【信息管理】

基于CLOUD法案的美国数据主权战略解读

黄海瑛 何梦婷

【摘 要】在竞争日益激烈的国际网络空间中，数据主权治理边界愈发模糊，各主权国家积极展开数据主权战略建设，保障本国数据主权安全。美国于2018年3月通过了CLOUD法案，力图通过法案解决跨境数据流动中的安全威胁，维护国家数据主权，对此法案进行研究对于提升我国数据主权战略、完善我国数据战略体系具有重要意义。本文全面剖析CLOUD法案，解读其基本内容，探讨其核心目标和构建模式。在此基础上，对比我国与美国数据主权战略建设现状，发现我国数据主权战略以“网络主权”为原则、以发展为核心诉求、以国家权力机关为核心主体、自上而下多级建设等特征。同时，借鉴CLOUD法案，从宏观顶层设计指导、考察具体管辖方略、促进国际数据交流、协作治理网络空间等方面对我国数据主权战略体系提出了建议。

【关 键 词】CLOUD法案；数据主权；战略体系；跨境数据流动；网络空间；数据安全

【作者简介】黄海瑛，武汉大学信息管理学院，博士，副教授，研究方向为数字人文、欧美制度与文化、语言大数据等，E-mail：huanghaiying@163com；何梦婷，武汉大学信息管理学院，博士生，研究方向为数据主权、政府大数据等，E-mail：hoomtwhu@163.com（武汉 430072）。

【原文出处】《信息资源管理学报》（武汉），2019.2.34～45

【基金项目】本文系教育部人文社科重点研究基地重大项目“大数据资源的制度规制和国家治理研究”（17JJD870001）和国家社会科学基金重大项目“健全国家大数据主权的安全体系研究”（国家十九大专项）（18VSJ034）的成果之一。

随着数据主权重要性的不断凸显，在秩序与自由、发展与安全的博弈下，如何保障本国主权安全、占据数据主权竞争优势成为各国关注的热点。当前，各主权国家已开始通过立法、立规、司法及行政实践等丰富方式，打造以数据主权为核心的新国家安全战略体系，力图保障本国主权不受侵犯，同时提升在国际数据争夺中的话语权。其中，美国的数据主权战略发展最早，以130余部关联法案形成了当今国际最为完备的数据主权战略体系。美国于2018年发布的《澄清域外合法使用数据法案》（*Clarifying Lawful Overseas Use of Data Act*，简称CLOUD法案）最为突出地体现了美国在新信息环境下的战略新选择，标识了未来美国数据主权战略的发展方向。

本文着重剖析CLOUD法案，解读其核心内容与关键目标，探索其战略模式，以此为切入点形成对国际数据主权战略发展实践的全方位认知。在此基础上，对比我国当前的数据主权治理实践，思考我国数据主权战略体系的模式选择和发展不足，借鉴相关战略，提出针对性建议，为我国在新信息时代下的数据主权战略体系建设提供理论支撑和实践指导。

1 数据主权的兴起

主权理论的阐释与现代领土国家的诞生是同步的[1]。传统的国家主权概念总是与地理空间因素相关联，而互联网技术的出现，将国家疆域扩展到了网络空间，传统物理主权观念难以应对新技术冲击，主权理论由此延伸至虚拟的网络世界。云计算和大数据的发展，进一步催生“网络主权”完成至“数据主权”的嬗变，这对新时代背景下国际法和国际秩序的构建都产生了深层次的影响。基于对数据主权演化过程的分析，本文认为数据主权在全球范围内的兴起，主要是基于以下4个方面的核心背景。

1.1 后棱镜时代全球数据安全焦虑呼吁数据主权回归

2013年6月，美国“棱镜”(PRISM)秘密监控项目曝光，即美国国家安全局(NSA)和联邦调查局(FBI)直接与微软、雅虎、谷歌等跨国网络巨头合作，通过这些公司的服务器直接挖掘数据、获取情报。“棱镜”计划在国际社会引起巨大争议，全球由此陷入数据安全焦虑。网络空间在发展历程中，一直将主权国家视为对立面，标榜“绝对自由”，反对将现实空间的任何政府管制延伸至网络空间。“棱镜门”将国家数据安全和个人隐私安全危机暴露出来，传统的依靠企业等非国家权力主体的“自律”和互联网行业的“行业标准”实现网络空间“自我监管”的治理方式已经被全方位宣告无效，数据主权的介入成为对抗数据霸权和捍卫国家安全的必然出路。在此背景下，“数据主权”概念在全球网络空间回归，各国纷纷开始加快数据立法，如欧盟、俄罗斯、澳大利亚、巴西等，力图通过数据本地化、数据流通限制等方式，捍卫数据主权。

1.2 网络技术与数据流动对国家主权现有体系的冲击

互联网技术的迅速普及，极大扩展了公众的信息获取渠道，使得海量信息获取成为可能。新信息时代的到来也使得主权国家难以对信息的产生和利用进行有效的控制和管理，主权国家的信息安全面临巨大的威胁。同时，技术的发展带来了数据的跨境流动，在跨境流动的过程中，数据存储、管理、利用的主体都发生了变化[2]，这使得“国家疆界”变得模糊，国际数据跨境流动中的管辖权重叠纠纷屡见不鲜。当前尚未出现国际通用的数据跨境流动规则，国际冲突中缺乏国际规则予以制约，各主权国家以自身国家利益出发争取数据管辖权，国家主权治理进一步趋向复杂。在虚拟空间，适用于现实领域的法律体系已远不能满足对其调整和规制的需求，现有的主权规制体系面临着巨大冲击，亟待重构和扩展，以应对新信息环境下的新问题。

