论数据本地化全球趋势下的中国应对

卓力雄*

（中共中央党校政治与法律部，北京，100091）

摘 要：目前，世界各国正在悄然掀起一场争夺“数据”的“战争”，数据本地化逐渐成为一种国际趋势。数据本地化的支持者提出了他们的理由，反对者则针锋相对地进行了批驳，认为这些理由难以成立，数据本地化还有可能造成适得其反的结果。我国目前也加入了数据本地化的队伍之中。对于我国的数据本地化，我们需要分别看待，数据本地化短期带来一些有利结果，但长期而言，可能造成很多负面影响。为了打破数据“割据”，促进数据的自由流动，我国应当逐步减少数据本地化，并加强数据跨境流动的国际合作，推动关于数据流动国际条约的签订和支持相关国际数据保护组织的成立。

关键词：数据本地化，数据跨境流动，个人数据，数据主权

数据自由流动对世界贸易、世界经济的巨大推动作用已成共识。据麦肯锡研究，2015年的跨境数据流动所产生的经济价值首次超过了传统的商品贸易流动。[①]据预测，2020年跨境电子商务将拥有10亿消费者，年销售总额达1万亿美元。[②]毫无疑问，数据是现代全球经济的命脉。[③]数据的重要性与其重要价值正在飙升，数据的自由流动所带来的价值正日益显现。然而，在数据自由流动迅猛发展的同时，世界各国却在悄然掀起一场争夺数据的“战争”，限制数据跨境流动与实现数据的本地化逐渐成为一种国际趋势。

为何如此众多的国家纷纷采取数据本地化措施？其背后的原因何在？本地化措施能否解决支持者所担忧的问题，实现其预设目标？我国目前也采取了数据本地化的举措，其背后的考量是否与其他国家相似？是否存在独特的因素？数据本地化措施对我国的影响可能有哪些？为了打破数据“割据”，让数据更加自由地跨境流动，从而推动我国和世界经济的发展，我国应当如何应对？

对于以上问题，本文将在已有文献的基础上进行深入的分析与探讨。本文将对世界各国目前采取的数据本地化的措施作一个相对详细的介绍。在此基础上，本文将结合数据本地化支持者与反对者的意见，指出数据本地化措施不仅难以解决支持者所担忧的问题和实现预期目标，还带来更大的负面影响。不过，我国在采取数据本地化措施时，却因为一些独有的因素，使得我国的数据本地化措施带来的影响具有多样性。为了更好地赢得数据经济发展的主动权，我国应当逐步减少数据本地化的适用范围，主动加强数据跨境流动的国际合作，推动关于数据流动国际条约的签订。

一、数据本地化：日益扩大的国际趋势

数据本地化（Data Localization），目前并没有统一的学术定义，通常指一种要求在特

*本文是国家留学基金委支持项目。

卓力雄（1991-），男，广东湛江人，中共中央党校法学博士生，美国波士顿大学法学院联合培养博士。

特别感谢 Michael J Meurer 教授、Ken Mortensen 教授对本文所给予的宝贵意见和建议。

① McKinsey Global Institute: Digital globalization: The new era of global flows, March 2016, p.3

② Susan Lund; Laura Tyson, Globalization Is Not in Retreat: Digital Technology and the Future of Trade, 97 Foreign Aff. 132-133 (2018)

③ NIGEL CORY, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? information technology&innovation foundation, MAY 2017, p.1

定管辖区内储存在该管辖区域内收集的数据的公共政策措施。④换言之，数据本地化指相关组织应当将其在本地收集的数据储存于本地的一种法律或者政策规定。数据本地化有狭义与广义之分。狭义的数据本地化仅指明确的规定要求相关组织在当地收集的数据只能储存于该区域，广义的数据本地化还包括各种对数据跨境流动所采取的相关限制规定和措施。本文根据数据本地化狭义和广义的划分，将世界各国（地区）的数据本地化措施分为两类：一种是明确地规定要求本国（地区）收集的数据只能储存于本国（地区）境内。这种数据本地化措施具体又可以细分为两种：全部的数据本地化和部分的数据本地化。前者指所有在本国（地区）境内收集的数据都必须储存于该国（地区），后者指只要求某部分或某类在本国（地区）收集的数据储存于该国（地区）。另外一种是对相关数据的跨境流动作了一定的限制，只有符合相关法律规定时数据才能跨境流动。目前，无论是发达国家还是发展中国家，都有不少国家采取相应的数据本地化措施，这些国家遍布世界五大洲。

第一，全部明确要求本国（地区）收集的数据只能储存在本国（地区）境内。这一类的数据本地化国家主要有俄罗斯、哈萨克斯坦、越南、尼日利亚等。俄罗斯是世界上最先实施最为广泛的数据本地化措施的国家之一。俄罗斯于 2014 年先后批准的第 97-FZ 号联邦法（“在线内容法”）和第 242-FZ 号联邦法（“数据本地化法”）两部法律，对个人数据本地化提出了广泛的要求，尤其是第 242-FZ 号联邦法明确规定，任何关于俄罗斯联邦公民个人数据的记录、系统化、聚集、储存、调整（更新、修改）与提取的运营设备都必须位于俄罗斯境内，而且这些数据库的运营商必须披露其数据中心的地理位置。⑤此外，俄罗斯总统普京于 2016 年 7 月 1 日签署的第 374-FZ 号联邦法要求所有的通信运营商和互联网提供者都要将其收集的所有数据储存于俄罗斯境内，储存时间从 6 个月到 3 年不等。⑥哈萨克斯坦自 2005 年就开始要求所有使用哈萨克斯坦顶级域名 “.kz”的网站将其全部数据储存于该国。⑦2015 年 11 月，哈萨克斯坦对 2013 年颁布的《关于个人数据及其保护》法律进行修订，出台了新的《关于哈萨克斯坦共和国某些立法法案有关信息化问题的修正案》，并于 2016 年 1 月 1 日生效。该修正案第 12 条对个人数据的储存作出明确的规定，要求所有储存个人数据的数据库应当放在哈萨克斯坦境内，个人数据本地化的要求适用于哈萨克斯坦境内设立的公司、个体经营者和外国公司的分支机构和代表处。⑧越南于 2013 年 9 月生效的《关于互联网服务和在线信息内容的管理、提供和使用的法令》（第 72 号法令）要求所有国内和国外的互联网运营公司都至少设置一台服务器于越南境内，2016 年关于第 72 号法令的修订草案要求所有互联网服务提供商在本地储存数据。⑨尼日利亚于 2013 年 12 月 3 日颁布的《尼日利亚信息和通信技术内容发展指南》对数据本地化作了很详细的规定。根据该指南，所有的尼日利亚信息和通信技术公司都应当在该指南生效后 18 个月内使用本

