中美数字贸易规则视角下跨境数据流动安全与优化路径

王思语[1]　徐瑞希[1]　毛　培[2]

（1. 上海对外经贸大学，上海 201620；2. 海关总署研究中心，北京 100005）

摘　要：跨境数据流动在促进开放与合作的同时，也对国家安全、数据主权及个人隐私保护构成挑战与威胁，平衡数据“开放”与“安全”关系尤为关键。数字贸易规则中跨境数据流动的治理框架聚焦三大核心领域：跨境数据流动与数据存储本地化、个人信息权益与隐私保护机制以及跨境数据知识产权保障与促进。深入分析中美在数字贸易规则与数据跨境管理上的差异可见，双方诉求与路径存在根本分歧。中国既有市场与技术优势，也面临国际规则压力。面对美国“规锁”策略，中国需统筹安全与发展，稳步推进数据有序流动，构建中国特色跨境数据治理体系，以增强在全球数字治理中的制度影响力。

关键词：数字贸易规则；跨境数据流动；数据安全；中美关系

中图分类号：F49/F744　　**文献标识码：**A　　**文章编号：**1006-1894（2026）01-0107-12

一、引言与文献综述

数据要素被视为国家新型基础性战略资源，成为数字贸易的驱动力量和新型比较优势来源。与此同时，数据流动已跃升为贸易对象，摆脱了作为贸易附属品的传统定位。数据一旦上升为国家的战略资源，数据安全便成为国家安全的新边界。从国家安全保障与数字经济发展双重战略视角审视，数据安全已成为主要经济体战略规划的重点。美国《联邦数据战略及 2020 行动计划》与《国防部数据战略 2020》明确将数据定位为战略资源加以发展，并实施严格的安全措施以保障关键数据安全，构筑国家安全防护体系。中国依托《网络安全法》（2016）与《数据安全法》（2021），对国内重要数据资源实施管控与安全评估。《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（2022）强调，应统筹发展和安全，贯彻总体国家安全观，强化数据安全保障体系建设，确保数据在供给、流通、使用过程中安全无虞，明确监管界限。

跨境数据流动指数据处理者向境外提供数据读取、存储和处理的活动。随着物联网、云计算等技术的飞速发展，跨境数据流动规模爆炸式增长，成为推动全球经济互动的命脉。《全球数字治理白皮书（2023）》提出，2022 年全球跨境数据流动规模达 99.7 万 GBPS，近 3 年平均规模增速超过 30%。同时，跨境数据流动正重塑全球产业链与价值链，加速推动中高端环节向那些具备数据资源和智能技术优势企业及地区转移。然而，数据跨境流动在带来多方面正面影响的同时，数据的采集、加工、使用、储存等每个环节都可能存在安全漏洞。在数字地缘政治加速演进的背景下，放大对国家安全、数据主权和个人隐私安全的挑战与威胁。因此，必须把握好跨境流动尺度，在“发展”与“安全”之间寻找平衡点，推动跨境数据安全有序地流动。

在大数据时代，跨境数据流动的监管成为平衡数据保护与自由流动的关键（许可，2021）。在跨境数据治理领域，学者们深入剖析区域贸易协定中的电子商务与数字贸易条款，尤其是“跨境

作者简介：王思语，上海对外经贸大学国际组织学院（贸易谈判学院）副教授，研究方向：数字贸易、全球价值链；徐瑞希（通信作者），上海对外经贸大学国际经贸学院硕士研究生，研究方向：数字贸易；毛培，海关总署研究中心宏观经济部副研究员，研究方向：数字贸易。

基金项目：国家社科基金一般项目“数智化提升制造业创新效能的机制与路径研究”（项目编号：25BTJ026）。

数据自由流动”与“计算设施的位置”规定，以洞察各国的政策导向（周念利和陈寰琦，2019；李墨丝，2020；陈寰琦和陆锐盈，2022）。不同协议间跨境数据规则的差异性反映了各国在商业利益与监管模式上的分歧（Gao，2021）。Zheng（2021）指出，跨境数据传输面临个人数据保护、信息自由流通与国家管辖权扩张之间的根本性冲突，往往只能选择其中两者。欧盟、美国与中国在监管范式上的不同抉择，构成了全球数据流动的法律壁垒与区域化的数据自由流通趋势（Zheng，2021）。欧盟采取“基于地域”的数据流动政策，对域内域外实施差异化管理。美国虽原则上支持数据跨境自由流动，但在关键技术与安全领域实则奉行数据保护主义（Yang，2021）。中国以数据主权为核心的数据本地化策略，与美国的开放市场数据治理模式及欧盟的《通用数据保护条例》（GDPR）框架形成鲜明对比。至此全球数字治理架构的分歧加剧，竞争性数字边界显现，亟需构建全球数据治理框架以应对数据流动规则碎片化及数据本地化政策滥用或过度使用问题（谢卓君和杨署东，2021）。Chin 和 Zhao（2022）亦强调，尽管区域贸易协定在跨境数据流动方面达成了一定共识，但其地域性限制未能解决建立国际监管体系以避免数据流动碎片化的根本挑战，仅可作为阶段性治理方案。在此背景下，全球数字经济竞争日益激烈，数字服务贸易竞争的核心优势不在于技术先进性的绝对领先，而在于谁能够主导并塑造相关贸易规则的制定框架（张应良和谢向伟，2024）。据 ITU 与 TeleGeography 统计，2019 年中国跨境流通数据量跃居全球之首，占全球总量的 23%，规模近乎美国两倍。[①]中国国际经济交流中心预测，到 2025 年中国数据跨境流动量将占全球约 27.8%，位居全球数据圈之首。[②]然而，中国在跨境数据流动规则制定上的影响力与其庞大的跨境数据流量及数字经济发展水平不匹配，凸显规则制定权和话语权缺失问题。相比之下，美国凭借其技术优势、国际合作与联盟、长臂管辖权以及数据治理规则制定等多方面的优势，在全球跨境数据规则制定中占据主导地位，不仅成功捍卫了自身的数据利益，还对中国等新兴国家形成了数据“规锁”之势。总体而言，中美两国在数据政策领域呈现竞争与冲突并存的态势，美国积极寻求在全球数据治理中占据主导地位，中国亦在积极参与和推动全球数据治理框架的构建。双方在数据安全保障和跨境数据流动规则等方面存在显著的利益分歧与不同考量。本文从中美两国跨境数据流动的国际承诺和国内数据法律框架、政策动向进行分析，揭示中美在追求跨境数据流动安全道路上的核心诉求与分歧，旨在有效地应对来自美国的技术竞争和国家安全挑战。

