数据本地化和数据防御主义的合理性与趋势*

刘金河　　崔保国

【内容摘要】 在全球数字贸易规则形成中，数据跨境流动政策是各方谈判焦点，数据本地化则是其中要害。全球数据跨境流动规制正进入第三次浪潮。不同于此前西方国家设计数据权利保护工具的逻辑，当前一些新兴经济体和发展中国家采取的是一种国家战略上的数据本地化诉求。本文构建了一个理论解释模型——基于有限理性的数据防御主义，即面对全球信息技术强弱不均的国家实力结构以及数据往往向强势国家流动的现状，一个国家会以守住对自有数据控制权的方式确保自身安全。但决策的有限理性让一个国家在数据跨境流动政策的选择上追求“满意”而不是“最优”目标。一个处于相对竞争劣势的国家更有可能采取防御型互联网治理政策，表现为强烈的网络主权立场，并诉诸数据主权的话语工具。中国未来需要结合国际形势的变化，积极建立一种以效率发展为路径的跨境数据有序自由流动秩序。

【关键词】 数据跨境流动　数据本地化　数据防御主义　数据主权

【作者简介】 刘金河，清华大学互联网治理研究中心助理研究员、公共管理学院博士后（北京　邮编：100084）；崔保国，清华大学新闻与传播学院教授（北京　邮编：100084）

【中图分类号】 F11　　**【文献标识码】** A

【文章编号】 1006-1568-(2020)06-0089-19

【DOI 编号】 10.13851/j.cnki.gjzw.202006005

* 本文系教育部哲学社会科学研究重大课题攻关项目“构建全球化互联网治理体系研究”（17JZD032）的阶段性成果，同时受清华大学自主科研计划资助；感谢弥尔顿·穆勒、李晓东、王融、鲁传颖、许可、付伟等师友的讨论意见以及匿名评审专家的宝贵意见。

一场围绕数据跨境流动规制的全球大辩论和国际规则大博弈正在展开。在数字经济浪潮下，数据跨境流动规制不再仅仅是一个公民权利保护的问题，而是关乎国家安全、国民经济发展与国家竞争力的重大决策，是国际贸易规则竞争的新阵地。2019 年 6 月，二十国集团（G20）大阪会议《G20 贸易及数字经济部长的声明》提出“信任的数据自由流动”主张，数据跨境流动规则成为全球数字经济贸易的核心议题，[①] 各大国间的规则竞争激烈展开。其中，数据跨境流动议题中最核心的数据本地化（Data localization）不是一个短期出现的现象，而是随着全球化深入而日益严峻的挑战。[②] 在全球科技竞争日趋激烈、国家间信任日益减弱的大背景下，数据本地化趋势将进一步凸显。现有文献对全球数据跨境流动规制的立法和政策的描述已非常充分，[③] 但制度规则之下的本质需要被追问，因此本文研究的核心问题是：在全球数字贸易时代，为什么一个国家会采取数据本地化的严苛限制措施？

在理论上，研究者试图建构数据本地化这一复杂现象的解释框架，提出数据与民族主义叙事结合而成的数据民族主义[④]、作为贸易保护新形式的数字保护主义[⑤]、抵抗西方霸权的反数据殖民主义[⑥] 等不同角度的理论解释。

① 根据麦肯锡的数据，2004—2014 年，数据跨境流动为全球经济贡献了 3%的增长，2014 年带来 2.8 万亿美元的产值。与数据跨境流动对数字贸易的重要性形成对比的是，目前国际数字贸易规则供给不足，谈判正在各个国际组织中展开，如 WTO、G20 以及其他地区性自由贸易协定等。同时，数据跨境流动问题也是当下中美贸易谈判中的焦点问题。参见：McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, March 2016; UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, April 2016；柯静：《WTO 电子商务谈判与全球数字贸易规则走向》，《国际展望》2020 年第 3 期，第 43—62 页。

② Christopher Kuner, “Foreword,” in W. Kuan Hon, *Data Localization Laws and Policy: the EU Data Protection International Transfers Restriction Through a Cloud Computing Len*s, Edward Elgar Publishing, 2017, p. X.

③ 对于数据跨境流动政策的综合梳理和分析具有代表性的研究参见：Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2017; Anupam ChanderandUyên P. Lê, “Data Nationalism,” *Emory Law Journal*, Vol. 64, No. 3, 2015；王融：《数据跨境流动政策认知与建议》，《信息安全与通讯保密》2018 年第 3 期等。

④ 毛维准、刘一燊：《数据民族主义：驱动逻辑与政策影响》，《国际展望》2020 年第 3 期，第 20—42 页。

⑤ 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 年第 6 期，第 108—118 页。

⑥ Arindrajit Basu, et al., “The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India,” *The Centre for Internet and Society*, India, No. 19, March 2019, p. 12; Rahul Matthan, “Colonialism 2.0–Truly,” *SWARAJYA*, January 2, 2019.

但是，既有理论大多缺乏国际关系和互联网治理的视角，对数据本地化的本质未能准确揭示。事实上，数据跨境流动问题关乎信息的跨国流动和互联网的全球连接，其所规制的对象是国际互联网的核心要素，产生了规范外溢效应，是一个处于国内和国际交叉路口的极其特殊的国际互联网治理问题，本质上是一个国际交往与竞争的问题。因此，本文从国际关系和互联网治理的角度提出“数据防御主义”以解释数据本地化现象背后的因果逻辑。

一、数据跨境流动规制的核心：数据本地化

数据跨境流动问题深度交织于国际贸易、地缘政治以及国际互联网治理规则设计等全球治理议题之中。正如有研究者指出，在当前网络空间治理政策中，没有哪类议题能够像数据跨境流动一样，包含如此复杂的讨论维度：数据主权、隐私保护、法律适用与管辖乃至国际贸易规则。[①] 对于解释数据跨境流动规制的动机，人们通常认为个人隐私保护、国家安全、国内执法、产业保护等是数据跨境流动规制的几个常见理由，而且往往将其并列。[②] 大量文献对欧洲近半个世纪数据跨境流动限制历史的分析，往往落脚到个人信息保护的动机，这种分析虽然对理解欧洲立法提供了有益的知识贡献，但对理解当前的全球数据跨境流动政策而言，却具有一定程度的迷惑性。

