

基于隐私保护的政府 大数据治理研究

李政¹, 洪莹²

1. 中国联通国际有限公司, 北京 100032; 2. 北京工商大学商学院, 北京 100048

摘要

5G时代数据的基础性战略资源属性进一步突显, 数据是政府推进国家治理体系和治理能力现代化的有力支撑资源和工具。与此同时, 个人隐私也逐渐受到关注, 成为进一步运用政府大数据需要解决的核心问题之一。在分析5G时代政府大数据隐私新特征、现有数据法律对政府大数据隐私保护的影响的基础上, 提出一个基于隐私保护的政府大数据治理模型, 探讨5G时代背景下政府如何在利用好自身大数据资源改善服务质量和效率的同时保护公众隐私, 以期对新时代政府治理能力提升有所助益。

关键词

隐私; 大数据; 政府治理; 5G; 个人信息

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-0271.2020015

Study on big data management for government based on privacy protection

LI Zheng¹, HONG Ying²

1. China Unicom Global Ltd., Beijing 100032, China

2. Business School of Beijing Technology and Business University, Beijing 100048, China

Abstract

5G highlights the basic strategic resource attribute of data, which could be treated as powerful tool and resource in modernization of governance system and capacity for Chinese government. In the meanwhile, privacy has been concerned by masses much more seriously, while privacy protection became one of the core issues need to be solved in the further use of government big data. Based on the analyses of new privacy features of government big data in 5G, as well as the impact of existing data laws on government big data privacy protection, a big data management model focusing on privacy protection for government was advanced. The question of how to make use of government big data in improving administrative service quality and efficiency while protecting privacy was discussed, so as to be helpful to Chinese government in governance promotion in new era.

Key words

privacy, big data, government governance, 5G, personal information

1 引言

进入21世纪以来,以互联网、移动互联网为代表的数字经济,在世界主要国家和经济体中所占的比重迅速提升,数字经济已经成为众多国家经济发展的重要引擎和新动力。以中国为例,根据中共中央网络安全和信息化委员会办公室《数字中国建设发展报告(2018年)》^[1]公布的数据,2018年我国数字经济规模已达到31.3万亿元,占国内生产总值(gross domestic product, GDP)的34.8%。数字经济的快速发展,给各国的经济、社会、政治、文化带来了显著而深远的影响。数字经济参与实体通过持续引入新的技术和生产工具,以“客户至上”“快速迭代”等理念为指导,不断创新,开创新商业模式服务新需求,优化重塑传统经济,注入新活力,有效提升了社会生产资料的配置效率,极大改善了社会总福利。

在这一过程中,数据作为数字经济的生产原材料,其重要性日益凸显。国内方面,中国共产党第十九届中央委员会第四次全体会议明确提出“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制”,首次将数据纳入了生产要素范畴,体现了中国政府对数据这一数字经济关键资源的高度重视。国际方面,2019年G20日本大阪峰会^[2]、金砖国家巴西峰会等国际会议,均将数据流通、数据治理等内容作为重要的讨论议题。

作为数字经济中重要的参与方之一,政府在数据治理中持续扮演着重要角色。一方面,数字经济属于新生事物,将很多现有法律、法规、制度直接应用于数字经济会受到很多限制,这在隐私和个

人信息保护方面体现得尤为突出,政府作为监管者,需依据数字经济特征及时完善或制定相应政策。另一方面,无论是从历史沿革角度,还是从未来的发展趋势(智慧城市)角度,政府本身就拥有数量巨大、种类丰富、涵盖广泛的细颗粒度数据,责任重大,客观上需提升自身的数据治理能力。

随着21世纪第3个十年的到来,政府大数据治理面临着一些突出的新变化。其一,2019年世界迎来了5G元年,各国政府相继发放了5G商用牌照,2020年将进入5G快速发展期。5G网络基于增强移动带宽、低功耗大连接、低时延高可靠三大应用场景^[3],将会持续高效地赋能新技术与新技术,支持增强现实(augmented reality, AR)/虚拟现实(virtual reality, VR)、无人驾驶、物联网、工业互联网、智慧城市等高数据交互应用的联网需求,促进数字技术与社会治理、工业、商业、服务业更广泛地融合,带来网络基础设施与数字经济繁荣之间的相互促进。在这一过程中,5G必将带动上行数据流量的大幅增加,政府从源头上获得更大量级、更多种类、时效性更高的数据成为现实。其二,随着2019年以来一系列重大数据滥用、泄露、技术运用事件的相继爆发,民众在网络上的个人信息保护意识日益增强,越来越多的普通人开始关注和重视网络隐私问题。大数据隐私问题是数字经济发展质量的重要影响因素之一,将对公众对政府等数据拥有者的信任产生深远影响,进而从伦理、技术、管理等层面给政府治理体系、能力建设提出新要求。

基于以上原因,本文针对5G数字经济背景下的政府大数据隐私保护问题进行研究,探讨5G时代数据隐私新特征、大数据隐私保护法律法规对政府大数据治理的影响,提出基于隐私保护的政府大

数据治理模型,以期助力政府数据治理能力提升。

2 5G时代的数据特点及政府大数据隐私新特征

5G将在网络峰值速率、用户体验速率、频谱效率、移动性、网络时延、连接数密度、网络能效以及流量密度8个方面(如图1所示)带来突破性的进展^[4-5]。5G技术的运用在给数字经济发展提供机遇的同时,也带来了数TB、EB的数据,这些数据自身以及应用过程中体现出的特征、这些特征给个人隐私带来的变化、这些变化在政府大数据管理中的体现,是本节讨论的主要内容。