④ Bret Cohen; Britanie Hall; Charlie Wood, Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy, 32 Antitrust 107 (2017)

⑤ See Mihaylova, Iva, Could the Recently Enacted Data Localization Requirements in Russia Backfire? (July 11, 2015). U. of St. Gallen Law & Economics Working Paper No. 2015-07, p.4-6; Anupam Chander; Uyen P. Le, Data Nationalism, 64 Emory J. 701-702 (2015); Bret Cohen; Britanie Hall; Charlie Wood, Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy, 32 Antitrust 110 (2017)

⑥ Ksenia Koroleva, “Yarovaya” Law - New Data Retention Obligations for Telecom Providers and Arrangers in Russia, Legislative & Regulatory Developments, Privacy, Security, July 29, 2016. Available at https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/

⑦ FREEDOM HOUSE, FREEDOM ON THE NET 2013: A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA 441 (Sanja Kelly et al. eds., 2013), Available at https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf

⑧ Rhiannon Webster, Kazakhstan: Localization of personal data, 1 January 2016. Available at https://www.dacbeachcroft.com/en/articles/2016/january/kazakhstan-localization-of-personal-data/

⑨ See Bret Cohen; Britanie Hall; Charlie Wood, Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy, 32 Antitrust 111-112 (2017); NIGEL CORY, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? information technology&innovation foundation, MAY 2017, p.30

地制造的 SIM 卡提供数据和电话服务，在尼日利亚境内储存所有订户和消费者数据；所有数据和信息管理公司都必须在国内储存所有政府数据。⑩

第二，部分要求本国（地区）收集的数据储存于本国（地区）境内。这类国家和地区主要有澳大利亚、加拿大、印度、印度尼西亚等。澳大利亚总体上不限制数据的跨境流动，但要求个人数据的跨境流动不得违反澳大利亚的隐私原则（Australian Privacy Principles），否则将禁止相关数据的跨境流动。⑪另外，澳大利亚 2012 年颁布的《个人控制的电子健康记录法》第 77 条明确禁止在澳大利亚境外处理能够识别出个人或实体的健康记录数据，⑫这实质上是要求所有的健康相关数据只能储存于澳大利亚境内。加拿大没有全国性的限制数据跨境流动的法律，但有两个省立法明确要求相关数据必须储存在加拿大境内。不列颠哥伦比亚省 1996 年颁布的《信息自由和隐私保护法》第 30.1 条明确规定所有公共机构保管或控制的个人数据只能保存在加拿大境内，除非存在符合法律规定的例外情况。⑬同样，新斯科舍省于 2006 年颁布、2010 年修正的《个人信息国际披露保护法》第 5 条也明确规定，公共机构及相关服务提供者必须确保其保管或控制的个人数据保存在加拿大境内。⑭印度国家安全委员会于 2014 年 2 月提出一项政策，要求所有电子邮件提供商建立本地服务器，希望与印度两个用户之间的通信相关的所有数据都保留在国内。⑮印度中央银行于 2018 年 10 月 15 日强制要求所有与支付系统相关的实体，如支付系统提供商及其服务提供商、中介机构、第三方供应商和支付生态系统中的其他实体，都要将其所有相关的数据储存在印度本地的系统中。⑯印度尼西亚于 2012 年颁布的第 82 号法令《关于电子系统和交易操作的法令》对数据本地化作出了明确规定，根据该法令第 17 条（2）款规定，电子系统公共服务的运营商应当将数据中心和灾难恢复中心置于印度尼西亚境内，根据第 43 条规定，所有在印尼境内进行的电子交易都应当将其数据储存于印尼境内。⑰

第三，没有明确要求数据本地化，但对相关数据的跨境流动作了相应的限制，符合规定的数据才可以跨境流动。这一类的国家和地区主要有欧盟、阿根廷、日本、台湾等。欧盟总体上没有实施数据本地化的措施，但其 2016 年生效、2018 年全面实施的《一般数据保护条例》却对个人数据转移到第三国或国际组织作了许多限制，这些规定适用于所有欧盟成员国。根据《一般数据保护条例》第五章第 44 条至第 50 条的相关规定，将欧盟境内的个人数据转移到欧盟境外的第三国或国际组织时，只有在欧盟委员会认定相关的第三国或国际组织能够提供充分的保护时，这些数据才可以自由跨境转移；或者存在第 49 条所规定的数据主体同意、履行合同、实现数据主体利益、为了公共利益、进行法律辩护、保护数据主体关键利益或者根据登记册进行的七种条件之一才可以进行转移。⑱阿根廷对数据

⑩ Nigerian Federal Ministry of Communication Technology, Guidelines for Nigerian Content Development in Information and Communication Technology(2013), p.12,16 Available at https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf

⑪ DATA PROTECTION LAWS OF THE WORLD(Full Handbook), 28 January 2019, p.39 Available at https://www.dlapiperdataprotection.com/index.html

⑫ Personally Controlled Electronic Health Records Act 2012 (Cth) s 77 (Austl.)

