

数字贸易国际治理：重塑 WTO 中心化地位

吴晓丹

(中央财经大学 法学院, 北京 100081)

摘要：数据的经济、人权、安全和主权等多元属性及相关问题复杂性导致各国规制跨境数据传输的价值理念、政策取向与路径方法存在重大分歧，成为隐形非关税壁垒。美国、欧盟等以自我价值取向和利益为基础，推进双边和区域贸易协定的俱乐部式规制集团，是国际治理分散化和 WTO 电子商务谈判不顺的根本原因，必须重塑 WTO 数字贸易国际治理的中心化地位。具体方向和路径为顺应法律多元主义，推进多中心治理；基于数据的人权属性推进个人隐私和国家安全一体化保护；结合政治和法律手段灵活规制国家安全例外。重视规制自主权和数据发展权的中国方案对于重塑 WTO 极为重要，应细化规制自主权和数据发展权的国际叙事，以建制性规则体系强化国际竞争力，拓展国际影响力。

关键词：数字贸易国际治理；跨境数据流动；世界贸易组织；电子商务谈判；中国方案

[中图分类号 F744 [文献标识码]A [文章编号]1002-4034(2025)02-0011-21

引 言

数字经济方兴未艾，改变了传统的贸易形式，以数字方式连接全球经贸活动，使企业将有形的商品、无形的服务拓展至世界各地的消费者，也催生了以数据要素和服务为交易对象、数据订购和交付为主要特征的数字贸易。作为数字经济与贸易的重要基础和载体，数据流动的赋能作用日益突出。2011 年以来，全球数字服务贸易持续稳定增长，服务贸易占比稳定在六成以上，预计 2025 年，数据流动对全球经济增长的贡献将达到 11 万亿美元^①。数字贸易已成为拉动全球经济增长的新动力，而其中数据在不同国家(地区)之间的跨境传输成为关键因素。数据作为第五大生产要素具有商业价值和经济属性^②，又是个人隐私和基本权利保护对象，作

[收稿日期]2024-09-28

[作者简介]吴晓丹(1978—)，女，黑龙江林口人，中央财经大学法学院副教授，研究方向：国际法、外空法、数据法

①中国信息通信研究院. 2022 年全球数字治理白皮书[EB/OL]. 2023-01-15[2024-12-11]. http://www.caict.ac.cn/kxyj/qwfb/bps/202301/t20230110_413920.htm.

②2020 年《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》分类提出了土地、劳动力、资本、技术和数据五个要素领域的改革方向和完善市场化配置举措，首次明确了数据的生产要素地位。

为战略资源还涉及国家主权和安全议题。数据的多元属性以及相关问题的复杂性导致各国规制数据收集、存储和传输方面的价值理念、政策取向与路径方法存在重大分歧,导致数据无法顺畅地跨境流动,成为隐形非关税壁垒。全球层面的数字贸易治理进展有限。策略上,美国和欧盟将双边和区域贸易协定作为推进国际规则形成的主要方式,而这些协定是以美国和欧盟的自我价值取向和利益为基础,协定中相关规则不完善、不合理,无法系统解决数字贸易涉及的发展、人权、主权、国家安全等复杂、敏感事项。繁复重叠的国内规制和贸易协定并未促进全球数据流动的协调治理,反而造成了规则的碎片化、差异化和供应不足问题。不同国家(地区)推动数据流动的主张演变为共同阻碍流动的现实,限制了数字贸易和数字经济的竞争活力和科技创新,跨境数据流动摩擦、纷争不断。面对数字贸易带来的挑战,国际社会必须重新强调统一协调和全球治理方法的重要性(Kirby, 1991)。本文旨在探讨数字贸易治理如何回调到全球规制方向,即更新世界贸易组织(World Trade Organization, WTO)规则体系和治理理念的需求、方向和路径,以重塑其中心化地位,进而确立中国方案。

一、数字贸易分散化治理与重塑 WTO 中心化地位

数字贸易国际治理面临的不是规则缺失问题,而是多方主体各自主张形成了相互重叠和交错竞争的数据流动政策与规范。相比国内、双边和区域层面数据跨境流动规制的蓬勃发展,数字全球治理明显滞后。作为全球唯一致力于贸易自由化的专门性国际组织——WTO 地位仍不可替代,应重回全球治理轨道和重塑 WTO 中心化地位。

(一)跨境数据流动规制的中国、美国和欧盟间竞争

数字经济和数字贸易快速发展凸显数据的重要性,多国纷纷监管跨境数据流动(Chander 和 Lê, 2015),但各国数据政策和法律并未趋同,政策取向与规制方法差别明显。这是因为价值理念、数据控制和治理能力差别导致各国的监管重点不同,包括维护人权与个人信息保护、促进互联网经济发展、确保数据安全、数据合理使用、金融监管、消费者保护和贸易保护主义等。中国、美国和欧盟等主要经济体的跨境数据流动规制形成了差异化竞争甚至对抗状态。

第一,以美国为代表的放任政策。美国一直采取开放和自由的互联网政策,联邦法不限制跨境数据流动,提倡自我规制,要求企业自我评估、行业自律。将个人置于数据市场之中,数据保护更多地置于消费者保护法之下(Bulford, 2007; Yakovleva, 2017)。这与美国的自由主义传统有关,更与美国互联网企业掌控数据的能力以及美国政府根据国内立法能够和企业共享信息有关。例如,《美国联邦政府云计算战略》要求企业必须根据网络安全审查制度签署网络安全协议,通常要求通信基础设施必须设在美国境内,通信数据、交易数据、用户信息等仅存储在美国境内。美国外国投资审查委员会(The Committee on Foreign Investment in the United States, CFIUS)常以“威胁国家安全”为由拒绝外国服务提供商进入美国市场。因此,美国可以在不受主权利限制的情况下获得数据,在事实上完成了数据本地化。

第二，以欧盟为代表的重视个人数据和隐私保护的规制主义。欧盟和美国在数据隐私和数据安全发展上有相似的历史脉络。然而，欧盟与美国在数据隐私观念及相关立法方面存在着较大的分歧，美国是市场主导型的，欧盟则是权利主导型的（Reidenberg，1999）。欧盟历来看重技术与人权之间的关系，以重视个人数据和隐私保护来平衡人权和数字贸易；设定法定许可和标准允许数据在特定条件下流动，以高保护标准构建数字经济的信任基础，促进贸易发展。根据欧盟《通用数据保护条例》，获得充足性认定的国家或地区才能跨境传输欧盟个人信息；以整体考量的认定方法进行广泛评估，数据传输国家和地区的法治环境、是否存在独立有效运作的监管机关、国际协议或国际承诺、与欧盟的政治关系、隐私保护体系是否与欧盟法律保护实质性等同等诸多因素均影响充足性认定。目前获得欧盟充足性认定的只有15个国家和地区^①，其他国家和地区须有理由方可跨境传输数据，并通过“适当的保障措施”弥补目的地数据保护的不足^②。自欧盟数据保护制度建立之日起，始终有批评声音认为欧盟“监管过度”（Ford，2003；Naef，2023）。

第三，以中国为代表的国家主义模式。基于对国家利益和公众利益的关注，中国等一些国家以政策、立法和实践确立数据本地化要求。中国《网络安全法》第37条规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。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。”此后的《个人信息保护法》《数据安全法》《关键信息基础设施安全保护条例》《促进和规范数据跨境流动规定》《网络数据安全条例》等根据《网络安全法》，确立了中国数据跨境流动的基本原则。数据本地化包括要求服务提供者于国内设置服务器，数据传输或存储皆须通过国内服务器；或依法律要求，通过某种程序才能跨境传输。关于数据本地化程度，各国之间存在差异，有的全面禁止数据跨境流动，有的有条件允许数据跨境流动；有的要求数据存储和处理均在其境内，有的允许数据在境外复制以供处理，但前提是在本地基础设施中有复制数据。美国和欧盟一贯强调，数据本地化法律要求扰乱了数字贸易，与互联网无边界的特性和贸易自由化原则相冲突。

数据具有非属地性、可共享性和可重复性等无形特征，对数据的控制范围往往超出了国家领土的物理边界。即使高度实行数据本地化的国家，亦无法回避网络空间的物理无边界特性。主权国家监管互联网不可避免地具有域外影响，数据法必然产生规范外溢效应。21世纪以来，多国确立和强化本国法的域外适用和域外管辖权的行使，有意识的溢出举措破坏了原有的隐私保护状态，增加了数据合理流动的企业合规成本，扼杀了数字经济和贸易的活力。其中，美国和欧盟的溢出效应最为明显。自20世纪90年代中期以来，欧盟一直在全球范围内维护其数据保护法的管

^①获得欧盟充足性认定的15个国家和地区包括安道尔、阿根廷、加拿大、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、韩国、瑞士、英国和美国（仅在隐私保护协议框架下）。

^②The European Commission, Adequacy Decisions of Data Protection [EB/OL]. 2016-05-04 [2024-12-11]. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_lt.

