国际法研究

数据主权的博弈与理论重构

汤　铮

内容提要:随着全球数字化进程的加速,数据主权已成为国际社会关注的焦点。数据主权是国家主权权能在数据治理上的具象化,为国家进行有效的全球数据治理提供理论基础。然而,数据主权的理论并不成熟,导致其在具体应用中出现了诸多分歧和博弈。数据主权的实施原则,如数据所在地原则、效果原则、行为发生地原则和数据控制者原则,在应对数据的流动性、分布式存储和跨境传输过程中出现的监管冲突时,均面临不同程度的局限性。同时,数据本地化和数据出境治理这两大实施机制在实践中也引发了国家间的管辖权冲突。应当以国家对无形物的主权及保护义务为基础,建立以合理联系与国家责任为核心的主权实施机制。这样中国可更有力地主张全球数据治理话语权,并在多边框架下推动达成更有弹性和包容性的规则共识。

关键词:数据主权　属地主义　数据本地化　数据出境　管辖

汤铮,武汉大学国际法研究所教授。

一　问题的提出

主权的概念源于1648年签订的《威斯特伐利亚和约》,该和约确立了国家在其领土范围内拥有最高统治权以及对外独立的权利。〔1〕传统上,国家行使主权严格以领土为边界。然而,随着数据在经济和战略层面的重要性日益凸显,出现了“数据主权”概念,强调国家对无形的数据同样享有管控和治理的权力。国家可以通过立法、行政和司法手段,确保数据处理活动符合国家的法律与政策,维护国家的安全和利益。〔2〕

数据主权概念提出之初并未获得广泛认同,很多国家批评其属于“数据保护主义”,

〔1〕 参见冉从敬、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年第6期,第20页。

〔2〕 See Franziska von Scherenberg, Malte Hellmeirer & Boris Otto, Data Sovereignty in Informationa Systems, 34 *Electronic Markets* 14, 15 (2024).

对无形数据流动进行人为阻断。[3] 另一种观点主张,因为数据的生成、使用与流动牵涉国家安全、经济秩序与国民权利,国家对数据理应享有相应的立法、司法与执法权。[4] 虽然存在理论上的争议,但是随着数字经济的快速发展,各国对数据的治理意愿逐步加强。尤其是在“棱镜门”事件后,各国更是加强了对数据的管治。即使主张数据自由流动的美国,也对某些类型的数据实施出境管控,并积极扩展对数据的域外管辖权,这本质上就是在行使数据主权。时至今日,几乎所有国家都行使了不同程度、不同范围的数据主权,数据主权的存在已经成为实践共识。[5]

数据主权作为数字时代国家主权的延伸,实质上关乎国家间权力的分配,因而是一个重要的国际法问题。数据主权的兴起源于数字技术的快速发展和数据跨境流动的复杂性。各国出于国家安全、经济利益和个人隐私保护的考虑,纷纷出台法律法规对数据跨境流动进行监管,行使数据主权。然而,这种实践更多是针对现实需求的应急反应,而非基于系统性理论构建。数据监管问题的紧迫性使得各国在实践中“先行一步”,而理论层面的探讨却相对滞后。这种“实践先于理论”的格局造成了两方面问题:其一,数据主权尚未形成统一的理论基础,导致传统主权原则在数字环境中的适用面临诸多争议,特别是在数据的跨境流动与属地控制难以匹配的情况下,管辖权归属缺乏一致认定依据。其二,各国在缺乏理论共识的背景下,依据各自政策偏好与利益逻辑采取了分化的数据治理策略,加剧了国际规则的不兼容性,并引发数据管辖冲突与地缘政治摩擦。

本文旨在对数据主权的基本理论进行探讨,比较数据主权不同实施原则的利弊及其在全球数据治理中的博弈,分析数据本地化和数据出境治理的实践争议,并在此基础上重构数据主权的理论框架。

二 数据主权实施原则之争

数据主权的实施原则是各国行使数据主权的基础,也是全球数据治理博弈的核心领域。这些原则为国家对数据的控制、管理以及跨境流动的监管提供了理论依据,同时也成为各国在数据治理中争夺主导权的焦点。本文将当前数据主权的实施原则总结为以下四个:数据所在地原则、效果原则、行为发生地原则和数据控制者原则,这些原则为国家行使数据主权提供了多样化的路径。然而,由于各国在数据治理目标、经济利益和安全需求上的差异,这些原则在实际应用中引发了广泛的分歧与博弈,加剧了全球数据治理的碎片化。

(一)数据所在地原则

1. 数据所在地原则的理论基础与实践应用

数据所在地原则是当前数据主权实施中最具影响力的原则。尽管数据是无形的,但

---

〔3〕 See Alexandra V. Orlova, “Digital Sovereignty”, Anonymity and Freedom of Expression: Russia’s Fight to Re-Shape Internet Governance, 26 *U. C. Davis Journal of International Law & Policy* 225, 225-248 (2020).

〔4〕 参见高岚、高国柱:《基于领土性的数据主权理论证成及治理》,《海峡法学》2023 年第 3 期,第 19-20 页。

〔5〕 See Anupam Chander & Haochen Sun, Sovereignty 2.0, 55 *Vanderbilt Journal of Transnational Law* 283, 290-305 (2022).

其存储依赖于物理载体,如服务器或数据中心。这些物理设施将数据的存储位置固定化,从而为国家行使数据主权提供了明确的物理基础。基于传统国际法中的属地原则,国家对其领土内的物项享有排他性管辖权。数据所在地原则通过将数据的物理存储位置和主权管辖范围相结合,为国家对境内数据行使主权提供法理依据。另外,数据所在地原则还源于国家对境内物理载体的实际控制能力。国家可以通过扣押、封存或监管境内的服务器或数据中心,对储存在其境内的数据直接施加控制。[6]《塔林手册 2.0》明确指出:"所有专家一致认为,数据所在的国家将拥有对该数据的完全管辖权。"[7]这一共识反映了国际社会对数据所在地原则的广泛认同。

2. 数据所在地原则的局限

数据的分布性和动态性使其物理位置难以确定,导致数据所在地原则在数字时代面临诸多挑战。一方面,数据可以分割。利用数据这一特征,可以利用计算机技术对数据进行分布式储存。如云计算技术使得数据可以分布式存储在全球多个数据中心,单一国家难以对全部数据实施有效控制。虽然国家可以对存储于境内的部分数据片段行使管辖权,但是部分数据并不能提供任何有意义的信息,从而削弱了数据所在地原则的实际效力。[8]

另一方面,数据可以快速流动,使得数据的物理位置难以固定。[9] 在跨境数据传输中,数据可能从一国流出并存储于另一国的服务器,使得原数据所在国难以继续行使主权,而数据流入国则可能基于属地原则主张主权。这一点与许多国家的数据监管理念相悖。如欧盟认为,当个人数据的来源和主体是欧盟公民时,欧盟有义务保护其隐私权。根据《通用数据保护条例》(*General Data Protection Regulation*)第 3 条第 2 款,如果外国数据处理者在欧盟提供商品或服务时获取个人数据并将其存储于外国,该公司必须遵守欧盟数据处理的规定。但是,根据数据所在地原则,欧盟并非数据所在地,只有数据流入国才可以主张主权。比如印度根据数据所在地原则,授权其执法部门拦截、监控及解密境内存储或接受的任何数据,[10]这就直接造成与欧盟数据保护法的冲突。

(二)效果原则

1. 效果原则的理论依据与国际实践

效果原则允许国家对在其境内产生实质性影响的行为行使主权,不论行为发生地位于何处。[11] 效果原则的核心在于,行为的"效果"而非行为发生地是国家行使主权的基础。当一国境内自然人的数据被收集、分析、处理或传输时,行为对自然人的隐私和个人

〔6〕 See Patrik Hummel, Matthias Braun et. al., Data Sovereignty: A Review, 8 *Big Data & Society* 1, 7 (2021).