二、数字贸易规则下跨境数据流动安全条款探析

全球跨境数据流动规模激增，但数据治理尚付阙如。目前全球缺乏统一的数据治理规则，使得事关全球经济和国家安全的重大问题悬而未决。由于多边贸易规则难以适应跨境数据流动的发展，主要经济体转向单边、双边或区域贸易协定等多元路径，导致跨境数据治理出现碎片化、离散化现象。美国在区域贸易协定（RTAs）中推动跨境数据自由流动与限制性措施并行，体现“开放模式”；欧盟在“隐私保护优先”原则下，温和处理跨境数据流动，域内自由域外管辖，为“中间模式”；中国强调数据主权、安全与发展，确保数据安全的同时，寻求个人信息保护与国际规则协调以及数据传输自由，代表“安全模式”。由此可见，美国、欧盟、中国等主要贸易经济体的数据治理范式分歧明显，形成新的“数字鸿沟”（陈寰琦，2022）。

数字贸易的蓬勃发展依赖数据的自由流动，因此，数字贸易规则体系自然包含了直接或间接涉及数据流动的条款。近年来，通过双边或区域贸易协定管理跨境数据流动的做法已逐渐成为主流趋

① Nikkei Asia.China Rises as World’s Data Superpower as Internet Fractures[EB/OL].2020,Nikkei Asia.https://asia.nikkei.com/Business/Technology/China-rises-as-world-s-data-superpower-as-internet-fractures.[2020-11-24](2025-12-25).

② 上海证券报.数字贸易:带动数字经济发展的关键抓手[EB/OL].2024,中国服务贸易指南网.https://tradeinservices.mofcom.gov.cn/article/szmy/zjyjgd/202405/163614.html.[2024-05-08](2025-12-25).

势（Chin and Zhao，2022）。以《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《数字经济伙伴关系协定》（DEPA）、《区域全面经济伙伴关系协定》（RCEP）等为代表的新兴亚太地区经贸机制，正日益成为推进跨境数据治理的主要平台（王惠敏，2023）。与此同时，美国主导的《美墨加协定》（USMCA）、《美日数字贸易协定》（UJDTA）等双边和多边经贸协议，也逐渐成为美国推动与之价值理念相近、经贸往来密切的国家实现跨境数据规则对接与协调的重要工具。尽管“美式模板”和“亚太模板”下的数字贸易规则在数字贸易和数据保护主义的采用上似乎达成了坚定的共识，但这些话语背后的价值结构却存在分歧。本文从数据流动和安全保护角度梳理数据治理规则（表1），将其分为跨境数据流动与本地化存储、个人信息权益与隐私保护机制、跨境数据知识产权保障与促进3个核心领域，分析“美式模板”和“亚太模板”下的数据规则，揭示不同经济体在跨境数据流动与安全领域的立场和分歧。

表1　RCEP、DEPA、CPTPP、UJDTA和USMCA相关条款梳理

条款		中国加入或申请加入		美国主导		
		亚太模板		美式模板		
		RCEP	DEPA	CPTPP	UJDTA	USMCA
		2020.11	2020.6	2018.3	2019.11	2018.11
跨境数据流动与本地化存储	跨境数据自由流动	12.15 8.1.9	4.3	14.11	11	19.11
	计算设施的位置	12.14	4.4	14.13	12 13	19.12 17.18
个人信息权益与隐私保护机制	个人信息保护	12.8 8.1.9、8.5	4.2	14.8、11.8	15	19.8 32.8
	在线消费者保护	12.7	6.3	14.7	14	19.7
	非应邀商业电子信息	12.9	6.2	14.14	16	19.13
跨境数据知识产权保障与促进	源代码	N	N	14.17	17	19.16
	使用密码技术的ICT产品	N	3.4	N	21	N

注：根据相关协定内容整理得到；表中的数字表示该条款在协定中的章节与编号；N表示无此条款；表2同。

（一）跨境数据自由流动与存储非强制本地化

中美在数字贸易规则领域的核心分歧在于数据跨境自由流动及存储非本地化（李杨等，2016；Gao，2018）。跨境数据自由流动与数据存储非强制本地化构成了跨境数据治理的核心框架，旨在促进数据流动、降低数据存储与处理成本，同时保障国家安全。该治理模式通过设立例外条款应对数据流动带来的安全风险，为各国制定数据政策提供参考，体现数据流动与安全之间的平衡考量。RTAs在制定跨境数据流动条款时普遍参考这一框架，但约束力存在显著差异：“美式模板”条款的约束力日益增强，而“亚太模板”则更多依赖例外条款，约束力相对较弱。

1. 跨境数据自由流动

跨境数据流动监管在不同经济体间存在显著差异，体现了各自的文化偏好和政策目标。监管方式多样，包括无监管、事后问责、有条件流动等，且同一司法管辖区可能对不同数据类型采取不同监管方式。同时，为保护数据安全，还设有若干例外情况。RTAs在跨境数据自由流动条款中均采取“自由流动为原则，限制监管为例外”模式，但在例外条款的范围、具体内容等方面存在分歧。RCEP规定缔约方应保障跨境数据自由流动，但可采取本地化措施以实现合法公共政策目标。缔约方有权决定何为“合法的公共政策”，并自主判断安全例外（洪延青，2021）。RCEP包含安全例外条款，显示其谨慎态度。它允许在特定条件下进行跨境金融信息转移，同时保留监管和审慎例外以及个人敏感信息例外。DEPA和CPTPP在跨境数据流动方面有相似措辞，相较于RCEP，两者对例外情形的适用条件设定更严格，涵盖监管例外和公共政策目标例外。美国主导的UJDTA和USMCA积极