1.3 恐怖主义与霸权主义为数据主权治理提供了正当性诉求

信息技术本质只是作为一种应用工具存在，但信息技术对国家政治、经济、文化的全面渗透使得其成为恐怖主义的新武器。恐怖主义势力利用信息网络，将网络空间瞄准为新的攻击目标，网络恐怖主义成为破坏各主权国家的日常运行、社会稳定、国家安全的重要风险之一。同时，以美欧为代表的网络优势国家，依托其技术优势，积极争夺全球数据资源，推行网络霸权主义，大肆扩展其数据主权边界，不断威胁其他主权国家的数据主权。网络恐怖主义和霸权主义的肆虐，使得网络空间迫切需要数据主权的规制，运用法律来应对严峻的主权风险问题，避免网络空间成为不受控制的法外之地。

2013年4月，北约正式发布《塔林手册》(*Tallinn Manual*)，指出“国家有权对其主权领土范围内的网络基础设施和网络行为实施控制，对他国的网络基础设施进行的任何干涉都是对主权的侵犯”[3]。2013年6月，第6次联合国大会通过联合国“从国际安全的角度来看信息和电信领域发展政府专家组”(UNGGE)所形成的决议的第20条规定“国家主权和源自主权的国际规范和原则适用于国家进行的信息通信技术活动，以及国家在其领土内对信息通信技术基础设施的管辖权”[4]，实际确认了网络空间中国家主权的存在。2017年2月出版的《可适用于网络行动的国际法的塔林手册2.0版》(*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*)第1条“主权(一般原则)”明确否定了网络空间“全球公域说”，认为“尽管(全球公域)定性在法律之外的方面可能是有用的，国际专家组并不接受这一定性，原因是它忽略了网络空间和网络行动中那些涉及主权原则的地域属性”[5]。

主权概念在全球安全焦虑的背景下，必须回应新兴信息技术和信息行为的冲击，同时，恐怖主义、霸权主义的直接侵犯为主权国家全方位介入网络空间提供了正当性理由，应对互联网新阶段下新的主权问题成为当今世界的核心议题之一。

1.4 数据主权问题已经引起学术界关注

学术界尚未对“数据主权”提出统一的定义。但“数据主权”的存在及其重要性已经通过国内外的各类国际协议、国家法律得到承认，且其内涵不断被完善。数据主权概念自提出之时，就因其与地理区域

和国家政治的紧密联系，而与数据的跨境流动密不分可。目前的大数据主权研究中，相当多的研究从全局视角研究数据跨境的相关问题。Meltzer认为主权国家应制定新的数据贸易规则，进一步规范互联网及跨境数据流动[6]。Syuntyurenko探讨了新的信息技术在社会交往和社会制度发展中的影响[7]。Paladi等人讨论了由不同的司法管辖区和数据所有者的数据争论带来的云数据的地理定位问题[8]。Vulimiri等人针对广域大数据(WABD)的跨数据中心的数据传递与数据主权限制不兼容的问题，提出了一系列解决方案[9]。Shin根据个人信息跨境流动，从管理和体制方面研究政府、企业和个人作为利益相关者如何解决数据安全问题[10]。Mosch等人提出了r-Cloud个人安全云的建设方案，力图解决现有的云解决方案在个人数据主权问题上的安全隐患，使得用户可保障自身数据的主权安全[11]。Anna关注俄罗斯与欧盟在云服务上的系统建设开发与国家政策制定，总结俄罗斯公民在云服务上的个人数据处理问题[12]。总的来看，目前的大数据主权研究处于起步阶段，但已经引起了学术界的广泛关注。

2 各国数据主权治理模式分析

信息技术和互联网的发展冲击了传统的主权观念，随着信息流动加速和网络安全风险的不断凸显，国家数据治理、国家主权安全及公民个人数据保护面临的严峻挑战要求必须要在网络空间“再主权化”。各主权国家对数据资源的价值与意义已经形成共识，新一轮的大国竞争焦点已转向了通过大数据资源增强对世界局势的影响力和主导权，国家间围绕数据所有权和利用的博弈愈演愈烈，各国的数据主权治理实践也越来越凸显出其重要性。

在近年来的网络空间主权维护实践中，国际主流考虑以国家概念为元点，结合信息主权的理论基石——主权论的内涵，着力思考主权国家如何对跨境数据流动进行管制，从而逐步扩展并形成数据主权战略发展的三种核心模式。

2.1 强主权模式：完全独立自主管制

依据《联合国宪章》第2条和联合国大会相关决议，国际社会逐步形成对“未经主权国家的同意，信息在主权国家内外的流动都属于侵犯国家主权”这一观点的广泛认知。这一观点使得主权国家在实施自身数据主权权利时，可不受“人权”观点的束缚，完全自主管制数据信息。强主权模式下，国家对于信息的流动拥有强有力的控制权，可对数据流通设置完善的准入和监控标准。

强主权模式可带来数据主权的极端加强，相应地减少数据主权风险，一定程度上保障国家的数据主权安全。但同时，随着新型信息传输工具出现，国际信息来源及流量显著增加，信息流动大大加快。在新的信息环境下，数据主权也不断暴露出其弊端。一方面，新信息技术的广泛运用，使得跨境信息流动难以被完全监控；另一方面，强主权下每一信息都需“本地存储”和“使用批准”的话将带来巨大的行政和司法成本，从而一定程度地降低数据流动效率。

