

数据主权主体论

冉从敬 刘 妍

摘 要 数字经济飞速发展催生数据主权,深刻影响国家数据安全和全球数据治理实践。出于管辖、隐私和商业利益等因素考量,现有研究分别提出了国家、个人和企业三类数据主权归属主体,模糊了国家作为唯一主权者的权威身份。通过追溯历史、分析现状可以发现,个人与企业不可能成为数据主权的行使主体,个人和企业的利益诉求可用个人信息权利、企业数据权利等制度安排以蔽之,无论从性质上还是内容上讲,都不属于数据主权的范畴。对于个人而言,其主权主张滥觞于信息自决权,且个人缺乏对海量数据的掌控能力,个人作为数据的产生者并非理所当然的是数据的所有者和主权者;对于企业而言,其因数据分析和处理能力获取的数据权力使之仅处于支配地位而非法律地位,更不能将其提升至主权地位,企业依旧是被监管者。事实上,自博丹以来的主权学说和国家间主权实践确立了国家不可动摇的主权者地位,在虚拟空间维护国家安全和人民利益的主权责任只有国家能够承担,受新一轮产业技术革命赋能的多元主体作用的提升并未侵蚀主权,相反,国家数据主权在应对新问题、新挑战的过程中获得了增强。

关键词 数据主权;国家主权;信息自决;数据权力;主权责任

中图分类号 D920.0 **文献标识码** A **文章编号** 1672-7320(2024)02-0041-10

基金项目 国家社会科学基金重大项目(21&ZD169)

2022年7月21日,国家互联网信息办公室(以下简称“国家网信办”)依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国行政处罚法》等法律法规,对滴滴全球股份有限公司(以下简称“滴滴公司”)违法过度收集用户数据等问题处以人民币80.26亿元罚款,引发了我国业界和学界对数据安全和数据主权问题的讨论。事实上,早在2021年7月2日,国家网信办就依据《中华人民共和国国家安全法》第九条对意图在美国上市的滴滴公司启动网络审查下架,原因亦是海量数据牵涉到了国家安全、人民利益乃至国家主权问题^[1]。在数据主权热度高涨时,也出现了个人数据主权、企业数据主权和国家数据主权这样的说法,在一定程度上模糊了数据主权的行使主体,乃至错误理解了数据主权的内容、功能和意义,给国家更好地在网络空间开展数据治理和安全建设带来困难。在许多学者眼中,尤其是在法学研究视野下,数据主权的主体当之无愧为国家,但数据主权实乃一个多学科视野下的研究议题,有的学科关注国家职能、国家安全,有的学科关注国际关系、经济效益,不同学科对数据主权行使主体的理解存在事实上的偏差。因此,在理论层面分析数据主权应当作何理解、厘清数据主权的行使主体到底是谁,既是理解实践中类似滴滴公司引发的数据安全事件的重大前提,也是奠定数据主权研究基调、丰富数据主权研究成果的必要探讨。

主权是特定历史条件下的产物,最初是为了维护世俗君主的绝对统治权力、对抗教会权力而提出的,从诞生的那一刻开始就蕴含着政治要求和国家利益。国家利益在不同的时期会有不同的体现,主权相应地也体现出不同的形态。在大数据时代,国家主权衍生发展出了数据主权,即便场景由传统的陆

地、海洋等空间转变到网络空间,但依旧是为了维护国家的发展利益,因此,数据主权的主体不论从历史维度还是理性维度都应当归属于国家。众多学者所强调的企业数据权和个人数据权,的确对有效协调个人数据保护、企业利益维护与国家数据安全及数据主权的繁荣发展发挥着重要意义,但并不能通过解释性的位移越位到数据主权。本文简要回顾了现有数据主权利/力的归属研究,并对个人与企业为何不能作为数据主权主体进行了讨论,对国家作为数据主权主体的地位进行了历史、实践与职能的确认。

一、文献回顾:数据主权的归属主体

法律意义上的主体,是指活跃在法律之中,享有权利、负有义务和承担责任的人或组织。数据主权的归属主体,即数据主权的权利/力行使者和责任承担者。现有研究对谁来享有数据主权存在一定的争议,被称作数据主权主体的一般有个人、企业^①和/或国家,具体如表1所示。

表1 有关数据主权主体归属的观点

序号	归属主体	主要观点	代表性学者
1	个人、企业和国家	数据主权按照数据归属共分三类,即国家(组织机构)数据主权、企业数据主权及个人数据主权	冯伟 ^[2] 、卜学民 ^[3] 、Meriem Rafik ^[4]
2	个人和国家	广义的数据主权包含个人数据主权与国家数据主权,国家数据主权是个人数据主权得以实现的前提,而国家数据主权又依赖于个人数据主权的支撑和表达	Joel P. Trachtman ^[5]
3	国家	数据主权是国家主权在网络空间的自然延伸,因此数据主权的主体理应是国家	蔡翠红 ^[6] 、齐爱民等 ^[7] 、李爱君 ^[8] 、冉从敬等 ^[9] 、Irion et al. ^[10] 、Jin et al., Rainie et al. ^[11]
4	个人	个人所创造的数据属于个人,数据主权是用户完全控制其数据的能力	Sinica Alboaie and Doina Cosovan ^[12] , Krahn and Rietz ^[13]
5	企业	企业对数据市场的影响力增强,是网络空间新的主权者和治理者	翟志勇 ^[14] 、Edmund F. Byrne ^[15]