倡导跨境数据流动的高度开放立场，将数据自由流动作为其数字贸易战略的核心原则。相关条款在坚持开放导向的同时，亦为基于合法公共政策目标的例外情形保留了必要空间。

2. 计算设施的位置

数据本地化存储可视为跨境数据自由流动条款的对立面，涵盖从无需本地存储到严格本地存储并附带国内外数据传输处理条件的多种要求，这些要求背后涉及国家安全、行业监管及产业政策等多方面考量。各数字贸易协定均认同，不得以在其领土内使用或设置服务器、数据中心等计算设施作为授予业务运营权的先决条件，其间区别主要在于实施细节与约束力度不同。这映射各协定在处理跨境数据流动议题时，均将数据本地化存储要求作为一项例外条款的处理方式。RCEP 更多地考虑通信安全和保密的要求，允许为实现合法的公共政策目标和保护基本安全利益而采取本地化措施，并在金融服务数据跨境存储议题上承诺开展对话。DEPA 继承了 CPTPP 此项条款，在保留监管例外和合法公共政策目标例外的基础上，不对跨境数据存储实施强制性的位置限制。美国主导的 UJDTA 与 USMCA 将数据本地化政策升级为无例外责任，剔除监管要求和公共政策等例外规定，限制了缔约方的政策空间。同时，若金融服务供应商在境外计算设施上存储或处理的信息能够即时、直接、完整且持续地供金融监管当局访问，则豁免其在金融服务领域的数据本地化要求。这可能导致出口商面临在本地服务器中存储数据的高代价。

总体来看，“美式模板”对跨境数据流动与存储的限制条件较少，其中，相对于 CPTPP，USMCA、UJDTA 呈现更高的自由化水平。“亚太模板”中 DEPA 基本继承了 CPTPP 的数据流动与本地化条款，承诺有约束力的跨境数据自由流动与禁止数据本地化。而 RCEP 在跨境数据的流动与保护标准方面灵活处理，利用广泛的例外条款，为各方维护自身合法利益、保障国家数据安全留下了政策调整空间。从美国主导的 RTAs 和中国签署或正申请加入的 RTAs 来看，中国更加注重跨境数据流动的安全，而美国更倾向于推动跨境数据自由流动。

（二）个人信息权益与隐私保护机制

隐私保护作为跨境数据流动的核心议题之一，推动个人信息保护认证机制逐步被纳入国际规则框架。在此背景下，贸易协定不断强化个人信息保护条款，旨在促进不同保护体系间的兼容与数据的安全流动。这些努力共同致力于构建一个更加安全、可信的数字环境。

首先，个人信息保护认证机制是保障数据跨境安全流动的必要条件，已成为国际通行准则，包括欧盟的 GDPR、亚太经济合作组织（APEC）的《数据跨境隐私规则》（CBPR）与《数据处理者隐私识别》（PRP）等认证体系。当前认证机制已成为国际上通行的个人信息跨境传输保护的重要准则。具体而言，GDPR 在第 42 条和第 43 条规定了针对数据控制者和处理者的数据保护认证程序，并在第 42 条第 2 款及第 46 条第 2 款明确，经认证的数据处理活动可作为个人数据向第三国或国际组织传输时的合规保障措施之一。APEC 亦建立了相应的认证框架，包括 CBPR 认证体系和其配套的 PRP 机制，以加强数据跨境流动的隐私保护。新加坡的《个人数据保护条例》（PDPR）框架下的监管指南认可 CBPR 与 PRP 认证作为个人数据跨境传输合规评估的参考机制。

其次，贸易协定逐渐包含个人信息保护条款，鼓励或要求缔约方建立或维持个人信息保护法律制度，以平衡个人隐私保护与国家安全需求，同时推动不同个人信息保护体系之间的兼容性和交互操作性。各贸易协定均致力于保护消费者隐私和在线消费安全，采取透明高效的措施防止欺诈商业行为，同时强调数据流动需附带个人数据保护机制，隐私和个人数据保护原则呈现趋同态势。1980 年，经济合作与发展组织（OECD）发布的《保护隐私和个人数据跨境流动指南》作为国际隐私保护的开创性文件，平衡了个人隐私与国家安全的双重需求，为后续贸易协定提供了隐私保护条款的

基准。尽管贸易协定未直接详述隐私原则，但它们逐步纳入了个人信息与在线消费者保护的相关条款，旨在激励缔约方构建并维护个人数据或隐私保护的法律架构。

在“美式模板”下，CPTPP 等协定强调构建全面的保护个人信息法律框架，并提出兼容机制与加强沟通的安排，尤其在金融服务领域严格保护个人财务信息。USMCA 援引 OECD 准则，参考 APEC 的 CBPR 机制，以增强制度兼容性。相比之下，“亚太模板”中的 DEPA 更为具体，明确原则，采用数据保护可信任标志机制，推动体系间的交互操作。RCEP 在个人信息保护上立场较为宽松，鼓励政策公开与合作，但未提出具体国际标准或深入讨论体系兼容，显示出软约束特性。

个人数据源自消费者，其安全性提升、隐私保护以及免受欺诈侵害，均为各缔约方深切关注的核心议题。各相关协议均致力于推行透明且高效的举措，以保障消费者在电子交易活动中远离欺诈与欺骗性商业行为的侵害。同时，各协议在非自愿接收的商业电子信息（如“垃圾邮件”）的相关条款上达成共识，着重强调增强信息接收者的屏蔽能力，并明确规定信息的发送需事先征得接收者的明确同意，以期最大限度地减少此类信息的传播，共同营造一个更为清朗、健康的网络消费环境。总体而言，贸易协定在强调数据流动对于数字时代贸易活动至关重要的同时，也日益认识到数据流动必须伴随个人数据保护的坚实保障。各协定在隐私与个人数据保护的原则上逐渐趋于一致，共同致力于构建一个更加安全、可信的数字贸易生态。

（三）跨境数据知识产权保障与促进

知识产权在跨境数据流动中的重要性体现在数据传输的合规性、核心技术转让与国家安全、源代码披露与数字产权等议题。跨境数据流动的常态化衍生了数据知识产权保护议题。跨境数据的存在形式，如软件代码、设计图纸、专利信息、商业机密等作为智力成果必然涉及大量知识产权范畴。企业需要确保其传输的数据不侵犯他人的知识产权，同时也要保护自己的知识产权不被侵犯。这涉及对知识产权的识别、保护和合规性评估。在跨境数据传输、存储及处理的各个环节，企业可能面临来自东道国的多重风险，如强制技术转移和商业秘密窃取等。尽管数据作为知识产权保护的新客体在国际上尚存争议，且其认定、权属及拥有方式尚未统一，但数字贸易规则已将数据流动视为优化知识产权的关键议题（Burri，2017）。区域贸易协定聚焦源代码条款及 ICT 产品条款（表 2），旨在通过额外法律保护层保障新技术和新产品涉及的知识产权，消除数字贸易中的歧视或壁垒。然而，以“源代码或算法”保护为核心的规则也限制了政府在监管和司法领域对源代码的访问能力，在一定程度上影响数据流动的自由度和政府监管能力。因此，在推动数字贸易发展的同时，如何平衡数据私有性与共享性、国际化与地域性保护之间的冲突，以及数据流动与数据保护之间的关系，成为跨境数据知识产权规则的关键考量。

