DOI:10.16775/j.cnki.10-1285/d.2023.01.001

国家安全视域中
我国数据主权安全面临的挑战及其对策

毛欣娟　任珈炎 *

【摘　要】数据作为事关国家安全的战略资源，数据主权安全与国家安全、综合国力紧密相关。尤其是在日益严峻的数据安全环境下，数据主权安全风险愈演愈烈。有效应对数据主权安全风险、保障数据主权安全已成为国家发展亟待解决的关键问题之一。本文从国家安全视域出发，以数据主权安全问题为研究目标，采用文献研究、政策分析等方法对相关研究、政策和法规等资料进行剖析，明确数据主权安全概念、起源背景及相关界定，总结我国国家安全视角下数据主权面临四个维度的风险：数据生成与存储、数据跨境流入与流出、数据分析与利用、数据域外管辖与强国霸权。结合我国数据主权安全保障体系现状，提出构建数据主权领土、完善法律体系、发展核心技术、寻求国际合作四个方面可落于实处的对策建议，为构建我国数据主权安全保障体系建言献策。

【关键词】国家安全；数据主权安全；数据主权风险；数据治理；数据对策

一、引言

随着互联网技术的深入发展，日益庞大的数据体量仍在剧增，数据正在渗透到人类日常生活结构中，甚至在某种程度上推动了社会变革。①数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各环节，深刻改变着生产方式、生活方式和社会治理方式②。互联网数据中心（IDC）显示，数据资源总量将由2016年的16.1ZB增长到2025年的163ZB（约合180万亿GB）③。由于数据在地理国界上的无限性，传统意义上的国家主

*　毛欣娟，中国人民公安大学国家安全学院教授，博士生导师；任珈炎，天津市公安局民警。本文系中国人民公安大学研究生课程建设项目“政治安全前沿问题”（编号：2022YJSKCJS028）阶段性成果。

① Barbara L.Data Governance: A Quality Imperative in the Era of Big Data, Open Data and Beyond, *A Journal of Law and Policy*, 2015（3）.

② 《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》，人民网，http://politics.people.com.cn/n1/2022/1219/c1001-32589890.html，访问日期：2022年12月30日。

③ 《〈数据时代2025〉预测2025年全球数据将攀升至163ZB》，新华网，http://www.xinhuanet.com/fortune/2017-05/11/c_129601736.htm，访问日期：2022年9月12日。

权和领土不再适应国家利益边界与国家物理边界的范畴，进而催生了两者之间的扩张不平衡差距问题。“绝对主权”“领土等于主权管辖范围”等以国家领土为核心的传统国家安全时代已经终结，网络空间由此成为国家间博弈的“第五疆域”。数据主权的诞生改变了国家安全威胁的特点及运行范式，成为现今各国国家安全战略博弈的新领域。2021年是我国数据安全领域的立法元年，与数据主权安全相关工作也进入新阶段，我国数据主权安全政策体系建设取得重大战略进展。然而，与数据主权安全相关的问题及争端在实践中不断出现。在“滴滴赴美上市”事件中，掌握着我国各领域海量数据资源的技术公司被安全审查，由此，从个人数据安全到国家层面的数据安全问题引发了广泛关注。国家数据主权之下的关键行业领域数据一旦出现问题，或将直接对国家安全产生威胁。有鉴于此，深入了解数据主权安全所存在的风险，做好相应的制度保障措施，对保证社会政治稳定、保障我国国家安全具有巨大且重要的现实意义。

基于数据资源越发重要的社会现实，数据主权及数据主权安全问题日趋成为学界关注与研究的热点。在中国知网以“数据主权安全”为关键词进行知识元检索，显示“数据主权安全”检索词相关文献分布在以下十个学科类别中：行政法与地方法制、计算机软件及计算机应用、互联网技术、信息经济与邮政经济、中国政治与国际政治、新闻与传播、公安、行政学及国家行政管理、法理及法史、民商法。其中，在行政法与地方法制领域、互联网技术领域以及中国政治与国际政治领域相关探讨较为集中也较为深入。

二、数据主权安全概念、内涵与外延

保障“数据主权安全”是响应各国家在大数据时代维护国家主权和独立的需求，数据主权安全的多层次内涵使得该领域问题变得重要而复杂。在数据主权安全问题丛生的背景下，其概念的确立及内涵与外延的明晰十分必要。

