Dispute Settlement 争议解决, 2024, 10(4), 125-132
Published Online April 2024 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2024.104208

Hans汉斯

浅析数据跨境流动背景下中国数据治理之策

刘泽宇

华东政法大学国际法学院，上海

收稿日期：2024年2月26日；录用日期：2024年3月4日；发布日期：2024年4月17日

摘　要

数字经济在世界经济发展中所占据的重要地位致使数据成为一项重要的生产要素，而数据的流动是影响数字经济发展的重要推手之一，但当前国际社会中频繁的数据跨境流动在带动世界数字经济发展的同时也为各国基本数据安全利益造成了威胁。在这样的背景下，各国开始以数据主权为依据采取一系列管制措施，从而加强自身对数据的规制，我国也相继出台多部法律法规维护我国的数据权益。然而，需要意识到的是，目前构建数据主权在法理和现实两个层面上均有较大难度，急于构建数据主权可能无法适应数据跨境流动治理的需要。因而，面对平衡好数据安全利益与数字经济发展两者关系的现实要求，我国采用何种治理模式和路径显得尤为重要。对此，本文将首先阐明当下构建数据主权的不合理之处。随后，本文将立足于我国目前的数据规制体系，提出获取具体数据管辖权、建立统一数据管理实体及积极参与国际统一数据治理规则制定三条治理路径，从而平衡好我国国内数据治理和涉外数据治理两个维度，在维护我国数据安全利益的前提下，保障数字经济平稳发展。

关键词

数据跨境流动，数据主权，数据治理

Analysis of China’s Data Governance Strategies in the Context of Cross-Border Data Flow

Zeyu Liu

International Law School, East China University of Political Science and Law, Shanghai

Received: Feb. 26th, 2024; accepted: Mar. 4th, 2024; published: Apr. 17th, 2024

Abstract

The important position occupied by the digital economy in the world’s economic development has

文章引用: 刘泽宇. 浅析数据跨境流动背景下中国数据治理之策[J]. 争议解决, 2024, 10(4): 125-132.
DOI: 10.12677/ds.2024.104208

made data become an important factor of production, and the flow of data is one of the important driving forces affecting the development of the digital economy; however, the frequent cross-border flow of data in the current international community not only drives the development of the world's digital economy, but also poses a threat to the basic data security interests of various countries. In this context, countries have begun to take a series of control measures based on data sovereignty, so as to strengthen their regulation of data, and China has also introduced a number of laws and regulations to safeguard the rights and interests of data from China. However, what is important to realize is that it is difficult to build data sovereignty at both legal and practical levels, and the rush to build data sovereignty may not be able to adapt to the needs of governance of cross-border data flow. Therefore, in the face of the realistic requirements of balancing the interests of data security and the development of digital economy, what kind of governance model and path our country adopts is particularly important. In this regard, this paper will first elucidate the irrationality of the current construction of data sovereignty. Subsequently, based on the current data regulation system in China, this paper will propose three governance paths, namely, acquiring specific data jurisdiction, establishing a unified data management entity, and actively participating in the formulation of international unified data governance rules, so as to balance the two dimensions of China's domestic and foreign data governance, and to ensure the smooth development of the digital economy under the premise of safeguarding China's data security interests.

Keywords

Cross-Border Flow of Data, Data Sovereignty, Data Governance

1. 引言

自第三次工业革命开始，信息技术的高速发展推动了传统国际经贸往来模式的变革，世界进入数字经济时代。数据的流动成为推动数字经济发展的重要因素，数据已然成为信息化社会不可或缺的生产要素之一。然而，数据跨境流动在带来巨大经济价值的同时，也可能会造成数据安全问题，这将触及到一国的基本安全利益。因而，数字大国目前均将数据治理作为一项重要的国家事务对待，并围绕这一议题在政治、法律、科技等多个层面展开了激烈竞争，数据跨境流动的自由、限度及管辖权归属进而成为了各国争议的焦点[1]。各国结合自身实际国情，开始对数据跨境流动治理采取不同的规制模式，通过颁布和出台一系列的数据法律政策争夺数据跨境流动治理领域的话语权。