归纳前人研究,可得出三个结论:第一,现有数据主权归属的观点可以总结为共享主权观、个人数据主权观、企业数据主权观与国家数据主权观。第二,主流观点即便在数据主权具体权能的划分上有所差异,但基本形成了数据主权应当归属国家的共识,即国家数据主权观是国内外学者较为统一的认识。学者们普遍认同数据主权概念的提出乃基于主权国家维护其权威和合法性的需求,数据主权是一个国家独立自主对本国数据进行管理和利用的权力,而依据一直以来的国家主权实践,数据主权不外乎是国家主权在网络空间的自然延伸。第三,在学者们对数据主权权属主体进行划分的时候,也隐含地揭示了保留各种价值观的数据主权内涵。一种认为数据主权是权力,是引导数据流和(或)管理数据资源的能力;一种认为数据主权基本上相当于使个人能够发展控制个人数据所需的相关能力;也有的认为数据主权是国家的经济利益和在网络空间的发展利益;还有一种将数据主权等同于无视数据隐私权的数据殖民主义工具^[16]。

具体展开这些观点,可以发现,主张共享主权观的,即认为数据主权应当在多个主体之间共享的,是将数据主权看作公民社会或合作经济协会中的参与者制定的原则和实践,因此,认为这种数据的新兴价

① 在本文中,企业指的是拥有海量数据的实体,亦可以称作数据公司、数据巨头企业、数据企业等等,为了行文方便,以企业作为以上概念的统称。

值应当被共同持有,而非私有化^[17]。但事实上数据主权是一个不可分割的实体,不存在共享主权的情况,分割主权就是毁灭主权,主权只能有单一主体,能在多个主体间共享的就不是主权。

主张个人数据主权观的,一是十分重视个人作为个人数据来源主体的地位,认为数据的来源和数据的归属从理论上讲理应是同一个主体,即个人;二是出于对数据安全风险的焦虑,譬如Krahn认为,个人数据已经遭到了广泛披露,引发了较大风险,泄露后的个人数据也很难再界定个人对其的所有权,因此,应更加关注消费者对自身数据主权的主观体验,从而实现数字自决^[13];三是基于数据利用的便利性考量,譬如Sinica认为,当前政府和大数据企业对个人信息的收集、存储和共享行为便利了政府和企业的行动,但却并没有便利于个人,当人们需要获得某项存储在第三方的个人信息时需要访问多个链接,进行多重操作,且在此过程中又遗留下了新的数据,阻碍了个人对自己数据的使用、撤销、删除等控制行为^[12]。

主张企业数据主权观的,一是认为现今企业的数据收集、存储和处理能力非常强,已经成为数据世界的实际支配者,并将这样的数据能力或数据商业能力视作企业的数据主权^[14];二是认为企业对这些数据的加工和处理生产出了海量的新数据、新产品,企业对此具有所有权;三是由于算法技术的衍生作用,企业积累了许多数据优势和经济优势,通过这些优势企业可以对用户进行精准推送,利用其平台“操纵”个人的选择,同时企业也获得了一定程度的事实上的规则制定权、行政执法权甚至纠纷裁判权,成为一种新类型的“国家”,因此,企业应当作为数据主权的主体或者主体之一。

本文认为,数据主权的主体有且仅有一个,那就是国家。首先,将数据主权作为共享主权的理论将牵扯出系列复杂的问题:这几类数据主权的效力如何?是否具有相同的法律效果?几者的优先性又应当如何安排?当这几类数据主权产生冲突时适用什么法律来保护、调解和裁决?其次,个人数据主权观和企业数据主权观乃是混淆了数据主权与信息自决权、数据主权与数据财产权。事实上,数据主权是公法意义上的概念,既不是私法上的财产权,也不是个体意义上的人格尊严。最后,从本质上思考,个人对数据主权的“欲”能转化成“能”吗?企业的数据能力是否等于数据主权?个人和企业又是否拥有承担数据主权相关责任的能力?主权从古至今的本质是否体现了让渡给个人和企业的可能性和必要性?国家在网络空间的数据主权实践又是怎样的体现?回答这些问题,就能够廓清数据主权到底归属哪一行为主体。

二、个人作为数据主权主体之不能

对数据的控制和自决是个人数据主权观的核心主张,但个人是否有能力对数据进行有效控制、个人的这种数据产出是否能当然地获得数据上的权利,以及这种权利是不是数据主权,都是值得考虑的问题。这些问题的答案也直接揭示了个人在事实上和法律上都不会是数据主权的主体。

