数据主权规则博弈的中国进路*

隽　薪

【摘　　要】通过对数据主权理论的梳理发现，网络乌托邦主义下的数据主权虚无论是美国为追求数据霸权而推行数据自由流动的重要理论支撑；其他国家强调将传统主权理论向网络空间延伸则是对美国威胁的直接防御。当前，国家之间的数据主权规则博弈主要围绕对数据控制权与管辖权竞争的“进攻”与“防守”展开。此局面正随着数据主权地缘政治竞争的日趋激烈而呈现交错形态，增加了未来数据治理格局演变的不确定性。中国应坚守传统主权，同时拓宽数据主权的合作维度，深化其安全意蕴；从被动防御向注重效率倾斜，推动数据有序自由流动；增强与其他国家的政治互信，搭建数据流动“朋友圈”；统筹推进域内数据法治和涉外数据法治，通过内外联动引领全球数据治理规则的发展。

【关 键 词】数据主权　网络空间主权　数据跨境流动　长臂管辖

【作者简介】隽薪，法学博士，广州大学法学院讲师。

【中图分类号】D99　　【文献标识码】A

【文章编号】2097－1125（2024）06－0058－21

数据是数字经济时代的核心生产要素，是人工智能、物联网、区块链、云计算等数字化技术发展的基础。随着数据的指数级增长、网络安全形势的挑战加剧、全球政治经济动荡，确定数据的存储位置、数据由谁控制、数据如何流动以及数据管辖原则对国家而言变得更加重要，数据主权在此背景下已经演变为激烈的国际竞争中的一个关键问题。

20 世纪 90 年代中期以来，美国为商业利益开始积极推动数据跨境自由流动，并依托网络乌托邦主义的主权虚无论迷惑各国放弃对网络空间的

* 本文系广州大学“数字经济与智慧管理学科与科研创新平台”的阶段性成果。

监管，以成就其数据霸权。而欧盟等国际组织和其他国家在“棱镜门”事件之后开始推动传统国家主权向网络空间延伸，以抵挡因美国的信息监控与数据霸权支配而引发的不安。近年来，随着世界各国越来越重视数据促进经济增长的引擎作用，主要国家之间围绕着数据控制权与管辖权竞争的“进攻”与“防守”持续上演，数据主权的地缘政治格局正在经历深刻调整。美国一贯主张数据跨境自由流动，在数据规则层面呈现一种扩张与进攻的模式，但也以政治防御的态度严格限制数据向中国、俄罗斯等国家流动；而巴西以及欧盟等新兴国家和国际组织除了在个人数据隐私、国家安全等方面做好防守、通过立法限制数据跨境流动，为制衡美国并分享数字经济红利，也开始积极寻求数据管辖权的对外扩张。随着数字经济与技术的不断发展，国家之间的数据主权规则博弈也会更加激烈，这增加了未来全球数据治理格局演变的不确定性。深入梳理数据主权的理论渊源，剖析数据主权规则博弈背后的深意，揭示国家之间围绕数据控制和管辖的地缘政治角力，对完善我国数据主权规则体系与推动构建全球数据治理体系均具有重要意义。

一、数据主权的理论分野：主权虚无论与传统主权论

数据的经济和战略意义在大数据、云计算出现后才更加鲜明地进入公众视野。在此之前，人们更加关注网络这一数据传输渠道应当如何治理的问题，并提出了网络空间自治、多利益共同体共治、国家网络空间主权等多种治理理论。鉴于互联网生成的数据可以被视作网络空间的客体，因而以上网络空间治理理论与数据主权理论的发展息息相关。只有追本溯源，沿着发展脉络对数据主权的理论渊源进行梳理，才能明晰当今国家间围绕数据主权展开争论的根源所在，理解各国制定数据主权规则背后的深意，从而认清国家数据主权规则博弈的实质是国家之间的地缘政治角力。

（一）网络乌托邦主义下的数据主权虚无论

网络乌托邦主义（cyber-utopianism），又被称为网络自由主义，其核心观点为网络空间是一种无国家地理边界、不受政府管制、无权威干涉的自由空间。[①] 网络乌托邦主义最初由互联网先锋人士倡导，随后成为美国政府“互联网自由”议程以及技术全球化的理论支撑。在此理念之下，网络空间实行自治，国家在这里无主权，因而也就不存在国家的数据主权，数据本身

① 参见 Jack Goldsmith and Tim Wu, *Who Controls the Internet ? Illusions of a Borderless World*, Oxford: Oxford University Press, 2006, pp. 13 – 22。

及其流动不受政府管制。可以说，数据主权虚无论寓于网络乌托邦主义之中，成为后者的一项必然推论。对美国政府而言，其重点在于确保数据在全球范围内的自由流动。

1. 政治乌托邦：互联网先锋人士的网络主权主张

自网络技术及服务诞生以来，主权概念在其上发挥的作用一直较为有限。① 早在 20 世纪 90 年代，随着互联网以一种无国界的方式把全世界深度地捆绑在一起，一些互联网先锋人士提出与传统国家主权概念截然相反的网络主权观念，声称网络空间有它自己的主权领域。在此观念中，互联网独立于任何主权国家，不受任何政府的强制，决策权掌握在服务提供者和用户手中。1996 年，互联网先驱约翰·佩里·巴洛（John Perry Barlow）在《网络空间独立宣言》中阐释了网络主权："你们没有任何道义上的权力来统治网络空间，你们也没有任何使我们惧怕的方法来执行……网络空间不存在于你们的领域之内。"②

巴洛为人们描绘了互联网作为"理想国"的美好政治愿景，他援引杰斐逊起草的美国《独立宣言》，疾呼网络空间的独立与自由，宣称这里没有边界、没有政府、没有特权或偏见，任何人在网络空间的任何地方都可以自由地表达自己，通过在网络中创造思想文明，将建立一个比由国家政府统治的世界更公平、更人道的世界。巴洛的追随者相信通过技术能够实现政治变革，从而实现网络空间自治。

2. 经济乌托邦：美国的互联网自由议程

如果说巴洛的网络主权是一种政治乌托邦，那么美国政府随后推行的"互联网自由"议程的内核则是遵循商业和市场逻辑的一种经济乌托邦。从 1991 年万维网的发布，到 1995 年微软公司发布 Internet Explorer 1.0 浏览器，互联网开始大范围地商业化。为适应这种发展，1997 年克林顿政府开始对外推行"互联网自由"议程，该议程以商业不监管原则和反审查原则为基础，公开反对将主权概念延伸至互联网领域。③

商业不监管原则是 1997 年《全球电子商务框架》的要旨。这份由美国政府为全球绘制的所谓"互联网治理蓝图"指出："互联网提供了一种全新的市场经济的可能性，一种真正开放和民主的市场经济，各国政府必须对电

① 参见郑琳、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，第 55 页。

② 参见 John Perry Barlow, A Declaration of the Independence of Cyberspace, https://www.eff.org/cyberspace-independence, 2023 年 10 月 2 日。