在此背景下，数据主权的概念成为一国规制数据跨境流动的理论依据[2]，越来越多的国家开始基于自身利益诉求加强对数据的规制，积极推进数据主权化进程，试图强化国家主权对数据这一重要资源的控制。但在法律层面，目前世界各国对数据主权的存在及其内涵仍有较大争议。近几年来，我国先后出台了《网络安全法》《数据安全法》《个人信息保护法》及《关键信息基础设施安全保护条例》等一系列法律法规和政策，国内的数据保护已经出现了基本明确的框架。但由于各国数据治理的分歧，且统一的国际规则尚不存在，我国作为目前世界上最大的跨境电子商务市场，需要对数据跨境流动治理的基础理论等加以厘定，并立足我国现有的数据立法体系，不断完善改进，以更好地应对当下国际环境，提升我国在国际数据治理竞争中的地位。

2. 数据主权化理论的合理性探讨

目前世界各国均积极主张对数据加以规制，以数据主权化为理论基础，试图加强本国对数据的控制与监管。但国家在国际法上所享有的数据权利能否被称为主权、数据是否适合被主权化这一问题值得探讨。

2.1. 数据主权化的法理基础

应当承认，国际法上的国家主权概念并非绝对的，而是随着国际关系的发展而不断发展、演变的。然而，国家主权的概念不能无限制地作扩张解释和延伸。主权这一概念主要是指在一个特定领域内，国家独立自主地处理其一切内外事务的最高权力，这意味着国家对其领域内的一切人、事、物均享有统治权力，且这种权力排除外来侵犯和干涉。因而，需要认识到“国家主权”这一概念能够划定国家所能合法管辖的疆域，设置相对清晰的法律界限，进而明确国家权力的行使范围和内容，遏制他国实施越界行使权力的不法行为，避免不同国家因领域权利归属和管辖界限的不明确而产生争端与冲突，最终引发战争。不难看出，特定领域的界限是一国主权存在的必然要素，一旦超出该领域的边界就会进入其他国家的主权范围或国际公域，该国的主权将丧失其权能，故相对确定的边界对于主权的存在和行使至关重要。然而，在当前全球化背景下，数据的跨境流动日益频繁，数据在产生、存储、转移及处理等过程中会与多个主权国家产生各种各样的联系，一国对数据不受制约的独占管辖可能会对他国数据权利构成侵犯，数据主权的边界难以厘定，高度不确定的边界进而难以成为国家建立一定数据主权的基础，现有国际法也难以要求国家在领域界限模糊的情况下相互尊重彼此间的权利，可见数据主权化理论违背了主权概念的基本内涵，也不具有一定的可行性。

2.2. 数据主权化的必需性

目前来看，国际社会已经出现了承认一国网络空间享有主权的趋向。2003 年联合国信息社会世界峰会通过了《日内瓦原则宣言》，该宣言的第 49 条第 1 款明确提出“与互联网有关的公共政策问题的决策权是各国主权”[3]。《网络活动适用国际法塔林手册 2.0》承认，在本国领土范围内的互联网基础设施以及在本国范围内从事的有影响的网络活动，国家拥有绝对的管辖权，应当受制于其本国的法律[4]。此外，联合国信息安全政府专家组(UN. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security，以下简称 GGE)相继于 2010，2013 和 2015 年出具专家组报告，文中提到：与主权原则相关的国际习惯、规则适用于网络空间，主权国家对本国疆域内的关键网络基础设施具有法律规制的权力[5]。GGE 于 2021 年再次出具报告对过往报告的内容作出了重申，提出国际法尤其是《联合国宪章》，对维护和平与稳定以及促进开放、安全、稳定、无障碍、和平的信通技术环境是适用且不可或缺的，该报告还促请各国避免和不采取任何不符合国际法、特别是《联合国宪章》的措施[6]。基于上述一系列文件，我们可以认为以 2013 年 GGE 报告的通过为主要标志，国际社会出现了国际法（其中包括国家主权原则）适用于网络空间的共识趋向，即承认一国享有对以计算机网络为基础构建的虚拟空间(包括位于一国或地区内的信息基础设施、在此空间内产生的数据以及数据产生、传递和接收全过程、网络参与者及其活动)进行规制的权力。数据作为一种存储后经过整理和分析的信息之集合，其是网络空间唯一的客体，网络空间无法脱离这一客体而存在，二者呈现出紧密结合的关系[7]。在这样的条件下，结合上述文件，一国对数据的管辖，凭借领土主权或网络空间主权即可实现，无需再构建数据主权这一新的主权形式。同时，领土主权和网络空间主权的存在意味着，即使否定数据主权也不会影响到国家对本国数据安全利益加以维护的需要，因为侵犯他国对于数据的管辖权可能构成对他国领土主权或网络空间主权的侵犯，进而违反相关国际法。