数据跨境流动从 20 世纪 70 年代初便是欧美竞争的焦点。20 世纪 90 年代以前由欧洲主导了规则建立，2000 年后美国主动建构美国版的数据跨境流动管理规范，而最近十年以来，全球数据跨境流动规制进入第三次浪潮。过去 50 年左右的数据跨境流动规制历史中，前 40 年西方国家主要的关注焦点是个人隐私保护，而后十年随着新兴国家开始对此议题的“觉醒”，纷纷从本国发展的角度加入规则建构，数据跨境流动的问题不再仅仅是个人隐私

① 王融：《数据跨境流动政策认知与建议》，第 41 页。

② 主要文献包括：Anupam Chander and Uyên P. Lê, “Data Nationalism,” pp. 677-739; Nigel Cory, “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?” The Information Technology and Innovation Foundation, May 2017; Jonah Force Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders,” The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, 2014。

保护问题，而更是国家财富的争夺，[①] 在数字贸易背景下展开了新一轮全球大辩论，从隐私权利保护规则转移到了数字贸易规则的博弈。

数据跨境流动规制的历史反映出了两种逻辑：前 40 年主要在于对权利保护工具的设计与争论，近 10 年来核心在于提出数据本地化的诉求。与此对应，早期的数据是限定在个人信息，如今的数据涉及几乎所有的信息，核心在于具有商业价值的一切可流通信息；当前阶段的行为体发生了很大变化，提出新方案的基本上是新兴国家，其诉求与以往也有很大区别，核心是数据本地化。数据本地化广义上是指对数据跨越国境所采取的各种类型的限制，包含了从附带条件的流动到完全禁止。而狭义的数据本地化指要求将数据的储存和处理放在数据来源国境内的数据中心和服务器，根据宽严程度不同的类型，实践中通常有：仅要求在当地有数据备份而并不对跨境提供进行过多限制；数据留存在当地，且对跨境提供进行限制；数据留存在境内的自有设施上，不得向境外提供；要求特定类型的数据留存在境内；等等。[②] 目前不少文献在广义上使用数据本地化概念，[③] 但是事实上，“数据跨境流动限制”（Restrictions on cross-border data flows）包含了严苛程度不同的各类限制，是更为综合的概念，也符合众多文献讨论的语境。为了聚焦于本质逻辑，本文所指的数据本地化是后者，也就是狭义上的，其核心是要求数据本

① 将数据作为财富最为典型的是中国和印度。中国国务院 2015 年发布的《促进大数据发展行动纲要》提出，“数据是国家基础性战略资源”；2019 年 11 月，中国共产党十九届四中全会提出，“健全劳动、资本、土地、知识、技术、管理和数据等生产要素按贡献参与分配的机制”，这是中央首次正式提出数据可作为生产要素按贡献参与分配。2019 年 6 月，印度外交秘书顾凯杰（Vijay Gokhale）召开新闻发布会，针对美国总统特朗普在 G20 会议上批评数据本地化，表示“数据是国家财富的新形式（new form of wealth），发展中国家需要引起重视”，参见：“Data ‘new form of wealth’, take it into account of developing nations' needs: India,” *The Economic Times*, June 28, 2019, https://economictimes.indiatimes.com/tech/internet/data-new-form-of-wealth-needs-to-take-into-account-developing-nations-needs-india/articleshow/69988888.cms。

② 参考了世界银行《2016 年世界发展报告：数字红利》的定义，同时结合李海英和王融的定义做了进一步解释，参见世界银行：《2016 年世界发展报告：数字红利》，清华大学出版社 2017 年版，第 310 页；李海英：《数据本地化立法与数字贸易的国际规则》，《信息安全研究》2016 年第 9 期，第 782 页；王融：《数据跨境流动政策认知与建议》，第 42 页。

③ 典型如 Anupam Chander and Uyên P . Lê, “Data Nationalism,” Anupam Chander and Uyên P . Lê, “Breaking the Web: Data Localization vs. the Global Internet,” UC Davis Legal Studies Research Paper No. 378, April 2014; Christopher Kuner, “Data Nationalism and Its Discontents,” *Emory Law Journal* Online, Vol. 64, 2015, pp. 2089-2098。

地存储和处理。

数据本地化是数据跨境流动规制的最严苛程度，其动因与其他数据跨境流动限制有本质的区别，而且具有更深刻的地缘政治意义。数据本地化的根本目的在于对数据所承载的安全和价值进行直接而又极端的控制以实现国家战略，而其他的数据跨境流动限制着眼于设计旨在对附着在数据流上的权利进行保护的政策工具，即“国家发展战略”与“权利保护工具”二元政策目的的区别。因此本研究的分析是建立在鼓励数据流动和限制数据流动（本地化）两种立场之上的二元极化分析。

二、数据本地化的逻辑：数字经济下的数据防御主义

数据是一种资源和资本，是各方追逐的对象。[①] 农业经济以劳动力、土地为核心生产要素，工业经济以资源、技术和资本为核心生产要素，而数字经济是以数据和信息技术为核心生产要素。[②] 那么在数字经济时代，当数据资源在国家间流动转移，一个国家将会如何应对这种基于数据资源的竞争？

数据跨境流动规制本质上是一种国家间的竞争行为，遵循现实主义的博弈逻辑。现实主义学派认为，由于国际体系是无政府状态，国家实力不尽相同，导致不平等的国际体系结构，因此每个国家需要通过自助战略来确保自身安全。[③] 根据获得安全的最有效途径的不同，现实主义被划分为“进攻性现实主义”和“防御性现实主义”。[④] 进攻性现实主义者认为，国际体系为国家牺牲对手以获得权力创造了巨大的诱导因子，当利益超过成本时，它们就会抓住这一机会。[⑤] 防御性现实主义则提出，在这个无政府的自助系统中，

① 杨剑：《数字边疆的权力与财富》，上海人民出版社 2012 年版，第 26—30 页；Nick Couldry and Ulises Mejias, “Making Data Colonialism Liveable: How Might Data’s Social Order Be Regulated?” *Internet Policy Review*, Vol. 8, No. 2, 2019, pp. 1-16。

② 崔保国、刘金河：《论数字经济的定义与测算》，《现代传播（中国传媒大学学报）》2020 年第 4 期，第 122 页。

③ Hans Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 5th ed., New York: Alfred A. Knopf, 1978.

