数据民族主义：驱动逻辑与政策影响*

毛维准　　刘一燊

【内容摘要】 数据本地化和数字保护主义正成为网络空间国际治理和数字经济的重要议题。数字数据是一种战略资源，一些国家通过相关政策争夺数据所有权，数据议题日益与民族主义叙事相结合，数据民族主义由此产生。作为一种由市场、社会与国家等驱动逻辑共同促成的复杂现象，数据民族主义关注数据的排他性控制权，具有明显的政治回应性、国家中心主义和议题拓展等特征。数据民族主义是一种合理的客观政治现象，也是对数据领域全球化与国际权力争斗的一种反应，对全球数字贸易制度、国家主体性、网络空间国际治理和大国互动都有较大政策影响。中国和国际社会应该认识到数据民族主义的必然性，预防其潜在风险，关注其合理诉求，维护各国数据治理自主性，约束数据处置流程中的封闭化和政治化倾向，倡导负责任的数据民族主义，在主权、能力、安全和利益之间达成平衡，积极推进全球数据治理。

【关键词】 数据民族主义　数据治理　数据本地化　国际秩序　网络空间

【作者简介】 毛维准，南京大学政府管理学院副教授，南京大学亚太发展研究中心研究员（南京　邮编：210023）；刘一燊，南京大学政府管理学院硕士研究生（南京　邮编：210023）

【中图分类号】 D81　　**【文献标识码】** A

【文章编号】 1006-1568-(2020)03-0020-23

【DOI 编号】 10.13851/j.cnki.gjzw.202003002

* 本文系国家社科基金“人类命运共同体视角下的中国国际责任体系建构研究”（18BGJ033）的阶段性成果。感谢南京大学法学院彭岳教授和匿名评审人的建设性意见。

新一轮科技革命的发展正在推动国际政治和国际秩序的转变。数字经济（digital economy）及其技术竞争已经成为大国竞争的焦点。[①] 在数字时代，数字数据（data）成为一种关系国家战略的关键资源。联合国《2019 年数字经济报告》预计，到 2022 年，全球互联网协议（IP）流量将达到每秒 150 700 千兆字节，是 2002 年 IP 流量的 1 500 多倍，这些数字数据恰恰是数字经济扩张的驱动因素。[②] 面对具有战略价值的海量资源，各国纷纷在国际和国内层面展开数据治理（data governance）和数据控制权争夺。数据的控制与存储问题被认为事关国家安全、社会公共道德与公共秩序、个人隐私、消费欺诈、国内执法管理和产业发展等各项政策，[③] 也正因为如此，诸如“数字保护主义”（Digital Protectionism）、“数据主权”（Data Sovereignty）、“数据本地化”（Data Localization）和“数字现实政治”（digitalpolitik）等新概念应运而生。[④]

其中，一个值得关注的现象是大国战略竞争背景下的数据所有权与民族主义的交融。各大国在数据资源所有权问题上展开了战略竞争，[⑤] 地缘政治竞争和政府管制行为正在塑造当前的数字经济，国际社会正滑向一个数字“失序”的时代，数字“冷战”结构可能出现。[⑥] 有研究发现，自 2010 年以来，全球各国推行数据本地化措施的力度日益上升，而且几乎所有的二十

① Paul Laudicina, Erik Peterson, and Courtney Rickert McCaffrey, *Competing in an Age of Digital Disorder*, Washington, D. C.: A.T. Kearney’s Global Business Policy Council, June 2019；阎学通：《数字时代的中美战略竞争》，《世界政治研究》2019 年第 2 辑，第 1—18 页。

② UNCTAD, *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*, New York: United Nations, 2019, pp. xvi, 9-10.

③ 彭岳：《数据本地化措施的贸易规制问题》，《环球法律评论》2018 年第 2 期，第 178—192 页；陈咏梅、张娇：《跨境数据流动国际规制新发展：困境与前路》，《上海对外经贸大学学报》2017 年第 6 期，第 37—52 页。

④ Susannah Hodson, “Applying WTO and FTA Disciplines to Data Localization Measures,” *World Trade Review*, Vol. 18, No. 4, 2019, pp. 579-607; Sean McDonald and An Xiao Mina, “The War-Torn Web,” *Foreign Policy*, December 19, 2018, https://foreignpolicy.com/2018/12/19/the-war-torn-web-internet-warring-states-cyber-espionage/; 张国红：《全球数字保护主义的兴起、发展和应对》，《海关与经贸研究》，2019 年 11 月 27 日，第 1—8 页；杜雁芸：《大数据时代国家数据主权问题研究》，《国际观察》2016 年第 3 期，第 1—14 页；蔡翠红：《云时代数据主权概念及其运用前景》，《现代国际关系》2013 年第 12 期，第 58—65 页。

⑤ 阎学通：《数字时代的中美战略竞争》，第 1—18 页。

⑥ Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, pp. 1-2.

国集团（G20）成员都采取了某种形式的数据本地化政策。[①] 与此同时，民族主义情绪和民粹主义政治势力崛起。诚如沃尔特（Stephen M. Walt）所言，当前世界民族主义林立，无论如何民族主义都不会消逝。[②] 在网络时代，民族主义“内生的对抗结构”逐渐加剧了国内外张力与冲突，[③] 并从物理空间映射到网络空间，网络民族主义（Cyber Nationalism）或数字民族主义（Digital Nationalism）现象日益流行。[④]

数字数据也被纳入民族主义叙事之中，国家竞争视角下的跨境数据存储、控制、流动和交易等环节以及数据隐私与安全等也都面临着民族主义的审视。[⑤] 数据民族主义（Data Nationalism）浪潮已经出现。[⑥] 根据统计，当当前世界上 17 个主要国家和欧盟地区已经对跨境数据流动实施了管制强度各异、分类和部门不同的数据民族主义政策。[⑦] 基于此，本文通过市场—社会—国家分析框架对这种数据管理方面的民族主义潮流进行探讨。

① Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, p. 14; and William Alan Reinsch, “A Data Localization Free-for-All?” Center for Strategic and International Studies, March 9, 2018, https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all.

② Stephen M. Walt, “You Can’t Defeat Nationalism, So Stop Trying,” *Foreign Policy*, June 4, 2019, https://foreignpolicy.com/2019/06/04/you-cant-defeat-nationalism-so-stop-trying/.

③ Florian Bieber, “Is Nationalism on the Rise? Assessing Global Trends,” *Ethnopolitics*, Vol. 17, No. 5, 2018, pp. 519-540; 毛维准：《“大逆转”结构下的民粹崛起与秩序重建》，《学海》2018 年第 4 期，第 36—45 页。

④ Farzaneh Badii, Karl Grindal, and Milton Mueller, *Cyber Nationalism and Digital Trade: IGP Workshop Report*, Internet Governance Project, School of Public Policy, Georgia Institute of Technology, June 12, 2018, https://www.internetgovernance.org/2018/06/12/cyber-nationalism-and-digital-trade-igp-workshop-report/; and Akash Kapur, “The Rising Threat of Digital Nationalism,” *The Wall Street Journal*, November 1, 2019, https://www.wsj.com/articles/the-rising-threat-of-digital-nationalism-11572620577.

⑤ Scott Stephenson, “Nationalism and Data Privacy: Think Globally, Data Locally,” *Forbes*, August 15, 2017, https://www.forbes.com/sites/scottstephenson/2017/08/15/nationalism-and-data-privacy-think-globally-data-locally/#2a98ea68747c; and Scott Stephenson, “Data Nationalism in Motion: The Emerging Challenge to Global Business,” *Verisk Review*, Spring 2017, https://www.verisk.com/verisk-review/spring-2017/data-nationalism-in-motion-the-emerging-challenge-to-global-business/.

⑥ Christopher Kuner, “Data Nationalism and Its Discontents,” *Emory Law Journal*, Vol. 64, No.3, 2014, p. 2098.