管辖权(Svantesson, 2013; Ford, 2003), 通过标准合同条款、行政执法与法院审查、企业自愿实践、签署监管协议等多种做法, 使得《通用数据保护条例》的域外影响显著增强。多国通过立法、修法或者调整市场实践适应欧盟的要求, 称为“布鲁塞尔效应”(Branford, 2020)。美国通过内国法域外适用和长臂管辖权强化外溢效果。美国国内法适用于收集美国个人信息的海外实体(Gregory, 2020)。2001年以来, 美国多部立法致力于防止恐怖主义袭击和其他公共安全威胁, 其中《爱国者法案》授权行政机关调取第三方记录对境外企业产生重大影响, 导致许多境外大型企业向美国境内传输数据。2013年, 美国“微软案”促使美国将长臂管辖权扩展至数据跨境流动。2018年, 美国《澄清海外合法使用数据法》要求国内数据服务提供商提交其存储于海外的数据, 据此对数据跨境传输行使长臂管辖权。加拿大、新西兰等也有类似规定, 被称为攻破域外隐私堡垒的“特洛伊木马”(Gunasekara, 2007)。

(二) 双边和区域贸易协议的发展与先天不足

国际对于跨境数据流动的关注几乎与实践同步展开, 但总体进展有限(Estadel-la-Yuste, 1991)。1968年, 《世界人权宣言》发表20周年之际, 联合国会议的一个议题便是电子产品对人权的可能影响, 试图为“数据革命”探寻法治基础(Hondius, 1980)。1974年, OECD成立跨境数据流动政策分析专门工作组, 随后发布的1980年《个人数据隐私和跨境数据流动保护指南》(OECD保护指南)和1985年《跨境数据流动宣言》等文件确立了个人隐私保护的最低准则, 是早期关注跨境数据流动的国际文件。为了克服数字贸易规则的碎片化, 国际社会展开讨论和对话, 但严重的立场分歧导致谈判举步维艰。联合国国际贸易法委员会(UNCITRAL)试图解决电子商务法律问题, 2005年达成《联合国国际合同使用电子通信公约》, 至今只有18个缔约国^①。WTO电子商务谈判迟迟没有实质性进展, 目前成果主要体现为双边和区域自由贸易协定。2007年签署的《美韩自由贸易协定》系首个规范电子商务的双边协定。2016年美国推动的《跨太平洋伙伴关系协定》(TPP)是首个系统规制数字贸易的区域协定。近年签订生效的主要区域贸易协定都有多个条文和专章规则涉及数字市场准入、降低数字服务准入壁垒、减少数据跨境流动限制和维护网络安全等数字贸易问题, 包括2018年12月生效的《全面与进步跨太平洋伙伴关系协定》(CPTPP)(2017年美国退出, 但保留了TPP的主要条款)、2020年6月生效的《数字经济伙伴关系协定》(DEPA)、2020年7月生效的《美国-墨西哥-加拿大协定》(USMCA)和2022年1月生效的《区域全面经济伙伴关系协定》(RCEP)。2000年至2023年5月通知WTO的近400个区域贸易协定中, 有140多个包含电子商务/数字贸易条款或章节(石静霞, 2023)。

双边和区域贸易协定已成为规范数字贸易的重要机制, 在一定程度上塑造和影响了跨境数据流动的监管环境, 但规范数字贸易的全球国际合作框架尚未形成。

^①UNCITRAL, Status of UN Convention on the Use of Electronic Communications in International Contracts[EB/OL]. 2023-01-07[2024-12-11]. https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications/status.

Wu(2017)、Basedow(2018)认为贸易协定的滥觞是全球层面数字贸易谈判停滞的重要原因。首先,贸易协定的概念和规则开放性不够,违反了非歧视性原则。美国借此选择贸易协定的“合格”参与者,与合作理念背道而驰。USMCA号称是21世纪的高标准贸易协议,旨在北美实现更自由的市场和更公平的贸易,但数字贸易章节明确禁止强制性数据本地化。“大毒丸条款”(即非市场经济国家自由贸易协定条款)和“小毒丸条款”(即不适用墨西哥-美国投资争端协议条款)将中国、俄罗斯等国家排除在外。其次,贸易协定体现了主导国家的利益和做法,规则不尽完善合理。美国主导的TPP和USMCA体现了美国长期坚持的做法,以强大的技术实力为后盾,强调个人在数字产品和服务中的选择自由,约束国家对数据流动的限制,以促进数据的自由流动。TPP和USMCA例外条款的结构和措辞对WTO规则构成重大挑战,自由贸易可能超越和凌驾于人权、主权和国家安全之上,忽视了一国合理的公共政策需求。再次,规则差异明显,无法为日益增长的数据隐私和国家安全关切提供协调性的监管机制,无助于跨境数据自由流动。以国家安全例外为例,各个协议的自裁决性质和规制宽严口径不一。为了防止缔约方利用自裁决采取单方面行动或为数据本地化寻找借口,TPP直接否定以安全为由限制数据流动,缔约方只能援引第29章“例外和总则”中的一般例外,而且无权自行判断。美国退出TPP后,由TPP演变而来的CPTPP第29条确立了安全例外,但依旧缺少成员方“认为必要”指向的自行判断。中国、韩国、印度等重视跨境数据流动可能给国家安全造成的损失和不利影响,因此RCEP第12章确认安全例外条款的必要性,明确缔约方不得阻止电子信息的跨境传输,同时尊重缔约方对电子手段传输信息的监管要求,以灵活的公共政策和国家安全例外为各方留下足够的政策调整空间。

(三)重回全球治理轨道与重塑WTO中心化地位

当国内法、双边和区域贸易协定的价值取向与规制方法不一致甚至冲突时,各自主张和强化数据流动限制不可能发挥作用,反而给数据驱动行业带来了极大的不确定性,导致国际贸易摩擦不断。中国、美国和欧盟在数据保护、信息隐私、网络安全和国家安全等事项持续产生争端,每隔几年就会以新的形式重新出现。斯诺登事件之后,欧盟法院系列判决根据基本权利保护的重要性,否定了数据保留制度(Zalnieriute, 2018),继而在数据保护政策和监控措施日益安全化的背景下,十年间两次推翻了大西洋两岸数据传输的法律基础,即关于数据跨境传输的安全港协议和隐私盾协议^①(Cors, 2019; Zalnieriute, 2022)。中美贸易争端升级,数据跨境流动是争论焦点。2005年以来中国数据跨境流动增长迅速,2019年超过美国。出于遏制中国科技和经济发展的政治目的,美国政界提出中国正在建立美国公民数据库的荒谬主张(Dunlap, 2014),对华数据跨境流动发生重大政策和监管转变,导致两国数据安全信任危机和数据脱钩风险。其一,美国利用国家权力制裁中国企业。

^①Court of Justice of the European Union, Case C-362/14, Maximilian Schrems v. Data Prot. Comm'r, ECLI: EU: C: 2015: 650, 11 96-106, Oct. 6, 2015. Court of Justice of the European Union, Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximilian Schrems, ECLI: EU: C: 2020: 559, July 16, 2020.

2020 年，特朗普总统针对 TikTok 和微信发布系列行政令，指控其为中国政府挖掘个人数据且规模巨大，威胁国家安全^①(Clausius, 2022)。美国法院判决最终阻止了行政令的生效^②。2024 年，拜登总统接连签署两项法案，限期 TikTok 从中国母公司剥离，否则将面临禁令^③。第二项法案获得了美国参众两院支持。2025 年 1 月，美国最高法院裁定支持非卖即禁法案，次日候任总统特朗普将禁令推迟 90 天以完成合规的资产剥离，但延期的合法性和资产剥离交易的可行性都不明确，TikTok 仍受禁令的影响。其二，美国基于国家安全考量改变了数据自由流动立场，创建了美国人数据跨境传输审查机制，限制、切断敏感数据甚至一般数据传输至中国。2021 年美国《对抗性平台防范法案》直接针对中国，要求软件所有者确保母公司不能通过子公司访问美国消费者的数据，不能在涵盖国使用美国消费者的数据，不能将美国消费者的数据转移到涵盖国，不能将美国消费者的数据存储在境外。2024 年 2 月，拜登总统根据美国《国际紧急经济权利法案》颁发行政令，本着特定主体获取批量美国人敏感数据和美国政府相关数据对国家安全构成不可接受风险的逻辑，限制和禁止大批量此类数据向中国传输^④。美国两届政府的密集举措不仅涉及法律、道德、逻辑以及现实可行性争议，更将中国与美国、中国人与美国人在互联网上隔离，背离人权保护、贸易自由化和全球化的基本要求。

20 世纪 90 年代，数据跨境传输多被视为电子数据交换加以监管。技术迅猛发展，不同行业、不同设备型号等导致 20 世纪 60 年代以来建立的数据标准难以统一。于是，国际社会试图在 WTO 框架内展开谈判。1998 年 WTO 部长级会议通过了《全球电子商务宣言》，电子商务议题成为正式议程，成立了专门工作组以促进贸易规则的相应变化^⑤。2001 年以来的多哈回合谈判中电子商务进展缓慢，成效甚微(Mitchell 和 Mishra, 2019)。唯一可见成果是 2019 年《电子商务联合声明》启动的部分成员方磋商^⑥；2024 年，90 多个成员方达成《电子商务协议》^⑦。但这个进展对于数字贸易治理的政治象征意义大于规范实质意义。其一，《电子商务协议》经 166 个全体成员协商一致纳入 WTO 法律框架的前景不乐观。部分成员方参与的多边磋商纳入 WTO 的成功案例寥寥无几。如参与谈判的《促进发展的投资便利化协定》有 128 个

①Presidential Executive Order No. 13942, Addressing the Threat Posed by TikTok and WeChat, 6 August 2020. Presidential Executive Order No. 13943, Taking Additional Steps to Address the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain, 6 August 2020.