2.1 5G时代数据自身的特点

5G时代数据的特点主要体现为超大规模和强实时性。

(1) 超大规模

5G的特点之一就是可以满足超高连接密度。随着物联网传感器等技术的迅速发展,未来越来越多的物品都将纳入联网序列中。根据应用需求,这些联网物品不断地生产、传输、分析和消费数据,从数据生成主体、数据种类维度方面迅速提升了5G时代的数据量,也为智慧城市、智能交通等新社会治理/应用模式源源不断地贡献新的数据。

(2) 强实时性

5G技术与边缘计算等新技术相结合,使得提供毫秒级低时延的数据服务成为可能,实时特点更加鲜明。在5G时代,数据的有用性与实时性更加紧密相连,很大一部分数据的价值将随着时间的推移迅速降低,如在无人驾驶场景下,高时延将极大降

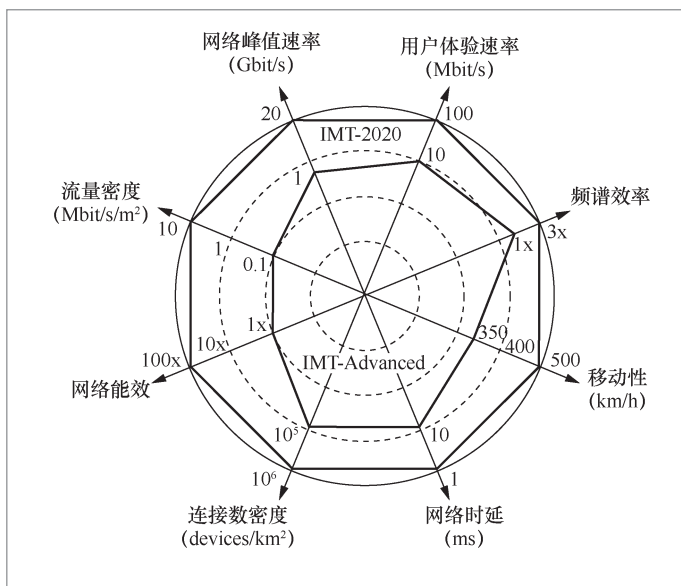


图1 5G IMT-2020 系统性能

低数据的可用性,甚至是带来灾难性的后果,这也给数据治理提出了新的挑战。

2.2 5G时代数据的应用特点

5G时代,数据除自身的特点外,在服务于各类创新性的社会治理模式、商业模式过程中,也呈现出一些突出的新特点,包括高度关联性、处理复杂性、严格安全性、高度流动性、数据资产性。

(1) 高度关联性

5G时代,数据收集的主体、种类、频次等都将有极大的飞跃。更为重要的是,5G时代的数据应用将摒弃以往孤立运用的思维模式,通过在数据集合之间建立更为广泛的关联,打通各类数据集合,通过综合分析挖掘潜在价值,形成价值闭环。例如,在智慧城市的智能交通应用场景下,道路数据、天气数据、车辆行驶数据、交通信号数据等将作为建模的输入,结合人工智能、图像识别、传感等技术通过关联进行综合性分析,进而形成5G时代

应用。

(2) 处理复杂性

5G时代智慧城市、智慧交通等大规模建设给数据提供了更丰富、更多样化的应用场景,也给政府改善治理成果带来新的契机。在新的应用场景中,往往根据需求将人工智能、云计算、物联网、区块链等新技术、新技术单独或结合运用,这也在客观上导致5G时代的数据在分析、处理过程中面临更加复杂的环境,并需要与新技术更有效地结合。

(3) 严格安全性

5G时代给人类带来的变化是前所未有的,但与此同时,随着数据量的爆发以及基于数据的商业模式、管理模式的涌现,由此带来的安全问题也日益突出。例如,从健康角度来看,对病人病情数据的实时收集和监测是一个很大的进步,可以带来医疗福利的极大改善。但是,如果不能很好地保证数据收集、传输、处理的安全,则会给病人带来极大的危险,甚至威胁病人的生命。

(4) 高度流动性

5G时代数据的应用将产生高度的关联,由此将带来数据的流动。例如在《通用数据保护条例》(GDPR)中,欧盟明确规定了数据的可携带权,明确数据主体可以将自身数据从一个数据控制者转移到另一个数据控制者,但是在实践中是否会带来行业的恶性竞争以及是否会给数据管理、政府治理带来挑战,还需要时间的检验。

(5) 数据资产性

随着5G时代的到来,数据作为未来的新能源,作为最重要的基础性资源,得到了政府和企业的高度认同。为了更好地开发这一资源,很多政府部门开始了数据开放化进程,也涌现出了一些数据开放模式,如政府主导的数据开放平台、基于商业的数据交易平台等。数据资产性是一

把双刃剑,利用好数据资产性将带来数据资源利用效益的提升,如处理不当将会对数据主体的安全、隐私产生较大的负面作用,相关的政策、方式方法也正处于探索过程中。

2.3 5G时代的政府大数据隐私新特征

5G时代的数据体现出的特点将反作用于个人信息和隐私数据,并对其产生深远的影响。政府则需要关注5G时代隐私特征的前提下,积极做出调整。5G数据特点及隐私特征关系如图2所示。