⑦ 此外，中国台湾地区也实施了相应的管制政策；参见 Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla, *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*, The Centre for Internet and Society, India, March 2019, pp. 49-60；也有统计显示，世界上 107 个国家曾经颁布与数据保护相关的法律条例，参见 UNCTAD, *Information Economy Report 2015: Unlocking the Potential of E-Commerce for Developing Countries*, New York: United Nations, 2015, pp. 65, 70-74, 109-114。

一、数据民族主义的概念界定

当前，学界并没有一个被普遍接受的数据民族主义定义。尽管若干研究使用了数据民族主义的术语，但是却很少对其进行具体的界定，[①] 大多将其简单视为与数据本地化相关的政策实践或理念。例如，世界银行《2016 年世界发展报告》将数据民族主义定义为“一国数据应该储存在国界之内”的“理念”。[②]

但是，政治性是民族主义的首要特性，界定数据民族主义就必须进行政治考量。基于目前的研究，本文将数据民族主义定义为在数字时代国家通过特定权威方式控制与支配数据的存储、处理及所有权等相关问题来实现政治经济利益目标的一种政治导向。它也可以被看作是一种确保国家控制数据的“框定策略”（framing device）。[③] 一般来说，数据民族主义概念主要包含以下三个特征。

第一，数据民族主义具有明显的政治回应性。数据民族主义的指涉对象与数据本地化（Data Localization）概念大致相同，大部分学者在使用过程中也没有区分数据民族主义与数据本地化。[④] 数据本地化主要指特定国家所实施的要求某种具体数据必须存储在本国领土之内的服务器或者数据中心的相关措施，或在更宽泛的意义上指阻止数据跨国界传输的相应措施等。[⑤] 在“棱镜门”事件之后，面对美国国家安全部门的情报搜集与监听，作为一种回应，其他国家坚持将本地数据中心纳入本国司法管辖（national jurisdiction）

① 以钱德（Anupam Chander）和黎（Uyê P. Lê）被广为引用的研究为例，他们的研究以“数据民族主义”为题目，但并未正式界定这个概念。参见 Anupam Chander and Uyê P. Lê, “Data Nationalism,” *Emory Law Journal*, Vol. 64, No. 3, 2014, pp. 677-739。

② The World Bank, *World Development Report 2016: Digital Dividends*, Washington, D. C.: International Bank for Reconstruction and Development/The World Bank, 2016, p. 226.

③ Arindrajit Basu, et al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*, p. 11.

④ Christopher Kuner, “Data Nationalism and Its Discontents,” p. 2089.

⑤ Susannah Hodson, “Applying WTO and FTA Disciplines to Data Localization Measures,” p. 580; and Anupam Chander and Uyê P. Lê, “Data Nationalism,” p. 680.

之下，并严格限制特定等级数据的跨境处理。[①] 这些行动强化了各国数据本地化的趋势。目前，世界上主要国家都实行了数据本地化政策，试图管制跨境数据的流动。[②] 关于数据的民族主义氛围其实早已存在，许多国家要求本国数据只能存储在本国，从而为本国数据提供更好的保障。[③] 从某种意义上来说，数据民族主义是受制于保护主义情绪兴衰起伏的短期政治现象。[④] 这种回应性还体现在数据殖民主义（Data Colonialism）或技术“殖民主义 2.0”（colonialism 2.0）的建构中，它们以此来证明数据民族主义政策是为了回应西方的霸权力量。[⑤]

第二，数据民族主义的议题范围处于持续拓展中，已经超越数据本地化的内涵。从广义上来说，数据民族主义是一种“整体控制”（total control），除数据本地化之外，它还包括互联网的数据流动审查与监视措施等。[⑥] 数据民族主义实际上囊括了“具有不同动机”的若干同类倡议。[⑦] 在这里，数据本地化只是数据民族主义的一种具体举措而已。特别是伴随网络民族主义与数字民族主义的拓展，大国之间的“数字冷战”和“分裂网络”（splinternet）趋势也将加剧。加之在网络安全与个人权利等诉求刺激之下，数据存储与处理亦将复杂化，数据民族主义的范围势必进一步拓展。[⑧]

第三，数据民族主义概念具有清晰的国家中心特征。一方面，数据民族

① Ronald J. Deibert and Louis W. Pauly, “Mutual Entanglement and Complex Sovereignty in Cyberspace,” in Didier Bigo, Engin Isin, and Evelyn Ruppert, eds., *Data Politics: Worlds, Subjects, Rights*, Oxon: Routledge, 2019, p. 84.

② Susannah Hodson, “Applying WTO and FTA Disciplines to Data Localization Measures,” p. 580.

③ Scott Stephenson, “Nationalism and Data Privacy: Think Globally, Data Locally.”

④ Christopher Kuner, “Data Nationalism and Its Discontents,” p. 2098; 2017 年，有观察指出，自 2008 年金融危机以来，全球最大的 60 个经济体采取了 7000 多项贸易保护主义措施，参见 Marc Jones, “World Has Racked up 7 000 Protectionist Measures since Crisis: Study,” *Reuters*, November 15, 2017, https://www.reuters.com/article/us-global-economy-protectionism/world-has-racked-up-7000-protectionist-measures-since-crisis-study-idUSKBN1DF005。

⑤ Arindrajit Basu, et al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*, p. 12; and Rahul Matthan, “Colonialism 2.0–Truly,” *SWARAJYA*, January 1, 2019, https://swarajyamag.com/magazine/colonialism-20-truly.

⑥ Anupam Chander and Uyê P. Lê, “Data Nationalism,” p. 677.

⑦ Christopher Kuner, “Data Nationalism and Its Discontents,” p. 2090.

⑧ Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, pp. 1-2; and Matthew Bey, “The Age of Splinternet: The Inevitable Fracturing of the Internet,” *Stratfor*, April 25, 2019,https://worldview.stratfor.com/article/age-splinternet-inevitable-fracturing-internet-data-privacy-tech.

主义的逻辑起点是数据主权。数据所有权也被称为电子领主权（electronic encomienda），[①] 它强调对数据的主权控制（sovereign control）。[②] 数字数据可以充当一种展现政治、军事和商业影响力的杠杆，因此，各个国家和个体都正在发展新的能力来保护这种战略资源。[③] 例如，印度极力从数据民族主义角度强调其推行数据本地化政策的必要性，宣称印度需要同科技公司与敌对国家滥用数据“作斗争”，数字民族主义“恰逢其时”。[④] 另一方面，数据民族主义也是国家推行的数字贸易保护主义行为，其基本逻辑是互联世界中的重商主义（Mercantilism）或电子重商主义（Digital Mercantilism）。[⑤]

综上所述，数据民族主义已经形成一种鼓吹数据资源的战略属性并强调其排他性控制权的政策趋势。从内容上来看，数据民族主义拥有双重维度。首先，它是一种网络空间对物理空间的映射，即国家试图将网络空间衍生的数据资源和权力互动延伸到夹杂着政治、经贸和科技诸领域斗争的物理空间。其次，这也是一种战略资源化过程，它将网络空间视为陆、海、空、天之外的第五大战略空间，以政治化视角聚焦作为未来收益巨大的“新油田”（new oil）的数据资源。[⑥]

---

① Didier Bigo and Laurent Bonelli, “Digital Data and The Transnational Intelligence Space,” in Didier Bigo, Engin Isin, and Evelyn Ruppert, eds., *Data Politics: Worlds, Subjects, Rights*, Oxon: Routledge, 2019, pp. 104-105.

② See Arindrajit Basu, et al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*.

③ Matthew D. Johnson, “Cyber Espionage,” in Paul Joseph, ed., *The SAGE Encyclopedia of War: Social Science Perspectives*, California: Sage, 2017, p. 437; and Sean McDonald and An Xiao Mina, “The War-Torn Web.”

