美国数据跨境监管立场转向：从自由流动到安全流动

周　辉　闫文光*

摘　要：美国早期以数据自由流动为基本理念，以宽松的国内监管与广泛的国际合作为支柱，在国内建立了市场导向的数据监管体系，在国际上形成了双边与多边并重的数据合作战略。然而，随着全球战略竞争格局的深刻调整，美国数据监管政策逐步转向以安全为前提的有限自由流动模式，具体体现为在数字贸易领域强化国家监管，对特定竞争对手国家实施带有明显政治色彩的限制措施，并建立针对敏感数据流动的管控体系。美国监管立场转变的主要原因在于其泛化数据出境国家安全风险、推行贸易保护主义以及其信息技术霸权受到冲击。但是，转向后的美国数据跨境监管制度的落实面临诸多不确定性，包括国内法规的限制、国内商界的批评以及美国盟友的质疑。总体来看，美国未来将对中国等所谓“对手”国家加强数据出境监管，对盟友国家采取在安全前提下有条件的数据自由流动政策。中国应通过建立企业海外维权机制、利用 WTO 争端解决机制、建立中国的数据跨境国际合作体系等措施积极应对美国的数据跨境监管政策。

关键词：美国数据跨境　数据跨境流动　数据跨境监管　数据跨境自由流动　国家安全泛化

一　问题的提出

2024 年 2 月 28 日，美国时任总统拜登签署了《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》（Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern，下称《敏感数据行政命令》）。[①] 该命令首次规定了审查、限制并可能禁止将美国人的数据传输到特定目的地的制度。2024 年 12 月 27 日，美国司法部发布全面的最终规则，[②] 标志着《敏感数据行政命

* 周辉，中国社会科学院法学研究所副研究员；闫文光，中国人民大学法学院博士研究生。本文获中国社会科学院学科建设“登峰战略”资助计划资助，编号 DF2023XXJC07。本文所引用网络资源的最后访问时间均为 2025 年 4 月 30 日。

① See “National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern”, Federal Register, https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

② See “Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons”, U.S. Department of Justice, https://www.justice.gov/nsd/media/1382521/dl?inline.

令》的最终落地。在此之前的2023年10月25日，美国贸易代表办公室声明，美国在WTO电子商务谈判中撤回该国长期以来坚持的部分数字贸易主张，包括数据跨境自由流动。[①] 上述系列措施一脉相承，反映了美国数据监管政策的转变，即通过撤回全球性的数字贸易提案，为国内强化科技公司监管和限制数据自由流动预留空间。这将对全球数据流动和跨国企业运营产生深远影响。

从推崇全球性自由流动到强调安全流动的“小院高墙”[②] 战略，美国数据跨境监管的立场转向不仅反映了其对数据安全与国家利益的重新评估，也折射出国际竞争态势与全球数据治理格局的变化。这一政策将对中国等其他国家产生重要影响，我们需要洞悉美国的这一政策是基于何种背景和考量而产生的，其监管逻辑是否产生了根本性变化。在当前学界研究中，有学者基于美国早期的数据跨境政策，研究了美国数据的自由流动面向，[③] 但尚未深入分析美国对数据跨境的限制面向。随着美国数据跨境监管“宽进严出”趋势的凸显，有学者的研究深入到了美国限制本国数据跨境的层面，[④] 认为美国数据跨境监管的双重面向是其霸权思想在数据领域的延伸，形成了“数据殖民主义”。[⑤] 但仅有部分学者专门总结分析美国数据跨境自由流动的具体支柱以及当前阶段美国如何进行标志性转向，也较少有研究注意到美国数据跨境监管政策变化的深层次原因，国内现有研究对于监管转向面临的不确定性和来自国内外的约束条件也未深入分析。

本文将首先总结梳理美国在数据跨境方面的监管变化，分析其前期数据自由流动的支柱，进而从3个面向讨论其从自由流动到安全流动转向的表现，再从政治、经济、技术方面分析美国数

---

① See David Lawder, “US Drops Digital Trade Demands at WTO to Allow Tech Regulation with Teeth”, https://arizonadigitalfreepress.com/us-drops-digital-trade-demands-at-wto-to-allow-room-for-stronger-tech-regulation/.

② “小院高墙”是美国的对华科技防御新策略，“小院”指的是直接关系到美国国家安全的特定技术和研究领域，“高墙”是指为这些领域划定的策略边界。

③ 相关代表性文献可参见徐拥军、王兴广：《总体国家安全观下的跨境数据流动安全治理研究》，载《图书情报知识》2023年第6期，第20—30页；张生：《美国跨境数据流动的国际法规制路径与中国的因应》，载《经贸法律评论》2019年第4期，第79—93页；王燕：《数据跨境流动治理的国别模式及其反思》，载《国际经贸探索》2022年第1期，第99—112页；林福辰、杜玉琼：《发展与蜕变：多边视域下数字贸易规则建构路径之审思》，载《江海学刊》2020年第5期，第158—164页；刘文杰：《美欧数据跨境流动的规则博弈及走向》，载《国际问题研究》2022年第6期，第65—78页；王雪、石巍：《数据立法域外管辖的全球化及中国的应对》，载《知识产权》2022年第4期，第54—75页。See also François LeSieur, “Regulating Cross-Border Data Flows and Privacy in the Networked Digital Environment and Global Knowledge Economy”, (2012) 2 *International Data Privacy Law* 93, pp. 100-103; Dan Jerker B. Svantesson, “Privacy, the Internet and Transborder Data Flows: An Australian Perspective”, (2010) 4 *Masaryk University Journal of Law and Technology* 1, pp. 15-20; Aaronson Susan, “Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security”, (2015) 14 *World Trade Review* 671, pp. 689-693.

④ 相关代表性文献可参见罗文华：《基于生命周期的数据跨境流动程序性与实质性监管》，载《中国政法大学学报》2021年第5期，第142—154页；陈元馨、康宁：《美国数据跨境流动规制的国内研究观点分析》，载《情报杂志》2023年第4期，第132—139页；冉从敬、陈贵荣、王欢：《美国跨境数据流动的管辖模式研究及对中国的启示》，载《图书情报知识》2020年第6期，第136—143页。

⑤ 相关代表性文献可参见许可：《数据主权视野中的CLOUD法案》，载《中国信息安全》2018年第4期，第40—42页；华佳凡：《美国跨境数据流动国际倡议与国内政策的差异及其成因》，载《情报杂志》2024年第1期，第99页。See also Renata Avila Pinto, “Digital Sovereignty or Digital Colonialsim”, (2018) 15 *SUR International Journal on Human Rights* 15, pp. 18-23; Nick Couldry, Ulises A. Mejias, “Data colonialism: Rethinking Big Data's Relation to the Contemporary Subject”, (2019) 20 *Television & New Media* 336, pp. 336-340.

