跨境数据流动的全球治理

——进展、趋势与中国路径

刘宏松　　程海烨

【内容摘要】 跨境数据流动领域并未形成全球性规制体系。国际机制因缺乏效力、难以平衡良好的数据保护和跨境数据自由流动、无法保持自身独立性等问题，并未达到理想的治理效果。当前，跨境数据流动治理主要在欧盟和美国两个独立法域内实施，但美国和欧洲在价值理念和规制模式上的根本性差异、数字化企业竞争，在隐私保护、境外管辖权和数字服务税等问题上产生了难以弥合的分歧。在此情形下，跨境数据流动的全球治理呈现两个发展趋势，一是规制多极化和规制标准的俱乐部化，二是美欧将继续争夺跨境数据流动规制的主导权。作为全球第二大数字经济体，中国同美国和欧盟一样，也是跨境数据流动议题领域的一个重要行为体。面对上述发展趋势，中国正加快参与跨境数据流动的全球治理步伐。目前，中国可通过加入亚太经济合作组织框架下的跨境隐私规制体系、与《一般数据保护条例》的实施方欧盟进行规制协调、将中国跨境数据流动规制体系推向“一带一路”沿线国家三条路径，积极参与跨境数据流动的全球治理。

【关键词】 跨境数据流动　数据保护　数字经济　全球治理　中国路径

【作者简介】 刘宏松，上海交通大学国际与公共事务学院教授（上海　邮编：200030）；程海烨，上海外国语大学国际关系与公共事务学院博士研究生（上海　邮编：200083）

【中图分类号】 F11　　**【文献标识码】** A

【文章编号】 1006-1568-(2020)06-0065-24

【DOI 编号】 10.13851/j.cnki.gjzw.202006004

联合国《2019 年数字经济报告》指出，数字经济已成为全球经济发展和贸易增长的新动能。[①] 作为数字经济驱动的产物，跨境数据流动[②]（transborder data flow）通过提高生产和流通效率推动全球经济增长。据估计，2009—2018 年，全球跨境数据流动拉动的经济增长占全球 GDP 总量的 3%，相当于 2.3 万亿美元，使全球 GDP 增长 10.1%，预计到 2025 年其为全球 GDP 贡献的价值将达到 11 万亿美元。[③]

目前，跨境数据流动治理领域并未形成全球性规制体系。经济合作与发展组织（OECD）、亚太经济合作组织（APEC）、二十国集团（G20）和世界贸易组织（WTO）等国际机制，成为参与全球跨境数据流动治理的主要多边机制。美国和欧盟作为两大独立法域，正积极开展跨境数据流动治理和规制协调。作为世界第二大数字经济体，[④] 中国在跨境数据流动治理领域扮演着重要角色，而其他发展中国家的数字经济水平不及中国，在跨境数据流动治理领域的影响力有限。因此，本文将聚焦 OECD、APEC、G20 和 WTO 等多边机制、美国和欧盟两大独立法域以及中国在跨境数据流动治理领域发挥的作用。

---

① 《2019 年数字经济报告》，联合国贸发会议网站，2019 年 9 月 4 日，https://unctad.org/en/PublicationsLibrary/der2019_overview_ch.pdf。

② 跨境数据流动主要有两层含义：第一层是指个人数据发生移动和位置转移至第三国；第二层是指数据虽然没有跨越国界，但允许被第三方主体访问。以下国际机制对“跨境数据流动”（cross-border data flow / transborder data flow）提出明确界定。1980 年 9 月，OECD 发布《关于隐私保护和跨境个人数据流动指南》（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data），其中的第 1 条第 3 款将“跨境个人数据流动”定义为“跨越国家界限的个人数据移动”。1984 年，联合国跨国公司中心（UNCTC）将“跨境数据流动”定义为“一种能够跨越国界开展对计算机可读的数据进行处理、存储和读取的活动”。1985 年，OECD 在《跨境数据流动宣言》（Declaration on Transborder Data Flows）首次对“跨境数据流动”做出法律解释，即“计算机化的数据或者信息在国际层面的流动”。

③ 参见 Joshua P. Meltzer and Peter Lovelock, “Regulating for A Digital Economy: Understanding the Importance of Cross-border Data Flows in Asia,” The Brookings Institution, March 20, 2018, p. 8, https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_working-paper.pdf; James Manyika et al., “Digital Globalization: The New Era of Global Flows,” McKinsey Global Institute, March 2016, pp. 74-83, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows。

④ 欧盟整体没有计入全球数字经济体排名。参见中国信息通信研究院：《全球数字经济新图景（2019）》，中国信通院网站，2019 年 10 月，第 9 页，http://www.caict.ac.cn/kxyj/qwfb/bps/201910/P020191011314794846790.pdf。

既有研究以美国和欧盟为主要研究对象，围绕立法规制、数据主权与隐私安全、数据民族主义、数字贸易等议题展开讨论，而且大多将跨境数据流动视为网络空间治理的一个分支议题，忽视了其数据主权之外的数字经济特质。[①] 与此类研究不同，本文将研究视域扩展到全球层面的多边规制行动，并关注跨境数据流动的数字经济特质。本文将首先理清 OECD、APEC、G20 和 WTO 等国际机制开展的多边规制行动及其面临的困境，继而探讨美国和欧盟在跨境数据治理领域的分歧及其主要原因，并在此基础上分析跨境数据流动的全球治理发展趋势，最后提出作为世界第二大数字经济体的中国参与跨境数据流动治理的可行路径。

一、既有多边规制行动及其困境

尽管联合国发布了《计算机处理的个人数据文档规范指南》，[②] 但该指南仅对个人数据存档给予规范性指导，并不涉及跨境数据流动的全球治理。在这一领域，OECD、APEC、G20 和 WTO 等国际机制开展了多边规制行动。

（一）既有多边规制行动

第一，鼓励跨境数据流动，推动全球数字经济发展。OECD、APEC 和 WTO 等组织通过制定跨境数据流动规则，释放全球数字经济发展潜力。OECD 是全球首个提出跨境数据流动执行原则的国际组织。其在 1980 年发布的《隐私保护和跨境个人数据流动指南》（以下简称《OECD 指南》（1980））中指出，成员国应避免以保护个人隐私和自由的名义，限制跨境数据自由流

① 参见 Eriksson Johan and Giampiero Giacomello, “The Information Revolution, Security, and International Relations Relevant Theory,” *International Political Science Review*, Vol.27, No. 3, 2006, pp. 221-244；沈逸：《后斯诺登时代的全球网络空间治理》，《世界经济与政治》2014 年第 5 期，第 144—155 页；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；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。

② 该指南对各成员国规范计算机处理个人数据文档提出要求。参见 UN General Assembly, “Guidelines for the Regulation of Computerized Personnel Data Files,” December 14, 1990, https://www.refworld.org/docid/3ddcafaac.html。

动。[①] APEC 通过 2005 年发布、2015 年修订的《APEC 隐私框架》指导亚太地区跨境数据自由流动。[②] WTO 作为全球首要多边贸易机制，主要通过减免数字产品关税、推动跨境数据自由流动，来促进全球范围内信息技术产品的自由贸易。目前，82 个 WTO 成员已签署《信息技术产品协议》（Information Technology Agreement, ITA），尝试取消一系列计算机、软件和电子通信产品关税，促进世界范围内信息技术产品的贸易自由化，为跨境数据流动提供更好的技术保障。[③] G20 则积极倡导各成员国抓住数字机遇，推动全球经济实现包容性发展。各国在 2016 年 G20 杭州峰会上发起《二十国集团数字经济发展与合作倡议》，为释放更多的数字经济潜力、应对数字鸿沟创造更多有利条件。[④]