④ Jack Snyder, *Myths of Empire: Domestic Politics and International Ambition*, Ithaca:Cornell University Press, 1991, pp. 12-13.

⑤ 典型代表如：[美]约翰•米尔斯海默：《大国政治的悲剧（修订版）》，上海人民出

相对弱的国家往往采取防范措施促使均势得以维持，以便确保自身安全，守住而不是增加权力才是国家的目标。[①] 纵观历史发展，我们的世界已经从 1945 年前的进攻性现实主义世界（即大多数国家都是掠夺者）演化到了今日的防御性现实主义世界（即多数国家是温和的）。[②]

面对新的技术环境，对于新的生产要素——数据，处于相对弱势的国家采用实用主义的策略以追求国家整体利益的最大化，呈现出数字时代紧缩的立场，抑或称之“数据防御主义”。数据防御主义核心要素在于，面对全球信息技术强弱不均的国家实力结构，以及数据往往向强势国家流动的现状，一个国家会采取以守住对自有数据的控制权的自助方式确保自身的安全。守住而不是进攻，是数据防御主义的核心特征。这种数据防御主义强调了安全需求，此时的安全是广义上的，即国家安全、经济安全、公民安全，公民隐私等个人权利保障被纳入了安全范畴。数据含有一国国民和国家的信息，大数据量级具有更强大的信息能力，因此，数据流转到境外控制者手中存在安全风险。[③] 这种担忧在美国棱镜门事件后成为各国不得不面对的现实。[④]

当数据流出自身控制的管辖边境时，如果一国技术发展水平高、产业发达、安全威胁不那么紧迫，那么该国就会采取鼓励数据跨境流动策略；反之，技术发展水平不高、产业不发达、安全威胁紧迫，该国则会采取紧缩的数据跨境流动策略，具体表现为数据本地化。不过，如果国内产业规模太小、信息通信技术（ICT）发展程度太低，该国对国外互联网技术和服务往往高度

版社 2014 年版。

① 典型代表如：Kenneth Waltz, *Theory of International Politics*, Reading: Addison-Wesley Publishing Company, Inc. 1979。

② 唐世平：《我们时代的安全战略理论：防御性现实主义》，北京大学出版社 2016 年版，第 144—145 页。

③ 全国人大常委会法制工作委员会在对《网络安全法》的权威解释中强调：“重要数据如果转移至境外，关键信息基础设施的运营者对其控制力必将削弱，其安全风险将增加”。不过，美国智库信息技术与创新基金会（ITIF）2013 年发布的一份报告指出，数据安全不在于存储地，而是怎么保护的法律机制问题。但是棱镜门事件证实了法律和合同的保护并不足以保障数据的安全，特别是涉及国家社会的重要信息而不仅仅是个人信息和隐私的保护问题。参见：杨合庆主编：《〈中华人民共和国网络安全法〉释义》，中国民主法制出版社 2017 年版，第 96 页；Daniel Castro, “The False Promise of Data Localization,” The Information Technology and Innovation Foundation, December 2013。

④ Jonah Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders.”

依赖，因此无力提出数据本地化诉求。外部环境和自身要素禀赋决定一个国家对跨境数据流动的控制程度，即一国 ICT 技术发展、产业规模、安全需求三个主要因素的强弱引起该国对跨境数据流动策略的放宽或收缩。具体来说，具有一定 ICT 产业规模且正处于高速发展中的国家，基于产业和技术发展以及安全的考虑，往往会做出数据本地化的选择。当然，这种防御主义区别于保护主义和重商主义。重商主义是极端的贸易保护主义，将贸易和国家权力扩张捆绑在一起，主张排他性贸易机会，在历史上带来了殖民主义、帝国主义和与之相关的冲突。数据防御主义虽然带有自我保护的成分，但是更多的是在外来强大对手面前采取的防卫性措施，并不以限制贸易为目的。

数据防御主义在当今的国际竞争中普遍存在。本文针对全球主要的 60 个国家，统计一国的数据跨境流动立场与该国 ICT 发展程度和网络安全受威胁程度的关系，形成了分布图（见图 1）。在分布图上，纵轴是网络安全受威胁程度（2018 年），其得分越高意味着网络安全威胁程度越高；横轴是国际电信联盟（ITU）ICT 发展指数（2017 年），其得分越高意味着发展程度越高。欧盟国家的数据跨境流动政策以《通用数据保护条例》（GDPR）和《非个人数据自由流动条例》为代表，虽然强调权利保护，但是原则上鼓励数据跨境流动；由美国主导的亚太经合组织跨境隐私规则体系（CBPRs）倡导数据跨境自由流动，目前有 8 个成员加入[①]，这两类主体主要落在了右上角的圆圈内。而其中，在国内法律政策中明确规定数据本地化的国家，以俄罗斯、中国、马来西亚、印度、伊朗、土耳其、越南、印度尼西亚、尼日利亚 10 国为典型代表（图中粗体字），全都落在了左下角的圆圈内。[②] 该图清楚地显示，网络威胁程度较高、ICT 技术发展指数较低的国家或地区更

① 分别是美国、日本、韩国、新加坡、加拿大、墨西哥、澳大利亚等。

② 安全需求的因素严格来说指的是来自境外的威胁，该模型中的网络安全受威胁得分指标由于包含了国内网络威胁，因此只具高度的相关性，而不是准确的对应关系。如图表显示，俄罗斯和土耳其等国被列为网络威胁较低的国家；但事实上，它们的外部威胁更为紧迫。数据本地化对 ICT 发展和网络安全的影响不会造成两个指数的大幅度变化，也就是并不是因为数据本地化导致了网络安全系数低和 ICT 发展落后的原因，因为跨境数据流只是信息通信技术和互联网的一部分，而且颁布了严格的数据本地化政策也只是最近几年才出现的现象，效果并未充分显现。此外，巴西曾在 2014 年《互联网民法（草案）》中明确规定数据本地化，即使后来并没有通过该规定，但由此可以看出巴西落在了左下角圈的区域，具有数据本地化的动机。