（一）数据主权的起源

主权代表一个国家独立自主处理其内外事务、管理国家的最高权力，是国家基本要素之一，也反映了国家在国际舞台上的基本地位。随着互联网、大数据和物联网、云计算等现代信息技术的发展，安全风险边界在不断泛化，国家主权也处在动态发展调整的状态。当今时代，国家主权被赋予新的内涵，主权的概念及内涵不断丰富，并逐渐发展演变为以网络主权、数字主权和数据主权为代表的新概念。不容忽视的是，大数据时代，由于缺乏统一的具有世界公认的管控标准，使得国家间基于数据主权方面的博弈愈演愈烈，多重管辖冲突激烈，网络空间安全的失序状态极大地阻碍了数据本身价值的发挥。依据网络空间层级划分逻辑，网络主权相应地划分为“物理层”“逻辑层”和“数据层”三个层次[①]。“物理层”主要立足国家在其领土上运行网络活动的主权；“逻辑层”主要指计算机代码层面的国家主权，尤其指数据传输通信协议和网络互联方面的主权，关键在于对域名系统（DNS）的控制问题；“数据层”主要是由于数据生成地与储存地的割裂、数据所有者、存储者与使用者在地理位置上处于相对分离的状态，由于世界各国暂未形成数据安全治理框架共识，因此在数据管辖权和数据所有权方面极易产生国家间的主权纷争。因此，在《国家安全法》和《网络安全法》框架内，数据主权理应成为“网络空间主权”的下位概念。又由于网络空间主权是国家主权

① 冯硕：《TikTok被禁中的数据博弈与法律回应》，《东方法学》2021年第1期。

延伸到网络空间的结果，所以数据主权也应当成为国家主权的重要组成部分之一，同样具有国家主权的平等性[①]。

学术界关于数据主权的观点有广义和狭义之分。本文基于国家安全视域，以狭义的数据主权为研究对象，认为数据主权的主体是国家而非个人。关于数据主权的概念，目前学界尚无统一的定义。孙南翔和张晓君认为，数据主权是指国家对数据管辖权及控制权，同样包括与数据相关的技术、服务及设施，体现为对其管辖范围内数据的绝对管辖权以及对外参与国际事务的合作权、独立自主的权力[②]。齐爱民和祝高峰认为数据主权是国家对其管辖范围内主体产生的数据享有的最高权力，内涵主要包括三个方面：对数据的立法权、控制权以及对该产业技术的自主发展权[③]。赵刚等认为数据主权在某些特定方面会与网络主权交叉和融合，因而体现了一国对其数据及相关技术、服务内容的相关控制权和管辖权[④]。帕特里克·W.弗兰泽兹认为网络空间依附国家主权，所以其主权安全同样需要保护[⑤]。目前，“数据主权”概念是以原则性条例的形式提出于部分国家与相关国际组织的制度中：《塔林手册2.0版》提出，各国有权对其境内的数字基础设施和网络活动行使主权，并在全球可出于自身需要实施网络治理；2015年，我国国务院印发的《促进大数据发展行动纲要》要求增强网络空间数据主权保护能力，虽然是首次从官方层面提出数据主权，但是未有概念界定；2021年我国出台的《数据安全法》凸显“数据主权”概念[⑥]，要求重要的数据在出境时必须经过国家安全审查。

数据主权概念应与国家主权理论的含义及内涵要求相符合，应以网络空间安全为现实基础，根据技术发展和现实情况，不断完善和扩展国家主权的概念和内涵。国家主权理论将一国主权分为两部分，对外独立和对内自主，具体表现为四个部分：独立权、管辖权、平等权、自卫权。以此为基础，数据主权应该是国家对其所管辖地域范围内的数据具有最高权力，即能够对内控制、管理和保护本国数据信息的生成、存储、流动、分析和利用，以及对外参与国际合作和不受其他国家和组织干扰的独立性和自主性。

（二）数据主权安全的概念、内涵与外延

一般意义而言，“安全”是指“免受威胁的性质或者状态”。黄海瑛和文禹衡将数据主权安全定义为“主权国家为了保证其管辖范围内的数据处于相对有效控制和保护的状态而能够采取一系列自主措施”，同时提出了数据主权安全能力的概念，将其定义为“为保障数据主权的安全，国家在政策战略、文化教育、传播媒体、立法和司法等方面采取相应的保障措施”[⑦]。本文基于相关研究与政策文本，认为数据主权安全的概念应该以数据主权概念为基础，国家拥有对所管辖地域范围内的数据享有最高权力处于免受威胁的状态，即能够控制、管理和保护本国数据信息的生成、存储、流动、分析和利用，及对外独立自主参与国际合作并且免于他国和其他组织干涉。数据主权安全的可持续性是国家主权在新时代发展形势下新的表现形式，也是在全球化进程中各国为维护国家主权、