〔7〕 See Michael N. Schmitt (ed.), *Tallinn Manual* 2.0 *on the International Law Applilcable to Cyber Operations*, Cambridge University Press, 2017, p. 63.

〔8〕 参见郭烁:《云存储的数据主权维护——以阻断法案规制"长臂管辖"为例》,《中国法律评论》2022 年第 6 期,第 74-75 页。

〔9〕 See Patrik Hummel, Matthias Braun et. al., Data Sovereignty: A Review, 8 *Big Data & Society* 1, 6 (2021).

〔10〕 See Basu Subhajit & Richard Jones, Indian Information and Technology Act 2000, 19 *International Review of Law, Computer & Technology* 209, 209-230 (2005).

〔11〕 Harvard Research on International Law, Jurisdiction with Respect to Crime, 29 *American Journal of International Law* (*Supplement*) 435, 487-494 (1935); United States v Alcoa, 148 F. 2d 416 (2d Cir. 1945).

信息将产生影响;当涉及境内公共利益和基础设施的重要数据被泄露或滥用时,行为对境内公共利益和公共安全将产生影响。根据效果原则,即使数据存储于境外或数据处理行为发生于境外,只要处理数据的效果及于境内,国家就有权行使主权。欧盟《通用数据保护条例》第 3 条体现的就是效果原则。不论数据处理者是不是欧盟企业,也不论数据处理行为发生在何地,只要处理数据的行为构成向欧盟境内数据主体提供商品或服务所需之环节或对欧盟境内数据主体的行为进行监控,均受《通用数据保护条例》的管辖。〔12〕 我国《数据安全法》第 2 条规定,发生在中国境外的数据处理活动,如果损害了我国国家安全、公共利益或公民、组织合法权益,可以依照该法追究责任。《个人信息保护法》第 3 条也规定,在境外处理中国境内自然人个人信息的活动,如果以向境内自然人提供产品或服务为目的,或用以分析、评估境内自然人的行为,应受该法管辖。

2. 效果原则的局限

尽管效果原则已经成为多国实施数据主权的重要原则,但仍面临诸多争议。

第一,效果原则可能导致不同国家之间的管辖权冲突,特别是与数据存储地和行为实施地的冲突。在“谷歌诉法国数据保护机构案”(下称“谷歌案”)中,法国数据保护机构(CNIL)要求谷歌在全球范围内删除用户请求链接,实施欧盟《通用数据保护条例》赋予欧盟境内自然人的被遗忘权。基于效果原则,即使数据存储地和处理行为均在欧盟境外,只要影响欧盟公民就应当适用欧盟数据保护法。但是谷歌认为,依据属地原则,欧盟监管机构无权要求谷歌在全球范围内删除信息。〔13〕 在“史莱姆斯 II 案”中,爱尔兰数据保护组织基于效果原则,质疑美国大规模监控侵犯欧盟《通用数据保护条例》赋予欧盟数据主体的隐私权。美国则根据数据存储地原则,认为美国政府有权获得已经存储于美国境内的欧盟个人数据。该冲突最终以欧洲法院裁定《欧美隐私盾协议》(*EU-US Privacy Shield*)无效而结束。〔14〕

第二,效果原则的实际执行面临困难。国家虽然可以基于效果原则主张主权,但是主权权力的真正行使需要对行为人或标的物施加强制措施,而一国对境外的人、物或行为可以实施的有效措施非常少。执法机关通常无法在境外对行为人进行惩处,也无法采取查封、没收等执法措施。除非国家可以其很强的经济、金融实力将国家力量传输到海外,否则效果原则存在执行上的困难。〔15〕 在上述“谷歌案”中,由于美国不支持全球适用被遗忘权,美国谷歌决定不需要执行法国命令。即使法国可以对谷歌的法国子公司罚款,也无法直接影响其美国总部的决策。欧洲法院最终裁定被遗忘权不具有全球效力,这反映出效果原则的局限性。

第三,某些数据处理行为虽然与本国关系密切,但由于未对本国产生直接影响,效果原则难以适用。例如,本国自然人的数据在境外被匿名化处理,或本地的非个人、非敏感、

〔12〕 参见刘天骄:《数据主权与长臂管辖的理论分野与实践冲突》,《环球法律评论》2020 年第 2 期,第 188 页。

〔13〕 Case C-507/17 Google v CNIL, ECLI:EU:C:2019:772.

〔14〕 Case C-311/18 Data Protection Commissioner v Facebook Ireland & Schrems (Schrems II), ECLI:EU:C:2020:559.

〔15〕 参见杨永红:《次级制裁及其反制——由美国次级制裁的立法与实践展开》,《法商研究》2019 年第 3 期,第 164-167 页。

非重要数据在境外被用于学术研究。尽管这些数据与本国存在紧密关联,但由于其处理行为未对本国产生实质性影响,国家无法依据效果原则行使管辖权。

(三)行为发生地原则

1. 行为发生地原则的优势

传统国际法中的属地管辖权给予国家管治其领土内所有事务的权力,不但包括人和物,也包括行为。行为发生地原则主张,国家对发生在境内的所有数据处理行为均可行使主权。如我国《数据安全法》第 2 条、《个人信息保护法》第 3 条均明确该法适用于在我国境内开展的数据处理行为。这一原则的优势一方面在于行为的可追溯性。数据处理行为通常有明确的物理发生地,使得行为发生地原则有较强的可适用性。另一方面,国家可以通过对境内行为的直接监管,实现对数据的有效控制。执法部门可以直接要求本国境内的数据处理者进行或停止数据处理行为,也可以拦截境内的数据传输,达到监管的目的。

2. 行为发生地原则的局限

根据行为发生地原则行使数据主权仍然存在挑战。首先,数据的可远程操作性使得数据处理行为与数据存储地分离。例如,云计算技术使得数据处理者可以通过网络处理存储在境外多个国家的数据。[16] 虽然行为发生地国可以对数据处理行为进行有效控制,但当数据和行为发生地缺乏任何实质联系时,强行行使主权不仅缺乏实际意义,还可能引发与他国主权的冲突。这种冲突在数据过境情形中尤为突出。数据过境是指数据被传输至第三国进行处理后再传回原数据存储地。尽管数据处理行为发生在第三国,但数据与第三国并无实质联系,行为的目的和结果仍集中在原数据存储地。因此,第三国根据行为发生地原则对数据行使主权,既不符合商事活动的目的,也不符合国家利益。[17] 我国国家互联网信息办公室 2024 年出台的《促进和规范数据跨境流动规定》(下称"《数据跨境规定》")第 4 条也明确了对未涉及境内个人信息或重要数据的数据过境行为免除数据出境安全评估和认证要求。