“美式模板”确立源代码禁止披露原则，禁止将源代码的转移或获取作为市场准入条件，设置强制披露例外以维护监管权益。此原则在 USMCA 与 UJDTA 中得到拓展，涵盖源代码算法表达、关键基础设施软件及大众市场软件的范畴。“亚太模板”中的 DEPA 未触及源代码议题，RCEP 虽有对话倡议却未制定具体规则，显示其在数字知识产权保护方面的审慎态度，这或许源于对技术发展、市场竞争及公共利益的综合考量。数据加密技术对跨境数据流动安全至关重要，能有效防御非法截获与篡改。随着 ICT 产品出口成为推动世界贸易增长的新动力，“美式模板”下的 UJDTA 引入“使用密码技术的 ICT 产品”议题，明确规定市场准入不得与密码技术专有信息的转让或访问挂钩，并保护制造商及服务提供商免受强制性要求。而“亚太模板”中的 DEPA 对此进行了更为详尽的阐述，明确禁止以技术法规或合格评定程序强制要求转让密码相关信息。此外，UJDTA 与 DEPA 均将金融类 ICT 产品排除在适用范畴之外，体现了对特定行业的特殊考量。

表 2　跨境数据知识产权条款

知识产权条款	RCEP	DEPA	CPTPP	USMCA	UJDTA
源代码	N	N	源代码禁止披露；基础设施软件例外；专利相冲突例外；商业合同及缔约方要求修改源代码例外	源代码禁止披露；监管例外；相比于 CPTPP 剔除基础设施软件例外；剔除商业合同及缔约方要求修改源代码例外；剔除专利相冲突例外	与 USMCA 措辞相似
使用密码技术的 ICT 产品	N	取消对使用密码技术的 ICT 产品市场准入限制；金融产品例外	N	N	在“美式模板”的基础上明确提出不得强制实施以技术法规或合格评定程序的形式要求转让密码相关信息；金融产品例外

三、中美跨境数据流动安全路径对比

中美作为关键国家在跨境数据流动上的分歧将影响现有框架。上文梳理的具有代表性的区域贸易协定分别凸显了美国与中国的战略利益诉求。中国强调数据主权与安全的跨境数据流动监管模式，与美国倡导的数据自由流通原则形成鲜明对照，导致数字空间边界的重叠与潜在冲突。这种政策差异构建了新的数据鸿沟，为跨国企业在中美之间进行跨境数据流动带来了合规性挑战。随着中国数字企业的崛起和高端芯片的突破，美国调整了数据监管取向，将数据安全纳入外国投资审查、出口管制和产业监管等政策工具，并对部分中国企业实施限制性安排（表 3）。同时，中国亦在其数据安全治理框架下，对个别涉及敏感领域的美国企业和机构采取相应应对措施，相关实践显示中美在数据安全领域的政策互动呈现双向化趋势（表 4）。在此背景下，如何在保障安全的同时实现跨境数据高效流动、增强数字产业竞争力，成为亟需回应的核心议题。

（一）中美数据跨境流动分歧：美国“两面派”策略与中国渐进式开放

美国在跨境数据问题上采取双重标准，一方面推动数据主权战略，吸引数据流入，并与盟友建立“数据流动圈”，声称支持数据自由流动，美国利用其在该领域的优势主导了全球数据规则；另一方面，美国以国家安全为借口，限制国内数据流出。与美国不同，中国采取渐进式开放数据流动的治理模式，逐步扩大数据开放，同时确保数据安全。

一方面，美国通过 APEC、G20 和 WTO 等平台推广跨境数据自由流动和禁止数据本地化存储的承诺，以促进全球数据流入美国。为保持其数据领导地位，美国采取长臂管辖权和限制数据自由流动的策略，以应对潜在的数据资源挑战。2023 年 WTO《电子商务联合声明倡议》（JSI）期间，美国宣布放弃跨境数据自由流动，表明其将收紧数据流动政策，为实施包括数据出口管制在内的措施提供逻辑基础。另一方面，美国监管方式原则上支持跨境数据自由流动，但在关键技术和安全领域采取数据保护主义（表 5）。2018 年 CLOUD 法案基于“数据控制者”原则，允许美国政府获取存储在第三国的数据，并在达成行政共享“协议”的前提下允许与他国进行数据交换，规避了数据所在国的监管。美国还通过法案将数据跨境流动与国家安全捆绑，限制特定数据流到国外。《外国投资风险审查现代化法案》（FIRRMA）授权美国外国投资委员会（CFIUS）对境外企业进行数据调取，审查涉及关键基础设施、技术和敏感个人数据的外国投资，特别是来自中国的投资。在出口方面，《出口管理条例》（EAR）不仅限制硬件出口，还包括软件出口，防止科技数据转移到国外服务器。美国还加强对关键数据基础设施的管理，将中国列为特别关注国家，实施年度数据安全评估，并制裁多家中国高科技公司，禁止美国企业与其业务往来。这些措施加强了美国对数据资源的控制，并建立了数字贸易壁垒，意图限制技术竞争力强的国家获取美国数据资源，维护其在全球数字经济中的领先地位。