有可能采取数据本地化策略；反之，则倾向于鼓励数据自由流动。

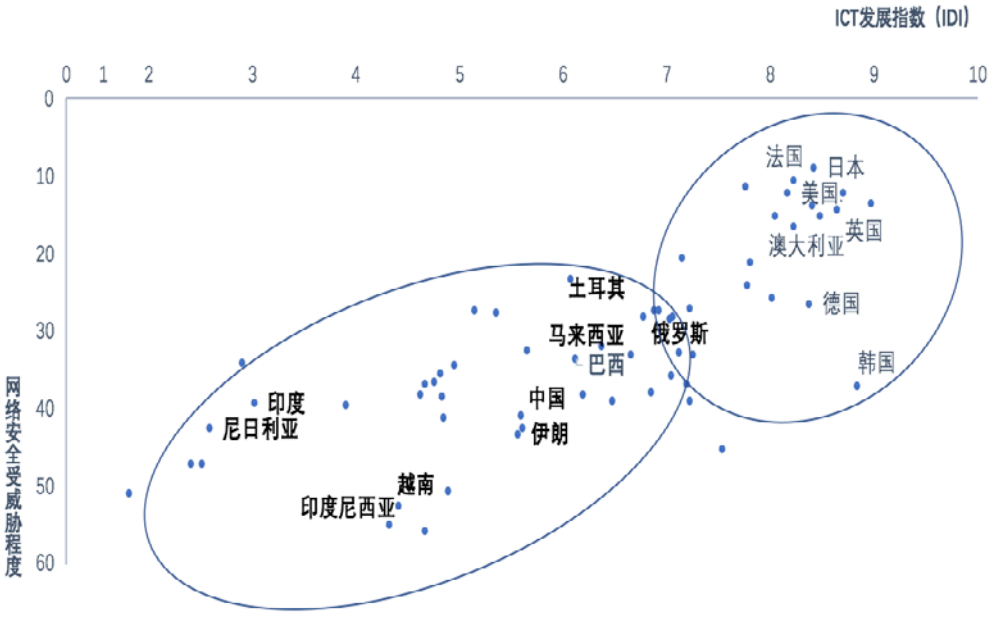

图 1　数据跨境流动立场与网络安全受威胁程度和 ICT 发展指数分布图

资料来源：作者根据 Kaspersky Lab、ITU、CSIS、Comparitech 的数据制作。网络安全受威胁程度引自 Comparitech 网络安全指数（Cybersecurity Rankings），其综合了 Kaspersky Lab, ITU, CSIS 的数据；ICT 发展指数（ICT Development Index, IDI）引自 ITU，是衡量各国 ICT 发展水平的权威指标。

从全球数据跨境流动规制的实践来看，美国的数据跨境政策由贸易利益驱动，鼓励数据自由流动，核心是维护美国在全球贸易中的主导地位。[①] 而欧盟从公民权利保护出发，积极推广个人数据充分保护制度，对数据自由流动持有限制立场。总体来看，欧美发达国家处于强势地位，因此原则上鼓励数据自由流动；而新兴国家信息技术能力相对较弱、安全需求强烈，更加倾向于把数据截留在本国境内。

① 美国的跨境数据流动管理机构主要集中在贸易领域，包括美国商务部、联邦贸易委员会、贸易代表办公室及司法部等，具体分析见付伟、于长钺：《美欧跨境数据流动管理机制研究及我国的对策建议》，《中国信息化》2017 年第 6 期，第 55—59 页。

全球互联网带宽占比也印证了这一事实。据统计和预测，2006 年北美占据全球带宽总量的 97%，2018 年占据 85%，而到 2024 年将依然占据 80%，从全球各大洲之间的带宽容量来看，相对于其他大洲之间，北美和西欧之间一直占据绝对领先地位。[①] 占据全球流量强势地位的国家往往立于鼓励数据自由流动的立场，而相对弱势的国家更有可能要求数据本地化。在此逻辑下，世界范围内不同的数据经济区正在建立，这种竞争在当下的数字贸易谈判中引发了激烈博弈。[②]

另一个实证经验证据来自正在进行的世贸组织（WTO）电子商务和数字贸易规则谈判。针对数据跨境流动，参与谈判的 80 个经济体中，不同阵营呈现不同的立场。中国等发展中国家成员普遍倾向于采取限制数据跨境流动措施，将计算机设施本地化、披露或者转让源代码作为在本地开展业务的前提条件。这些国家的提案或是未涉及这部分内容，或是强调保留政策空间。美国将跨境数据自由流动和禁止本地化要求视作消除壁垒的关键。欧盟、日本、加拿大等发达经济体与美国的立场基本一致，区别仅在于相较美国更加认同监管的必要性，它们对合法公共政策目标的容忍度较高。[③]

三、数据本地化的实现：有限理性与数据主权

数据本地化带来的明显损害[④] 并不是可以漠视的，但相关国家依然坚持做出了看似不利的选择。经济学家赫伯特•西蒙（Herbert A. Simon）的有限理性理论（Theory of Bounded Rationality）或许能够解释这一令人费解的现象。西蒙用“满意的行为”代替了最大化（maximizing）或最优化（optimizing）

① Alan Mauldin (TeleGeography), “Back to the Future,” Pacific Telecommunications Council Annual Conference, January 20-23, 2019, https://www.ptc.org/PTC19/Proceedings/WK_TELEGEO_Mauldin_Alan.pdf

② Susan Aaronson and Patrick Leblond, “Another Digital Divide: The Rise of Data Realms and its Implications for the WTO,” *Journal of International Economic Law*, Vol. 21, No. 2, 2018, pp. 245–272.