④ Srijan Shukla, “‘Data Nationalism’ Needed to Combat Misuse by Tech Firms, Hostile Countries: Mohandas Pai,” *The Print*, December 5, 2019, https://theprint.in/india/data-nationalism-needed-to-combat-misuse-by-tech-firms-hostile-countries-mohandas-pai/330977/; and PTI, “Data is National Asset, It Must be Protected; Digital Nationalism Need of the Hour: SJM,” *The Economic Times*, December 8, 2019, https://economictimes.indiatimes.com/news/politics-and-nation/data-is-national-asset-it-must-be-protected-digital-nationalism-need-of-the-hour-sjm/articleshow/72427342.cms?from=mdr.

⑤ Ashok K Nag, “Data Localisation: Mercantilism in a Networked World,” *The India Forum*, August 2, 2019, https://www.theindiaforum.in/article/data-localisation-mercantilism-networked-world.

⑥ 刘建伟、余冬平：《试论网络空间的政治化》，《国际关系研究》2013 年第 6 期，第 119—131 页；周宏仁：《网络空间的崛起与战略稳定》，《国际展望》2019 年第 3 期，第 21—34 页；Paul Laudicina, et al., *Competing in an Age of Digital Disorder*; Anupam Chander and Uyê P. Lê, “Data Nationalism,” pp. 677-739; *Digital Economy Compass 2019*, Statista, 2019, p. 4; Scott Stephenson, “Nationalism and Data Privacy: Think Globally, Data Locally”。

二、数据民族主义的驱动逻辑

数据民族主义政策通常至少受到市场、社会和国家三个层面的驱动。不同国家在数据民族主义方面的态度分歧源于该国在这三个层面的综合考量。

（一）市场驱动逻辑

数据民族主义的市场驱动逻辑强调数据保护主义和数据本地化措施背后的经济考量，其逻辑关键词是利益。

市场驱动逻辑认为，国家推行数据民族主义政策的目的是促进本国经济的发展。[①] 数字经济已经成为当前国际经贸的一种主流形态。[②] 但是，从地理上来看，数字经济发展并不均衡，呈现高度数字化国家和联结度低下国家并存以及中美等大国数字竞争等特征。[③] 这种失衡的现状使众多发展中国家开始推行以数字保护主义为代表的数据民族主义政策。根据美国国际贸易委员会的界定，数字贸易保护主义主要包含数据本地化、跨境数据流动限制、市场准入限制、政府采购政策、知识产权侵权、强制技术转让、网页拦截和过滤以及地理屏蔽等贸易壁垒。[④]

第一，从市场驱动逻辑来看，数据民族主义兴起带来了一个看似矛盾的国际现象。一方面，不论是发达国家还是发展中国家，主要大国都在推行这种市场逻辑驱动的数据保护行为。从二分法来看，美国等发达国家更倾向于主张跨境数据自由流动，而发展中国家则倾向于采取数据本地化措施。[⑤] 另一方面，这些大国也希望通过世界贸易组织、俱乐部式的国家间论坛（如OECD）、双边贸易协定等手段保障数据自由流动或者协调彼此间的数据本

① 汪晓风、周骁：《数字贸易壁垒：美国的认知与政策》，《复旦国际关系评论》2019 年第 1 期，第 1—15 页。

② 彭岳：《数据本地化措施的贸易规制问题》，第 178 页。

③ UNCTAD, *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*, pp. xv-xvi.

④ USITC, *Digital Trade in the U.S. and Global Economies, Part 1*, Investigation No. 332-532, U.S. International Trade Commission, 2013, www.usitc.gov/publications/332/pub4415.pdf.

⑤ 薛亚君：《数字贸易规则中的数据本地化问题探究》，《对外经贸实务》2019 年第 8 期，第 17—20 页。

地化举措。例如，在 2007 年以后，美国与韩国、欧盟等分别在双边和多边贸易协定框架内制定了跨境数据流动的相关条款，并将这种政策实践拓展到《跨太平洋伙伴关系协定》（TPP）及《跨大西洋贸易与投资伙伴关系协定》（TTIP）等倡议中。①

第二，市场驱动逻辑在政策上存在态度与实践不一致的情况。作为市场驱动逻辑实践的代表国家，美国虽然实施了若干数据保护主义政策，但具有讽刺意味的是，它却对数字保护主义总体上持反对态度，批评其会威胁经济增长。② 即使如此，美国对数字保护主义的态度也经常陷入消除贸易壁垒与掌控主导权以及强调隐私权与推行信息监管等自相矛盾的境地。③

第三，市场驱动逻辑源于美国所拥有的互联网技术优势。美国倡导数据自由流动和利用贸易协议来解决跨境互联网事宜的前提是其在互联网技术领域中的绝对优势。美国的技术优势帮助其在数字经济领域维持着绝对竞争优势。同时，其他国家则希望通过数据民族主义政策强化本国数字产业的竞争力，摆脱对美国的依赖，打破美国的垄断地位。④

当然，偏重经济考量也引发了一些学者对市场驱动逻辑的批评。经济发展是国家的重要目的但不是唯一目的，公民权利与国家安全的重要性同样不容忽视。在美国占据技术优势的结构下，其他国家正面临潜在的信息安全威胁。因此，超越经济和市场的考量转而思考自身价值与安全的数据民族主义政策随之兴起。⑤

（二）社会驱动逻辑

数据民族主义的社会驱动逻辑将落脚点放在保护公民基本权利上。欧洲国家是该逻辑在实践领域的代表。在“棱镜门”事件后，欧洲民众因各国情报部门对个人隐私数据的监控而产生极大恐慌，个人数据隐私保护的正当性

① 张生：《美国跨境数据流动的国际法规制路径与中国的因应》，《经贸法律评论》2019 年第 4 期，第 79—93 页。

② Rob Lever, “U.S. Commerce Secretary Warns of ‘Digital Protectionism,’ ” *Phys.org*, June 22, 2016, https://phys.org/news/2016-06-commerce-secretary-digital-protectionism.html.

③ [美]苏珊·阿里尔·阿伦森：《数字贸易失衡及其对互联网治理的影响》，《信息安全与通信保密》2017 年第 2 期，第 65—67 页。

④ 同上，第 65—66 页。

⑤ Ronald J. Deibert and Louis W. Pauly, “Mutual Entanglement and Complex Sovereignty in Cyberspace,” p. 84.

问题随之引起各国和国际组织的关注。特别是自斯诺登（Edward Snowden）曝光美国国家安全局大规模跨国监听项目后，多个欧洲国家如德国、法国对此表示强烈不满，并加快了推动数据保护体系建设的步伐。[①]

第一，重大理念冲突是社会驱动逻辑的基础。欧盟与美国因在数据保护上的理念冲突而无法达成一致。[②] 相对于美国强调无条件的数据跨境自由流动，欧盟则坚持在保障数据跨境流动与维护个人隐私之间找到平衡。欧盟将涉及个人信息的数据视为公民权的一部分，强调其在社会规范层面的价值，试图通过建立完整的个人数据保护体系来平衡自由市场和公民权利，坚持市场竞争不应与社会“脱嵌”。[③]

第二，社会驱动逻辑强调数据在社会规范层面的价值。该逻辑认为，偏重市场驱动逻辑的贸易保护主义并非数据民族主义产生的唯一原因。以库勒（Christopher Kuner）为代表的德国学者指出，国家可能出于非经济考量推行数据民族主义政策，这些考量包括民众对全球化的担忧、试图在互联网中维持国家边界等。[④] 这种规范性基础来源于公民社会的基本价值和相应权利，核心在于强调公民社会在数字化时代的重要性。相对于美国对市场和自由贸易的重视，欧盟更重视将个人数据作为公民权利的延伸。[⑤]《通用数据保护条例》正是在强调保障作为个人基本权利的个人数据基础上制定的。[⑥]

第三，对技术价值的认知也是社会驱动逻辑者坚持数据民族主义立场的重要原因。欧盟采取数据民族主义政策的社会逻辑可以归因于其技术地位不强、数字经济地位面临冲击、保守民族心理及文化传统影响等因素。[⑦] 特别

① Laura Smith-Spark, “Germany’s Angela Merkel: Relations with U.S. ‘Severely Shaken’ over Spying Claims,” CNN, October 24, 2013, https://edition.cnn.com/2013/10/24/world/europe/europe-summit-nsa-surveillance/; Adrian Croft, Arshad Mohammed, Alexandria Sage, and Mark John, “UPDATE 1-France Summons U.S. Ambassador over Spying Report,” Reuters, October 21, 2013, https://www.nytimes.com/reuters/2013/10/21/world/europe/21reuters-france-nsa.html.