2.2 弱主权模式：一定程度独立管制

弱主权模式的核心为“国家的正当性支撑着主权的合法性”，即认为一国法律可干预或管制数据跨境流动的前提是，该国家在其领土范围内尊重人权并进行民主治理。

弱主权模式的核心与数据主权诞生的理论基础紧密关联。与传统物理主权相同，国家的数据主权实质来源于公民共同让渡的权利。权利与权力复合，在主权国家的行使下，数据主权由此诞生。同时，根据社会契约理论，由于数据主权来源于社会大众的共同权利让渡，因此数据主权在行使中必须保障社会大众的基本利益，使得社会大众可以更好地实现自身的权利。由此可见，数据主权的诞生有其深厚的道德理论基础，即：社会大众的权利让渡使得主权国家必须对数据流动予以管制，且主权国家的管制行为也需要予以限制，保证国家在权利实施中不影响社会大众的权利行使与利益保障。这种权利赋予与限制的道德理论即为弱主权模式的核心主张——主权国家只有尊重人权并实行民主政治，才有资格对数据流动予以管制。虽然弱主权模式在赋予国家管制数据权利的理论基础上具有创新，且在理论上极大尊重了广大社会公众的权利，但实质上，当我们以公民为独立个人而不是法律抽象的概念来重新衡量弱主权模式时，会发现其存在着理论上的诸多短板，且无法在实践上得到落实。

2.3 程序主义模式:通过公平程序管制

程序主义模式关注各主权主体之间的直接交互,认为无论是在现实空间或虚拟空间,数据主权都不应受到空间的约束,而是应通过各主权主体在交互的过程中被不断定义与扩展。在数据主权的保护和规制问题上,程序主义认为必须要通过主权国家积极参与国际交互、通过制定国际决定的公平程序予以解决。同时,在通过公平程序做出国际决定时,无论主权国家的国力强弱,各国的主权和诉求都应被公平反映。在实施中,程序主义也同样要求,通过公平程序做出的国际决定,无论是否与主权国家的偏好相符,都应得到参与制定国家的认可和执行。程序主义追求公平、正义的理论核心有其进步性,强调国际合作与交互的管制方式也与大数据环境下的数据主权治理实践相符,但其忽视了各主权国家在长期的政治经济发展过程中积累的实质不平等对国际决策程序的影响,过于强调程序上的公平而忽略实质公平问题。程序主义追求的无分强弱、公平公正地均能反映各主权国家利益诉求的"程序公平"难以落实到实践中。

3 CLOUD法案解读与数据主权战略模式分析

美国的数据主权安全保障及其战略建设起步于20世纪80年代,作为全球最早开始建设数据主权战略的国家,至今已形成130余部相关的法案制度,打造了涵盖互联网宏观整体规范及微观具体规定等各方面的完备数据主权战略体系。在这庞大的数据主权战略体系中,CLOUD法案以其产生背景、立法目的、形成模式具有突出的代表意义。

3.1 CLOUD法案的立法目标

美国国会于2018年3月紧急通过了CLOUD法案,对"微软公司诉合众国案"(Microsoft Corp. v. United States)提出了针对性的解决方案:"无论通信、记录或其他信息是否存储在美国境内,只要上述通信内容、记录或其他信息为该服务提供者所拥有、监护或控制,服务提供者均应当按照本法所规定的义务要求,保存、备份、披露通信内容、记录或其他信息。"[13]该法案对美国此前的系列数据主权法案做出了针对性的补充修正,紧急回应此案中暴露出的跨境数据流通中的主权风险问题,围绕美国数据主权核心利益,主要力图达成如下3个层次的核心目标。

(1)解决数据主权新问题,完善现有战略体系

美国紧急推出CLOUD法案的直接目的是为了修改1986年生效的《存储通信法案》(*Stored Communications Act*,SCA)。SCA没有明确美国政府搜查令能否要求通信服务商提交其存储在境外的数据,在此关键问题上的模糊,直接导致"微软公司诉合众国案"中长达4年的法律争议。CLOUD法案面向美国在跨境访问数据中出现的新问题,解决了在执法所需的数据恰好存储在国外和外国执法机构需要访问存储在美国的数据这两个数据流动场景中的关键主权问题,并提出了解决方案。CLOUD法案的出台,直接解决了微软一案的核心争端,同时面向新问题,修改了现有战略体系中关于跨境数据获取和利用的漏洞,进一步完善了现有战略体系。

(2)保障对本国数据的域外控制能力,扩张数据主权效力范畴

"微软公司诉合众国案"一案在美国数据搜查令的域外效力这一核心议题上,暴露出了美国现有跨境执法协助机制难以满足跨境调取数据执法需求的现实问题。CLOUD法案之前,美国执法部门一般依靠条约、协定、警方间的合作这三种途径访问存储于其他国家的数据。但现有途径和法律存在覆盖范围小、行政程序复杂,同时处理成本高的问题,并不能满足当前跨境调取数据的执法需求。美国急需制定新的法案来弥补当前的法律弊端,加快数据调取进程,满足美国跨境调取数据的执法需求,从而保障美国对于本国数据的域外控制能力。CLOUD法案重新确认了美国对本国数据在境外的控制能力和主权所有,同时,依靠这一法案,美国在其企业、机构的助力下,实际扩张了其数据主权的效力范畴,长臂管辖至各主权国家的境内范畴,美国的数据主权得到进一步强化。

(3)对抗境外数据本地化浪潮,争夺国际数据资源

互联网浪潮下,新的大国竞争实质上已演变为围绕数据占有和利用的博弈。数据博弈中,为应对来自美国的严重威胁,以欧盟、俄罗斯为代表的主权国家,均在其数据战略中强调实施本地化存储和扩展域外管辖权,力图通过强制数据本地化存储、强制