③ 柯静：《WTO 电子商务谈判与全球数字贸易规则走向》，第 48 页。

④ 数据本地化的经济伤害数据：Matthias Bauer et al.,“The Costs of Data Localisation: Friendly Fire on Economic Recovery,” European Centre for International Political Economy, March 2014。

行为的古典概念。其依据心理学上的证据指出，复杂性和不确定性致使全面理性不可能，因此反观“活动者处理能力限度”，提出决策的有限理性。[①] 这种有限理性同样适用于个人和组织，在面对多种备选方案时往往将最优化准则换成了满意性能准则。[②] 根据有限理性理论，行政主管部门和公司一样，拥有多重目标，它们并不期待最好或者最优的结果，而是期待“足够”的结果，即足以满足（satisficing）多种目标的需要。[③] 布雷布鲁克和林德布罗姆进一步提出，政策制定者们倾向于把问题分解成各个部分，以便能够进行渐进的或边际的选择，而不是作出影响深远、难以逆转的决策，这是一种实用经验主义的做法。[④] 因此，数据本地化虽然不理想但却合理，是具有实用色彩的策略性选择。

相对于鼓励数据自由流动的国家来说，从现实的国家利益到抽象的观念价值，从整体的社会福利到个人的公民权益，选择数据本地化的国家往往有更为复杂的目标有待实现。具体来说，则包括国家安全、公民权利保护、产业保护、技术发展、国际贸易、外国投资、网络主权等。对于正在快速发展的新兴国家来说，在面临相对较高的网络风险和相对较弱的国内信息技术产业竞争力条件下，优先保障发展和安全是其最为重要的目标。为实现这一优先目标，在推进数据本地化的过程中，相关国家政府面对外来阻力往往显示出坚定的信念，典型如中国、俄罗斯、印度的数据本地化政策虽然引起了跨国公司、外国政府和国际组织的激烈反对，但是这一政策依然被坚持。在经济全球化时代，防御主义往往被批评为贸易保护主义，引起国际社会的反弹甚至制裁。在当前一系列数字贸易谈判中，发达国家将限制数据跨境流动和本地化要求作为重要的数字贸易壁垒，发展中成员则提出“数据国家主义”的理由来实施此类措施。[⑤]

---

① [美]赫伯特•西蒙：《现代决策理论的基石》，杨烁、徐立译，北京经济学院出版社 1989 年版，第 45—57 页。

② 同上，第 62 页。

③ [英]苏珊•斯特兰奇：《权力流散：世界经济中的国家与非国家权威》，肖宏宇、耿协峰译，北京大学出版社 2005 年版，第 17 页。

④ David Braybrooke and Charles Lindblom, *A Strategy of Decision*, New York: The Free Press, 1963, pp. 71-79.

⑤ Anupam Chander and Uyên P . Lê, “Data Nationalism;” 石静霞：《数字经济背景下的

互联网的根本之处在于信息的交流，网络空间治理归根到底是对数据的治理。数据跨境流动规制虽然面向国际贸易，但是其本质属性上是一个互联网治理的议题，遵循一国互联网治理的基本原则和逻辑。随着互联网演变为网络空间，互联网治理的议题也逐渐从底层的技术协议管理上升到上层的内容应用开发与经济社会行为规制，互联网治理的属性也从技术治理逐步演变为综合的社会治理，国家主权在网络空间逐步得到确立。今后，网络主权的意义也将从政治逻辑更多地转向实实在在的商业逻辑，即确保本国用户的数据不被国外互联网公司搜集和利用，这不仅体现在各个层面的资本控制上，也体现为对跨境数据贸易和服务贸易的限制。[①] 总的来看，各国在网络空间主权问题上的主张和实践均折射出其当下的核心利益诉求，[②] 由此在全球网络空间治理体系中呈现出明显的有利于规则主导国的“非中性”[③] 特征。对“主权”的诉求在某种意义上具有防卫性质，以排他性的绝对权来免除外来的侵犯，但同时也将自己限制在领土边界的范围之内。这是典型的防御性现实主义的路径逻辑在网络空间和跨境数据流动上的体现，网络主权和数据主权就成为实现这种数据防御主义的途径。

在有限理性的数据防御主义逻辑下，一个处于相对竞争劣势的国家更有可能采取防御型的国际互联网治理政策，表现为强烈的网络主权立场。网络主权及其所包含的数据主权成为数据本地化的叙述方式，换言之，数据本地化通过对网络主权的声索而实现。

四、数据防御主义下中国数据本地化的动力机制

在刚过去的 21 世纪第二个十年里，数据本地化成为一股声势越来越浩

WTO 电子商务诸边谈判：最新发展及焦点问题》，第 176 页。

① 胡凌：《信息基础权力：中国对互联网主权的追寻》，《文化纵横》2015 年第 6 期，第 105 页。

② 郎平：《主权原则在网络空间面临的挑战》，《现代国际关系》2019 年第 6 期，第 48 页。

③ 张宇燕、任琳：《全球治理：一个理论分析框架》，《国际政治科学》2015 年第 3 期，第 15—16 页。

大的浪潮，中国是其中最坚定的倡导者之一。2016 年 11 月 7 日通过的《网络安全法》是中国在网络领域里第一部具有全局性的基本大法，首次在法律上对数据跨境流动进行了明确规定。《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存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。"此举被认为是确定了中国数据跨境流动规制的"本地储存，出境评估"制度。不过，中国数据跨境流动的制度设计依然还在形成过程中，具体评估措施依然处于征集和讨论之中。[①] 虽然在具体的制度设计上并不成熟，但国家要求数据本地存储的意志是坚定的。[②]

中国数据本地化是一个复杂的政策选择，通过有限理性的数据防御主义理论可以探寻其背后的动力和机制。[③] 需要特别说明的是，数据跨境流动规制的主体是国家，其制度设计不可避免地带有国家视角，所以本研究采用国家路径探寻中国数据本地化的动力运作机制。[④]

（一）数据防御主义的认知基础

数据本地化是中国互联网治理的一项重要制度选择，这种重大的制度选择根源于中国社会的认知形态。追根溯源往往能够更清晰地理解当下，从中

① 2020 年 7 月 3 日全国人大常委会发布的《数据安全法（草案）》征求意见稿第 10 条规定："国家积极开展数据领域国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。"这与此前政策文件和发布的立法草案中一贯的"安全有序自由流动"原则的表述有所不同，后续立法值得关注。