据跨境监管立场转向的原因，最后针对美国数据跨境监管的未来发展趋势及面临的约束条件，提出中国的应对策略。

二　美国数据跨境自由流动的理念与支柱

美国作为全球数字经济的引领者，其对数据跨境流动的态度与政策取向对全球数据治理具有深远影响。美国历来主张自由贸易理论，将自由贸易视为国家和社会发展的主要目标之一。[①] 不论是政府还是公民都倾向于通过多元、宽松的手段追求经济的发展，通过事后救济的方式来规制风险。[②] 在全球数据流动生态中，美国凭借领先的数字经济实力和完善的科技产业链，自然而然地成为了全球数据的主要汇聚地和处理中心，数据自由流动更符合其科技产业的发展需求。[③] 因而美国积极地将数据跨境自由流动与自由贸易绑定，在自由贸易协定（下称 FTA）中将数据跨境流动纳入电子商务章节，在国际经贸协定谈判中对数据流动的限制进行约束，敦促其他国家和地区降低数据跨境的门槛，弱化监管和司法限制，并通过数据自由流动促进信息传播以便更好地获取全球信息，为其外交决策提供支持。

（一）曾经的基本理念：数据自由流动

数字贸易的一大特点是依赖于数据传输，数据跨境流动是进行数字贸易的前提。[④] 美国长期以来支持并推动全球性的数据跨境自由流动政策，通过国际经贸谈判、国际磋商倡导数据自由流动，并将数据本地化等行为称为“数据保护主义”“数据民族主义”[⑤]。早在 20 世纪 80 年代，美国国会预见性地指出了数据流动壁垒对国民经济构成的潜在风险。[⑥] 随后，这一观念在 1983 年的《国际投资政策声明》（Statement on International Investment Policy）中得到进一步强化，该声明呼吁发达国家减少数据流动壁垒，并倡导在全球范围内采取更为开放和自由的数据跨境流动策略。

进入 21 世纪，美国在数据自由流动方面的立场更为坚定，特别是在 2015 年通过的《两党国会贸易优先事项与问责法》（The Bipartisan Congressional Trade Priorities and Accountability Act of 2015）中，美国明确将促进数据自由流动置于其国际贸易政策的核心地位，并坚决反对其他国家实施的数据本地化措施。在奥巴马政府时期签署的《跨太平洋伙伴关系协定》（Trans-Pacific Partnership Agreement，下称 TPP）以及后来的《美国—墨西哥—加拿大协定》（United States – Mexico – Canada Agreement，下称 USMCA）中，美国都明确反对数据本地化要求。[⑦] 美国在 WTO 电子商务谈判的提

① See Paul M. Schwartz, Karl-Nikolaus Peifer, “Transatlantic Data Privacy Law”, (2017) 106 *Georgetown Law Journal* 115, pp. 125 – 127.

② See Danielle Keats Citron, Daniel J. Solove, “Privacy Harms”, (2022) 102 *Boston University Law Review* 793, pp. 821 – 823.

③ 〔英〕戴恩·罗兰德、伊丽莎白·麦克唐纳著：《信息技术法》，宋连斌等译，武汉大学出版社 2004 年版，第 308 页。

④ 谭观福：《国际经贸规则对数字贸易的规制》，中国社会科学出版社 2024 年版，第 93 页。

⑤ See Segal Adam, “The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age”, (2016) 92 *International Affairs* 1263, pp. 1264 – 1266.

⑥ See George W. Coombe, Jr. and Susan L. Kirk, “Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations”, (1983) 39 *The Business Lawyer* 33, p. 34.

⑦ 参见刘云：《中美欧数据跨境流动政策比较分析与国际趋势》，安全内参，https://www.secrss.com/articles/28983。

案中，更是将数据自由流动列为讨论的重要议题。此外，美国还支持其他国家提出类似倡议，例如日本提出的“基于信任的数据自由流动”（Data Free Flow with Trust）概念。这些政策表明，美国长期以来将数据自由流动作为其国际贸易政策的核心部分，并在此方面发挥了领导作用。①

（二）战略支柱：市场导向的国内监管与广泛的国际合作

1. 国内措施：市场导向的监管体系

美国构建了一套相对开放的数据流动制度，包括宽松的数据保护法规和市场导向的监管措施，以及鼓励技术创新与商业应用的法律框架。在制度体系上，美国未在法律层面对数据跨境传输作出限制性规定，长期以来没有实施类似欧盟《通用数据保护条例》（General Data Protection Regulation，下称 GDPR）那样全面的数据保护法规，而是依赖行业自律、市场机制和一系列分散的联邦及州级法律来管理数据跨境流动。② 同时，美国为了促进商业利益，其国内的数据隐私法规也未采取严格的知情同意等数据授权原则，③ 而是更强调对消费者权利的保护，且对个人数据和消费者权利的保护也是出于自由贸易的考量。④ 因此，美国对数据跨境传输中的个人信息保护采取较为宽松的态度，为数据跨境自由流动创造了有利条件。

在规制路径层面，美国则采取事后救济以及行业自律规制路径，以国籍管辖为基准，遵循事后“问责制”原则。对于国内数据的出境，美国相关法规不设置事前的评估和许可，总体而言较为自由。即使是在特定情况下会限制数据的出口（特别是当这些数据的传输被认为威胁到国家安全或有悖于美国的外交政策目标时），也更多体现为对特定技术、软件、硬件的出口管制，包括但不限于半导体、微电子、量子信息技术和人工智能芯片等领域。美国的技术出口管制立法，如《出口管制条例》（Export Administration Regulations）和《出口管制改革法》（Export Control Reform Act），主要目的在于防止敌对国家军事实力的提升，以及加强国家安全、促进对外政策执行和控制国内短缺物资。⑤ 这些立法并未直接提及对数据出口的限制，而是侧重于技术和物资的出口管制。通过控制包含敏感数据的产品和技术的出口，美国政府对数据流动施加了一定程度的间接控制。真正对于数据进行大规模、高标准的直接控制，则是以拜登政府发布的《敏感数据行政命令》为标志。

2. 国际战略：双边数据跨境流动合作

以双边谈判方式推动数据自由流动是美国最常用的手段之一。与各国进行双边谈判时，美国通常会争取纳入数据自由流动条款，以消除数据本地化壁垒，其对象主要为日本、韩国、英国等核心盟友。美国通过与盟友签订双边协定，推广更为自由化的数据流动规则，形成了数据跨境流动的生态圈。⑥ 2012 年美国与韩国签订《美国—韩国自由贸易协定》（U. S. – Korea Free Trade

---

① 参见华佳凡：《美国跨境数据流动国际倡议与国内政策的差异及其成因》，载《情报杂志》2024 年第 1 期，第 99 页。

② 参见谭观福：《国际经贸规则对数字贸易的规制》，中国社会科学出版社 2024 年版，第 95 页。

③ See William McGeveran, “Friending the Privacy Regulator”, (2016) 58 *Arizona Law Review* 959, pp. 970 – 973; Paul M. Schwartz, “The EU – U. S. Privacy Collision: A Turn to Institutions and Procedures”, (2013) 126 *Harvard Law Review* 1966, p. 1976.