表 3　美国以数据安全为由制裁中国企业（部分）

时间	制裁方	被制裁方	制裁措施	制裁原因
2016 年至今	美国	深圳市大疆创新科技有限公司	通过《反中国无人机法案》(Countering CCP Drones Act)，大疆公司被列入联邦通信委员会（FCC）黑名单；2024 财年《国防授权法》，禁止联邦机构和联邦资金购买或使用被认定对美国国家安全构成“威胁”的国家制造的无人机等产品	保护美国网络数据安全，减少数据泄露和国家安全风险
2017 年 12 月	CFIUS	蚂蚁金服	否决蚂蚁金服收购速汇金（MoneyGram）的交易	担忧泄露美国消费者敏感金融数据
2019 年 3 月	CFIUS	北京昆仑万维科技股份有限公司	要求其必须出售在交友软件商 Grindr 中所持股权	担忧 Grindr 被中国企业控制，无法保障用户数据安全，进而影响美国国家安全
2019 年 4 月	CFIUS	深圳独角兽公司碳云智能	出售其在美国公司 PatientsLikeMe 中持有的多数股权	担心 PatientsLikeMe 被中国企业控制，泄露或滥用用户数据，对美国公民个人隐私和国家安全构成威胁；技术安全
2019 年至今	BIS；CFIUS	华为技术有限公司	将华为及其 70 家附属公司列入出口管制实体清单，要求美国企业出口商品、技术或服务须获得许可；禁止华为使用包含美国技术的半导体元器件；撤销相关芯片出口许可	担忧华为设备存在“安全隐患”，认为其可能收集并传输敏感数据给中国政府，损害美国公民和企业的隐私权益
2020 年 3 月	CFIUS	北京中长石基信息技术股份有限公司	要求剥离其已经完成的对美国酒店软件公司 StayNTouch 的收购	危害美国数据安全
2024 年 3 月	CFIUS	北京字节跳动科技有限公司	要求字节在一年内剥离 TikTok，否则将禁止该应用在美国运营	认为 TikTok 可能会泄露美国用户数据给中国政府，威胁美国国家安全

资料来源：作者根据相关资料整理得到；下表同。

表 4　中国在数据安全领域反制裁美国（部分）

时间	制裁方	被制裁方	制裁措施	制裁原因
2023 年 5 月	中国网信办	美国芯片制造商美光（Micron）公司	美光未通过网络安全审查，根据《网络安全法》等法律法规，中国国内关键信息基础设施的运营者应停止采购美光公司产品	美光在中国销售的产品存在大量网络安全隐患
2023 年 12 月	中国政府	美国情报数据公司卡隆（Kharon）	根据《中华人民共和国反外国制裁法》，对卡隆公司及其主要人员采取反制措施	卡隆公司长期在中国境内搜集涉疆敏感信息，为美国政府针对中国的非法制裁提供情报支持
2024 年 1 月	中国政府	美国军工企业 Data Link Solutions 等 5 家企业	根据《中华人民共和国反外国制裁法》，对该公司实施制裁，包括冻结在中国境内的动产、不动产和其他各类财产，禁止中国境内组织、个人与其进行交易、合作等	多次向中国台湾提供 Link-16 战术数据链，干涉中国内政，损害中国主权和安全利益

中国的数字经济起步相对较晚，初期主要采取防御性策略以保护数据主权，因此被认为是对跨境数据流动实施较为严格限制的经济体系。这一观点未全面反映中国政策转型动态。中国通过立法确立数据主权，构建以数据本地化为核心、辅以安全评估的治理机制，明确政府主导监管角色，实施单项数据流动控制（表 6）。《网络安全法》作为数据主权规则建设里程碑，确立数据属地管辖原则，强调“关键信息基础设施”安全，规定境内数据须本地存储。但随着数字经济全球化深化和国际环境变化，单纯数据本地化策略难以全面保障数据安全，可能形成数据孤岛，阻碍可持续发展。因此，中国积极参与区域贸易规则制定，如在 RCEP 等国际协议中，推行有管理的跨境数据流动和基于特定目标的数据本地化措施。《数据安全法》首次提出“数据安全自由流通原则”，倡导数据分级分类保护，强化数据安全审查与评估机制。同时，《数据出境安全评估办法》针对数据出境设定具体程序性规则，确立“本地存储、出境评估”的基本治理模式，在维护数据主权和数据安全的前提下，为跨境数据流动提供制度化路径。

表 5　美国跨境数据流动相关法案与行政命令（部分）

颁布时间	政策名称	相关内容
2018 年 3 月	《澄清境外数据的合法使用法》（CLOUD 法案）	实施“数据控制者”标准，要求美国企业提供其控制的存储于海外的数据
2018 年 8 月	《外国投资风险审查现代化法案》（FIRRMA）	授权 CFIUS 调查涉及“维护或收集可能以威胁国家安全的方式被利用的美国公民的敏感个人数据”和导致外商能够决定“使用、开发、获得和披露美国公民敏感个人数据”的投资交易
2020 年 1 月	《FIRRMA 最终实施细则》	降低外资审查门槛：即使未获得控制权，但只要涉及在美关键技术、关键基础设施和敏感个人数据业务的外商投资，仍需接受 CFIUS 审查；包括为美国政府或军事机构提供产品或服务的企业，以及维护、收集或以此为主要业务组成部分、规模超过 100 万人的敏感个人数据企业
2024 年 2 月	《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》（第 14117 号行政命令）	明确禁止受关注国家获取美国公民的敏感个人数据及政府相关数据；建立数据活动安全风险评估与持续监督机制，强化政府与私营部门协作，防范数据滥用和泄露风险
2024 年 3 月	《保护美国人免受外国对手控制应用程序法案》(TikTok 法案）	以国家安全为由要求字节跳动剥离 TikTok 业务，并授权对特定国家背景的社交媒体应用实施禁令或限制；为避免禁令，相关应用需通过股权出售解除控制关系，并将外资持股比例限制在 20% 以下
2024 年 4 月	《保护美国人数据免受外国对手侵害法案》（《数据隐私法案》）	禁止数据经纪人把美国个人的敏感数据传输给中国、俄罗斯等“外国对手”或者外国对手控制的实体

表 6　中国跨境数据流动相关法律和规定（部分）

颁布时间	政策名称	主要相关内容
2016 年 11 月	《网络安全法》	首次对跨境数据流动作出统一规范；关键信息基础设施运营者收集的重要数据和个人信息须在境内存储，确需出境的应事先通过安全评估；金融、电信等重点行业适用更严格的跨境数据监管要求
2021 年 6 月	《数据安全法》	考虑数据安全治理和发展的国际交流与合作，鼓励数据安全、无障碍地跨境流动
2021 年 8 月	《个人信息保护法》	关键信息基础设施运营者和达到一定规模的个人信息处理者须在境内存储数据；个人信息确需出境的，应通过国家网信部门组织的安全评估，并明确跨境提供个人信息合规路径，包括安全评估、个人信息保护认证和标准合同等方式
2022 年 5 月	《数据出境安全评估办法》	对重要数据和大规模个人信息出境实施安全评估，实行申报评估、持续监督与再评估相结合的管理机制，设置复评程序，评估结果有效期为两年，期满需重新申报
2024 年 3 月	《促进和规范数据跨境流动规定》	明确免于申报数据出境安全评估、标准合同和个人信息保护认证的数据类型；自贸试验区可在国家数据分类分级框架下制定数据出境负面清单；不涉及个人信息或重要数据，以及特定情形下的必要个人信息出境，免履行相关法定程序；完善个人信息出境标准合同与认证制度