② 从最早 2011 年银行业实质要求数据本地化存储到后来其他重点行业陆续推出相同规定，证明中国数据本地化储存并不是纯粹由 2013 年斯诺登事件激发的冲动。另外，中国国家安全立法曾要求数据全面本地化存储，而且是没有留下可协商空间的刚性规定。2014 年《反恐怖主义法（草案）》第 15 条规定，"在中华人民共和国境内提供电信业务、互联网服务的，应当将相关设备、境内用户数据留存在中华人民共和国境内。拒不留存的，不得在中华人民共和国境内提供服务。"不过最终通过的法律把该条款直接删除，不再就数据跨境流动做出规定。由此可见中国数据本地化的决心是连贯而坚定的。

③ 中国数据本地化的制度动力的进一步分析参见：Jinhe Liu, "China's Data localization," *Chinese Journal of Communication*,Vol. 13, No. 1, 2020, pp. 84-103。

④ 著名汉学家费正清从历史和文化的角度指出，一个统一的中国是历来民众为之奋斗的理想，也是中国根深蒂固的传统，只有一个统一的中央政府才能维持这种传统。这点对理解当代中国政治体制以及本文所分析的关于数据跨境流动规制的制度设计有重要的启发作用。参见[英]费正清等：《剑桥中华人民共和国史》（第 14 卷：革命的中国的兴起，序言），谢亮生等译，中国社会科学出版社 1990 年，第 18—25 页。

国对技术和安全的理解中可以寻找数据规制的底层来源，即从总体国家安全观到数据安全，从技术民族主义到网络强国。强调提升自我技术能力以抵御外来危险的安全防御思想，是中国数据防御主义的认知建构基础。

在充满不确定的外部环境下，中国将对国家安全的严峻形势的认识提高到前所未有的高度。2013 年习近平总书记指出，“在互联网这个战场上，我们能否顶得住、打得赢，直接关系我们意识形态安全和政权安全。”[①] 2014 年，中央国家安全委员会成立，习近平首次提出“总体国家安全观”，要求“以政治安全为根本，以经济安全为基础”，走出一条中国特色国家安全道路。[②] 中国特色的社会主义道路是中国最大的国情，这就决定国家政治安全至关重要，其中最突出的问题就是意识形态安全。[③] 如果说网络数据是一种信息符号的话，从内容视角来看，网络数据还是一种价值判断，背后体现的是意识形态和伦理的冲突。[④] 有学者指出，数据资源存储和分配及其基础技术由少数跨国公司直接控制或由外国政府间接控制，将会因过度集中而形成强大的支配力，足以威胁到国家数据主权安全。[⑤] 《网络安全法》以总体国家安全观为指导思想，要求保护政治、经济、社会等领域的全方位安全，意识形态安全被放在突出的位置。数据安全关乎意识形态安全和政治安全，特别是美国的棱镜门事件给中国带来极大警示作用。

科学为民族国家提供了文化脚本，使民族国家按照其规定而行动。[⑥] 这种文化脚本让国家的发展建立在科学技术基础上。在当代中国，信息技术不仅被视作科学和技术进步的最现代指针，也被认为是国家现代化的象征。[⑦] 这种情结或者信念可以被归结为技术民族主义的一种，即“对国家安全和经

① 《在全国思想工作会议上的讲话》（2013 年 8 月 19 日），摘自中共中央党史和文献研究院《习近平关于总体国家安全观论述摘编》，中央文献出版社 2018 年，第 103 页。

② 《习近平：坚持总体国家安全观 走中国特色国家安全道路》，新华网，2014 年 4 月 15 日，http://www.xinhuanet.com/politics/2014-04/15/c_1110253910.htm。

③ 高飞：《中国的总体国家安全观浅析》，《科学社会主义》2015 年第 2 期，第 13 页。

④ 鲁传颖：《网络空间中的数据及其治理机制分析》，《全球传媒学刊》2016 年第 4 期，第 11 页。

⑤ 肖冬梅、文禹衡：《在全球数据洪流中捍卫国家数据主权安全》，《红旗文稿》2017 年第 9 期，第 35 页。

⑥ Gili Drori etai., eds., *Science in the Modern World Polity: Institutionalization and Globalization*, Stanford University Press, 2002, p. 268.

⑦ 郑永年：《技术赋权》，东方出版社 2014 年版，第 24 页。

济繁荣来说，技术是最根本的，一个国家的发展政策必须拥有明确的战略支撑，技术必须不惜一切代价本土化，并使其在整个制度中扩散”[①]。面对数据跨境流动，技术本地化直接表达为数据本地化，关于数据的防御系统正在逐渐形成。

（二）有限理性下的优先选择

中国互联网监管肇因于发展和安全需求之间的政策价值矛盾。[②] 事实上，在数字时代，对于数据跨境流动的任何政策都会引起复杂的效应，行政主管部门必须在众多目标中进行取舍。从现实的利益平衡来看，与数据跨境流动相关的制度即包含着政策制定者的多重考量，得失的考量体现了有限理性的决策逻辑。这些复杂的考量真切地反映出数据跨境问题的挑战性。在现实环境下，保障国家安全和社会安全、保障国内产业和科技发展成为国家优先保护的现实利益。中国所担心的安全并不仅是数据被恶意利用，更重要的是这种危险来源于境外势力或外国政权的恶意监控，甚至有可能危及国家基本政治制度。在这个意义上，中国对数据安全的警惕主要是从国家核心利益层面出发的，是在总体国家安全观的框架下进行的。“没有网络安全，就没有国家安全”，国家安全逐渐统合了网络安全和数据安全概念。这种安全诉求最终体现在对数据相关技术的自主可控要求上，自然表现出一种防御型的互联网政策倾向。

《十三五国家信息化规划》等一些国家重要战略提出对科技的自主可控诉求。[③] 因为数字产业竞争力差距的存在，当今世界的基本现实是，数据产业竞争力较弱国家的用户是数据的主要提供者，数据产业竞争力较强国家的公司则是设备和服务的主要提供者，在不设限制的情况下，数据将自然向少数国家地理疆域之内汇聚。[④] 世界领先的数据存储、大数据、云计算等数据

① Evan Ferigenbanum, *China’s Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age*, Redwood City: Stanford University Press, 2003, p. 14.

