doi:10.16060/j.cnki.issn2095-8072.2026.02.006

WTO 法框架下的数据跨境流动规制*

任妍姣

（中央财经大学法学院，北京 100081）

摘　要：数据跨境流动规制是全球数字贸易治理的基础性问题，WTO 法是最适合用来协调各法域数据跨境流动的规制规范。数据跨境流动的规制取向分为数据自由流动和数据安全流动，其规制路径包括严格数据本地化措施和附条件数据流动机制。数据隐私、线上消费者保护、网络空间治理、数字产业政策等政策目标，可作为判断 WTO 法与两类数据本地化措施是否兼容的主要依据。从应然意义上讲，WTO 法应容许契合正当公共政策目标的数据本地化措施，并在混合监管、数字信任等原则的指引下紧扣相应政策目标完善规则体系。

关键词：数字贸易；数据跨境流动；世界贸易组织；服务贸易总协定；电子商务诸边谈判

中图分类号：D996.1　　**文献标识码：**A　　**文章编号：**2095－8072(2026)02－0084－13

一、问题的提出

在经济全球化和数字化趋势下，数字贸易中数据跨境流动的国际法规制成为全球数字贸易治理的一项基本议题。学界的相关研究主要分为两大层次：其一，以自由贸易协定为切口，关注数据跨境流动规制的依据（张晓君和屈晓濛，2022）、特定数据跨境流动的规程（马光和卜小翠，2022）、跨境数据隐私保护进路（彭岳，2022）和数据跨境流动规则的对接（宋云博，2024）；其二，以世界贸易组织（WTO）法律为中心，或是围绕多边贸易协定改革话题，建议筛选基本框架协调数据跨境流动规则（谭观福，2022）、汲取自由贸易协定经验补强有关规则（刘影，2023），或是结合诸边贸易协议谈判背景，概述关于数据跨境流动的立场建议（许多奇，2022）。

依上所述，虽然双边或区域贸易法中的数据跨境流动监管安排得到了充分梳理，但如何形塑WTO法中的数据跨境流动监管安排仍有学理分歧。并且，WTO成员通过“联合声明倡议”启动的电子商务诸边谈判未结，亦导致延长全球数字贸易监管制度构建的不确定性。质言之，作为一个通过内外视角重要性检验的论题，WTO法视角下的数据跨境流动规制富有研究价值。有鉴于此，本文侧重挖掘WTO法文本蕴含的文化倾向，在此基础上思考如何从应然层面优化WTO法体系。

二、数据跨境流动规制的基本面向

数据跨境流动是数字服务固有的现实需求，包括数字服务本身的跨境提供和使用服务时发生的跨境数据流动，其本质是数据要素在技术架构层次间具有互操作性的互联网中实现的跨境移动（Palfrey & Gasser，2012）。各国数据跨境流动法律可能同互联网开放、安全的预期阈值相冲突，各国会在其国内政策目标的指引下采取不同规制路径作为数据跨境流动的监管手段，致使全球

* 基金项目：本文受中央财经大学“科教融合研究生学术新星孵化计划”项目“数据跨境流动标准合同条款制度研究”（项目编号：202317）的资助。

数据跨境流动监管制度出现碎片化（贺小勇和刘真宇，2026）。在数据跨境流动规制法域可能发生重叠的情形下，国际法上只有具有完整性的WTO法最适合用来协调不同法域的法律冲突。

（一）数据跨境流动规制的价值取向

互联网的开放性和安全性是数据跨境流动规制价值取向的起点。互联网的开放性要求数据自由流动，互联网开放的本质是“数据全球自由流动”，即“数据通过网络的流动不受不必要或不合理干扰”（Box，2016）。就内涵解构而言，不能把网络中立等同于互联网的技术开放。其中，前者作用于“阻塞、减缓、付费优先”等具体实践相关的国内市场竞争条件，[①]通过防止任意和歧视性阻碍数字服务促进国内互联网的开放性；后者旨在保障用户“自行决定希望使用的应用程序、服务和希望访问、创建或同他人共享的合法内容”的权利（Aaronson，2014），因不限于促进国内互联网的开放性而意义更为广泛。此外，经济合作与发展组织（OECD）的报告也提示应注意互联网开放的其他方面，即经济开放要求用户通过联网用网拓展经济机会并将之用于生产用途，社会开放要求用户利用互联网拓展联络他人、获取资讯、表达观点等非经济机会。[②]