③ 参见 Jack Goldsmith, The Failure of Internet Freedom, https://s3.amazonaws.com/kfai-documents/documents/0f969b7a13/The-Failure-of-Internet-Freedom.pdf, 2023 年 10 月 2 日。

子商务采取一种不受监管、面向市场的方法，各国政府应避免对电子商务施加不当限制，即使需要治理，也应该由私营、非营利、利益攸关方等机构进行治理，而不是与国家或地理联系在一起。”① 商业不监管原则帮助苹果、谷歌、脸书和亚马逊等公司赢得了巨大的全球市场份额，互联网也成为美国越来越有价值的“摇钱树”。反审查原则的目标在于确保互联网言论自由和互联网信息的自由流动，最初是为了促进电子商务的发展，后来演变为一项试图影响外国政治结构的策略。由于获取信息意味着创新与巨大的商业利益，美国政府为此极力推广互联网言论自由。

3. 技术乌托邦：美国的互联网霸权

在网络乌托邦主义者眼中，网络空间是纯粹技术性的自主空间，其治理方式应是技术代码和自治伦理，因此，网络乌托邦主义也被视为技术乌托邦主义的一个子类。技术乌托邦主义者通常信奉技术决定论，认为技术是社会发展的主导力量，并奉自由市场经济为圭臬，对政府监管怀有敌意。结合彼时全球化的时代背景来看，互联网发展即全球化的技术层面表现，而“超级全球化主义”也的确是技术决定论者认同的理论，他们声称，由于技术的广泛应用，加速全球化是不可避免的。② 技术决定论的内核与经济全球化之下美国推行的新自由主义政策惊人地不谋而合，这一时期一种被称为“加州意识形态”的技术乌托邦理念概括了二者的关联。③ 同一时期美国政府推行的“互联网自由”议程，倡导互联网无政府主义和信息自由流动，可以说正是新自由主义政策的网络空间版。进一步而言，正如新自由主义是实现美国政治、经济、文化霸权的理论工具，美国在网络空间推行“互联网自由”议程也是为了构建其互联网霸权，而其他国家在网络空间主张主权无疑将成为美国追求霸权的阻碍。

美国构建互联网霸权的重要支撑来自其对互联网基础设施、技术规则制定权与大型科技公司的控制。对全球互联网接入至关重要的 13 个根服务器中有 10 个位于美国境内。互联网名称和代码分配机构（ICANN）、互联

① William J. Clinton and Albert Gore, Jr., A Framework for Global Electronic Commerce, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html, 2023 年 10 月 2 日。

② 参见 Jan Nederveen Pieterse, Globalization, Kitsch and Conflict: Technologies of Work, War and Politics, *Review of International Political Economy*, Vol. 9 (1), 2002, p. 3。

③ “加州意识形态”是美国 20 世纪 60 年代开始的反文化运动、技术乌托邦主义以及对新自由主义的政策支持相结合而产生的一种理念。该理念的提出者指出，20 世纪 90 年代硅谷互联网技术的兴起与美国新自由主义之间关系密切，并催生了政治上左翼和右翼对技术决定论的一种融合与矛盾相互交织的所谓“信仰”。参见 Richard Barbrook and Andy Cameron, The Californian Ideology, *Science as Culture*, Vol. 6 (1), 1996, pp. 46 - 51。

网工程任务组（IETF）等制定互联网治理规则和标准的非政府组织位于美国且与美国有着千丝万缕的历史联系。有学者直言，互联网治理的规则实际上就是一种隐晦的“美国规则”。[①] 大型互联网科技公司也主要是美国公司。事实上，美国政府早已持有网络空间主权的观念。相对早期网络乌托邦主义者的理想而言，美国政府对互联网的控制代表主权国家的显性回归。[②]

综上，美国在网络乌托邦主义包装下的数据主权虚无论在本质上是为构建美国的数据霸权服务的。美国以其自身对互联网的绝对控制为前提，通过一种乌托邦理想将网络空间特定化为无国家主权的自治空间，旨在迷惑其他国家放弃对其中数据的主权管辖与控制，实现数据在全球范围内的自由流动，从而为美国大型互联网公司的全球化经营奠定基础。反过来，美国又凭借其大型互联网公司在全球收割数据，最终实现全球数据流向美国，使美国成为全球数据中心，以成就其数据霸权。

（二）传统国家主权理论下的数据主权论

与网络乌托邦主义针锋相对的一种观念是主张将传统国家主权延伸至网络空间的网络空间主权论。网络空间主权指的是一国对本国境内的网络设施、网络主体、网络行为及相关网络数据和信息等享有的对内最高权和对外独立权。[③] 而数据主权通常被认为是网络空间主权的下位概念，即国家对网络空间产生的数据享有的主权，[④] 具体包括国家对数据享有取得、占有和管辖的权利。然而，作为信息的载体，数据的发送和接收还可以通过电报、遥感技术、卫星传播等途径实现，也就是说，数据主权的范围不只局限于网络空间。[⑤] 因此，广义的数据主权与网络空间主权实际上是一种交叉重叠的关系。尽管如此，本文主要还是从网络空间出发探讨数据主权，因为在大数据时代，网络空间无疑是当前数据主权行使的最重要场域，也是国家之间数据主权博弈的主战场。

1. 网络空间主权的回归

网络空间主权论来自非西方国家对互联网规则是由西方国家制定的这一

① 参见 Andrew Keane Woods, Litigating Data Sovereignty, *The Yale Law Journal*, Vol. 128 (2), 2018, p. 367。

② 参见刘晗：《域名系统、网络主权与互联网治理：历史反思及其当代启示》，《中外法学》2016 年第 2 期，第 532 页。

③ “网络空间主权”通常又被称为“网络主权”，本文在行文中使用“网络空间主权”一词以同前述巴洛提出的“网络主权”相区分。

④ 参见曹磊：《网络空间的数据权研究》，《国际观察》2013 年第 1 期，第 56 页。

⑤ 参见孙南翔：《网络空间经贸规则法治机制研究》，中国社会科学出版社 2022 年版，第 29 页。

事实的一种天然的反感与不安。主权主义者将乌托邦主义者的理想视为一场闹剧，在他们看来，这是伪装成全球主义的美帝国主义；而乌托邦主义者指责主权主义者试图分裂互联网，他们经常把争论定义为互联网是应该“开放”还是“巴尔干化”。① 20 世纪 90 年代后期，在互联网商业化之后，随着传统社会各类主体进入网络空间，在利益纷争与文化碰撞之下，乌托邦主义者在现实中已经无力维持网络空间自治。2003 年，联合国信息社会世界峰会（WSIS）首次提出“网络空间主权”，随后 WSIS 开始倡导包括政府、私人部门和网络市民社会的多利益共同体网络治理模式。由于对互联网的事实控制权仍然在美国手中，自 2005 年以来，欧盟以及诸多发展中国家试图加强对网络空间的控制，维护其在网络空间的安全和发展权利，并先后多次提出将互联网治理权交给联合国下属的政府间国际组织，从而将 ICANN 纳入联合国体系下进行管理与运作，但均被美国拒绝。② 各国政府在这一时期开始具有明确的网络空间主权观念，并积极倡导联合国管理下的互联网多边共治，只是在美国的阻挠下困难重重。

