有效规范数据平台的信息处理行为,为公民数据权提供全方位的保障③。当然,通过行政监管来强化国家保护义务也是有边界的,即应尽可能避免因为监管过度而侵犯ChatGPT模型服务提供者的经营自由权,进而触发防御权模式。

最后,就事后阶段而言,应强化司法机关的权利救济义务。司法救济同样是数据权国家保护义务的重要机制。当今世界,无论是英美法系国家还是大陆法系国家,在数字政府建设过程中,都愈发重视法院在数据权保障中的能动作用。有鉴于此,一方面,应完善数据权举证责任体系。“举证难”一直是数据权主体维权的一大障碍,考虑到现有数据权举证规则不甚清晰,今后应该明确数据侵权适用过错推定责任。正如有学者所言,采用过错推定原则能够更好地平衡当事人双方的利益诉求④,即在减轻数据弱势群体举证责任的同时,还能课以数据平台基本的注意义务,从而更好地保障数据权主体的基本权益。另一方面,应完善数据权集体诉讼机制。考虑到公民个人作为弱势群体在维护自身数据权过程中的不利地位,今后应适时引入集体诉讼机制,如将科技行业协会作为诉讼代表,从而改变数据权主体在数字政府建设中的被动地位,让数据权救济更加有的放矢⑤。

(四)技术培育:加强对ChatGPT技术的引导与研发

当前,数字技术已经成为国家数据主权竞争以及数据安全维护的重要依托⑥。国家在建设数字政府的过程中,不能一味奉行“技术拿来主义”,对ChatGPT技术进行配套的引导与研发同样不容忽视。

一方面,加强对ChatGPT技术的伦理性引导。理念是行动的先导,ChatGPT模型作为一项颠覆

① 于海防:《个人信息处理同意的性质与有效条件》,《法学》2022年第8期。

② 陈征:《基本权利的国家保护义务功能》,《法学研究》2008年第1期。

③ 谭海波、史钰宏:《政府对互联网信息服务平台的约谈有选择性吗?——基于2018—2021年网信办94份行政约谈数据的分析》,《行政论坛》2022年第6期。

④ 陈吉栋:《个人信息的侵权救济》,《交大法学》2019年第4期。

⑤ 此前,德国联邦司法与消费者保护部公布了一项法律草案,草案建议对《不作为之诉法》进行修改,通过修改赋予团体对企业的信息数据侵权提起集体诉讼的权利,也就是说在个人救济不力的时候,可以让消费者协会来承担集体诉讼。参见徐苗:《德国消费者团体诉讼研究——兼论其对中国消费公益诉讼的借鉴意义》,南京大学硕士学位论文,2016年,第9-10页。

⑥ 保建云:《世界各国面临数据与数字技术发展的新挑战》,《人民论坛》2022年第4期。

传统人工智能的新型技术,其在植入数字政府的过程中始终隐藏着一定伦理性挑战,且稍不留意就会产生诸如国家数据主权风险、数字技术资本侵蚀以及公民数据权侵犯等一系列安全隐患。因此,我们必须妥善处理好ChatGPT技术发展与伦理价值约束之间的关系。早在2004年,简·芳汀(Jane E. Fountain)就明确指出,信息技术究竟是强化还是颠覆人类传统价值伦理,是任何国家都必须明确的问题①。其中,一项数字技术是否符合特定国家、社会的伦理和价值观,更是其推广和应用的重要标准②。对于我国而言,中华民族的价值伦理集中体现在社会主义核心价值观之中③。为减少ChatGPT模型对我国价值伦理的侵蚀,今后应将ChatGPT模型植入社会主义核心价值观的语境下,切实发挥伦理调节、伦理评估以及伦理督导的作用,从而将ChatGPT模型的应用纳入持续、包容、健康、和谐的轨道。

另一方面,加强对ChatGPT技术的公益性研发和投入。ChatGPT模型的发展需要以各项核心技术作为支撑,其不仅涉及传统的芯片技术,更涉及最前沿的生成式人工智能以及大型语言处理模型。与之相应,ChatGPT模型的研发和投入往往具有投资大、耗能高、周期长等特质。尽管国内诸如百度、阿里、科大讯飞、腾讯等公司先后计划发布类似ChatGPT的产品,但受制于市场主体的自利性、自发性和短视性,产品服务质量难以保障,同时还存在一定的资本侵蚀风险。因此,为了强化国家主权保障的技术支撑作用,维护我国数据主权安全和国家情报安全,今后必须加强我国自主的类ChatGPT技术的创新与研发。在其中,尤其要注重发挥新型举国体制的优越性,将不同区域、不同领域、不同行业的科技资源集中起来,在短时间内有效克服各类科技难题,以此实现国家创新体系的协同攻关④。申言之,唯有加强对ChatGPT模型的公益性研发和投入,我国才能打破国外技术垄断,为数字政府建设提供一套安全、自主、可靠的技术体系。