互联网的安全性要求数据安全流动。网络安全、数字安全、信息安全等术语曾被用于指代互联网安全（Drake et al.，2016）。笔者认为，互联网安全同样是网络安全以及数据安全所延伸的应用安全、隐私安全的广义集合。在没有现实网络可以绝对安全的前提下，网络安全须以最大限度保持网络的稳定性与完整性为要义。顾名思义，应用安全指互联网技术架构的最上层——应用层的安全，其实现有赖于网络安全和数据安全的结合。鉴于数据保护是“隐私权的表达”，隐私是“数据保护的核心”（Kokott & Sobotta，2013），隐私安全可谓数据安全和应用安全基础上的最高级安全形态。以数据访问的情形为例予以解释，应用安全的精髓在于防止未经授权的盗窃行为，而隐私安全的精髓在于防止未经同意的越轨行为。

（二）数据跨境流动规制的实施路径

以严格限度为标准，可将数据跨境流动规制的实施路径分为严格数据本地化措施和附条件数据流动机制。前者的表征是直接影响互联网的物理层或传输层，其形式包括本地存储要求，[③]本地存储和处理要求，[④]以及设置本地存储、处理和访问要求的数据传输禁令；[⑤]后者的要旨是对目的地国和（或）数据控制者、数据处理者施加条件，其载体多为个人数据跨境传输同意要求等数据隐私或网络安全相关条件。[⑥]现实中，某些国家的国内法明确支持严格数据本地化措施与附条件数据流动机制的并用，如俄罗斯第242–FZ号联邦法第2条要求本地存储和处理，但第152–FZ号联邦法第3条第1项、第12条也允许有条件地将数据传输至符合特定国际标准的国家。

根据作用机理不同，可以将数据跨境流动规制的实施路径分为两种情形：其一，规制路径为针对底层数据流动和数字服务的性质或内容，其中阻止提供容纳非法内容和敏感内容的数字服务[⑦]、限制提供影响网络环境清洁的数字服务[⑧]均为典例；其二，规制路径为针对数据被存储、传输、处

① FCC, Restoring Internet Freedom, 2017.
② OECD, Economic and Social Benefits of Internet Openness, 2023.
③ Russian Federal Law No. 242–FZ, Article 2.
④ Regulation (EU) 2018/1807 on the Free Flow of Non–Personal Data, Article 3.
⑤ Turkish Law No. 6493, Article 23.
⑥《中华人民共和国个人信息保护法》第3章。
⑦《计算机信息网络国际联网安全保护管理办法》第4~6条。
⑧《工业和信息化部关于清理规范互联网网络接入服务市场的通知》第2部分。

理和（或）防止未经授权的侵入方式，其中“专门阻碍数据跨国界传输”的数据本地化措施即为典例（Chander & Le，2015）。就这一意义而言，数据本地化措施的外延包括能够影响数据跨国界传输的严格数据本地化措施和附条件数据流动机制。更进一步，数据本地化措施不仅关注数据跨境流动干预程度的限制性政策，也成为被“引述最多的、阻碍数字贸易的政策措施”，造成了数字贸易壁垒。[①]综上可知，数据本地化分类的交叉性增加了数据跨境流动规制的复杂性，这与数据自由流动、数据安全流动等规制取向的尺度性相呼应。

（三）数据跨境流动规制的法域协调

一方面，数据跨境流动规制的法域协调可借助国际贸易法这一中介加以实现。数字贸易对于推动企业参与全球供应链至关重要，尤其能够使企业迅速有效地在各国间迁移数据。一些政府或政府间组织甚至直接承认数据跨境流动对数字贸易增长的重要性。[②]在全球数字贸易稳步发展的态势下，限制数据跨境流动的数据本地化措施往往引发贸易限制效应，这是因为数据的属地性致使其受到国际贸易法的审查。从法律渊源来看，最为主要的无疑是几乎涉及国际贸易法的所有领域的WTO法。当基于现行WTO法审查数据本地化措施时，审查依据应限缩为适用于服务贸易的《服务贸易总协定》（GATS），审查内容应为能否根据GATS一般例外条款证明WTO成员方数据本地化措施的正当性，审查目标随之指向维持服务贸易自由化与国内政策目标的平衡。