其次,随着技术的发展,数据处理行为分为自动和非自动两类。[18] 非自动行为由人工直接实施,依据行为发生地原则行使管辖权尚有合理性。自动行为则通过设备、算法和程序自动完成,或通过物联网设备、摄像头、GPS 等自动收集数据,或通过网络爬虫、批处理等技术自动抓取、传输和分析数据。此类行为无需人工干预,其发生地往往难以确定。固定物理设备的数据处理行为发生地通常是设备所在地,但设备的设置及监控可能由境外主体远程实施。设备所在地虽然能以没收、查封等方式控制设备,却难以有效规制域外主体的行为。在此情况下,行为发生地原则的适用显然存在局限性。更复杂的是,当数据处理通过网络算法进行时,行为发生地会变得更加模糊。算法本身是无形的,且可以通过网络远程抓取和处理数据,比如云计算平台通过分布式算法在全球范围内处理数据,所以

〔16〕 参见田新月:《云计算环境中数据处理行为的法律规制研究》,《重庆邮电大学学报(社会科学版)》2016 年第 4 期,第 38 页。

〔17〕 See Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013, pp. 15-16.

〔18〕 参见田新月:《云计算环境中数据处理行为的法律规制研究》,《重庆邮电大学学报(社会科学版)》2016 年第 4 期,第 38 页。

数据处理行为的发生地几乎无法确定。

（四）数据控制者原则

1. 数据控制者原则的理由

数据控制者原则的核心在于将对数据的管辖权从数据本身转移到对数据控制者的管辖上。数据控制者作为拥有访问和处理数据权力的主体，即使数据的物理载体位于境外，仍然能够对数据进行有效控制和处理。这一原则认为，行使数据主权的有效方式并非直接对领域内的数据行使主权，而是通过对领域内控制数据的主体进行管辖来实现。换句话说，只要数据的控制者或所有者位于一国领土范围内，即使数据存储于境外，该国仍可有效行使数据主权。〔19〕

这一观点已被多个国家的立法实践所采纳。例如，美国《澄清境外合法使用数据法案》（*Clarifying Lawful Overseas Use of Data Act*，下称“《云法案》”）明确规定，美国可以对由美国数据控制者控制的数据行使管辖权，无论这些数据实际存储于何地。〔20〕类似地，欧盟在 2023 年出台的《关于刑事诉讼中电子证据的欧洲提交令和欧洲保全令以及刑事诉讼后执行监禁刑罚的条例》[*Regulation（EU）2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings*，下称“《刑事电子证据条例》”]也采用了相同的方法，允许欧盟成员国的刑事执法部门和法院要求欧盟境内的数据控制者提供电子证据，无论数据存储地位于何处。

从有效控制的角度来看，数据控制者原则可以很好地解决数据属地原则、行为属地原则和效果原则在远程数据处理中的监管缺陷。其核心优势在于，主权行使的对象是控制数据的主体，而非数据本身。即使数据存储于境外，或通过自动化算法进行处理，只要能够控制拥有数据处理权的主体，便可以实现对数据的有效监管。该原则还可以解决数据分布式存储在多个国家带来的数据获取难题。

2. 数据控制者原则的域外管辖争议

数据控制者原则在国际社会中引发了广泛的争议，其核心问题在于主权国家试图通过对境内数据控制者的管辖，间接实现对境外数据的管控。从主权博弈的视角来看，主权国家通过控制境内实体，将管辖权延伸至境外数据，这种做法本质上是对传统主权边界的突破。国际法上的属地管辖虽然包括境内的人，却不包括这些主体拥有的境外物项。数据控制者原则通过将管辖对象从数据本身转移到数据控制者，实质上是对主权作用对象的转换，以达到延伸管辖权的目的。这种通过境内主体管辖境外数据的做法，并不符合习惯国际法承认的域外管辖原则，其国际合法性存疑。〔21〕

数据控制者原则可能会引发国家间的管辖权冲突，加剧数据领域的主权争夺。在

〔19〕 参见刘天骄：《数据主权与长臂管辖的理论分野与实践冲突》，《环球法律评论》2020 年第 2 期，第 182 页。

〔20〕 参见郭烁：《云存储的数据主权维护——以阻断法案规制“长臂管辖”为例》，《中国法律评论》2022 年第 6 期，第 72-81 页。

〔21〕 参见周梦迪：《美国 CLOUD 法案：全球数据管辖新“铁幕”》，《国际经济法学刊》2021 年第 1 期，第 14-24 页。

“微软诉美国案”中,美国执法机关要求微软提供存储在爱尔兰的用户数据,受到了爱尔兰、欧洲委员会和欧洲律师协会的一致反对。[22] 之后美国通过《云法案》规定美国数据控制者有应执法要求提供数据的义务。欧盟一方面通过《欧盟数据治理条例》[*Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act)*]和《关于公平获取与使用数据的统一规则条例》[*Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)*]阻断外国执法和司法机关单边调取数据,另一方面通过《刑事电子证据条例》采用了同样的数据控制者原则允许欧盟执法机关获取欧盟境外数据。其他国家则采取数据本地化、数据出境限制等方法,阻断数据控制者原则的效力。[23] 如何协调数据控制者原则与数据存储地原则的冲突,成为国际数据治理的重要课题。

(五)小结

数据主权的实施原则及其在全球数据治理中的博弈,反映了数字时代主权国家在数据控制权上的复杂竞争。数据所在地原则、效果原则、行为发生地原则以及数据控制者原则,在具体实施中均面临不同程度的局限性和挑战。数据所在地原则虽然具有理论和实践支持,但在数据分布式存储和跨境流动的背景下,其实际效力受到削弱;效果原则尽管为保护本国数据主体和公共利益提供了灵活的工具,却可能引发管辖权冲突和执行难题;行为发生地原则在技术上难以应对远程操作和自动化处理带来的挑战;数据控制者原则虽然试图通过控制主体间接实现对数据的管辖,但其域外管辖的合法性仍存争议,并可能加剧国家间的管辖权冲突。

三 数据主权实施机制的冲突与博弈

数据主权的行使并不依赖统一的国际机制,而是国家基于自身治理的需要,通过具体的制度设计实现数据治理。数据主权的实施机制将抽象的主权原则转化为可操作的实践工具,其核心目标是通过有效的制度设计,确保国家对数据的控制权和管理权得以实现。目前最主要的两类实施机制是数据本地化和数据出境治理。二者在核心理念和治理路径上存在差异,但在实际运行中并非相互排斥,而是共同构成协同治理的制度工具。数据本地化要求数据在产生国境内存储或处理,旨在确保国家对数据的完全控制;数据出境规则通过设置前置条件,限制数据的跨境流动,以保护国家安全、公共利益和个人隐私。当前,数据主权实施机制的组合与运用,在全球范围内呈现出多样化的形态,导致了规则之间的冲突与博弈。

---

〔22〕 Microsoft Corp. v US, 138 S. Ct. 1186 (2018).