在经济激励、技术竞争、国际数据治理规则构建需求和国际贸易协定承诺等因素推动下，中国正加速政策转型，其跨境数据政策正从规制转向促进数据开放发展的方向。2024 年发布的《促进和规范数据跨境流动规定》体现了中国扩大数据开放的决心。该规定简化数据出境的法定程序，放宽跨境流动条件，传递了放松监管、促进数据流动的信号。天津自贸试验区响应此规定，出台了首个数据出境管理负面清单，为企业提供数据流动指引。上海自贸试验区临港新片区也发布了数据跨境流动的正面和负面清单，允许风险可控的数据跨境流动，并通过清单目录指导实践。这些举措展示了中国在数据跨境流动治理方面的创新和开放，有助于建立更公平、透明、高效的跨境数据流动体系，为全球数字经济注入新活力。

（二）个人信息跨境数据流动政策转变：美国趋于封闭与中国逐步放宽

在处理跨境数据流动和隐私保护问题时，中美两国采取了不同的治理路径。中国在 RCEP 中排除了个人信息的跨境传输，而美国则支持更自由的数据流动，优先考虑数字贸易。美国的 USMCA 和 UJDTA 新增条款减轻了平台在监管个人信息方面的责任，中国则强调互联网平台在保护客户数据安全和隐私方面的责任。美国在个人信息保护法律框架上参考了 APEC 和 OECD 的原则，而中国则采取积极策略，鼓励国际合作，并在立法中参考国际标准。

中国在法律上高度重视个人信息安全。《个人信息保护法》和《网络安全法》不仅总体规定了个人信息保护，还针对特定行业提出了具体要求。同时，对个人信息出境实行严格监管，要求数据出境进行安全评估，并对个人数据出境安全评估范围进行了适度收窄。对于跨境业务活动，如确需传输个人信息，数据处理者可免予申报。例如中国首次对10万规模以下个人信息跨境流动实施豁免，数据监管重点转向批量数据。北京自贸试验区的出境数据负面清单显示，对重要个人信息出境限制放宽，特别是民航、零售及现代服务业等领域，仅需对特定类别且规模超500万人的个人信息进行出境安全评估。这将减轻中小企业及跨国公司在合规上的负担。政策转变旨在通过精准放宽核心数据出口条件，实现数据安全与发展的动态平衡。

美国监管变化与中国的方向形成对比，强调国家安全和公民隐私保护，限制敏感个人数据和政府数据跨境流动。第14117号行政命令体现了美国在外国投资和知识产权领域的传统做法，并将个人数据跨境流动限制纳入最新法律规则，显示了加强数据安全和隐私统一监管的趋势。TikTok法案和《数据隐私法案》提升了个人数据安全标准。《数据隐私法案》禁止美国数据经纪人向对手国家传输敏感个人数据，限制了数据的跨境流动。TikTok法案特别针对TikTok，以国家安全为由要求字节跳动剥离TikTok。美国近年来多次以数据安全尤其是“敏感个人数据”为由，阻止中国企业收购美国公司，反映其排斥特定国家和产业主体的政策倾向。

（三）跨境数据知识产权规则：守护跨境数据流动安全屏障

美国主要通过限制向中国出口关键技术来维护其技术优势。鉴于源代码披露可能损害其高科技企业的商业利益，因而“美式模板”设立了源代码禁止披露规则，同时规定强制披露情形，以实现合法监管目标。为保护跨国公司敏感信息，如密钥和算法，防止其被强制公开或转让，“美式模板”扩展了源代码保护范围，并新增了针对使用密码技术的ICT产品条款。《出口管理条例》限制知识产权数据跨境流动，规定美国商品、技术和软件以及含有这些美国元素的国外产品都受美国管辖。在美国境内，个人向外国国民披露或转让技术和源代码也被视为“出口”，受到政府监管。相比之下，中国基于安全监管考量，在数字贸易规则的跨境数据知识产权保护上持审慎立场。尽管RCEP提出启动源代码对话，但源代码规则及含密码技术的ICT产品条款尚未明确，反映中国数字知识产权保护标准与国际高标准存在差距，特别是在大数据、人工智能等新兴领域及专利保护方面略显滞后。尽管中国目前未实施软件源代码强制披露制度，且法律未要求企业向政府提交源代码，总体上与CPTPP等保持一致。然而，《网络安全法》及《信息安全技术移动应用网络安全评价规范》规定，网络关键设备与网络安全专用产品须通过相关部门安全审查，在此过程中外国在华企业源代码或将面临披露要求。随着中国数字企业的崛起以及中国申请加入CPTPP、DEPA，中国在数字知识产权领域亟需实现突破性进展。

四、中国跨境数据流动安全优化路径

本文全面梳理了“美式模板”和“亚太模板”下的跨境数据治理规则，揭示中美两国在跨境数据流动与数据安全领域的利益取向和治理路径差异。中国在跨境数据治理中以安全优先为基本原则，强调数据主权和个人信息保护，并在审慎监管基础上逐步推进制度型开放，探索与高标准国际经贸规则的衔接路径。相比之下，美国采取兼具开放与限制特征的策略，在对外层面推动数据自由流动和规则外溢，在对内及对盟友层面强化数据安全约束，通过制度安排塑造有利于自身的跨境数据流动格局。与此同时，中国在跨境数据知识产权和数字产品开放方面仍相对滞后，叠加中美数据政策差异及美国政策不确定性，对中国企业应对美国客户数据合规要求构成现实挑战。跨境数据流动框架的构建与谈判已超越技术协调与经济融合范畴，深度嵌入国际政治博弈与战略竞争之中。《欧美