④ See Anupam Chander, Paul Schwartz, “Privacy and/ or Trade”, (2023) 90 *University Chicago Law Review* 49, pp. 67 – 69.

⑤ 参见〔美〕唐纳德·H·西弗曼著：《美国对技术转让——计算机硬软件的出口限制》，马守仁译，贾名校，载《环球法律评论》1990 年第 4 期，第 39 页。

⑥ 参见张生：《美国跨境数据流动的国际法规制路径与中国的因应》，载《经贸法律评论》2019 年第 4 期，第 80—81 页。

Agreement），首次在电子商务章节中规定了数据跨境流动条款，要求成员国应努力避免对数据跨境流动设置不必要的阻碍，积极推动数据跨境流动并为之创造条件。2019 年，美国与日本签署的《美国—日本数字贸易协定》（U. S. – Japan Digital Trade Agreement）被美国称作“有史以来解决数字贸易壁垒的最全面和最高标准的贸易协定”。[①] 2023 年 6 月，美国时任总统拜登与英国时任首相苏纳克在白宫会谈后共同发布《大西洋宣言：21 世纪美英经济伙伴关系框架》（The Atlantic Declaration：A Framework for a Twenty – First Century U. S. – UK Economic Partnership），[②] 双方在宣言中承诺建立美英数据桥（U. S. – UK Data Bridge），允许通过“欧盟—美国隐私框架的英国扩展”（UK Extension to the EU – US Data Privacy Framework）进行美英间数据跨境传输，以实现英美相关组织之间的数据自由流动。2023 年 7 月 10 日，欧盟委员会批准跨大西洋数据传输新协议《欧盟—美国数据隐私框架》（EU – U. S. Data Privacy Framework），该协议旨在确保美国企业对欧盟个人数据的保护水平与欧盟法律要求相当。

此外，美国一直积极参与并推动国际组织框架下的数据流动规则制定。作为经济合作与发展组织（下称 OECD）的创始成员国，美国参与了全球首个关于个人数据跨境流动的保护标准——OECD《隐私保护与个人数据跨境流动指南》（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）的制定和修改。[③] 美国在 OECD 的国际会议中率先发声并提出了“透明度原则”和“责任原则”，[④] 强调数据自由流动的重要性。2004 年，APEC 成员国制定《亚太经济合作组织隐私框架》（Asia – Pacific Economic Cooperation Privacy Framework），并于 2007 年推出《跨境隐私规则体系》（Cross-Border Privacy Rules）。该体系构建了一个由隐私监管机构、责任代理机构以及企业主体共同参与的三维保护模型，为数据跨境流动的安全性、合规性和可信度设立了全新的标杆。[⑤] 目前已有 9 个经济体参与《跨境隐私规则体系》，包括美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、中国台湾地区和菲律宾。近年来，美国在数据跨境管理和整体贸易政策之间建立了更为紧密的联系，频繁在 FTA 中纳入数据跨境自由流动条款。[⑥]

三　美国数据跨境监管立场转向：安全阴影下的自由流动

随着国际竞争格局与国内监管重点的变化，美国正在从倡导全球性数据自由流动向安全流动转变：一方面，对于欧盟、日本、韩国等盟友，一直保持相对自由的政策，虽然时有分歧与调

① 博鳌亚洲论坛：《亚洲经济展望与一体化进程 2020 报告》，对外经济贸易大学出版社 2020 年版，第 35 页。

② See “The Atlantic Declaration：A Framework for a Twenty – First Century U. S. – UK Economic Partnership”，GOV. UK，https：//assets. publishing. service. gov. uk/government/uploads/system/uploads/attachment _ data/file/1161879/THE _ ATLANTIC_ DECLARATION. pdf.

③ See Coombe，George W. Jr. and Susan L. Kirk，“Privacy，Data Protection，and Transborder Data Flow：A Corporate Response to International Expectations”，（1983）39 *The Business Lawyer* 33，pp. 35 – 40.

④ 参见王佳宜、王子岩：《个人数据跨境流动规则的欧美博弈及中国因应——基于双重外部性视角》，载《电子政务》2022 年第 5 期，第 100 页。

⑤ 参见弓永钦、王健：《APEC 跨境隐私规则体系与我国的对策》，载《国际贸易》2014 年第 3 期，第 30—35 页。

⑥ 参见陈斌彬、王斌楠：《数据主权视阈下我国数据出境的法律规制及完善》，载《华侨大学学报（哲学社会科学版）》2024 年第 2 期，第 56—58 页。

整，但总体而言还是保持自由流动的态势；另一方面，对于中国、俄罗斯、朝鲜等国家，则是以所谓保障国内基础设施、网络系统等的安全为由泛化国家安全，对本国重要技术数据和特定领域的相关数据实施数据本地化措施，限制重要数据、敏感数据出境。

（一）强化数据流动的国家监管

美国作为全球数字经济的引领者，希望保持其在数字领域的优势地位，同时出于对国家安全、数据安全以及地缘政治的考虑，开始强化对数据流动的国家监管。以《敏感数据行政命令》为主要标志，美国历史上首次针对数据跨境传输设置审查机制，在数据政策上从倡导自由流动向限制自由流动进行调整，禁止或限制美国主体与“受关注国家”及其有关的受限制主体开展涉及特定美国主体大量敏感个人数据及美国政府相关数据的交易，包括数据经纪交易、基因组数据交易、供应商协议、雇佣协议以及投资协议等。2024 年 3 月通过的《2024 年保护美国人数据免受外国对手侵犯法》（Protecting Americans' Data from Foreign Adversaries Act of 2024）在内容上与上述行政令十分相近，进一步强调了对数据流向朝鲜、中国、俄罗斯、伊朗的限制，全面禁止个人隐私数据、生物数据、医疗卫生数据和联邦机构敏感数据被传输给以上 4 国。