(一) 个人数据主权滥觞于信息自决权

世界各国普遍认为,个人作为数据主体一方,政府和企业对其个人数据的处理应当尊重其个人意志,因此赋予了个人知情权、决定权、查阅权、复制权、更正权、补充权和删除权等权利,这些权利保证了个人能有效决定和监督其个人数据的处理活动,从理论上可归溯到信息自决。当前之所以有个人数据主权、公民数据主权的说法,实际上是混淆了主权与自主权^[9],在信息自决视野下提出的个人数据主权本质是在谈论基于数据自主的个人数据保护、控制、利用,隶属于个人数据权利体系,而非主权理论体系。从范畴来讲,个人数据权利是建立在数据主权体系之下的。

信息自决权是一般人格权的一部分。1984年,德国联邦宪法法院在“人口普查案”中以司法判例的方式确立了信息自决权的宪法地位,这也是信息自决权在世界范围内首次获得国家法律的确定。从理论上讲,个人信息自决权的具体主张是对所有个人信息的控制权,个人可以决定向谁告知哪些和他相关的信息、哪些可以隐瞒,本质上保护的是个人信息之上承载的人格权益^[18]。换言之,信息自决权的设置

是为了赋予个人对其数据一定程度的控制权,其逻辑在于个人信息作为个人事务应当由个人来自我决定,目的在于保护个人信息权益、维护个人尊严和决定自由,但这并非是给予个人对数据的治理权或所有权,或者说在法律上赋予个人所谓的个人数据主权。一方面,数据主权实际上是公法层次的概念,而个人信息自决权的消极救济一般通过私法实现。譬如,人格尊严和自由可以通过侵权救济予以实现,而个人信息权利的主动行使,如个人信息的开发利用,则更多与企业等主体有关,个人对其数据的经济利益通常通过合同等市场行为来调解分配,而非通过设置所谓的个人数据主权来让个人去决定和管理流通中的个人数据。另一方面,主权并不是信息自决所谓控制权、所有权的概念,而是以平等权、独立权、管辖权和自卫权等作为内容,个人数据主权的提法本身就存在性质上的谬误。

(二) 个人缺乏对海量数据的控制能力

如果个人是数据主权的主体,那么个人应当对其数据具有最基本的控制能力,但是在实践中,个人对其数据既不足以控制,也不可能控制。

其一,个人没有技术能力或场地设施处理海量数据,缺乏对数据的事实控制。数据主权是大数据时代的产物,作为一种数据类型,大数据是指其大小和规模超出一般数据库的数据集,对其收集、存储和处理需要具备较强的数据管理和分析能力,不论是从数据量还是数据管理难度方面,远非人力可以完成。而数据价值产出依赖于数据收集者或者平台企业的大数据应用,个人缺乏对数据的加工利用能力,凭借个人的力量难以挖掘数据的价值。

其二,个人数据所涉主体众多,难以有效确定归属主体,个人不享有排他支配的权利。从概念上讲,个人数据是识别特定个人的信息,而识别个人是社会交往和运营的工具,因此,个人信息并非属于个人所有^[19],或者说,个人数据作为人际交流和表达的产物,一诞生就带有一定的公共属性^[20],并且实践中很多个人数据从一开始就具有共有的性质,这些数据无法独立赋权给某个人。譬如,医疗数据源于个人,形成于为患者提供诊疗过程中医疗机构的采集、制作和保管。对于患者而言,医疗数据是对患者健康状况的记录、描述或反映;对于医疗机构而言,医疗数据是其为患者提供诊疗服务的记录,是医疗机构的一种重要资源。因此,很难说个人对其数据享有绝对控制的权利。

其三,个人对其数据的控制不是数据主权所指向的控制,数据主权视野下的控制、管辖具有特别的功能,可以实现社会认知效果、社会行为干涉效果或整个社会的治理效果。在面对数据主权的这种工具价值时,个人既没有控制海量数据的条件,也没有实现数据主权多重价值的能力,自然无法承受数据主权的主体地位。

(三) 个人数据产生者不等同于主权者

认为个人拥有数据主权的观点,大多数遵循着个人是数据的来源“主体”因而应当具备个人数据主权这一逻辑,然而这里存在三个问题:个人作为数据主体不一定是数据的生产主体,也不一定就是个人数据所有者,同时个人数据并不能够完全组成数据主权范围内的数据。

其一,个人一般只是数据的来源者或者说产生者,而不涉及数据如何生成。数据的来源(产生)与生产是两个概念,来源于个人的数据并不意味着一定是个人生产的,只有个人在提供或创制了数据时才是数据的生产者,数据生产者是对数据生产作出实际贡献的主体,这些贡献包括设计数据采集工具设备或系统、进行数据采集工作等^[21]。质言之,数据生产是将客观事物数据化的过程,个人更多的时候是作为这一被记录、被分析的客观事物对象,因此个人更应当被理解为数据的产生主体,而非数据的生产主体。