反加密制度、单方面主张域外管辖权等多项政策防范美国的信息监控和数据垄断，加强对本国数据的控制权，削弱美国在全球数据争夺中的优势。其他国家的一系列数据本地化和数据域外管辖的行动直接威胁到了美国在全球数据主权竞争中的优势地位，美国迫切需要扩展其国际数据资源争夺渠道，强化其数据资源获取能力，保障其数据主权安全。CLOUD法案为美国争夺境外数据提供了法理和渠道支撑，从而进一步提升了美国对抗境外数据本地化浪潮的能力，有效地巩固了美国在国际数据资源争夺中的优势。

3.2 CLOUD法案解读

CLOUD法案有针对性地改革了美国的数据主权战略体系，共分为101～106六条，其主体内容实质为102～105的四个条文。

3.2.1 102条解读：立法原因及考虑因素

第102条明确指出CLOUD法案的考虑因素主要为：①及时获取通信服务提供商持有的电子数据是政府保护公共安全和打击包括恐怖主义在内的重大犯罪的关键；②因无法获取境外储存的数据，政府打击重大犯罪的努力受到阻碍，而监管、控制或拥有这些数据的通信服务提供者本身受到美国法律的管辖；③为了打击重大犯罪，他国政府也越来越多地要求获取美国通信服务提供者的数据；④当他国政府要求通信服务提供者提供美国法律可能禁止披露的数据时，通信服务提供者面临着潜在的法律义务冲突；⑤按照美国法典第18卷第121章(通称为《存储通信法》SCA)的规定，美国要求披露他国法律禁止通信服务提供者披露的电子数据时，同样可能会造成类似的相互冲突的法律义务；⑥美国与相关外国政府对法治和保护隐私做出相同承诺和达成国际协定中，包含了解决潜在冲突的法律义务机制。

从102条的规定可以明晰CLOUD法案的主要考量因素。当前美国互联网企业在提供网络产品和服务方面优势地位明显，因此存在许多国家向美国申请调取数据而不得的情况，同时当前美国的数据获取申请处理速度也无法满足国际数据获取的需求。另一方面，美国向其他国家调取数据也需通过双边司法协助途径，而不直接面向企业。因此，如何在这个时代里，充分利用数据来减少犯罪，打击恐怖主义，推动全球数据协作，这是美国法案中提到的立法的考量目标。

3.2.2 103条解读：美国信息记录的保存规则

CLOUD法案采用“数据控制者标准”，明确：“无论通信、记录或其他信息是否存储在美国境内，服务提供者均应当按照本章所规定的义务要求保存、备份、披露通信内容、记录或其他信息，只要上述通信内容、记录或其他信息为该服务提供者所拥有、监管或控制。”[14]同时，CLOUD法案也提供“抗辩”渠道，规定当服务提供者可在以下情形下提出“撤销或修正法律流程的动议”：①对象不是“美国人”(the United States Persons)且不在美国居住；②提供数据将为服务提供者带来违反“适格外国政府”(qualifying foreign governments)立法的实质性风险[15]。同时，对于“抗辩”的处理，CLOUD法案设置了严格的“礼让分析”(comity analysis)规则，明确“动议”处理的3种核心情形和7个核心考虑要点。考虑到技术边界的不确定性，CLOUD法案进一步添加主体锚点(必须为电子通信服务和提供商或远程计算服务提供商这两类科技公司)与行为锚点(拥有、保管、或控制数据)，进一步强化CLOUD法案的实施稳定性。

CLOUD法案进一步发展了《存储通信法案》(SCA)，在数据主权的效力边界问题上，明确地采取了“数据控制者标准”，使得数据主权可以超出传统范畴限定，从物理上的空间边界，延伸至技术上的控制边界，即以数据的实际技术控制者为效力对象予以划定主权的效力边界。同时，由于数据的实际技术控制者标准存在其不确定性，CLOUD法案进一步添加主体因素和行为因素作为锚点，增强法案实施的稳定性。

3.2.3 105条解读：外国政府获取存储于美国境内数据的规则

CLOUD法案允许“适格外国政府”可以基于与美国的行政协定，直接向美国境内的相关组织获取数据。CLOUD法案主要通过对“适格外国政府”的资格认定和“发布命令”的严格限制，明确外国政府对存储在美国境内数据的获取规则。在对“适格外国政府”的认定上，基于“外国政府的国内立法，包括

对其国内法的执行，是否提供了对隐私和公民权利足够的保护”[14]这一核心准绳，要求外国政府必须符合如下核心因素：①在网络犯罪和电子证据方面，拥有充分的实质性、程序性法律，加入了《布达佩斯网络犯罪公约》或其国内法与该公约相关内容吻合；②遵守国际人权义务或展现出对国际人权的尊重；③展现出对全球信息自由流动和维护互联网开放的决心和承诺。同时，对于发布的命令内容，设置了如不得有意地针对“美国人”或位于美国境内的个人、不得在美国政府或其他第三国政府的要求下发出命令等细致且严格的限制，要求“适格外国政府”向美国提供互相访问数据和定期审核的权利，且规定美国可保留停止外国政府获取数据命令的权利。

CLOUD法案在明确美国获取存储于境外的数据的权利同时，也充分考虑到了国际社会的平衡，设置了“适格外国政府”对美国境内数据的获取规则。但通过对第105条法案内容的解读，可以发现，CLOUD法案对“适格外国政府”的资格认定和获取行为都有严格的限制，同时强制要求外国政府承认美国数据自由思想和开放数据权利给美国政府，从而实际反向进一步强化了美国数据霸权优势，拓宽了美国的数据主权在其境外的效力和实施范畴。