① 梁坤：《基于数据主权的国家刑事取证管辖模式》，《法学研究》2019年第2期。
② 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 齐爱民、祝高峰：《论国家数据主权制度的确立与完善》，《苏州大学学报(哲学社会科学版)》2016第1期。
④ 赵刚、王帅、王碰：《面向数据主权的大数据治理技术方案探究》，《网络空间安全》2017年第2-3期。
⑤ Franzese Patrick W. Sovereignty in Cyberspace: Can it Exist?, *The Air Force Law Review*, 2009（64）.
⑥ 黄海瑛、何梦婷、冉从敬：《数据主权安全风险的国际治理体系与我国路径研究》，《图书与情报》2021年第4期。
⑦ 黄海瑛、文禹衡：《数据主权安全能力的成熟度模型构建研究》，《图书与情报》2021年第4期。

抵制数据霸权的必然要求[①]。

大数据、云计算背景下，数据规模不断呈现爆炸式增长态势，数据主权安全的本质起源是为应对大规模数据的安全问题而提出的名词，反映了新时代技术发展带来的新变化。数据主权安全既关注广义上的数据，也关注狭义上的数据。国家对其管辖范围内的数据拥有对内的最高数据管控权和对外的数据处理权。数据主权安全同时体现了国际性和综合性两种特性[②]。

数据主权安全的内涵主要包括两个方面内容：数据管辖权安全和数据所有权安全。数据管辖权安全主要是指国家对其管辖范围内的数据所进行的生成、存储、流动、分析和利用等一系列活动拥有管理权，以及对于数据领域所发生的纠纷情况拥有司法管辖权，相对来说这些权力是处于无威胁状态；数据所有权安全是指国家对其管辖范围内的数据所采取的保护措施权力相对处于不受威胁的状态，即保护其数据免受更改、篡改、破坏、盗窃或泄露的威胁。

在全球科技前沿技术不断发展和创新的背景下，在全球各方利益新的战略平衡中，衍生了一系列新概念。21世纪，欧盟连续发布了一系列战略性文件，包括《欧洲的数字主权》研究报告、《欧洲数据战略》，明确提出了“技术主权”概念及“数字主权”等概念，欧盟在该领域的战略方针主要为争夺规则的制定权。由此可见，数据主权安全延伸概念呈现不断演化的趋势，但数字主权安全及技术主权安全仍以数据主权安全为核心和基础。

三、我国数据主权安全面临的挑战与风险

大数据时代，作为数据载体的互联网存储着种类多、来源广、不同性质的海量数据。数据安全问题最突出的可以总结为四个维度的风险：数据生成与存储、数据跨境流入与流出、数据分析与利用、数据域外管辖与强国霸权。当前全球数据主权发展态势下，“数据主权”的提出反映了各国为维护本国主权利益及限制数据强国滥用权力的现实要求。数据主权的争夺成为各国在网络空间博弈的新领地，我国数据主权安全面临着一系列现实问题。

（一）第一维度：数据生成与存储风险

大数据时代数据所涉及的对象、主体及利益呈现出多元化、多维度特征。据国际数据公司、中商产业研究院整理的数据显示，作为人口基数庞大的国家，我国数据产生量约占全球数据产生量的23%[③]。然而不断涌现的新技术使得数据的“位置”与数据的“归属”两个重要属性更模糊，数据的生成与存储存在着安全隐患。

1. 数据对象被过度采集

个人数据与重要数据安全问题一直是互联网平台数据安全问题的讨论重点。长期以来，数据安全事件层出不穷，被违规采集的数据对象被存储在非正规区域，极易产生如个人隐私信息泄露、数据“黑灰产”等安全问题。而个人数据的汇集所产生的危害影响甚至会涉及国家安全问题。我国《个人信息保护及隐私政策》中强调了收集、保留、使用和分享个人数据的权利。然而，根据之前

① 何傲翾：《数据全球化与数据主权的对抗态势和中国应对——基于数据安全视角的分析》，《北京航空航天大学学报（社会科学版）》2021年第3期。

② 齐爱民、祝高峰：《论国家数据主权制度的确立与完善》，《苏州大学学报（哲学社会科学版）》2016年第1期。

③ 《中国数据产生量占比约23% 2022年全球大数据储量分析（图）》，中商情报网，http://kns.cnki.net/kcms/detail/11.1762.G3.20220217.1815.006.html，访问日期：2022年4月17日。

的个人数据保护和隐私政策，其中定义的个人数据范围包括面部识别、音频、身份证号码、银行卡号和IP地址等。显然，在国家数据保护框架尚不完备的情况下，对个人数据的过度收集和保留远远超出了正常使用各类软件应用平台基本功能所需的范围。海量个人数据聚集可能会直接引发个人数据安全问题转化为国家重要数据安全问题，使得引发国家主权安全问题及风险的可能性增大。