总体而言，美国转向后的数据跨境监管政策呈现双重特征，体现为在安全考量前提下对盟友采取有条件开放，对竞争对手实施严格限制。在对待盟友方面，美国允许与欧洲部分国家、日本、韩国等传统伙伴保持一定程度的数据自由流动，并着力在数字贸易框架内构建范围可控的跨境数据合作网络，服务于维护美国与盟友在金融交易、情报交换等核心领域的战略合作关系，形成利益共同体并实现多方共赢。美国支持暂停“印太经济框架”（Indo – Pacific Economic Framework）中有关数字问题的工作和加入隐私执法全球合作的安排，目的之一也是重新评估和调整其在亚太地区的经济和战略参与方式，确保与盟友的数字政策协调一致。在对待对手方面，美国针对中国、俄罗斯等所谓对手国家，以保护国家安全为由对数据流动进行严格限制。这反映了美国对数字监管的深层调整。

这种“盟友的自由流动和对手的安全流动”的区分，本质上是美国在数字贸易领域推行霸权主义和双重标准的体现，即美国可能正在寻求一种更为平衡的立场，既维护其数字贸易的竞争力，又响应对数据保护和安全的普遍关切，是对全球数字治理格局变化的一种回应。对于盟友，数据自由流动是为了维护美国与盟友之间的利益共同体，进一步巩固其在国际政治和经济中的同盟关系；而对于对手，所谓的“安全流动”限制则是美国遏制对手发展、维护自身霸权地位的手段。这一政策导致了国际数据流动的不平衡和不稳定，破坏了全球数字贸易的公平竞争环境，也对跨国企业的运营和全球产业链的稳定带来巨大挑战。许多跨国公司需要在不同国家的监管要求之间艰难地寻找平衡，增加了合规成本和运营风险。

（二）限制竞争对手国家

当前，随着网络空间治理中的“数据战”愈发激烈，美国在双边关系上更多考量政治利益。对中国等被视为对手的国家，美国从政治角度限制数据流向这些国家的公司，以防止对美国的所谓国家安全造成潜在“威胁”。

美国在与中国、俄罗斯、古巴、朝鲜等国家的双边关系上采用阻击和封杀的方式，从政治角度出发，基于公司的国籍限制数据流向对手国家，其既定目标是消除对手国家政府获取特定美国

人信息或人口统计信息而可能造成的所谓“国家安全危害”。例如，拜登于 2024 年 4 月 24 日签署《2024 年保护美国人数据免受外国敌对势力侵害法》（Protecting Americans' Data from Foreign Adversaries Act of 2024），其核心条款规定数据经纪人出售、许可、出租、交易、转让、发布、披露或以其他方式使外国敌对势力接触居住在美国的特定个人的可识别敏感数据的行为是非法的，错误地把矛头指向朝鲜、中国、俄罗斯、伊朗或由这些国家控制的实体，或者总部位于该国或由该国人员拥有的实体。美国以国家安全为名，行单边主义和霸权主义之实，不仅侵害他国合法权益，也损害美国营商环境和国际信誉。

（三）重点管制敏感数据流动

美国认为，本国的敏感数据流动至境外会对其国家安全产生重大影响。当数据涉及敏感行业可能对美国的国家安全产生影响或威胁时，则应通过严格的国家安全审查。根据《敏感数据行政命令》第 2 条，当向中国等国家进行数据传输时，如果任何 12 个月内传输的数据数量超过特定预设阈值，数据传输行为将被禁止，如超过 100 名美国人的基因组数据、超过 1000 名美国人的地理位置数据和生物识别标识符、超过 10000 名美国人的健康和财务数据以及超过 10 万名美国人的个人标识符的数据传输等。2024 年 3 月 5 日和 10 月 29 日，美国司法部为实施《敏感数据行政命令》，先后发布了有关拟议规则的预先通知（Advance Notice of Proposed Rulemaking）[①] 和有关拟议规则的制定通知（Notice of Proposed Rulemaking）[②]，并向社会征求意见。在充分考量公众意见后，美国司法部于 2024 年 12 月 27 日发布了《防止受关注国家及相关人员访问美国敏感个人数据和政府相关数据的规定》的最终规则（Final Rule：Provisions Pertaining to Preventing Access to U. S. Sensitive Personal Data and Government - Related Data by Countries of Concern or Covered Persons），[③] 将包括中国在内的 6 个国家列入“受关注国家”之列，从而进一步限制美国人地理位置、生物识别、金融信息等敏感数据的出境。2025 年 1 月 14 日，美国商务部工业和安全局发布《确保信息和通信技术及服务供应链的安全：网联汽车》，[④] 对“嵌入了外国对手信息通信技术或服务的网联汽车”启动国家安全审查，以免“受关注国家的进口汽车”对美国的国家安全和公民个人隐私带来重大威胁。

在《敏感数据行政命令》颁布之前，美国还通过其他法规加强了对基因数据、金融数据、高科技数据的管制。例如美国的《基因信息非歧视法》（Genetic Information Nondiscrimination Act）在一定程度上限制基因数据的外流，防止基因数据被用于生物武器开发等不当用途。《银行

① See “Justice Department to Implement Groundbreaking Executive Order Addressing National Security Risks and Data Security”, U. S. Department of Justice, https://www.justice.gov/archives/opa/pr/justice-department-implement-groundbreaking-executive-order-addressing-national-security.

② See “Justice Department Proposes New Regulations to Modernize Foreign Agents Registration Act Administration and Enforcement”, U. S. Department of Justice, https://www.justice.gov/archives/opa/pr/justice-department-proposes-new-regulations-modernize-foreign-agents-registration-act.

③ See “Justice Department Issues Final Rule Addressing Threat Posed by Foreign Adversaries' Access to Americans' Sensitive Personal Data”, U. S. Department of Justice, https://www.justice.gov/archives/opa/pr/justice-department-issues-final-rule-addressing-threat-posed-foreign-adversaries-access.

④ See “Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles”, Federal Register, https://www.federalregister.gov/documents/2024/09/26/2024-21903/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles.

保密法》（Bank Secrecy Act）等相关法规要求金融机构对银行账户信息、信用记录等数据的跨境流动进行严格控制，防止金融诈骗、洗钱等风险。高科技企业的技术数据同样也在重点管制的敏感数据范围内，美国政府通过出口管制法规和数据隐私法规来限制这些企业技术数据的跨境流动。例如，美国的《出口管制条例》（Export Administration Regulations）对一些涉及高科技的数据和技术出口（包括跨境数据传输）进行严格管控。2019 年 11 月，美国又在《澄清域外合法使用数据法》（Clarifying Lawful Overseas Use of Data Act）基础上公布了《国家安全与个人数据保护法》（National Security and Personal Data Protection Act），对“特别关注科技企业”和“非特别关注企业”均提出了严格的数据出境限制要求，为维护所谓的“国家安全”，可通过实施数据安全措施或加强外资审查等方式禁止这两类企业向中国、俄罗斯等“特别受关注国家”直接或间接传输任何用户数据，以及可能用于破译该数据所需的信息。①