(1) 隐私数据密度下降,数量上升

5G时代的数据具有大规模、强实时的特点,数据的数量、种类、非结构化程度以及数据收集的频次、实时性、颗粒度将产生极大幅度的提升,数字经济发展也将在数据处理技术时代进一步释放潜力。在5G技术支持下的大规模数据收集会更多地触及个人信息和隐私信息,虽然这些信息在整体信息中占据的比重会有所降低,但是从绝对数量上看,则会同步大幅增加,给隐私保护带来新的挑战。对于政府治理来说,在智慧城市建设中会更多地收集重点区域的人员、车辆运动轨迹数据,如果结合人工智能(artificial intelligence, AI)面部识别等技术,则会将大量的数据转化为隐私数据(如生物特征数据、身份数据),给与数据相关的主体带来潜在威胁。

(2) 数据高度关联,隐私牵一发而动全身

5G时代众多场景下的应用高度依赖数据的关联操作,这在创造更多价值的同时,也大幅提升了隐私数据的管理难度。对于政府来说,传统分析框架下的数据区隔较为明显,却也将隐私数据限定在了有限的范围和部门内。而在5G时代,更多的数据

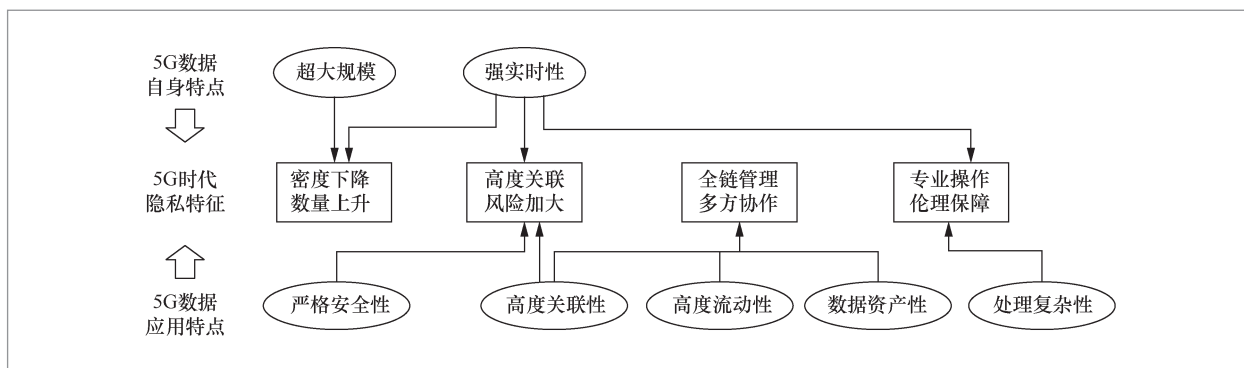


图2 5G数据特点及隐私特征关系

被打通，贯穿使用，与隐私数据关联后的各类数据也很可能变得高度敏感，虽然可以采取脱敏、去标识化等技术在应用过程中加以处理，但由于整体环节众多，隐私泄露潜在威胁点也随之增加。此外，5G时代的数据的准确性、实时性都将产生飞跃的发展，建立于其上的各类应用在满足生产、生活、管理需求的同时，也必将更多地渗入关系国计民生的关键领域（如医疗、健康、金融），一旦隐私数据被泄露，将产生非常严重的后果。

(3) 全产业链管理，多方协作治理

数字经济背景下，数据资源的价值已被充分认可，借助数据流动、数据开放等方式，数据中蕴含的价值可得到更有效的挖掘和发挥。大数据产业链中围绕数据全生命周期各个环节（收集、传输、存储、应用、销毁）的参与者、数据处理者也随之迅速增加，技术更新迭代加快。与此同时，产业链的繁荣也使得隐私保护变得更加复杂，不但涉及各主体的数据合同签约、法律合规、流通评估等事项，更涉及行业标准、资质认定、认证等一系列内容。对于政府来说，一方面需要打通同级部门墙和数据烟囱，加强不同部门之间、中央和地方之间的数据交互；另一方面也需要逐步探索在学术交流、商业应用等方面的数据开放

共享模式。在此过程中，政府单靠自身力量无法满足数据处理、应用建设及运营的所有需求，必然要依靠企业、社会的力量。由于涉及诸多参与主体和环节，需全盘考虑并设计隐私保护机制，以确保个人信息和隐私安全。

(4) 数据处理专业性强，坚守伦理底线

随着AI的快速发展，深度神经网络（deep neural network, DNN）等新技术得到了更广泛的运用。基于AI的数据处理很多是基于黑盒模式的，这会导致非专业人士了解数据处理过程变得非常困难，且容易导致如数据歧视、算法歧视等伦理问题。此外，5G时代数据的实时性更强，一旦误用将造成更加严重的后果。对于政府来说，其职责应是为各服务主体提供公开、公平、公正的服务，应尽量避免产生非正当原因的服务差异性，尤其是涉及个人隐私的服务，要更加谨慎细致。

3 数据法律政策对政府大数据隐私保护影响的分析

隐私保护并非一个新的概念，世界上大部分国家的法律中涉及了此概念，近年

来部分国家或地区制定了针对数据或个人信息保护的专项法律,对数字经济下的隐私保护进行规范和要求。政府作为数字经济活动中重要的参与方之一,其数据管理活动也必须在法律法规的指引下合规进行,因此对国内外最新数据法律进行梳理,对于我国政府大数据管理来说,既有前瞻意义又有借鉴意义。

3.1 部分主要国家/地区的数据保护法律

目前,世界主要国家/地区数据保护法律法规既体现出了一定的共性,同时也因结合了各个国家/地区的自身发展情况、国家意图而有所区别。部分主要国家/地区数据保护政策见表1。