2. 数据主体被违规存储

跨国互联网公司成为新“数据主体”，在如今经济全球化、数字化浪潮下发挥着不可替代的作用。作为数据控制者的跨国互联网公司，海量数据在互联网公司生成、汇聚、交互，体现数据价值的同时也带来巨大的数据安全风险，甚至拥有的权力对国家安全足以产生影响。根据国务院发布的《中国经济报告》，部分跨国互联网公司在相关领域所取得的市场地位及影响巨大，在全球仍具有一定的影响力。在过度采集数据的过程中，跨境互联网公司如果不能具备足够的数据主权安全意识和数据安全保障意识，数据的生成与存储不规范，容易导致滋生数据滥用等安全风险及合规问题，将会直接对国家的数据主权造成威胁。

（二）第二维度：数据跨境流入与流出风险

“数据跨境流动”是指“在一个国家以电子方式产生的信息记录，由他国的个人或公权力机关读取、储存、使用或‘处理’”①。数据自由流动是大势所趋，也是数据主权产生的先决条件之一，但前提必须是保障国家及公民的安全。然而随着数据价值的不断提升，跨境数据能否安全、有序、自由地跨境流动，潜藏了国家数据主权安全隐患。

1. 防范数据跨境“取”

当前关于数据“入境”规则已经有了实质性的改变，主要表现为国家机关对存储于境外的非公开数据实施强制性“长臂管辖”调取。为了扩大其“域外管辖权”的有效性，数据强国接连出台一系列制度，甚至通过本国立法、行政和司法等部门的紧密配合，立法授权其国家机关获得获取其他国家数据的权力，从而使得其他主权国家丧失对其领域内数据保护的权力。我国现有的法律制度多是侧重于保护和监管的角度，强调数据的规范使用与利用，存在数据权属与利益分配不明问题。在当前国际上对抗数据主权和数据全球化的趋势下，我国仍不足以有效应对部分强权国家的管辖主张，容易引发威胁国家安全的风险。

2. 防范数据跨境“出”

相比较数据跨境流入，各国对数据跨境流出的限制更为重视。到目前，我国关于数据出境的法律法规主要包括《网络安全法》及一系列评估指南、评估办法等法规。数据跨境流出，强调的是将境内收集和产生的数据提供给境外，其风险重点来源于数据出境的合规类风险。近年来，出现了一批掌握海量个人信息资源的中国科技公司开展海外业务，甚至在境外上市，这个过程中就可能涉及大量的数据出境。针对这一情况，国家互联网信息办公室发布的《数据出境安全评估办法（征求意见稿）》明确了数据安全评估的具体情形，但还未正式颁布，因此不具有法律效力。在数据跨境流出的过程中，如何保障数据在出境前、传输过程、数据落地后等过程中是否存在违法风险，在现有的法律制度中仍是不明确的问题。在出境商业活动稳定发展的背景下，企业需要确保出境数据不存在违反国家法律法规标准要求的风险，尤其是数据在出境前、传输过程中和落地后是否存在违反法律标准和对国家安全构成威胁的风险仍需重点关注。

① 许可：《自由与安全：数据跨境流动的中国方案》，《环球法律评论》2021年第1期。

（三）第三维度：数据分析与利用风险

在数据主权范畴下，数据风险越发呈现隐匿化、复杂化趋势，如何在合理的范围内对所掌握的数据进行有限度的分析与利用，不单单是跨国互联网与科技公司层面需注重的难题，更是在国家层面亟待解决的关键性问题。

1. 数据技术发展落后

数据作为技术产物，数据主权面临着技术发展带来的挑战。在国家层面，核心基础技术自主可控具有重要意义，我国国家数据主权安全面临着技术性风险。近些年来，虽然我国数据产业取得了一定进展，但也存在着数据技术落后、企业创新能力较弱等“数据核心”的制约因素。当今网络空间，发达国家提供信息基础设施和关键应用，发展中国家只能作为互联网的使用者①。在该领域的发展中，全球互联网的基础技术受美国主导，尤其在数据传输方面，美国已经显示出其作为技术大国的绝对优势。美国政府已控制了互联网域名的空间分布，在域名系统、根服务器系统、互联网协议地址等②领域占据了绝对控制权。例如在国际顶级域名主服务器领域，我国未能掌握这一关键性资源，只能在美国服务器的控制下，与其他国家网络的“域名”之间进行数据传输。美国《澄清合法使用境外数据法案》的实质物质基础，还是依据美国网络运营商在世界各地的网络设施和数据中心。理论上，只通过封锁美国根服务器上的中国域名，我国的国家顶级域名网站就能立即被从网络上删除。在数据活动的其他环节，我国也存在着与发达国家的数据技术差距，以及在数据领域缺乏竞争力的难题。