在此次《敏感数据行政命令》出台前，美国的出口管制更多地集中在对技术和产品的限制上。随着贸易保护主义抬头和地缘政治格局变化，美国逐步调整其对数据跨境流动的监管政策，从自由流动转向更加关注安全面向、隐私保护，从以市场自由发展为导向逐步转向强化政府控制、对敏感行业和特定领域的数据不断设置安全审查壁垒，从而提高本国数据出境的门槛，且近年来这些措施有愈发严格的趋势。例如，美国参议院人工智能工作组于 2024 年 5 月发布的《推动美国人工智能创新：美国参议院人工智能政策路线图》强调，要支持一项强有力的、全面的联邦数据隐私法来保护个人信息，以解决与数据最小化、数据安全、消费者数据权利、同意和披露以及数据经纪人相关的问题。②

四　美国数据跨境监管立场转向的原因

美国的数据跨境监管从自由流动转向安全流动，是全球数据竞争多重因素共同作用的结果，主要包括政治、经济、技术因素。

（一）政治因素：泛化数据出境国家安全风险

国家安全是各国限制数据出境的出发点之一。特朗普在第一任期就注重将国家安全与经济安全紧密结合，在很多政策中扩大国家安全例外条款的适用范围，将其应用到技术、数据等领域，试图通过重塑全球经济格局来维护美国的技术霸权，进而保障美国的全球领导地位和军事优势。③ 早在 2006 年，美国就通过《网络空间作战国家军事战略》（National Military Strategy for Cyber-space Operations）④ 宣示其在数字领域维持所谓领导地位的立场。⑤ 在科技、5G 建设、供应

① See “National Security and Personal Data Protection Act of 2019”, GovInfo, https://www.govinfo.gov/app/details/BILLS-116s2889is.

② See Schumer, Charles E., “Driving U.S. Innovation in Artificial Intelligence: A Roadmap for Artificial Intelligence Policy in the United States Senate”, https://www.govinfo.gov/app/details/GOVPUB-Y1_3-PURL-gpo229697.

③ See Sara Gerke, Delaram Zaeikhonakdar, “Privacy Shield 2.0—A New Trans-Atlantic Data Privacy Framework between the European Union and the United States”, (2023) 45 *Cardozo Law Review* 351, pp. 375-386.

④ See Ilai Saltzman, “Cyber Posturing and the Offense-Defense Balance”, (2013) 34 *Contemporary Security Policy* 40, p. 49.

⑤ 参见沈逸：《后斯诺登时代的全球网络空间治理》，载《世界经济与政治》2014 年第 5 期，第 153—154 页；朱兆一、陈欣：《美国“数字霸权”语境下的中美欧“数字博弈”分析》，载《国际论坛》2022 年第 3 期，第 56 页。

链安全等问题上，特朗普政府常常援引“国家安全”作为理由，实施出口管制、技术禁令、经济制裁等措施。特别是在特朗普第一任期内的中美贸易战期间，美国加大了数据出口管制力度。拜登政府进一步强化了这一趋势，发布了一系列行政命令和拟议规则，丰富了美国限制数据跨境流动的法律框架。

2024 年 11 月 19 日，美中经济与安全审查委员会（US China Economic and Security Review Commission）发布的 2024 年年度报告建议“全面审查中美经贸关系及其对美国国家安全的影响”，加大对华经济遏制和打压力度，实现“确保美国在与中国的战略竞争中占据优势地位”的战略目标。[①] 可以看出，随着中美贸易战再次升级，特朗普第二任期将继续以“国家安全”为由强化此前的数据跨境监管立场。

美国 2022 年《国家安全战略》（National Security Strategy，2022）将数据，特别是涉及人工智能、基因组学、地理定位、生物识别等前沿领域的敏感数据，视为国家安全的核心资产和关键基础设施的一部分。[②] 2023 年《国家网络安全战略》（National Cybersecurity Strategy，2023）也强调防止所谓敌对势力通过信息技术威胁国家安全。

在泛化国家安全的叙事体系下，美国通过不断发布行政命令、立法议案和舆论炒作夸大数据流动风险，力图构陷抖音国际版（TikTok）、微信（WeChat）等数字应用程序存在“数据窃密”，限制和阻止抖音国际版和微信在美国的运营。由此，在数据跨境涉及的国家安全问题上，美国两党也形成一致立场。尽管侧重点可能有所不同，但对外国政府可能获取敏感数据的担忧成为两党不同政见的少有共识交叉点。例如，特朗普在第二任期开始后宣布撤销拜登政府的若干政策，却保留了《敏感数据行政命令》。2024 年通过的《保护美国人数据不受外国监视法》（Protecting Americans' Data from Foreign Surveillance Act）进一步强化对个人数据的管制，防止个人数据流向所谓的对手国家。

（二）经济因素：贸易保护主义

美国受益于经济全球化，也率先实现了互联网的商业化。在过去的 30 多年里，美国通过塑造其与贸易伙伴间的低保护数据流动政策，推动数据要素向美国汇聚，实现了数字经济的繁荣。[③] 但是，美国互联网企业全球布局，利用向外国关联方公司支付知识产权特许权使用费、签署成本分摊协议、转移定价、成立混合实体、进行债务分配等方式，把收入从美国向其他离岸低税收管辖区和避税天堂转移避税，影响了美国国内的税收收入。[④] 而且，跨国互联网企业的“离岸外包”模式也影响了美国国内的就业岗位。受这些因素的影响，美国的数字经济在“美国优先”的导向下，对外向式扩张中的数据要素外流有了更多顾虑。

另一方面，随着数据成为驱动生产和技术发展的关键要素，数据跨境流动的战略价值更加

---

① 参见刘敬东：《美涉华经贸立法新动向及中国的因应》，载《中国法律评论》2025 年第 2 期，第 161 页。

② See “National Security Strategy”, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

③ 参见洪延青：《推进“一带一路”数据跨境流动的中国方案——以美欧范式为背景的展开》，载《中国法律评论》2021 年第 2 期，第 31—35 页。

④ See Fair Tax Foundation, “The Silicon Six and their Enduring Global Tax Gap”, pp. 8-10, https://fairtaxmark.net/wp-content/uploads/Silicon-Six-Report-2025.pdf; Jane G. Gravelle, “Tax Havens: International Tax Avoidance and Evasion”, pp. 11-16, https://sgp.fas.org/crs/misc/R40623.pdf.