②TikTok v. Trump, 507 F. Supp. 3d 92, 98 (D. D. C. 2020).

③Protecting Americans from Foreign Adversary Controlled Applications Act, H. R. 7521, 14 March 2024. 21st Century Peace through Strength Act, H. R. 8038, 17 April 2024.

④Presidential Executive Order No. 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-related Data by Countries of Concern, 28 February 2024.

⑤WTO, Work Programme on Electronic Commerce, WT/L/274, 30 September 1998.

⑥WTO, Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019.

⑦WTO, Agreement on Electronic Commerce, INF/ECOM/87, 26 July 2024.

成员方,但历经四次谈判未完成列入《马拉喀什建立WTO协定》附件4的目标^①。2023年,美国放弃长期坚持的以自由流动和禁止本地化为重点的电子商务谈判议案,为强化其国内监管留出空间^②。10个参与磋商成员方基于国内法和其他考量对协议文本没有给出正式同意。《电子商务协议》免除了电子传输关税,未参与磋商的印度和南非对此持保留意见^③。其二,《电子商务协议》有关数字贸易的内容粗泛,难以构成体系性规范。《电子商务协定》“前言”明确尚未解决数据贸易的一些重要议题,只简单提到保护个人数据国内法框架与兼容性,以及个人数据保护例外措施,没有区域协定中常见的数据跨境自由流动原则和相应的义务,也没有确立承诺时间表。无论如何,WTO的成立与运作是全球自由贸易规则发展的集中体现,几乎所有贸易问题均可在WTO框架下展开讨论。虽然一些学者和非政府组织认为WTO无法胜任数字贸易谈判(Singh, 2018; International and Regional Organizations, 2019),但他们低估了数字贸易在竞争中实现协调合作的可能性。Davidow和Malone(1991)坚持认为WTO是确立数字贸易全球治理和解决跨境数据流动争端的最佳场所。因此,应继续推进在WTO框架内就跨境数据流动规则展开磋商和谈判,确立以此为全球数字贸易治理机制。

二、WTO框架下数字贸易治理规则与理念的更新需求

WTO基本原则支持数据开放流动,不限制成员方出于正当理由对互联网进行监管,但未能考虑到数据跨境流动的特殊性。WTO基于区隔主义的治理理念,为货物、服务等传统贸易确立分类别的规则体系,无法满足数字贸易的发展需求。究其根本,WTO没有直接促进数字信任,因此有必要更新数据流动自由、隐私保护和网络安全等方面的规则体系和治理理念。

(一)更新前互联网时代的规则体系

数字贸易可分为两种:一是贸易的数字化,作为贸易形式,基本等同于电子商务,即以电子方式生产、分配、销售、出售或运输商品与服务的经济模式,既有服务贸易属性,也涉及货物贸易(Aaronson, 2018),如物联网的交叉性;二是狭义的数字贸易,即以数据要素和服务作为交易标的的贸易类型。WTO电子商务的谈判范围和各方提案没有细分贸易的数字化和数字贸易^④。以起(终)点作为跨境的判定

①Incorporation of the Investment Facilitation for Development Agreement into Annex 4 of the WTO Agreement, WT/GC/W/927/Rev. 1, 14 May 2024.

②U. S. Trade Representative Statement on WTO E-Commerce Negotiations[EB/OL]. 2023-10-24[2024-12-11]. <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations>.

③Proposal of India and South Africa, Moratorium on Customs Duties on Electronic Transmission; Need for Re-think, WT/GC/W/747, 13 July 2018. Communication from South Africa and India, Reinvigorating the Work under the 1998 Work Program on Electronic Commerce, WT/GC/W/747, 4 December 2020.

④Communications and proposals from participating parties to Joint State Initiative on E-commerce Negotiations[EB/OL]. 2024-07-26[2024-12-11]. https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm#how.

标准, 依赖标的种类从货物贸易拓展至服务贸易、技术贸易、与贸易有关投资和知识产权, WTO 以单独文件完成补贴式的规则完善。数据的多重属性和贸易形态导致数字贸易具有跨贸易类别属性, 互联网不同于传统贸易的跨境运输起(终)点, 现有文件难以适用于数字贸易, 只有单独协议才能填补规则空白。

第一, 数字贸易无法与传统贸易简单对等, 导致在贸易分类上面临规则选择的困境。货物贸易和服务贸易分别适用《关税贸易总协定》(GATT)和《服务贸易总协定》(GATS), 两个文件确立了不同的规则和自由度。简言之, 前者以国民待遇为核心, 后者以成员方的具体承诺确定。数字贸易中难以区分与货物和服务相关的措施, 适用减让关税和开放承诺的正面清单存在障碍, 不能归类于货物贸易的税则分类号或服务贸易的部门分类, 解释成员方在 GATT 和 GATS 下国民待遇和市场准入承诺是否涵盖某个部门的数据流动较为困难。以 GATS 为例, 其服务部门归类对应于成员方的开放承诺, 数字贸易难以清晰地归属于“分类清单”中的任何一类, 可能涉及的服务部门有计算机与相关设施、电信设施以及视听服务等, 而且各国的贸易统计口径不一, 无法就跨境数据流动统一归类。美国为推动数字贸易自由化, 倾向于用 GATT 规范数字贸易, 多数发展中国家更倾向于适用 GATS 以保护本国相关产业和市场。在现有达成的贸易协定中, 部分协定模糊处理归类以回避“二选一”难题。例如, DEPA 明确数字产品定义不涉及归类于货物还是服务, 缔约方自行在非歧视基础上选择适用 GATT 还是 GATS。这种处理方式将导致数字化贸易在 DEPA 项下待遇标准的不确定, 显然是阶段性的折中方案。另外, 近年谈判朝向不同于以往的框架, 即从降低壁垒的目标出发建立共同的标准或协调的行动, 负面清单模式成为发展方向。为了推进贸易自由, 如何拟定负面清单以规范限制数据流动措施是未来数字贸易协议的重要课题。

第二, 数据本地化措施在 GATS 框架下的合法性判定存疑。虽然没有专门的数字贸易规则, GATS 确实提供了一个保护基线, 禁止过度限制数据跨境流动措施, 同时允许成员方就数据本地化作出承诺。GATS 可适用于数据本地化措施主要有: 一是数字技术涵盖的范围是使其他类别的服务能够跨境提供, 如电子支付服务; 二是成员方承诺表涉及一些数据服务市场准入和国民待遇的具体明确承诺, 如数据库和数据处理服务。虽然 WTO 争端一般性涉及 GATS 对互联网服务的适用性, 但尚未具体考量 GATS 对数据本地化措施的适用性^①。成员方对本地化措施的合法性分歧较大。美国和欧盟强调禁止数据本地化, 欧盟仅允许依据个人数据保护而对跨境流动作出限制, 拒绝承认其他合法公共政策目标作为例外, 而美国虽然承认合法公共政策目标, 但以数据自由流动为由否认其他国家的本地化自主权, 同时借助互联网企业掌控数据的能力以及与企业共享信息的国内立法完成了事实上的美国数据本

^①Panel Report, United States—Measures Affecting the Cross-border Supply of Gambling and Betting Services, WT/DS285/R, 10 November 2004, paras. 6. 287; Panel Report, China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, WT/DS363/R, 12 August 2009, para. 412.