第二，构建与数字经济发展相匹配的数据隐私保护框架和数字技术信任体系，消除跨境数据流动壁垒。OECD 将个人隐私看作公民的基本权利，倡导构建能够推动跨境数据流动的数据隐私保护框架。《OECD 指南》（1980）强调各成员国应当确保个人数据在跨境流动中安全的可持续性。[⑤] APEC 则重视同时建立消费者信任的数据隐私保护框架和数字技术信任体系。《APEC 隐私框架》启动了跨境隐私规则（Cross-Border Privacy Rules, CBPR）体系，通过设立以“保护个人隐私、获得消费者信任”为宗旨的“问责代理”机构，在确保企业符合 APEC 隐私保护标准的同时，提升消费者对电子信息平台的信任。[⑥] G20 的各成员也在构建数据隐私保护框架与数字技术信任体系上达成了共识。在 2017 年 G20 汉堡峰会和 2018 年 G20 布宜诺斯艾利斯峰会上，

① OECD, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” September 1980, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

② APEC, “APEC Privacy Framework 2015,” August 2017, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015); APEC, “APEC Privacy Framework 2005,” December 2005, https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

③ 《信息技术产品协议》，世贸咨询网，2013 年 10 月 16 日，http://chinawto.mofcom.gov.cn/article/ap/p/201412/20141200838293.shtml。

④《二十国集团数字经济发展与合作倡议》，G20 网站，2016 年 9 月 20 日，http://www.g20chn.org/hywj/dncgwj/201609/t20160920_3474.html。

⑤ 《OECD 指南》（1980）第三部分第 16 条，参见 OECD, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”。

⑥ APEC, “What is the Cross-Border Privacy Rules System?” April 15, 2019, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

各国领导人承诺，将致力于建设保护个人隐私的法律框架，并不断重申打造消费者信任的数字技术体系的重要性。[①] WTO 则致力于确保跨境数据的流动体现数字贸易的公平性，构建数字贸易信任体系。例如，WTO《服务贸易总协定》（GATS）强调市场准入义务和国民待遇义务；其附加协议《关于电信服务的附件》（Annex on Telecommunications）第 5 条还规定，即使 WTO 成员没有开放本国的电信市场，也要确保本国的公用电信网络符合非歧视原则。[②]

第三，关注跨境数据流动规制的风险管控和互操作性。《OECD 隐私框架》（2013）提出了国家隐私战略（national privacy strategies）、隐私管理程序（privacy management programs）和安全漏洞通知（security breach notification）三个概念，强调对个人隐私的风险管控及全球层面隐私监管的互操作性。[③]《APEC 隐私框架》下的 CBPR 体系要求申请加入的企业所在国至少有一个隐私执法机构加入跨境隐私执法安排（Cross-border Privacy Enforcement Arrangement, CPEA），监督参与跨境数据流动企业的隐私保护情况，提升各经济体隐私执法机构的互操作性。[④] 在前三届峰会成果基础上，2019 年《二十国集团领导人大阪峰会宣言》提出，不仅要创新数字化产业和新兴技术，还要创新跨境数据流动的风险监管，弥合数字鸿沟等。[⑤]

（二）既有多边规制面临的困境

上述国际机制在跨境数据流动治理领域开展了一系列行动，但也面临以

① 参见 G20, “G20 Leaders’ Declaration: Shaping an Interconnected World,” July 7, 2017, https://www.g20germany.de/Content/EN/_Anlagen/G20/G20-leaders-declaration_nn=2186554.html; G20, “G20 Leaders’ Declaration: Building Consensus for Fair and Sustainable Development,” November 30, 2018, https://g20.argentina.gob.ar/en。

② WTO, “General Agreement on Trade in Services,” 1995, https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm.

③ OECD, “The OECD Privacy Framework 2013,” July, 2013, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

④ 目前，有 8 个国家（地区）的 22 个隐私执法机构加入了跨境隐私执法安排（CPEA），其中包括美国联邦贸易委员会、日本 15 个隐私执法部门以及澳大利亚、新西兰、加拿大等。参见弓永钦、王健：《APEC 跨境隐私规则体系与我国的对策》，《国际贸易》2014 年第 3 期，第 30—35 页；APEC, “APEC Privacy Framework 2015”。

⑤ “G20 Osaka Leaders’ Declaration,” Japanese Foreign Ministry, June 28, 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.

下三个困境。

第一，效力不足。《OECD 隐私框架》（2013）是指导性框架，仅为全球跨境数据流动提供了建设性指导方针。该框架第 6 条指出，“各成员国应达到个人隐私保护及个人自由的最低标准，”[①] 但并没有提出具体和明确的要求，也不具备法律效力。《APEC 隐私框架》属于自愿性框架协议，且只有自愿加入 CBPR 体系，并通过 CPEA 认证，达到 APEC 对消费者隐私保护要求的企业，才能从法律意义上保护消费者隐私。[②] G20 是跨境数据流动的全球治理倡议平台，没有强制执行机制。尽管各成员国对数字经济展开较多讨论，提出跨境数据自由流动的理想模式，但并未形成良好的多边规制体系来约束成员国行为。WTO 框架下的 GATS 虽对成员国有约束力，但因其部分条例相互矛盾，法律效力在一定程度上遭到削弱。例如，GATS 第 2 条规定了成员国的最惠国待遇，但第 7 条却允许成员国对来自不同国家或地区的服务提供商实行差别对待。[③] 此外，GATS 并未取得令人满意的执行效果。大多数成员国仅根据 GATS 做出承诺，并未付诸实际行动。[④]

第二，难以平衡良好的数据保护和跨境数据自由流动。数据保护和跨境数据自由流动，如同天秤的两端，天秤偏向任何一端，都会对另一端造成消极影响。OECD、APEC、G20 和 WTO 都未能在两大目标之间实现平衡。《OECD 指南》（1980）、《OECD 隐私框架》（2013）虽在前言部分强调尊重个人隐私的重要性，承认数据保护是各国开展跨境数据自由流动的前提，但事实上，OECD 更加偏重跨境数据自由流动。[⑤] APEC 反对为跨境数据流动设置障碍，主张成员国只需达到数据保护的最低标准。《APEC 隐私框架》序言第 3、4 条明确提出，限制数据自由流动或对其设置障碍会对全球贸易产生不利影响，要求各成员国“确保”数据能够自由流动，仅表示“鼓

① OECD, “The OECD Privacy Framework 2013.”
② APEC, “APEC Privacy Framework 2015.”
③ WTO, “General Agreement on Trade in Services.”
④ 张玉环：《WTO 争端解决机制危机：美国立场与改革前景》，《中国国际战略评论》2019 年第 2 期，第 105—119 页。
⑤ 例如，《OECD 指南》（1980）第 17 条指出成员国不应限制个人数据的跨境流动；第 18 条指出成员国应避免以保护隐私和个人自由的名义，阻碍跨境数据的自由流动等。参见 OECD, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”。

励”数据保护。[①] G20 成员对是否应在数据充分保护的前提下开展跨境数据自由流动存在分歧。[②] WTO 虽然在数据隐私保护方面采取了规制行动，但总体上偏重于跨境数据自由流动。尽管 WTO 正对 GATS 进行改革，试图通过与互联网治理机构开展合作来降低数字服务的网络安全风险，但目前看来，WTO 的规制重点仍是推动跨境数据流动、促进数字贸易自由化。[③]

第三，既有多边规制受到欧盟和美国两大规制体系的影响，无法保持自身独立性。《OECD 指南》（1980）是参照欧洲尊重个人隐私权的价值导向制定的。以德国和法国为代表的欧盟成员国，始终坚持将个人的尊严、自由和安全置于首要位置，主张通过严格的法律法规加强对个人隐私的保护。《APEC 隐私框架》及 CBPR 体系则带有很强的美国色彩，强调构建以市场为主导、以跨境数据流动为目标的规制体系。[④] 目前，部分国家担心如果完全接受 OECD 和 APEC 规制体系，会成为欧盟和美国两大法域竞争的“牺牲品”。因此，印度、俄罗斯、阿根廷、巴西、伊朗等新兴和发展中经济体为维护本国数据本地化处理的自主权开展了相关立法工作。[⑤]

二、美欧两大规制体系的分歧及其主要原因

既有多边规制面临上述困境，意味着跨境数据流动的全球治理并没有真正实现。当前，跨境数据流动治理主要在欧盟和美国两个独立法域内实施。欧盟和美国拥有庞大的数字市场规模。2018 年，美国数字产业化规模高达 1.5 万亿美元，其产业数字化规模达到 10.8 万亿美元。欧盟成员国中的两大

① 参见 APEC, “APEC Privacy Framework 2015;” Graham Greenleaf and David Lindsay, *Public Rights*, Cambridge: Cambridge University, 2018, pp. 91-120。

② 阿里巴巴数据安全研究院：《全球数据跨境流动政策与中国战略研究报告》，中国大数据网站，2019 年 9 月 1 日，http://www.chinabigdata.com/cn/contents/3/253.html。

③ Andrew D. Mitchell and Neha Mishra, “Regulating Cross-Border Data Flows in a Data Driven World: How WTO Law Can Contribute,” *Journal of International Economic Law*, Vol. 22, No.3, 2019, pp. 389-416.