凸显，数据的竞争成为国家间竞争的重要内容。随着中国等国家在全球数字经济价值链中的地位上升，美国实施限制数据跨境的策略，设置贸易限制、投资审查等一系列贸易和投资壁垒，试图限制这些非美国企业在美国的运营，一方面保护 Meta、谷歌等本土企业的市场份额，另一方面维系其数字经济霸权，打压中国等国家的发展空间。①

当然，从宏观的国家整体经济安全层面来看，美国针对数据跨境监管机制的调整并非综合性调整，而是针对挑战其霸权的特定国家的定向调整。美国企图通过控制关键数据的跨境流动以减少对有竞争力的外国数据处理服务的依赖，避免关键经济领域因数据控制权分散而影响其竞争力和霸权利益。对于其他没有竞争力或美国可以实质影响控制的国家或地区，美国仍然强调数据的自由流动，以延续其既有的数字经济优势。

（三）技术因素：信息技术霸权受到冲击

与数字经济竞争格局调整同步，美国的信息技术霸权也正面临来自中国等发展中国家的竞争。互联网商业化以来，信息技术先后经历了网络化、数字化、智能化发展的不同阶段。在网络化阶段，美国的信息技术具有显著领先优势。进入数字化阶段，中国已经和美国同处领先梯队，也是彼此的主要竞争对手。② 这一时期，在电子商务、短视频、社交媒体领域，中国互联网企业通过商业模式创新和成本优势，已经对美国本土企业形成竞争压力。在生成式人工智能发展带来的智能化新阶段，在美国打压下，中国企业进一步加大追赶步伐。这一形势引发高度重视人工智能技术并致力于巩固和扩大其战略优势的美国政府的战略焦虑。例如，深度求索（DeepSeek）技术创新带来的冲击，引发了美国强烈反应。美国国会议员甚至发起了《2025 年美国人工智能能力与中国脱钩法案》（Decoupling America's Artificial Intelligence Capabilities from China Act of 2025），企图通过对使用中国人工智能大模型的行为设定最高 20 年监禁和 1 亿美元的高额处罚构建封锁。

高质量数据已经成为人工智能技术进步的核心驱动资源。中国人工智能技术的快速发展甚至突破，进一步助推了美国数据跨境政策的转向。如果说其他国家通过数据本地化加强网络防御的行为促使美国在国际层面倡导自由流动的战略，那么中美技术竞争则塑造了美国增强网络防御的意愿和数据本地化政策。③ 美国在感受到来自中国的竞争压力后，转而提倡数据本地化处理，对国外跨国公司施加限制，甚至直接禁止外国公司进入。④ 美国通过限制敏感数据和高价值数据的流出，尤其是对那些可能被用于训练和优化中国人工智能大模型的数据，以维持在数据驱动创新上的优势，降低技术外溢的风险，避免所谓的中国借助数据分析对美国的先进技术进行反向工程。在芯片等硬件软件限制之外，数据跨境出口管制也成为美国打压中国人工智能技术发展的重

---

① See Bernard Horowitz, Terence Check, "*TikTok v. Trump* and the Uncertain Future of National Security – Based Restrictions on Data Trade", (2022) 13 *Journal of National Security Law and Policy* 61, pp. 72 – 101; Saeed Samiee, "Transnational Data Flow Constraints: A New Challenge for Multinational Corporations", (1984) 15 *Journal of International Business* 141, p. 149; Susan Ariel Aaronson, "At the Intersection of Cross-Border Information Flows and Human Rights: TPP as a Case Study", https://www2.gwu.edu/~iiep/assets/docs/papers/2016WP/AaronsonIIEPWP2016 – 12.pdf.

② 参见阎学通：《数字时代初期的中美竞争》，载《国际政治科学》2021 年第 1 期，第 24—25 页。

③ 参见华佳凡：《美国跨境数据流动国际倡议与国内政策的差异及其成因》，载《情报杂志》2024 年第 1 期，第 99 页。

④ See Saeed Samiee, "Transnational Data Flow Constraints: A New Challenge for Multinational Corporations", (1984) 15 *Journal of International Business Studies* 141, pp. 149 – 150.

要工具和其“小院高墙”战略的重要内容。

可以看出，美国政府对数据跨境监管政策的调整并非孤立存在，而是与美国维护其在全球科技竞争特别是信息技术霸权的总体战略紧密相连。这也是特朗普再次上任后虽然废除了拜登政府的多项行政命令，但仍保留《敏感数据行政命令》的重要原因。

五　美国数据跨境监管立场转向的前景及中国的应对

虽然美国政府以国家安全为由不断强化对数据跨境的监管，试图在全球范围内重塑数据跨境格局，但其转向后的监管政策在实施上仍然存在不确定性，面临许多国内外的约束条件，包括国内法规的限制、商界的批评以及盟友的质疑等。因此，美国未来在具体路径上将遵循“封杀对手”和“数据盟友”的“两手”进路，在风险可控的情况下仍保留参与全球贸易的意愿。中国应当积极采取措施，系统应对美国数据跨境监管带来的不利影响。

（一）监管转向基调下的不确定性：国内外约束条件

转向后的美国数据跨境监管政策在实施上仍然存在诸多不确定性。一是国内法律体制的限制。在美国的政治体系中，政党政治下的“三权分立”原则确立了立法、行政、司法三分支之间的竞争博弈框架。总统选举、利益集团以及媒体和公众舆论等多元力量，也可以对总统的权力行使施加限制。美国众议院在 2023 年成立了“中美战略竞争特设委员会”（Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party），并高调召开了一系列听证会推进涉华议题。虽然两党在数据跨境流动问题上存在一些总体共识，但其成员在具体涉华议题上的立场仍然难免出现分化，美国国内外也出现了对该委员会不满的声音。这些因素都不同程度制约着该委员会的工作。[①] 总统发布的《敏感数据行政命令》，尽管具有与法律同等的效力，但其有效性前提在于不得与美国宪法或任何联邦法律相冲突。在现行国内法规框架下，美国对数据跨境的限制性政策和具体措施可能会遭遇不小的挑战和阻力，需要在现有法律和政治结构中寻找平衡点。司法审查同样能够发挥限制数据跨境政策实施的重要制衡作用。[②]《敏感数据行政命令》及其配套规则的实施，如果对特定企业开展调查、带来限制性影响，相关企业可以在美国提起诉讼以维护自身利益，甚至可以对《敏感数据行政命令》合宪性提出质疑。

二是国内商界的批评。美国的数据跨境监管转向，更多关注的还是国家整体层面的利益，而非仅仅是某些企业“一城一池”的得失，因此必然难以照顾到所有企业的利益。但企业由于天然的逐利性，尤其是谷歌、亚马逊、微软等全球化程度非常高的大型科技企业，对数据自由流动具有强烈需求，其个体利益与国家经济利益之间并不必然完全重合，甚至在某些情况下存在相反的考量。加之美国对 WTO 框架下数字贸易提案的撤回以及《敏感数据行政命令》的出台，本身

① 参见陈佳骏：《美国众议院“中国特设委员会”的活动及影响评析》，载《当代美国评论》2023 年第 4 期，第 19—22 页。

② 〔美〕戴维·B·马格莱比、保罗·C·莱特著：《民治政府：美国政府与政治》（第 23 版·中国版），吴爱明、夏宏图编译，中国人民大学出版社 2014 年版，第 14 页。