② 彭岳：《数据本地化措施的贸易规制问题》，第 178—192 页。

③ Peter Nedergaard, “The Ordoliberalisation of the European Union?” *Journal of European Integration*, Vol. 42, No. 2, 2020, pp. 1-18.

④ Christopher Kuner, “Data Nationalism and Its Discontents,” p. 2090.

⑤ 薛亚君：《数字贸易规则中的数据本地化问题探究》，第 17—20 页。

⑥ 其第一条强调“保护自然人的基本权利与自由，特别是自然人享有的个人数据保护的权利。”参见 *General Data Protection Regulation*, https://gdpr-info.eu/art-1-gdpr/。

⑦ 周念利、李玉昊：《全球数字贸易治理体系构建过程中的美欧分歧》，《理论视野》

是面对美国的技术中立立场，欧洲坚持技术不中立，聚焦技术内在价值之外的社会价值，因此，数据技术的使用必须考虑其社会影响。[①]

当然，社会驱动逻辑也面临不少争议。例如，与数据民族主义的数据保护权利不同，数据自由跨境流动也被视为一种基本人权，因此，社会驱动逻辑可能威胁民主与法治的潜在价值。[②] 特别是数据民族主义无助于缓和公民对隐私泄露的担忧，美国等国家的技术优势足以打破数据民族主义政策为公民个人信息所提供的保护。[③]

（三）国家驱动逻辑

数据民族主义的国家驱动逻辑强调国家和政府在数据处置过程中所扮演的角色。在日益白热化的全球数据战背景下，国家与政府在网络治理中的作用更为显著。[④]

美国国际关系学者丹尼尔·德雷兹纳（Daniel W. Drezner）指出，国家特别是大国在处理由全球化和网络导致的社会和政治外部性议题中依然是主要行为体。[⑤] 2019 年以来，越来越多的国家试图对数据施加更大的主权控制。[⑥] 同时，国家在建构全球网络治理框架中的积极角色也得到了认可。联合国强调“全政府式回应”的重要性，并认为合适的国家政策在推动数字价值方面发挥着关键作用。[⑦] 国家驱动逻辑包含两个维度，即主权与能力。

第一，数据民族主义首先是一种国家主权的体现，它是数据主权的一种延伸。首先，数据主权已经成为一些国家保护大数据的基本原则。[⑧] 它致力

2017 年第 9 期，第 76—81 页。

① 薛亚君：《数字贸易规则中的数据本地化问题探究》，第 17—20 页。

② Christopher Kuner, “Data Nationalism and Its Discontents,” p. 2096.

③ Anupam Chander and Uyê P. Lê, “Data Nationalism,” p. 680.

④ Samm Sacks and Justin Sherman, “The Global Data War Heats Up,” *The Atlantic*, June 26, 2019, https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/.

⑤ Daniel W. Drezner, “The Global Governance of the Internet: Bringing the State Back In,” *Political Science Quarterly*, Vol. 119, No. 3, 2004, p. 478.

⑥ Arindrajit Basu, “The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam,” *The Diplomat*, January 10, 2020, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/.

⑦ UNCTAD, *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*, p. xviii.

⑧ 齐爱民、盘佳：《数据权、数据主权的确立与大数据保护的基本原则》，《苏州大学学报（哲学社会科学版）》2015 年第 1 期，第 64—70 页。

于突出主权国家维护权威和提升合法性的需求。[①] 各国将数据视为主权的一个基本假定是，网络空间是国家竞争的新场域，政治化和政治、军事持续博弈互动是未来网络空间发展的重要趋势。[②] 因为主权具有排他性和独立性，所以数据主权假设存在可能损害自身的潜在敌对者，并认为敌对者可能会利用数据对自己采取战略行动。[③] 其次，国际数据治理实践表现出主权思维的回归。尽管西欧已经步入所谓“后主权”（Post-Sovereignty）时代，[④] 但是，欧盟各国却在数据和数字基础设施方面坚持主权框架。例如，欧盟提出数字主权（digital sovereignty）概念，并致力于展现欧洲对技术基础设施的主权和控制，它已经变成一个相当宽泛的概念。[⑤] 数字主权的重要目标之一是数据主权，以德国为首的欧盟成员国呼吁，欧洲应维护数据主权和相应数据基础设施。[⑥] 德国总理默克尔指出，“数据主权至高无上。”[⑦]

当然，目前国家数据主权的理念并未得到普遍认可，全球数据保护工作也不成体系，不同国家的数据监管方式也大相径庭，甚至一些发展中国家在数据本地化规制方面仍然存在立法空白。[⑧]

① 蔡翠红：《云时代数据主权概念及其运用前景》，第 58 页。

② 任政：《网络空间政策的形成和界定》，《国际研究参考》2019 年第 9 期，第 9—17 页。

③ Zachary Peterson, Mark Gondree, and Robert Beverly, “A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud,” HotCloud’11: Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing, 2011, https://www.usenix.org/legacy/events/hotcloud11/tech/final_files/Peterson.pdf.

④ Richard Bellamy, “A European Republic of Sovereign States: Sovereignty, Republicanism, and the European Union,” *European Journal of Political Theory*, Vol. 16, No. 2, 2017, pp. 188-209.

⑤ Kenneth Propp, “Waving the Flag of Digital Sovereignty,” Atlantic Council, December 11, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/; and Scott Fulton III, “Continental Drift: Is Digital Sovereignty Splitting Global Data Centers?” Data Center Knowledge, January 2, 2020, https://www.datacenterknowledge.com/regulation/continental-drift-digital-sovereignty-splitting-global-data-centers.

⑥ Scott Fulton III, “Continental Drift: Is Digital Sovereignty Splitting Global Data Centers?”; Federal Ministry for Economic Affairs and Energy, Federal Ministry of Education and Research, *Project GAIA-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem (Executive Summary)*, Germany, October 14, 2019, https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6.

⑦ Die Bundesregierung, “Datensouveränität ist höchstes Gebot,” Deutschland, October 29, 2019, https://www.bundesregierung.de/breg-de/themen/digitalisierung/kanzlerin-bei-digitalgipfel-1686406.