④ APEC, “APEC Privacy Framework 2015.”

⑤ Nigel Cory, “Cross-Border Data Flows: Where are the Barriers and What Do They Cost,” ITIF, May 1, 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

巨头德国和法国的数字产业化规模分别为 2 410 亿美元和 1 728 亿美元，产业数字化规模分别达到 2.15 万亿美元和 9 822 亿美元。[①] 欧盟和美国凭借庞大的市场规模，成为跨境数据流动议题领域的重要行为体。

（一）美欧两大规制体系的分歧

尽管美国和欧盟之间在开展跨境数据流动领域先后达成了《安全港协议》（Safe Harbor Framework）和《隐私盾协议》（Privacy Shield Framework），但双方在隐私保护、境外管辖权和数字服务税等问题上的分歧难以弥合。

第一，隐私保护问题。自 2013 年“棱镜门事件”后，美国脸书（Facebook）公司在 2014 年又被指控向美国政府泄露用户的个人数据。[②] 由此，2015 年 10 月 6 日，欧洲法院做出了废除《安全港协议》的判决，[③] 明确指出美国在执行该协议时，将其国家安全、公共利益和执法需要置于更高位置，在公民隐私数据泄露时漠视监管要求。[④] 《安全港协议》的废除标志着美欧在跨境数据流动领域的冲突达到了顶点。尽管双方此后又达成了《隐私盾协议》，但欧盟数据保护委员会（EDPB）对该协议执行和监管的评估结果并不满意，认为美国方面缺乏实质性监督。[⑤] 2020 年 7 月 16 日，欧洲法院判决《隐私盾协议》的适用性无效，这意味着脸书、谷歌等诸多美国企业将被迫停止与欧盟开展跨大西洋数据流动。[⑥] EDPB 认为，自脸书泄露用户信息事件发生后，美国至今并未对国内数据隐私保护做出根本性调整。目前看来，美欧双方实现进一步协调的可能性微乎其微。

第二，境外管辖权问题。欧盟以“地理区域”为基准，对境内外凡是使

① 中国信息通信研究院：《全球数字经济新图景（2019）》，第 15—18 页。

② 《5000 万用户信息泄露，脸书失去对数据的控制？》，新华网，2018 年 3 月 24 日，http://www.xinhuanet.com/world/2018-03/21/c_129833176.htm。

③ Federal Trade Commission, “Updated on the U.S.-EU Safe Harbor Framework,” July 25, 2016, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

④ Yann Padova, “The Safe Harbor is Invalid: What Tools Remain for Data Transfer and What Comes Next?” *International Data Privacy Law*, Vol. 6, No. 2, 2016, pp. 139-161.

⑤ EDPB, “EU-U.S. Privacy Shield-Third Annual Joint Review Report,” November, 2019, https://edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en.

⑥ Court of Justice of the European Union, “The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield,” July 16, 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

用欧盟数据的企业都实施监管。GDPR 的“长臂管辖”条例明确规定，即使数据控制者或处理者不在欧盟境内设立实体机构，只要涉及欧盟业务，也需接受欧盟的监管。[①] 此外，大多数云服务提供商必须与客户签订合同，保证数据从欧盟转移到美国时接受欧盟的监管。[②] 美国则以“国籍管辖”为基准，对境内外所有美国企业实行数据流动监控和管辖。为了打破 GDPR 长臂管辖的约束，美国于 2018 年出台了《澄清域外合法使用数据法》（CLOUD Act），将美国对跨境数据流动的司法管辖权由“数据所在地”更改为“数据控制者所在地”，规定“无论通信、记录或信息存储是否在美国境内，服务提供商都应根据电子通信法律，保存、备份或记录信息等”。也就是说，此后美国在开展跨境搜查时，微软公司需要向美国相关部门提交其存储在爱尔兰的用户电子邮件内容。[③] 这势必加剧美欧在跨境数据管辖权问题上的冲突。

第三，数字服务税问题。在数字经济背景下，传统国际税收秩序面临双重挑战。一方面，跨境数字交易呈现无边界状态，影响了以地理为基准的传统国际税收范围。互联网企业可以在税率相对较低的国家或地区缴税，抵扣税率相对较高国家或地区应缴金额，从而合法规避高额税款。另一方面，跨国企业可以重新配置以数据为主的无形资产结构，实现全球利润最大化。[④]

---

① “长臂管辖”（long-arm jurisdiction）指《一般数据保护条例》（GDPR）第 3 条：适用于设立在欧盟内的控制者或处理者对个人数据的处理，无论其处理行为是否发生在欧盟内。参见 The European Parliament and the Council, “General Data Protection Regulation,” Intersoft Consulting, May 2018, https://gdpr-info.eu/; Christopher Kuner, “Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law,” *International Data Privacy Law*, Vol. 5, No. 4, 2014, pp. 235-245; 刘天骄：《数据主权与长臂管辖的理论分野与实践冲突》，《环球法律评论》2020 年第 2 期，第 180—192 页。

② See EDPB, “Guidelines 3/2018 on the territorial scope of the GDPR (Article 3),” November 12, 2019, https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en; and Peter Church, Caitlin Potratz, “U.S. Cloud Act and GDPR,” Linklaters, September 13, 2019, https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe.

③ U.S. Department of Justice, “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of The CLOUD ACT White Paper,” April, 2019, https://www.justice.gov/opa/press-release/file/1153446/download; The United States Department of Justice, “Division V-CLOUD Act,” March 21, 2018, https://www.justice.gov/dag/page/file/1152896/download.

④ 参见唐巧盈：《全球数字税：国际规则制定的新桥头堡》，《光明日报》2020 年 6 月 11 日，第 14 版；贾开：《“数字税”全球治理：双重挑战与未来变革》，腾讯新闻网，2020 年 3 月 28 日，https://new.qq.com/omn/20200328/20200328A0LFR800.html。

例如，2010 年，美国互联网跨国巨头谷歌公司被披露通过转移定价实现利润的全球转移与再分配，合法避税近 600 亿美元。[①] 为了应对挑战，从 2018 年 3 月开始，欧盟委员会发起了关于数字服务税的立法提案，拟调整对大型互联网企业的征税规则。西班牙、奥地利和法国等欧盟成员国也开展了数字服务税方面的立法工作。2019 年 1 月，西班牙政府内阁会议通过数字服务税计划，准备对全球年收入超过 7.5 亿欧元和在西班牙年收入超过 300 万欧元的公司征收 3%的新税；2019 年 4 月，奥地利财政部长在内阁周例会上公布了“一揽子数字征税”计划；2019 年 7 月，法国参议院通过了数字服务税草案，全球首部数字服务税法落地实施。[②]

欧盟部分成员国征收数字服务税的单边行动，引起了美国的强烈不满。美国反对欧洲国家的征税方式和征税范围，认为其仅对数字广告和跨境数据流动征收数字服务税是出于贸易保护目的。[③] 因此，美国启动“301 条款”对法国进行调查，并对价值 13 亿美元的法国商品征收 25%的报复性关税。[④] 同时，美国借助 OECD、G20 等多边机制推动国际税制改革，如 2013 年发布的 OECD《税基侵蚀和利润转移行动计划》（BEPS）、[⑤] 2020 年发布的《OECD/G20 关于实现包容性数字税框架的“双支柱”路径的声明》[⑥] 等标志性文件，鼓励各国签署一致性国际税制改革协定，实现征税权的重新配置，促进反税基侵蚀的全球合作，应对数字服务税带来的挑战。[⑦] 然而，上述指

① Josse Drucker, “Google 2.4% Rate Shows How $60 Billion is Lost to Tax Loopholes,” Bloomberg, October 21, 2010, https://www.bloomberg.com/news/articles/2010-10-21/google-2-4-rate-shows-how-60-billion-u-s-revenue-lost-to-tax-loopholes.