3.3 CLOUD法案的数据主权战略模式选择

20世纪80年代，美国的数据主权战略建设实践逐渐起步，随后通过密集立法不断完善，当前已建设完成较为完善的数据主权战略体系。1998年，美国政府发布《保护美国关键基础设施总统令》，从国家层面明确对数据主权战略的关注；2000年，颁布《美国国家安全战略报告》，数据安全被纳入国家安全战略中；2001年，“9·11”恐怖袭击事件后，《爱国者法案》应运而生，网络和信息安全成为国家安全领域的关注热点，对企业及个人信息的监控和审查大大强化；2003年，《网络空间国家安全战略》颁布，数据主权被正式列入国家安全战略之中。总的来说，美国是全球最早制定数据主权战略的国家，其数据主权战略体系内容丰富，综合了各主体、各方面的战略需求，同时随着环境变化不断进行方向转换和调试，不断纳入新的手段和方法，由此形成了独具特色的数据主权战略体系。

CLOUD法案是美国在新的数据跨境流动背景下的数据主权战略新选择，该法案的公布，进一步扩大了美国的数据主权范畴，并有向数据霸权演化的趋势，美国新信息环境下的数据主权战略模式的轮廓进一步变得清晰。通过与前文国际数据主权战略建设的对比和战略模式的分析，基于如下核心特征，本文将CLOUD法案总结为创新性的“非对等强主权治理模式”。

(1)强主权：以维护美国利益为核心，保障数据主权的域外控制能力

CLOUD法案的直接催生因素即为微软一案，法案始终是以美国的数据主权利益诉求为核心的。法案首先解决在数据跨境流通新背景下的新主权问题，同时基于本案暴露出的数据主权漏洞，进一步强化数据主权体系。CLOUD法案中，美国诉求是完全独立自主地严格管理本国的跨境数据流动，以主要篇幅确定了美国对存储于其域外的数据资源的所有权和管辖权，法案基本上允许美国从世界任何地方获取任何数据。在解决跨境数据调用中出现的核心矛盾的同时，法案进一步对美国的数据主权进行强化保护，为其他国家利用美国数据设置屏障，创造监视和利用他国数据的机会。

CLOUD法案的实质即为进一步强化的强主权治理模式。表面上，此法案直接丰富了政府间跨国数据获取渠道和模式，但更多地，基于强主权治理模式，法案对美国数据流通设置了完善的准入和监控标准，结合美国网络服务商和设备提供商的市场优势，进一步强化了美国对其自身数据的控制和境外管辖，确保了美国对于信息的流动拥有强有力的控制权，极大地保障了其数据主权优势。

(2)非对等：表面“互惠”兼顾数据流动，实质扩张数据主权至他国领域

CLOUD法案的核心是提供美国调取域外数据的法律基础和制度渠道，同时也考虑到互惠原则，允许满足一定条件的“适格外国政府”调取位于美国境内的数据，并为此消除了程序障碍。为平衡美国政府与“适格外国政府”间的关系，CLOUD法案中增添了一系列限制和平衡的补救措施。但通过对比可发现，法案以较大的篇幅，对“适格外国政府”获取存储

于美国的电子数据披露进行了极其细致的法律限制,但关于美国执法部门通过数据披露程序获取境外电子数据的法律限制的介绍就极其简单,实际上并没有充分落实法案中所谓的“互惠”(reciprocal)理念。

首先,法案要求任何撤销或变更的动议都必须符合美国利益。CLOUD法案中对动议程序设定的发起理由仅有两点,并有严格的时间限制,还新增了“个案考量”的因素,即在不会影响美国利益的情况下才可撤销或变更法律程序。其次,CLOUD法案并未根本性地提高外国政府调取美国数据的效率。借助CLOUD法案,美国的境外数据管控和数据主权治理效率大大提升,反之,当外国政府要求调取美国数据时会发现,尽管CLOUD法案已缩减此前法律规定的烦琐程序,但各项资格审核、实质性检视、听证、审查等步骤仍相当烦琐和复杂。而真正通过CLOUD法案“互惠”审核的国家,必须同时接受开放本国数据权利给美国并同意美国政府定期开展的审核。综上,无论从实体上还是程序上,CLOUD法案中对外国政府调取存储于美国的数据都更为复杂,权利内容和实施方式的改变实质上都仍是为了将美国数据主权扩张到其他国家的主权管辖范围之中。

4 CLOUD法案对中国的战略借鉴

2019年2月,中国互联网络信息中心(CNNIC)发布第43次《中国互联网络发展状况统计报告》。报告显示,截至2018年12月,我国网民规模为8.29亿,其中手机网民占比达98.6%,互联网普及率达59.6%[16]。我国互联网蓬勃发展,互联网越来越深入渗透人民群众日常生活,大数据、人工智能、物联网等前沿科技和产业服务被列入国家重点发展方向。

数据资源的跨境流动越来越频繁,数据开放共享与安全保护的博弈越来越激烈,敏感数据的情报萃取、反渗透、反窃密等数据主权保护行为越来越频繁。随着大数据、云计算、物联网、区块链和人工智能等新技术新应用的跨越式融合发展,在国际国内挑战的双重压力背景下,我国数据主权治理的国际环境日趋复杂,治理难度也逐步升级。本文力图以CLOUD法案为切入口,深入探析美国数据主权战略核心内容与发展模式,结合我国实际发展情况,思考我国数据主权发展方向和战略构建建议,为我国增强数据主权竞争实力、保障数据主权安全提供理论和实践支撑。

4.1 中国的数据主权选择

我国对网络安全的认知起步较早,最早在1996年的《中国公用计算机互联网国际联网管理办法》中就提到要加强对网络的管理。但对将网络安全上升到国家安全层次,将数据安全与国家主权结合起来的认知则发展较晚,在2010年后才开始有所论及,并直到2015年的《国家安全法》才首次提出了法律上的“网络空间主权”的概念,明确提出要“维护国家网络空间主权、安全和发展利益”。回顾我国的数据主权治理历程,我国当前尚未有统一的数据主权法律,主要通过各项数据保护、网络安全法律进行分散立法(见表1)。