表1 部分主要国家/地区数据保护政策

国家/地区	重要法律	特点	敏感数据/信息界定	是否设立专门监管部门
美国	《隐私法案》1974年生效	立法层面重视公共领域个人数据规制;关注个人数据经济性和价值;各行业、各州制定各自的隐私法律,并鼓励行业自律、认证等机制的制定;随着一系列隐私和个人数据事件的发生,高度关注新技术引发的数据问题	健康数据、财务数据、信用数据;生物特征数据;学生数据、13岁以下儿童的个人数据;可用于进行身份盗窃或欺诈的数据	否
中国	《中华人民共和国网络安全法》2017年生效	明确各政府部门的监管责任;相关条款分散于不同法律中;《数据安全法》《个人信息保护法》等法律还在制定中	一旦泄露、非法提供或滥用就可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息(《信息安全技术个人信息安全规范》 ^[61])	否
俄罗斯	《个人信息保护法》2014年生效	重视数据保护,强调历史沿革;强调个人数据的本地化存储;所有与个人相关的信息均界定为敏感数据	种族、民族、政治见解、宗教和哲学信仰;健康状况、亲密关系、生物特征数据	否
巴西	《通用数据保护法》2020年2月生效	统一数据保护立法,不区分公共和私营部门;基本条款与GDPR有很大程度的相似性;以保护自由和隐私的基本权利及自然人人格的自由发展为立法目的;政府拥有更多自由裁量权	种族或民族血统、宗教信仰、政治见解;贸易同盟、宗教、哲学或政治组织成员;健康或性生活、遗传或生物特征数据	是
印度	《2019年个人数据保护法案(草案)》尚未生效	统一数据保护立法,不区分公共和私营部门;基本条款与GDPR有很大程度的相似性;重视公民利益、贸易和工业利益、国家利益三者平衡	密码、财务数据;身体、生理、心理健康状况;性倾向、病历和病史;生物识别数据	否
南非	《个人信息保护法案(2013)》2018年生效	比照GDPR前身——欧盟1995年颁布的《数据保护指令》制定;不区分公共和私营部门;平衡个人隐私权与信息自由流动	宗教或哲学信仰、种族或族裔血统、工会会员资格、政治说服力;健康或性生活、生物识别数据;犯罪行为数据	否
日本	《个人信息保护法》2017年5月生效	区分个人数据和个人信息;重视个人数据跨境流动	人种、信仰、社会地位、病史、犯罪前科、犯罪被害信息	是
欧洲	《通用数据保护条例》2018年5月生效	欧盟范围内统一框架,又赋予各国家一定的自由度;同时适用于私营和公共机构;强调数据主体权利;政府拥有长臂管辖权;关注新技术运用(如用户画像)	种族、民族、政治观点、宗教和哲学信仰、公会成员身份;具体个人的基因数据、生物识别数据;健康数据、性取向或性经历	是

3.2 当前法律法规对5G时代政府大数据管理中隐私保护的影响

通过前述汇总分析可以看出,各个国家/地区对于数据和隐私保护的立法各有侧重,在政府大数据治理趋势方面产生的影响主要体现在以下几点。

(1) 积极体现国家意志

目前世界对于隐私和数据的治理主要有2种模式:一种是政府强监管模式,另一种是政府与行业的“分治”管理模式^[7]。其中,前者以欧盟为代表,典型的法律包括《通用数据保护条例》,其特点包括强调数据主体权利、加重数据控制者和数据处理者的义务、突出政府的长臂管辖、制定高额罚款等,该法律同时适用于私营和公共机构;后者以美国为代表,立法方面更注重规定政府机关利用数据的行为,对私营机构更多地通过市场化、行业自律方式进行规范与监督,全国不建立统一的私营机构隐私保护法律,鼓励各州结合自身需求因地制宜。

这种分类方式与国家的意图紧密相关。欧洲国家希望通过建立欧盟范围内统一的数据立法,既可以在1995年颁布的《数据保护指令》的基础上统一各个国家的法律,又可以率先建立一个标准和样板,在数字经济竞争中抢占先机。印度、巴西各国希望承接一部分欧洲数字经济产业链环节(如数据分析),实现迅速跟进,但又体现一些自身特色。美国有一些知名互联网公司,采用平衡个人信息保护与科技进步、产业发展的方式,以期在隐私保护和促进发展之间取得平衡。对于政府利用大数据来说,这一特点要求政府在利用大数据时,必须充分分析所在国家的数据和隐私保护政策特点,明确国家意志,同时结合国民对隐私和个人信息的态度、敏感度

以及对政府的信任度等因素,制定综合性的利用机制。

(2) 加强对敏感个人数据、特殊群体数据的管理

在各个国家/地区数据保护的法律法规中,虽然界定稍有差异,但是基本对与隐私紧密相关的敏感数据(如民族、信仰、生物特征、健康、犯罪等信息)进行了界定,对敏感数据的收集、使用、存储等做了更严格的要求。此外,对于一些特殊群体的数据也有单独的阐述,如对儿童数据的收集,各国都做了特殊的规定,有些国家还制定了专门的法规,如中国2019年颁布的《儿童个人信息网络保护规定》,突出强调儿童信息保护。

对于政府来说,要特别注意上述信息和数据主体的隐私保护。以生物特征数据为例,政府公安等部门掌握了公民的面部、指纹等数据,这类数据的特点是无法改变,一旦泄露将给数据主体带来难以挽回的损失。因此在政府大数据治理中,要特别注意对这类数据的保护,保护好数据主体的隐私。同时,政府的教育部门掌握了非常多的未成年人数据,儿童和青少年是国家的未来,关于这类数据国家要充分研究相关政策,同时提高相关部门意识,采取先进的技术、完整的流程进行强有力的保护。