其二,数据产生者或者数据生产者也很难被认为是数据的所有者。前文已述,个人作为数据主体面临着个人数据公有和共有的困境,使其无法成为个人数据的所有者,而数据生产者同样面临数据共有的问题,并且数据生产者的生产行为或者说劳动行为并不一定就能够获得法律上的权利。现有立法实际上已经对这一结论给出了很多类似的规定,如专利法中的职务发明规则。职务发明制度对劳动成果管理的多元化推动了权属机制从法定向约定的转变,国家可以通过奖酬等各种替代性措施调整生产与获

得不平衡,可以利用法律规范重塑社会关系,这种被重塑的社会关系反过来又夯实了法律规范。

其三,个人、个人数据和个人数据行为仅仅是数据主权所管辖范围的很小一部分,个人缺乏作为数据主权主体的基础。从构成要素来看,数据主权既囊括了构成网络物理构造的网络基础设施,又包括数据本身、参与其中的数据主体,以及衍生出的数据行为。数据主权在各要素中都得到彰显,是对网络基础设施、数据本身、数据主体和数据行为的主权。其中的数据构成要素是各类能够用于表达、存储、加工和传输的电磁信号,以及与电磁信号产生交互的量子信号、生物信号等。因此,在数据主权语境下的数据自然包括个人所产生和生产的数据,但更多的是组织运营、机器生产的数据。从数据主权的广度来看,个人掌握的数据是有限的,而数据主权是一种大数据主权,大数据的体积、规模、速度和种类非常巨大,涉及经济、文化、航空、海事等各个产业和社会发展的方方面面,不仅仅是个人数据,因此,个人作为数据主权的主体是不完备的。

三、企业作为数据主权主体之不能

在数字经济场景下,企业的数据产品、数据推销已经渗透于人们的经济活动和社会生活中,许多跨国企业给国家司法管辖带来了难题。企业数据主权说认为,企业的数据能力使得企业应当得到主权的分享,企业享有数据主权并行使治理权力。但从企业的主体性质和替代性的治理方式来看,企业不能也没有必要成为数据主权的主体。

(一) 企业的数据权力是支配地位而非法律地位

对企业作为数据主权主体的最大误解,是将企业与用户基于契约关系发生的系列服务行为、推荐行为和一定程度的大数据监控和操纵行为错当成国家权力般的管辖和控制,混淆了支配与权威。实际上,当人们使用企业权力的时候,是将“权力”界定为一种社会学概念——其表示的是实际支配,而非法律地位^[22]。

虽然非国家行为体越来越重要、企业数据权力越来越大,但从法治层面来讲,国家依旧对他们具有决定性的影响,这些商业主体仍受国家多方面的规制。以数据跨境为例,企业的数据跨境行为需要在主权国家的法律框架内进行,受到主权国家的规范和制约、接受和认可,违反本国数据规则的企业将受到惩罚。因此,从主体层面而言,全球数字经济的推动者和主导力量仍然是国家,企业只是能够发挥主观能动性的被调整的对象。从国家的根本属性来看,主权是历史和时代的产物,是政治、法律、经济和文化的统一体,并不仅仅只由经济的发展所决定。长久以来,主权的内涵随着时代的发展得到充分的延伸和拓展,动态演进成一个内容不断扩充的权能束体系,形成了一个综合性的主权权力概念。主权权能不再局限于政治、军事和外交领域,更是扩充到文化、环境(自然资源)和经济等方面,形成了文化主权、环境主权和经济主权等新的主权权力^[23],现在的网络主权、数据主权也是主权在数字时代全新的弹性表现。在经济领域中,从国际法渊源来看,1974年联合国大会通过的《建立国际经济新秩序宣言》和《各国经济权利和义务宪章》都充分表明,东道国对于本国境内的一切经济活动享有完整的、永久的主权,对境内外国有资本和跨国公司也享有管理监督权。因此,本国数据企业所进行的经济活动理所当然地受到国家的监管和控制,企业对数据的获得和拥有并不能使其超越主权框架获得主权者身份,而是受到国家经济政策的监督和指导。

(二) 企业数据权力的增强并非主权地位的取得

全球化时代商业能力强大的跨国企业,其数据权力的获得是数据驱动时代数字经济蓬勃发展的结果,其发生与发展具有时代的因素,是人类文明向前迈进的象征,而非企业获得国家主权地位的体现。将企业数据权力的兴起视作主权削弱论的根基,与20世纪七八十年代初期自由主义相互依赖理论质疑全球化侵蚀了国家主权的观点十分相似。当时,自由主义相互依赖理论认为二战后占主流观点的现实主义理论(国家是至高无上的,主权及主权国家是一个既定的前提假设)是失效的,理由是全球化的政治