另一方面，互联网的开放性和安全性有助于依托GATS实现数据跨境流动规制的法域协调。前互联网时代的GATS显然并非针对数字贸易而设计，该缺陷可通过构思互联网开放与互联网安全的平衡安排加以弥补。这里以所涉程序性证据规则为例加以说明。在涉及一般情况例外的前提下，WTO专家组获准评估与GATS不符的数据本地化措施，判定其是否符合正当公共政策目标或遵守与GATS相符的国内法。[③]鉴于互联网开放和互联网安全的互补性，数据本地化措施对互联网开放和互联网安全平衡的影响因素，也可作为评估政策目标实现措施之必要性、寻求其他较少限制性替代措施等方面的重要证据。证据收集途径包括但不限于，邀请技术和政策专家提供相关意见或技术证据[④]、审查有关国际机构或民间社会组织提交的“法庭之友”（amicus curiae）意见书。[⑤]

三、数据跨境流动规制与 WTO 法的交点

“为与在线交易有关的适当保障措施提供可预测性和互操作性的环境，对于数字贸易生态系统的繁荣至关重要”，[⑥]数据本地化措施能否与WTO法相适应，可反映WTO法律体系与上述数字贸易发展需求的匹配度。作为兼具数据跨境流动限制效果的数字贸易壁垒，数据本地化从国内政策的角度体现WTO成员的安全利益诉求。具体判断它们是否违反WTO法的自由贸易宗旨，则有赖审视面向服务贸易部门的GATS有关规则，以及可能化为未来规则的WTO电子商务诸边谈判提案。

（一）数据本地化措施与个人数据隐私

个人数据隐私保障是数据本地化背后的主要政策目标之一，GATS第14条一定程度上认可其作

① USITC, Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, 2017.
② USITC, Digital Trade in the U.S. and Global Economies, 2014; UNCTAD, Data Protection Regulations and International Data Flows: Implications for Trade and Development, 2016.
③ Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, Article 14.
④ Marrakesh Agreement Establishing the World Trade Organization, Annex 2, Para. 13.2.
⑤ *United States–Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, para.105–108.
⑥ IMF, OECD, UNCTAD, et al., Digital Trade for Development, 2023.

为公共政策目标的正当性。首先，GATS第14条第a项的“保护公共道德”可解释为涵盖“保护个人隐私”（Mishra，2020）。其次，GATS第14条第c项第2目在“措施的适用方式不得构成情况相似国家间任意或无理歧视或变相限制服务贸易”的前提下，直接禁止“阻止任何成员采取或执行保证遵守不与本协定抵触的法律或法规（含涉及处理和传播个人数据方面的个人隐私保护与个人记录和账户保密者）所必要的措施”。由此观之，GATS对WTO成员以保障个人数据隐私为由的适用数据本地化措施予以责任豁免，但前提是能够满足必要性和合比例性测试的双重条件。

遗憾的是，上述关于个人数据隐私保障的规定与数字贸易的可预测性和互操作性需求不甚匹配。第一，它们不能确保WTO成员普遍落实稳健的个人数据隐私法律。其限于笼统支持WTO成员合规适用数据本地化措施以保障个人数据隐私的权利，实则无法惠及仍未创制数据保护和隐私立法的发展中成员和最不发达成员。第二，它们无力协调WTO成员间不同个人数据隐私法律间的冲突。虽然GATS在第7条就互认机制作出专门规定，但其明确“成员可承认（服务提供者）在特定国家取得的学位或经验、满足的资格或获得的执照或证书”，个人数据隐私法律赫然不在所述对象范围内。概言之，GATS不干预WTO成员选择特定的个人数据隐私法律，在个人数据隐私法治统筹上几乎无作为。