2. 数据主权意识的觉醒

在美国操控下用于迷惑世人的所谓“自由、开放、安全的互联网”形象随着“棱镜门”事件的发生轰然坍塌。2013 年，美国中央情报局（CIA）前技术分析员爱德华·斯诺登（Edward Snowden）揭露了美国国家安全局（NSA）对各国政府实施的大规模监控，此即“棱镜门”事件。该事件改变了互联网自由、安全和治理方面的地缘政治格局，开放互联网世界的愿景被打破，并重新引发围绕未来互联网治理模式的辩论。今天人们普遍认为数据主权作为一个法律概念在全球范围内的提出可以追溯到该事件。此后，欧盟和其他国家纷纷加快数据立法，推动数据本地化，对数据跨境流动予以限制，捍卫数据主权。因此，有学者称“棱镜门”事件为“数据民族主义”的开端。③

对美国大型互联网平台的戒备是各国主张数据主权的另一项理由。谷歌、亚马逊和脸书等互联网公司在全球范围内都具有巨大的影响力。然而，数据泄露与数据操控频发，仇恨言论和虚假信息横流，“乌托邦”已然成为“沼泽地”。大型互联网平台的商业模式建立在收集、整合个人数据基础之

① 参见 Andrew Keane Woods, Litigating Data Sovereignty, *The Yale Law Journal*, Vol. 128 (2), 2018, p. 368。

② 参见刘晗：《域名系统、网络主权与互联网治理：历史反思及其当代启示》，《中外法学》2016 年第 2 期，第 531 ~ 532 页。

③ 参见 Anupam Chander and Uyên P. Lê, Data Nationalism, *Emory Law Journal*, Vol. 64 (3), 2015, p. 691。

上，相当于私人公司在全球范围内对亿万民众实施无差别监控，所有的现实和人类生活都成为一种商品，平台公司则从中提取数据、制作用户画像，最后通过出售给广告商等第三方来实现货币化。学者形象地称这种商业模式为“监控资本主义”（surveillance capitalism）。① 这些大型互联网平台的用户遍布全球，平台有能力影响世界各地的思想与行为，通过对海量数据的收集和分析来利用和控制人心，并左右国家政治。各国担忧大型互联网平台和外国势力操纵数据，并认为维护数据安全迫在眉睫。国家的数据主权意识全面觉醒。

3. 对数据主权内涵的理解

依据传统理论，国家主权强调对内最高和对外独立，即国家对本国领土和管辖范围内的人、事、物具有最高的、排他的权力。然而，在现实世界中清晰的主权概念，在网络环境中却是模糊的，这是因为数据是无形的、可分割的、可移动的和相互关联的，其转瞬即逝的特征与领土的空间固定性形成了鲜明对比。② 有学者认为数据的这些特点令国家难以在地理空间范围内对其加以控制，因此数据正在破坏领土原则的稳定性。③ 有学者指出主权是个富有弹性的概念，并不一定与领土联系在一起。④ 无论如何，在现实当中每个国家都声称在网络空间拥有主权和领土，数据的流动和存储也正受到国界的限制。⑤

事实上，数据作为网络空间的客体，虽然是无形物，却仍具有一定的物理属性。⑥ 数据存储在服务器和数据中心，这些服务器与数据中心存在于国家领土内，构成了国家行使数据主权的物理基础。因此，数据主权可以概括为国家对数据的最高的控制权和排他的管辖权。许多学者也表达了类似的观

① Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: PublicAffairs, 2019, pp. 7 – 11。

② 参见 Nico Krisch, Jurisdiction Unbound: (Extra) territorial Regulation as Global Governance, *European Journal of International Law*, Vol. 33 (2), 2022, p. 494。

③ 参见 Jennifer Daskal, The Un-Territoriality of Data, *The Yale Law Journal*, Vol. 125 (2), 2015, pp. 369 – 378。

④ 参见 Cristos Velasco, Julia Hörnle and Anna-Maria Osula, Global Views on Internet Jurisdiction and Trans-Border Access, in Serge Gutwirth, Ronald Leenes and Paul De Hert, eds., *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Dordrecht: Springer Netherlands, 2016, pp. 465 – 476。

⑤ 参见 Takahisa Kawaguchi, Emergence of “State-Centrism” in Cyberspace, *Japan Review*, Vol. 3 (3 – 4), 2020, p. 46。

⑥ 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。

点——“数据主权涉及通过国家管辖权对数据流的控制”，[①]“数据主权涉及对数据和云加以控制的范围和限度，国家间围绕二者争相提出主权权利主张，并通过具有域外效力的方式来监管互联网”。[②] 当前，国家数据战略的核心也聚焦于对数据的控制与管辖。各国在“棱镜门”事件后产生了关闭“网络领土”的反射性要求。[③] 决策者们旨在借助数据主权从外国科技公司和贸易伙伴手中夺回对数据的控制权和管辖权。[④] 国家之间围绕数据管辖权和控制权展开的数据主权规则博弈，目前主要涉及数据的存储位置、数据由谁控制、数据如何流动以及数据管辖原则等核心问题。

二、以自由为核心：美国维护数据霸权与主权的多重规则路径

为了巩固数据霸权，美国在数据控制权与数据管辖权上均呈现对外扩张的总体趋势。在数据控制权上，美国主张数据的跨境自由流动，并凭借其互联网巨头企业的垄断优势尽可能地掌握和控制全球数据，力图成为全球数据中心。当然，美国只是在数据流向美国时对数据自由流动持欢迎态度，一旦在数据要离开美国或者脱离美国控制时，美国就经常以国家安全为由实行强监管或者严禁数据流向特定国家，这种控制数据“宽进严出”的做法表明美国的数据主权意识一直都存在。在数据管辖权上，随着越来越多的国家主张数据主权，美国开始有意识地对抗境外的数据本地化浪潮，并通过立法强化其获得域外数据资源的能力，同其他国家开展全球数据主权竞争。

（一）数据跨境自由流动规则：APEC 框架下的 CBPR 体系

美国长久以来以所谓“自由、开放、可信”的跨境数据流动观自居，致力于树立反数据本地化、维护自由贸易的形象，实则看重数据自由流动带来的经济利益。美国一边从国家战略层面推动数据自由流动，一边利用经济

① Patrik Hummel, Matthias Braun and Max Tretter et al., Data Sovereignty: A Review, *Big Data & Society*, Vol. 8 (1), 2021, p. 1.