⑧ 刘杨钺、张旭：《政治秩序与网络空间国家主权的缘起》，《外交评论》2019 年第 1

第二，能力维度也是数据民族主义国家驱动逻辑的重要支柱。首先，能力本来就是主权概念的内在要素。斯蒂芬·克拉斯纳（Stephen D. Krasner）认为，主权是一种与国家管理跨边界活动的能力相关的排他性控制权。[①] 安妮-玛丽·斯劳特（Anne-Marie Slaughter）也认为，将主权视为一种能力更符合当今的国际现实。[②] 因此，数据主权是一种基于数据掌控能力的权力，数据主体的行为能力构成数据主权的重要基础，它的分散则将挑战数据主权的现实应用。[③] 其次，国家能力也是影响数据民族主义政策的重要变量。多国数据规制的实践显示，国家能力是决定数据本地化措施的一个关键变量，强大的国家能力能够推动市场完善、建立相关规范并支持数字经济的发展；与之相对，能力较弱的国家仅能部分实现数据民族主义的目标，最终可能对国家经济和数字经济转型带来负面影响。[④] 实际上，政府需要一定的政策空间来规范数字经济以实现其公共政策目标；同时，数据监管和处理涉及若干价值目标，如人权、贸易、经济价值创造与获取、执法和国家安全，这也要求国家和政府首先具备政策制定与实施的国家能力。[⑤] 再次，技术能力是数据民族主义得以持续的重要基础。在全球竞争的背景下，数字技术能力决定着各国在数字经济中的竞争力。[⑥] 从本质来看，数据保护自始至终都是一种技术议题。[⑦] 但是，一些采取数据民族主义政策保护自身的举措恰是为了回应对技术的恐惧，试图消除因美国运用技术进行监控带来的恐惧。[⑧] 各国也

期，第 122 页；联合国贸易和发展会议：《信息经济报告 2017：数字化、贸易和发展（概述）》，联合国，2017 年，第 7 页。

① Stephen D. Krasner, *Sovereignty: Organized Hypocrisy*, Princeton: Princeton University Press, 1999, p. 4.

② Anne-Marie Slaughter, *A New World Order*, Princeton: Princeton University Press, 2004, p. 266.

③ 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，第 113—119 页；蔡翠红：《云时代数据主权概念及其运用前景》，第 58—65 页。

④ Kaushambi Bagchi and Sashank Kapilavai, "Political Economy of Data Nationalism," presented at The 22nd Biennial Conference of the International Telecommunications Society: "Beyond the Boundaries: Challenges for Business, Policy and Society," Seoul, Korea, International Telecommunications Society (ITS), June 24-27, 2018.

⑤ UNCTAD, *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*, p. xx.

⑥ Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, p. 18.

⑦ "Technology Monitoring," European Data Protection Supervisor, https://edps.europa.eu/data-protection/our-work/technology-monitoring_en.

⑧ Stewart Room, Peter Almond, and Kayleigh Clark, *Technology's Role in Data Protection:*

都是基于技术（通信技术和信息技术等）能力来制定数据本地化的相关政策。[①] 无论是个人隐私还是网络安全抑或数据检视，都需要技术系统和相应能力的支撑。例如，欧盟致力于将技术因素主权化，它发起技术竞赛试图追赶美国和中国的步伐，[②] 并强调其拥有可以与美国和中国竞争的技术能力，因此，欧盟通过投资新一代技术来巩固数字能力，推动“敏捷数据”（data-agile）经济的成功，从而维护其在关键赋能技术和数据经济基础设施方面的技术主权。[③] 欧盟委员会主席冯德莱恩（Ursula von der Leyen）认为，技术主权的概念能够展现欧洲必须根据自身的价值观并遵守自己的规则来做出自由选择的能力。[④]

然而，技术能力并非所有国家都具备，也并不是所有国家都有能力建立并支撑采取数据民族主义政策所需要的技术支柱。数字经济大多是技术密集型和资本密集型产业，数据安全是一种关于行为体技术、组织和财政能力的“函数”，这些要素都关系到国家的技术能力。不少国家不仅缺乏有效保护数据的能力，也缺乏适配人力资源和安全审核机制的资源。[⑤]

（四）互动中的三元驱动逻辑

数据民族主义是一种由多种因素共同驱动产生的国际政治现象。不同国家对市场、社会和国家不同层面驱动逻辑的侧重，造成了它们在采取数据民族主义措施方面的差别。简言之，市场驱动逻辑将数据民族主义视为一种与利益紧密相关的新型贸易保护主义；社会驱动逻辑则关注数据保护政策中的公民权利、自由、人权与安全等合法价值；国家驱动逻辑将数据处理的落脚点放在国家主权和能力维度之上。

The Missing Link in GDPR Transformation, PWC, January 2018.

① Anupam Chander and Uyê P. Lê, “Data Nationalism,” pp. 677-739; and Nigel Cory, “Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?” Information Technology and Innovation Foundation, May 2017.

② Graig J. Willy, “Europe’s Tech Race-Trying to Keep Pace with US and China,” *EU Observer*, June 2018, https://euobserver.com/opinion/142056.

③ European Commission, *A European Strategy for Data*, Brussels: European Union, February 2020, pp. 3-5.

④ Ursula von der Leyen, “Shaping Europe’s Digital Future: Op-ed by Ursula von der Leyen, President of the European Commission,” European Commission, February 19, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260.

⑤ Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, Brookings, March 2018, pp. 19-20.

第一，数据民族主义的根源不仅仅是保护主义。[①] 单个维度的驱动逻辑并不能解释一个国家的数据民族主义政策，不同驱动逻辑之间的张力依然显著。伴随着数据政治化和全球竞争程度的提升，各国在制定本国数据本地化政策时都各有侧重地纳入三种驱动逻辑。它们在制定政策时可能会同时权衡这些存在内在冲突的因素。例如，面对市场驱动逻辑，数据民族主义不仅只是一种源于保护主义情绪的政治现象，它也必须要考量社会驱动逻辑中因全球化和社会不确定性所衍生的对基本价值（fundamental values）的关切。[②]

第二，即使社会驱动逻辑并非出于贸易保护主义的目的，但它在事实上却扮演了贸易壁垒的角色，制约着数字经济的发展。例如，欧盟数字经济生产与消费的失衡为欧盟提供了贸易保护的动机，信息保护系统实际上发挥了贸易壁垒的作用。[③] 美国商务部长罗斯（Wilbur Ross）也认为，严格的个人数据保护规范在未来将制造新的贸易壁垒。[④] 当然，社会驱动逻辑也面临内部张力的冲击。其中的理念冲突、价值隔阂和制度差异都影响着美欧双方的跨境数据管制。[⑤]

第三，国家驱动逻辑在数据民族主义政策中的主动角色变得日益显著。例如，尽管美国明确支持数据自由流动，但其也积极推动国家与市场的互动，它的市场逻辑与国家驱动逻辑合流，并充分体现在国家政策中。美国除利用自身技术霸权攫取数据不对称优势之外，还积极利用国防与安全理由来推行“无条件”管制。[⑥] 实际上，国家在数据民族主义拓展过程中扮演着一个略显矛盾的角色。各个国家和政府都担心自己的数据被转到国界之外，但它们同时又希望将国外数据置于本国管辖之下，或希望推动本国的跨国公司成为

① Christopher Kuner, “Data Nationalism and Its Discontents,” p. 2097.

② Christopher Kuner, “Data Nationalism and Its Discontents,” pp. 2097-2098.

③ 田晓萍：《贸易壁垒视角下的欧盟〈一般数据保护条例〉》，《政法论丛》2019 年第 4 期，第 124 页。

④ Wilbur Ross, “EU Data Privacy Laws are Likely to Create Barriers to Trade,” *Financial Times*, May 30, 2018, https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c.

⑤ 彭岳：《数据本地化措施的贸易规制问题》，第 178—192 页；James Whitman, “The Two Western Cultures of Privacy: Dignity versus Liberty,” *Yale Law Journal*, Vol. 113, No. 6, 2004, pp. 1151-1223.

⑥ Arindrajit Basu, et al., *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*, p. 59.