② 王融：《中国互联网监管的历史发展、特征和重点趋势》，《信息安全与通讯保密》2017 年第 1 期，第 52 页。

③ 在《十三五国家信息化规划》文本中，“自主”一词使用频率高达 12 次，在附件中的重点任务分配方案中第一条就是“打造自主先进的技术体系”。

④ 上海社会科学院：《全球数据跨境流动政策与中国战略研究报告》，2019 年 8 月。

相关的公司大都集中在美国，甚至处于垄断地位，这在很大程度上是由于世界范围内的数据源源不断地流入美国所致。中国对自身短板有着清晰的认识，技术产业生态系统不完善，自主创新能力不强，最大软肋和隐患是核心技术受制于人，这已成为中国的广泛共识。实现技术自主的战略路径是以大数据、物联网、云计算、人工智能等先进的核心技术为推进手段，通过网络强国来实现“数字中国”。数据在这个宏大的战略目标中被赋予极为重要的地位，提升到“国家重要的基础性战略资源”[①]层面。

当然，数据本地化政策也会给经济发展和国际贸易带来不利影响。[②] 同时，严苛的数据本地化要求有可能会引起国外对等性保护主义，亦即中国企业走出去很有可能受到其他国家的同等限制。不久的将来，中国互联网企业将大规模走向海外，基于对等限制的国外市场限制可能是今后中国企业面临的一个重要挑战。数据本地化显然也能带来可以预见的负面影响，但是基于当前的需要，我们又不得不保持战略目标的优先性。

由于巨大的网民数量，[③] 中国数据产生量远远高于世界平均水平。根据国际数据公司（IDC）测算，中国数据产生量几乎占到世界的五分之一。[④] 通过“发挥数据的基础资源作用和创新引擎作用”[⑤]，服务于建构以数据为关

① 国务院：《促进大数据发展行动纲要》，新华网，2015 年 9 月 5 日，http://www.xinhuanet.com/politics/2015-09/05/c_1116464516.htm?from=groupmessage。

② 麦肯锡指出，数据流动过去十年里给全球 GDP 贡献了大约 3%的增长，参见 McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*。欧盟国际政治经济中心（ECIPE）指出，实施数据本地化立法措施将会使中国 GDP 降低 1.1%，参见 Matthias Bauer et al., “The Costs of Data Localisation: Friendly Fire on Economic Recovery”。数据跨境与国际贸易紧密相连，当做出数据本地化政策要求的时候，往往会产生更深远的贸易保护主义指控，近期中美贸易摩擦便是一例。2017 年 9 月，美国向 WTO 贸易服务委员会提交针对中国网络安全法即相关措施的申辩文件，其中主要指出中国的数据本地化储存措施将会对跨国贸易服务产生严重负面影响。参见美国向 WTO 贸易服务委员会提交的申辩文件：WTO, *Measures Adopted and Under Development by China Relating to Its Cybersecurity law*, S/C/W/374, 26 September 2017。

③ 截至 2020 年 3 月，中国网民数量达到 9.04 亿，而截至 2019 年底全球网民数量大约 41 亿，中国超过全球总数的五分之一。参见 CNNIC：《第 45 次中国互联网络发展状况统计报告》，2020 年 4 月；ITU, *Measuring Digital Development: Facts andFfigures 2019*, November, 2019。

④ IDC, *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in The Far East*, December, 2012.

⑤ 习近平：《实施国家大数据战略 加快建设数字中国》，新华网，2017 年 12 月 9 日，http://www.xinhuanet.com/2017-12/09/c_1122084706.htm。

键要素的数字经济，将大量的数据留在国内显然也是符合国家战略的一个现实选择。海量的数据将成为中国科技进步的驱动力，或者说是不可或缺的基本要素。同时，数据保护也是保障国家安全的直接选择。

（三）数据主权的表达与落地

中国的数据跨境流动规制是网络主权的代表性实践之一，它使网络边界清晰化。数据跨境流动规制立法在网络主权原则的指导下，更多被视为国家内部的互联网管理事务，体现为对数据主权的主张。国家视数据为国家基础性战略资源，自然适用主权原则。因此，用国家疆界划出数据流动的管辖边界被视为国家主权的应有之义。数据本地化是数据主权的规则表达，而数据主权通过网络主权完成了理论建构。

与欧盟和美国的长臂管辖不同，中国是基于管辖权范围而进行规制的。这是防御主义的逻辑，与网络主权的逻辑是一致的。《网络安全法》第 2 条规定，“在中国境内建设、运营、维护和使用网络以及网络安全的监督管理，适用该法”，这一带有明显属地色彩的规定具有自我设限的特征，可限制中国法律的域外管辖，但反过来也会激励监管者采取数据本地化措施，以确保《网络安全法》得以适用。[①] 同时，中国要求在华跨国互联网公司与本地公司合资运营数据存储以及云计算业务便是相关的实际行动。[②]《网络安全法》出台前后三次引起国际相关团体的关切，其重点指向了数据本地化存储政策。[③] 但是中国最终坚持了自己的原则，并没有因为国外势力或机构抗议而延缓进程。可以说，这是网络主权原则在立法层面首次得到最全面的贯彻。

网络主权往往是互联网后发国家的自我防护手段。数据主权作为网络主权的核心主张，数据本地化同样带有强烈的防御色彩。也就是在这个意义上，中国坚定地发展自己的数据本地化存储方案并不是要将自己游离于国际互

① 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 189 页。

② 近几年，在云计算领域，外国公司纷纷与中国公司合资运营，较为有名的案例如苹果与云上贵州、微软与世纪互联、亚马逊与光环新网等。

③ 例如，2017 年 5 月 15 日，54 个国际商业机构联名发表公开信，呼吁中国推迟实施《网络安全法》；2017 年 9 月 25 日，美国正式向 WTO 会提交针对中国《网络安全法》相关措施的申辩文件。