各国对于实现在线隐私保护的最佳办法缺乏国际共识（Kuner，2013），此般“各扫门前雪”的极端后果是诱发数据保护主义这一主观政治现象。为此，WTO电子商务诸边谈判试图统一规定个人数据隐私的法律法规。美国的提案是制定或维持“处置侵犯隐私行为的消费者保护法或处置侵犯隐私行为的其他法律”，[①]从中体现其“数据隐私法的整个领域为消费者合同法所涵盖”的法治特色（Ben-Shahar & Levitz，2017）。欧盟的提案则是“商定的纪律和承诺不得影响缔约方/成员各自保障措施对个人数据和隐私的保护”，[②]其在宪法意义上明确个人数据权独立于隐私权的做法与之呼应。[③]澳大利亚在最新一轮诸边谈判中提交了一项新提案，即“不应妨碍缔约方采取或维持保护个人数据和隐私的措施（含有关数据跨境传输者），前提是缔约方的法律规定在保护被传输数据的一般适用条件下允许传输的文件”。[④]

（二）数据本地化措施与线上消费者保护

线上消费者保护是数据本地化背后的另一主要政策目标，GATS第14条也在一定程度上认可其作为公共政策目标的正当性。第14条第c项第1目与第14条第c项第2目共享同一前提，但转向禁止“阻止任何成员采取或执行保证遵守不与本协定抵触的法律或法规（含涉及防止欺诈和欺骗做法或处理服务合同违约影响者）所必要的措施”。该规定直指欺诈交易、合同违约两种损害消费者权益的不当外部行为。据此有理由认为，GATS可豁免WTO成员为保护线上消费者而适用的满足必要性、合比例性双重测试的数据本地化措施。

纵然如是，国际法上的线上消费者保护规则整体缺位，与数字贸易的可预测性需求背道而驰。从法源适用来看，单一适用国内法难以确保自律监管的有效性。目前，线上消费者权益的取得、行使及实现由数字服务合同及其当事人约定的国内法所调整。然而，“当今快速变化且日益复杂的全球数字环境也催生了新的消费者损害形式”。[⑤]另外，国内法自身面临消费者保护色彩的限度之

① WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023: C.2. para.1,3.
② WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023: C.2. para.1,3.
③ EU Charter of Fundamental Rights, Article 7~8.
④ WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023: C.2. para.1,3.
⑤ OECD, Consumer Vulnerability in the Digital Age, 2023.

困。例如，美国虽以消费者保护立场保障个人数据隐私，却受市场化导向的影响鲜少在消费者合同法中运用规制性手段（Winn & Webber，2006）；欧盟虽在数据保护立法中广泛纳入消费者保护要素，但约束基于数据的用户画像和营销策略、Cookie确认弹窗的同意要求等规则受到批判。[①]换言之，只有国际法和国内法共同致力，才能加强数字服务提供者的自律监管。

正因如此，WTO电子商务诸边谈判通过以下三类提案，才能切实推动线上消费者保护的国际立法。第一类是在保障个人数据隐私之余涉及线上消费者保护的提案，这类提案涉及对电子商务用户的信息披露、禁止对数据主体的歧视性待遇、个人数据跨境传输的同意规则等。[②]第二类是在规范电子商务应用之余涉及线上消费者保护的提案，这类提案涉及电子商务交易的完整性与真实性、电子发票和电子支付的跨境互操作性、个人软件源代码或算法开放的禁止及其例外等。[③]第三类是直接旨在保护线上消费者的提案，这类提案涉及线上消费者的公平交易权、消费者保护机构跨境合作、线上消费者救济或追索等，[④]其中关于源代码和算法开放禁令目前尚有争论。

（三）数据本地化措施与网络空间治理

网络安全和网络主权既是网络空间治理的关键支点，也是数据本地化背后的两项主要政策目标。虽然GATS第14条对网络主权并无涉猎，但其一定程度上认可网络安全作为公共政策目标的正当性。首先，第14条第a项的“维持公共秩序”可解释为涵盖保障网络安全的正当公共政策目标，因为网络安全威胁能够达到脚注所言“对一项社会基本利益构成真正和足够严重威胁”的程度。[⑤]其次，第14条第c项第3目与第14条第c项第1~2目共享同一前提，但转向禁止“阻止任何成员采取或执行保证遵守不与本协定抵触的法律或法规（含涉及安全者）所必要的措施”，如此更为直接地允许WTO成员为保障网络安全而适用满足必要性、合比例性双重测试的数据本地化措施。不过，这些规定没有径直推行网络安全监管框架，抑或引导WTO成员加强网络安全监管国际合作，故对数字贸易的可预测性及互操作性需求的满足水平有限。