(3) 关注成本性、技术性考量

世界主要国家的最新数据法律政策积极关注了成本与技术问题,订立了一些规则。如在GDPR中,关于个人数据“可携带权”的论述,阐述了需在技术可行、成本可承受范围内实现;同时对自动化决策、用户画像等内容进行了单独的阐释。

如前所述,5G时代的到来将导致数据资源量大幅提高,隐私数据密度降低,但绝对数量提升。政府一方面要积极跟进研究法律中的相关条款,积极分析相关要求

带来的成本变化,提升在数据处理、隐私保护等方面的投资效率;另一方面,要积极研究并运用各种新的技术和工具(如云计算技术、隐私保护工具),结合自身需求,在加强数据处理全生命周期保护的同时,降低单位数据的保护成本。此外,还需要对一些技术(如人工智能等)进行跟踪,分析该项技术给隐私、伦理带来的新变化、新挑战,关注社会上关于这些技术运用的讨论和大众舆情,避免盲目使用给政府带来损害。

(4) 重视数据流通与开放

数字经济的快速发展以及数据产业链的扩展和专业化,使得数据在不同主体、不同地域甚至不同国家之间的流动迅速加快。各国在制定相关政策时,也高度关注数据流通,有些国家制定了专门的跨境流通条款或者法律。另外,自2012年以来,政府部门的数据公开也已经成为趋势,很多国家建立了各自的政府数据公开网站^[8],这给数据保护和隐私保护带来了很大的挑战。

对于政府来说,数据的流通与开放在促进数据价值开发的同时,加大了隐私泄露风险。尤其政府掌握了很多关系国计民生的重要数据和隐私数据,各部门数据在进行数据流通和公开时要特别注意,树立风险管理意识,建立以数据安全为核心的数据保护制度和流程,做好数据流通和开放前的评估、脱敏、使用检测等工作。

(5) 例外条款的规定与运用

各个国家/地区的数据保护法律大多规定了一些例外条款,其中很大一部分涉及公共利益。如在GDPR中,围绕保障公共安全、维护公共利益、保护公共健康等问题,对数据的收集、处理、传输等环节规定了一些例外情况。对于政府来说,其以服务社会大众为目的,其数据收集和处理过程

很大程度上也是为了服务公共安全、公共健康、公共利益,因此可加强对这些例外条款的研究,加强相关内容的运用。

4 5G时代基于隐私的政府大数据管理

隐私保护是一个综合性的系统工程,涉及法律政策、信息技术、受众认知、管理机制等诸多领域。在实践中,随着移动互联网、物联网、云计算、大数据等新技术的兴起,隐私与数据的关系体现得愈加紧密。

4.1 数据管理理论及模型

数据管理并非新理念,一些数据集中的行业(如金融行业、通信行业)很早便高度重视数据的收集与运用,通过建立操作支持系统(operation support system, OSS)、业务支撑系统(business support system, BSS)等对数据进行管理。近些年来,随着社会对数据资源属性的高度认可,数据管理的内涵也逐步丰富。尤其是自2012年以来,越来越多的学者开始结合大数据技术和趋势,探索大数据背景下的数据管理与治理。如从大数据管理信息系统角度,杜小勇等^[9]认为,当前大数据管理系统具有模块化和松耦合的特点,未来大数据管理系统将具有多数据模型并存、多计算模式融合、可伸缩调整、新硬件驱动、自适应调优等特点。从标准体系角度,代红等^[10]在梳理当前中国数据管理和治理标准的基础上,提出了大数据治理标准体系框架以及下一步标准化工作建议。

部分研究机构通过结合企业的操作实践,提出了一系列的数据管理评价

模型^[11-15] (见表2), 为各政府机构、企业评价自身的数据管理水平提供了借鉴。国际上比较典型的几个数据模型包括: 国际数据管理协会(DAMA)提出的数据管理知识体系^[11]、国际信息系统审计与控制协会(ISACA)旗下CMMI研究院提出的数据管理成熟度(DMM)模型^[12]、企业数据管理(EDM)理事会提出的数据管理能力评估模型(DCAM)^[13]等。

部分学者对政府大数据进行了针对性的研究, 研究的角度主要围绕数据治理。根据我国的标准, 数据治理是指“对数据进行处置、格式化和规范化的过程”^[16]。在具体的研究或应用中, 随着数据科学的快速发展, 不同学者从各自角度对“数据管理”和“数据治理”的内涵进行了解读, 两者有时候也会被互换使用, 但一般可以认为数据治理更加倾向于对数据利益相关者关系的梳理, 数据管理涵盖的内容则更趋广泛, 可将数据治理视为整体数据管理的一部分^[11-14]。针对政

府数据的研究, 往往沿用政府治理的理念使用“数据治理”概念, 但研究范围并不限于数据利益相关者、上下游关系描述, 可以扩展至如数据处理、数据分析、技术架构等内容。如范灵俊等^[17]提出, 政府大数据治理需要摸清各部门数据家底, 实现政府大数据融合, 建立内部对接和共享机制以及外部开放模型, 关注数据融合、防泄密与隐私保护、数据定价等技术。安小米等^[18]从宏观层顶层设计要素(概念体系、体系架构)、中观层实施方案(管理机制、信息治理计划、全面质量管理)、微观层落地操作规范(治理主体要求、治理客体要求、治理工具要求)建立了政府大数据治理体系构成框架。张宇杰等^[19]则构建了政府大数据治理成熟度评测指标体系(战略规划、制度保障、组织保障、技术架构、数据管理、治理能力)和政府大数据治理成熟度评测模型。本文更希望使用“数据治理”概念, 建立一个综合性、系统性的政府大数据模型。