② Andrew Keane Woods, Litigating Data Sovereignty, *The Yale Law Journal*, Vol. 128 (2), 2018, pp. 333 – 335。

③ 参见 Georg Glasze, Amaël Cattaruzza and Frédérick Douzet et al., Contested Spatialities of Digital Sovereignty, *Geopolitics*, Vol. 28 (2), 2023, p. 922。

④ 参见 Nigel Cory and Luke Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, *Information Technology & Innovation Foundation*, July 19, 2021, https://www2.itif.org/2021 – data – localization.pdf, 2023 年 10 月 2 日。

合作与发展组织（OECD）、亚太经济合作组织（APEC）、二十国集团（G20）等平台主导跨境数据流动规则的话语权，向全球推广数据自由流动规则。美国在 1980 年 OECD《保护个人信息跨国传送及隐私权指导纲领》与 2004 年《APEC 隐私框架》的制定中均发挥了主导作用，二者在跨境数据流动规则上一脉相承，但后者对消费者权利的保护进一步弱化，更加重视贸易利益。2011 年，APEC 领导人又批准了跨境隐私规则体系（以下简称 CBPR 体系），CBPR 体系是一种自我监管型体系，实质是通过提供较低保护水平的跨境数据流动机制，削弱加入其中的国家和地区自主管控跨境数据的权力，实现美式跨境数据自由流动规则的扩张。①

美国力推 CBPR 体系建设，不断将其盟友纳入该体系，如将 CBPR 体系纳入《美墨加三国协议》（USMCA）的“数字贸易”一章。2020 年 8 月，美国首次提出将 CBPR 体系独立于 APEC 框架外，便于非 APEC 成员加入，以进一步扩展数据跨境自由流动圈。2022 年 4 月，在美国倡导下，美国、加拿大、日本、韩国、菲律宾、新加坡等联合发布《全球跨境隐私规则宣言》（Global Cross-Border Privacy Rules Declaration），宣告成立全球跨境隐私规则论坛（以下简称 GCBPR 论坛），致力于促进数据自由流通与有效的隐私保护。2022 年 8 月，澳大利亚宣布加入。2023 年 4 月，英国也提交了加入该体系的申请。该宣言在本质上是将 APEC 框架下的 CBPR 体系从一种区域性框架转换为全球性框架，将更多国家纳入数据跨境自由流动圈。GCBPR 论坛不仅是美国“印度—太平洋”战略的一个重要组成部分，也是美国企图阻止欧盟《通用数据保护条例》（GDPR）成为全球个人数据保护标准而提供的一项替代办法。

（二）《云法案》下对域外数据的长臂管辖

欧盟以及其他国家近年来的一系列数据主权立法与战略行动对美国数据霸权地位构成了直接威胁，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。《云法案》就是美国维护其数据霸权的重要组成部分。

2018 年出台的《云法案》，全称为《澄清境外数据的合法使用法案》（Clarifying Lawful Overseas Use of Data），其出台背景要追溯到“微软公司诉美国案”。2013 年，美国纽约南区地方法院向微软公司签发调取数据的令状，但这些数据存储在爱尔兰的一个数据中心，微软公司辩称美国法院无权针对存储在国外的数据签发令状。虽然美国纽约南区地方法院认为，无论数据存储在何处，对数据的实质性控制足以使微软公司遵守该项命令，但美国第

① 参见李艳：《大国博弈下的跨境数据流动国际规则构建》，《当代世界》2023 年第 5 期，第 27 页。

二巡回上诉法院认为国会没有授权《储存通信记录法》（Stored Communication Act，以下简称 SCA）可以域外适用。美国政府就第二巡回上诉法院的裁决向联邦最高法院提出上诉。在联邦最高法院做出裁决之前，美国国会通过《云法案》，对 SCA 做出修订，明确规定电子通信服务提供商和远程计算服务提供商必须遵守美国政府对数据的法律要求，“无论此类通信、记录或其他信息是位于美国境内还是境外，电子通信服务提供商和远程计算服务提供商有义务保存、备份或披露有线或电子通信的内容以及该提供商拥有、保管或控制的与客户或用户有关的任何记录或其他信息”。①

根据传统主权原则，数据的管辖无疑是以其存储地管辖为主的。这意味着，只要数据位于该国的领土内，该国就可以合法地主张对该数据的管辖权。《云法案》改变了 SCA 中的数据存储地标准，确立了数据控制者标准，令美国能够通过美国公司来调取域外数据。只要数据在美国公司的控制之下，就默认美国政府能够直接从全球各地调取，仅存在少数例外，而且例外均由美国法院单独裁量决定。借此，美国政府的数据攫取之手可以更方便地延伸至境外，做到了“国内国外一盘棋考虑”。② 根据国际公法，跨境数据获取可以通过司法互助条约保证数据来源国的数据主权，同时，一国不能到另一国领土上行使执法管辖权也已经是公认的国际习惯法规则。而根据《云法案》的规定，美国可以绕开数据主权国，并通过对属人管辖做扩大解释，依据控制者标准通过美国公司行使域外执法管辖权，将全球数据视为其囊中之物，严重践踏了数据来源国的数据主权。③

《云法案》单方面确认美国政府调取美国公司在境外存储的数据的合法性，彰显了美国寻求世界网络控制权的意图，它试图界定数据主权边界，但未尊重他国合作治理网络空间的“共治权利”。④ 尽管《云法案》规定了数据控制者对境外数据的强制披露义务仅在涉嫌危害美国国家安全的犯罪、严重的刑事犯罪等重大案件时才可适用，然而鉴于当前全球范围内日益加剧的地缘政治斗争形势，美国泛化与滥用“国家安全”获取域外数据以达到其政治目的的可能性非常大。因此，这种限定难以消除欧盟与其他主权国家的数据主权危机感。

---

① Clarifying Lawful Overseas Use of Data Act, Section 103. Preservation of Records; Comity Analysis of Leagal Process § 2713.

② 参见洪延青：《美国快速通过 CLOUD 法案 明确数据主权战略》，《中国信息安全》2018 年第 4 期，第 35 页。

③ 参见杨永红：《美国域外数据管辖权研究》，《法商研究》2022 年第 2 期，第 150 页。

④ 参见夏燕、沈天月：《美国 CLOUD 法案的实践及其启示》，《中国社会科学院研究生院学报》2019 年第 5 期，第 106 页。

（三）对数据出境的多重限制

美国在获取别国数据时倡导自由开放政策，对本国数据向外流动则施加各种限制，这种“宽进严出”的做法也说明美国并非否认或不关注数据主权。美国对待 TikTok 的做法就是最好的例证。为防止数据外流，美国威胁要禁用或将 TikTok 国有化，有学者指出这是美国采取本地化措施维护数据主权的一个分水岭事件。①

美国目前正采取多种方式控制境内数据外流。第一，严格限制外国公司访问美国数据，除非它们与美国政府达成协议，即所谓行政数据共享协议。这项协议是非互惠的，它以美国政府为主导，外国科技公司需要做出妥协以换取在美国市场上市。第二，利用出口管制手段限制高科技、军民两用技术数据出境。美国近年来以“国家安全”为由对 TikTok 等中国投资企业发起调查，防止它们收集和存储的美国用户数据被中国政府获取。第三，《云法案》除了规定美国政府可以从境外调取数据，还规定满足条件的外国政府能够调取存储在美国的数据，但其规定的条件远远严苛及繁复于美国政府调取域外数据要满足的条件，任何其他国家都很难满足，这种美国自由裁量下对数据“宽入严出”的做法，是单边主义和以美国为中心的表现。② 美国采取的这一系列措施清楚地表明，美国意识到保护美国境内产生的数据并对外国科技公司实施限制的必要性，体现了美国政府对数据主权的维护。③