〔23〕 参见陈爱飞:《“数据控制者标准”取证模式及中国因应》,《法商研究》2024 年第 3 期,第 68-73 页。

(一)数据本地化的实践争议

1. 支持数据本地化的理由

数据本地化源于一国境内的数据必须在本国境内存储或处理的要求。首先,数据本地化的支持者认为,数据本地化可通过控制数据的地理位置,确保国家对数据的控制权。例如,在著名的“德莱赛公司案”中,[24]美国母公司通过切断与法国子公司的数据链接,导致法国子公司无法履行与苏联的合同。这一事件使得法国政府意识到,获取数据对国家利益至关重要,而数据本地化是确保国家对数据实施控制权的关键手段。[25]

其次,数据本地化能够有效减少因数据跨境存储而引发的管辖权冲突,并降低域外执法的难度。[26] 在数据跨境流动的背景下,同一份数据容易被多个国家主张主权,导致法律适用上的冲突。例如,美国《云法案》和欧盟《刑事电子证据条例》均要求境内的数据控制者应执法机关的要求提供存储于境外的数据。然而,这种要求往往需要进行复杂的利益衡量测试,以平衡数据输出国与数据存储地国之间的法律冲突和利益分歧。这种跨境数据调取的机制将数据控制者置于两难境地:一方面,数据控制者需要遵守本国的法律要求,向执法机关提供数据;另一方面,他们又可能因提供数据而违反数据存储地国的法律,面临法律风险甚至处罚。

最后,数据本地化有助于保护国家安全、公共利益和公民隐私,防止数据在境外存储或处理时被泄露或滥用。[27] 出于保护性的要求,大多国家都实施了数据本地化政策。有的国家采取了严格的数据本地化措施,如俄罗斯在“斯诺登事件”后实施了全面的个人数据本地化政策,要求俄罗斯公民个人数据的收集和存储必须使用位于俄罗斯境内的服务器,并采取严格的执法措施,防止外国政府通过其科技公司获得俄罗斯公民的数据。[28] 2016 年,莫斯科法院因领英没有使用俄罗斯境内的服务器存储数据,命令俄罗斯信息监管局断开与领英的链接。有的国家虽然原则上并未采取数据本地化措施,但对特定数据仍然实施本地化要求,如澳大利亚《我的健康记录法》(*My Health Records Act 2012*)第 77 条要求个人健康数据在本地存储。欧盟虽未强制要求个人数据本地存储,但《通用数据保护条例》对个人数据出境设置了严格条件。监管风险和出境成本导致企业倾向于在本地存储数据,形成“软性数据本地化”。[29]

2. 反对数据本地化的理由

反对者认为数据本地化的真正动机是保护本地企业免受外国竞争的影响,而这将导

---

〔24〕 The Dresser Pipeline Case (1982).

〔25〕 See Theodore Christakis, European Digital Sovereignty, Data Protection, and the Push toward Data Localization, in Anupam Chander & Haochen Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford University Press, 2023, p. 376.

〔26〕 See Chan-Mo Chung, Data Localization: The Causes, Evolving International Regimes and Korean Practices, 52 *Journal of World Trade* 187, 192 (2018).

〔27〕 See Sanghyun Han, Data and Statecraft: Why and How States Localize Data, 26 *Business and Politics* 263, 264, 279 (2024).

〔28〕 参见《俄罗斯联邦法第 242-FZ 号》(*Federal Law No. 242-FZ*)第 18 条。

〔29〕 See Anupam Chander, Is Data Localization a Solution for Schrems II?, 23 *Journal of International Economic Law* 771, 774 (2020).

致不公平竞争。[30] 首先,对于跨国企业而言,数据本地化要求其在多个国家建立和维护数据存储和处理设施,显著增加运营成本。数据本地化使得数据分散程度加大,企业将难以统一运用有效的、适合规模经济和国际经验的方式管理数据安全。其次,数据本地化将全球市场分割成局域市场,可能阻碍国际贸易。最后,数据本地化可能违反比例原则,尤其是在数据基础设施和技术水平较低的国家,本地化可能无法有效保护数据安全,反而增加数据泄露风险。[31]

绝大多数国家并没有采取全面的、绝对的数据本地化措施,而是将本地化与数据出境管制结合进行数据治理。即使实施严格数据本地化的国家,如俄罗斯,也并不禁止个人数据在通过安全审查之后向境外传输,并在外国存储"镜像"数据。有的国家根据数据的特点和类型,利用分类分级的方法使得数据本地化更加科学合理。如中国仅要求重要数据、批量个人数据、政府处理的个人数据、关键信息基础设施运营者和批量个人数据处理者在境内收集和产生的个人数据在本地存储。[32] 还有很多国家曾试图采用严格本地化措施,但是在经济和贸易压力下,最终仅采用有条件出境的方法保护数据安全。如印度、巴西和南非都曾出台全面数据本地化的立法草案,但最终均采用了与欧盟类似的有条件出境政策,即软性数据本地化措施。

美国出于对自身经济利益的维护,长期以来反对数据本地化政策。美国是全球大多数数字巨头公司的母国,这些公司依赖全球数据的自由流动来运营和扩展业务。数据本地化政策会增加这些企业的合规成本,限制其获得大量外国数据,也限制其在全球拓展市场,从而可能削弱美国的经济优势。[33] 美国通过控制全球数据流动,也可以为本国企业提供竞争优势。美国《云法案》的有效运作,就是建立在外国数据可以自由出境的基础上,进一步巩固了美国的数据霸权地位。但是即使是美国,也要求敏感政府数据在境内存储,在实践上并非完全排除本地化。[34]

(二)数据出境治理的主权博弈

实施数据主权的另一个重要机制是数据出境治理。由于国家对境外数据的管控存在困难,许多国家通过设置数据出境的前置条件,确保主权的强制力不因数据出境而削弱,保护本国利益不因数据跨境流动而受损。数据出境治理是数据主权在数据全球流动中的体现,也是数据主权突破属地控制向域外扩张的手段,以维护国家对本国数据保持持续的控制权。

---

〔30〕 See Theodore Christakis, European Digital Sovereignty, Data Protection, and the Push toward Data Localization, in Anupam Chander & Haochen Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford University Press, 2023, p. 375.

〔31〕 参见彭岳:《数据本地化措施的贸易规制问题研究》,《环球法律评论》2018 年第 2 期,第 180-181 页。

〔32〕 《网络安全法》第 37 条,《个人信息保护法》第 36 条、第 40 条。

〔33〕 See John Selby, Data Localization Law: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?, 25 *International Journal of Law and Information Technology* 213, 215-216 (2017).

〔34〕 Federal Acquisition Regulation, § 39. X02-2 (b) (1) (2023 年美国国防部等部门提议加入明确的本地化条款,参见 proposed by the Defense Department, the General Service Administration, and the National Aeronautics and Space Administration on 10/03/2003, https://www.federalregister.gov/d/2023-21327/p-241, 最近访问时间[2025-07-14]); Defense Federal Acquisition Regulation Supplement, § 239.7062-2.