2. 法律规制有待完善

在数据分析与利用阶段，主要面临着数据使用因缺乏有效规制、边界不清晰导致的国家数据主权安全风险。与国外相比，我国的数据主权保障路径起步较晚，未能形成如同欧、美等国家所建立的完整的、清晰的国家数据主权战略发展路径。我国数据主权战略以《国家安全法》为总纲，以《网络安全法》《数据安全法》《个人信息保护法》为核心，并围绕上述法律不断进行标准、办法等政策增补，但仍存在着相关规定较为零散，隶属于多个独立政策之下的情况，缺乏宏观层面上的体系性设计，并未形成美欧等国数据战略中不同法案、政策以及标准等相互配合、共同协作、彼此协调的关系③。在国家战略方面，相较于美欧等国家及地区制定的数据战略和顶层设计，我国目前暂无一套完整的针对保障数据主权的规制，这样规制的缺失会削弱我国在跨境数据治理国际规制中的主导权和话语权。我国国家安全战略体系仍以防护为主，而事实上，数据所有权只是作为国家数据主权的权力内容之一。在以安全防御为主的数据主权战略下，如何在符合我国的“总体国家安全观”下促进数据高效流通、发展大数据产业，既是国家数据主权权力内容的重要组成部分，也是我国大数据战略发展的最终目标。

（四）第四维度：数据域外管辖与强国霸权风险

数据主权作为国家主权的延伸与扩展，在世界各国对全球数据支配力强弱不均的情形下，承载着通过制定数据规则来抵制数据霸权、捍卫国家安全的重要使命④。随着国际社会日益认识到数据域外管辖权的重要性和影响，世界各国意识到数据主权安全对国家安全的巨大意义，对此纷纷布局

① 李传军、李怀阳：《网络空间全球治理问题刍议》，《电子政务》2017年第8期。

② 肖冬梅、文禹衡：《在全球数据洪流中捍卫国家数据主权安全》，《红旗文稿》2017年第9期。

③ 郑琳、李妍、王延飞：《新时代国家数据主权战略研究》，《情报理论与实践》，2022年第6期。

④ 黄海瑛、何梦婷、冉从敬：《数据主权安全风险的国际治理体系与我国路径研究》，《图书与情报》2021年第4期。

并出台各国的数据规则。

1. 数据多种管辖冲突

近十年来，数据的主导权成为各方争夺数据资源的焦点。在数据所有权的博弈中，明确数据主权是确定一国对某一数据是否具有所有权力的前提。由于数据生成地与储存地之间的分割，数据所有者、存储者与使用者在地理上的分离，以及世界各国缺乏全面和统一的治理规则，因此极易导致在数据控制权和所有权方面的主权争端。

为维护和扩展本国利益、建立法理权威，各个国家和地区在抢占国际数据规则制高点的数据主权治理上选择了不同的模式与进路。美国和欧洲的数据主权战略属于“进攻型”，通过打造自身离岸“长臂管辖权”，允许跨越一国传统地域主权限制获取境外数据，将执法范围扩大到国界之外；中国、俄罗斯等新兴经济体的数据主权战略属于“防守型”，侧重于本地化解决冲突。由于发展中国家对国际贸易市场的过度依赖，欧盟和美国凭借自身技术、资源优势主导了贸易体系中的数据流动规则。“长臂管辖”在很大程度上改变了全球数据主权博弈的规则，同时也加剧了与他国在数据执法权及管辖权方面的冲突。这种制度安排不利于数据的双向流动和国家间的双边合作，也使得全球数据流通治理方面受到了约束。目前，我国数据主权制度的域外规制力较弱，数据管辖多限于单边管控，对强权国家和发达国家的管辖主张不足以进行有效应对。同时我国也缺乏区域间数据联合协作机制的保障，在数据域外管辖中容易遇到冲突和壁垒。