数据存储的领导者。[①]

第四，数据民族主义的有效性面临质疑。数据民族主义事实上无益于个人或企业信息安全的保护。[②] 研究发现，鉴于法律制度不健全和信息技术差距等原因，数据民族主义宣称的数据隐私和安全目标都无法实现。[③] 因此，面对当前将数据本地化措施视为国家安全的必然要求的观点，有学者认为这一主张能否在国际交往层面获得普适性和优先性仍需进一步论证。[④]

三、数据民族主义政策的国际影响

在数字化时代，数据资源已经对政治、经济和社会等多个领域产生了影响。在大国竞争日益加剧的背景下，数据民族主义会成为一股不容小觑的政治潮流，可能对当前的全球数字经贸秩序、大国关系互动、国家主导地位和网络空间全球治理带来较大影响，并反映出其较强的政策含义。

（一）对全球数字经贸秩序的影响

一方面，数据民族主义直接冲击跨境数据的自由流动和全球数字经济的顺利开展。在国际经济领域，数据民族主义表现为以贸易壁垒为特征的数字保护主义。[⑤] 在以邻为壑的数字保护主义影响下，互联网的碎片化不可避免，这将阻碍全球数字贸易的正常发展。[⑥] 数字保护主义政策会导致相关企业的成本上升和市场竞争力的下降，进而制约全球数字经济、国际数字贸易、技术扩散创新和全球价值链的健康发展。同时，数字保护主义多以非关税壁垒

① Anupam Chander and Uyê P. Lê, “Data Nationalism,” p. 725.

② Daniel Castro, “The False Promise of Data Nationalism,” Information Technology and Innovation Foundation, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

③ 周念利、李玉昊：《全球数字贸易治理体系构建过程中的美欧分歧》，第 76—81 页。

④ 彭岳：《数据本地化措施的贸易规制问题》，第 180 页；王玥：《试论网络数据本地化立法的正当性》，《西安交通大学学报（社会科学版）》2016 年第 1 期，第 56—57 页。

⑤ John Selby, “Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?” *International Journal of Law and Information Technology*, Vol. 25, No. 3, 2017, pp. 213-232.

⑥ Sarah Box, *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*, Centre for International Governance Innovation and Chatham House, May 2016.

形式为主，国际社会面临数字贸易规则与争端解决机制匮乏等问题。[①] 因此，数据民族主义政策必然会损害全球规模经济视角下的科技产业经济逻辑，[②] 并成为互联网产业的致命威胁。[③] 有研究发现，数据民族主义政策导致了多国国内生产总值（GDP）的下降。[④] 如果不调整相关政策，数据民族主义对国家经济的负面影响还将持续。[⑤] 据估计，数字保护主义可能会导致全球经济增长率下降 1.7%。[⑥]

另一方面，数据民族主义政策冲击全球数字经济治理的规制，加剧了当前国际贸易制度改革面临的困境。当前全球贸易体系面临的挑战之一是全球贸易规则缺乏对数据保护的具体规定，也未形成与数字贸易发展相匹配的国际监管环境。[⑦] 数据民族主义政策已经对跨境数据流动国际制度的建构构成障碍，这对试图实现跨境数据自由流动目标的多边贸易谈判，特别是美国主导的相关倡议提出了挑战。[⑧] 当前以 WTO 为中心的全球贸易协定文本实际上没有正式触及与数字贸易相关的问题，在数据本地化方面，相关法律适用也面临着不确定性，各国因数字规制陷入争论。在此背景下，以数据本地化和数字保护主义为特征的数据民族主义政策对当前的国际数字制度建构形成直接挑战。[⑨]

① 张国红：《全球数字保护主义的兴起、发展和应对》，第 1—8 页。

② Neha Mishra, “Data Localization Laws in a Digital World: Data Protection or Data Protectionism?” *The Public Sphere (2016): NUS Centre for International Law Research Paper*, No. 19/05, 2015.

③ Anupam Chander and Uyê P. Lê, “Data Nationalism,” p. 681.

④ Matthias Bauer, et al., “The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce,” *European Centre for International Political Economy*, March 2013, https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

⑤ Matthias Bauer, “Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization,” *Global Commission on Internet Governance Paper Series*, May 10, 2016, https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization.

⑥ Susan Lund and Laura Tyson, “Globalization Is Not in Retreat: Digital Technology and the Future of Trade,” *Foreign Affairs*, Vol. 97, No. 3, 2018, p. 137.

⑦ Manfred Elsig, Michael Hahn, and Gabriele Spilker, “Introduction: Current Challenges and Future Scenarios,” in Gabriele Spilker, Manfred Elsig, and Michael Hahn, eds., *The Shifting Landscape of Global Trade Governance: World Trade Forum*, Cambridge: Cambridge University Press, 2019, pp. 2-3; 张国红：《全球数字保护主义的兴起、发展和应对》，第 1—8 页。

⑧ 陈咏梅、张姣：《跨境数据流动国际规制新发展：困境与前路》，第 37—52 页。

⑨ 彭岳：《数据本地化措施的贸易规制问题》，第 178—192 页。当然，也有学者认为，

（二）对大国互动关系的影响

数据民族主义是大国竞争在数据资源方面的体现，它也必然会加剧大国之间的竞争。目前，数据存储与数据本地化已经成为中、美、俄、欧等大国或地区竞逐的重要领域。伴随着数据利用价值与使用方式的变化，管辖权成为各国对抗的焦点。[①] 目前，全球数据战和数字贸易战已经开始，数据本地化和隐私权之争等只是这场战争在监管方面的体现。[②]

在数据民族主义和技术民族主义旗帜下，以中美为代表的大国（还包括欧盟、日本、韩国、俄罗斯和印度等国家和地区）在数字技术（包括 5G 技术和人工智能技术等）和跨境数据流动方面展开了全面竞争，并具有越来越显著的地缘政治色彩，最终将导致出现一个政府管制行动强化与全球数字主导权竞争加剧并存的“数字失序”时期。[③]

数据民族主义政策抬升了大国政策互动中权力政治逻辑的地位，导致国家间竞争出现日常化和碎片化特征。一方面，各国的数据本地化政策引发了美国政府的不满，导致美国与这些国家产生经贸、外交和政治摩擦，加剧了主要国家之间的竞争。其他国家则试图通过立法手段来防止美国滥用技术霸权干涉本国并损害本国利益，而美国则竭力阻止其他国家出台这种政策或将数据本地化置于地区贸易协定之中。[④] 例如，特朗普政府曾利用签证手段来制裁印度等执行本地化政策的国家。[⑤]

在当前《服务贸易协定》指导下的自由贸易协定谈判是解决数字贸易壁垒的可能方式，参见 Susannah Hodson, “Applying WTO and FTA Disciplines to Data Localization Measures,” pp.579-607.

① 王志安：《云计算和大数据时代的国家立法管辖权——数据本地化与数据全球化的大对抗?》，《交大法学》2019 年第 1 期，第 19—20 页。

② Dan Ciuriak and Maria Ptashkina, “Started the Digital Trade Wars Have: Delineating the Regulatory Battlegrounds,” International Centre for Trade and Sustainable Development, January 9, 2018, https://www.ictsd.org/opinion/started-the-digital-trade-wars-have-delineating-the-regulatory-battlegrounds; Samm Sacks and Justin Sherman, “The Global Data War Heats Up.”

③ Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, pp. 15-23.

④ John Selby, “Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?” pp. 213-232; and Annegret Bendiek, “Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection,” *SWP Research Paper No. 5*, Stiftung Wissenschaft und Politik, March 2014.

⑤ Arindrajit Basu, “India’s Role in Global Cyber Policy Formulation,” *Lawfare*, November 7, 2019, http://www.indiasoftwarebrief.com/520508-india-s-role-in-global-cyber-policy-formulation-lawfare.