各国对数据出境治理的路径选择,体现出不同的数据主权理念。目前,全球范围内的数据出境治理可以分为自由流动模式、安全优先模式、人权保护模式和利益平衡模式。自由流动模式以美国为代表,对数据出境采取的基本原则是反对本地化,允许自由流动,仅对少数重要数据(如政府数据、军用技术)的出境加以限制,或者限制批量个人数据与敏感个人数据传入“受关注国家”(Countries of Concern)。[35] 该模式强化了美国的全球治理逻辑,即国家应通过域内企业的全球运营能力维持技术主导,而非直接限制数据流动,并利用针对性出境管控维护美国的经济实力与技术霸权。而以欧盟为代表的人权保护模式则通过《通用数据保护条例》为境内数据主体提供了一系列权利,并要求这些权利不受数据出境而减损。为实现这一目标,根据该条例第 44-47 条,欧盟委员会有权将达到欧盟数据保护标准的国家列入“充分性认定”白名单,允许数据向这些国家自由出境;对于未被列入白名单的国家,数据出境则需要通过标准合同条款、约束性公司规则、安全认证或行业规范等工具。欧盟的数据出境制度虽然以属地生成为前提,但是强化属人导向和人权价值的输出。以俄罗斯为代表的安全模式则强调国家对本国数据的绝对主权,在全面数据本地化的基础上,对个人数据出境实施严格的安全审查,对数据主张属地控制的排他性。[36] 而采取利益平衡模式的我国,则通过 2024 年出台的《数据跨境规定》,尝试在发展、安全、人权中寻找制度协调空间,通过数据分类分级保护制度与场景豁免机制,在保障我国数据安全的同时促进数据有序自由流动。[37]

四大数据出境治理模式不仅反映了各国在数据主权与全球数据流动之间的权衡,更是大国主权博弈的核心领域。

首先,发达国家与发展中国家在数据治理上的分歧明显。发达国家借助其强大的经济实力和治理能力,更倾向于突破主权的属地原则对外进行规则输出。如欧盟通过“充分性认定”机制,将符合其数据保护标准的国家列入数据出境白名单,促使许多国家修改本国数据保护法,推动了欧盟数据保护标准的国际化。[38] 美国一方面推动数据自由流动的治理框架,试图将全球数据流动规则与其经济利益绑定,另一方面通过对境内外企业的经济控制,限制敏感数据的跨国流动。[39] 此外,欧美均允许权力机关单方面调取域外数据。为应对外部单边域外管辖扩大的压力,发展中国家不得不通过数据本地化措施和出境限制来维护数据主权。例如,俄罗斯实施全面数据本地化和出境申报要求,我国《个人信息保护法》第 41 条明确禁止个人信息处理者非经中华人民共和国主管机关批准或基于

〔35〕 See Protecting Americans' Data from Foreign Adversaries Act ("PADFA"), H. R. 815, 118th Cong. Div. I (2024); Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Exec. Order No. 14,117, 89 Fed. Reg. 15421 (2024); Preventing Access to U. S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 2024-31486 (90 FR 1636) (2025).

〔36〕 《俄罗斯联邦个人数据保护法》第 12 条第 10 款。

〔37〕 《数据跨境规定》第 3、4、5、6、8 条。

〔38〕 参见金晶:《个人数据跨境传输的欧盟标准——规则建构、司法推动与范式扩张》,《欧洲研究》2021 年第 4 期,第 91-92 页。

〔39〕 See Maria Vasquez Callo-Muller, From APEC to Global: the Establishment of the Global CBPR Forum, 20 *Global Trade and Customs Journal* 130, 130-143 (2025).

互惠原则向外国司法或执法机构提供存储于中国境内的个人信息。这些措施直接构成了对美欧单边获取域外数据的阻断,体现了发展中国家在数据主权上的防御姿态。

其次,发达国家之间的博弈同样存在。如美国的自由流动模式与欧盟的人权保护模式之间形成了显著张力。欧盟对数据主体人格权的高标准保护,使其在“史莱姆斯 I 案”和“史莱姆斯 II 案”中两次认定欧盟与美国之间的数据流动协议(“安全港”和“隐私盾”)无效。欧洲法院认为,欧盟对个人数据权的保护是全方位和多层次的,不仅要求数据出境后免被私人公司滥用,还要求政府不得轻易获取个人数据,并为数据主体提供充分的救济途径。[40] 尽管欧美在 2023 年针对这两点要求再次签订了《数据隐私框架》[*Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data under the EU-US Data Privacy Framework*],但其能否有效防止美国政府过度监控仍有待观察。这种模式之间的冲突不仅反映了欧美在数据治理理念上的分歧,也凸显了全球数据流动规则的复杂性。

再次,有的数据出境工具虽以技术中立和权利保障为名义制定,但在实践中却显现出政治考量。以“充分性认定”制度为例,虽然设计初衷是衡量目标国家的数据保护水平是否达到同等标准,但该机制在实施中往往不仅考察目标国的数据立法与执法机制,还隐含评估该国与认定国之间的文化、经济与地缘战略上的关系。如欧盟的“充分性认定”名单中,包括马岛、泽西、根西等微小行政区,以及一些数据保护机制存在疑问但是与欧盟存在紧密政治经济联系的国家,如阿根廷、英国、美国。[41] 俄罗斯的“充分性认定”名单也包括马里、加蓬和哈萨克斯坦等法治体系较薄弱,数据保护未达到欧洲委员会第 108 号公约,即《个人数据自动化处理中的个人保护公约》(*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*)的数据保护标准,但是与俄罗斯有紧密联系的国家。“充分性认定”的选择性与政治性适用,加剧了全球数据治理体系的分化,使得国家间的数据跨境安排丧失统一标准。

最后,数据出境治理的分歧已日益呈现出强烈的地缘政治色彩,成为不同国家主权理念与治理目标交锋的重要领域。我国 2024 年出台的《数据跨境规定》意在通过差异化规则安排,实现对数据流动的分类管理与有条件开放,在确保国家安全与个人隐私的前提下,为国际贸易、科研交流等活动释放更多数据要素活力,以推动数字经济发展。同年,美国相继出台行政命令与监管规则,明确限制敏感个人信息、政府数据及大规模用户数据向包括中国、俄罗斯在内的所谓“高风险国家”传输,表明美国的数据出境治理仍是维护国家安全和战略竞争的工具。[42] 在全球数据治理尚未形成统一规范的背景下,二者的治理分歧在国际合作、法律互认和制度兼容性上制造了深刻张力,成为未来数据主权国际合作必须直面的挑战。

---

〔40〕 Case C-362/14 Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650; Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, ECLI:EU:C:2020:559.

〔41〕 See Duncan McCann, Oliver Patel & Javier Ruiz, *The Cost of Data Inadequacy*, 2020, pp. 9-12, https://neweconomics.org/uploads/files/NEF_DATA-INADEQUACY.pdf, 最近访问时间[2025-06-15]。

〔42〕 参见王海滨:《美国涉华数据出境限制政策评析》,《现代国际关系》2025 年第 1 期,第 105-149 页。

(三)数据主权实施机制冲突之根源

尽管国家间的域外管辖权冲突长期存在,但在数据高度流动化与国际化的背景下,这种冲突愈发激烈和复杂,已经对全球数字经济的稳定运行构成实质性干扰。当前,各国围绕数据本地化与数据出境治理所展开的制度对抗,并非仅源于技术性手段或监管路径的差异,其深层根源在于国际社会未能就数据主权的归属原则及适用边界达成基本共识。在这一核心问题上,既缺乏统一明确的判断标准,也没有形成具备权威性的优先适用规则或主权分配机制,导致各国在行使数据主权时发生冲突。由于数据主权的边界不清,一些国家可能滥用传统管辖原则不当向域外扩张管辖权,造成国家间的政策张力。而与相关数据有实质利益联系的国家,虽然可以基于属地原则对本国境内生成并存储的数据主张主权,但数据出境进入接收国的领域之后,原属地主权国家对数据的控制力难以维系。而数据流入地可以根据属地原则,对源于他国的数据实施有效管控。持续治理与本国有实质联系的数据只有两种方法,第一是将数据保留在境内,形成数据本地化机制,对抗外国对源于本国的数据实施控制的行为;第二是对数据出境进行审查和限制,通过限制数据的跨境流动,达到维持本国对数据持续控制的目的。