幸运的是，WTO电子商务诸边谈判逐步树立以风险为本、合作最优的网络安全治理准则。对于事前阶段，初步确定沿用韩国、日本、美国、乌克兰、英国的提案。以“负责应对网络安全事件的国家机构”为单位推进能力建设，并“就识别和缓解影响缔约方/成员电子网络的恶意入侵或恶意代码传播、及时处置网络安全事件、打击网络犯罪、共享信息以提高认识和推广最佳实践开展合作”。[⑥]对于事中阶段，初步确定沿用美国、英国的提案。“风险路径在应对网络安全威胁上可能比指令性监管/方法更有效”，其适用依据由“公开透明的行业标准/协商一致的标准和风险管理最佳实践”，扩张为“风险管理最佳实践和以协商一致、透明和公开的方式制定的标准”。[⑦]

若将数据主权理解为“领土主权在数据领域的延伸”，并结合“网络主权是传统国家主权在网络空间的自然延伸”这一观点，便可确认数据主权与网络主权之间至少存在一定的结构性关联（翟志勇，2018；刘晗和叶开儒，2020）。由此可进一步推断，作为“数据主权具体表现形式”的数

① The Hurdles of Article 22 GDPR Explained. (2022-03-04) [2026-01-15]. https://reflect.ucl.ac.uk/laws0338-privacy-data-and-surveillance-law-2122-class-blog/author/harsh-arya-21/.
② WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023: C.2. para.1,6,10,15.
③ WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023: A.1. para.1~5, C.3. para. 1.
④ WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023: C.1. para.1,3,5,6.
⑤ 例如，面向政府工程承包商的勒索邮件攻击可能摧毁某一国家或地区的能源供应等公共事业。
⑥ WTO Electronic Commerce Negotiations Text, INF/ECOM/57, 19 August 2020: D.2. para.2; WTO Electronic Commerce Negotiations Text, INF/ECOM/62, 15 November 2023: C.4. para.2.
⑦ WTO Electronic Commerce Negotiations Text, INF/ECOM/57, 19 August 2020, D.2. para.3; WTO Electronic Commerce Negotiations Text, INF/ECOM/62, 15 November 2023, C.4. para.3.

据本地化措施与网络主权密切相关（姜伟和龙卫球，2023）。我国在WTO电子商务诸边谈判中一贯主张网络主权，提案保留了将“维护网络空间主权”归入“正当公共政策目标”的内容，[①]弦外之音是期待WTO正视成员对其管辖网络空间内的数据跨境流动的控制权，以及将之同政治、经济、文化、社会等目的相联系的决定权。

（四）数据本地化措施与数字产业政策

现实中，印度、南非将数据本地化措施当作扶持本国数字初创企业的数字产业政策工具。[②]不过，此举可能符合GATS第16~17条的行为不法要件。其一，数据本地化措施可能违反市场准入义务。跨境提供的市场准入承诺覆盖含电子方式在内的所有交付方式，[③]其违反情形覆盖数据本地化措施对提供数字服务造成实际妨碍，届时符合GATS第16条第2款第3项“限制服务交易总量或服务产出总量”的禁止性规定。其二，数据本地化措施可能违反国民待遇义务。事实上，数据本地化是否违反GATS第17条存在学理争议。肯定者主张其当然构成违反国民待遇原则的歧视性措施（Ramesh，2018），否定者则强调其是否违反国民待遇原则无统一答案（Zhang & Mitchell，2021）。

评估数据本地化措施对发展中成员数字发展权的必要性，对满足数字贸易的可预测性需求具有重要意义。部分发展中成员确需更多时间开放服务贸易部门加入国际数字市场竞争，因为“贸易自由化不会自动增加贸易机会，更不用说促进贸易发展”（Córdoba，2008）。但也有实证研究表明，发展中成员推行数据本地化措施的经济回报不如预期（Badran，2018）。WTO基本原则中的经济发展原则旨在帮助发展中成员融入全球经济，增加境内成员获得质优价廉的数字服务的机会，是发展中成员缩小与发达成员数字鸿沟的必要途径之一。[④]以数据本地化措施为遏制数字初创企业的竞争对手背书，终将适得其反地抑制发展中成员的数字经济水平。