经济世界中存在着多个行为体,而国家只是其中一个,非国家行为体在资本、货物、文化全球化的过程中发挥着重要的作用,有的甚至直接参与到国际政治和经济活动中,削弱了国家主权^[24]。然而,这是仅仅将国家主权视为对其资源客体实际掌握、控制的结果,换言之,仅仅关注到了国家主权的权能,却忽视了主权首先体现为身份权威——主权还是一个界定和表征着主体地位、身份关系的范畴^[23],就如同 Thomson 所言,“主权不是有关国家控制的,而是有关于国家权威”^[25]。因此,从发展的眼光来看,不只是网络空间的无国界性冲淡了国家边界,全球化也导致过类似的结果,也不只是大数据时代才有非国家行为体的兴起与权力扩张,全球化时代跨国公司的资本雄起也产生过类似的结果。自 1500 年马克思提出现代资本主义和华勒斯坦提出现代世界体系以来,世界很长时间都处于相互依赖、相互影响的整合化的趋势中,无论是跨国、跨区域贸易还是文化交流,都未曾真正削弱过国家主权;相反,国家主权在一次次技术挑战与环境变化中发展演进,塑造成了一个更加稳定和经得起考验的国家主权。

(三) 企业作为“权力者”祛魅后的被监管者身份

法治社会对权力的第一要求,便是权力必须由国家法律授予和确定,这可以解决权力来源的合法性问题^[26],如果权力可以随时获得或者依据所谓的数据能力获得,既不符合法治要求,也会造成权力紊乱,影响数据主权的有效行使,并给滥用权力埋下隐患。现在许多学者提到,企业在网络空间治理中的角色经历了中介、参与者、私权力主体和守门人、私人监管者的演变历程,基于企业的大数据分析处理能力和对人民生活的影响能力,应当赋予其网络监管者的地位,或者在一定程度上获取国家数据主权的治理权威,这一问题既是数据主权问题,也是法律设置合理性的问题。“如无必要、勿增实体”,否则运用一个含义不确定甚至模糊的概念进行理论和实务的表达,极易造成概念的混乱和资源的浪费,导致理论研究呈现出“新瓶装旧酒”“热闹而不深刻”的现象^[27]。

当前,规制私权力有反垄断、公司治理、公用事业监管等多种手段,且已有相关实践,如今赋予企业数据主权的观点乃是下策。国家目前对网络空间难以一一触及的事务,在事实上也给企业赋予了一定的数据治理权限,如平台规则的制定权、执行权和对用户在平台上违规行为的处罚权等,但这并非给予企业什么监管者的地位,更不是对国家权威的侵蚀,国家将部分数据治理权下放给企业实际上是坚持和强调主权本质的体现,而不是削弱或放弃主权。进一步从本质上讲,将企业权力发生学的治理问题视作数据主权之身份资格问题的误解,实际上是对企业的经济活动以及主权的认识都不够全面。将企业权力扩张导致其对数据的掌控能力、对公民生活的干涉能力增强的现象看作权力者地位的获得,仍是自由经济发展中的形变,并不能撼动政治根基,自然也无法将企业的地位上升到统治者或主权者。就如同第二次工业革命后铁路等新公用事业的兴起垄断了市场上绝大部分经济利益,但铁路公司在整个国家政治体系来说仍是受监管者而非监管者,其经济活动受到反垄断法和反不正当竞争法的规制。因此,在面向企业利用跨业务整合能力获得过度的经济和政治权力的“新布兰代斯运动”中,关键不是赋予企业当下流行的数据守门人地位或者主权者地位,而是应当探讨如何在已有的框架内更好地对其进行监管。

四、国家作为数据主权当然主体的理性确认

从历史和国家主权实践来看,无论技术如何发展、参与主体如何多元,也无论是谈论信息主权、网络主权抑或是数据主权,都不外乎是国家主权在不同社会时代和技术背景下的弹性延伸,其主体永远都是国家,权能由国家行使。

(一) 博丹以来的主权学说对国家主权原则的确立

追溯主权理论,可以明晰古今中外主权的主体经历了哪些流变、又是如何默契地确定国家主权原则作为最重要的国际关系原则的。

主权学说的起源可追溯到亚里士多德的《政治学》以及古典罗马法,前者承认国家中必定存在最高权力,且该权力可以由多人掌控,后者认为国王的意志具有法律的力量。首次系统讨论主权本质的是法

国学者让·博丹,他将主权定义为“国家绝对和永久的权力”,认为君主是主权的代表,其本人也因此成为法国君主制赖以建立的主权学说的创立者。后来的学者对博丹的君主主权学说予以了驳斥,阿尔瑟修斯在其《政治学的系统考察中》指出,主权是“管理通常事关国家成员之灵与肉之安全与福利等事务最高和最普遍的权力”,而这一权力属于人民,人民是主权永久的适格主体^[28](P7-9)。胡果·格劳秀斯的《战争与和平法》介于博丹的专制主义学说与阿尔瑟修斯的反君主主义学说之间,认为国家是主权的拥有者,这开始接近国家主权观念^[28](P10-12)。其后,英国学者托马斯·霍布斯将君主主权推向极致,比博丹的君主主权学说更为绝对化。约翰·洛克和让·雅克·卢梭则反对君主主权,认为人民是主权的真正拥有者。纵观这一阶段,总的趋势是维护统治者的政治权利,而对国家主权的适当阐述缺少;之后,黑格尔塑造的崇高国家观念在许多政论家手中得到有机性的解释,主权最终赋予了被看作最具有有机人格属性的国家^[28](P77)。换言之,主权的权力归属在历史上已产生诸多学说间的激辩,也有许多正反面论据或支撑、或否定国家作为主权者的身份,最终支持人民主权、君主主权的观念被支持国家主权的理念取代,国家主权理论得到历史的承认与现实的巩固。