表1　　我国数据主权战略立法实践

时间	治理实践	战略内涵
1996	《中国公用计算机互联网国际联网管理办法》	加强对互联网国际联网的管理,促进信息交流的健康发展
1997	《计算机信息网络系统安全保密管理暂行规定》	核心在于保护计算机信息系统处理的相关国家秘密安全
2000	《互联网电子公告服务管理规定》	制定电子公告服务提供者在开展相关活动时应遵守的相关规定
2002	《中国互联网行业自律公约》	旨在规范从业者行为,依法促进和保障互联网行业健康发展
2006	《信息安全等级保护管理方法》	旨在划分信息安全等级规范与标准,指导信息安全主管部门的信息安全等级保护管理工作
2010	《中国互联网状况》白皮书	明确我国境内的互联网属于我国主权管辖范围,全面介绍中国互联网发展的基本情况
2015	《国家安全法》	首次提出并规范了我国法律上的“网络空间主权”的概念
2016	《国家网络安全战略》	表明我国维护国家网络安全和数据主权的坚定决心,阐述我国的数据主权原则
2017	《网络安全法》	我国首部关于网络安全基础性、大纲性的法律,代表着我国网络和信息安全保护法律体系发展到一个新阶段

这其中，以2017年6月1日正式实施的《网络安全法》最为核心。《网络安全法》展现出了我国坚决捍卫国家网络安全和数据主权的决心，是我国对于网络安全的首部全面指导性的法律法规。相对于其他类型细分领域法规制度，《网络安全法》展现出更多的基础性、针对性、大纲性的特征，明确表达了我国的“网络空间主权原则”，也同时制定了如在关键信息基础设施安全保护、相关重要数据跨境流动等数据主权核心安全问题上的治理规则。以《网络安全法》为代表，我国的数据主权战略建设开始向着体系化方向发展，并开始不断强化对我国数据主权治理目标和治理诉求的宣示，这也预示着今后数据主权战略体系的建设将成为我国网络空间建设的核心议题。

以《网络安全法》为核心，本文将我国的数据主权战略制度与美国对比，可以发现我国的数据主权战略建设具有如下核心特点：

(1)以“网络主权”为核心战略原则，以发展为核心战略诉求

与美国的“网络自由”口号不同，我国始终坚持“网络主权”战略原则，聚焦大国战略互信，倡导国际社会应广泛合作，共同解决网络空间治理难题、协作推进全球网络空间治理体系的变革，共同打造安全、开放的国际网络空间。以“网络主权”为核心原则，我国在各项数据主权立法和战略规划中都明确表达了对维护本国数据主权、尊重他国数据主权的坚定立场。

同时，我国当前在国际网络主权竞争中处于弱势地位，我国的网络空间治理诉求并不是争夺国际数据主权霸权，而是立足自身，积极发展关键信息基础设施，保障本国数据主权安全。《网络安全法》中就用近三分之一的篇幅强调了网络运行安全，尤其是对关涉国家安全和人民生活重要财产的关键信息基础设施运行安全的保障。

(2)战略体系呈防御性特征，体系框架呈多级扩散特点

与美国主要对外扩张、积极进攻的数据主权战略体系对比起来，我国主要采取的是防御性战略，核心内容主要围绕维护国家网络和信息安全的基础建设层面。这与我国当前所处的国际数据主权争夺地位密切相关。我国为代表的网络技术发展中国家，在网络主权的博弈中，首要目标始终是保障本国数据主权安全，同时不断增强本国数据实力，不断增加本国数据资产。

同时，我国的数据主权整体框架呈现多级扩散特点。与美国等国家兼具法案、行政规章、行业标准、组织宣言等多方面多层次的战略体系框架不同，我国主要采用法律、行政法规、部门规章三个效力层级进行战略体系建设，具体内容主要偏向计算机系统安全和网络保护措施方面，从而呈现出金字塔形的多级扩散的发展特点。

(3)各细分领域战略内容为主，政府主导下的严格控制建设模式

我国在《网络安全法》之前，主要是对网络安全所涉及的相关细分领域进行规范和治理，缺少如欧盟一样的整体宏观层面的指导性战略。即使是在《网络安全法》中，法条也是在制定全面的网络安全等级保护制度的基础上，再通过列举如金融行业、公共通信行业、水利行业等细分行业的行业标准进行结合，从而形成规范网络安全的判断标准。这也反映出了当前我国在愈加复杂的数据主权治理环境下所面临的整体治理困境，我国亟待出台整体性、框架性、指导性的上层政策来支撑我国相关主体在国际上的主权保护实践。

同时，我国在战略制定、建设和实施上采用政府主导下的严格控制模式，战略推行主要依靠国家权力机关，日常监管主要依靠政府部门间的协同管理，且各个部门之间各自独立，合作较少。

由此可见，我国以“网络主权”为主要原则，以发展为核心诉求，以国家权力机关为主要建设和实施主体，建设了独具特色的防御为主、细分为主、自上而下的多级数据主权战略体系。这一体系选择与我国当前在国际数据主权竞争中所处的地位相符，也与我国的根本利益相匹配，能够推动我国的数据主权战略的全面实施和不断发展。但同时，这一主权战略的模式选择也暴露出其缺乏顶层设计、缺乏国际国内合作等问题，亟待进一步调整以适应新技术背景下我国数据主权发展的新需求。