地化。中国等国家强化数据本地化要求,一些国家则反对禁止数据本地化^①。WTO 专家小组和上诉机构渐进扩大解释 GATS 以将某些承诺适用于在线服务供应,但是电子商务谈判进展乏力,这些解释难以转化为有约束力的义务。依靠争端解决机制确定 GATS 下互联网服务的覆盖范围和具体规则,这不是基于共识的谈判,无法全面反映成员方立场,降低了法律的可预见性和权威性。

第三,在数据隐私保护与国际监管规范缺位的情况下,一般例外规则无法解决成员方规制差异造成的数字贸易壁垒(Burri, 2017)。从各国立法实践来看,虽然具体理念、标准和方法差异较大,数据的隐私和人权属性认定与保护原则有着一致的基调和方向。1980 年 OECD 保护指南强调个人数据隐私的基本自由权利。受此影响,各国纷纷制定了个人信息保护法,4/5 的国家已经或正在为数据和隐私保护立法^②。国际人权文件明确隐私权为人权,如《世界人权宣言》和《公民权利和政治权利国际公约》。虽然这些文件没有设想个人数据的普遍获取和商业化趋势,但自 2013 年以来联合国大会的多项决议反复重申,其所载的隐私权同样适用于数字隐私领域^③。在保护人权方面,数据保护和信息隐私变得越来越重要。跨境数据流动特别强调个人信息保护(数据保护、隐私保障)(Blume, 2018; Macdonald 和 Streatfield, 2014)。在商业化和全球化的冲击下,数据隐私的人权特性有些受影响,但总体而言,数字时代的发展使公众了解个人信息被谁收集、收集的范围、收集和处理的目的是否重要。隐私保护是限制数据跨境流动的最常见理由,是数字贸易国际治理最为重要的关切。有关个人信息、数据保护和数字贸易的国际讨论时常导向本质的指向,即自由权。美国和欧盟在《跨大西洋贸易和投资伙伴关系协定》(TTIP)谈判进程中,个人信息和数据保护始终是首要阻碍。GATS 第 14 条的一般例外条款,作为合法限制措施,难以适用于数字贸易。该条款允许成员方为正当的国内政策目标实施必要的限制措施,包括国内互联网安全政策,许多成员方据此确立和采取限制跨境数据流动的措施(Wu, 2006; Winsch-Vincent, 2006)。因数据隐私国际保护标准缺位,使一般例外政策目标的正当性不明,导致这些例外措施的合规性和正当性缺乏法理基础。数据本地化限制影响服务提供模式的承诺履行,涉及 GATS 一般例外的合规性分析,但援引一般例外的必要性不确定(Mitchell 和 Hepburn, 2017)。GATS 第 14 条涉及承认出于隐私保护限制措施的合法性,即便违反了成员方的贸易承诺,只需要证明该措施的必要性。然而,简单的必要性门槛不能确保所有成员方在数据保护、隐私保护方面采取合理、积极的措施,只是重申了其施加限制措施以保护个人隐私、保护电子传输的机密性和安全性的权利。同样, GATS 并

①Work Programme on E-commerce, Statement by the Africa Group, WT/MIN (17)/21, 6 December 2017.

②UNCTAD, Global Cyberlaw Tracker. 2021-12-14 [2024-12-11]. <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

③UN General Assembly Resolutions, The Right to Privacy in the Digital Time, A/RES/68/167, 18 December 2013; A/RES/69/166, 18 December 2014; A/RES/71/199, 19 December 2016; A/RES/73/179, 17 December 2018; A/RES/75/176, 16 December 2020; A/RES/77/211, 5 January 2023.

未为通过消费者保护法以确保服务质量或安全而设定具体要求，仅作为一个例外，为保护消费者利益而限制数据流动的规则也是不充分的。

（二）更新贸易与安全的区隔主义治理理念

第二次世界大战后的国际经济秩序长期依赖于国家安全政策与普通经济事务相对分离的监管框架。从 GATT 发展到政府间国际组织，WTO 自觉划定治理边界，仅关注与贸易直接相关的议题。不同于货物、服务和技术的单一或主导经济属性，数据多重属性交错，区隔主义治理理念存在明显的狭隘性，不适应数字贸易的复杂治理需求。GATT 第 21 条和 GATS 第 14 条设定了国家安全例外，成员方有权据此限制数据流动，但两协议未提及网络安全和数据安全，更谈不上制度安排。在国家安全泛化情况下，“安全”“经贸”的二分法和国家安全的自裁性导致例外条款的滥用，侵蚀了以规则为基础的国际经济秩序。

为了平衡国际贸易与国内政策，WTO 设定了国家安全例外，并授予成员方完全的裁量权(Pinchis-Paulsen, 2020)。这是一种传统且务实的操作，既能促进国际贸易发展，又保留一定的主权空间，学界称为“冷战解决方案”(Heath, 2020)。其一，在普通经济行为与国家安全措施之间划定简单的界限，经济全球化与国家安全成为相对独立的领域。这种界分与美国坚持在多边贸易中保留安全问题的立场有关，因彼时美国预料到未来可能与苏联发生冲突，必要时国家安全例外能够发挥关键作用(Wilcox, 1949)。因此，GATT 和 GATS 国家安全例外内容宽泛模糊，允许成员方逃避其贸易承诺，以广泛多样的例外情况豁免国家安全措施不受普通经济规则的约束。其二，国家安全属于“自我判断”的范畴，主要通过外交谈判实现相互间的自我克制。成员方自行决定是否适用例外原则和具体措施，只要它们愿意为该措施承担相应的政治和经济代价(Lindsay, 2003)。国家安全例外不受其他国家或者国际组织的审查，也不受任何形式的司法审查，典型案例如 1985 年尼加拉瓜诉美国案^①。美国里根总统以行政令禁止与尼加拉瓜的大部分贸易^②，尼加拉瓜认为总统令应是战争或其他国际关系紧急情况下，保护基本安全权益所必需的，而美国则认为国家安全利益属于国内治理范畴。WTO 专家小组虽然认定美国措施对于保护任何基本安全利益不是必要的，但最终将第 21 条交给主权国家阐明和管理，无论这些行动在第 21 条下是否实际有效。这一裁定导致了不干预国内行动原则成为 WTO 的一个重大缺陷(Gardner, 2020)。

冷战结束后，国家安全的概念扩张和泛化援引打破了经贸和安全二者之间的既有平衡。在广泛解释下，国家安全从敌对模式转变为与日常执法、人权政策、环境保护、公共卫生和经济全球化纠葛在一起的多层次概念。成员方发现国家安全例外能够凌驾于国际经济秩序之上而满足己方需求，导致出现危险的泛化和滥用趋势。成员方通过歧视性的抑制或制裁措施，以纠正它们认为其他成员方的违法或不合乎己方安全

^①Panel Report, United States Trade Measures Affecting Nicaragua, L/6053, 13 October 1986, paras. 5.1-5.17.

^②Presidential Executive Order No. 12513, Prohibiting Trade and Certain Other Transaction involving Nicaragua Source, 1 May 1985.

利益的行为,也可以绕过国内行政程序甚至颠覆监管框架的合理性。国家安全概念扩张至保护互联网,私人企业收集敏感个人数据越来越被视为国家安全问题。随着对安全威胁认知的转变,数据跨境传输的监管变得更为严格,数据流动成为数字贸易规制中的显著问题。数据安全在一定程度上确实能够威胁国家安全,“剑桥分析”^①等事件揭示了个人信息和数据平台可能会增加国家安全风险和加剧地缘政治紧张局势。但国家安全例外的自裁性导致援引门槛越来越低,相互克制变得极度脆弱,严重损害了国际经济法律秩序。美国的外国投资审查机制及其运作便是例证,外国投资委员会没有界定国家安全,但审查范围逐渐扩张,包括关键技术、关键基础设施、敏感个人数据等。事实上,每一项数据传输均有潜在的安全隐患,对于网络的监控将国家陷入战争与和平的混合状态,使得战争与非战争、国外与国内的国家安全界限变得难以区隔(Brownell, 2000; Bay, 2005; Yoo, 2017)。许多在传统、常规原则下看似与对外政策、军事政策无关的部门也或多或少牵涉到“国家安全”标号下的政府活动中(牛可, 2010)。其他国家有类似做法,英国、澳大利亚、新西兰等基于国家安全原因禁止在5G网络中使用中国华为设备,印度以有损主权、国防和国家安全为由禁止中国的多个手机应用程序。如果不及时弥补,滥用安全例外条款的漏洞将导致世界经济沿着地缘政治路线分裂甚至崩坏(杜明, 2023; East Asia Forum Editorial Board, 2023)。

WTO争端解决机构深感自己有义务以审查促进法治,但突破原有做法反而扰乱了国际经济秩序。2019年俄罗斯过境案中,WTO专家小组首次试图解决“贸易”和“安全”二分法冲突,宣布可以审查援引安全例外条款^②。该案为安全例外确立了两步式框架解释方法:(1)客观地审查“战争”“紧急情况”或其他援引依据的存在;(2)成员方是否谨慎地判定相关措施对于保护其基本安全利益的必要性。这个审查权的启用限制了成员方对国家安全的任意性扩大解释,否定了GATT第21条的自我审查性。这种突破性解释方法标志着WTO实现了重大转变,从法律主义转向以外交、权力为基础的争端解决模式(Shaffer, 2018)。欧盟、中国等成员方对此表示支持和肯定,而美国表示异议,甚至声称退出WTO,成员方之间截然相反的立场削弱了WTO的国际地位和权威性。

三、WTO框架下数字贸易治理的更新方案与路径

多数国家和学术界普遍认同,WTO更新其基本目标的核心是在个人数据保护的基础上,建设消费者和企业之间的信任,促进互联网开放和数据治理包容,为合理的一般例外和国家安全考量确立一个灵活细致的框架(Mitchell和Hepburn, 2017; Burri, 2017; Peng和Liu, 2017; 石静霞, 2015)。这就需要进一步思考:如何继承和借鉴国内立法和典型的贸易协定,通过真正民主化的多边对话、协调、合作在全球层面实现这些目标。中国、美国和欧盟数据自由理念和数据规制方法差异明显,

^①Facebook违反了平台与用户的隐私保护协议,向政治咨询公司——“剑桥分析”不当泄漏数千万用户数据,基于大数据分析试图影响美国、印度、尼日利亚等国家的选举和英国脱欧公投。

^②Panel Report, Russia—Measures Concerning Traffic in Transit, WT/DS512/R, 5 April 2019, paras. 7.5.3.