国家主权原则同样是国际普遍承认的约束国际关系的原则。国家这一政体最初兴起于欧洲,第一批兴起于13世纪中叶到15世纪下半叶的西欧,而到17世纪上半叶得到巩固,二战后国家主权原则在危机中涅槃前进,迈出欧洲走向世界,成为指导国际关系的最关键原则。在此之后,国家主权原则经历了全球化、信息技术革命、跨国公司兴起、自由主义相互依赖理论等情景和理论的挑战,由主权国家来组成国际社会成为当前世界政治中唯一被普遍接受且由实践检验最为实用的规范^[24]。我们当前所处的大数据时代固然有与全球化时代不同的特征,但本质上都是出现了新的主体挑战或权威挑战,长久以来确立的主权的最高统治权威和独立管辖权能始终没有被国际社会放弃,拥有主权的国家仍是当今世界经济和国际关系中最基本的行为主体,实践证明了国家主权原则是最经得起考验的国际原则^[29]。国家主权不是一成不变的价值观念,其内涵和结构都在随着国际环境的变换而不断调整,但不变的是主权仍旧是构成国家的合法性基础、是国际法和国际关系的准则。

(二) 国家主权原则在网络空间进一步增强

认为企业或者国际组织等非国家主体实力的扩张削弱了国家主权的观点也是不成立的。从当前的现实来看,不同国家的经济政治实力和数字技术能力虽有很大的不同,数字化转型的战略目标也有很大差异,但没有任何国家宣布放弃自己在网络空间的主权;相反,俄罗斯等国家通过一系列网络安全立法收紧国家对数据的整体控制,强化了数据主权,我国也希望与国际社会一道,尊重网络主权。即便是最开始强调网络自由且一直没有官方承认网络空间主权或数据主权称谓的美国,也在以实际行动巩固本国数据主权——以“进攻型”的长臂管辖扩张其跨境数据司法权^[30]。换言之,各国在主权受到企业数据能力增强以及他国数据管辖权力外溢的时候,也在通过各种手段强化国内外主权意识和主张,增强国家数据主权能力。与此同时,各国在本国内部主权维护方面,力度还在不断增强,主要体现在运用多种方式提高本国政治、经济、法律和文化力量上。譬如,我国从接入互联网开始就高度重视网络空间的政治问题,党的十八大明确提出了完善国家安全战略和工作机制、高度关注网络空间安全和健全信息安全保障体系等主张;2021年颁布的《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》也多方位规定了数据跨境流动的规则和规范,并对数据控制者的权责做了详细规定;2022年党的二十大报告再次强调,要推动形成良好网络生态,将我国建设成网络强国。美国近年通过的《澄清域外合法使用数据法案》(The Clarifying Lawful Overseas Use of Data Act,又称《云法案》)、《统一个人数据保护法》(Uniform Personal Data Protection Act,UPDPA)等立法,对数据收集控制者、第三方控制者和处理者赋予了更加明确的责任,强化了管辖权在网络空间的行使。日本也在2021年颁布了《跨境数据流动指南》,进一步细化了信息流动的事项和程序,严格保护个人信息、网络安全和知识产权。

可见,各国都在积极通过立法、行政或司法措施明确表明自身主权不容侵犯的立场,在政治、经济或

社会领域都加强了努力,致力于提高政府的数字服务效能、加强政府对数字经济的监督和引导、协调对外政策和数据跨境问题。在这样的背景下,全球互联互通的数字化与其说削弱了国家的数据主权,还不如说是增强了各国政府的责任,各国政府在充分分析本国国情和政策现状的基础上,都积极采用适当的监管手段有效地行使数据主权。换言之,国家数据主权并未得到削弱,而是在提升应变对新问题、新挑战能力的同时获得了加强,各国的网络空间治理实践也通过对数据主权的认同强化了主权在网络空间的合法性。

(三) 国家是能够承担网络空间主权责任的唯一主体

如前所述,主权不仅仅是一种权力,也是一种责任,是国家承担的对国内人民和国际社会的责任,这些责任包括保护人权、维护国际和平与安全、捍卫国家领土完整和促进国际经济健康发展等^[23],而这些责任只有国家有能力承担。个人、企业是国家数据主权责任的受益者而非承担方^①,在国家积极承担主权责任的情况下,个人隐私权益得以保障,企业参与全球数字经济市场的机会得以保留,个人与企业在网络空间的其他权利得以充分实现。实际上,国与国之间的贸易行为、政治文化行为也在国家主权责任的承担中得以正常有序开展。这意味着国家主体身份建构的存续与数据主权利力行使和责任承担是相互作用的,国家是当然的数据主权主体。