当前全球数据主权实践呈现高度碎片化趋势,尽管可通过双边谈判与国际协议在技术层面予以一定缓解,例如美欧在历经“安全港”和“隐私盾”机制两度失败后,重新达成《数据隐私框架》协议,重启跨境数据流动合作。但从更深层次看,这种碎片化反映了传统主权理论在数字时代所遭遇的内在困境。在数据主权的基本理念与适用原则尚未形成国际共识的背景下,现有国际合作机制难以实现实质性突破。因此,有必要构建一个能够统筹各国核心关切的创新性理论框架,借助系统性研究重新界定数据主权的适用规则与边界,从而为国际合作奠定更为坚实的规范基础。

四 数据主权的理论重构

传统主权理论在面对数据的非物质性和流动性等特征时适应性不足。由于数据主权缺乏坚实的理论基础支撑,导致在跨境数据治理中出现频繁的冲突。因此,亟需从理论层面对数据主权的基本范畴、归属逻辑与行使边界进行系统重构,确立符合数字时代特征的解释框架。

(一)数据主权的理论基础

1. 当前数据主权理论基础的缺陷

当今理论界对数据主权的理论基础存在不同的理解,最具代表性的有两种观点。

第一种观点认为,数据主权是网络空间主权的分支。[43] 网络空间主权的实施基于属地管辖原则,即国家对位于其领土内的网络基础设施和网络行为具有管辖权。联合国《关于从国际安全的角度看信息和电信领域发展政府专家组报告》(Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in

〔43〕 参见翟志勇:《数据主权的兴起及其双重属性》,《中国法律评论》2018 年第 6 期,第 196-197 页。

the Context of International Security)第20条明确承认国家对信息通信技术基础设施的管辖权。而《塔林手册2.0》第1条也提出"一国可对其主权领土内的网络基础设施和网络行为实施控制"。换言之,因为国家对位于其领土内的网络基础设施和网络行为具有管辖权,因此也对网络上运行的数据存在管辖权。〔44〕这个理论支持了实施数据主权的行为发生地和控制者所在地原则。然而,数据与网络空间并不能完全等同。首先,数据的存在并不必然依赖网络。根据我国《数据安全法》第3条,数据是"任何以电子或者其他方式对信息的记录"。即使没有网络,数据仍然可以通过硬盘、光盘、纸质记录等物理介质存储和传输。〔45〕因此,数据主权的客体不仅包括网络上运行的数据,还包括物理介质中存储的数据。〔46〕此外,网络空间的治理对象主要是网络基础设施、网络行为和网络协议,旨在保护网络安全;而数据的治理对象则主要是数据处理活动以及数据主体的权利和义务,旨在保护数据安全和数据主体的权利,二者的治理目的存在差异。

第二种观点认为,数据需要依靠载体才能被记录、存储和呈现,因此数据存在一定的物理属性,数据主权是基于对载体的主权。〔47〕这一理论直接支持了数据所在地原则。然而,这一论证未能准确把握数据与载体之间的本质区别,也混淆了国家对载体和对数据本身的权力范围。数据与载体虽然在形式上密不可分,但在性质上存在根本差异。数据是无形的、抽象的,其价值在于其所承载的信息内容;而载体是有形的、具体的,其价值主要在于其物理属性。数据的无形性和信息属性使其具有高度的流动性和可复制性,而载体的有形性则使其受限于物理空间和属地管辖。当数据分布式存储于多个载体时,多个载体所在地国家可能同时主张主权,这不仅不符合数据治理的目标,还可能导致管辖权冲突。当数据关系国家利益并与国家建立了密切联系时,国家对数据的治理权力不应当因为载体出境而消失。

2. 数据主权是对无形物的主权

因此,学术界需要重新审视数据主权的理论基础。本文主张数据可被类比为"无形物"。〔48〕国家对领域内的物拥有主权,这是主权的基本表现形式。尽管无形物缺乏物质形态,但它们通常由国家通过公权力创设、承认或保护,并与相关国家存在天然联系。因此,国家对无形物可以主张主权。〔49〕

应当承认,学界对于数据的属性远未达成共识。很多学者反对将数据视作民法上的"物",主要理由是数据的非独占性与物权基本理论体系存在结构性冲突。〔50〕传统物权理论强调物的稀缺性和排他性,与数据无限复制性和共享性矛盾。然而,这个观点混淆了

〔44〕 参见徐凤:《网络主权与数据主权的确立与维护》,《北京社会科学》2022年第7期,第57-58页。

〔45〕 参见师华、郭乔:《国际法语境下的数据主权规则探究》,《海关与经贸研究》2023年第2期,第4页。

〔46〕 参见冉从敬、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年第6期,第21页。

〔47〕 参见张晓君:《数据主权规则建设的模式与借鉴——兼论中国数据主权的规则构建》,《现代法学》2020年第6期,第137页。

〔48〕 See Melissa Lukings & Arash Habibi Lashkari, *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective*, Springer, 2022, pp. 5-6.

〔49〕 See Jeffrey Ritter & Anna Mayer, Regulating Data as Property: A New Construct for Moving Forward, 16 *Duke Law & Technology Review* 220, 220-277 (2018).

〔50〕 参见郑佳宁:《数据信息财产法律属性探究》,《东方法学》2021年第5期,第49-50页。

无形物的自然属性与法律属性。以知识产权为例,专利的本体是科学发现、规则和方法;商标的本体是商品和服务来源方面的信息;著作权的本体是文艺或科学思想的表述。这些无形财产的本体都是信息,而信息本身具有可复制性、可传播性和非排他性。然而,由于信息具有经济价值,国家通过立法赋予信息创造者排他性权利,以鼓励创新和保护经济利益。因此,排他性和稀缺性并非知识产权的自然特性,而是法律赋予的特性。〔51〕 同理,尽管数据的自然特性是可复制和可共享,但由于其具有财产利益,国家可以通过立法对数据的收集、处理、使用和转让进行规制,赋予数据类似于其他无形财产的排他性和稀缺性。〔52〕

即使数据不完全符合民法上无形物稀缺性和排他性的法律特征,这些差异也并不妨碍国家比照无形物对数据主张主权。证成数据主权并不需要完全解决数据在民法上的属性问题,而只需要关注主权行使的基础。主权的行使依赖于客体与国家的联系。虽然这个联系主要基于属地原则,但是国际法还认可国家根据其他合理联系对无形客体行使主权。〔53〕 例如,专利、商标、证券等无形财产需要通过国家公权力创设,该国因此获得对其的管辖权,与无形财产的载体(如专利许可证、证券凭证等)的地理位置无关。而商誉等无形财产虽无需国家公权力创设,但国家可以根据相关企业或市场与国家的联系对商誉进行保护。与此类比,国家也可以基于数据与国家的合理联系,如数据在境内产生或涉及该国主体的权利,对数据这一无形物行使主权。