此外，值得关注的是，美国近年来还陆续提出多项法案，旨在限制个人数据向外流动，其中均具有相似的政治化条款。目前这些法案尚未生效。例如，2019 年美国《国家安全和个人数据保护法案》（NSPDPA）对美国用户数据出境予以明确限制，旨在规制所有基于数据提供在线服务的公司（包括“受管辖公司”），不得将任何用户数据或解密该数据所需的信息传输到中国、俄罗斯等任何在其眼中“有疑虑的国家”，而其定义的“受管辖公司”非常广泛，大部分互联网企业都可归入其监管范围。2021 年美国《敏感个人数据保护法案》明确要求数据处理企业应向消费者说明“数据是否提供给中国、俄罗斯、伊朗或朝鲜”。2022 年美国《数据隐私和保护法案》也做出了同样的规定。2024 年 2 月 28 日，由美国总统拜登签发的《关于防止受

① 参见 Nwachukwu T. Obi II, The Balkanisation of the Internet: Data Nationalism in the European Union and Its Effects on the Development of Technology, https://arno.uvt.nl/show.cgi?fid=157767, 2023 年 10 月 2 日。

② 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 144～145 页。

③ 参见 Chunmeizi Su and Wenjia Tang, Data Sovereignty and Platform Neutrality: A Comparative Study on TikTok's Data Policy, *Global Media and China*, Vol. 8 (1), 2023, p. 61。

关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》从规制“商业交易”出发，授权美国司法部颁布条例，限制向包含中国在内的6个所谓“受关注国家”传输美国人敏感个人信息及美国政府相关数据。美国宣称此举旨在填补所谓“国家安全”漏洞，相关规则将进一步强化美国对数据出境的监管力度。

三、以安全为要旨：其他国家维护数据主权的多重规则回应

美国政府对其他国家进行信息监听与干涉令各国政府倍感担忧，各国对数据主权的需求越来越迫切。数据主权使各国能够控制在其境内创建和存储的数据，许多国家并不担心追求数据主权导致互联网的“巴尔干化”，它们更担心美国利用其大型科技企业收割全球数据，从而威胁其他各国公民隐私与国家安全。为应对美国威胁，以欧盟、俄罗斯为代表的国际组织和主权国家多以一种防御的姿态，在其数据战略中强调实施本地化存储和扩展域外管辖权，力图通过限制数据自由流动、强制数据本地化存储、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竞争中的优势。①

（一）欧盟对数据跨境自由流动的限制

1. 欧盟的《通用数据保护条例》

欧盟通过保护个人数据权利的方式来限制数据的跨境流动。欧盟于1995年出台的《个人数据保护指令》（以下简称95《指令》）确立数据充分保护原则，明确禁止向保护水平低于欧盟的国家转移个人数据。2016年4月，欧盟议会通过《通用数据保护条例》（GDPR），该条例于2018年5月正式生效并取代95《指令》。GDPR比95《指令》更进一步强化数据主体权利的进路，对数据跨境流动的要求做出更加细致的规定。GDPR规定向非欧盟国家传输个人数据必须符合第五章规定的特定传输条件：第一，传输目的地获得欧盟委员会的充分性认定；第二，该数据传输行为得到适当的保障。当传输目的地已通过欧盟委员会的充分性认定，欧盟国家向其传输数据无须获取额外授权，只需遵守GDPR对数据传输的普通规定即可。如果传输目的地没有通过充分性认定，但能够提供适当的措施来保护数据主体的权利和自由，并且数据主体可以申请法律救济，那么向其传输数据也是被允许的。由

① 参见黄海瑛、何梦婷：《基于CLOUD法案的美国数据主权战略解读》，《信息资源管理学报》2019年第2期，第38页。

于满足充分性认定条件的国家较少，为遵守 GDPR，企业和有关组织必须实施和维护“合理的安全”程序和保护措施，以保护欧盟公民的数据安全。目前，企业传输数据较为常见的保障措施包括约束性企业规则（BCR）和标准合同条款（SCC）。

GDPR 实现了欧盟在数据规则领域的“布鲁塞尔效应”。[①] 跨国公司都倾向于采用 GDPR，许多国家的数据立法也以 GDPR 为蓝本，GDPR 已经成为数据跨境流动领域的全球基准。GDPR 的出台以及随之而来的巨额罚款，令各国企业和有关组织开始更加认真地审视欧盟的数据主权要求和能力。有学者指出，除了保护公民的隐私权，欧盟想将 GDPR 打造成一个“最严监管范本”以增加其在对美贸易谈判中的筹码。[②] 因此，GDPR 实则是欧盟应对美国数据主权竞争的利器。欧盟的这种做法化被动为主动，不但保护了个人数据安全，而且树立了一套与美国抗衡的话语标准。[③]

2. 欧美之间的数据跨境流动机制

在 95《指令》框架下，欧盟认为美国并没有为欧盟个人数据隐私提供足够的保护，因而禁止个人数据传输到美国。为解决数据的跨境传输问题，欧美之间于 2000 年达成了《安全港协议》（Safe Harbor）。2015 年欧洲法院在 Schrems I 案裁决中以《安全港协议》违反《欧盟基本权利宪章》为由宣布该协议无效。2016 年双方又达成了《隐私盾协议》（Privacy Shield）。相比《安全港协议》，《隐私盾协议》在数据传输的透明度和规则遵守的监督方面有更高的要求。但 2020 年欧洲法院又在 Schrems Ⅱ 案裁决中宣布《隐私盾协议》正式作废，因为法院认为美国法律无法确保转移到美国的个人数据将获得与欧盟同等程度的保护。

数据影响着 7.1 万亿美元的跨大西洋贸易与创新，美欧双方都希望尽早找到继续推进数据传输的解决方法。2022 年 3 月，欧盟与美国共同宣布推出新的数据跨境流动协议——《跨大西洋数据隐私框架》（以下简称《隐私框架》），着重解决欧洲法院在 Schrems 系列诉讼裁决中提出的对欧美之间数据传输机制的担忧问题。同年 10 月，美国总统拜登签署了一项关于“加强对美国信号情报活动的保障”的行政令，以采取步骤履行《隐私框架》下的承诺。2023 年 7 月，欧盟委员会宣布《欧盟 - 美国数据隐私框架》已通

① “布鲁塞尔效应”（Brussels effect）一词最早由哥伦比亚大学法学院芬兰裔教授阿努·H. 布拉德福德（Anu H. Bradford）于 2012 年提出，主要指欧盟凭借市场力量对全球市场进行单边监管的能力。通俗而言，该词用以描述欧盟监管政策的全球影响。

② 参见赵璐：《GDPR 或成美欧谈判重要筹码》，https://www.sohu.com/a/313603056_632979，2023 年 12 月 2 日。