⑬ FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT 1996(Canadian) s30.1

⑭ the Personal Information International Disclosure Protection Act. 2006, c. 3, s. 1.

⑮ Thomas K Thomas, National Security Council proposes 3-pronged plan to protect Internet users, businessline, February 13, 2014. Available at https://www.thehindubusinessline.com/info-tech/National-Security-Council-proposes-3-pronged-plan-to-protect-Internet-users/article20727012.ece

⑯ DATA PROTECTION LAWS OF THE WORLD(Full Handbook), 28 January 2019, p.346 Available at https://www.dlapiperdataprotection.com/index.html

⑰ REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA NUMBER 82 OF 2012 CONCERNING ELECTRONIC SYSTEM AND TRANSACTION OPERATION, Art.17,43. Available at http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html

⑱ See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p.60-65

跨境流动也实施一定的限制。根据阿根廷《个人数据保护法》规定，阿根廷禁止向那些没有对数据提供充分保护的国家或国际组织转移，除非数据主体同意、为了国际司法合作、作为某些医疗数据交换的条件、银行或证券交易所转账、履行国际条约义务或进行国际合作。⑲日本同样对个人数据转移作了一定限制。根据日本于 2017 年修正的《个人信息保护法》规定，只有数据接收方所在国提供与该法类似的隐私保护或者是该法规定的白名单国家时，这些个人数据才能够进行跨境转移。⑳我国台湾地区总体上不限制数据的跨境流动，但禁止一些数据的跨境流动。2015 年 12 月 30 日修正的《个人资料保护法》第 21 条明确规定当数据涉及国家重大利益，或国际条约或协议有规定，保护不足或通过外国转移来规避台湾法律时，这些数据都不得进行跨境流动。[21]

除了以上这些国家和地区，世界上还有英国、巴西、哥伦比亚、泰国、中国（详见本文第三部分）、中国香港等众多国家和地区都采取了或多或少的数据本地化措施，数据本地化呈现出日益扩大化的国际趋势。

二、关于数据本地化的争论

数据自由流动所带来的价值不言而喻，可为何世界上如此众多的国家和地区都不约而同地采取各种形式的数据本地化措施？为了回答这一问题，我们需要深入分析数据本地化的支持和反对观点。

1. 支持理由

这些国家实施数据本地化的理由很多。第一点理由在于数据本地化措施是为了保护个人隐私和国家网络安全不被侵犯。在他们看来，随着互联网越来越深入地融入我们的生活，我们面临的来自黑客、犯罪组织或者他国政府网络监视、盗取个人数据的风险在极大增加。为了更好地保护公民个人隐私，实施数据本地化是被迫之举。他们相信，通过将这些数据储存于本国（地区）内，尤其是将一些与公民健康或财务相关的敏感数据储存于本地，就会减少被外国黑客和网络犯罪组织的攻击机会，从而保护个人数据。上文提及的澳大利亚、加拿大、印度等就是典型例子。同时，国家安全是这些国家限制数据跨境转移的共同理由。[22]斯诺登揭露的美国全球监视行为让不少国家感到愤怒，通过限制本国数据跨境转移成为他们对美国监视行为的回应。[23]例如，“斯诺登事件”后，欧盟废止了与美国的“安全港框架协议”（EU-U.S. Safe Harbor Framework），转而签订对个人数据保护要求更为严格的“隐私盾协议”（EU-U.S. Privacy Shield Framework），欧盟还在 2016 年通过的《一般数据保护条例》中严格限制个人数据的跨境转移。俄罗斯、越南等国更是把数据本地化作为维护国家网络安全的重要手段，他们希望通过实施全面的数据本地化措施，将所有境内收集的数据保留在本国来减少被外国监视和攻击的机会。

支持数据本地化的第二点理由在于数据本地化能够促进本地经济发展。众所周知，随着大数据时代的到来，数据的价值越来越重要，被称为未来社会的“新石油”。谁能掌握更多的数据，谁就能从数据经济中获取更大利益。借助数据本地化来减少本国数据被他国拥有，从而拥有更多的数据经济发展机会，掌握数据经济发展的主动权成为这些国家的预设目标。这种通过数据本地化措施来刺激地方和国家经济发展的愿望很好理解。[24]毕竟，

⑲ DATA PROTECTION LAWS OF THE WORLD(Full Handbook), 28 January 2019, p.33 Available at https://www.dlapiperdataprotection.com/index.html

⑳ Ib. At 389.

21 《个人资料保护法》（台湾）第 21 条，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=I0050021

22 Andrew D. Mitchell; Jarrod Hepburn, Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer, 19 Yale J.L. & Tech. 188 (2017)

23 Anupam Chander; Uyen P. Le, Data Nationalism, 64 Emory J. 714 (2015)

24 SJS, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION,

数据本地化措施使得许多跨国公司只能将与数据相关的工作转移到他们国家，而且，每个数据中心的建设成本都不菲，新增的数据中心建设意味着新增的投资和工作岗位。这些新增的投资、技术和工作岗位都会直接或间接地推动本国数字经济的发展。另外，这种类似于关税保护政策的数据本地化措施，增加了跨国公司的运营成本并提高了他们的进入门槛，这还会间接为本国数据企业的发展和国际竞争提供机会，给本国数字经济的发展赢得更多优势。尼日利亚、印度、印度尼西亚等国通过数据本地化措施来促进本国经济发展就是典型例证。