也包含限制和约束大型科技公司的意图。因此，美国的部分跨国企业和商业团体会担心这些限制数据跨境自由流动的新规则影响其自身的正常国际业务。当拜登政府决定撤回美国对 WTO 数字贸易条款的支持时，一个由 32 名议员组成的两党小组写信给拜登，称美国贸易代表办公室的举动将造成“政策真空”，有可能使中国和俄罗斯决定全球数字贸易规则。① 针对数字贸易规则中的数据跨境问题，2024 年 6 月 12 日，来自 45 个州的 150 多个州和地方商会与美国商会一起致信白宫国家安全委员会和国家经济委员会，敦促拜登政府改弦易辙，指出：“去年年底，美国贸易代表推翻了美国长期以来对数字贸易规则的支持，这有可能削弱美国的领导地位，并威胁到许多美国企业的全球竞争力。我们敦促政府改变方向，重申支持美国企业的强有力的数字贸易规则。”②

三是盟友的质疑。美国的数据出口管制政策和国际合作所面临的难题和挑战已经显而易见。有些盟友会怀疑，美国的数据出口限制是一种以邻为壑的政策，在利用出口管制政策封锁中国等对手国家的同时，也在以牺牲盟国利益为代价重新分配与盟国之间的经济和政治利益。因此，如果美国无法合理解释其所谓的“国家安全受到威胁”，则其贸易伙伴可能会怀疑美国数据跨境政策转变的真正动机，从而没有动力加入美国的数据跨境体系。面对跨大西洋贸易关系的紧张态势，美国商会指出，尽管就新的隐私保护协议达成共识，以保障美国以数据为驱动的企业能够合法获取所需数据至关重要，但欧洲的数字法规及其提出的数字税种可能逐渐演变为一种数字保护主义的形态，③ 这种强势态度使得美国很难与盟友取得一致的观点，自 2016 年《跨大西洋贸易与投资伙伴关系协定》（Transatlantic Trade and Investment Partnership）谈判暂停以来，双方已经难以再取得共识。④

（二）监管转向的未来趋势

通过从贸易、国家安全和隐私的角度进行分析，美国的数据跨境监管大抵会遵循 4 种模式。第一种模式以自由贸易为核心，强调数据自由流动，通过与中国的自由贸易获得利益。但随着中美贸易战和中美脱钩，这一模式在中短期内显然不可能复现。第二种模式以国家安全为核心，强调避免敏感的国家安全信息落入竞争对手国家手中，防止自由贸易对国家安全造成危害。第三种模式以隐私保护为核心，要求制定全面的隐私立法以规范数据跨境流动，但这一模式需要建立在两党共识之上，目前显然也难以实现。第四种模式以团结盟友为核心，强调在风险可控的情况下，保留参与全球贸易的意愿。

---

① See “32 Bipartisan Senators Call on White House to Reverse Course on Digital Trade and Stand Up to China, Support American Workers and Human Rights”, the United States Senate Committee on Finance, https://www.finance.senate.gov/chairmans-news/32-bipartisan-senators-call-on-white-house-to-reverse-course-on-digital-trade-and-stand-up-to-china-support-american-workers-and-human-rights.

② See “State and Local Chambers Urge Administration to Support Digital Trade Rules”, U.S. Chamber of Commerce, https://www.uschamber.com/international/u-s-chamber-of-commerce-state-and-local-chambers-urge-administration-to-support-digital-trade-rules.

③ See “Transatlantic Relations: Convergence in Principle, Divergence in Fact?”, U.S. Chamber of Commerce, https://www.uschamber.com/international/transatlantic-relations-convergence-principle-divergence-fact.

④ See “Statement from USTR Spokesperson Adam Hodge”, Office of the United States Trade Representative, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/statement-ustr-spokesperson-adam-hodge.

美国数据跨境监管政策的转向，秉持其一贯的霸权思维、国家安全考量以及“美国利益优先”原则，但这并非一蹴而就。特朗普第二任期开始后，出台了一系列政策措施强化“美国利益优先”原则，例如废除拜登政府于 2023 年 10 月 30 日签署的“安全、可靠和值得信赖的人工智能开发和使用”行政命令以强化本国人工智能的竞争优势，退出《巴黎协定》（The Paris Agreement）、世界卫生组织、联合国人权理事会等以脱离多边合作框架。

参考上述 4 种模式，美国在具体路径上更可能遵循“以国家安全为核心”和“以团结盟友为核心”的“两手”进路。一方面，针对中国、俄罗斯等特定竞争对手，美国将继续采取更为严厉的数据跨境管制。例如，特朗普在当选后表示，他上任后将废除拜登政府宣布的每一项行政命令。但截至 2025 年 5 月，特朗普并未废止数据跨境相关行政命令，且《敏感数据行政命令》已在 2025 年 4 月 8 日生效，并于 2025 年 4 月 11 日发布了“常见问题解答”、[①]“前 90 天实施政策”、[②]“合规指引”[③] 3 个文件，明确给出 90 天时间帮助企业落实合规义务。可以看出，特朗普政府对该行政命令的执行逻辑是国家安全而非个人信息保护，即《敏感数据行政命令》是一部“涉及数据的国家安全法”，而不是一部个人数据保护法。[④] 另一方面，美国继续与其盟友在数据领域加强合作，通过保持或签订新的双边或多边协议，共同构建数据安全防护体系，确保数据在同盟国家间安全流动。

不过，我们尚需关注另一个问题，即虽然美国在 WTO 电子商务谈判中撤回了包括数据跨境自由流动在内的部分数字贸易主张，但是美国与多个国家签署的 FTA 仍然保留了数据跨境自由流动的规定。美国是否需要对这些已有的数据跨境自由流动规则进行重新谈判？本文认为，这一问题取决于美国与“数据盟友”之间的利益需求是否发生变化。

相较于多边贸易协定，FTA 具有较强的灵活性，即使美国撤回了在 WTO 中的立场，仍然可以通过与其他“数据盟友”保持现有的或签署新的 FTA 来维持跨境数据流动自由化的规则。因此，美国不一定需要在已有的 FTA 中重新谈判这些条款。现有的 FTA 规定仍然有效，除非双方有新的政治或经济需要重新调整这些条款。例如，美国可能要求在 FTA 中加入更多的隐私保护条款，或者要求对方国家采取符合美国标准的数据保护措施。此外，美国可能会在其他国际平台（例如 G7、G20 等）上推动全球统一的数据流动与隐私保护标准，试图通过 WTO 之外的多边框架来落实其主张。这也可能导致美国在未来的 FTA 中要求采用这些全球标准，以确保其在跨境数据流动方面的主导地位。

（三）中国的应对措施

美国的数据跨境监管转向，可能导致中国企业在获取美国用户数据方面面临更多的审查和限制，这增加了商业活动的不确定性和成本，将对中国的数字产业发展和相关企业的业务开展产生

---

① See “Data Security Program: Frequently Asked Questions”, U. S. Department of Justice, https://www.justice.gov/opa/media/1396351/dl.