③ 参见叶开儒：《数据跨境流动规制中的“长臂管辖”——对欧盟 GDPR 的原旨主义考察》，《法学评论》2020 年第 1 期，第 115 页。

过充分性认证，欧盟委员会认为根据这套美欧跨境数据传输机制 3.0 版，美国能够确保对从欧盟向美国公司转移的个人数据提供与欧盟程度相当的充分保护，个人数据可以安全地从欧盟流向参与框架的美国公司，不必实施额外的数据保障措施。

相较《隐私盾协议》，《隐私框架》有许多改进。第一，规定了若干关于获取数据的保障措施，将美国情报机构获取数据的权限限制在保护国家安全的必要和相称的范围内。第二，赋予欧盟个人数据主体以新的权利，如查阅资料、改正或删除不正确或非法处理资料的权利。第三，公司的数据保护义务趋于严格，参与的公司必须承诺遵守一系列隐私义务，如目的限制、数据最小化和数据保留、与第三方共享数据的义务等。第四，在数据处理不当时提供不同的补救渠道。美国政府建立了新的具有约束力的两级补救机制来解决个人投诉问题，包括免费的争端解决机制和仲裁小组。

从《安全港协议》到《隐私盾协议》，再到当前的《隐私框架》，欧盟不断提升对数据的控制权，防止数据流向美国，美国则不遗余力地阻止欧盟关闭数据流动的阀门，这反映出美国与欧盟在数字地缘战略中的利益分歧。[①] 表面上欧盟似乎“降伏”了美国，令美国做出更多让步，但事实上由于数据主要从欧盟流向美国，故而在这场博弈中美国才是更大的赢家。

（二）其他国家的数据本地化措施

OECD 将数据本地化措施定义为：在特定的管辖范围内，直接或间接规定数据应被排他性或非排他性地存储或处理的强制性法律或行政要求。[②] 人们普遍认为，“棱镜门”事件是数据本地化措施的关键催化剂。针对美国情报机构进行电子间谍活动带来的主权与安全威胁，许多国家认为保护数据的最佳方式是将数据存储在一国的领域内。近年来，数据本地化措施在世界各地迅速蔓延。颁布数据本地化规定的国家数目几乎翻了一番，从 2017 年的 35 个增加到 2021 年的 62 个；数据本地化措施总数增加了一倍多，从 2017 年的 67 个增加到 2021 年的 144 个。[③] 事实上，早在 20 世纪 70 年代，数据本地化措施就已经存在，只不过在最近的短短几年里，其数量不断增加，这

① 参见鲁传颖：《全球数字地缘政治的战略态势及其影响》，《当代世界》2023 年第 5 期，第 41 页。

② 参见 Dan Svantesson, Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines, *OECD Digital Economy Papers*, No. 301, OECD Publishing, Paris, 2020 - 12 - 22, p. 8。

③ 参见 John Selby, Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?, *International Journal of Law and Information Technology*, Vol. 25 (3), 2017, p. 213。

与各国对国家数据安全的担忧有关。尽管实施数据本地化措施的动机还包括保护个人隐私、促进国内经济发展以及保障国内执法利益，但保护主义是主要动机。欧洲许多国家以及印度和南非等都采取数据本地化措施以保障本国利益和安全。①

从广义上讲，目前各国采取的数据本地化措施大致可以分为四种类型。第一，对数据出境有地理限制，要求对数据的存储或处理必须在特定的国家和地区范围内进行，如俄罗斯。第二，允许将数据复制到来源国以外进行处理，但需要在本地基础设施中留存副本，如印度、印度尼西亚和马来西亚，旨在发展当地经济。第三，基于许可的法规要求，机构必须获得特定个人的同意才能传输数据，如巴西和阿根廷等国要求银行传输数据必须获得客户的明确许可。第四，基于标准体系的数据出境限制，即要求数据出境必须采取标准化的步骤，以确保数据安全和隐私保护。如果将数据本地化理解为泛指对数据跨境流动的任何限制，那么欧盟的 GDPR 当然也属于一种数据本地化措施。

反对数据本地化的观点认为，数据本地化将影响全球互联，为数据流动设置壁垒可能会给国内企业带来短期商业利益，但也将以牺牲创新和更广泛、持久的全球经济增长为代价。互联网“巴尔干化”会降低经济效率、扼杀竞争的道理不难理解，但在一个缺乏政治信任的世界中，数据本地化措施数量的增长说明了各国在确保数据安全与促进经济增长之间更倾向于前者，毕竟国家安全、政治稳定才是经济繁荣的前提与基础。这同时也说明了推动构建一个全球性的数据治理体系的紧迫性与重要性。

（三）域外数据管辖权的扩张趋势

当前，许多国家将域外管辖权规则纳入其数据主权地缘政治战略之中。作为整体战略的一部分，域外管辖权规则能够发挥重要作用。在数据管辖权方面，美国作为大型科技公司的母国，对全球数据的获取具有天然的优势。美国在 2013 年“微软公司诉美国案”中将这种优势付诸实践，随后更是用《云法案》将这种长臂管辖固定下来。美国这种凭借对企业的控制权将手伸向域外数据的长臂管辖令其他国家倍受威胁，但由于缺乏实力与之抗衡，其他国家只能尽可能地通过立法扩展自己对域外数据的管辖权来制衡美国。

目前，对域外数据进行长臂管辖已经成为一种趋势，其中欧盟的 GDPR 最具影响力。GDPR 将长臂管辖范围扩展到覆盖整个世界，并且被很多国家

① 参见 Nigel Cory and Luke Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, *Information Technology & Innovation Foundation*, July 19, 2021, https://www2.itif.org/2021-data-localization.pdf, 2023 年 10 月 2 日。

效仿。根据 GDPR 第 3 条，GDPR 适用于欧盟内外处理欧盟居民个人数据的任何数据控制者或处理者。第一，依据属人原则，对欧盟境内设立的控制者或处理者，无论其处理行为是否在欧盟境内，均适用 GDPR。第二，依据效果原则，对非设立在欧盟境内的数据控制者和处理者，当“向欧盟境内的数据主体提供商品或服务，不论是否要求数据主体支付对价”，以及“对发生在欧盟境内的数据主体之活动进行监控”时适用 GDPR。

2020 年 9 月生效的巴西《一般数据保护法》（LGPD）主要受到欧盟 GDPR 的启发，因此这两部法律在控制者和处理者以及数据主体权利的原则、范围、定义等关键领域高度相似，但它们在处理域外适用问题上存在差异。LGPD 在第 3 条和第 4 条第 4 项中定义了其领土适用范围，依据这些规定，无论数据处理公司总部位于何处或数据存储在何处，LGPD 适用于：第一，旨在向位于巴西的个人提供或供应商品和服务的加工业务；第二，处理巴西境内人员的个人数据；第三，处理在巴西境内收集的个人数据。LGPD 具有比 GDPR 更广泛的域外适用性。印度于 2023 年 8 月颁布了新的《2023 年数字个人数据保护法》（DPDP）。DPDP 适用于印度境内的个人数据处理，如果此类处理与向居住在印度的数据主体提供商品或服务有关，则也适用于印度境外的个人数据处理。可以看出 DPDP 也以效果原则为管辖标准，从而适用于全球处理印度个人数据的企业。