支持数据本地化的第三点理由在于数据本地化有利于本国法律和政策的有效执行。在他们看来，如果没有数据本地化措施，当本国境内发生严重的威胁公共安全、恐怖袭击或者刑事案件时，政府部门可能很难获得关键的电子数据。例如，当印度警方在侦查一个刑事谋杀案或者恐怖袭击案时发现嫌疑人的 Gmail 和 Facebook 账户可能存在重要的证据线索，警方与谷歌或者 Facebook 联系希望他们能够让警方访问相关数据时，他们很有可能会以其为美国注册的公司，他们的数据储存在美国总部，只有美国政府才有权要求他们提供相关数据为由进行拒绝。这意味着印度官员在执行本国法律时也得向美国寻求帮助才能够获得关键证据。[25]这给相关国家打击犯罪、执行法律带来很大麻烦。然而，如果实施了数据本地化政策，他们就直接可以根据本国法律对相关数据进行访问，不存在法律执行障碍的问题。另外，数据本地化还能够防止一些违反本国道德或公共政策的互联网内容的传播。如纳粹纪念品、色情作品、宣传赌博、违反本国宗教政策等相关内容可能因为违反本国公共道德或政策而被限制在本国的存在。[26]

2. 反对理由

然而，在反对者看来，数据本地化支持者所提出的三点理由都难以成立。

首先，数据本地化保护个人隐私和国家安全的理由根本难以成立。数据本地化不仅不能保护个人隐私还可能导致个人隐私遭受更大的泄露和侵犯。原因在于两方面：一是实施数据本地化政策的国家很可能缺乏相应的安全设施和技术人才，或者其数据保护的安全标准相对较低，这使得保存在本地的数据更容易受到黑客攻击。印度尼西亚作为实施数据本地化政策的国家，因长期缺乏对网络基础设施的投资，使得该国成为世界上黑客攻击最为严重的地方，被戏称为“网络犯罪的避风港”。[27]越南光 2013 年就有超过 2045 个网站被攻击，却缺乏足够的网络安全专家来应对这些问题。[28]二是数据本地化加大了数据丢失的风险和本国政府监视的可能。数据高度集中储存于某个地方所面临的风险远高于分散储存于不同地方。数据集中储存于某个地方，一旦出现自然灾害等各种问题，将很有可能导致数据的永久丢失，而分散储存于不同地方，还有机会复原。另外，数据本地化还为本地政府监视本国公民提供了便利。通过数据本地化，当地政府能够根据自己的法律和程序访问受欢迎的数据而不必担心受到其他国家的制约。[29]这使得公民所有的网络活动都将置于本国政府的监视之下，公民很难在政府面前保持相应的隐私和自由，政府很有可能利用所掌握的信息来实现政治压迫和侵犯公民个人权利，[30]尤其是对一些专制或者威权政府而言，数

Albright Stonebridge Group, September28, 2015 Available at https://www.albrightstonebridge.com/news/data-localization-challenge-global-commerce-and-free-flow-information

25 See Andrew Keane Woods, Against Data Exceptionalism, 68 Stan. L. Rev. 746 (2016)

26 Meltzer, Joshua, The Internet, Cross-Border Data Flows and International Trade (December 17, 2014). Asia & the Pacific Policy Studies (APPS), 2014, p.8 Available at SSRN: https://ssrn.com/abstract=2546110

27 Andrea Huspeni, Think China is the No. 1 Country for Hacking? Think Again. ENTREPRENEUR, October 16, 2013 Available at https://www.entrepreneur.com/article/229474

28 HA NOI, VN at risk over lack of cyber-security,Viet Nam News, October, 30, 2013 Available at https://vietnamnews.vn/economy/246923/vn-at-risk-over-lack-of-cyber-security.html#RPWA91QjmfXLLuAv.97

29 Jennifer Daskal, Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues, 8 J. Nat'l Sec. L. & Pol'y 477 (2016)

30 Erica Fraser, Data Localisation and the Balkanisation of the Internet, 13 SCRIPTed 366 (2016)

据本地化给他们监视本国民众，维护自身统治提供了难得的机会，公民在政府面前更难以拥有个人隐私。同时，数据本地化不太可能限制其他国家开展国外监视活动的能力。[31]其实，美国等国家进行的国外监视活动与数据储存的地理位置没有太大关系，与数据储存的安全技术有关。单纯改变数据的储存位置并不会减少这些监视行为。相反，数据本地化实际上可能有助于外国监视。[32]数据本地化使得一国的数据更加集中，尤其是一些数据保护技术水平较低的国家，其集中的数据实际上让外国情报机构能够更加集中地监视该国公民。

其次，数据本地化不仅不能促进经济发展，还可能给本国经济发展带来负面影响。根据一些学者研究，数据本地化对本国经济增长总体有着明显的负面效果，全面数据本地化将使巴西的 GDP 下降 0.8%，中国、韩国和欧盟的 GDP 下降 1.1%，印度下降 0.8%，印度尼西亚下降 0.7%，越南下降 1.7%。[33]数据本地化对经济的阻碍主要表现在以下几点：一是数据中心建设所创造的就业岗位和税收十分有限，但其带来的经济成本却远超其预期收益。例如，苹果在美国北卡罗来纳州梅登小镇建造的价值 10 亿美元的大型数据中心仅需 50 个操作人员。[34]而数据中心建设所需的服务器和其他硬件基本上需要向美国等互联网技术强国进口，并不会对本地经济有太大帮助，数据中心建成后所消耗的电力资源和维护成本都是很大的负担。二是会增加企业成本，导致用户费用增加或服务减少。[35]昂贵的数据中心建设给数据企业带来不小的经济成本，企业运营成本增加的结果只会是消费者负担增加或者享受的服务变少。毕竟，羊毛总是出在羊身上。三是不利于本国企业参与国际经济和国际竞争。俄罗斯实施数据本地化后，已经对俄罗斯的一些企业参与国际经济带来了负面影响，如导致俄罗斯航空公司与外国售票公司合作的终止等。[36]实施数据本地化的国家很可能遭到他国报复，当本国企业与他国进行贸易时，很容易受到相对应的限制，不利于本国企业参与国际竞争。尤其在大数据技术迅猛发展的当今，数据本地化容易导致本地企业错失利用全球互联网平台参与国际贸易与创新的机会。