2.3. 数据主权化的现实困境

鉴于当下数字产业的高度全球化、数据本身的流动性以及日益频繁的跨境转移，一组数据的连结点往往存在于多个国家之内，数据在产生、存储、传输及利用的过程中会与多国产生联系，这无疑大大增加了国家进行有效管辖的难度。如苏格兰足球联盟曾在英国高等法院起诉，指控位于德国和瑞士的两家企业盗用其数据，并将其分别储存到位于德国和奥地利的终端设备上[8]。在这种情形下，相关国家均有可能援引国际法中的管辖原则(如属地管辖或属人管辖)，同时对某一组数据主张管辖权，存在管辖权竞合的几个国家或通过协商解决，或由居于强势地位的数字大国进行管辖，而其他国家的数据主权最终只会流于形式。即使国家间通过协商解决，国家对数据管辖的实现也会变得主要依赖于国际合作，这就导致管辖的专属性成为了例外，数据主权的构建进而更多地仅具有一种宣示意义。

综上所述，就目前的国际环境而言，由于法理与现实层面的种种难题，数据主权在国际法上缺乏现实意义，数据主权化理论仍有许多问题亟待厘清。考虑到建构数据主权这一新兴主权形式需要面临的种种障碍，急于构建数据主权不仅可能无法在法理上自洽，而且可能不利于实质性地促进对一国数据权利的保障。

3. 我国相关立法现状

数据安全始终是我国政府的重要关切，但与此同时，大力发展数字经济以提升综合国力，提升自身在国际数据治理中的话语权也是我国的发展目标之一。我国目前已经完成了数据立法的基本框架，以《网络安全法》《数据安全法》及《个人信息保护法》为基础的数据法体系正在逐步完善。这其中，涉外数据治理部分主要包括数据分类分级、本地化存储和数据出境安全评估三个部分。

3.1. 数据分级

数据分级最初规定在《网络安全法》第 21 条第 4 项中，要求网络运营者自行采取数据分类分级的措施，并对重要数据进行备份加密，[1]但并未明确分类分级的标准。《数据安全法》第 21 条明确建立数据分类分级保护制度，分类分级的标准包括特定数据在社会经济发展中的重要程度，遭到篡改、破坏、泄露或非法获取利用后对国家安全及公共利益的损害程度等。[2]此外，从 2023 年 1 月 1 日开始实施的《工业和信息化领域数据安全管理办法(试行)》第 8 条第 2 款对数据级别规定为三级，即一般数据、重要数据及核心数据，并在后续的条文中明确了构成这三类数据需要满足的条件，[3]这对《网络安全法》和《数据安全法》作出了进一步的细化。

3.2. 数据本地化存储

《网络安全法》第 37 条首次提出数据本地化存储的要求，并规定境外转移数据需进行安全评估。[4]在之后颁布的《个人信息保护法》中，第 40 条再次确认了数据本地化存储的措施，[5]用以限制关键个人

[1]《中华人民共和国网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露或者被窃取、篡改：……(四) 采取数据分类、重要数据备份和加密等措施；……

[2]《中华人民共和国数据安全法》第二十一条：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。

[3]《工业和信息化领域数据安全管理办法(试行)》第八条第二款：根据数据遭到篡改、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、组织合法权益等造成的危害程度，工业和信息化领域数据分为一般数据、重要数据和核心数据三级。

[4]《中华人民共和国网络安全法》第三十七条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

[5]《中华人民共和国个人信息保护法》第四十条：关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

信息的跨境传输。一方面，数据本地化措施有利于维护我国公民个人隐私权，保障我国数据安全。另一方面，数据本地化措施要求运营商将在我国境内运营过程当中产生和收集到的个人信息和重要数据保留在我国境内进行存储，这有利于我国法院进行司法管辖，增加司法管辖的便利，避免国与国之间的管辖权争议。但过激的数据本地化措施也有可能对数据的正常跨境流动造成不良限制，一定程度上对一国正常稳定的数字经济发展带来制约，如俄罗斯近几年修订的《通信法》等法律[9]，以及印度颁布的《个人数据保护法案》及相关政策[10]。