② See “Data Security Program: Implementation and Enforcement Policy through July 8, 2025”, U. S. Department of Justice, https://www.justice.gov/opa/media/1396346/dl? inline.

③ See “Data Security Program: Compliance Guide”, U. S. Department of Justice, https://www.justice.gov/opa/media/1396356/dl.

④ 参见《防止中国获取美国人敏感数据的联邦法规生效，中企美国子公司需格外注意一点》，东不压桥研究院，https://mp.weixin.qq.com/s/Rk4KSQr1ZLLwt1ujLKCvKA。

较大影响。同时，《敏感数据行政命令》可能会进一步加剧中美之间的技术脱钩趋势，减少中国企业在美国的投资和技术转移机会。为应对美国的数据跨境管制的不利影响，中国可以采取一系列法律与外交手段，充分利用美国国内法规的保护机制以及国际规则的杠杆效应，基于对局势的分析伺机而动，从而创造在数据领域契合本国发展的有利条件。

一是建立中国企业的海外维权机制，通过提供资金、法律专家等方式支持受美国制裁的中国企业，鼓励其利用美国国内法规进行法律层面的应对。一方面要设立专项涉外法律应对基金，对企业提供资金援助，缓解企业可能因漫长的法律诉讼而产生的资金压力，确保企业在应对制裁过程中有充足的资金保障，避免因资金短缺而放弃法律维权。另一方面要整合国内的国际法、美国法以及数据领域的法律专家，成立专门的涉外法律应对专家智库，建立涉外法律研究平台。智库和平台应深入剖析美国在数据跨境规定上的漏洞、与国际通行规则的冲突之处，及时将研究成果分享给企业，并定期组织针对受制裁企业的培训和指导。此外，政府要加强各部门之间的政策协调，商务、司法、外交等部门形成合力，鼓励企业积极运用法律手段进行海外维权。

二是利用 WTO 争端解决机制遏制美国在数据跨境领域泛化国家安全的行为。在因美国阻挠，WTO 上诉机构无法实质作出有效裁决的情况下，我们仍要重视 WTO 法律行动的政治效果和为后续反制措施提供合法性支撑的特有价值。美国一直未能清晰界定和证明数据跨境领域国家安全的具体威胁类型，缺乏充分的证据来证明数据跨境流动会对其国家安全构成哪些实际威胁，因而使得国家安全例外条款成为非安全领域的贸易保护工具。当美国的国家安全泛化措施对中国数据跨境企业造成实质性损害时，中国应果断提起 WTO 争端解决程序，[①] 依据以往 WTO 争端解决实践中确立的审查标准和原则，组织有力的证据，证明美国措施的违法性，维护中国企业在国际市场的公平竞争环境。如果相关主张能获得 WTO 专家组支持，专家组意见可以在中美谈判时引用，从而对美国施加道义上的压力。进一步地，专家组意见还可以作为中国开展数据跨境国际合作、获取更多国家支持的有力理据。

三是建立中国的数据跨境国际合作体系。首先，在理念上应继续以开放普惠助推协同共治。中国可以协同其他国家和地区共同落实《人工智能能力建设普惠计划》、[②]《全球数据跨境流动合作倡议》，[③] 通过人工智能技术和产业更好赋能其他国家发展，为数据有序自由流动营造更好环境。其次，在加强政府间数据跨境政策协调的同时，鼓励中国企业增强进入欧盟等发达经济体和东盟、中东、非洲等地区新兴经济体合规运营的能力，通过市场机制加强与其他国家的数据跨境合作。最后，通过不断完善中国版本的数据跨境流动方案，推动中国方案的成效得到更多国家认同，进而在更多国际规则中体现。此外，中国应积极参与联合国国际贸易法委员会、国际电信联

① 参见彭阳：《国际经济治理中的国家安全泛化：法理剖析与中国应对》，载《国际法研究》2022 年第 5 期，第 100—107 页。

② 中国在 2024 年 9 月 25 日联合国总部举行的“人工智能能力建设国际合作高级别会议”上发布《人工智能能力建设普惠计划》，提出“合作推动数据依法有序自由跨境流动，探索构建数据共享的全球性机制平台，维护个人隐私和数据安全”。

③ 《全球数据跨境流动合作倡议》由习近平主席在 2024 年 11 月的亚太经合组织第三十一次领导人非正式会议上提出，并于 2024 年世界互联网大会乌镇峰会正式发布全文。该倡议呼吁：政府、国际组织、企业、民间机构等各主体坚守共商共建共享理念，发挥各自作用，推动全球数据跨境流动合作，携手构建高效便利安全的数据跨境流动机制，打造共赢的数据领域国际合作格局，推动数字红利惠及各国人民。

盟等国际组织的数据治理相关工作，在联合国框架下推动数据跨境国际规则朝着更加公平、合理的方向发展。

The Shift in U. S. Cross-Border Data Regulation: From Free Flow to Secure Flow

Zhou Hui and Yan Wenguang

Abstract: In its early stages, the United States established a market-oriented data regulatory system domestically and forged a data cooperation strategy emphasizing both bilateral and multilateral frameworks internationally, rooted in the core philosophy of free data flows and supported by lenient domestic regulations and extensive international collaboration. However, with the profound realignment of global strategic competition, U. S. data regulatory policies have gradually shifted toward a model of "limited free flow under the premise of security". This transformation is manifested in three key dimensions: strengthening national regulation in digital trade, imposing politically charged restrictions on specific competitor nations, and establishing a control system for sensitive data flows. The primary drivers behind this regulatory pivot include the overgeneralization of national security risks associated with cross-border data flows, the promotion of trade protectionism, and challenges to its information technology hegemony. Nevertheless, the implementation of the revised cross-border data regulatory regime faces multiple uncertainties, including constraints from domestic laws, criticism from the business community, and skepticism from allies. Overall, the U. S. is expected to intensify cross-border data regulation toward so-called "adversary" nations like China while advocating for data free flow among allies under security safeguards. China should proactively respond by establishing overseas rights protection mechanisms for Chinese enterprises, leveraging the WTO dispute settlement mechanism, and constructing an international cooperation framework for cross-border data flows.

Keywords: U. S. Cross-Border Data Flows, Cross-Border Data Flows, Cross-Border Data Regulation, Free Cross-Border Data Flows, Overgeneralization of National Security

（责任编辑：谭观福）