② 中国信息通讯研究院：《全球数字经济新图景（2019）》，第 6—7 页。

③ 孙南翔：《全球数字税立法时代是否到来》，《经济参考报》2019 年 8 月 7 日，第 8 版。

④ Jim Tankersley, “U.S. Will Impose Tariffs on French Goods in Response to Tech Tax,” *The New York Times*, July 10, 2020, https://www.nytimes.com/2020/07/10/business/us-will-impose-tariffs-on-french-goods-in-response-to-tech-tax.html.

⑤ OECD, “Action Plan on Base Erosion and Profit Shifting,” 2013, https://www.oecd.org/ctp/BEPSActionPlan.pdf.

⑥ OECD, “Statement by the OECD/G20 Inclusive Framework on BEPS on the Two-Pillar Approach to Address the Tax Challenges Arising from the Digitalization of the Economy,” January 2020, http://www.oecd.org/tax/beps/statement-by-the-oecd-g20-inclusive-framework-on-beps-january-2020.pdf.

⑦ 贾开：《“数字税”全球治理：双重挑战与未来变革》。

导性改革方案并未实质性解决美欧双方在数字服务税问题上的分歧。[①]

（二）美欧两大规制体系产生分歧的主要原因

美欧两大规制体系在价值理念和规制模式上的根本性差异，导致其在隐私保护和境外管辖权等问题上产生了分歧。美欧因数字服务税产生的分歧则是双方争夺数字化企业竞争优势的表现。

第一，美、欧两大规制体系在价值理念和规制模式上存在根本性差异。

在价值理念方面，欧盟将个人隐私保护视为开展跨境数据流动的前提条件，并将构建法律规制体系作为保护个人隐私必不可少的手段。[②] 1950 年，欧洲国家就已经达成了专门保障公民基本权利的《欧洲保障人权和基本自由公约》；[③] 自 20 世纪 60 年代起，旨在保护个人隐私的《关于自动化处理个人信息保护公约》（以下简称“《第 108 号公约》”）[④] 以及奉行“充分保护”原则的《数据保护指令》（1995）[⑤] 相继生效。欧盟跨境数据流动规制体系逐步建立，涉及数据保护的法律文件亦愈发严格。在 2016 年的《数字化单一市场版权指令》[⑥] 指引下，欧洲理事会和欧洲议会批准了《一般数据保护条例》（GDPR）。该条例通过执行“单套规制”[⑦] 来打造统一的规制

① 例如，在征税权管辖方面，美欧征税范围、税收制度等存在差异；在最低税率标准方面，美欧之间和欧盟内部各国都有不同的税基计算标准。此外，各国过于关注规避“双重征税”问题，却忽视了“双重不征税”情形。参见茅孝军：《从临时措施到贸易保护：欧盟“数字税”的兴起、演化与省思》，《欧洲研究》2019 年第 6 期，第 72 页。

② Holly Kathleen Hall, “Restoring Dignity and Harmony to United States-European Union Data Protection Regulation,” *Communication Law and Policy*, Vol. 23, No. 2, p. 145.

③ 该公约第 8 条提及“尊重公民隐私和家庭生活的权利”。参见 Council of Europe, “Convention for the Protection of Human Rights and Fundamental Freedoms,” *European Treaty Series*, No. 5, November 4, 1950, https://rm.coe.int/1680063765。

④ Council of Europe, “Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 108,” October 1981, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

⑤ 该指令第 25 条为“充分保护”原则，即跨境数据流动前，应先评估数据转移目的国是否满足数据充分保护的条件。参见 The European Parliament and the Council, “Data Protection Directive 1995,” EUR-Lex, October 24, 1995, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML。

⑥ European Commission, “Directive on Copyright in the Digital Single Market,” September 14, 2016, EUR-Lex https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX: 52016PC0593.

⑦ “单套规制”（one single set of rules）指《一般数据保护条例》不需要成员国在国家层面单独批准，可直接适用于欧盟所有成员国。参见方芳：《欧盟个人数据跨境流动政策的演变：市场统一与贸易规范》，《复旦国际关系评论》2019 年第 1 期，第 22 页。

体系，以高额罚金等惩罚性措施来加强数据保护。[①]

美国则将数字经济发展置于首位，致力于确保跨境数据自由、高效流动，以充分释放数据流动的经济效能。在美国看来，GDPR 对数据的保护过于严苛，既妨碍跨境数据自由流动，又会对数字经济发展造成不利影响。因此，自《隐私权法》[②] 颁布后，美国国内没有另行出台过于严格的数据隐私保护法律，仅针对特定的领域和人群提出保护用户个人信息的具体要求。例如，《电子通信隐私法》是一部旨在保护电子通信领域个人信息不受第三方窃听或拦截的法律；[③]《录像隐私保护法》规定，在电子视频传播时禁止公开个人可识别的盒式磁带或试听资料等信息；[④]《儿童网上隐私保护法》主要针对美国 13 岁以下的儿童群体，要求互联网企业遵守保护儿童上网信息的六项基本原则；[⑤]《加州消费者隐私法》则赋予加州公民四项新的隐私保护权利，将企业对用户数据的使用决定权归还消费者，使加州公民在消费时拥有更多的个人信息控制权。[⑥]

在规制模式方面，欧盟和美国采用不同的跨境数据流动规制模式。欧盟采用以地理区域为基准、充分保护为前提的事前防御规制模式。欧盟《第 108 号公约》第 12、14 条提出，缔约国间开展跨境数据流动时，应具有“同等水平”的数据保护力度。[⑦]《数据保护指令》（1995）则要求欧盟成员国在向第三方跨境数据流动前，先确认第三方的数据处理能力是否已达到“充

① “高额罚金”是指《一般数据保护条例》第 83 条。该条第 4 款规定，依照本条例第 2 款，违规者将被处以最高达 1000 万欧元的行政罚款，或对企业处以上一财政年度全球营业额总额 2%以下的行政罚款，且以较高的数额为准；该条第 5 款规定，依照本条例第 2 款，违规者将被处以最高达 2000 万欧元的行政罚款，或就一项经营而言，最高可处以上一财政年度全球年营业额的 4%，两者以较高数额为准。参见 The European Parliament and the Council, “General Data Protection Regulation”。

② U.S. Department of Justice, “Privacy Act,” 1974, https://www.justice.gov/opcl/privacy-act-1974.

③ EPIC, “The Electronic Communications Privacy Act,” 1986, https://epic.org/privacy/ecpa/.

④ EPIC, “Video Privacy Protection Act,” 1988, https://www.epic.org/privacy/vppa/.

⑤ U.S. Federal Trade Commission, “Children’s Online Privacy Act,” 1998, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy.

⑥ Californians for Consumer Privacy, “California Consumer Privacy Act,” 2018, https://www.caprivacy.org/.