3.3. 数据出境安全

2022 年，我国网信办发布了《数据出境安全评估办法》，该评估办法明确规定了四种需要通过所在地省级网信部门向国家网信部门申报数据出境安全评估的情形。[6]评估内容大体包括出境目的、范围和方式，数据内容、规模、种类和风险，境外接收方资质、义务和承诺以及拟定立的法律文件内容等。2023 年网信办又发布了《个人信息出境标准合同办法》，以示范性标准合同的形式指引企业履行个人信息保障义务，该办法明确要求个人信息的处理者在与境外接收方订立个人信息出境合同时，应严格适用该办法，[7]但也允许在与附件内容不冲突的情况下约定其他条款。[8]其中第 4 条则对信息处理者以订立标准合同的方式向境外提供个人信息的条件作出限制。[9]同时，该办法第 5 条也要求个人信息处理者在向境外提供个人信息前，应开展影响评估，评估内容与《数据出境安全评估办法》规定的相关内容类似。《数据出境安全评估办法》的出台解决了大规模个人信息、重要数据的安全出境问题，但是对于出境数据规模不大、不属于关键信息基础设施运营者的其他企业而言仍有缺漏。《个人信息出境标准合同办法》则对此进行了填补。目前我国在数据出境安全领域，《网络安全法》《数据安全法》和《个人信息保护法》构建了基本制度架构，《数据出境安全评估办法》和《个人信息出境标准合同办法》等则进一步完善了数据出境安全体系的具体内容，且相互间起到填补衔接的作用。

4. 我国的数据治理路径

就目前国际社会来看，数字经济的高质量发展离不开数据的供给与流动，数字大国和一些大型跨国企业在数据的获取、存储、转移与利用等方面占据着越发强势的地位，多国政府和公民均意识到有必要进一步加强对本地数据的控制。在这样的背景下，人们开始呼吁增强国家对数据的管辖能力，各国也在尽可能加强自身对数据的控制。但如前所述，由于理论与现实层面的重重困境，当前构建数据主权仍有许多不合理之处，要将数据作为一种新的主权形式加以对待仍然存在障碍。我国虽然建立起了较为完整的数据规制体系，对完善数据跨境管理制度和推动数据领域国际合作有重大意义，但仍然面临与国际社会进一步接轨以及国际层面并未形成统一数据治理规则的难题。本文认为我国在推动数据治理的过程中，需要平衡好国家安全与经济发展两个方面的需求，有必要重视国家管辖的自我克制，协调好数据国内规

[6]《数据出境安全评估办法》第四条：数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：(一) 数据处理者向境外提供重要数据；(二) 关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；(三) 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；(四) 国家网信部门规定的其他需要申报数据出境安全评估的情形。

[7]《个人信息出境标准合同办法》第二条：个人信息处理者通过与境外接收方订立个人信息出境标准合同(以下简称标准合同)的方式向中华人民共和国境外提供个人信息，适用本办法。

[8]《个人信息出境标准合同办法》第六条：标准合同应当严格按照本办法附件订立。国家网信部门可以根据实际情况对附件进行调整。个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。标准合同生效后方可开展个人信息出境活动。

[9]《个人信息出境标准合同办法》第四条：个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形：(一) 非关键信息基础设施运营者；(二) 处理个人信息不满 100 万人的；(三) 自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；(四) 自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。法律、行政法规或者国家网信部门另有规定的，从其规定。个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