数据隐私框架协议》旨在修复美欧关系，并在数字治理规则层面回应与中国的战略竞争。美国推动“印太经济框架”（IPEF）的重要动因之一，亦在于通过制度性安排强化其在印太地区的地缘政治影响力，并在数字贸易规则领域塑造对华竞争优势。特朗普再次执政以来，美国对多边和区域经贸机制的态度趋于审慎，其贸易政策延续对双边谈判的偏好，并对既有区域合作框架进行重新评估。尽管美国未加入 RCEP 与 CPTPP，仍试图通过双边或“小多边”安排参与亚太经贸规则塑造，这一取向在数字贸易与跨境数据治理领域尤为明显。同时，美国对 USMCA 的复审安排进一步提升全球贸易与跨境数据治理环境的不确定性。总体来看，美国在对华技术与数字领域的竞争呈现长期化和制度化特征，并持续以数据安全和国家安全为政策依据，扩大对华投资与技术合作限制，重点指向人工智能等战略性新兴领域。在此情形下，跨境数据流动中安全与开放之间的张力进一步凸显。为了在保障数据安全的同时释放数据要素跨境流动所蕴含的技术革新与经济增长潜力，中国应针对跨境数据流动的治理困境，秉持安全与发展并行的原则，优化跨境数据流动路径，推动跨境数据安全、有序流动。

（一）坚持渐进式开放，构建中国特色的跨境数据流动体系

坚持“维护国家主权、安全和发展利益”的出发点，以“自由为原则，限制为例外”为基本思路，渐进式开放数据出境，让数据放心“进来”，放心“出去”，构建中国特色的跨境数据流动体系。首先，建立多元化跨境数据管理体系，明晰跨境流动数据界限、范围和监管强度，为企业提供清晰的政策指导。具体而言，进一步细化数据分级分类，不同类别的数据实施不同类型的数据本地化措施，以平衡数据安全与经济效益。一般数据允许自由跨境流动，关键数据在确保安全的前提下适度跨境传输，而敏感数据则需严格限制其跨境流动，以防范对国家安全构成的潜在威胁。可借鉴 DEPA，鼓励企业采用数据保护可信任标志，探索可信任的数据自由流动。其次，完善数据出境安全管理制度，平衡数据安全和自由流动诉求。中国已构建以“重要数据”与“个人信息”为核心的出境监管“双轨并行”框架。下一步，亟需进一步细化数据分类与出境评估标准，降低企业合规负担，简化出境评估流程。特别是在金融、医疗、汽车等关键行业，现行监管框架仍存在对数据出境或本地化存储的较严格限制，应在对接国际规则的基础上优先修订重点行业数据管理规定，并配套发布跨境数据流动操作指南和典型应用场景示范，提升企业开展数据出境自评的可操作性与效率。同时，鼓励自贸港和自贸区深入推进数据跨境传输安全管理试点和“数据特区”建设，探索数据出境负面清单管理制度。在风险可控前提下，支持部分地区率先加入区域性数据自由流动制度安排。最后，为维护国家数据主权，可在传统领土管辖权的基础上补充效力管辖原则（Svantesson，2014），明确数据管辖范围。同时，完善数据基础设施建设，推动技术创新与自主研发，提升外部数据风险抵御力。优化国家计算设施的数据安全系统，提高数据基础设施的国产设备比例，并开发计算设施保护预警系统。

（二）提出数据跨境流动规则的“中国方案”，构建全球数据流动合作圈

中国数据开放成就显著，但跨境数据流动方案在贸易协定中体现不足，尚未与主要经贸伙伴建立数据传输通道，且面临美国等数据同盟体系的“规锁”风险。因此，中国需积极参与跨境数据流动国际协调，推动制定或签署双多边跨境数据流动国际规则。第一，根据“全球数据安全倡议”，针对跨境数据传输、数据本地化要求以及隐私保护等核心议题，拟定中国的应对方案。通过调整优化例外条款、负面清单等限制性措施，并明确数据流动豁免范围，促进“正当可控”的数据有序流动。可借鉴 APEC 跨境隐私规则（CBPR），强化数据跨境流动审查、重要数据境内储存以及数据主体审核机制，确保数据立法的域外效力和数据主权。第二，采取双边带多边、区域带整体的策略，推动“一带一路”倡议和“数字丝绸之路”下跨境数据流动协议的扩展和认可。充分尊重各国数据主权、

发展诉求，坚持多元主体共同参与数据规则制定，推动构建全球互信互通的跨境数据流动、共享和监管体系。持续推进中国加入 DEPA、CPTPP 进程，并确保国内个人信息保护、数据安全立法与高水平国际经贸规则相协调。第三，秉持数据命运共同体理念，积极参与国际跨境数据流动治理议题，推动构建全球数据流动合作圈。推动设立全球统一且安全的数据流动标准、数据存储基础设施框架和国际执法合作机制，通过统一标准实现不同国家间数据的互操作和兼容性，降低企业的合规成本。特别是在重点行业推动建立友好互信的国际数据空间，促进行业性数据的开放与交换。

（三）完善个人信息跨境流动法律与监管体系，建立国际互认机制

首先，完善个人信息跨境流动的法律和规则是当前的紧迫任务。尽管中国已经初步建立了个人信息监管框架，但监管主体的局限性以及立法细节的不足仍需解决。因此，有必要制定专门的行政法规，以细化个人信息跨境流动的原则、限制、审查及监管机制，确保数据主体的权益得到充分的保护。欧盟将个人数据视为基本人权，强调“隐私保护优先”原则下的跨境数据流动。可参照欧盟 GDPR 的充分认定机制，建立跨境数据流动白名单制度，仅允许经过认定的国家或企业接收我国数据，从而提升跨境信息流动和境外接收的标准，从根本上有效防止用户信息的非法跨境传输；同时，也可借鉴 GDPR 的标准合同条款（SCC）和约束性公司规则（BCR），制定企业个人数据跨境传输的规则，确保我国个人数据在跨境流动中的安全。其次，优化个人信息跨境流动监管机制。可借鉴欧盟的金字塔监管结构，明确我国“国家—部门—地方”三层监管模式的职责和权限划分。国家网信部门应发挥统筹协调的核心作用，专业部门负责特定领域的监管，地方政府部门应制定更为详细的监管细则。最后，积极参与并推动个人信息保护认证和国际互认。参考发达国家经验，结合国情制定个人信息保护认证标准；通过签署协议、参与国际组织，加强个人信息保护认证合作与交流，建立互信机制；借助粤港澳大湾区、东盟、“一带一路”等区域合作机制，推动与周边国家和地区的个人信息保护认证互认，逐步构建区域性互认体系，为跨境数据流动中的个人信息安全提供更为坚实的保障。