最后，法律执行的问题不需要数据本地化也能解决。诚然，数据本地化能够减少国内法律执行障碍的问题。但是，不用通过数据本地化也一样达到这一目的。众所周知，需要通过访问数据来执行的法律问题绝大多数情况都属于刑法问题，而且属于比较严重的刑事犯罪问题。目前对于严重的刑事犯罪的法律执行问题，世界各国基本上都已经有相关的双边协议或多边协议，借鉴目前世界各国存在的司法互助多边协议与双边协议，相关国家完全可以通过多边或者双边协议来解决政府在特殊情况下访问数据以执行国内法律的问题，完全没必要通过数据本地化来解决。在有其他可行的解决方法的情况下，这种会带来许多负面影响的数据本地化措施明显是一种不理智的选择。

3. 支持理由与反对理由的再分析

根据反对者的理由，不难发现，数据本地化措施的理由很难成立。进一步分析就会发现，数据本地化措施若不断扩大，还会造成两个不利后果：一是在全球层面阻碍数据的自由流动和技术进步。众所周知，数据的价值在于流动，全球层面数据流动创造的价值和带

31 Erica Fraser, Data Localisation and the Balkanisation of the Internet, 13 SCRIPTed 364 (2016)
32 Anupam Chander; Uyen P. Le, Data Nationalism, 64 Emory J. 717 (2015)
33 Bauer, Matthias; Lee-Makiyama, Hosuk; Van der Marel, Erik; Verschelde, Bert (2014) : The costs of data localisation: Friendly fire on economic recovery, ECIPE Occasional Paper, No. 3/2014, p.2 European Centre for International Political Economy (ECIPE)
34 Rosenwald, Michael, Cloud centers bring high-tech flash but not many jobs to beaten-down towns, Washington Post. November 24, 2011. http://www.washingtonpost.com/business/economy/cloud-centers-bring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_print.html
35 Andrew Keane Woods, Against Data Exceptionalism, 68 Stan. L. Rev. 752-753 (2016)
36 Mihaylova, Iva, Could the Recently Enacted Data Localization Requirements in Russia Backfire? (July 11, 2015). U. of St. Gallen Law & Economics Working Paper No. 2015-07, p.12 Available at SSRN: https://ssrn.com/abstract=2629533

来的技术进步是难以想象的，尤其是大数据技术、云计算技术运用所引发的创新将很有可能引发新一代技术革命。在全球经济发展低迷的情况下，新一代技术革命对全球经济发展的重要性不言而喻。然而，新一代技术革命的前提是要有足够多的数据关联和对这些数据的自由获取和利用。不断扩大的数据本地化措施会导致全球数据遭到人为的分割，给全世界的数据自由流动带来障碍。二是使得互联网走向分裂，最后导致互联网络的中断。[37]互联网的本质是开放和全球共享，但数据本地化措施很可能像贸易保护主义阻碍全球贸易一样阻碍全球互联网的连通，导致互联网的分割与全球互联网的瓦解。不难理解，在全球各国人员、资本、货物、数据等高度互联互通的情况下，数据本地化这种本质上的保护主义政策是一种开历史倒车，最终结果就是全球经济的整体倒退。

数据本地化可能导致的后果之严重，难道这些实施数据本地化措施的国家没有考虑？那为什么依旧有如此多国家采取数据本地化措施？对此，我们不能仅分析数据本地化的利弊，而应该从更高的维度来分析这些国家实施数据本地化的真实意图。

其实，数据本地化政策背后存在着复杂的国际博弈。通过对这些实施数据本地化的国家进行分析，可以看出一个明显的特征：实施数据本地化的发展中国家，如印度、印度尼西亚、越南、尼日利亚等都是人口大国，而且都是经济发展比较迅速的国家。这些发展中国家希望借助数据本地化政策扩大其在全球市场的影响力，[38]提升其在互联网领域的话语权。他们相信这一措施能够为本国带来一定的竞争优势。退一步讲，即使这一措施不能提升本国的影响力，还可能带来一定的负面影响，但是，这一措施是对美国互联网技术优势形成的“互联网霸权”的一种主权宣誓。根据传统主权理论，主权国家有权对其境内的人、事、物行使主权，他们理应对本国境内的数据流动具有管辖权。然而，互联网的发展，尤其是全球互联网技术的迅猛发展，给这些国家的主权行使带来很大的挑战。美国因为其绝对的互联网技术优势，使得世界上大多数国家绝大多数最受欢迎的互联网服务和提供服务的人员、规则都来自美国。虽然说互联网是全球互联网，但适用规则却仅有一个，那就是美国的规则。[39]在这种情况下，许多国家发现他们难以管控其境内互联网上的信息、数据的流动，对互联网缺乏话语权和管辖权，美国还经常利用其技术优势对他们“指手画脚”。通过数据本地化，让互联网上的数据储存于本国境内，使其置于本国的主权管辖之内，借此表明，作为主权国家，本国有权对发生于境内的数据流动进行规制，全球互联网并非仅有“美国规则”。

三、数据本地化的中国实践与考量

目前，中国也实施了相应的数据本地化措施。2011 年，中国人民银行发布的《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第 6 条规定，“在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。”[40]2014 年，国家卫计委发布的《人口健康信息管理办法（试行）》第 10 条规定，“不得将人口健康信息在境外的服务器中储存，不得托管、租赁在境外的服务器。”[41]2016 年，国家新闻出版广电总局、工业和信息化部联合发布的《网络出版服务管理规定》第 8 条（3）款规定，图书、音

37 Mishra, Neha, Data Localization Laws in a Digital World: Data Protection or Data Protectionism? The Public Sphere, 144(2016)

38 Ib. At 147

39 Woods, Andrew Keane, Litigating Data Sovereignty, Yale Law Journal, Vol. 128, p.39,37, 2018

40 《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》，见国务院公报网址 http://www.gov.cn/gongbao/content/2011/content_1918924.htm