3. 数字主权的义务本源

主权不仅是国家对其领土内一切事务的最高权力,同时也伴随相应的义务。〔54〕 国家有义务运用其主权权力,保护人民基本权利和公共利益。〔55〕 在数字时代,数据作为新型社会资源,其保护和管理已成为国家主权的重要组成部分。特别是个人数据、群体数据以及关键数据,涉及人格权利、公共利益和国家安全,国家对其负有保护义务。

个人数据具有人身权利属性,是个人区别于他人的客观特征,也是人格权和隐私权的重要体现。数据主体对其个人数据享有知情权、更正权、删除权、携带权、查阅权等一系列权利。〔56〕 这些权利不仅是个人隐私保护的核心内容,也是现代法治社会的基本要求。国家有义务通过立法和执法手段,确保本国数据主体的权利得到充分保障。〔57〕 即使数据被外国公司收集、处理或存储于境外,只要数据主体是本国公民,国家对其数据的保护义务就并不因数据的地理变化而消失。

群体数据关系群体所在国的公共安全。随着大数据和信息技术的发展,海量数据中隐藏的人类行为模式可以被精准分析、识别甚至模拟,其中潜藏着公共安全风险。例如,通过对群体数据的分析,外部势力可能对特定群体进行精准操控,影响社会稳定。〔58〕

〔51〕 参见李琛:《论〈民法总则〉知识产权条款中的“专有”》,《知识产权》2017 年第 5 期,第 12-16 页。
〔52〕 参见梅夏英:《数据的法律属性及其民法定位》,《中国社会科学》2016 年第 9 期,第 164-183 页。
〔53〕 参见孙南翔:《法律域外适用体系建设中的管辖权:演化规则与关联结构》,《法学》2024 年第 1 期,第 175-192 页。
〔54〕 参见杜国胜:《有关“国家主权”的法律思考》,《中共山西省委党校学报》2012 年第 6 期,第 62-65 页。
〔55〕 参见蒋银华:《论国家义务概念之确立与发展》,《河北法学》2012 年第 6 期,第 56-66 页。
〔56〕 参见姚佳:《个人信息主体权利的实现困境及其保护救济》,《中国法律评论》2022 年第 6 期,第 132-142 页。
〔57〕 参见郑贤君:《论数据权利保护的宪法规范逻辑》,《人权》2024 年第 6 期,第 76-77 页。
〔58〕 参见隽薪:《数据主权规则博弈的中国进路》,《中国社会科学院大学学报》2024 年第 6 期,第 63-64 页。

此外,涉及国家关键基础设施的运行数据,一旦被滥用或泄露,可能破坏基础设施的正常运作。[59] 类似地,供应链和物流管理数据的泄露可能影响食品安全、药品供应和生产安全。环境监测、公共卫生和气象预报数据的篡改可能危及公共健康,干扰抗疫防灾措施。因此,国家有义务对这些数据进行管理,保护公共利益和国家安全。

从国家义务的角度看,数据主权不仅是国家对数据的控制权,更是其对国民权利和公共利益的保护责任。这种义务伴随数据的流动性和无形性,必然要求主权行使超越传统的属地边界,这是主权在数字时代的合理延伸与扩展。

(二)基于合理联系与保护义务确定主权归属与优先权

基于以上分析,数据主权的理论基础可以归结为国家对无形物的主权以及国家对数据主体和公共利益的保护义务。然而,现有的数据主权实施原则,并未完全体现这一理论内核。虽然效果原则与该理论较为接近,但效果原则的核心在于行为的实质性影响,强调行为对国内利益的实际效果,而数据主权理论更注重数据与国家之间的合理联系。

在此背景下,有必要确立更符合数据特性和国家利益归属的数据主权实施原则:以数据与国家之间的合理联系以及国家承担的保护义务为基础,明确国家间对数据管辖的优先权。数据与国家之间的合理联系主要体现为两个因素。其一是数据生成地。数据的生成通常与产生地的法律、经济、社会和文化环境密切相关。例如,一国境内的主体在境内生成的数据,必然受到该国法律规制,并与该国的国家治理结构和公共利益相连。因此,以数据生成地作为连接点,不仅体现数据主权的属地属性,也能够有效体现数据与产生国之间的制度性联系。这种联系不仅是物理联系,更是法律和经济上的结构性联系,因为数据的生成、存储和处理往往依赖于产生国的法律框架和基础设施。其二是数据关联对象。数据关联对象泛指数据所表征、描绘或反映的实体。数据反映或承载特定自然人、法人或社会组织的信息内容。当数据关联的对象与某一国在身份、住所、注册地、经营地等方面存在紧密联系时,该国对数据的保护义务随之确立。即使数据由外国平台处理、存储或控制,该国的保护责任亦不因物理位置变更而消失。国家承担对其国民的权利保障及社会秩序基本治理的职责,这一义务在数据治理领域同样延伸适用。

需要强调的是,该原则的目的并非在已经存在的多个数据主权实施原则之外再建立一个新的原则,也非取代现有的数据主权实施原则。根据国际法的现状,各国在未违反国际义务的前提下享有设定数据主权规则的裁量空间,且当前的国际法尚未对数据的单边域外管辖明确设定限制。[60] 本文建立的原则是在数据主权冲突发生时判断哪一国对特定数据拥有正当主权主张与优先治理地位的标准。例如,美国公司为中国自然人提供产品或服务而收集中国自然人的个人数据,并将数据存储于爱尔兰境内。美国根据《云法案》主张对数据行使控制,爱尔兰基于数据存储地主张管辖权,而中国可根据《个人信息保护法》主张管辖权。由于数据反映中国境内自然人的信息,中国与数据有合理联系,并

〔59〕 参见张盛杰、何冰等:《乌克兰停电事件对全球能源互联网安全的启示》,《电力信息与通信技术》2016 年第 3 期,第 77-83 页。

〔60〕 参见张晓君:《论数据管辖权的冲突与协调》,《政法论丛》2025 年第 1 期,第 98 页。

对其有保护义务,中国应当具有数据管治的优先权。该原则也为国际数据治理合作提供依据。如爱尔兰是数据存储地,对数据拥有实际的控制权,在此框架下,中国可以基于国际合作机制请求爱尔兰提供数据。由于中国拥有合理联系和保护义务,爱尔兰应当提供协助。即使数据处理者位于美国境内,但是由于中国与数据有合理联系,美国公司在外国处理数据依然应当遵守中国的数据保护规则。换言之,在多国基于国内法对同一份数据主张主权时,合理联系是确定主权优先顺序的标准,其功能相当于国际私法处理法律适用连接点冲突时适用的“最密切联系原则”。〔61〕

数据生成地与数据关联对象这两个标准通常指向同一个国家,但偶尔也可能发生冲突。此时,应当综合考量与数据联系最密切的国家。当数据关系到一国居民的权利,或该国的社会状况和经济运行,数据与该国的联系较数据产生地更为紧密。例如,根据《个人信息保护法》第 3 条,中国用户使用美国平台在美国服务器上产生数据,数据虽然产生于美国,但是数据主要关联对象是中国公民,中国更有理由主张管辖权并履行保护义务。再如,外国游客在中国旅行过程中产生大量不涉及个人隐私,却关系城市管理、社会秩序、公共交通的数据,此类数据与数据产生地具有更加密切的联系,中国作为和数据有合理联系的国家应当具有数据管辖优先权。