（四）强化数字知识产权保护，构建中国源代码规则新框架

在国际层面，源代码的管理规则正逐渐趋于一致，普遍接受禁止公开源代码的原则。中国在制定源代码管理规则时，应避免采取与国际趋势相反的强制性公开措施。在确保安全和可控的前提下，可以分阶段、有计划地推进源代码的公开。长期目标应是全面解除限制，但在中短期内，应以有条件地放开为基础，开展试点项目和探索性研究，鼓励企业基于自愿原则非强制性地公开源代码。同时，必须明确并严格执行例外条款，例如针对国家安全、公共采购项目、知识产权审查以及关键基础设施等特定领域的特殊规定，以防止因规则不明确而形成数字贸易壁垒。在确保监管和安全的基础上，逐步缩减源代码禁令的应用范围。同时，需持续增强数字知识产权保护的法律框架，及时与国际高标准接轨。增强数据安全技术的研发投入，提高数据加密、脱敏、审计、数字水印等技术能力，防范黑客攻击，确保数据传输和存储的完整性和安全性。特别是对于那些拓展国际市场的数字企业，应考虑在全球范围内强化自身的数据安全防护措施，以缓解其他国家对其数据收集和使用的顾虑。

（五）优化跨境数据税收征管体系，建立公平合理的国际税收环境

首先，针对跨境数据流动特性，对传统税制进行适应性调整。强化区块链、大数据、人工智能等前沿数字技术在跨境税收征管中的应用，探索“以数据为驱动”的税收管理新模式，并建立健全企业数据仓库（CDW）与国际金融账户涉税信息自动交换（CRS）等机制，促进涉税信息的无缝对接与高效共享，减少信息不对称现象，提升税收管理的透明度与效率。构建更加完善的税务数据分析平台与预警系统，以增强税务管理的数字化、智能化水平。其次，中国应积极参与并推动国际数字交易税收制度体系的建构。鉴于跨境数据流动涉及众多经济体，其税收治理亟需一个基于国际共

识、高效且公正的税收制度框架。中国应致力于成为规则制定的引导者，倡导关注发展中国家税基侵蚀和利润转移问题。依托“一带一路”倡议等国际合作平台，推动建立跨境数据流动涉税争议解决机制，建立更加公平合理的国际税收秩序。另外，借助加入 CPTPP 和 DEPA 谈判的契机，通过运用负面清单和例外条款，合法且有序地开放数字产品市场，构建一个灵活的数字产品市场准入管理框架，同时兼顾发展与安全。

参考文献：

[1] 陈寰琦 . 国际数字贸易规则博弈背景下的融合趋向——基于中国、美国和欧盟的视角 [J]. 国际商务研究 ,2022(3).

[2] 陈寰琦 , 陆锐盈 .DEPA 数据安全规则解析及对中国的启示——基于和 CPTPP/USMCA/RCEP 的比对 [J]. 长安大学学报 (社会科学版),2022(2).

[3] 洪延青 . 数据竞争的美欧战略立场及中国因应——基于国内立法与经贸协定谈判双重视角 [J]. 国际法研究 ,2021(6).

[4] 李杨 , 陈寰琦 , 周念利 . 数字贸易规则“美式模板”对中国的挑战及应对 [J]. 国际贸易 ,2016(1).

[5] 李墨丝 .CPTPP+ 数字贸易规则、影响及对策 [J]. 国际经贸探索 ,2020(12).

[6] 王惠敏 . 中美数字贸易竞争格局及中国应对策略 [J]. 国际商务研究 ,2023(6).

[7] 谢卓君 , 杨署东 . 全球治理中的跨境数据流动规制与中国参与——基于 WTO、CPTPP 和 RCEP 的比较分析 [J]. 国际观察 , 2021(5).

[8] 许可 . 自由与安全 : 数据跨境流动的中国方案 [J]. 环球法律评论 ,2021(1).

[9] 张应良 , 谢向伟 . 数字贸易国际规则博弈与中国因应——基于制度型开放视角 [J]. 开放导报 ,2024(2).

[10] 周念利 , 陈寰琦 . 基于《美墨加协定》分析数字贸易规则“美式模板”的深化及扩展 [J]. 国际贸易问题 ,2019(9).

[11] Burri, M.The Regulatory Framework for Digital Trade in the Trans-Pacific Partnership Agreement[R].Social Science Electronic Publishing,2017.

[12] Chin, Y. C., Zhao, J.Governing Cross-border Data Flows:International Trade Agreements and Their Limits[J].Laws,2022(4).

[13] Gao, H.Digital or Trade?The Contrasting Approaches of China and US to Digital Trade[J].Journal of International Economic Law,2018(2).

[14] Gao, H.Data Regulation in Trade Agreements:Different Models and Options Ahead[C].Smeets,M.Adapting to the Digital Trade Era: Challenges and Opportunities.Geneva:WTO Press,2021.

[15] Svantesson, D. J. B.The Extraterritoriality of EU Data Privacy Law:Its Theoretical Justification and Its Practical Effect on US Businesses[J].Stanford Journal of International Law,2014,50(1).

[16] Yang, X.Regulatory Approaches of Cross-border Data Flow in the Big Data Era:China's Choice[C].Journal of Physics: Conference Series.2021.

[17] Zheng, G.Trilemma and Tripartition:The Regulatory Paradigms of Cross-border Personal Data Transfer in the EU,the US and China[J].Computer Law & Security Review,2021(43).

Research on the Security and Optimization of Cross-border Data Flow under the Perspective of China-U.S. Digital Trade Rules

WANG Siyu　XU Ruixi　MAO Pei

Abstract: The promotion of openness and cooperation in the context of cross-border data flows is accompanied by the accelerated development of digital geopolitics, which poses challenges and threats to national security, data sovereignty and individual privacy protection. The balancing of the relationship between openness and security of data is particularly critical. The governance framework of cross-border data flow in digital trade rules focuses on three core areas: cross-border data flow and localization of data storage, personal information rights and privacy protection mechanism, and cross-border data intellectual property protection and promotion. An in-depth analysis of the digital trade rules and the governance mechanism of cross-border data flows between China and the U.S. reveals significant differences in the core interests and paths of the two sides. China has demonstrated unique advantages in this area, but also faces complex international challenges.In the game of global data governance, especially in the context of the U.S. data “lockdown” strategy, China should insist on data security and development in parallel, gradually open up data flows, and build a cross-border data flow rule system with Chinese characteristics.

Keywords: digital trade rules; cross-border data flows; data security; U.S.-China relations

（责任编辑：张建华）