从国际层面来讲,数据主权毫无疑问地已经成为许多希望重返大国赛场的国家的新战马^[4]。欧洲联盟因此积极开展《跨大西洋数据隐私框架》(Trans-Atlantic Data Privacy Framework)谈判,不断在网络空间部署数据主权战略,颁布GDPR、《数字市场法》《欧洲数字主权》《塑造欧洲的数字未来》等数据法案或数据战略。俄罗斯政府则于2019年出台《主权互联网法》(Sovereign Internet Law)加强互联网控制审查,维护国内数据安全和主权独立。印度政府则在2020年初通过禁止TikTok软件的使用,以控制国内数据跨境传输风险。美国也在积极践行网络空间主权,在其毗邻国家间“拉帮结派”,签署了一系列条约实现有利于己的数据流动和不利于他的数据封锁,如《全球跨境隐私规则声明》(Cross-Border Privacy Rules)、《互联网未来宣言》(A Declaration for the Future of the Internet),这些文件的签署者包括英国、加拿大、以色列、中国台湾、乌克兰等美国军事盟友及经济伙伴。以上案例一方面是国家作为数据主权主体在网络空间的主权实践,另一方面也暗涌着各国在网络空间的数据博弈。在这些场景下,只有国家具有参与国家间谈判、合作和治理的实力与勇气。尤其是在网络冲突日益严峻并上升至网络战的背景下,国家是唯一能够进行队伍组织和财政资源支持的行为体。换言之,在遇到严峻网络空间数据主权风险的情况下,只有国家才能承担安全和治理的关键责任。从主权责任的效果来看,数据主权的设立是为了实现一定的功能,譬如通过构建数据跨境制度发展繁荣本国数字经济、保护本国数据安全,并与其他国家实现规则上的融洽发展;或者通过营造一个健康有序的网络文化空间,引导本国人民进行健康友善的网络活动,促进网络文化繁荣发展;或者通过全球数据主权共识创造全球网络空间命运共同体、分工治理网络犯罪等大数据时代的新兴刑事问题,通过跨境司法合作完成跨国数据调取。因此,数据主权具有政治功能、经济功能、文化功能和社会治理功能,这些价值和功能显然是个人或者企业无法有能力实现的。

主权的设置是为了维护国家利益,数据主权的兴起在于它比传统的政治形式更能够承担促进社会、文化,尤其是经济现代化的职责和使命。正如立法权、行政权、司法权并不构成主权的本身而仅仅是主权的某些方面、主权的某些属性,是最高权力的派生物,数字时代国家在网络空间的治理权也仅仅是国家主权在内容上的拓展,即便有众多主体参与,也带来了诸多与以往所不同的挑战。但国家作为数据主

① 当然,国家数据主权责任的充分实现很多时候需要企业和个人等多方主体的配合,国家作为主权责任的唯一主体并不代表国家是主权治理的唯一主体。在实践中,国家可以通过“主权让渡”的方式来更好地承担国家治理任务。一般认为,主权的身份不可让渡,但其权能可以让渡,是主权国家为了最大化国家利益以及促进国家间关系良性互动和国际合作的工具。

权主体这一基本性质和属性不会变,主权的最高权力主体只有一个,那就是国家。从亚里士多德伊始,主权学说经历了君主主权、人民主权、教会主权、国家主权的流变,政治家、学者、各国宪法实践得出的结论均警示我们,主权是完整的、不可分割的、统一的,数字企业、数据巨头的经济能力再强、对公民日常生活的影响再大,也不可能获得作为主权者的权力。当然,本文所探讨的数据主权主体的唯一性并非代表数据主权本身的绝对性,数据主权是相对的和受限的,具有与生俱来的弹性,这体现在国家参与全球网络治理层面。在明确数据主权的权力和责任主体之外,数据主权的价值实际上还有待在各国的国际实践和国内实践中予以挖掘,如何共治数据主权风险、携手共建网络空间命运共同体是下一步亟待讨论的议题。