2. 强国数据霸权

在新兴的数字技术领域的发展下，近年来迅速扩张的美国霸权已成为他国数据主权安全的首要风险源[①]。在美国掌握着相对数据垄断的权力下，在全球呈现出数据强国与其他国家之间权力不平衡。全球互联网用户多数分布于发展中国家，然而美国实行“单边主义”，利用其自身掌握的关键技术、优质资源及在数据流动中所产生的连锁效应，其影响力和吸引力在全球战略中极大扩增。从数据主权角度来看，美国推行数据霸权政策早在小布什执政时期就已开启，以“应对间谍活动”为由利用网络和卫星监控全球数据流，追踪特定目标并收集其他国家的情报，著名的“棱镜门”事件就是典型例证，严重侵犯他国的数据主权与安全。2018年美国颁布《澄清合法使用境外数据法案》，将美国“单边主义”数据主权模式延伸至全球范围，并通过输出意识形态带偏他国社会思潮来推行“网络霸权”，满足其数据治理主张。在美国网络霸权不断扩张背景下，美国数据权力依靠其保障而形成数据霸权，对全球他国的数据主权安全造成严重威胁。

四、构建和完善我国数据主权安全保障的建议

整体而言，在建立国家数据主权治理体系方面，一些重要环节还存在不足和安全隐患。基于国际政策框架和我国的实际需要，从我国数据主权安全面临的四个维度风险，来探讨数据主权安全保障对策，更有针对性地完善我国数据主权建设体系，捍卫数据主权安全。

（一）构建数据领土，保障数据生成与存储安全

在大数据时代的巨变中寻求发展和安全，需要广泛借鉴国际社会经验，数据主权国家应当积极建立新战略和新思维，秉持“对内建设数据强国，对外构建数据空间命运共同体的战略理念与政策

① 黄海瑛、何梦婷、冉从敬：《数据主权安全风险的国际治理体系与我国路径研究》，《图书与情报》2021年第4期。

主张”的目标。

构建“数据领土”是建设数据强国的基础。数据本地化存储作为构建“数据领土”的基本方式，意味着在内部收集、处理和存储国家公民的相关数据，以保护本国公民隐私、商业利益、促进数据执行保护和国家安全。“数据领土”的规模取决于国家掌握的数据量，而缺乏对国家数据的控制则意味着“数据领土”的丧失。在数据的生成及存储过程中，我国同样应当注重数据本地化存储与数据自由流动之间的平衡，在保障国家经济发展的前提下做好稳妥的数据主权安全保障措施，实现静态与动态的有机统一①。

把握数据保护与高新产业发展的天平，面对我国数据主权安全现存的焦点问题——跨国互联网公司与数据的关系。这些跨国互联网公司不仅是数据流通的中介，更是不可忽视的基础设施，作为数据控制者它们有能力记录和提取与用户之间的在线行为和互动相关的所有数据。用户的庞大数量和交易的巨额数量决定了信息设施的安全性，国家安全、国计民生和公共利益彼此交织，这些关键信息基础设施运营主体者拥有的数据可以间接反映出中国人口的区域分布、商业密度、人口流动、商业活动和贸易流动，并与经济发展和社会及社会利益紧密相连。可以说，基于对数据的有效占有和使用，跨国互联网公司在跨境数据流通中拥有着巨大的权力和影响力。数据的利用已经成为数字经济中创造新优势的“助推剂”，数据主权安全已经成为国家主权的高度层面。一方面，保护数据主权安全刻不容缓，层间迭现的数据泄露事件为全球各国的数据监管敲响了警钟；另一方面，数据相关信息是互联网企业发展的基础，若是对其进行高度限制将不利于数据经济发展。在海量数据得以挖掘和利用的前提下，掌握着高尖端科技手段的跨国互联网公司能否在商业价值面前保证对数据的生成、存储和利用是合规合法的，把握好高新数据产业发展和数据主权安全的天平至关重要。

考虑域外效应，注重同他国的规制体系衔接。在构建“数据领土”进行本地化存储的同时，还需要新思维和新的国家战略，既要考虑到国内数字经济的发展，也要对美欧数据主权战略加以掌握，兼顾到与国际规则相协调。尤其是在数据存储方面，在坚持数据本地化的基础上，我国应当充分考虑域外效应，注重同美欧等国数据管理规制体系的衔接、融合，以保障经济、技术发展和国际合作，提升我国在数据治理体系中的域外治理能力和话语权。

（二）完善法律体系，保障数据跨境流动安全

当前，在数字经济全球化的背景下，数据跨境流动成为推动其发展重要途径之一。与此同时，数据在跨境流动的过程中也存在一定的安全风险。法治是数据主权的重要原则，因此应形成更完善的对内与对外规制体系，以明确的、具体的法律法规对我国数据主权的法律地位进行保护，使得抽象、绝对的主权概念转为具体、相对的，保障在司法、执法实践中能够有法可依、有法必依。主要包括三个方面：