⑦ Council of Europe, “Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 108.”

分保护”水平。[①] GDPR 第 3 条设置了长臂管辖条例，第 5 条则提出了个人数据处理原则，包括合法、公正、透明、数据使用最小化等处理方式。[②] 美国采用以国籍管辖为基准、问责制为前提的事后监管规制模式，通过行业自律的方式要求企业保障个人数据传输的安全性。[③] 此外，在美国推动下达成的 CBPR 体系也强调企业的责任意识，要求企业先进行自我评估，再接受问责代理机构的评估；如评估通过，则被认定为符合隐私保护标准的企业。欧盟和美国曾先后达成《安全港协议》和《隐私盾协议》，尝试协调双方不同的规制模式。[④] 由于美国泄露用户隐私事件频发，欧盟始终对《安全港协议》的数据保护效果持不信任态度，该协议最终被《隐私盾协议》所取代。《隐私盾协议》将规制对象扩展至美国政府及国家安全部门，救济机制从简单的商业纠纷解决条款转变为企业申诉和强制性终局仲裁，并增加了数据主体权利等内容；同时进一步明确了数据转移前的问责制、增加了对数据使用目的的限制、资源可信度原则等。[⑤] 然而，由于美国方面缺乏实质性监督，欧洲法院已判决其适用性无效。

第二，美国和欧洲争夺数字化企业竞争优势。与美国相比，欧盟的数字化企业竞争力存在一定差距。在 2019 年世界数字竞争力排名中，前 5 位分别是美国、新加坡、瑞典、丹麦和瑞士，德国和法国分别排在第 17 位和第 24 位。[⑥] 2019 年 6 月，欧盟委员会发布的《数字经济与社会指数》报告强调，欧盟各成员国在企业数字化方面存在较大差距，欧盟需要努力提升企业

① The European Parliament and the Council, “Data Protection Directive 1995.”

② The European Parliament and the Council, “General Data Protection Regulation.”

③ 许多奇：《个人数据跨境流动规制的国际格局及中国应对》，《法学论坛》2018 年第 3 期，第 131 页。

④ Yuko Suda, *The Politics of Data Transfer: Transatlantic Conflict and Cooperation over Data Privacy*, pp. 22-23; and William J. Long, Marc Pang Quek, “Personal Data Privacy Protection in an Age of Globalization: the US-EU Safe Harbor Compromise,” *Journal of European Public Policy*, Vol. 9, No. 3, 2002, p. 330.

⑤ U.S. Department of Commerce, “Privacy Shield Framework,” February 2016, https://www.privacyshield.gov/eu-us-framework.

⑥ 该排名基于以下三个指标：知识（knowledge）、技术（technology）和未来准备（future readiness），参见 International Institute for Management Development, “IMD World Digital Competitiveness Ranking 2019,” September 2019, https://www.imd.org/research-knowledge/reports/imd-world-digital-competitiveness-ranking-2019/。

的整体数字化实力，只有这样才能在全球舞台上与美国企业展开竞争。[①] 此外，由于脸书、优兔（YouTube）、推特（Twitter）等全球使用人数较多的社交平台均来自美国，[②] 欧盟对此有很强的商业危机感。在欧盟国家看来，以美国科技巨头为代表的数字化企业不断侵吞初创企业，影响了欧洲公平的竞争环境。同时，美国科技巨头掌握的大量有价值的数据信息，又使其逐渐形成数据获取与经济发展相互促进的良性模式。[③] 美国企业的良性发展模式会导致欧盟数字化企业的发展空间受到挤压，而征收数字服务税可以在一定程度上减少这种情况的发生。

三、跨境数据流动全球治理的发展趋势

鉴于既有多边规制面临诸多困境、美欧两大规制体系之间的分歧难以弥合，跨境数据流动的全球治理呈现以下两个发展趋势：一是规制多极化和规制标准的俱乐部化；二是美欧将继续争夺跨境数据流动规制的主导权。

（一）规制多极化和规制标准的俱乐部化

第一，规制多极化。各国颁布并实施数据隐私保护法是参与跨境数据流动和促进数字经济发展的前提基础。除美国、欧盟、日本外，澳大利亚、新加坡等国家也分别先后出台了《隐私法》和《个人数据保护法》等法律。[④] 同时，印度、俄罗斯等国也正逐步完善各自跨境数据流动方面的法律法规，并积极与其他国家开展跨境数据流动治理协调。例如，印度出台了《印度电子

① 该报告指出，芬兰、瑞典、荷兰、丹麦评分最高，之后是英国、卢森堡、爱尔兰、爱沙尼亚和比利时等，其他国家还有很长的路要走。参见 European Commission, “The Digital Economy and Society Index,” June 11, 2019, https://ec.europa.eu/digital- single-market/en/desi。

② James Manyika et al., “Digital Globalization: The New Era of Global Flows,” p. 6.

③ 顾登晨：《美欧“数字博弈”升级》，《经济观察报》2020 年 2 月 15 日，http://www.eeo.com.cn/2019/1212/371696.shtml。

④ See Office of the Australian Information Commissioner, “The Privacy Act,” 1998, https://www.oaic.gov.au/privacy/the-privacy-act/#:~:text=The%20Privacy%20Act%201988%28Privacy%20Act%29%20was%20introduced%20tomillion%2C%20and%20some%20other%20organisations%2C%20handle%20personal%20information; and Singapore Statutes Online, “Personal Data Protection Act,” 2012, https://sso.agc.gov.sg/Act/PDPA2012.

商务：国家政策框架草案》，[①] 要求以数据本地化政策为前提促进本国数字经济发展。同时，印度积极与欧盟就跨境数据流动合作展开谈判。俄罗斯则出台了《主权互联网法案》，[②] 在数据回流至本国进行处理的原则下，允许数据自由流向《第 108 号公约》的 53 个缔约国和 23 个被俄罗斯联邦委员会列入“白名单”的国家。[③] 阿联酋颁布了《迪拜国际金融中心数据保护法》，旨在与欧盟等开展跨境数据流动方面的合作。[④] 阿根廷出台了《个人数据保护法》，成为拉美地区首个获得 GDPR“充分性”评估认可的国家。[⑤] 南非也针对数据保护制定了《个人信息保护法》。[⑥] 此外，博茨瓦纳、肯尼亚、尼日利亚、多哥等非洲国家也相继出台并实施个人数据保护法。截至 2019 年底，全球共有 142 个国家对数据隐私进行立法。[⑦] 由此可见，跨境数据流动的全球治理正在显现出规制多极化的发展趋势。

第二，规制标准的俱乐部化。一方面，美国和欧盟除了借助多边机制推广其规制标准外，还各自组建了 CBPR 体系和满足充分保护要求的 GDPR“白名单”国家两个规制标准俱乐部。另一方面，各国也努力使本国规制符合美国或欧盟主导的俱乐部标准。例如，新加坡通过《个人数据保护法》对接美国主导的 CBPR 体系，力图实现数据在亚太地区的自由流动。[⑧] 巴西出台了了首部综合性《通用数据保护法》，[⑨] 效仿欧盟数据保护机制，设立国家数

① “Electronic Commerce in India: Draft National Policy Framework,” August 2018, http://www.medianama.com/wp-content/uploads/Draft-National-E-commerce-Policy.pdf.

② Nathan Hodge and Mary Ilyushina, “Putin Signs Law to Create an Independent Russian Internet,” CNN, May 1, 2019, https://edition.cnn.com/2019/05/01/europe/vladimir-putin-russian-independent-internet-intl/index.html.

③ 阿里巴巴数据安全研究院：《全球数据跨境流动政策与中国战略研究报告》。

④ Dubai International Financial Center, “Mohammed Bin Rashid Enacts New DIFC Data Protection Law,” June 1, 2020, https://www.difc.ae/newsroom/news/mohammed-bin-rashid-enacts-new-difc-data-protection-law/.