另一方面，数据民族主义政策也推动不同大国之间的阵营对峙与联盟重组，加剧了不同网络空间治理模式的博弈。例如，美国联合其二十多个盟友在联合国舞台上围绕联合国政府专家组等制度架构展开争夺，也在“国家主导”网络治理模式和“多利益攸关方”治理模式方面展开竞争。[①] 在数据治理实践方面，以企业为中心的美国模式、以国家为中心的中国模式和以个人为中心的欧盟模式已经开始竞逐。[②] 例如，在 2019 年 G20 大阪峰会上，金砖国家特别强调坚持数据主权的必要性。[③] 另外，尽管金砖国家内部存在一定合作潜力，但是它们在数字与网络治理方面也存在从宏观原则到具体规则方面的冲突和摩擦。[④]

（三）对主权国家主导地位的影响

数据民族主义提升了国家在数据保护、数字经济和网络空间治理中的主导地位，可能驱使各国频繁诉诸竞争策略和安全化举措。第一，国家与政府提升了其在管制体系中的权威。当数字化发展面临地缘政治、国家安全和民族主义时，大型科技跨国公司就必须承受来自国家的政策管制与大国战略竞争导致的整体政治环境变迁。当前，大型科技公司陷入了“技术后冲/抵制”（techlash）处境，网络治理领域中的政府与市场的平衡态势被逐步打破，科技类跨国公司面临日益严重的质疑和敌意，民众不信任感与日俱增。[⑤] 有学者预测，2020 年全球性“技术后冲”将“从话语变为行动”，并将形成一种“暴徒心态”（mob mentality）。[⑥] 在此背景下，国家借助数据民族主

① Nicole Lindsey, “Cyber Governance Issues Take on High-Profile Status at the UN,” *CPO Magazine*, October 14, 2019, https://www.cpomagazine.com/cyber-security/cyber-governance-issues-take-on-high-profile-status-at-the-un/.

② Kyle L. Evanoff, “Cyber Governance: More Spam than Substance?” Council on Foreign Relations, June 14, 2019, https://www.cfr.org/blog/cyber-governance-more-spam-substance.

③ Arindrajit Basu, “India’s Role in Global Cyber Policy Formulation.”

④ 高望来：《金砖国家网络安全合作：进展与深化路径》，《国际问题研究》2017 年第 5 期，第 70—74 页。

⑤ Adrian Wooldridge, “The Coming Techlash,” *The Economist*, November 18, 2013, https://www.economist.com/news/2013/11/18/the-coming-tech-lash; and Eve Smith, “The Techlash against Amazon, Facebook, and Google–and What They Can Do,” *The Economist*, January 20, 2018, https://www.economist.com/briefing/2018/01/20/the-techlash-against-amazon-facebook-and-google-and-what-they-can-do.

⑥ Mark Scott, “In 2020, Global ‘Techlash’ Will Move from Words to Action,” *Politico*, December 31, 2019, https://www.politico.eu/article/tech-policy-competition-privacy-facebook-europe-techlash/; and Robert D. Atkinson, et al., “A Policymaker’s Guide to the ‘Techlash’ –What

义逐渐挤占企业的活动空间，并成为应对“科技后冲”问题的主导者，政府、市场、企业及个体之间的互动方式正在承受国家力量的重新塑造。[①] 企业所代表的市场力量日益边缘化，与此同时，国家的力量却越来越显著地塑造着一种竞争而非合作的数字化环境。[②]

第二，国家仍将继续采取安全化手段增强自身在数字领域中的话语权。制造安全理由与塑造敌对话语是国家在数字相关领域实施安全化手段的主要策略。[③] 例如，美国将数据保存与互联网监控、知识产权和大国竞争等议题结合，建构所谓包括中国在内的一些国家对其构成“威胁”，强调他国若在具体部门（如高科技部门）中掌握相关技术将冲击美国主导地位或干涉美国国内政治等，坚持认为所谓的“假想敌”国家（如俄罗斯和中国等）的相关政策可能会危及美国国家安全。[④] 对其他国家而言，诉诸数据民族主义或倡导数据主权本身就是对美国数据霸权的一种回应。[⑤] 在这种恶性循环中，国家行为体坚持其权威、强力和主权等支柱必然会扮演更为强大的角色；拥有超凡实力的跨国公司也需要在由各国建构的冲突性政策空间内找到自身的角色。[⑥] 有研究认为，在全球网络战中，大多数国家都遵循民族主义的逻辑，利用数字化技术来巩固国内权力并对外施展影响力。[⑦]

（四）对全球网络空间治理的影响

数据民族主义政策瓦解了网络空间治理体系的合作基础。第一，数据民族主义加剧了各国关于网络空间全球治理的政治张力，制约着全球网络空间治理和国际数据管理的制度建构。国际网络空间治理是全球治理中的重要议

It Is and Why It’s a Threat to Growth and Progress,” Information Technology and Innovation Foundation, October 28, 2019, https://itif.org/publications/2019/10/28/policymakers-guide-techlash.

① Sean McDonald and An Xiao Mina, “The War-Torn Web.”

② Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, p. 1.

③ Laura Fichtner, “What Kind of Cyber Security? The Rising Cyber Security and Mapping Approaches,” *Internet Policy Review*, Vol. 7, No. 2, 2018, pp. 1-19.

④ Greenberg Center for Geoeconomic Studies, “The Rise of Digital Protectionism: Insights From a CFR Workshop,” Council on Foreign Relations, October 18, 2017, https://www.cfr.org/report/rise-digital-protectionism; 美国近来受民族主义影响的外交转变可参见毛维准：《美国国际秩序观：特朗普冲击下的图景转向》，《南大亚太评论》2019 年第 2 辑，第 51—116 页。

⑤ 杜雁芸：《大数据时代国家数据主权问题研究》，第 1—14 页。

⑥ Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, p. 1.

⑦ Sean McDonald and An Xiao Mina, “The War-Torn Web.”

题。自 2015 年以来，网络空间全球治理进展缓慢，国际合作的紧迫性与全球协调缺乏并存。尽管各方呼吁合作，但是网络治理依然止步不前。[①] 据调查显示，多位智库学者将网络空间治理的挑战置于全球治理议题的第六位，将网络空间治理取得突破的可能性设定为 C 级，即全球网络领域已经分裂为多个不相容的体系，全球合作障碍很多，突破的可能性不大。其中，数据保护议题在全球网络空间治理中拥有最高优先度。[②]

第二，数据民族主义是国际合作的一种负面因素，其蔓延将使网络空间国际治理的合作困局雪上加霜。目前，联合国试图推动相应的数字合作倡议，但是，在这种“寒冰式的地缘政治环境”中，网络空间国际治理改善的可能性依然不大。有研究指出，网络空间治理虽有“纸面上的规范、原则和声明”，但是它们无法约束各国的行为。[③] 与此同时，各行为体之间的信任正在遭受侵蚀，因此不论是 2018 年的“巴黎倡议”还是安倍晋三在 2019 年 G20 大阪峰会上提出的“可信赖的数据自由流通”，都将信任置于显著位置。[④]

（五）数据民族主义的政策影响

政策是国际制度和全球治理体系发挥功能的主要工具，也是特定国际秩序得以具体化的重要载体。数据民族主义政策对国际秩序各维度的影响还会进一步传导到国际数据治理和网络空间治理的整体框架中。

第一，数据民族主义政策可能激发国际社会围绕数字经济和数据治理实施政策对冲和制度竞争。21 世纪贸易协议的一个重要合理性基础是寻找跨境监管的共识，但问题在于这种共识并不存在。[⑤] 数据民族主义突出了各国关注的“谁的规则”（Whose Rules）的问题，瓦解了数字治理的基础。特别是缺乏统一的全球标准将会进一步加剧数字治理的碎片化。[⑥] 在国内层

① Kyle L. Evanoff, “Cyber Governance: More Spam than Substance?”

② Council of Councils, “2019 Report Card on International Cooperation,” The Council on Foreign Relations, https://www.cfr.org/interactive/councilofcouncils/reportcard2019/#!/opportunities/2019.

③ Kyle L. Evanoff, “Cyber Governance: More Spam Than Substance?”

④ “Paris Call for Trust and Security in Cyberspace,” November 12, 2018, https://pariscall.international/en/.