制与涉外治理两个层次之间的关系。

4.1. 加强对具体数据管辖权的获取

强化国家对于数据的管辖和规制，既有利于防止重要数据泄露以维护国家基本安全利益，也有利于一国维护本国公民和企业的数据权益，从而促进数字经济的发展。但由于目前国际社会就何种数据应适用何种规则尚未达成共识，某一组特定数据之上可能存在不同国家间彼此冲突的管辖权。因此，各国均能凭借本国与一组特定数据或紧密或疏远的联系确定自身对其享有的管辖权力，即使在权力的行使上与他国产生竞合或冲突，也会因国际社会中统一判断规则和标准的缺位而难以被评价为不法行为。这种模糊的状态在现实中极易引发国家间的冲突，例如在棱镜门事件曝光后，欧洲法院于 2020 年 7 月，以美国未能有效保护欧盟公民数据权利为由，单方废止了双方构建的隐私盾数据跨境机制。部分国家为了应对这一冲突开始频繁采取强力的数据本地化措施，但数据的跨境流动是数字经济发展的必然趋势，真正有效的解决方案是要在国际法上厘定数据管辖权分配，划定数据管辖的国家边界。在这样的背景下，有必要分析何种管辖权分配规则有利于我国数据安全与发展利益。考虑到数据主权建构的难度，我国可以明确具体的数据管辖权，即以列举的方式，在法律层面对我国能够管辖的数据类型加以明确，管辖的范围可以包括在我国境内硬件设施上存储的数据、在我国境内进行分析和处理的数据、对我国公民和企业以及向我国境内提供的数据产品等。同时，我国也可与其他国家订立国家间的双、多边协定，共同确定彼此间数据跨境流动的管辖权分配规则，减少管辖争议及冲突。同时，需要意识到一国在推动数据管辖权分配规则建构时，不仅在对他国权力进行约束，也会在一定程度上限制自身权能的行使[1]。例如，若我国主张对领域内数据信息终端上存储的数据享有管辖权。那么，当他国以某一组数据存储于其领域内终端为由，拒绝我国对这些数据进行管辖时，我国也只得遵循自身主张的规则而放弃管辖。因而，我国在积极争取具体数据管辖权时，也有必要保持一定的克制。

4.2. 设立统一的数据安全行政主体

大量个体信息数据的积聚，不仅涉及到个人权益，而且很多时候会牵涉到公共利益。《数据安全法》虽明确了数据安全的负责主体，由中央国家安全领导机构负责数据安全工作和统筹协调，各地区、各部门、各行业主管部门负责本领域的数据安全，国家网信部门统筹协调网络数据安全与相关监管。[10] 但问题是数据具有极大的流动性和共享性，统一、协调的监管机构将更能够满足数据监管的需要，若各部门各自承担其负责领域的数据安全监管责任，可能会出现管理效率低下、相互推诿、政策矛盾及管理真空等问题，可以考虑将数据领域相关职责统归于一个部门，如欧盟设立了欧洲数据委员会(European Data Protection Board，简称 EDPB)管理欧洲数据安全事务。如此，该部门将负责数据法律法规及政策的具体落实、数据安全的风险评估、个人信息出境标准合同审查以及外国有关部门沟通和数据跨境流动治理等多个活动。此外，该部门在适当条件下还可为我国企业与公民就数据跨境流动提供信息上的支持与帮助，如商务部印发的对外投资合作国别(地区)指南，其内容涵盖一国的基本概况、经济概况、投资环境、法规政策等多项内容，并指导企业在当地建立起和谐关系、寻求帮助等，为我国法人与公民在当地开展经贸活动提供了极大的资讯帮扶。

[10]《中华人民共和国数据安全法》第五条：中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。第六条：各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

4.3. 国内与国际治理相结合

数据跨境流动的客观存在使得一国对某一组数据的管辖不仅要对国内法进行考量，还要考虑到现行国际规则的内容。国内规则与国际规则的良好衔接有利于完善我国的数据治理，积极参与国际规则也能够促进国与国、企业与企业之间的数据流动，建设更为开放的国内市场，并以此促进国内企业更加高效地走向境外市场，推动数字经济进一步发展。关于数据跨境流动的监管以及数据管辖权的分配，我国要积极参与国际规则与标准的构建：一方面，可以基于我国的数据治理经验提出切实可行的中国方案。我国目前已然凭借发达的数字经济产业步入数字大国之列，我国当下数字经济的体量仅次于美国，并领先于世界其他主要经济体[11]。在这样的背景下，我国的数据治理经验将成为相关国际规则制定所要考量的重要因素之一，这使得我国在构建国际数据监管规则的过程中占有着不可或缺的重要地位。我国应积极参与国际数据跨境流动治理规则的制定，厘清国家数据权力范围及管辖规则，积极构建公平公正统一的国际规则与标准，《区域全面经济伙伴关系协定》(Regional Comprehensive Economic Partner-ship，以下简称 RCEP)中关于国家安全与数据利用平衡的相关规定值得思考与借鉴[12]。另一方面，我国在接受相关国际规则或加入有关双多边协定后也应严格履行，采取必要措施，以保证相关法律在我国境内的履行。“条约必须遵守原则”(pacta sunt servanda)，这一国际法基本原则要求条约生效后缔约各方应严格按照条约的规定，行使自己的权利并履行义务，不得随意违反。2022 年 1 月，RCEP 正式对我国生效，其中包含针对数据本地化存储和数据跨境流动进行规制的内容。此外，我国积极申请加入《全面与进步跨太平洋伙伴关系协定》(Comprehensive and Progressive Agreement for Trans-Pacific Partnership，简称 CPTPP)及《数字经济伙伴关系协定》(Digital Economy Partnership Agreement，简称 DEPA)，其中也包含有保障数据自由跨境流动与利用的规定。我国在加入国际条约后，就应当积极采取有效措施，确保国内法与条约规定保持一致，展现负责任大国的正面形象，这无疑也有利于后续我国进一步参与国际数据治理。