联网治理体系之外，而是在自我保护的前提下参与国际交往。这种积极的国际交往诉求体现在立法过程和国家合作倡议之中。《网络安全法》立法过程中，有全国人大常委会委员提出，“在限制关键信息基础设施的重要数据在境外储存或者向境外提供的同时，也应该考虑国家合作中信息和数据交换共享的需要”[①]。《网络安全法》草案从第一稿就为国际合作留下空间，规定“法律、行政法规另有规定的，依照其规定。”值得关注的是，中国正在积极推进数字丝绸之路建设，加速与“一带一路”沿线国家的数字贸易往来。中央网信办网络协调局负责人在立法说明记者会上指出，《网络安全法》关于数据境内留存和出境评估的规定，不是要阻止数据跨境流动，更不是要限制国际贸易，数据跨境流动是推进“一带一路”建设的必要条件。[②] 2017 年 6 月，中国（贵州）“数字丝路”跨境数据枢纽港启动建设，同年中国主导发起《“一带一路”数字经济国际合作倡议》，旨在拓展“一带一路”沿线国家的数字经济领域合作。数据跨境传输安全管理试点也在国家和地方层面开展探索。2020 年，商务部提出在条件相对较好的试点地区开展数据跨境传输安全管理试点，指定北京、上海、海南、雄安新区负责推进。

五、中国制定数据跨境流动政策的关键

进入 21 世纪后，全球数据本地化浪潮此起彼伏，数据跨境流动的共识和规则依然欠缺。[③] 由于数据流动反而因此遵从地理国家边界线而画出网络空间的国家地图，导致对互联网碎片化的担忧不绝于耳。[④] 从这个意义上说，

① 《十二届全国人大常委会第二十一次会议审议网络安全法草案二审稿的意见》，杨合庆主编：《〈中华人民共和国网络安全法〉释义》，第 212 页。

② 国家网信办：《〈网络安全法〉施行前夕国家互联网信息办公室网络安全协调局负责人答记者问》，中国网信网，2017 年 5 月 31 日，http://www.cac.gov.cn/2017-05/31/c_1121062481.htm。

③ 参见龙坤、朱启超：《网络空间国际规则制定——共识与分歧》，《国际展望》2019 年第 3 期，第 35—54 页。

④ William Drake, Vinton Cerf, and Wolfgang Kleinwächter , “Internet Fragmentation: An Overview,” World Economy Forum, Future of the Internet Initiative White Paper, January 2016; and Milton E. Mueller, *Will the Internet Fragment?* New York: Polity, 2017.

规制跨境数据流正是网络空间国家控制权竞争的重要途径，是互联网全球治理所面临的时代挑战，也是中国在新形势下不得不直面的难题。2016 年《网络安全法》确定了数据本地存储、出境评估制度，但是相关配套法规的制定仍处于持续讨论中，数据跨境流动制度如何落地依然是一个重要的挑战。[①] 基于本文的实证分析和对跨境数据流动的本质性认识，中国数据跨境流动政策的设计应包括以下几个关键考量。

第一，从总体哲学高度提炼数据治理的意涵，赋予跨境数据流动治理中国智慧。从根本上讲，参与全球治理体现的是一国在享用全球治理成果时对世界所做的贡献，意味着世界各国都有责任和义务致力于各种全球性问题的解决。[②] 对数据流动的认识也就是对互联网和网络空间的认识，数据治理是网络空间治理的根本。网络空间是一个整体，在这样的网络空间里，中国应继续以“大者为下”的姿态，海纳百川地接纳全球数据流动，创造一个有序流动的数字世界。这是面向未来全球数据治理的中国哲学意涵。

第二，从消极被动转为积极主动，为数据跨境流动国际治理提供公共产品。数据本地化是一种策略性选择，并不是一成不变。随着自身禀赋和外部环境的变化，也就是国际均势的变化，特别是美国对华战略已经呈现出步步紧逼的进攻性，未来中国需要依据条件逐步去除消极防御色彩，更为主动地参与国际规则建构。作为新兴大国，中国应为数据跨境流动提供一种具有代表性的公共治理产品，即寻求最大公约数，建立一种以公平正义为依归，以效率发展为路径的跨境数据有序自由流动秩序。这种公共治理产品应该包含规则（rule）和标准（standard/protocol），也就是国际规则和技术方案，前者以网络主权为核心，后者以区块链信任协议技术为代表。同时，必须关注新技术带来的影响，既有的数据政策和理念均是围绕旧技术作出的假设，[③] 未来云计算、大数据、人工智能甚至量子计算技术的进一步发展将提出新的

① 2016 年通过的《网络安全法》第 37 条规定了数据本地化制度，但是制度落地的配套措施的出台却并非一帆风顺。2019 年 6 月，国家网信办出台新的评估办法征求意见稿，在安全评估思路上做出重大调整。目前具体的制度设计依然在讨论中。

② 张宇燕：《全球治理的中国视角》，《世界经济与政治》2016 年第 9 期，第 5—6 页。

③ 理查德•泰勒：《数据主权和数据跨境流动：数据本地化论战》，载张彬主编：《数字经济时代网络综合治理研究》，北京邮电大学出版社 2020 年版，第 189 页。

挑战和机遇，中国有必要进行前瞻性的评估和设计。不过，中国方案需要用实践来检验，“一带一路”倡议不失为一个好的突破口，可提升既有合作基础，加强规则建构。

第三，更具智慧地设计国内制度，提供更为立体灵活的机制安排。目前中国数据跨境流动制度在多重因素下初步成型，但是制度细节依然在酝酿和讨论之中，特别是数据出境安全评估制度设计正处于关键期。制度设计是一种精细的艺术，在国内制度设计中需要秉持比例原则和平衡原则，统筹考虑国家、市场以及社会三个层次的利益需求，积极寻求最合理方案。多元灵活安排更有利于应对数字时代的挑战，为今后发展留出战略空间。可以借鉴欧盟的丰富经验，为数据跨境流动提供更为立体的机制安排。应充分利用现有资源，通过多边合作机制寻求国际合作空间，通过国内自贸区试点开展数据安全跨境机制探索。[①] 同时值得注意的是，应审慎对待欧盟 GDPR 的全球示范效应，审慎立法，防止负面效果，恰当防御，谋求国家的长远发展。[②]

[责任编辑：樊文光]

① 全球范围内已经出现了不少跨境数据流动的新探索，值得研究借鉴，比如爱沙尼亚和卢森堡签订的“数据大使馆”以及巴林提出的基于数据外交豁免的国际数据中心建设法案。

② Martina Ferracane and Erik van der Marel, “Do Data Policy Restrictions Inhibit Trade in Services?” Research Paper, No. RSCAS 2019/29, Robert Schuman Centre for Advanced Studies, April 2019.