WTO 的更新主要在中美欧三方之间展开博弈，中国方案对于牵制美欧的偏激立场和极端做法至关重要。

（一）顺应数据规制多元主义，推进多中心治理

一般认为，单边数据限制阻碍了数字信任与创新，多边交流与合作比单边数据限制更为有效。而近年双边和区域贸易协定的发展制约了开放性多边和全球机制的发展。为了推进形成普遍适用的国际规则，需要更进一步思考的是：双边和区域规制跨境数据流动作为多边合作只是单纯地加剧国际贸易冲突，还是可能构建合理的竞争状态（Chin 和 Zhao, 2022）。此种思考有助于数字贸易朝着真正的多边主义和民主化治理方向发展，督促各国重新审视数据隐私和跨境监管的立法及其实践，重视并重回全球治理轨道。实现数字贸易国际治理的关键是基于法律多元主义的视角，在不同的方法、立场中寻找共识，关注并重视不同类型的国内和国际规范体系、治理水平之间的多样性和差异性，进而寻求一致性制度安排。在全球层面确立 WTO 的中心地位，为跨境数据更加自由的流动确立普遍适用的治理理念和规制办法，在国内法、双边和区域协定发展的基础上，吸纳已经获得共识的数字贸易规则，通过细化市场准入、国民待遇原则、例外规则等措施减少数字贸易壁垒。

相比限制，为数字贸易设定国际公认的数据保护模式更具现实意义。跨境数据流动的规制框架极为复杂，远超出传统的单一中心多边进程。重塑 WTO 中心地位需要多中心治理，将数字贸易与数字权利、国家主权关联起来，在隐私保护、公共政策和利益、国家安全、网络安全和数据流动之间建立分层、比例式、体系性规制运作方式。避免单一的监管理论，在法律多元化框架下采用多种规范性标准，特别是在人权保护和网络治理领域。WTO 缺乏评估非贸易相关的国内、双边和区域数据法律规范的能力，无法判断有关措施是否仅限制人权保护，是否影响互联网的开放性框架（Aaronson, 2018）。多数监管体系和机制均承认并强调数据保护的基本权利和人权属性。就隐私保护达成一致、合理、可互操作的全球标准，可以推动数据的自由流动和数字贸易（Mishra, 2019）。WTO 需要与联合国人权保护机制、区域性人权保护机制保持联系，以进一步细化保护基准，更好地落实一般例外条款。WTO《电子商务协议》第 16 条“个人数据保护”中，第 4 款要求各方的法律框架考虑有关国际机构和组织的原则和标准，第 7、第 8 和第 9 款鼓励各方通过多种安排和信息交换机制促进不同法律框架的兼容性。换言之，将数据保护的兼容任务留给了成员方，没有确立 WTO 的积极义务，更没有确立国际组织之间的协作机制，不足以推进落实数字贸易中的人权保护。传统上，WTO 与互联网治理利益攸关机构并无任何联系，应当调整并展开全面协调合作。世界贸易规则体系很少提及和指向国际标准、行业最佳实践和近年激增的“负责任行为”协议，尽管它们在数字世界中特别常见（Pauwelyn, 2014）。而目前网络安全全球治理制度和体系几乎均由非正式政府间机制和多利益相关方组成，体现了全球治理中非正式性的兴起（Sukumar 等, 2024）。私营部门的基础设施、专业知识、政策与利益导向具有实质性影响，非政府组织、跨国企业等非国家实体更为正式、系统地参与有关规则的制定过程和落实安排，为网络治理体系的确立和落实作出了重要贡献，形成了独特的多利益相关方

外交,虽有统一性不足的缺陷,但有效弥补了各国以及联合国、欧盟、国际电信联盟等政府间组织在正式外交上的不足(Johnstone等,2023)。

(二)推进个人隐私与国家安全的一体化保护

隐私保护是规制数据跨境流动的首要动机和目标,主权国家逐渐将其作为行使主权的方式,此时国家安全的重要性便得以凸显,但是滥用安全理由可能会导致不恰当的人权限制。在全球动荡的数字时代,国家安全考量的过度扩张容易导致人权保护标准的降低和减损,而且在不被注意的情况下发生。基于国家安全的考虑,政府要求企业等组织共享数据。斯诺登事件后,许多组织对于这种数据共享表现出了担忧(Gensbichler,2015)。一方面,个人信息保护水准决定着一个国家或地区与境外开展数据流动的范围、方式,数字贸易国际治理应防止和遏制国家安全宽泛性应用引起的不必要恐慌。另一方面,仅仅关注个人隐私和信息保护并非确保数据安全的充分条件,区隔出某些数据并以国家安全之名维护国家主权和公共利益虽具有正当性,但简单的区隔和粗暴的限制不是解决问题的办法。事实上,隐私、个人信息、数据以及个人、组织、国家在多数情形下高度关联,简单地划定界限无法厘清个人和组织对数据的权利、国家对安全的关切,粗暴切割容易忽视个人隐私、个人信息,无法达到保障国家安全的效果。法律将安全义务区分为个人、组织、国家的不同类型,看似各司其职,但可能导致个人、组织在数据活动中漠视公共利益,反之则因国家安全考量过度扩张,致使所有数据活动皆置于国家监管之下,严重违背“先市场后国家”的自由贸易规律。换言之,个人信息保护与数据安全在一定程度上应当是同一问题,个人信息保护是合理收集、处理、利用数据,而数据安全是指确保个人数据安全的政策、方式和方法。数据安全是个人信息保护的前提,个人信息保护的核心在于数据安全,维护网络安全是两者的结合。

自民族国家出现以来,国家安全的相关性问题始终是国际关系领域的核心议题,包括国家保护其公民免受恐惧、免受安全威胁。协定处理国家安全和个人隐私的问题需要权衡不同价值之间的关系,如何确定个人隐私权和私生活的保护涉及整个国家及所有公民的国家安全优先顺序。保护个人隐私和数据是数字时代人权保护的重要维度,作为促进和保障个人、国家和国家安全的途径,人权与国家安全应当是共存而非排他的。立法旨在以法治方式回应数字技术的发展,防止公权力的不正当干涉;对于重要、敏感数据,仍须在保护个人权利的前提下,才能基于国家安全行使支配权。大数据发展导致国家秘密与非国家秘密之间的界限模糊,但这并不意味着国家可以全面介入与渗透。国际社会尚未就适当的监管政策以及私人 and 公共数据收集处理的边界达成一致,数据的流动性导致各国的国家安全机构有权在全球范围内展开监视活动,所有国家均呈现出拥有获得一切信息或数据的权力。每个国家均以自己的方式行使数据主权,切断了政府与个人、组织的关联,割裂了国家与国际社会的互动。这种做法忽视了一个基本前提,数据安全并非科技创新、贸易发展和经济增长的对立面,而应当是全体人类良好生活品质的保障。互联网的有效利用有赖于高度创新和全球数据、服务的交换,各国应反思数据主权、网络主权究竟意

意味着什么。为了消除数据跨境流动壁垒,各国须以全球贸易自由化、人类社会整体的福祉为目标,重新审视国内数据规则和监管机制,探索适当的国际治理规则和理念以适宜全球经济发展的需求。