4.2 主要借鉴

基于对CLOUD法案的数据主权战略体系的深入剖析以及对我国数据主权战略体系的思考，以CLOUD法案为借鉴，本文对我国数据主权战略发展提出如下针对性建议。

4.2.1 宏观层面强化指导，加强数据主权的顶层设计

当前，美国已开始借助CLOUD法案为侵入他国数据主权领域奠定法律和渠道基础，这使得我国的数据主权保障态势愈发严峻。我国的数据主权战略建设起步较晚，与以美国为代表的发达国家有较大距离。在早期建设过程中，我国对网络空间和数据主权的重要性认识不够充分，且较少参与到国际网络空间合作治理实践之中，在此基础上建设的相关数据主权法律法规大多集中于国内各细分领域和具体技术问题，鲜见全局性、框架性的战略出现以支撑我国网络空间治理与数据主权战略整体发展。

在我国自身战略建设尚有不足的同时，当前网络技术的迅速发展也使得传统国际法难以规制网络空间中的新主权问题，国际上尚未有统一认可的数据主权理论框架和治理方案，以管辖权为标准的传统国际数据主权治理模式带来了大量的主权争端，以我国为代表的发展中国家难以寻求国际法的保障。面对这一背景，我国必须加快在宏观层面的战略建设，借鉴相关国家的战略发展经验，强化数据主权战略的顶层设计，推动形成主权战略实施的理论基础和指导框架，从而全面支撑我国的数据主权保护和数据资源积累实践。

4.2.2 跟进具体治理方略，考量数据主权的各种管辖模式

传统意义上，数据主权的管辖划界主要有属人管辖和属地管辖两种模式。属人管辖主要依据国籍划分，也就是某主权国家的公民所产生的数据归属该主权国家管辖。属地管辖主要根据国家物理空间予以划分，主权国家对其领土内的数据及其信息基础设施具有数据主权。随着网络空间的不断发展，国籍和领土限制均已被突破，属人和属地管辖的理论和现实基础被不断削弱。在新的信息时代，传统的属人、属地管辖模式仍有其合理性，但需要不断发展适应新需求，例如欧盟的《通用数据保护条例》(GDPR)就确立了以属地原则为主、其他原则为辅的管辖模式。

美国CLOUD法案的出台，为国家数据主权的治理模式建设打开了新的思路。美国CLOUD法案催生的关键因素即为传统属地管辖与属人管辖模式的冲突，同时两种模式都暴露出了无法满足主权国家跨境数据调取需求的弊端。由此诞生的CLOUD法案不再局限于属人或属地的原则，而是从数据控制者提供服务的角度出发，对执法机构下达调取数据命令的适用范围进行了域外扩展。这种“CLOUD模式”实际是以结果原则为理论支撑，认为主权国家可以在面对损害其主权安全及公民利益的行为时可以突破属地属人限制，根据可能或实质发生的危害来主张行使管辖权。

可见，无论是欧盟综合传统管辖模式，还是美国创新管辖模式，当前网络空间进一步趋向虚拟化、非中心化、全球化的特点使得各主权国家都在争相采取各种手段创新管辖模式，力图实现本国在网络空间竞争中的利益诉求。我国必须紧跟国际数据主权治理发展趋势，考量在新的信息环境下国家主权治理的各类模式，结合我国发展实际综合思考，构建我国数据主权的管辖模式，并不断跟进战略实施和主权管辖的具体方略，保障我国数据主权安全。

4.2.3 促进数据跨境安全流动，优化国际数据交流平台

CLOUD法案的诞生和形成体现了在国家数据主权治理的过程中，最为核心的关键问题即为规制数据的跨境流动治理和管辖。数据已经成为推动新信息时代技术创新和社会发展的关键生产要素，数据的开放及其高效流动对于国家的产业革新、经济增长、社会发展具有关键性作用，与国家的经济发展全局、国家网络安全、国家战略整体布局紧密关联。但同时，全球数据流动无可避免地孕育着数据隐私泄露、信息情报窃取、恐怖主义渗透等国家数据主权安全隐患。面对这一现实，我国必须推动与积极相关国家和区域数据的双向流动，并在流动规则上积极借鉴美国、欧盟等国做法，强化对数据出入境的风

险评估、安全监测、定期审核和价值评价，促进数据的跨境安全流动，保障国家数据主权安全。

在涉及关键信息的跨境流动上，我国一方面应积极建设国家级数据流动和网络安全态势感知平台，全面提升对数据流动的监测、分析、预警和响应能力，保障关键信息数据的安全流动与全面追踪。另一方面，可积极参与国际数据交流平台的建设，融入国际合作并协助打造各主权国家均能就信息主权问题发声、交换意见、互惠数据资源的国际数据交流平台，推动网络空间国际行为准则的形成，提升我国在网络空间中的话语权。

4.2.4 协作治理网络空间，加强国际数据管辖的平等合作

网络空间突破了主权国家的物理范畴，且以其广泛性、虚拟性将全球错综复杂地交融在一起。网络空间中虽然有各个主权国家的竞争，但更多地，仍是以合作为主流。尤其是在面对如恐怖主义、黑客攻击、网络间谍等单个国家无法解决但又至关重要的共同问题上，合作治理与开放交流是整体数据主权安全保障的必然要求，即使强势如CLOUD法案，也不断强调要加强与“适格外国政府”的数据交流和合作互惠。我国在传统的数据主权治理实践和网络空间发展上，较少与其他主权国家合作。随着大数据环境的到来，我国当前的数据主权司法和行政管辖上逐渐暴露出局限于传统的网络犯罪领域的弊端，关键信息基础设施和核心网络技术的发展水平有待提升，无法对当前新信息环境下的新型信息犯罪和新兴信息行为予以规制，也难以有效回应大数据环境带来的技术和安全冲击。如何有效规制新型信息犯罪、保障本国数据主权、提升数据主权实力成为我国需要解决的重点问题。这要求我国转变发展思路，在相互尊重信息主权的基础上，积极参与国际数据主权治理合作，尤其是在规则制定、司法协助、技术合作上，借鉴当前国际数据主权治理合作实践，不断扩展合作的范围和深度，进一步保障我国数据主权安全，提升我国数据主权实力。