41 国家卫生计生委关于印发《人口健康信息管理办法（试行）》的通知，见卫健委网址 http://www.nhc.gov.cn/guihuaxxs/s10741/201405/783ec8adebc6422bbebdf79db3868d0b.shtml

像、电子、报纸、期刊出版单位从事网络出版服务的，“其相关服务器和储存设备必须存放在中华人民共和国境内。”[42]2016 年，全国人民代表大会常务委员会通过的《中华人民共和国网络安全法》第 37 条规定，“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储存。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”。[43]对我国数据本地化措施的相关法律法规的梳理，可以清晰看到，我国的数据本地化措施呈不断扩大的趋势，从最开始的个人金融信息、健康信息到最后所有的关键信息基础设施的运营者在境内收集的个人信息（数据）和重要数据都应当储存于境内。

我国独有的因素使得我国的数据本地化措施相对其他国家，显得更为特别，也使得我国有足够的动力去推动数据本地化。上文曾提及，反对者认为数据本地化措施并不能保护个人隐私和国家安全、不利于经济发展。然而，中国的数据本地化措施却很有可能不存在这个问题。原因在于以下几点：

首先，中国互联网的迅猛发展，为数据本地储存的安全保障提供了坚实的技术基础。众所周知，因为“防火墙”的存在，美国互联网企业一直难以进入中国市场，这给中国的互联网企业发展提供了宝贵的机遇。经过这些年的发展，中国已经发展成为仅次于美国的互联网技术强国，在全球互联网领域已是一个不容忽视的存在。[44]中国强大的技术和人才保障储存于本地的数据不会轻易受到黑客的攻击和外国的监视。

其次，中国互联网企业绝大多数总部和数据中心都在中国，其绝大多数用户也都在中国，这决定了这些企业将在本地收集的数据储存于本地是一种逻辑必然。不同于谷歌、Facebook 这些跨国企业的用户遍布全世界，个人数据的本地化不会给中国的互联网企业带来过多的额外成本，而会对在中国提供服务的跨国企业（如苹果公司）带来额外成本，这反而给中国本地企业提供更多竞争优势。

再次，中国大陆巨大的互联网用户（近 8 亿，比欧盟和美国互联网用户总和还多）和消费能力意味着任何一个企业只要获得足够的中国市场，就能成长为一个世界型的巨无霸（如阿里巴巴和腾讯），中国巨大用户提供的天量数据已经足够让任何企业发展云计算和大数据分析等新一代技术，因此能够为中国的经济发展提供足够的动力。

最后，如果世界各国都采取数据本地化措施，美国这个互联网领域的绝对霸主遭受的损失将最大，中国凭借着巨大的人口、市场和技术积累反而可能获得相对竞争优势，成为新一代技术最有力的竞争者。

因此，快速发展的互联网技术和日益增多的人才、天量的数据使得中国的数据本地化不仅不会阻碍其技术创新和经济发展，还能够减少乃至杜绝中国境内个人数据向境外泄露的风险，减少被其他国家监视和攻击的机会，维护国家网络安全。这些独有的因素和考量使得我国具有足够的动力去实施数据本地化措施。

然而，从长远来看，数据本地化会给我国带来负面影响。

首先，我国的数据本地化很可能遭到他国报复。数据本地化本质上是一种“数据保护主义”，与全球贸易自由化相冲突，也与我国一直提倡的自由贸易相违背。当我国实施数据本地化而对他国企业或者经济发展造成影响时很容易会遭到他们的报复，[45]尤其很容易遭受互联网技术强国的技术封锁和报复，类似于中美“贸易战”的国家冲突将会不断增

42 《网络出版服务管理规定》第 8 条，见工信部网址 http://www.miit.gov.cn/n1146290/n4388791/c4638978/content.html

43 《中华人民共和国网络安全法》，见全国人大网址：http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

44 严瑜：从“中国模仿”到“模仿中国”，《人民日报海外版》，2017 年 12 月 11 日第 10 版。

45 See Anupam Chander; Uyen P. Le, Data Nationalism, 64 Emory J. 726 (2015)

加。这会阻碍我国的全球贸易，进而阻碍经济发展。作为全球自由贸易的较大受益国，我国现在已经与世界各国在人员、资本、贸易、数据等方面深度互联互通，当我们采取这种“保护主义”措施时，可能会引发他国针锋相对的“保护主义”报复，最终必将对我国造成巨大的利益损害。

其次，数据本地化不利于我国企业的国际竞争，进而不利于我国经济的发展。虽然我国市场足够大，能够为我国企业提供较大的发展空间，但在普遍实施数据本地化情况下，我国企业发展起来后就面临着难以走出国门，参与国际竞争的不利局面。不难理解，当我们采取数据本地化措施后，越来越多国家也会跟进，长此以往，我国企业基本上就难以获得国外市场，尤其是考虑到他国采取报复手段时，这些“开疆拓土”的企业很可能首当其冲，他们只能成为一个区域性的企业，而难以成为跨国巨无霸，也难以与国际巨头进行竞争。此外，当世界各国的数据“割据”不断扩大之后，虽然我国会凭着巨大的人口和相对的技术优势获得相对竞争优势，但我们却也因此失去世界市场，这种“保护主义”的数据本地化会使得世界的自由贸易深受阻碍，我们也将失去利用世界市场发展自我的机会。

最后，这种做法并不利于我国国际地位和国际影响力的提升。作为一个追求大国地位的国家，这种充满“算计”的数据本地化措施并不是理想选择。“防火墙”对中国互联网发展的作用不容否认，但也因为“防火墙”的存在，我国一直广受世界批评，被认为是实施互联网审查，缺乏互联网自由的国家。数据本地化措施只会加剧我国的负面印象，阻碍中国互联网企业被世界消费者的接受和认同。因此，数据本地化带来的长期负面影响值得我们重视。