五、结语

ChatGPT模型作为人工智能领域的重大技术突破,在数字政府建设过程中,一味地排斥或者接纳都不可取,唯有将技术赋能、技术风险以及技术规制加以综合统筹,才能摆脱“技术利维坦”的窘境,将数字政府建设纳入健康、包容和可持续的轨道之中。理论分析表明,ChatGPT模型有望使数字政府更加亲民、高效和智能,但同时也可能引发来自国家层面、政府层面以及个人层面的数字安全风险,这要求我们必须建立一个涵盖数据规范、责任导向、权利保障以及技术培育的完整体系。为了在最大程度上降低ChatGPT模型对公民数据权利的侵害,立法机关的风险预防、行政机关的侵害排除以及司法机关的权利救济尤为重要。总之,ChatGPT模型的植入应始终置于法治框架之中,即在把握人工智能技术发展规律的基础上,以客观辩证的思维、持续包容的理念以及系统规制的路径加以法治化调适,从而让ChatGPT模型更好地服务于我国数字政府建设。

① 参见姚清晨、郁俊莉:《嵌入与变构:数字化技术重塑政府治理体系的逻辑及其基层困境》,《甘肃行政学院学报》2021年第5期。

② Moses L. B., Chan J., “Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools”, *University of New South Wales Law Journal*, 2014, 37(2), pp.643-678.

③ 孙光宁:《社会主义核心价值观的法源地位及其作用提升》,《中国法学》2022年第2期。

④ 雷丽芳、潜伟、吕科伟:《科技举国体制的内涵与模式》,《科学学研究》2020年第11期。

Introducing ChatGPT Model to Digital Government Construction in China: Functions, Risks, and Regulations

Zhou Zhibo
(School of law, Tianjin University of Finance and Economics, Tianjin 300221, P.R.China)

Abstract: The construction of a digital government is related to the modernization of the state governance system and capacity. With the great technological breakthrough of the ChatGPT model, it is of great significance to grasp the technical adaptability between the ChatGPT model and China's digital government construction. It is not wise to simply reject or fully accept the ChatGPT model when it comes to the construction of a digital government. Only by comprehensively coordinating technology enablement, technology risks, and technology regulations, can the cognitive dilemma of "Technological Leviathan" be overcome. Then the construction of a digital government can be brought into a scientific, inclusive, and sustainable track. As a major technological breakthrough in artificial intelligence, the ChatGPT model has strong capability of technical enablement. Its deep language interaction ability, efficient information driving ability, and precise algorithm operation ability are of great benefit to the government engaging in public services. The ChatGPT model, as a deep interactive artificial intelligence system, can greatly improve the affinity, efficiency and intelligence of a digital government. However, artificial intelligence technology itself is a double-edged sword. When introducing the ChatGPT model to the construction of digital government, one must be fully aware of the security risks of national data sovereign, the governmental administrative publicity deconstruction, and personal data rights infringement. Risk and regulation are closely related. A complete system covering data regulation, responsibility orientation, rights protection, and technology cultivation should be established and only by this means can ChatGPT's technology application be regulated in a safe and controllable range. In order to reduce the ChatGPT model's impact on the digital government and reach an optimal balance between the utilization and regulation of ChatGPT model, the classification of the model's data must be exerted, the responsibility chain of the model must be improved. The national protection obligation of citizens' data rights, and the technical guidance and development of the model must be strengthened. It is underscored that in the process of protecting citizens' data rights, it is particularly important for the legislative organs to prevent risks, the administrative organs to eliminate violations, and the judicial organs to provide rights relief. To summarize, for better integration of ChatGPT to the digital government in China, we should ground our thinking in the rule of law, to clearly grasp the law of the development of artificial intelligence technology, and to make adjustments according to laws with thinking in objective dialectics, tolerance in consistency, and an approach of system regulation.

Keywords: Digital government; ChatGPT model; Technology enablement; Data rights

[责任编辑:岳　敏]