5. 结语

随着数字经济的快速发展，尽管各国所采取的措施因国情不同而存在差异，但世界各国均在致力于加快推进数据主权的建构，加强本国对数据的管辖。然而，数据主权与国际法上的国家主权概念并不吻合，数据主权因当下频繁的数据跨境流动而缺乏明晰的界限，无法明确国家权力的行使范围。数据主权这一新兴主权形式也因网络空间主权的存在而失去了其存在的必需性。此外，日益频繁的数据跨境流动导致多国连结点普遍存在，国家间的管辖权无法明晰，极易产生管辖权冲突，这无疑大大增加了数据主权的现实建构难度。

对我国而言，保障数据安全、维护我国基本利益固然重要，但也应认识到数据主权化理论的不合理之处以及依托领土主权和网络空间主权进行数据跨境流动治理的可行性与便利性。因此，一方面，我国在涉外数据领域应不断进取，考虑将数据监管职责集中于统一的数据安全监管行政主体，积极争取更加具体的数据管辖权，参与国际社会中统一数据治理规则和标准的制定，完善我国数据跨境流动的规制；另一方面，我国在主张数据管辖时也应保持一定的克制，明确自身利益诉求，尊重他国合法合理的数据管辖权，处理好国内法与国际法两个层面之间的关系，并积极结合我国的数据治理经验向国际社会提出切实可行的中国方案。

参考文献

[1] 陈曦笛. 法律视角下数据主权的理念解构与理性重构[J]. 中国流通经济, 2022, 36(7): 118-128.

[2] Ruohonen, J. (2021) The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, **31**, 439-456. https://doi.org/10.1007/s11023-021-09566-7

[3] 朱诗兵, 张学波, 王宇, 等. 世界范围内网络主权的主要观点综述[J]. 中国工程科学, 2016, 18(6): 89-93.

[4] 王爱玲, 达妮莎. 坚持“网络主权”的中国声音及国际认同分析[J]. 大连理工大学学报(社会科学版), 2020, 41(6): 6-13.

[5] UN. Secretary-General (2024) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note/by the Secretary-General. https://digitallibrary.un.org/record/753055?ln=zh_CN

[6] UN. Secretary-General (2024) Developments in the Field of Information and Telecommunications in the Context of International Security: Note/by the Secretary-General. https://digitallibrary.un.org/record/3908015?ln=zh_CN

[7] 师华, 郭乔. 国际法语境下的数据主权规则探究[J]. 海关与经贸研究, 2023, 44(2): 1-12+85.

[8] England and Wales High Court (2024) Football Dataco Ltd & Ors v. Sportradar GmbH & Anor. https://www.bailii.org/ew/cases/EWHC/Ch/2010/2911.html

[9] 何波. 俄罗斯跨境数据流动立法规则与执法实践[J]. 大数据, 2016, 2(6): 129-134.

[10] 戴永红, 陈思齐. 印度数据本地化: 网络利益边疆的碰撞与机遇[J]. 南亚研究季刊, 2022(2): 93-112+159.

[11] UNCTAD (2024) Digital Economy Report 2021. https://unctad.org/system/files/official-document/der2021_en.pdf

[12] 高通. 解析《区域全面经济伙伴关系协定》中的数据跨境流动规则[J]. 中国信息安全, 2021(5): 82-84+88.