四、数据跨境流动的中国应对

如上文所述，我国的数据本地化有着其特殊性和优势，但数据本地化可能给我国带来的负面影响决定了在应对数据本地化的全球趋势下，我国采取更加理性可行、顾全大局的应对举措才是明智之举。具体而言，中国应当对数据跨境流动采取以下举措：

第一，应当逐渐减少数据本地化措施，改为确立严格的数据跨境流动法律标准。

一方面，我国应当逐渐减少乃至废除关于数据本地化法律法规的要求。如上文所述，我国法律要求许多个人数据和重要数据都应储存于我国境内。无疑，我国的数据本地化措施要求是较为广泛的，在实施数据本地化措施的国家中是属于要求较为广泛的。经过对我国实施数据本地化的理由及其利弊的分析后，不难发现，我国应当重新审视我们的数据本地化政策，充分认识到创新技术和基于数据的商品和服务带来的巨大社会和经济效益，并承诺允许跨境自由流动数据。[46]尤其是应当逐渐减少对我国境内收集的相关数据的跨境流动，以这种开放的心态和做法激励更多的本国企业和外国企业参与到基于数据的相关商品和服务的生产和服务中，推动我国数字经济的进一步发展，使得我国逐渐成为支持数据自由流动的代表。

当然，另一方面，我国应当确立严格的数据跨境流动安全与透明性的法律标准。减少数据本地化并不意味着我们对相关数据的跨境流动放任自流，恰恰相反，我们应当确立严格的数据跨境流动的安全与透明性法律标准，实施数据跨境流动准入制度。任何组织，只有当他们对数据的跨境流动提供充分的技术和安全保障时，才可以自由地进行数据跨境流动。对于技术与安全性，则由该组织承担证明责任，若出现了任何的数据泄露，则由他们承担严厉的法律责任。与此同时，这些组织在收集和跨境转移数据时，应当提供足够的透明度来获得数据主体的信任。透明度是信任的基本要求。[47]这些组织只有提供足够的透明

46 NIGEL CORY, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? information technology&innovation foundation, MAY 2017, p.17

47 Jing de Jong-Chen, Data Sovereignty, Cybersecurity, and Challenges for Globalization, 16 Geo. J. Int'l Aff. 121

度，让数据主体知悉他们数据的可能去向和用途，才能消除他们的疑虑，才能消除建立在数据基础上的创新、服务与贸易的后顾之忧。否则，没有透明度的数据收集、跨境流动与建立在此基础上的任何相关活动都难以持续。

第二，应当加强数据跨境自由流动的国际合作。加强数据跨境自由流动的国际合作，是减少乃至防止因为数据流动导致的个人隐私泄露、国家网络安全被攻击的重要途径，尤其是在互联网领域还处于“野蛮生长的丛林法则时代”、数据流动缺乏国际规则时，我们应当主动倡导制定“关于数据地位的日内瓦公约”（Geneva Convention On The Status of Data）[48]。

首先，我们应当加强与互联网技术强国美国、数据保护先锋欧盟关于数据跨境流动方面的谈判与合作。目前，中国和美国是世界上互联网领域最为发达、技术最为先进的两个国家，也是数据自由流动获利最大的国家，两个国家在数据自由流动方面有着最为广泛的共同利益。这一客观现实决定了我国应当主动加强与美国在这方面的合作，尤其是中美两国可以通过交流协商确立关于数据跨境流动的相关技术、安全和透明度标准。两个互联网技术强国所共同商讨确立的相关标准，能够有效地打消其他国家关于数据跨境流动安全性的顾虑，这一标准也会为世界的数据流动提供参考样本。此外，我们应当加强与欧盟关于数据跨境流动的谈判与合作。作为数据保护领域的先锋，欧盟虽然互联网技术相对落后于美国与中国，但其通过系列立法和国际协议争夺互联网领域与数据跨境流动规则制定权的目标与影响力却不容忽视。欧盟的《一般数据保护条例》已经成为世界各国进行数据保护的重要参考，欧盟与美国签署的“美国—欧盟隐私盾协议”已经成为美国与欧盟数据跨境流动的基本依据。这一协议很有可能成为未来欧盟与其他国家进行数据跨境流动领域的参考标准，乃至成为世界各国关于数据跨境流动协议的重要参考依据。这些都说明，我国应当抓紧与欧盟在这方面的交流与合作，确保我们能在数据跨境流动领域规则制定方面拥有话语权。

其次，加强数据跨境流动的全球合作，倡导、推动保护数据自由流动国际协议的签订。除了与美国、欧盟协商关于数据跨境流动的合作外，我国更应当主动倡导、推动关于数据跨境流动的国际性协议的签订。目前，国际社会就网络空间适用的法律、规则和规范达成共识方面取得了一些重大进展，但关于积极的网络防御方面的国际法却很少。[49]这也是各国担忧数据跨境流动安全性的重要原因。因此，创建具有法律约束力的国际数据保护规则，是解决个人数据自由流动与数据保护之间冲突的最佳方法。[50]当前，跨太平洋伙伴关系协议（Trans-Pacific Partnership Agreement，TPP）是世界上第一个禁止对通过电子方式跨境转移数据进行干预的贸易投资协定，[51]该协议第 14 章第 14.11 条明确规定，协议各方应允许通过电子手段跨境转移包括个人数据的相关数据。[52]虽然该协议因为美国的退出而前途未卜，但该协议所反映出的关于促进数据自由流动的国际努力不容忽视。中国作为重要成员的跨太平洋合作组织（APEC）于 2015 年确立的隐私框架倡议（Privacy Framework）第 4 章第 69 条对数据跨境转移也做了相关规定。[53]虽然该规定不具有法律效力，但相关倡

(2015)