四、数据主权规则发展的中国进路

近年来我国在构建数据主权规则的道路上不断探索。依托《中华人民共和国网络安全法》（以下简称《网络安全法》）（2016）、《中华人民共和国数据安全法》（以下简称《数据安全法》）（2021）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）（2021），以及《数据出境安全评估办法》（2022）等法律法规，我国已经初步形成数据主权的规则体系，对数据进行分级分类管理，这体现了我国捍卫数据主权的决心。然而，从数据主权战略博弈的角度，我国数据主权的原则立场与具体路径仍有待澄清与完善。

（一）中国数据主权应坚持的原则立场

1. 坚守传统主权的核心要义

我国倡导的数据主权以传统主权理论为基础。我国一贯倡导国家主权平等原则与互不干涉内政原则，坚守主权独立的公正价值，坚定维护自身的主权、安全、发展利益，也支持其他国家，特别是广大发展中国家维护自身的主权、安全、发展利益；反对干涉别国内政，倡导各国在涉及核心利益和重

大关切的问题上相互支持。[①] 习近平总书记指出：“我们应该尊重各国自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。”[②] 这种数据主权观是各国在数字经济下获得安全与发展的保障，同时既包含权利维度又包含义务维度，强调国家间的相互性与对等性。这种数据主权观与美国主张的数据主权虚无论针锋相对，是一种在认清美国数据霸权真面目后的防御与自保。

2. 强调数据主权的合作维度

我国坚持的数据主权也绝非威斯特伐利亚时期那种专注各自最高性并与外国竞争的主权，而是一种适应经济全球化发展的主权，因相互依赖的加深而更强调合作性。有学者指出，网络空间应从“相互竞争的主权”转变为“相互依赖的主权”。[③] 相互依赖的数据主权绝非一国为维护私利可以任意取舍的工具。美国一向凭借经济、技术实力向世界其他国家发号施令，推行所谓的“基于规则的国际秩序”，这种路径依赖也延伸到数据领域，这正是所谓数据主权虚无论的本质，其真正目的在于维护美国的数据霸权。基于各国数据主权的多边合作并不符合美国利益，其屡次阻挠网络空间全球治理规则制定的事实印证了这一论断。数据主权也不应是国家为保护主义竖起的监管高墙，这既不符合数字经济发展现实规律，也不符合网络空间的特征。在“网络空间命运共同体”的理念指导下，我国应推广数据主权的合作性与包容性，同各国平等协商，合作共赢，共享数据经济红利，实现共同繁荣。

3. 深化数据主权的安全意蕴

当前，主要大国之间的数据主权战略博弈日趋激烈。美国采取战略进攻模式，加紧构筑所谓“数据同盟体系”；欧盟则采取防守反击模式，筑起“制度高墙”以谋求引领国际规则。[④] 而我国的数据主权战略则以防御为先，注重数据安全。[⑤] 我国长期以来主张以安全为中心的数据利用规则，视数据安全为数字经济发展的战略保障，强调安全和发展并重。在数据安全问题上，我国一贯持坦荡、开放、合作的观点。然而，从语义来看，域外对

① 参见何志鹏：《新时代中国国际法理论的发展》，《中国法学》2023 年第 1 期，第 286 页。

② 习近平：《习近平谈治国理政》第 2 卷，外文出版社 2017 年版，第 533 页。

③ 参见［美］劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》，李旭、沈伟伟译，清华大学出版社 2009 年版，第 299～333 页。

④ 参见熊鸿儒、田杰棠：《突出重围：数据跨境流动规则的“中国方案”》，《人民论坛·学术前沿》2021 年第 Z1 期，第 54 页。

⑤ 参见 Lizhi Liu, The Rise of Data Politics: Digital China and the World, *Studies in Comparative International Development*, Vol. 56 (1), 2021, p. 53。

“数据安全”的理解还停留在传统的数据的完整性、保密性和可用性上，这容易造成域外误以为我国以安全为由制造障碍和壁垒。[①] 同时，随着我国信息通信企业在国际上的竞争力越来越强，美国开始将其对其他国家的数据主权威胁有意引向我国以缓解自身压力，并试图用所谓“价值观”的旗号孤立中国。对此，我国要做到在战略上藐视，在战术上保持重视，积极做好应对。

未来，我国应进一步深化数据主权的安全意蕴。第一，在国家政治层面，数据安全意在不受他国监控与干涉。第二，在社会发展层面，数据安全包含对数据开放共享的治理。第三，在国际经贸层面，数据安全意味着数据跨境的合法有序流动。第四，在私人权利保护方面，数据安全对标个人隐私安全。深化数据安全意蕴的目的并非淡化国家安全的重要性，而是以安全为抓手，全方位构筑我国的数据主权规则体系，增加同他国进行数据主权对话与合作的交汇点。

（二）中国数据主权规则体系的构建与完善

1. 明确国家数据主权战略发展路径

相比美国和欧盟，我国的数据主权战略并不明朗。我国的数据主权战略起步较晚，规则体系以国家安全为要旨，目前仍然主要围绕数据的本地化存储以及数据出境的安全评估展开。当然，我国在数据主权问题上采取的此种防御姿态与我国在同美欧的地缘政治竞争中所处的不利地位相适应。近年来，美国为遏制我国科技发展，对我国科技企业采取出口管制措施与其他制裁措施进行打压，并联合其盟友对我国予以围堵。在此背景下，我国数据主权以防御为先、强调国家安全不无道理。但是，随着我国高新科技企业的快速发展，寻求国家安全的防御型数据主权战略难以激发数字经济的创新活力，此时应当适应变化，主动调整数据主权战略重心向效率倾斜，对此应尽快出台相关的顶层设计文件，做好总体部署和规划。

欧盟虽然在数字经济规模上不敌中美两国，但凭借在数字治理上的领先，成功跻身全球数字经济“第三极”。我国可以借鉴欧盟的数据主权战略，采取防御与进攻相结合的模式，强调数字经济的自主与创新，以数据主权话语为引领，从宏观、中观、微观三个层次深化数据主权战略。第一，勾勒国家数据主权战略的实施路线图，并将数据主权战略视为一个动态的进程，以适应技术发展与竞争态势转变带来的数据主权需求，如数据主权的内涵可能会随着数字经济发展而继续深化，现阶段各国博弈的重心

① 参见刘金瑞：《迈向数据跨境流动的全球规制：基本关切与中国方案》，《行政法学研究》2022 年第 4 期，第 84 页。

在于对数据的控制和跨境数据流动，随着数字经济发展可能更侧重数据如何高效流动与释放数据潜能等层面。第二，不断更新和调整法律和政策工具，坚持包容创新与审慎监管并举，注重平衡安全与效率，在把控安全风险之余强调数据跨境有序流动，构建国内外数据双循环利用的新发展格局。第三，构建相互衔接、彼此协作的数据治理规则体系，如借鉴欧盟区分个人数据与非个人数据分别制定保护与利用规则，持续激发数字创新活力。