根据合理联系和保护义务确定数据主权归属和优先顺序符合中国的数据治理政策。我国《网络安全法》《数据安全法》《个人信息保护法》并未实施全面数据本地化政策,而是对与国家安全、经济发展、公共利益密切相关的数据设定本地存储要求和出境审查机制。例如,对关键信息基础设施运营者在中国境内运营中收集或产生的个人信息和重要数据、国家机关处理的个人信息、批量个人数据等实施本地化措施。〔62〕 这些数据与国家公共利益和数据主体关联程度极高,国家有责任对其加强保护。2024 年《数据跨境规定》进一步体现合理联系结合国家义务原则的治理路径。该规定对一般数据跨境流动采取类型化、场景化的治理方法,特别是对国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的五类不涉及个人隐私和国家安全的数据允许完全自由出境。此类数据的国际性较强,通常不与某一个国家存在“最密切联系”,且不涉及数据主体隐私或国家安全等需要国家履行强保护义务的情形。此外,根据《数据跨境规定》第 4 条的规定,对于在境外产生的个人信息,在未引入境内个人信息或重要数据的前提下,亦可自由出境。此类“过境数据”虽然在中国处理并在中国存储,但是并不涉及中国国家、社会或数据主体的利益。可见,我国当前政策并非强调绝对数据本地化与属地治理,而是依据数据与国家的实际联系进行差异化管理,突出国家保护义务与治理合理性的统一。

从另一个角度看,该原则可以为数据主权的实施划分合理边界,防止一些国家借助技术控制力过度扩张域外管辖权。例如美国《云法案》和欧盟《刑事电子证据条例》均允许本国执法机关根据对本国数据控制者的属人管辖获取域外数据。但是,如果相关数据与

〔61〕 参见邱奕夫:《论对外国行政行为的承认:理论基础与制度构建》,《经贸法律评论》2022 年第 6 期,第 145 页。

〔62〕 《网络安全法》第 37 条;《数据安全法》第 31 条;《个人信息保护法》第 36 条、第 40 条。

请求国不存在合理联系,执法请求应当受到限制。如美国《云法案》第 2713(h)条引入礼让机制,要求法院在审查执法请求时综合考量多个因素,包括数据披露是否违反外国法律、外国是否具有重大主权利益、数据是否涉及外国主体或事务以及数据与美国的关联程度。如果法院认定美国与数据缺乏合理联系,或外国主权利益优先,可以依法拒绝执法机关获得外国数据的请求。类似地,欧盟《刑事电子证据条例》第 17.6 条亦规定,在跨境调取数据时应考量外国利益,特别是包括基本权利和安全利益等核心利益;同时要求法院考虑数据关联对象与第三国之间的属人联系。即使是在强化数据调取能力的制度中,“合理联系”依然应当被适用为划定域外管辖边界的标准。

可见,基于合理联系与保护义务的主权实施原则,不仅提供了判断管辖权归属与优先顺序的法律框架,也为跨国数据治理合作建立了协调基础。相较于以存储位置、数据控制者或数据处理行为为核心的传统管辖原则,该原则更能反映数字时代数据的流动性、共享性和多元属性,也更有助于缓解国家对域外数据主张管辖权时所引发的冲突。

五 结 论

数据主权作为数字时代国家主权的重要组成部分,其理论构建与实践机制在全球数据治理中具有重要意义。本文通过对数据主权实施原则和实施机制的分析,揭示了传统属地原则、效果原则、行为发生地原则及数据控制者原则在应对数据流动性、分布式存储和跨境传输方面的局限性。各国通过数据本地化、出境限制等方式行使数据主权,由此引发的张力和博弈,其根源在于对数据主权的归属和适用边界缺乏明确共识,从而导致治理规则冲突日益频繁。

为回应这些挑战,本文重构了数据主权的理论框架,主张以国家对无形物的主权及保护义务为基础,根据数据与国家之间的“合理联系”来判断主权归属。这一原则为在主权冲突中确定国家的优先治理权提供明确的判断依据,为推动全球数据治理秩序的协调发展与国际合作提供新的理论支撑与制度构想。对于中国而言,这一框架既为特定类型数据的出境安全审查与数据本地化政策提供了法理基础,也有助于在全球数据治理规则重构过程中反驳外国通过数据控制者原则不当扩张数据管辖权。通过建立以合理联系与国家责任为核心的主权实施机制,中国可更有力地主张全球数据治理话语权,并在多边框架下推动达成更有弹性和包容性的规则共识。

尽管构建数据主权理论共识在全球治理体系高度碎片化的时代面临现实障碍,但这并不意味着理论努力毫无意义。恰恰相反,提出一个具有包容性和协调潜力的理论框架,有助于为未来多边谈判、机制对接和规则互认提供基础与共识方向。本文尝试搭建起识别数据归属、厘清主权边界、减少制度冲突的理论,力求在国家间利益张力与制度协调之间找到可能的平衡点。

[本文为作者主持的 2022 年度教育部人文社会科学重点研究基地重大项目“数据跨境流动治理的重大国际法律问题研究”(22JJD820009)的研究成果。]

Contestation and Theoretical Reconstruction of Data Sovereignty

[**Abstract**] With the development of digital technology, data sovereignty has become a focal point in international data governance. Data sovereignty refers to a state's legislative, enforcement, and adjudicative authority over data, showing an extension of state sovereignty in the digital realm, and providing a theoretical foundation for effective global data governance. However, the theory of data sovereignty remains underdeveloped, leading to numerous disputes and conflicts in its practical application. This paper seeks to propose a new theoretical framework for data sovereignty, aiming to offer insights into and potential solutions to the problems in global data governance cooperation. It first analyzes four implementation principles of data sovereignty: the data location principle, the effects principle, the place-of-act principle, and the data controller principle, emphasizing territoriality, influence, behavioral control, and the jurisdiction of the controller, respectively. However, all these principles face challenges posed by the intangible, fluid, and distributed nature of data, resulting in jurisdictional conflicts and legal overlaps among states. Furthermore, conflicts frequently arise among nations when applying the two major mechanisms for data sovereignty implementation: data localization and cross-border data governance. These conflicts do not stem solely from differences in technical approaches or regulatory methods but are rooted in the lack of international consensus on the principle of data sovereignty attribution and the boundaries of its application. The traditional theory of sovereignty is insufficiently adaptable when dealing with the non-materiality and fluidity of data. Due to the lack of a solid theoretical foundation for data sovereignty, frequent conflicts arise in cross-border data governance. Therefore, it is urgent to systematically restructure the basic categories, attribution logic and exercise boundaries of data sovereignty at the theoretical level, and establish an explanatory framework that conforms to the characteristics of the digital age. Based on the state's sovereignty over intangible assets and its obligation to protect data subjects and public interests, the principle for implementing data sovereignty should be determined, which centered on reasonable connection and state duty of protection to determine the attribution of sovereignty and the priority of governance over specific data. This principle can not only counter the undue expansion of extraterritorial jurisdiction, but also establish clear boundaries of responsibility for international cooperation and cross-border data flows, thus providing theoretical support for the construction of a global governance framework that balances sovereignty protection with the free flow of data.

（责任编辑：贾　元）