一是加强数据主权战略治理体系的顶层设计，积极构建数据主权的国内法体系。采取“由上至下”的视角，全方位审视国家数据主权的权力内容、形式、维度和数据资源类型需求，尽量避免出现问题后再出台法律法规进行弥补的情况，尽早构建适用于我国国情的数据主权战略体系。《网络安全法》《数据安全法》等顶层法律制度的实施，在很大程度上为构建我国数据主权体系做好了奠基，但还欠缺和其相辅相成、互相配合的相应法律条例②。

① 李柏正：《论数据主权的理据、特征及保障》，《内江师范学院学报》2021年第11期。

② 程昊：《从“云幕”法案看我国数据主权的保护》，《情报理论与实践》2019年第4期。

二是通过法律来进一步明确数据主权的含义、范围，促进我国国内制度与国际数据框架相融合。我国应借鉴欧盟GDPR规则、美国“云法案”的相关经验，从多视角完善和协调各地区、各部门、各学科的数据分类标准，在法律中明确补充国家数据主权的含义和内容，构建并完善专门化制度体系，有效规制网络中的数据运行，做到有法可依。掌握他国数据主权战略布局及治理体系，在为我国数据主权战略及治理体系构建提供经验的同时，使我国的数据主权战略和体系与国际接轨、融合，并最终提升我国域外数据主权安全保障能力和话语权。

三是形成国际合作“白名单”机制，反制强国的数据霸权行为。我国出台的《个人信息保护法》《数据安全法》和《反外国制裁法》规定了针对境外非法数据转移的法律责任，及应对他国针对我国歧视性的禁止和限制所采取的反制措施。与此同时，上述法律的施行均需要行政法规的配合和落实。此外，可参考国际通行做法，梳理我国跨境公司及企业数据出境的主要目的地和现实场景，形成国际合作“白名单”机制，以防范数据强国通过跨国公司及企业侵犯我国的数据主权安全。

（三）发展核心技术，保障数据分析与利用安全

2020年美国政府对华为的制裁事件再次预示，我国互联网与科技头部企业被列入所谓的名单，并以限制通过数据技术和数据市场向中国出口高尖端技术和服务。我国在此威胁下，发展数据核心技术已经成为维护国家数据主权安全的重要突破口[①]。首先，提高核心技术自主可控水平，突破技术强国对我国技术的限制和封锁。近年来在核心技术层面，我国仍然存在技术短板，核心数据技术受制于人。“硬实力”方式可以是通过自主研发操作系统、建设网络基础设施、研发核心技术产品等。在充分探索与数据主权安全相关的先进技术和核心产品领域下，进一步跟随时代的脚步发展5G、区块链、人工智能等前沿技术。同时应当根据我国的实际国情，实施创新驱动发展战略，构建政府与企业之间良好的协同关系，完善主权保障的技术支撑体系，使得我国自主的科技核心技术水平能够赶上甚至领先于世界前沿水平[②]。

其次，强化网络技术的应对及防御能力，形成国家数据主权安全防御力量。建立数据安全加密体系，通过各类安全防护手段强化自身能力建设，提升网络保护水平和防御度，推动产业应用，在数据保密、防泄露等安全核心技术领域制定一系列保障措施，提升国家应对数据安全事件的处置能力，维护我国的数据主权安全。

最后，进一步拓展人才培养体系。高精尖的科学技术发展与数据人才的培养密不可分，应当高度重视数据安全领域专门人才的培养，进一步完善大数据及数据安全领域人才的培养机制，满足我国对顶级数据人才的需求。开辟符合数据核心技术的数据采集、处理和挖掘等专业领域，探索和推动中国数据安全领军人才的选拔和培养，发展前沿数据技术，培养复合型网络数据安全的高素质人才。

（四）寻求国际合作，保障全球数据治理环境安全

由于互联网空间具有无边界性的特性，尽管数据主权强调国家在数据层面的绝对性和排他性权力，但是在高度全球化的时代背景下，没有国家能完全独立于其他国家行使自己的数据主权，更不可能独自承担维护世界网络空间有序发展的重要责任。因此，中国作为数据体量增长最快的行为主