⑤ Ministerio de Justicla y Derechos Humanos, “Ley de Protección de DatosPersonales,” October, 2020, http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm.

⑥ South African Government Gazette, “Protection of Personal Information Act,” November 2013, https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf.

⑦ Anupam Chander, Margot E. Kaminski, and William McGeveran, “Catalyzing Privacy Law,” *Minnesota Law Review*, April 24, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3433922.

⑧ Singapore Statutes Online, “Personal Data Protection Act.”

⑨ Ministerio de Justicla y Derechos Humanos, “Lei Geral De Proteção de Dados Pessoais.”

据保护局、个人数据和隐私保护委员会等监督机构。日本则在《个人信息保护法》中，既参照 GDPR，在第 24 条和第 83 条中提出三种严苛的数据跨境转移标准和最高可达 1 亿日元的违规罚金要求，又在第 1 条宗旨中提及倡导数据流动自由化理念，以迎合美国主导的俱乐部标准。①

（二）美欧将继续争夺跨境数据流动规制的主导权

美国和欧盟将通过拓宽自身的数据流动圈，争夺全球跨境数据流动规制的主导权。美国正通过以下三种途径，开拓“数字边疆”、② 打造美国优先的跨境数据流动新格局。首先，借助 CBPR 体系主导亚太跨境数据流动圈。目前，加拿大、日本、澳大利亚等发达经济体和墨西哥、菲律宾等发展中经济体已加入 CBPR 体系，俄罗斯、新加坡、越南等也在积极申请加入。③ 其次，修改 OECD、G20 和 WTO 的跨境数据流动相关规则，使多边规制行动更加偏向促进跨境数据流动，以减少数据本地化处理等数字壁垒。再次，开辟新的双边或多边跨境数据流动规制体系。例如，美国与日本达成了《美日数字贸易协定》，确定双方将在个人信息保护的法律框架下，确保企业通过跨境数据流动促进数字贸易；④ 在日本的倡议下，美、欧、日将着手推动在数字贸易和电子商务领域的更多合作，并构建三方跨境数据流动圈；⑤《美墨加贸易协定》（USMCA）将禁止美国、墨西哥和加拿大的数据本地化保

① Personal Information Protection Commission, “The Act on the Protection of Personal Information,” December, 2016, https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

② 参见杨剑：《开拓数字边疆：美国网络帝国主义的形成》，《国际观察》2012 年第 2 期，第 1—8 页；Jeffery Cooper, “The Cyber Frontier and America at the Turn of the 21st Century: Reopening Frederick Jackson Turner’s Frontier,” *First Monday*, Vol. 5, No. 7, 2000, https://www.researchgate.net/publication/220168183_The_CyberFrontier_and_America_at_the_Turn_of_the_21st_Century_Reopening_Frederick_Jackson_Turner's_Frontier。

③ 目前，加入跨境隐私规则（CBPR）体系的 9 个国家（地区）分别是美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚和菲律宾等。参见 APEC, “APEC Privacy Framework 2015”。

④ Rachel F. Fefer, “Data Flows, Online Privacy, and Trade Policy,” Congressional Research Service, March 26, 2020, https://crsreports.congress.gov/product/pdf/R/R45584; and Office of the United States Trade Representative, “Fact Sheet on U.S.-Japan Digital Trade Agreement,” October 7, 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement.

⑤ G20 2019 JAPAN, “G20 Osaka Leaders’ Declaration.”

护主义，实现三方跨境数据流动。[①]

欧盟则在 GDPR 基础上，加大与其他发达经济体开展跨境数据流动合作的力度。目前，欧盟不仅与美国、澳大利亚、加拿大达成了《旅客姓名存储协定》，[②] 而且还与日本达成了《欧日经济伙伴关系协定》。该协定规定，欧日双方视对方的数据保护规制同等有效，将打造欧日双边数据自由流动圈。[③] 与此同时，一些发展中经济体也积极效仿 GDPR 制定跨境数据流动规则，以求在符合欧盟标准后与其顺利推动跨境数据流动。例如，巴西的《通用数据保护法》、韩国的《个人信息保护法》、泰国的《个人数据保护法》等，[④] 均认可 GDPR 标准。此外，欧盟还将通过向东盟（ASEAN）输入数字基础设施、数字信息技术，积极开拓亚洲数字经济市场，[⑤] 当前已具备向东盟输入 GDPR 的潜力。

四、跨境数据流动治理的中国路径

一个国家的数字经济发展水平是该国推动构建跨境数据流动规制体系的内在动力，而吸纳其他国家数字经济产品和服务的市场规模，则决定了该国在跨境数据流动规则制定方面的影响力。在跨境数据流动议题领域，中国同美国和欧盟一样，也是一个重要行为体。[⑥] 面对跨境数据流动全球治理的

① Agam Shah, Jared Council, “USMCA Formalizes Free Flow of Data, Other Tech Issues,” *The Wall Street Journal*, January 29, 2020, https://www.wsj.com/articles/cios-businesses-to-benefit-from-new-trade-deal-11580340128.

② European Commission, “Passenger Name Record,” April 27, 2016, https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en.

③ European Commission, “International Data Flows: Commission Launches the Adoption of Its Adequacy Decision on Japan,” September 5, 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5433.

④ Dan Simmons, “6 Countries with GDPR-Like Data Privacy Law,” Comforte Blog, January 17, 2019, https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws.

⑤ ASEAN, “The Joint Media Statement of the 19th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings,” October 25, 2019, https://asean.org/joint-media-statement-19th-asean-telecommunications-information-technology-ministers-meeting-related-meetings/.

⑥ 作为全球第二大数字经济体，中国 2018 年的数字经济总量为 4.73 万亿美元。其中，数字产业化规模和产业数字化规模分别为 9689 亿美元和 3.8 万亿美元（该统计不计欧盟整体）。2019 年，中国 GDP 总量约为 14.343 万亿美元，约占美国的 67%。参见中国信息通信研究院：《全球数字经济新图景（2019）》，第 9 页、第 15—18 页；The World Bank, “The World

发展趋势，中国提出了建设“网络强国”和“数字中国”的战略构想，出台了《中华人民共和国网络安全法》《中华人民共和国个人信息保护法（草案）》和《中华人民共和国数据安全法（草案）》等相关法律。[①]

当前，中国正加快培育数据要素市场，推进数据市场化配置体制机制改革。2019 年，中共十九届四中全会提出提升数据等生产要素推动经济高质量发展的总要求。2020 年，中国发布了关于完善要素市场化配置体制机制的文件，不仅将数据与土地、资本等传统要素并列为五大市场要素之一，而且进一步细化了数据市场化配置体制机制改革方向。[②] 同时，中国正加快参与跨境数据流动的全球治理步伐。目前，中国可以通过三条路径协同并进，推动跨境数据流动的全球治理，一是加入 APEC 框架下的 CBPR 体系，二是与 GDPR 的实施方欧盟进行规制协调，三是将中国跨境数据流动规制体系推向“一带一路”沿线国家。

（一）加入 APEC 框架下的 CBPR 体系

中国是 APEC 成员国，加入 APEC 框架下的 CBPR 体系，具有可行性。

第一，CBPR 体系在《APEC 隐私框架》内执行，它的最终目的是促进亚太地区电子商务和数字贸易的蓬勃发展。APEC 重视通过互联网和数字经济推动区域经济以更具创新、智能、可持续和包容性的方式增长。[③] 数字中国战略则倡导发展以数据为关键要素的数字经济，坚持数据开放、市场主导原则。[④] 因此，数字中国战略与 CBPR 体系的宗旨是相吻合的，二者具有相

Bank National Accounts Data, and OECD National Accounts Data Files,” 2019, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD。

① 参见《中华人民共和国网络安全法》，中国人大网，2016 年 11 月 7 日，http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm；《中国 2020 年将制定个人信息保护法、数据安全法》，中国新闻网，2019 年 12 月 20 日，https://m.chinanews.com/wap/detail/zw/gn/2019/12-20/9039098.shtml。

② 参见《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》，中国政府网，2019 年 11 月 5 日，http://www.gov.cn/zhengce/2019-11/05/content_5449023.htm；《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》，商务部网站，2020 年 5 月 21 日，http://www.mofcom.gov.cn/article/b/g/202005/20200502967296.shtml。

③ APEC, “APEC Framework for Security the Digital Economy,” November, 2019, https://www.apec.org/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy.