5 结语

当前，数据资源呈现大量流入发达国家，数据资源的所有权与治理权进一步分离，各国的数据主权治理边界愈发模糊。同时，国际网络空间数据流动治理和管理机构建设尚未成型，国际统一的数据主权管辖标准和法律框架也尚未出现，导致国际跨境数据流动与数据主权安全治理呈现零散化、碎片化的特征。在这一背景下，各主权国家均积极展开数据主权战略建设，保障本国数据主权安全，这其中以美国CLOUD法案最具代表性。

CLOUD法案围绕国家数据主权的边界，并主要瞄准了数据主权中最为重要的管辖权，将美国自身的权利行使边界转移到他国边界，使得美国数据主权战略的轮廓进一步变得清晰。

从2003年伊拉克战争“打印机”病毒植入、2010年伊朗“震网”(Stuxnet)攻击、2014年朝鲜制裁全面中断网络服务，到近年来中美贸易战中我国芯片产业的受制于人，国际网络空间的激烈竞争时刻为我们敲响警钟。未来围绕数据主权的争夺将进一步趋向白热化，对于数据主权的治理将关切到我国的总体安全和长治久安。我国在新的国际环境下，必须转变传统的数据治理思路和治理方式，强化我国的数据主权战略体系建设，为我国的数据安全提供更为全面的战略支撑。

参考文献：

[1]翟志勇.数据主权的兴起及其双重属性[J].中国法律评论，2018(6)：196-202.

[2]宋佳大数据背景下国家信息主权保障问题研究[D].兰州：兰州大学，2018：12.

[3]朱莉欣.聚焦《塔林手册》透视网络战规则[EB/OL].[2019- 03- 25].http://theory.people.com.cn/n/2015/1130/c386965-27870836.html.

[4]联合国裁军事务厅.从国际安全角度看信息和电信领域的发展[EB/OL].[2019-03-21].https://www.un.org/disarmament/zh/.

[5]Schmitt M. Tallinn manual 2.0 on the international law application to cyber operations(2nd edition) [M]. Cambridge: Cambridge University Press, 2017: 12.

[6]Meltzer J P. The Internet, cross-border data flows and

international trade[J]. Asia & the Pacific Policy Studies, 2015, 2 (1): 90-102.

[7]Syuntyurenko O V. Network technologies for information warfare and manipulation of public opinion[J]. Scientific & Technical Information Processing, 2015, 42(4): 205-210.

[8]Paladi N, Aslam M, Gehrmann C. Trusted geolocation-aware data placement in infrastructure clouds[C]//2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications Beijing, China. IEEE, 2014: 352-360.

[9]Vulimiri A, Curino C, Godfrey P B, et al. WANalytics: Geo- distributed analytics for a data intensive world[C]//ACM SIGMOD International Conference on Management of Data, May 31,2015, Melbourne, Victoria, Australia. ACM, 2015: 1087-1092.

[10]Shin Y J. A study on privacy protection tasks for cross-border data transfers[C]//2014 International Conference on It Convergence and Security, Beijing, China. IEEE, 2014: 1-4.

[11]Mosch M, GroßS, Schill A. User- controlled resource management in federated clouds[J/OL]. Journal of Cloud Computing: Advances, Systems & Applications, 2014, 3: e10.[2019-03-22]. https://doi.org/10.1186/s13677-014-0010-8.

[12]Anna Z. The salient features of personal data protection laws with special reference to cloud technologies, a comparative study between European countries and Russia[J]. Applied Computing & Informatics, 2016, 12(1): 1-15.

[13]Swaminathan A, Loeb R, Goldman B P, et al. The CLOUD Act explained[EB/OL].[2019-03-23]. https://www.orrick.com/lnsights/2018/04/The-CLOUD-Act-Explained.

[14]United States Congress. H. R. 4943- CLOUD Act[EB/OL].[2019- 04- 30]. https://www.congress.gov/bill/115thcongress/house-bill/4943.

[15]洪延青.美国快速通过CLOUD法案明确数据主权战略[J].中国信息安全,2018(4):33-35.

[16]中国互联网信息中心、中国互联网发展状况统计报告(2019年2月)[R/OL].[2019-03-25].http://www.cac.gov,cn/2019-02/28/c_1124175677.htm.

Interpretation of US Data Sovereignty Strategy Based on CLOUD Act

Huang Haiying He Mengting

Abstract: In the increasingly fierce international cyberspace, the boundaries of data sovereignty governance have become increasingly blurred, and sovereign states have actively launched data sovereignty strategies to ensure the sovereign security of their data. The United States passed the CLOUD Act in March 2018, aiming to resolve security threats in cross-border data flows and safeguard national data sovereignty. The study of this bill is of great significance for improving Chinas data sovereignty strategy and data strategy system. This article, with a comprehensive analysis of the CLOUD Act, interprets its contents and explores its core objectives and construction models. By a comparative study, it is found that China´s data sovereignty strategy has following features: it is based on the principle of "network sovereignty"; it takes development as its core goal; it has state power authorities as the core subjects, and it is of a top-down manner. Meanwhile, this paper, in light of the CLOUD Act, puts forward suggestions on Chinas data sovereignty strategy system in respect of macro top-level design guidance, inspection of specific jurisdictional strategies, promotion of international data exchange, and collaborative governance of cyberspace.

Key words: CLOUD Act; Data sovereignty; Strategic system; Cross-border data flow; Cyber space; Data security