48 DANIEL CASTRO AND ALAN MCQUINN, Cross-Border Data Flows Enable Growth in All Industries, information technology&innovation foundation, FEBRUARY 2015, p.15

49 Chris Cook, Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook, 29 Stan. L. & Pol'y Rev. 235 (2018)

50 Lingjie Kong, Data Protection and Transborder Data Flow in the European and Global Context, European Journal of International Law, Volume 21, Issue 2, 1 May 2010, p.456

51 Andrew D. Mitchell; Jarrod Hepburn, Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer, 19 Yale J.L. & Tech. 207 (2017)

52 See TPP Full Text, available at https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text

53 APEC PRIVACY FRAMEWORK (2015), p.32 Available at https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

议值得我们参考。因此，作为未来数据贸易的重要参与国，我国当然应当尽早加强与世界各国关于数据自由流动与数据保护方面的交流合作，尤其是借助我们大力倡导的“一带一路”合作倡议，推动与世界各国关于电子贸易、数据自由流动方面的合作，为世界数据自由流动贡献中国的智慧。

最后，支持相关数据保护的国际性政府组织、非政府组织的成立及相关工作的开展。经济、贸易等其他领域的国际性政府或非政府组织的重要作用启示我们，如果有一个专门的数据保护国际组织，对于全球的数据保护都将起着重要作用。由于专业性、高效性、相对客观性等优势，特定领域的国际组织在制定某些领域或特定类型数据的数据保护国际标准方面将发挥更大作用。[54]我国若能牵头倡导成立一个数据流动与数据保护的国际性组织，则将显著提升我国在这方面的国际影响力，也更有利于推动世界的数据自由流动和数据保护；或者支持现有的相关国际组织开展关于数据跨境转移的隐私保护工作，如目前 APEC 成立的跨境隐私规则系统（The APEC Cross-Border Privacy Rules System，CBPRs）就是在 APEC 成员支持下制定的旨在促进消费者、企业和监管机构对个人数据跨境流动相互信任的机制；[55]或者支持相关国际组织的改革以推进全球的数据流动和数据保护工作，如支持将数据流动、数据贸易问题纳入 WTO 框架中来解决，对那些过度实施数据本地化的国家进行一定的制裁，支持世界银行、国际复兴开发银行等组织提供资金帮助相关国家提高数据保护技术能力，以此强化世界各国促进数据自由流动和加强数据保护的国际责任。

五、结 语

数据自由流动是未来的必然趋势。在全球人员、资本、商品、技术等各方面已经高度互联互通的当今时代，数据的自由流动也将不可避免，任何人为的措施都难以阻挡。其实，实施数据本地化的各国也都明白，保护主义的数据本地化措施终将难以阻挡全球数据在全球范围的自由流动。然而，各国实施的数据本地化措施在短期内将难以得到改变，相反，数据本地化措施还将可能在全球范围内继续扩大。

虽然各国实施数据本地化的原因不尽相同，数据本地化措施也难以实现他们的预期目标，但数据本地化背后复杂的国际博弈和目前数据跨境流动领域国际规则的缺失，使得实施数据本地化措施成为一些国家应对互联网技术强国和保护本国公民隐私的无奈之举。尽管如此，但我们应当谨记，为每个人提供更好、更安全的互联网不应该是要求将其将其分裂。[56]数据本地化措施所带来的对全球互联网与全球经济的负面影响说明，各国理应减少乃至摒弃这一“损人不利己”的措施。

虽然中国具有的独特优势使得其数据本地化措施具有一定的有利结果，但在全球高度互联互通的今天，中国已经融入到全球大家庭之中，我们采取的任何措施都会通过全球贸易最终传导回我们自身，中国实施的不利于全球技术创新和经济发展的数据本地化措施最终也必将给自身带来负面影响。任由数据本地化的不断扩大，将会形成数据割据，导致“共输”局面的出现，这不符合任何一个国家的利益，更加不符合中国的利益。

因此，中国应当逐渐减少乃至摒弃数据本地化措施，通过加强与世界各国、尤其是与互联网技术强国和数据保护先行者在数据自由流动、数据保护方面的合作，通过数据自由流动方面的国际协议来保护个人隐私和国家网络安全，从而为新一代技术创新、数字经济的发展提供新的国际规则。这才是中国应对数据本地化全球趋势的可行之道。

54 Lingjie Kong, Data Protection and Transborder Data Flow in the European and Global Context, European Journal of International Law, Volume 21, Issue 2, 1 May 2010, p.456
55 See http://cbprs.org/
56 Anupam Chander; Uyen P. Le, Data Nationalism, 64 Emory J. 739 (2015)

Data localization: the global trend and China's response

Zhuo Lixiong
(Party School of the Central Committee of the C.P.C., Beijing)

Abstract: Many countries have taken the measure of data localization, which is gradually become a global trend. Proponents of data localization have put forward their reasons. However, the opponents have refuted them in a tit-for-tat manner, they believe that these reasons of data localization are wrong, what is more, data localization may produce counterproductive results. China has also taken the data localization measure. When talking about the data localization measure in China, it brings some favorable results in the short term, but in the long run, it may cause many negative effects. Therefore, in order to promote the free flow of data, China should gradually reduce the data localization measure, strengthen global cooperation on cross-border data flow, promote the signing of international agreements on data flows and support the establishment of international data protection organizations.

Keywords: Data Localization, Cross-border Flow of Data, Personal Data, Data Sovereignty

作者信息：

卓力雄，1991 年，男，广东湛江人，汉族，中共中央党校政治与法律部博士生，美国波士顿大学法学院联合培养博士，研究方向：法学理论，互联网法学，个人数据保护

北京市海淀区大有庄 100 号中共中央党校研究生院，1967 信箱，C2079，100091；

电话：15201640792（暂停使用）+1 6173317579（美国号码）；

邮箱：zhuolixiong828@163.com