⑤ [美]苏・阿里尔・阿伦森：《数字贸易失衡及其对互联网治理的影响》，第 67 页。

⑥ Stephanie Segal, “Whose Rules? The Quest for Digital Standards,” CSIS, February 22, 2019, https://www.csis.org/analysis/whose-rules-quest -digital-standards.

面，数据本地化和数据全球化两股政策潮流已经在各国的立法管辖权竞合平台上“狼烟四起”。[①] 在国际层面，中、美、俄、欧、印等大国和地区之间在数字治理方面依然无法跨越规则鸿沟而陷入长期博弈，尽管国际社会急需数字空间中更为统一的规则、标准和规范框架。[②]

第二，不同国家针对数字经济监管提出的相关政策倡议不仅没有融合，反而加剧了数字治理体系中的冲突与摩擦。[③] 例如，金砖国家与西方世界在网络空间、数字经济和数据治理方面存在巨大政策分歧；即使是各自小集团内部也存在明显不同步的现象。[④] 又如，G20 大阪峰会提出跨境数据流动的“大阪轨道”（Osaka Track），试图规范数据流通，提供全球通用的数字经济规则，但是印度基于民族主义情绪和国家财富的考虑并未在《大阪数字经济联合宣言》上签字。[⑤] 即使是盟友关系的西方国家，其数据保护偏好也大相径庭。例如，美国在 TTIP 和 TPP 中与欧盟、澳大利亚、新西兰和加拿大等在跨境数据流动规则方面存在不同意见。[⑥]

第三，数据民族主义的扩散也影响着其他相关部门的规则制定。作为一种“多维度建构”[⑦]，数据本地化等政策一方面影响经济、贸易、知识产权

① 王志安：《云计算和大数据时代的国家立法管辖权——数据本地化与数据全球化的大对抗？》，第 20 页。

② Matthew P. Goodman, “Time to Align on Digital Governance,” Center for Strategic and International Studies, January 24, 2020, https://www.csis.org/analysis/time-align-digital-governance.

③ Dan Ciuriak, “From Digital Trade Wars to Governance Solutions: The G20 and the Digitally Enabled Economy,” International Centre for Trade and Sustainable Development, August 28, 2018, https://www.ictsd.org/opinion/from-digital-trade-wars-to-governance-solutions-the-g20-and-the-digitally-enabled.

④ Arindrajit Basu, “The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam.”

⑤ Rohan Seth, “What Does Refusal to Sign the Osaka Track Mean for India?” *Asian Age*, October 16, 2019, https://www.asianage.com/opinion/oped/161019/what-does-refusal-to-sign-the-osaka-track-mean-for-india.html; and Daniel Hurst, “Did Japan Get What It Wanted from the Osaka G20 Summit?” *The Diplomat*, July 1, 2019, https://thediplomat.com/2019/07/did-japan-get-what-it-wanted-from-the-osaka-g20-summit/.

⑥ 参见陈咏梅、张姣：《跨境数据流动国际规制新发展：困境与前路》，第 41 页；John Selby, “Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?” pp. 213-232.

⑦ William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, *Internet Fragmentation: An Overview*, Future of the Internet Initiative White Paper, World Economic Forum, January 2016, p. 41.

和技术等不同领域，另一方面则与政治、社会与人权等议题密切相关。[①] 数据民族主义的蔓延必然会推动其他部门和议题的相关规则重构。例如，国际社会特别关注数据存储等本土化贸易壁垒（LBTs）问题，它涉及 WTO 规则调整、多边和双边贸易协定修订与全球制度改革等各种问题。[②] 此外，人权理由也经常被不同国家或集团置于数据保护的基本价值之上。[③] 数据民族主义政策会影响特定国家的人权考量，并可能影响国际人权法的实践。[④] 2018 年《世界贸易报告》在谈及隐私保护和跨境数据流通时特别强调，数据保护政策应该与国际人权法所规定的义务相一致。[⑤]

第四，大国竞争烈度的提升和主权国家主导地位的上升都会冲击国际制度的建构，阻碍网络空间国际治理取得进展。在数据民族主义政策大行其道的背景下，权力政治思维势必阻碍各主体在网络空间负责任管理方面取得进展。[⑥] 大国竞争的结构性因素逐渐瓦解了各国达成共识的政治意愿，没有哪个大国愿意被限制追求“认知中的技术优势”。[⑦] 网络空间国际治理可能陷入僵局。然而，只有当所有大国都参与并接受其主要条款时，网络空间国际治理机制才能有效运作。[⑧] 因此，有研究机构悲观地断言，数字监管的国际协议依然遥遥无期。[⑨]

---

① Matthew P. Goodman, “Time to Align on Digital Governance”; and Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, *Localization Barriers to Trade: Threat to the Global Innovation Economy*, The Information Technology and Innovation Foundation, September 2013.

② Stephen J. Ezell, et al., *Localization Barriers to Trade: Threat to the Global Innovation Economy*, pp. 68-75.

③ UNCTAD, The Ad Hoc Expert Meeting on Data Protection and Privacy: Implications for Trade and Development,” Geneva, April 19-20, 2016, https://unctad.org/meetings/en/SessionalDocuments/dtl_eweek2016_EMreport_en.pdf.

④ Christopher Kuner, “Data Nationalism and Its Discontents,” p. 2098.

⑤ *World Trade Report 2018*, World Trade Organization, 2018, p. 174.

⑥ Harriet Moynihan, “Power Politics Could Impede Progress on Responsible Regulation of Cyberspace,” Chatham House, December 3, 2019, https://www.chathamhouse.org/expert/comment/power-politics-could-impede-progress-responsible-regulation-cyberspace.

⑦ Camino Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* Carnegie Endowment for International Peace, August 2019, p. 37.

⑧ Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov, “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms,” Council on Foreign Relations, February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

⑨ Paul Laudicina, et al., *Competing in an Age of Digital Disorder*, p. 1.

结 束 语

数据民族主义在其多重逻辑的驱动下对当前国际秩序造成了较大影响，也对中国参与国际数据治理和网络空间国际治理提供了若干启示。

首先，数据民族主义是一种长期且具有合理性的民族主义。它是各国为因应大国竞争加剧、全球化逆转、数据资源战略性和美国技术霸权而作出的合理反应，也是一种具有某种时代特征且可能长期存在的客观政治现象。我们应在认识其合理性的基础上，立足当前潮流，制定适应本国发展需要的数据本地化政策，并在国际舞台上与伙伴国家一道反击美国的数据霸权。全球数据治理不应陷入“一家独大”的局面，各个国家的数据主权与自主性理应得到尊重，基于此，中国的相关数据本土化政策需要在自身能力、文化价值和目标利益之间找到平衡点。

其次，数据民族主义是一种需要加以约束的民族主义。它直接冲击当前的跨境数据流动，影响全球数字经济和贸易的顺利开展，并妨碍国际数字贸易制度的建构。作为数字经济大国，中国应采取切实措施降低其他各国数据民族主义政策对自身跨境数据治理与数字经济带来的负面影响，避免其他国家将中国视为敌对目标，积极以人类命运共同体理念和网络主权框架原则推进国际数字贸易制度和网络空间国际治理体系的建构，同时，也要防止个别国家利用极端数据民族主义危害中国利益。

最后，数据民族主义也是一种亟须治理的民族主义。它是政治逻辑嵌入数字经济领域并针对数据全球化做出的一种集中回应，更是民族主义意识形态在数字领域中的逻辑延伸。面对大国竞争结构下的数据全球化与本地化之间的张力，包括中国在内的国际社会各利益相关方应该积极承担国际责任，以负责任的态度约束各自的民族主义情绪，推行负责任的数据民族主义，既要认识其合理性，又要超越意识形态之争，推动国际数据治理取得进展。

[责任编辑：石晨霞]