表2 数据管理评价模型

名称	核心维度	提出者
数据管理知识体系	数据管理定义、数据伦理与道德、数据治理、数据架构、数据建模与设计、数据存储和操作、数据安全、数据集成与共享、文档与内容管理、参考数据与主数据、数据仓库与商务智能、元数据管理、数据质量、大数据与数据科学、数据管理成熟度评估、数据管理组织和角色、职责	国际数据管理协会
数据管理成熟度模型	数据管理战略(数据管理战略、沟通、数据管理功能、业务案例、项目资助)、数据治理(治理管理、业务词汇、元数据管理)、数据质量(数据质量战略、数据剖析、数据质量评估、数据清洗)、数据运营(数据需求定义、数据生命周期管理、供应商管理)、平台和架构(架构方法、架构标准、数据管理平台、数据集成、历史数据归档及保留)、支撑过程(度量与分析、过程管理、过程质量保证、风险管理、配置管理)	CMMI研究院
数据管理能力评估模型	数据战略、业务案例、流程保障、数据治理、数据架构、技术架构、数据质量、数据生命周期环境	企业数据管理理事会
数据管理能力成熟度评估模型 ^[14]	数据战略、数据治理、数据架构、数据应用、数据安全、数据质量、数据标准、数据生存周期	中国电子技术标准化研究院
数据资产管理主要内容模型 ^[15]	数据标准管理、数据模型管理、元数据管理、主数据管理、数据质量管理、数据安全、数据安全管理、数据价值管理、数据共享管理、制定战略规划、完善组织架构、建立制度体系、设置审计机制、开展培训宣贯	中国信息通信研究院、大数据技术标准推进委员会

4.2 隐私项目管理模型

隐私项目管理主要体现了“通过设计保护隐私”和“默认保护隐私”的理念。通过设计保护隐私是当前国际隐私保护实践推崇的一种理念,于20世纪90年代由经济合作与发展组织(Organization for Economic Cooperation and Development, OECD)提出,强调将隐私保护主动嵌入数据开发与挖掘技术、商业操作、网络架构中,将隐私保护作为数据资源利用的核心问题^[20]。默认保护隐私强调隐私保护应该成为商业流程设计、系统架构的必选项,而不只是一个选择项。GDPR突出强调了通过设计保护隐私和默认保护隐私设计理念的运用,指出隐私保护必须成为组织优先考虑、项目目标、流程设计、操作运营的基本项,必须嵌入每一个标准、协议、流程中^[7]。

国际隐私专家协会(International Association of Privacy Professionals, IAPP)提出了一个隐私项目管理框架,以

助于隐私专家审视自身工作,开展隐私保护工作^[21]。最新一版的框架主要包括9个维度的内容:隐私治理、适用法律法规、数据评估、隐私政策、数据主体权利、培训及感知、保护个人信息、数据泄露事件预防以及项目表现监督和审计。

在标准方面,2019年国际标准化组织提出了ISO/IEC27701^[22],阐释对个人隐私信息管理的要求和指引。

4.3 基于隐私保护的政府大数据治理参考模型

结合上述分析的5G时代大数据隐私特征、主要国家隐私法律政策对政府大数据治理的影响,参考上述数据管理模型、隐私项目管理模型,提出本文基于隐私保护的政府大数据治理参考模型,如图3所示。

本模型包括7个维度。其中,“理念与战略”维度主要从宏观角度,围绕企业隐私保护战略愿景、伦理展开;“数据治理”维度主要从中观角度,对数据利益相关者关系、责任归属、资源支持等治理方面进