④ 《习近平：实施国家大数据战略加快建设数字中国》，求是网，2017 年 12 月 9 日，http://www.qstheory.cn/yaowen/2017-12/09/c_1122085231.htm。

互对接的潜力。

第二，CBPR 体系的核心理念与中国的跨境数据流动治理理念基本吻合。CBPR 体系要求实现最大范围的跨境数据流动，不让网络封闭成为数字经济发展的障碍。加入这一规制体系的各个国家，在进行跨境数据流动时，即使数据接收方的数据保护水平不如数据输出方严格，也应准许数据流动，并且不得强制要求非 APEC 成员的数据接收方设置高于 APEC 的数据保护水平。[①] 中国的跨境数据流动治理理念是坚持在保障个人信息、数据安全、网络安全基础上推动数字经济创新发展。在 2019 年世界互联网大会上，中国提出开放是网络空间合作的前提，也是构建网络空间命运共同体的重要条件，中国愿搭建双边或多边国际合作平台。[②] 可见，CBPR 体系与中国的跨境数据流动治理理念均倡导构建开放合作的网络空间。

第三，加入 CBPR 体系，有助于提升中国在跨境数据流动议题领域的话语权，并且有助于避免全球治理规则与国内治理规则出现错位。[③] 中国在加入 CBPR 体系后，可以参与该体系的规则制定，有助于提升中国在跨境数据流动议题领域的话语权。此外，中国可以根据该规制体系要求，完善国内跨境数据流动规制，在亚太地区实现更加顺畅的跨境数据流动。

（二）与 GDPR 的实施方欧盟进行规制协调

中国可以在加入 CBPR 体系的同时，与 GDPR 的实施方欧盟进行规制协调。中国的市场规模虽不及欧盟，但处在同一级别。英国脱欧后，中国与欧盟的市场规模更加接近。因此，中欧双方具备开展规制协调的市场权力基础。[④] 同时，中国与欧盟开展跨境数据流动的规制协调也具有可行性。

第一，欧盟坚持以人为本的数字经济发展理念与中国以人民为中心的数

① APEC, “APEC CBPRs System Program Requirements,” December 26, 2012, https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Rules%20Program%20Requirements.pdf.

② 《携手构建网络空间命运共同体》，世界互联网大会网站，2019 年 10 月 16 日，http://www.wicwuzhen.cn/web19/release/release/201910/t20191016_11198729.shtml。

③ 上海国际问题研究院中国外交 70 年课题组：《中国外交 70 年专家谈（之三）——全球治理、军事外交、中东欧合作、中等国家关系》，《国际展望》2019 年第 5 期，第 5 页。

④ 2019 年，欧盟 27 国 GDP 总量为 15.593 万亿美元，中国 GDP 总量为 14.343 万亿美元。参见 The World Bank, “The World Bank National Accounts Data, and OECD National Accounts Data Files,” 2019。

字中国战略目标相符。欧盟在《塑造欧洲的数字未来》战略中，强调坚持以人为本理念，认为科技服务于民众，重视通过数字经济改善人们的生活。[①] 而中国在数字中国战略中，也明确提出运用大数据保障和改善民生，尤其是推动教育、就业、社保等领域大数据的普及。[②] 中国与欧盟秉持的数字为民理念构成了双方进行跨境数据流动规制协调的基础。

第二，中国和欧盟均重视个人隐私保护。如前文所述，欧盟重视隐私保护，看重数据接收国在隐私保护方面的法律保障体系。中国不仅重视个人信息保护，更关注数据安全和网络安全。由于 GDPR 的充分保护原则与美国强调的跨境数据自由流动原则存在冲突，美欧双方分歧不断。中国对网络安全、个人信息保护和数据安全的重视，使得中国和欧盟可以避免在核心原则上出现分歧，因而极大地提升了双方进行规制协调的可能性。

当然，加入 APEC 框架下的 CBPR 体系并与 GDPR 的实施方欧盟进行规制协调，也会为中国带来新的挑战。首先，APEC 框架下的 CBPR 体系是美国主导的俱乐部标准。虽然加入 CBPR 体系的国家不需要修改本国的数据隐私法，但该体系规定，参与国在管控个人信息出境时不得要求数据接受方提供超过《APEC 隐私框架》的保护水平。[③] 因此，参与国仍然需要根据 APEC 最低标准修改本国相关的跨境数据流动条例。这将在一定程度上限制中国在监管标准方面的自主权。其次，数据信息处理主体不对称，将增加国家与企业及企业之间的互操作成本。中国要求国家统一领导各地区、各部门对数据信息的处理。《中华人民共和国数据安全法（草案）》总则第 6 条指出，中央国家安全领导机构负责数据安全工作的决策和统筹协调，研究制定、指导实施国家数据安全战略和有关重大方针政策；[④] 而 CBPR 体系和 GDPR 认可个人数据的收集、处理和使用在企业层面完成。若中国加入 CBPR 体系并与欧盟进行规制协调，参与跨境数据流动的企业需要接受国家机关和数据

① European Commission, “Shaping Europe’s Digital Future,” February 19, 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.

② 《习近平：实施国家大数据战略加快建设数字中国》。

③ APEC, “APEC CBPRs System Program Requirements.”

④ 《〈中华人民共和国数据安全法（草案）〉全文发布》，等级保护资讯网站，2020 年 7 月 3 日，http://www.dengbao.net/news1/508.html。

流向国家及其企业数据保护机制等多方监督，这将增加跨境数据流动的互操作成本和执行风险。

（三）将中国跨境数据流动规制体系推向“一带一路”沿线国家

目前，中国正在为开展跨境数据流动做出相应的规制努力，在国内规制体系形成后，将其推向“一带一路”沿线国家具有可行性。

第一，相对于“一带一路”沿线国家，中国在市场规模上具有优势。2018年，中国从“一带一路”沿线国家的进口总额增长至 8 618.67 亿美元，是2013 年的 1.27 倍，占当年进口总额的比重约为 40.36%。[①] 与此同时，“一带一路”沿线国家在数字经济领域对中国的依赖也在不断加深。2017 年，马来西亚政府与中国阿里巴巴集团在吉隆坡启动“数字自由贸易区”，希望通过中国电商平台为其 2020 年国内生产总值贡献约 3 284 亿元。[②] 中国的互联网企业已成为推动“一带一路”国家数字经济发展的动力来源，沿线国家的商品正通过电商渠道越来越多地进入中国市场。[③] 庞大的市场规模有利于中国将自身规制标准推向“一带一路”沿线国家。[④]

第二，中国与“一带一路”沿线国家在“数字丝绸之路”建设方面取得了阶段性成果，这构成了中国在跨境数据流动治理领域与“一带一路”沿线国家开展对话与合作的基础。目前，中国已与 16 个国家签署了关于加强“数字丝绸之路”建设合作的谅解备忘录，与 19 个国家签署了双边电子商务合作谅解备忘录。[⑤] 例如，中国与东盟达成了《中国—东盟战略伙伴关系 2030 年愿景》，为加强双方规制的联通合作做好了准备。[⑥] 此外，中国与老挝、

① 《中国从“一带一路”沿线国家的进口规模显著增加》，中国经济网，2019 年 11 月 12 日，http://m.ce.cn/bwzg/201911/12/t20191112_33586642.shtml。

② 俞懿春：《借力中企，马来西亚建数字自贸区》，人民网，2017 年 3 月 23 日，http://ccnews.people.com.cn/n1/2017/0323/c141677-29164665.html。

③ 方芳：《“数字丝绸之路”建设：国际环境与路径选择》，《国际论坛》2019 年第 2 期，第 63 页。

④ OECD, “China’s Belt and Road Initiative in the Global Trade, Investment and Finance Landscape,” *OECD Business and Finance Outlook 2018*, 2018, https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf.