近年来，WTO特别关注电子传输关税这种数据本地化措施。一项WTO电子商务工作计划显示，印度、南非曾表示“暂停征收电子传输关税可能显著改变谈判达成的权利和义务平衡”，并认同“永久暂停征收电子传输关税将主要令发展中国家遭受重大关税损失”。[⑤]而WTO电子商务诸边谈判的讨论以免征电子传输关税为基调，其中澳大利亚、加拿大、瑞士、智利、欧盟、危地马拉、日本、韩国、挪威、新西兰、新加坡、乌克兰、英国和美国拥护电子传输关税禁令永久化，禁止对电子传输（含以电子方式传输的内容）征收关税。中国、沙特阿拉伯、土耳其意在暂时维持现状，即保持对电子传输免征关税。印度尼西亚、阿根廷实行区分对待，以保持对电子传输免征关税的做法为原则、根据公共政策目的酌情调整为例外，并将以电子方式传输的内容作为电子传输关税禁令的适用除外。[⑥]

四、数据跨境流动规制的 WTO 法应对

探讨WTO法规制数据跨境流动的理想图谱，既须直面数据本地化措施的去留之争，更要斟酌数据本地化主要政策目标和WTO法自由贸易宗旨的平衡之策。前一层次在WTO电子商务诸边谈判

① WTO Electronic Commerce Negotiations Text, INF/ECOM/62, 15 November 2023, D.1. para.2,9.
② The E–commerce Moratorium and Implications for Developing Countries–Communication from India and South Africa, WT/GC/W/774, para.5.
③ *Work Programme on Electronic Commerce–Progress Report to the General Council*, S/L/74, 27 July 1999, para.15.
④ World Bank Group, World Development Report 2016: Digital Dividends, 2016.
⑤ Moratorium on Customs Duties on Electronic Transmissions: Need for a Re–think–Communication from India and South Africa, WT/GC/W/747, 13 July 2018, para.2.2.
⑥ WTO Electronic Commerce Negotiations Text, INF/ECOM/62, 15 November 2023: B.1. para. Alt 1~3.

中具化为若干选择，笔者认为，中国、巴西的提案依托比较优势脱颖而出，即在规避普泛化自由之余保留特需性例外。[①]后一层次的根本要求是增强WTO自由贸易体制对成员安全利益诉求的包容性，基本步骤是基于前述价值取向之起点所延伸的全新原则，有的放矢地依赖全角色共治完善相应的WTO规则，以下展论之。

（一）原则再造：以安全交互为核心追求

1. 由互联网开放到混合监管

如前所述，互联网开放的一个方面是社会开放，利用联络他人的非经济机会是其行为表现之一。从文义解释出发，联络取“彼此交接、接上关系”之意，互联网治理的多利益相关方诉求“将所有利益相关方纳入基于合作、协作和伙伴关系的治理安排”[②]与之内在一致，由此抛出数据跨境流动规制嵌入互联网软法治理的合理性思考。作为“推进互联网界某些特定利益”的非政府授权组织（Waz & Weiser，2012），多利益相关方组织本身即为一种互联网软法实践。如要支持其取得数据跨境流动规制主体资格，便须让跨境监管突破以政府直接监管为传统的多边监管模式，转而走向以公私合作治理为特色的混合监管模式。相比于直接监管，混合监管的优势是对守法主义偏狭和执法僵化风险的适应性。Hirsch（2013）指出，“混合监管可能比直接监管更实际，并比自律监管更有效”。

在WTO法中贯彻混合监管原则具备可行性基础。其一，WTO对国际组织间合作的概念并不陌生。早前，WTO便就外汇管理、经济决策、营商环境评估等事宜，同国际货币基金组织、布雷顿森林机构、世界银行等开展合作。[③]由此及彼，有理由通过WTO和多利益相关方组织的合作追求数据跨境流动规制的更大一致性。其二，国际贸易与互联网领域的跨部门合作正在进行。如前所述，WTO电子商务诸边谈判业已认可适用风险管理最佳实践应对网络安全威胁。其三，贸易专家参加互联网治理论坛等开放式论坛的意愿有所增强。以2018年互联网治理论坛为例，其“数字包容性与可及性”专题会议涉及如何在规制数据跨境流动时协调贸易与非贸易价值。[④]