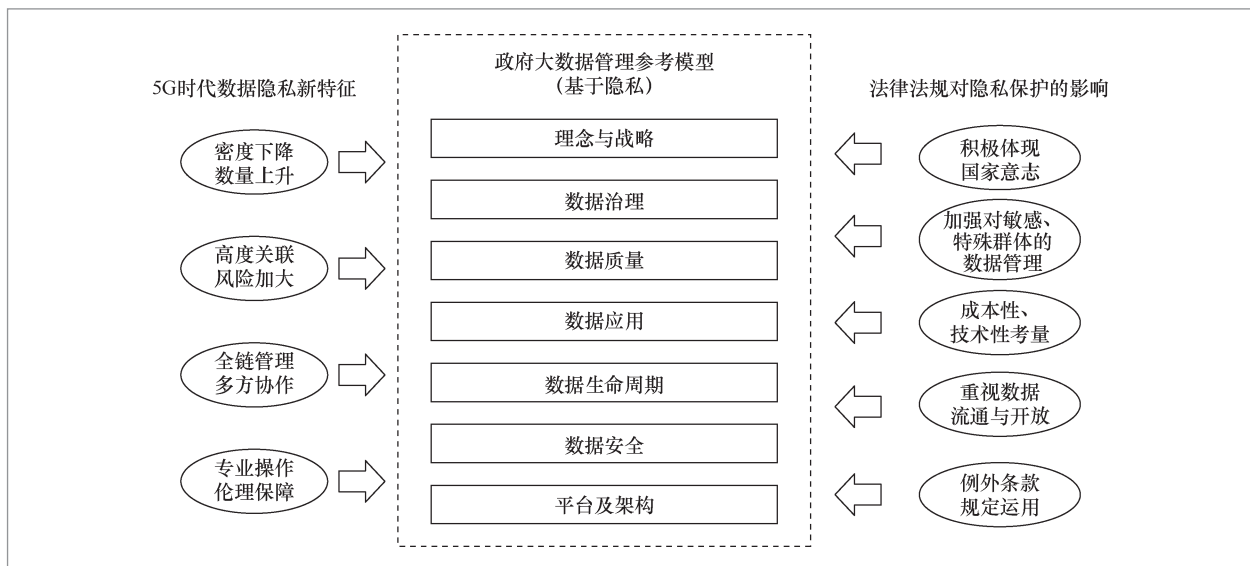


图3 基于隐私保护的政府大数据治理参考模型

行梳理；“数据质量”“数据应用”“数据生命周期”“数据安全”4个维度从微观角度，在数据的收集管理、建模与分析、流通与共享、安全与危机处理等方面对数据管理进行解析；“平台及架构”维度则参照国内外数据管理模型，从技术角度对数据管理涉及的架构、标准等进行分析。

本文模型的7个维度可进一步展开为21个过程域要素，充分参考国内外数据管理模型的核心维度和过程域，尽量涵盖主要维度并降低交叉。同时，结合政府大数据隐私管理需求、隐私项目管理理念及当前重点事件，着重聚焦数据和隐私保护，在每个过程域要素中，贯穿隐私保护理念，并展示出隐私保护的重点关注内容，具体见表3。

政府可以以本文提出的基于隐私保护的政府大数据治理参考模型为基础，结合自身的特征进行优化使用。尤其在当前社会大众对隐私和个人信息关注度不断提升的背景下，可以通过设计隐私保护和默认保护隐私设计理念为指导，突出关注模型中提出的隐私保护主要关注点，从而为社会提供更好的公共服务，不断提升政府大数据治理和运用的能力。

5 结束语

随着5G时代的到来，数字经济迎来了一个高速发展时期。这在给社会、经济带来新动力、新机遇的同时，也会给隐私和个人信息保护带来新挑战，需要政府在大数据管理过程中高度重视。本文首先分析了5G时代大数据特征，并在此基础上总结出5G时代政府大数据隐私新特征。其次，从世界主要国家/地区的数据保护法律入手，分析政策特征，并总结法律法规对5G时代政府大数据隐

私保护的影响。最后，在以上2个分析的基础上，结合主要数据管理模型和隐私项目管理模型，提出了涵盖7个维度、21个过程域要素的政府大数据管理参考模型，并对其中的隐私保护关注点进行了重点阐释，以期在推进国家治理体系和治理能力现代化方面，对政府在5G数字经济背景下的大数据隐私保护和治理能力提升有所助益。

参考文献:

- [1] 中共中央网络安全和信息化委员会办公室. 数字中国建设发展报告(2018年)[R]. 2019. Office of the Central Cyberspace Affairs Commission. Report of digital China construction and development (2018) [R]. 2019.
- [2] G-20 Osaka Summit. Osaka declaration on digital economy[R]. 2019.
- [3] JI Y F, ZHANG J W, XIAO Y M, et al. 5G flexible optical transport networks with large-capacity, low-latency and high-efficiency[J]. China Communications, 2019(5): 19-32.
- [4] Recommendation ITU-R M. 2083-0 IMT vision-framework and overall objectives of the future development of IMT for 2020 and beyond[R]. 2015.
- [5] 京华时报. 国际电联公布5G时间表[J]. 电信工程技术与标准化, 2015, 28(7): 67. Beijing Times. ITU released 5G timetable[J]. Telecom Engineering Technics and Standardization, 2015, 28(7): 67.
- [6] 中华人民共和国国家质量监督检验检疫总局, 全国信息安全标准化技术委员会. 信息安全技术个人信息安全规范: GB/T 35273-2017[S]. 2017. General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, National Information Security Standardization

表3 政府大数据管理参考模型的隐私保护关注点

维度	过程域要素	隐私保护主要关注点
理念与战略	服务愿景 ^[12-14,19]	战略层面认识到隐私保护的重要性； 隐私策略服务国家意志
	道德伦理 ^[11]	符合新技术下的伦理要求； 社会大众认可并接受
数据治理	治理结构 ^[11-15,18-19]	隐私保护嵌入政府大数据治理全程； 专门的隐私保护人员或团队，责任明确
	资源支撑 ^[12]	专门的隐私保护成本预算
	法律保障 ^[12]	对隐私涉及法律法规适用性研究并跟踪
	沟通培训 ^[12,15]	自上而下开展隐私保护公务员培训； 所有人员培训全覆盖，对隐私保护认同
	隐私政策 ^[17,21] 监督审计 ^[12,15,21]	完整、清晰、不断更新的政府网站和App隐私保护条款 对个人信息保护情况进行定期评估； 将隐私保护嵌入审计范畴
数据质量	元数据管理 ^[11-12,15]	特殊敏感数据、特殊服务群体的元数据保护
	主数据管理 ^[11,15]	特殊敏感数据、特殊服务群体的主数据保护
数据应用	数据建模 ^[11-12,15]	5G时代数据高度关联性下的隐私保护； 数据敏感性和隐私信息的转化
	场景应用 ^[12,14]	法律法规对隐私保护在特定场景下的规定； 例外条款中公共利益内容的运用
	技术保障 ^[21]	隐私保护工具和方法跟踪； 隐私保护技术升级方案规划
数据生命周期	流通管理 ^[13]	隐私数据流通必要性评估、接受对象评估； 流通过程中敏感数据的管理（匿名化、脱敏、保密传输等）
	合作方管理 ^[12]	数据提供者、数据处理者等合作方隐私保护水平核实、评估； 合作合同中隐私保护条款制定
	开放与共享 ^[11,15,17]	开放政策的参考与制定； 开放数据种类、开放范围、接受者审核； 是否与其他数据联合形成敏感数据
数据安全	安全管理 ^[11,14-15]	数据存储、传输、分析硬件安全； 信息系统安全； 隐私数据操作权限管理
	风险管理 ^[12,21]	隐私数据泄露事件应对预案； 隐私数据泄露调查方案
平台及架构	架构方法 ^[11-15,19]	系统架构对5G时代超大规模、超低密度隐私数据特征的支持（延展性、自适应调整、响应速度等）
	架构标准 ^[12,14]	ISO/IEC27001、ISO/IEC27002、ISO/IEC27701等标准； 全国信息技术标准化技术委员会大数据系列标准
	中台平台 ^[21]	大数据中台（隐私数据部分）