参考文献

- [1] 冉从敬. 数据主权治理的全球态势与中国应对. 人民论坛, 2022, (4).
- [2] 冯伟, 梅越. 大数据时代, 数据主权主沉浮. 信息安全与通信保密, 2015, (6).
- [3] 卜学民. 论数据本地化模式的反思与制度构建. 情报理论与实践, 2021, (12).
- [4] Rafik Meriem. *Data Sovereignty: New Challenges for Diplomacy, Artificial Intelligence and Digital Diplomacy: Challenges and Opportunities*. Cham: Springer International Publishing, 2021.
- [5] Joel P. Trachtman. Cyberspace, Modernism, Jurisdiction and Sovereignty. *Indiana Journal of Global Legal Studies*, 1998, 5(2).
- [6] 蔡翠红. 云时代数据主权概念及其运用前景. 现代国际关系, 2013, (12).
- [7] 齐爱民, 盘佳. 数据权、数据主权的确立与大数据保护的基本原则. 苏州大学学报(哲学社会科学版), 2015, (1).
- [8] 李爱君. 数据权利属性与法律特征. 东方法学, 2018, (3).
- [9] 冉从敬, 刘妍. 数据主权的理论谱系. 武汉大学学报(哲学社会科学版), 2022, (6).
- [10] Irion Kristina. Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, 2015, 4(3).
- [11] Stephanie Carroll Rainie, Jennifer Lee Schultz, Eileen Briggs, et al. Data As a Strategic Resource: Self-Determination, Governance and the Data Challenge for Indigenous Nations in the United States. *International Indigenous Policy Journal*, 2017, 8(2).
- [12] Sinică Alboae, Doina Cosovan. *Private Data System Enabling Self-Sovereign Storage Managed By Executable Choreographies*. IFIP International Conference on Distributed Applications and Interoperable Systems. Cham: Springer International Publishing, 2017.
- [13] Britta Krahn, Christian Rietz. *Digital Marketplaces Unleashed*. Berlin: Springer, 2018.
- [14] 翟志勇. 数据主权时代的治理新秩序. 读书, 2021, (6).
- [15] Edmund F. Byrne. In Lieu of a Sovereignty Shield, Multinational Corporations Should Be Responsible for the Harm They Cause. *Journal of Business Ethics*, 2014, 124(4).
- [16] Hummel Patrik, Braun Matthias, Tretter Max, et al. Data Sovereignty: A Review. *Big Data & Society*, 2021, 8(1).
- [17] Fraser Alistair. Land Grab/Data Grab: Precision Agriculture and Its New Horizons. *The Journal of Peasant Studies*, 2019, 46(5).
- [18] 杨芳. 个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体. 比较法研究, 2015, (6).
- [19] 高富平. 论个人信息保护的目的一——以个人信息保护法益区分为核心. 社会科学文摘, 2019, (3).
- [20] 关儒, 吴晓祺. 大数据时代个人信息的公共属性. 民主与法制时报, 2020-08-02.
- [21] 高富平. 数据生产理论——数据资源权利配置的基础理论. 交大法学, 2019, (4).
- [22] 刘晗. 平台权力的发生学——网络社会的再中心化机制. 文化纵横, 2021, (1).
- [23] 赵洲. 主权责任论. 北京: 法律出版社, 2010.
- [24] 任丙强. 全球化、国家主权与公共政策. 北京: 北京大学出版社, 2007.
- [25] Janice E. Thomson. State Sovereignty in International Relations: Bridging the Gap Between Theory and Empirical Research. *International Studies Quarterly*, 1995, 39(2).
- [26] 刘作翔. 法治社会中的权力和权利定位. 法学研究, 1996, (4).

- [27] 张志铭, 赵轩毅. 未来法治植根何处: 一种分析进路的概念省察. 国家检察官学院学报, 2022, (1).
- [28] 小查尔斯·爱德华·梅里亚姆. 卢梭以来的主权学说史. 北京: 法律出版社, 2006.
- [29] 黄仁伟, 刘杰. 国家主权新论. 北京: 时事出版社, 2004.
- [30] 孙祁, 尤利娅·哈里托诺娃. 数据主权背景下俄罗斯数据跨境流动的立法特点及趋势. 俄罗斯研究, 2022, (2).

The Owner of Data Sovereignty

Ran Congjing, Liu Yan (Wuhan University)

Abstract The rapid development of the digital economy has given rise to data sovereignty, which has profoundly affected national data security and global data governance practices. Due to different considerations such as jurisdiction, privacy and commercial interests, existing research has proposed three types of data sovereignty entities: the state, individuals and enterprises, which blurs the authoritative identity of the state as the sole sovereign. By tracing back history and analyzing the current situation, we can find that individuals and enterprises cannot become the subjects of exercising data sovereignty. The interests of individuals and enterprises can be covered by institutional arrangements such as personal information rights and enterprise data rights, both in terms of nature and content. None of them fall into the category of data sovereignty. At the individual level, their sovereignty claims originate from the right to information self-determination, and individuals cannot control massive data. As the generator of data, individuals are not the owners and sovereigns of the data. At the enterprise level, their claims are based on their data analysis and processing capabilities. The data power only puts it in a dominant position rather than a legal status, let alone raising it to a sovereign status. Enterprises are still regulated. In fact, the doctrine of sovereignty and the practice of inter-state sovereignty since Bodin has established the unshakable status of the state as a sovereign. Only the state can assume the sovereign responsibility of safeguarding national security and people's interests in the virtual space. Endowed by the new round of industrial and technological revolution, The enhancement of the role of multiple capable subjects has not eroded sovereignty. On the contrary, national data sovereignty has been enhanced in the process of responding to new problems and challenges.

Key words data sovereignty; national sovereignty; information self-determination; data rights; sovereign responsibility

-
- 作者简介 冉从敬, 武汉大学信息管理学院教授, 湖北 武汉 430072;
刘 妍, 武汉大学信息管理学院博士研究生。
- 责任编辑 桂 莉