⑤ 《“数字丝路”建设将成为全球发展新引擎》，中国经济网，2019 年 9 月 9 日，http://www.ce.cn/xwzx/gnsz/gdxw/201909/09/t20190909_33108649.shtml。

⑥ 参见《中国—东盟战略伙伴关系 2030 年愿景（全文）》， 新华网，2018 年 11 月 15 日，http://www.xinhuanet.com/world/2018-11/15/c_1123718487.htm；《李克强在第二十二次中

沙特、塞尔维亚、泰国、土耳其等国家共同发起了《“一带一路”数字经济国际合作倡议》，[①] 将从数字经济项目对接、数字人才培养和数字经济治理等方面对非洲敞开合作的大门，为形成中非跨境电子商务生态体系、保障跨境数据流动基础设施等方面做好铺垫。同时，中国与非洲达成了《北京行动计划（2019—2021）》，并将进一步实施“中非科技伙伴计划 2.0”等。[②] “数字丝绸之路”也引起了拉美国家的广泛关注。2018 年，中国与拉美国家在第二届中国—拉美和加勒比国家共同体论坛上达成了《中国与拉美和加勒比国家合作优先领域共同计划（2019—2021）》，提出了在网络安全、通信产业等领域开展合作的共同计划。拉美国家还发表了《“一带一路”特别声明》，明确表示愿意在中国推动下实现建设信息和通信的“数字丝绸之路”，在加强信息互联互通的同时，共同分享数字红利。[③] “数字丝绸之路”建设将通过与沿线国家在信息基础设施、经贸发展、文化交流等领域的全方位交流与合作，进一步缩小“数字鸿沟”，[④] 为下一步开展跨境数据流动、释放数据资源价值、推动数字经济高质量发展做好充分准备。

尽管将中国跨境数据流动规制体系推向“一带一路”沿线国家前景可期，但这一路径面临以下挑战。首先，建设“数字丝绸之路”跨境数据流动圈将引发新一轮美、欧、中三大力量的“数字地缘政治”竞争。在美国看来，“数字丝绸之路”将打造一条绕过美国的新型全球跨境数据流动“高速公路”，中国正以“数字威权主义”方式在“一带一路”沿线国家提升科技、经济和

国—东盟领导人会议上的讲话》，人民网，2019 年 11 月 4 日，http://www.gov.cn/xinwen/2019-11/04/content_5448268.htm。

① 参见《〈“一带一路”数字经济国际合作倡议〉发布》，中华人民共和国国家互联网信息办公室，2018 年 5 月 11 日，http://www.cac.gov.cn/2018-05/11/c_1122775756.htm；黄玉沛：《中非共建“数字丝绸之路”：机遇、挑战与路径选择》，《国际问题研究》2019 年第 4 期，第 56 页。

② 《中非合作论坛—北京行动计划（2019—2021）》，外交部网站，2018 年 9 月 5 日，https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t1592067.shtml。

③ 参见楼顶飞、杨剑：《拉美数字鸿沟消弭与中拉共建“数字丝绸之路”》，《国际展望》2018 年第 5 期，第 57 页；《中国与拉美和加勒比国家合作优先领域共同计划（2019—2021）》，中国—拉美共同体论坛网站，2018 年 2 月 2 日，http://www.chinacelacforum.org/chn/zywj/t1531608.htm。

④ 《数字丝绸之路建设成为新亮点》，人民网，2019 年 4 月 22 日，http://www.xinhuanet.com/zgjx/2019-04/22/c_137997345.htm。

文化等影响力，并争夺全球数字技术主导权。[①]《美国网络安全国家战略》（National Cyber Strategy）声称，中国已对美国的经济、民主、知识产权等领域造成破坏性影响。由此，美国启动了《美国人工智能倡议》，将包括华为在内的数家中国企业列入“黑名单”，并限制其使用源自美国的软件和技术。[②] 欧盟也担心“数字丝绸之路”对其技术主权造成潜在威胁，认为中国主导的“数字丝绸之路”通过带动沿线国家数字技术的进步，不仅提升了中国在全球数字经济领域的影响力，还有利于中国向外输出符合其战略目标的跨境数据流动标准与规范。出于这一考虑，欧盟将通过加快数字化进程、建立数据框架、建设可信赖的泛欧数字环境，提升欧洲数字战略自主性，[③] 意欲限制中国规制、标准的输出力度。其次，与“一带一路”沿线国家开展跨境数据流动将考验中国国内数据要素市场的监管体系。目前，中国数据要素市场处于全方位完善期，数据要素监管体系相对发达国家较为薄弱。进入“一带一路”沿线国家的数据难免存在“数据黑市”“数据黑产”等情况。[④] 因此，中国在将跨境数据流动规制体系推向“一带一路”沿线国家的同时，亟须加强对数据要素市场的监管。

结 束 语

为应对新问题和新挑战，共同构建和平、安全、开放、合作、有序的网络空间，中国已发起《全球数据安全倡议》，并明确将秉持多边主义、兼顾

① 参见赵明昊：《大国竞争背景下美国对“一带一路”的制衡态势论析》，《世界经济与政治》2018 年第 12 期，第 4—31 页；Council on Foreign Relations, “China’s Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism,” September 26, 2019, https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political.

② 参见 White House, “American Artificial Intelligence Initiative,” February 11, 2019, https://www.whitehouse.gov/ai/; Earl Carr, “Is China Threatening America’s Dominance in the Digital Space?” Forbes, January 20, 2020, https://www.forbes.com/sites/earlcarr/2020/06/20/is-china-threatening-americas-dominance-in-the-digital-space/#1d1061c53cd4。

③ Kristin Shi-Kupfer, Mareike Ohlberg, “China’s Digital Rise Challenges for Europe,” Merics Mercator Institute for China Studies, *Merics Papers on China*, No.7, April, 2019, pp. 7-12, https://www.merics.org/en/papers-on-china/chinas-digital-rise.

④ 戴双兴：《数据要素市场为经济发展注入新动能》，《光明日报》2020 年 5 月 20 日，第 16 版。

安全发展和坚守公平正义[①]，积极参与全球数字治理。跨境数据流动治理是全球数字治理的重要领域。鉴于当前跨境数据流动的全球治理进展、发展趋势以及中国在推动这一领域全球治理进程中面临的挑战，[②] 中国应做出具体政策应对。首先，积极参与既有多边平台的数字治理对话和协调，为全球数字治理贡献中国智慧。中国应积极参与 APEC、G20、WTO 等既有多边平台有关数字治理的对话和协调，为解决跨境数据流动面临的困境提出中国的应对方案。其次，中国应在保障数据安全的前提下，健全数据安全监管机制、创新数据要素市场监管模式，降低跨境数据流动的互操作成本和执行风险，营造各国可信赖的跨境数据流动规制环境。再次，中国应坚持以数字科技推动数字经济发展，不断扩大数字经济市场规模，以应对“数字地缘政治”竞争。数字科技是推动数字经济发展的重要手段，不仅能降低产业成本、增加产业收入、迭代商业模式，更能推动企业从“单边”到“共建”经营模式转变。在数字科技推动下，中国数字经济市场规模将不断扩大，这将有助于中国在“数字地缘政治”竞争中获得优势地位。

[责任编辑：杨 立]

① 王毅：《坚守多边主义倡导公平正义携手合作共赢——在全球数字治理研讨会上的主旨讲话》，外交部网站，2020 年 9 月 8 日，http://russiaembassy.fmprc.gov.cn/web/wjbzhd/t1812948.shtml。

② 参见：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。