Technical Committee. Information security technology—personal information security specification: GB/T 35273-2017[S]. 2017.

[7] 京东法律研究院. 欧盟数据宪章:《通用数据保护条例》(GDPR)评述及实务指引[M]. 北京: 法律出版社, 2018.
Jingdong Law Research Institute. EU data

- charter: comments and practical guidance of GDPR[M]. Beijing: Law Press China, 2018.
- [8] 鲍静, 张勇进, 董占广. 我国政府数据开放管理若干基本问题研究[J]. 行政论坛, 2017, 24(1): 25-32.
BAO J, ZHANG Y J, DONG Z G. Research on basic problems for data open management of government[J]. Administrative Forum, 2017, 24(1): 25-32.
- [9] 杜小勇, 卢卫, 张峰. 大数据管理系统的历史、现状与未来[J]. 软件学报, 2019, 30(1): 127-141.
DU X Y, LU W, ZHANG F. History, present, and future of big data management systems[J]. Journal of Software, 2019, 30(1): 127-141.
- [10] 代红, 张群, 尹卓. 大数据治理标准体系研究[J]. 大数据, 2019, 5(3): 47-54.
DAI H, ZHANG Q, YIN Z. Study on big data governance standard system[J]. Big Data Research, 2019, 5(3): 47-54.
- [11] DAMA International. DAMA-DMBOK (2nd edition): data management body of knowledge[M]. Basking Ridge: Technics Publications, 2017: 36-44.
- [12] CMMI Institute. Data management maturity (DMM) model[M]. Pittsburgh: CMMI Institute, 2018.
- [13] EDM Council. EDMC DCAM (version 1.0)[R]. 2015.
- [14] 中华人民共和国国家质量监督检验检疫总局, 全国信息安全标准化技术委员会. 数据管理能力成熟度评估模型: GB/T 36073-2018[S]. 2018.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, National Information Security Standardization Technical Committee. Data management capability maturity assessment model: GB/T 36073-2018[S]. 2018.
- [15] 中国信息通信研究院, 大数据技术标准推进委员会. 数据资产管理实践白皮书(3.0版)[R]. 2018.
CAICT, Big Data Technology and Standards Committee. Data asset management practice white paper (version 3.0) [R]. 2018.
- [16] 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. 信息技术大数据术语: GB/T 35295-2017[S]. 2017.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, National Information Security Standardization Technical Committee. Information technology-big data-terminology: GB/T 35295-2017[S]. 2017.
- [17] 范灵俊, 洪学海, 黄晔, 等. 政府大数据治理的挑战及对策[J]. 大数据, 2016, 2(3): 27-38.
FAN L J, HONG X H, HUANG C, et al. Challenge and countermeasure of governing government big data[J]. Big Data Research, 2016, 2(3): 27-38.
- [18] 安小米, 郭明军, 洪学海, 等. 政府大数据治理体系的框架及其实现的有效路径[J]. 大数据, 2019, 5(3): 3-12.
AN X M, GUO M J, HONG X H, et al. Framework of government big data governance system and effective way of implementation[J]. Big Data Research, 2019, 5(3): 3-12.
- [19] 张宇杰, 安小米, 张国庆. 政府大数据治理的成熟度评测指标体系构建[J]. 情报资料工作, 2018(1): 28-32.
ZHANG Y J, AN X M, ZHANG G Q. Construction of maturity evaluation index system for government big data governance[J]. Information and Documentation Services, 2018(1): 28-32.
- [20] 李延舜. 大数据时代信息隐私的保护问题研究[J]. 河南社会科学, 2017, 25(4): 67-73.
LI Y S. Discussion on the problems of information privacy protection in big data age[J]. Henan Social Sciences, 2017, 25(4): 67-73.
- [21] RUSSELL R D. Privacy program

management: tools for managing privacy within your organization[M]. Portsmouth: IAPP, 2019 .
 [22] ISO. Security techniques — extension

to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — requirements and guidelines: ISO/IEC27701: 2019[S]. 2019.

作者简介



李政 (1983-), 男, 博士, 中国联通国际有限公司高级工程师, 主要研究方向为大数据管理、网络用户隐私、个人信息保护。



洪莹 (1986-), 女, 博士, 北京工商大学商学院讲师, 主要研究方向为网络社区与大数据、网络用户行为、网络用户隐私。

收稿日期: 2020-01-17

基金项目: 教育部人文社科青年基金资助项目 (No.18YJC860010); 国家社科青年基金资助项目 (No. 19CXW034)

Foundation Items: The Social Science Foundation of Ministry of Education of China (No.18YJC860010), The National Social Science Foundation of China(No. 19CXW034)