(三)重新认识国家安全,灵活规制国家安全例外

随着国家安全概念内涵的扩张,其影响已渗透到全球经济和贸易领域,贸易与安全之间的界分和矛盾越来越受到关注。国家安全认知的扩张并演变为日常操作,最为典型的正是网络世界,网络安全和数据安全成了国家博弈的新战场。以例外框架应对网络安全常态化,国际贸易法体系正在发生着转变(Peng, 2015)。多边贸易体系初始目标就是缓解经济一体化冲突并防止世界大战,然而,新的国家安全挑战了这一结构。相对独立的国家安全和经济全球化正在发生巨大的冲突,传统的外交谈判和相互克制无法解决这种冲突,必须为解决数字贸易中的国家安全实践冲突确立新的安全例外机制。WTO《电子商务协议》第 22 条和第 23 条认可 WTO 协议的一般例外和安全例外,在此基础上,第 25 条明确了不妨碍为保护个人数据和隐私而采取限制数据流动的例外措施。这强化和扩大了自我裁断的自由度,没有为数字贸易的国家安全例外规制提供完整答案,更无法弥合现有协定、各方立场和做法的分歧。那么, WTO 如何管理这些冲突,为国家安全、国内公共政策作为例外情况提供更为明确的依据?各国不能将网络安全一律视为国家安全,应合理区分经济社会安全和国家安全;升级数据安全和规制方法,反思基于国家安全规制跨境数据流动的合理性。各国加强对数据的控制以限制流动,打破了企业依赖全球市场有效运营的模式,此举能否防止未经授权而对敏感数据访问、减少网络攻击对关键基础设施的损害,目前并未有支持性的实证数据,但负面效果值得警惕。以国家安全为由审查所有与数据隐私相关的交易,过于泛化。在没有证据表明禁止外国技术正当性的情况下,一味强调网络安全会迫使各国研发自己的技术和应用程序,减少国与国之间的互动,加剧国家之间的不平等。网络安全不应进一步分化国际社会和制造国际竞争,尤其是当这种分化可能会抑制创新时。

司法审查可以限制安全例外措施。因此,传统观点是探讨 WTO 争端解决机制是否有权审查成员方有关国家安全的立法内容和决策过程,以及如何判定例外措施的合法性(Alford, 2011; Schill 和 Bbiese, 2019)。据此,俄罗斯过境案为利用 WTO 的制度确立了一个嵌入性框架,即相关紧急措施对维护国家安全利益的必要性只需经过尊重型的善意测试。但善意测试依旧涉及国家安全的实质性审查,如对一些企业限制是否足以保障国家安全。鉴于国家安全认知的扩大,成员方可以辩称相关措施既涉及一国的基本安全利益,又貌似有助于保护这些利益,导致司法审查失灵,安全例外措施重新回归到政治层面的自我限制。如今全球经济秩序与国家安全概念紧密地交织在一起,难以分解。自我决断和法庭裁决均不可行,需要将国家安全置于国际贸易治理改革的背景之中,重新审视国家安全的挑战,防止改革陷入不可行的二分法窠臼;找到有效应对“新”国家安全瓦解经济秩序的解决方案,利用法律构建在国际贸易争端期间出现的“影子政治”,将政治和法律手段结合起来解

决安全争端,利用“去司法化”方案将安全措施的部分成本内化,使政策灵活性的需要与将国家安全纳入法律秩序的重要性相协调,以促进数字贸易与国家安全机制之间的相互承认和平衡。

(四) 提促重视规制自主权和数据发展权的中国方案

在某种程度上,美国和欧盟是数字贸易国际治理分散化和WTO电子商务谈判不顺的重要原因。欧盟要求向其法律制度看齐靠拢,美国则利用低水平保护机制让各国的个人信息方便地向美国集聚。这个背景下,中国对于WTO的重塑极为关键。中国一方面认同数据保护和自由流动的重要性,另一方面强调为主权、安全和发展留有国家干预和本地化监管空间极为重要。相比欧美,中国方案的价值取向最为全面均衡,对数据主权和数字贸易发展的包容度最高,与大多数国家的利益诉求趋同,具备了有效弥合各方分歧的潜力。首先,数字贸易国际治理涉及主权是题中应有之义。为了防范美国对全球数据的收集和监控,以及欧盟的高标准和过度监管给本国经济发展和国家安全带来的巨大威胁,各主权国家为了巩固数据主权而采取诸多限制。长期以来,发展中国家对跨境数据流动的监管多专注于威胁国家主权和安全等非经济因素(Feldman和Garcia,1982)。2020年,中国发起《全球数据安全倡议》,从尊重国家主权和数据安全的角度推动数据主权和规制自主权,强调各国不得要求本国企业将在国外生成或获取的数据存储在本国。目前,俄罗斯、巴基斯坦、柬埔寨、东盟、阿拉伯联盟等表示支持这一倡议。美国和欧盟以缺乏人权和隐私权对此倡议提出疑问。中国的国际主张与国内立法均体现了对国家主权、国家安全、个人数据保护和数据流动自由的平衡考量。为了推进中国倡议的国际认可度和主权人权的一体化保护,必须摒弃欧美在主权和人权问题上的双重标准和偏见。其次,中国秉持机会均等的发展权价值理念,基于共商共建共享原则,弥合数字鸿沟,以推动数字发展成果更多、更公平地惠及全世界^①。数字鸿沟不利于数字贸易自由化和可持续发展,数字霸权是部分数字贸易壁垒的产生根源,这是重回数字贸易全球治理之路必须面对的问题。归根结底,少数国家为维护创新资源和技术研发的绝对优势,借助泛化的国家安全概念不愿与他国共享基础成果,是很多发展中国家面临数字基础设施、能力缺失和技术落后等困境的根本原因。中国对发展权的重视与发展国家的人权立场一脉相承,有助于深化国际社会对数字鸿沟和数字霸权的认识与防范。数字技术发展的不平衡引起了国家社会普遍关注。印度学者主张发达国家的大型科技公司错误地从发展中国家个人获得资源,应称为数据殖民主义(Paco,2022)。鉴于数据大多存储在外国并为国际科技大公司所拥有,发展中国家试图通过国家主义特别是本地化授权扭转自由主义和规制主义带来的被动局面,避免在数字贸易发展进程中被边缘化。平衡贸易自由化和监管自主权的南北差异必将体现在

^①中国关于全球数字治理有关问题的立场(就制定“全球数字契约”向联合国提交的意见)[EB/OL]. 2023-05-24[2024-12-03]. https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202305/t20230525_11083602.shtml. 全球数据跨境流动合作倡议[EB/OL]. 2024-11-20[2024-12-03]. https://www.cac.gov.cn/2024-11/20/c_1733706018163028.htm.

更为细致的治理安排上,例如是否免除电子传输关税。在 WTO 电子商务谈判中,各方对此意见不一,印度和南非基于 UNCTAD 的数据鸿沟报告,认定免税会边缘化发展中国家利益,不利于推进以发展为导向的电子商务^①;澳大利亚、新加坡、瑞士等基于 OECD 电子传输关税报告,认为免税不会增加财政收入,反而会阻碍电子商务和技术发展,产生通胀风险,不利于提升消费福利和降低出口竞争^②。

中国初步构建了跨境数据流动监管框架,始终积极参与 WTO 有关谈判,并于 2021 年申请加入 CPTPP 和 DEPA。近年,国际地缘政治环境日趋复杂,数字贸易国际治理博弈升级,这对作为大型经济体的中国尤为艰难。在此背景下,进一步明确和细化中国方案极为紧迫。

第一,针对外界批评和指责,确立和完善中国方案叙事,有效回应和回击美欧表面自洽的逻辑和偏颇的叙事重点。中国是数据本地化要求的典型代表,以此为例说明叙事的整体性和针对性。首先,客观认识本地化监管措施的利弊和正当性,驳斥标签化批评。中国的数据本地化做法与许多国家的做法并无二致。美国简单设定所有数据本地化措施均有保护主义色彩是没有根据的,而且美国也采取数据本地化措施,适用于国防部工作的云计算服务提供商和存储或传输联邦数据。过去几十年,实行数据本地化的国家和地区激增至 140 多个。Peng 和 Liu (2017) 认为这影响了数字贸易发展,与互联网无边界的初衷背道而驰 (Peng 和 Liu, 2017)。产生此观点的部分原因在于发展中国家监管能力不足,往往采取过于单一的措施,导致过度保护和对本地化的误解,被误认为“数据民族主义”(Chander 和 Lê, 2015)。我们不应过度地否定数据本地化制度(王玥, 2016),不能完全否认数据本地化的益处 (Selby, 2017),更不能否认本地化措施维护国内利益目标的正当性(洪延青, 2017)。因此,关键不在于能否采取本地化限制措施,而在于本地化措施的正当性依据及其范围,应当明确主权国家有权认定数据本地化措施的合理界限及有权行使的手段,并确立基本的国际规范框架。其次,虽然指认中国本地化措施最为严格失之偏颇,但中国的规制理念过于保守,数据法侧重于规制和审查以确保安全,对促进数据自由流动和降低数字贸易壁垒的重视程度不够。数据自由跨境流动是大势所趋,数据不可能绝对本地化,限制只能是短期的、相对的。一国跨境数据流动规制的目标通常难以实现,数据存储高度集中容易遭受网络攻击或监控,而且容易使国内市场被孤立,本国企业难以参与国际竞争。有缔约国强调 CPTPP 严格限制本地化,对中国的本地化要求表示怀疑,DEPA 部分缔约国表达了类似的担忧。中国数据本地化

①UNCTAD, The Covid-19 Crisis: Accentuating the Need to Bridge Digital Divides, UNCTAD/DTL/INF/2020/1, 6 April 2020. Proposal of India and South Africa, Moratorium on Customs Duties on Electronic Transmission: Need for Rethink, WT/GC/W/747, 13 July 2018. Communication from South Africa and India, Reinventing the Work under the 1998 Work Program on Electronic Commerce, WT/GC/W/747, 4 December 2020.