2. 完善数据控制与管辖规则的实施细节

为实现对数据的控制，我国对数据进行分级分类管理，并构建了全面的数据出境监管制度，致力于推动数据跨境的安全、有序流动。《网络安全法》和《数据安全法》确立了重要数据治理的基本框架，即重要数据原则上在境内存储，确需向境外提供时应进行安全评估。《个人信息保护法》明确了个人数据出境的三种路径，包括数据安全评估、个人信息保护认证以及个人信息出境标准合同。然而，目前数据出境规则的许多方面仍然含糊不清，如数据安全评估在现实操作中常常令企业感到混乱，从而延缓审批程序；国家安全的内涵不明，涉及的行业缺乏限定，令监管部门和企业无所适从等。对此，我国应当尽快出台实施细则，弥补漏洞与缺陷，同时，在分级分类监管之外还要再细分敏感部门与行业，澄清审批流程，注重现实操作性，以减轻企业的合规负担。

在数据管辖方面，《数据安全法》采用了保护性原则，对在境外损害我国国家安全、公共利益与公民、组织合法权益的数据处理活动予以管辖。近年来，为防止外国法律对我国法人与公民的不当域外适用，我国也通过了“阻却立法”。但从数据的特征以及目前全球数据立法域外管辖权扩张的整体趋势出发，我国也应当适当扩大对域外数据的管辖权，如对一定规模的企业在域外处理我国公民数据的活动对我国造成严重影响的，适用效果原则主张管辖权。效果原则在有的领域运用已经非常普遍，如在反垄断法领域，包括我国在内的很多国家在立法中均规定了效果原则。在执法数据跨境调取方面，2018 年出台的《中华人民共和国国际刑事司法协助法》规定在我国向外国政府请求提供的证据类型中涵盖数据，但考虑到执法效率以及数据的特殊性，可以考虑同其他国家建立更多的双边互助机制，以更加高效快捷地调取跨境数据证据。

3. 注重搭建数据自由流动“朋友圈”

鉴于数据流动的巨大经济价值，目前数据跨境传输成为全球数据主权博弈的焦点。美欧加紧拓展以自身利益为核心的数据规则“朋友圈”，并重新为跨大西洋数据传输架设新的桥梁；一些国家则正努力通过签订数字经济协议和贸易协定等方式构筑新的数据流动圈，强化各自在数据经济中的地位，

如《英国－新加坡数字经济协定》（UKSDEA）。这些双边协调的方式虽然进一步加剧了数据跨境治理格局的碎片化，但解决了在缺乏全球机制下国家相互间数据跨境传输的政治互信问题，增强了不同国家数据法规框架间的互操作性。相比之下，我国亟须在数据跨境流动方面有所突破。

据研究，目前已有超过180个区域贸易协定中增设包括数据跨境流动在内的数字贸易规则专门章节或专门条款。[①] 我国仅加入《区域全面经济伙伴关系协定》（RCEP），而且其中的数据跨境流动规则为原则性规定，较为模糊、抽象。除申请加入《全面与进步跨太平洋伙伴关系协定》（CPTPP）和《数字经济伙伴关系协定》（DEPA）外，我国还应当积极探索加入其他区域性数据跨境流动制度安排。此外，开展个人数据跨境流动的国际合作需要以政治互信为基础，我国可以借鉴美国和欧盟在该问题上的经验，从双边层面寻求更多突破口。[②] 一方面，推进与我国的重要贸易伙伴签订双边数字经贸协议，优先选择与我国贸易交往密切、政治互信基础好的国家；另一方面，通过双边协商，推进建立互惠互利的数据规则互认机制，探索数据跨境流动与合作的新途径、新模式，以实现数据跨境流动“朋友圈”的扩容。

4. 推动全球数据治理规则的形成

碎片化的数据治理格局导致各国无法充分获取数字技术可能带来的价值。鉴于数据在引领数字化创新中的作用，制定跨境数据流动规则、避免数据保护主义、合理划分数据管辖权应是未来各国关注的重点问题，也应成为构建全球数据治理体系的方向。围绕这些方面，我国应当坚定自身立场，积极为国际社会提供中国智慧与方案，以赢得国际话语权。第一，积极向全世界宣传我国的数字治理理念，特别是构建和平、安全、开放、合作、有序的网络空间主张，以及在全球治理领域倡导的“和平合作、互利共赢、创新共享”等原则，以抵御西方国家对我国“价值观”的攻击。第二，正视不同数字经济发展水平国家的共同关切，包括经济发展、个人信息保护、国家安全等，推动数字经济有序竞争。第三，尊重各国数据主权，以属地原则为主要原则，合理划分国家数据管辖权，以减少各国数据管辖权的矛盾与冲突，促进数据证据跨境调取规则的形成，提高数据执法合作的效率。

当前我国对全球数据治理的影响可以通过不同的机制发挥作用。第一，我国应利用好“一带一路”倡议、上海合作组织、金砖国家等合作机

① 参见刘影：《数据跨境流动的国际治理》，《理论导报》2023年第5期，第62页。

② 参见谭观福：《数字贸易中跨境数据流动的国际法规制》，《比较法研究》2022年第3期，第185页。

制，制定数据领域的示范条款，促进数据跨境流动条约的缔结与数据管辖权国际习惯法的生成与发展。鉴于当前国家之间利益分歧较大，我国可以主导优先推进数据软法规则的生成，待条件成熟时再将之转化为有约束力的规则。由国际软法向条约等硬法转换的例子在经济、人权等领域并不鲜见。考虑到国际法缺乏有效的执行机制的现实，国际软法规则在规范有关国家行为方面不一定逊色于条约等硬法。第二，我国科技公司为新兴经济体提供信息和通信技术、电子商务平台和数字监控技术，通过我国企业在这些国家遵守我国数据规则而产生示范和传导效应，从而对新兴经济体产生影响。

五、结语

美国推动数据自由流动的目的在于构建数据霸权，其为迷惑各国放弃数据主权而描绘的网络乌托邦在“棱镜门”事件后轰然坍塌，带来其他国家更加强烈地主张传统主权向网络空间延伸的反弹效应。美国的数据霸权是促使其他国家通过数据主权规则限制数据自由流动、要求数据本地化存储的最大原因。随着数字经济向纵深发展，数据领域的地缘政治竞争愈演愈烈，各国凭借数据主权规则来抵御与平衡各自的安全与发展利益，国家之间的数据主权规则博弈呈现一种攻守交错的复杂态势。对我国而言，一方面，针对美国的数据霸权，我国应努力发展计算、通信与大数据技术，推动前沿科技创新，增强我国的数字经济竞争力；另一方面，我国应借鉴欧盟经验，重视数据在驱动创新方面的作用，推动我国的数据主权规则从当前以防御为主向注重效率倾斜，确保我国数字经济的快速与稳健发展。我国应继续完善数据主权规则体系，积极统筹推进域内数据法治与涉外数据法治，利用好现有机制与平台，积极扩大数据流动“朋友圈”，通过相互尊重数据主权建立更广泛的政治互信，提升我国在塑造数据治理规则方面的影响力。

（责任编辑：方　军）