① 黄海瑛、何梦婷、冉从敬：《数据主权安全风险的国际治理体系与我国路径研究》，《图书与情报》2021年第4期。

② 沈国麟：《大数据时代的数据主权和国家数据战略》，《南京社会科学》2014年第6期。

体之一，应当注重开展广泛的国际对话，形成多边合作关系，破除僵化的单打独斗模式而转化为彼此依赖的网络空间命运共同体的关系。

积极承担我国作为数据大国的责任，推动公平的国际规则制定。随着网络全球化的进程，未来网民数量与数据增长将主要出现在广大发展中国家和新兴国家，与此同时，这些国家的发展诉求也日益突出。我国应当承担起大国责任，结合“一带一路”等倡议加以推进帮助发展中国家数据主权能力与治理能力的建设，积极参与国际组织的协商和数据主权治理标准的制定，增强我们在国际合作框架中的国际认同，促使在国际社会的共识下形成共同规则，把握和提升在国际社会中的地位与话语权。针对我国对外构建网络空间共同的战略理念，根据自身发展需求建立多边合作框架，并与各国、各地区签订数据主权相关协议，在融入国际数据主权治理体系的同时，提升我国数据主权安全保障的能力和国际话语权的影响力①。

坚持“数据命运共同体”理念，搭建多方合作框架。针对数据主权安全问题，我国倡导和坚持“数据命运共同体”理念，推动达成全球数据主权安全理念的共识②，在与他国达成尊重彼此主权基础上兼顾“多利益攸关方”原则，使各国平等、开放地展开国际合作，促进“一带一路”沿线各国的合作，在经济发展优势下加强多边关系下的国际数据流动合作，在利用数据产业价值的同时保护各国国家数据主权安全。在积极引导建立包括更多主权国家诉求的新网络空间治理框架下，积极宣传并推动“网络命运共同体”“数据主权安全”等公平、规范的立场，反对数据霸权主义，在联合国的框架下尽早构建一个有序、规范、协调的全球数据主权安全保障体系框架。

注重构建新型大国关系，推广数据主权国际合作和安全保障的中国方案。在数字经济的新态势下，针对数据强国抢占国际数据资源以维系数据霸权的动态，我国需对美欧数据主权战略加以掌握。在全球竞争格局重组及数字经济的新态势下，美欧既是我国最大的合作伙伴，也是我国最大的竞争对手。在如今强调合作共赢的非传统安全领域，数据强国基于传统安全思维的单边主义必将受到挑战。我国应当通过首脑峰会等契机，与美国等数据强国建立战略互信，建立成熟、稳效的新型大国关系和国际体系大框架。

总而言之，21世纪以来，数据作为一种生产要素，已经与国家的总体发展密不可分。海量数据在生成、汇聚、流动的过程中，数据价值得以体现的同时也带来不容小觑的数据安全风险隐患。因此，数据主权安全已然成为主权国家维护国家安全权威的必然要求。数据主权安全问题不仅是一个具体问题领域的功能性问题，而且是涉及国内相关制度建构、国际体系调整的重大安全问题，其解决必然需要一段时间，需要协调多方面主体的共同参与。就国家层面而言，应当注重顶层安全制度的构建，同时还要直面因网络空间边界的不确定性而引发的国际管辖冲突问题。在“全球化”大背景下，国际国内双循环交互的背景下，数据强国的霸权行为不可能止歇，反而借此对我国的打压重塑可能不断加剧。对此，我国应当积极、迅速地推动数据主权安全保障体系与国际轨道接轨，从而保障国家利益和国家安全不受侵犯。

① 冉从敬、何梦婷、刘先瑞：《数据主权视野下我国跨境数据流动治理与对策研究》，《图书与情报》2021年第4期。

② Barbara L.Data Governance: A Quality Imperative in the Era of Big Data，Open Data and Beyond，*A Journal of Law and Policy*，2015（3）.

Study on Data Sovereignty Security in China from the Perspective of National Security

MAO Xinjuan REN Jiayan

[Abstract] Data is a strategic resource related to national security, and data sovereignty security is closely related to national security and comprehensive national strength. Under the increasingly severe data security environment, data sovereignty security risks are becoming more and more severe. How to resist sovereign security risks and ensure data sovereignty security has become a key issue that needs to be answered urgently for national development. Starting from the height of national security, this paper takes the issue of data sovereignty security as the research goal, and uses literature research, policy analysis and other methods to analyze relevant research, policies and regulations and other materials, and clarify the concept, origin, background and data of sovereignty security. Relevant definitions, summarize the risks of data sovereignty in four dimensions from the perspective of our country's national security: data generation and storage, data cross-border inflow and outflow, data analysis and utilization, data extraterritorial jurisdiction and power hegemony. Based on this, this paper puts forward practical countermeasures and suggestions from four perspectives: building data sovereignty territory, improving legal system, developing core technology, and seeking international cooperation, in combination with the current situation of our country's data sovereignty security system. our country's data sovereignty security system provides suggestions and suggestions.

[Key words] National Security, Data Sovereignty, Data Sovereignty Risk, Data Governance, Data Countermeasures

（责任编辑：朱瑞）