②Andrenelli A., López-González J. Electronic Transmission and International Trade: Shedding New Light on the Moratorium Debate, OECD Trade Policy Papers, No. 233, 13 November 2019. Communication from Australia, Canada, New Zealand, Singapore, Switzerland, etc., Broadening and Deepening the Discussion on the Moratorium on Imposing Customs Duties on Electronic Transmission, WT/GC/W/799/Rev. 1, 29 June 2020.

限制并非强制性,加入CPTPP和DEPA有助于弱化中国的本地化要求。为了更好地回应外界的质疑与批评,中国应强化鼓励数据流动的基本立场,同时细化数据主权规则以提升监管体系的系统性;对数据流动自由作出一般性承诺,以例外条款形式完善WTO一般例外和安全例外的规则与实践;根据数据的内容属性,对数据分类分级采取不同类型的本地化措施,削弱本地化措施对数据安全和经济效益的负面影响。

第二,从被动转为主动的关键是以建立制度性规则体系和治理机制强化国际竞争力。为了争夺主导权,规则竞争已经成为数字贸易竞争的主要方式。美国、欧盟的规则和策略都是在长期实践的基础上演化、发展而来。中国相关法律起步较晚,理论上和实践上存在与国际规则衔接并产生国际示范效应方面存在差距。首先,数字贸易制度的国际竞争力与国内隐私保护水准的提升密不可分,需对照国际人权标准,完善个人信息保护。多数国家将个人信息保护与个人隐私与自由保护为起点,建立在尊严、人格和信息自决等理念之上,而中国《个人信息保护法》和《民法典》等采取了区隔主义的做法,区分了隐私、信息、数据,并割裂了它们之间的内在关联,主要目的是促进数据产业的发展,但存在忽视权利保障的可能性(吴晓丹,2023;朱晓峰和黎泓玥,2023)。中国需进一步完善个人信息保护法律规范,将隐私权和个人信息保护确立为基本权利,恢复隐私、数据和信息之间的内在关联,既重视数据产业发展,也关注个人权利保障。其次,中国数据跨境监管虽然秉承着平衡安全与发展的大方向,但安全与发展边界以及平衡方法不清晰,实践中常因过度注重安全而出现“一刀切”的做法(叶传星和闫文光,2024)。中国需以基础理论为依据,推进形成科学、系统、一以贯之的具体制度设计,以行业透明度和问责机制构建数据要素市场,细化分级分类管理和提升数据安全的执法能力,实现安全与发展相平衡的规制导向(高秦伟,2024)。再次,在尊重他国数据主权和行使域外管辖权之间取得平衡,中国需进一步澄清国内法的域外效力,细化对侵犯国家安全、数据主权、公共利益行为行使域外管辖的情形。行政执法是中国数据法能否有效域外适用的重要环节,应确定罚款、没收违法所得等措施作为追究违反行政责任的手段,以规范违反中国《数据安全法》但尚不足以构成犯罪的域外行为。赋予法院充分权力的司法体系是重要基础和保障,将最高人民法院司法解释把国内法的域外管辖权合理扩展至跨境数据流动领域。

第三,增加国际层面互动,积极参与多边和双边谈判,推进数据跨境流动和数字贸易,拓展中国方案的影响力空间。顺应分散化竞争趋势,积极拓展双边或区域贸易协定;坚持推进WTO谈判,联合有共同利益诉求的国家,反驳西方国家的激进方案,确保数字贸易规则体系和价值理念发展的民主性、公正性和合理性。利用双边、多边协议形成数据保护合作态势,团结非西方国家推进数据互信建设,以凝聚数据主权和发展权共识。可以将与东盟的双边合作作为中国方案的样板,设计针对东盟的数据跨境流动认证和标准合同等工具,主动与东盟进行制度性对接,促成中国和东盟双向个人数据流动安全。在这些进程中,对个人信息保护、规制自主权、数据本地化、数据发展权、一般例外和安全例外的指导原则和制度安排提出具体建议。例如,在维护国家安全和推动数字贸易自由的双重前提下,确定WTO数

字贸易国家安全例外条款的存在,审慎对待其自裁决性质,细化例外规则内容,探索灵活结合政治和法律手段解决安全争端的办法。此外,互联网平台是值得关注的重要角色。基于市场力量和政府监管的互动,平台越集中,越容易与政府建立伙伴关系并共同应对公私领域的挑战。中国政府可以为中国平台企业提供更多的合规能力建设,协助平台利用技术手段和国内程序对政府越权监管行为提出疑问和挑战。借鉴西方的做法,强化平台自我规制和与政府直接合作能力,在特定事件中共享信息、识别威胁、同步政策响应,并与执法部门协调,加强平台之间以及与反恐、消费者保护、人权保护等关键政策领域利益攸关者之间的合作。提升所在国的一般安全和国家安全执法的透明度,限制隐私权和安全概念扩张,减少信息不对称,改善监管制度设计和监管行为,为中国方案提供民间外交和游说助力。

四、结 语

20世纪90年代以来,WTO始终致力于解决贸易自由化语境下的跨境数据流动规制问题。全球治理缺位、各方立法表述和贸易协定发展给数据驱动行业带来了极大的不确定性。在数据主权概念下,为了减少数据流动壁垒和降低成本,需要国家彼此间摒弃不友好态度,以相互兼容和公正客观的方式对待处理监管差异,在确保发展权和规制自主权的前提下推动全球治理。中国、美国、欧盟和其他主要经济体的个人信息保护和数据主权的重点有所差异,但都认同数据的隐私保护属性和数字贸易的发展方向,认同合理的数据流动是数字贸易和数字经济发展的迫切需求,这是重塑WTO中心化地位的共识性基础。中国缺席WTO规则体系和治理理念的创设过程,但在入世后,作为数字经济和贸易大国,中国有能力为重塑WTO做出建设性的贡献。

[参考文献]

- [1]杜明.国家安全的国际经济法回应:以华为诉瑞典仲裁案为例[J].国际法研究,2023(5):3-27.
- [2]高秦伟.个人信息保护视域下的数据经纪人及其规制[J].政治与法律,2024(6):159-176.
- [3]洪延青.在发展与安全的平衡中构建数据跨境流动安全评估框架[J].信息安全与通信保密,2017(2):36-62.
- [4]牛可.美国“国家安全国家”的创生[J].史学月刊,2010(1):63-90.
- [5]石静霞.国际贸易投资规则的再构建及中国的因应[J].中国社会科学,2015(9):128-145.
- [6]石静霞.中国加入CPTPP谈判中的服务贸易重点问题[J].中外法学,2023(4):845-864.
- [7]王玥.试论网络数据本地化立法的正当性[J].西安交通大学学报(社会科学版),2016(1):54-61.
- [8]吴晓丹.私密信息合理使用的规范体系及其限制[J].华东政法大学学报,2023(5):56-69.
- [9]叶传星,闫文光.论中国数据跨境制度的现状、问题与纾困路径[J].北京航空航天大学学报(社会科学版),2024(1):57-71.
- [10]朱晓峰,黎泓玥.私密信息与敏感个人信息区分保护论[J].经贸法律评论,2023(1):21-38.
- [11]AARONSON S A. What are We Talking about When We Talk about Digital Protectionism[J]. World Trade Review, 2018(1): 6-7.

- [12] ALFORD R P. The Self-judging WTO Security Exception[J]. *Utah Law Review*, 2011: 704-706.
- [13] BASEDOW R. The WTO and the Rise of Plurilateralism — What Lessons can We Learn from the European Union's Experience with Differentiated Integration[J]. *Journal of International Economic Law*, 2018, 21(2): 411-431.
- [14] BAY N C. Executive Power and the War on Terror[J]. *Denver University Law Review*, 2005(83): 376-377.
- [15] BLUME J D. Reading the Trade Tea Leaves; A Comparative Analysis of Potential United States WTO-GATS Claims against Privacy, Localization and Cybersecurity Laws[J]. *Georgetown Journal of International Law*, 2018 (49): 801-819.
- [16] BRANFORD A. The Brussels Effect—How the European Union Rules the World[M]. Oxford: Oxford University Press, 2020.
- [17] BROWNELL R E II. The Coexistence of United States vs. *Curtiss-Wright* and *Youngstown Sheet & Tube vs. Sawyer* in National Security Jurisprudence[J]. *Journal of Law and Politics*, 2000, 16(1): 7-16.
- [18] BULFORD C. Between East and West: The APEC Privacy Framework and the Balance of International Data Flows [J]. *Journal of Law and Policy for the Information Society*, 2007, 3(3): 707-709.
- [19] BURRI M. The Regulation of Data Flows Through Trade Agreements[J]. *Georgetown Journal of International Law*, 2017, 48(1): 438-448.
- [20] CHANDER A, LÊ U. Data Nationalism[J]. *Emory Law Journal*, 2015, 64(3): 677-713.
- [21] CHIN Y, ZHAO J. Governing Cross-border Data Flows: International Trade Agreements and Their Limits[J]. *Laws*, 2022, 11(4): 63-73.
- [22] CORS D. National Security Data Access and Global Legitimacy[J]. *Department of Justice Journal of Federal Law and Practice*, 2019: 67(4): 280-281.
- [23] CLAUSIUS M. The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes[J]. *Washington University Global Studies Law Review*, 2022, 21(2): 273-275.
- [24] DAVIDOW W H, MALONE M S. The Virtual Corporation: Structuring and Revitalizing the Corporation for the 21st Century[M], New York: Harper Business, 1991.
- [25] DUNLAP C. J. The Hyper-personalization of War: Cyber, Big Data, and the Changing Face of Conflict[J]. *Georgetown Journal of International Affairs*, 2014(15): 108-118.
- [26] East Asia Forum Editorial Board. The Gaping “National Security” Hole in the World Trade Regime[J/OL]. 2023-10-02[2024-12-03]. *East Asia Forum*, <https://doi.org/10.59425/eabc.1696248924>.
- [27] ESTADELLA-YUSTE O. Transborder Data Flows and the Sources of Public International Law[J]. *North Carolina Journal of International Law*, 1991, 16(2): 379-382.
- [28] FELDMAN M B, GARCIA D R. National Regulation of Transborder Data Flows[J], *North Carolina Journal of International Law*, 1982, 7(1): 1-10.
- [29] FORD P. Implementing the EC Directive on Data Protection — An Outside Perspective[J]. *Privacy Law and Policy Reporter*, 2003, 9(8): 141-149.
- [30] GARDNER W J. Divergent Strategies: A Legal History of the WTO's National Security Exception in the Context of a Globalized Economy, 1983-2019[J]. *University of Miami International and Comparative Law Review*, 2020, 28(1): 181-197.
- [31] GENSBICHLER G. Trusted Information Brokerage in the Times of the Snowden-Effect Dilemma: Private-Public Data Sharing in Cyber Security in Austria, Germany, and Switzerland[J]. *Georgetown Journal of International Affairs*, 2015(16): 30-57.
- [32] GREGORY W V. Cross-border Data Flows, the GDPR, and Data Governance[J]. *Washington International Law Journal*, 2020, 29(3): 485-507.
- [33] GUNASEKARA G. The “Final” Privacy Frontier-regulating Transborder Data Flows[J]. *International Journal of Law and Information Technology*, 2007, 15(3): 362-378.

- [34] HEATH J B. The New National Security Challenge to the Economic Order[J]. Yale Law Journal, 2020(129): 1020–1050.
- [35] HONDIUS F W. Data Law in Europe[J]. Stanford Journal of International Law, 1980(16): 87–90.
- [36] KIRBY M. Legal Aspects of Trans-border Data Flows[J]. Computer Law Journal, 1991, 11(2): 233–236.
- [37] International and Regional Organizations. Civil Society Letter against Digital Trade Rules in the World Trade Organization[EB/OL]. 2019-04-01[2024-12-03]. https://ourworldisnotforsale.net/2019/Digital_trade_2019-04-01-en.pdf.
- [38] JOHNSTONE I, SUKUMARA, TRACHTMAN J. Building an International Cybersecurity Regime: Multistakeholder Diplomacy[M], Glasgow: Elgar, 2023.
- [39] LINDSAY P. The Ambiguity of GATT Article XXI: Subtle Success or Rampant Failure[J]. Duke Law Journal, 2003(52): 1278–1313.
- [40] MACDONALD D A, STREATFIELD C M. Personal Data Privacy and the WTO[J]. Houston Journal of International Law, 2014(36): 627–638.
- [41] MITCHELL A D, HEPBURN J. Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-border Data Transfer[J]. Yale Journal of Law and Technology, 2017(19): 195–206.
- [42] MITCHELL A D, MISHRA N. Regulating Cross-border Data Flows in a Data-driven World: How WTO Law can Contribute[J]. Journal of International Economic Law, 2019, 22(3): 389–391.
- [43] MISHRA N. Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows[J]. Vanderbilt Journal of Transnational Law, 2019(52): 463–501.
- [44] NAEF T. Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law[M]. Switzerland: Springer, 2023.
- [45] PACO S A. Data Colonialism, the Danger It Poses to India's Democracy, and the Effectiveness of Data Localization Laws as Resistance[J]. Rutgers Computer and Technology Law Journal, 2022, 48(2): 254–264.
- [46] PAUWELYN J. Rule-based Trade 2.0? The Rise of Informal Rules and International Standards and How They may Outcompete WTO Treaties[J]. Journal of International Economic Law, 2014, 17(4): 739–751.
- [47] PENG S. Cybersecurity Threats and the WTO National Security Exceptions[J]. Journal of International Economic Law, 2015, 18(2): 449–478.
- [48] PENG S, LIU H. The Legality of Data Residency Requirements: How can the Trans-Pacific Partnership Help[J]. Journal of World Trade, 2017, 51(2): 183–199.
- [49] PINCHIS-PAULSEN M. Trade Multilateralism and U. S. National Security: The Making of the GATT Security Exception[J]. Michigan Journal of International Law, 2020, 41(1): 109–114.
- [50] REIDENBERG E J. Resolving Conflicting International Data Privacy Rules in Cyberspace[J]. Stanford Law Review, 1999, 52(5): 1315–1318.
- [51] SCHILL S, BBIESE R. “If the State Considers”: Self-judging Clauses in International Dispute Settlement[J]. Max Planck Yearbook of United Nations Law, 2019(13): 120–138.
- [52] SELBY J. Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both[J]. International Journal of Law and Information Technology, 2017, 25(3): 213–227.
- [53] SHAFFER G. Tragedy in the Making: The Decline of Law and the Return of Power in International Trade Relations[J]. Yale Journal of International Law, 2018(64): 41–42.
- [54] SINGH P J. Data Localization: A Matter of Rule of Law and Economic Development[J/OL]. 2018-09-15[2024-12-03]. <https://itforchange.net/data-localisation>.
- [55] SUKUMAR A, BROWDERS D, KELL M. The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-state Actors and Diplomacy[J]. Contemporary Security Policy, 2024, 45(1): 7–44.
- [56] SVANTESSON D A. “Layered Approach” to the Extraterritoriality of Data Privacy Laws[J]. International Data Privacy Law, 2013, 3(4): 278–286.

- [57] YAKOVLEVA S. Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade "Deals"[J]. *World Trade Review*, 2017, 17(3): 477-508.
- [58] YOO J. Embracing the Machines: Rationalist War and New Weapons Technologies[J]. *California Law Review*, 2017, 105(2): 443-446.
- [59] WILCOX C. The Promise of the World Trade Charter[J]. *Foreign Affairs*, 1949, 27(3): 492-493.
- [60] WINSCH-VINCENT S. The Internet, Cross-border Trade in Services, and the GATS: Lessons from US Gambling [J]. *World Trade Review*, 2006, 5(3): 319-335.
- [61] WU M. Digital Trade-related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multi-lateral Trade System[M]. *International Centre for Trade and Sustainable Development*, Geneva: ICTSD, 2017.
- [62] WU T. The World Trade Law of Censorship and Internet Filtering[J]. *Chicago Journal of International Law*, 2006, 7(1): 263-287.
- [63] ZALNIERIUTE M. Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement[J]. *Modern Law Review*, 2018, 81(6): 1052-1053.
- [64] ZALNIERIUTE M. Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security[J]. *Vanderbilt Journal of Transnational Law*, 2022, 55(1): 4-48.

International Governance of Digital Trade: Reshape the Centralized Role of WTO

WU Xiaodan

(Law School, Central University of Finance and Economics, Beijing, 100081)

Abstract: The multi-dimensional nature of data and the complexity of related issues led to the vital differences in values, policy orientation and approaches of national regulation of trans-border data flows and constituted non-tariff trade barriers. The bilateral and regional trade agreement spurred by the United States and the European Union worsened the fragmentation, differentiation and insufficiency of international rules for digital trade. It is of imperative to re-direct the fragmented regulation into global governance and reshape the central status of WTO. The approaches are establishing multi-centered global governance based the multi-dimensional nature of data; promoting the integrated protection of personal privacy and national security; and flexibly regulating national security exceptions by the combination of political and legal means. The WTO e-commerce negotiation is mainly among the cooperation and competition between China, the United States and the European Unions, and China's proposal emphasizing regulation autonomy and rights to development is important for the formation of rules on digital trade. To increase its international relevance, China's proposal shall be elaborated into a complete narrative and constructive regulation system.

Keywords: International Governance of Digital Trade; Trans-border Data Flows; WTO; E-commerce Negotiation; China's Proposal

(责任编辑 祝子白 刘建昌)