但是，满足多利益相关方诉求不等于推行多利益相关方模式。郭丰等（2017）指出，“它（多利益相关方机制）同样具有‘非中性’的特征”，其指代互联网名称与数字地址分配机构（ICANN）的多利益相关方模式。ICANN在维护全球互联网稳定上的成功令其成为典型互联网治理平台，但后移转时代[⑤]的ICANN对国际社会具有何种程度的代表性仍不明了。至少可确定的是，强化美国特权、维护网络霸权等批评反映出ICANN的多利益相关方模式具有非中性特征（Carr，2015）。这也反向突出WTO选择多利益相关方组织作为合作对象时的应然观念，即合作对象限于公正参与全球互联网治理的多利益相关方组织，如以构建网络空间命运共同体为宗旨的世界互联网大会。

2. 由互联网安全到数字信任

由于隐私安全是互联网安全子项中的最高级安全形态，因而实现隐私安全有助于使用户信任网

① “缔约方/成员应在受管辖主体从事商业活动时允许以电子方式跨境传输信息，但法律、法规另有规定除外”。参见：WTO Electronic Commerce Negotiations Text, INF/ECOM/62, 15 November 2023: D.1. para. 2,5.

② Internet Society, Internet Society Issues Paper on Intellectual Property on the Internet, 13 June 2013.

③ The General Agreement on Tariffs and Trade 1994, Article 15(1); Declaration on the Contribution of the World Trade Organization to Achieving Greater Coherence in Global Economic Policymaking, para.5; The B-READY Methodology Handbook, Chapter 7.

④ IGF, IGF 2018 Reports, 2018.

⑤ 后移转时代是指，自2016年10月1日起，ICANN的职能管理权从美国政府移交至全球互联网社区。详见：Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends. (2016-10-01)[2026-01-15]. https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en.

络和数字服务，从而促进将网络用于商业或其他目的。可见，数字技术已参与到信任关系中，成为影响信任建构的主体因素（张成岗和阿柔娜，2024），数字信任的概念应运而生。就概念界定而言，首先需要从信任主体的角度认识技术信任。用户更为信任的是开放网络而非封闭网络，因为后者一般由政府授权或由特定公司运营，可在其中轻松实现监控而致用户隐私易受侵犯，这也揭示出互联网开放和互联网安全的对立统一关系。其次，需要将技术信任扎根于特定应用场景。“和数字贸易相比，贸易数字化是一个过程，是数字化和外贸结合的应用场景”（邵宏华，2022），在该场景中，数字信任具化为对数字服务提供者和消费者间关系、互动、交易公正性的信心。

在WTO法中贯彻数字信任原则，将反向要求WTO成员保障用户数据隐私，保护消费者免受欺诈交易、网络攻击。值得肯定的是，GATS第14条中的正当公共政策目标与上述数字信任的进阶要求具有重合性。但就实现方式而言，GATS等WTO现行法律囿于间接促进数字信任，即授权WTO成员适用国内监管措施维护对相关政策目标正当性的信赖。其实，WTO有能力在促进数字信任上发挥更为积极的作用。WTO谈判和决策机制也应成为就数字贸易关涉的个人数据隐私、线上消费者保护、网络安全等问题谋求国际协调与合作的有用桥梁，如此才能通过“促进可信赖的信息关系”更好塑造“可持续发展的数字化未来”（Richards & Hartzog，2017）。当然，全球社会休戚与共的共生关系决定WTO的单方努力不足以确保数字信任。换言之，数字信任适合成为一项国际共识性原则。

需澄清的是，数字信任原则不同于日本前首相安倍晋三首倡的基于信任的数据自由流动（data free flow with trust, DFFT），二者对数据本地化的容忍度不同。DFFT要求排除“在本国境内存储数据”等数据本地化措施的干预，[①]而数字信任原则为WTO成员例外适用数据本地化措施提供豁免理由。事实上，纵使同为规避数据本地化措施滥用的方法，例外情形下的双重测试比全面禁止更加中庸，有利于在数字地缘政治战略竞争中凝聚最大共识。从WTO电子商务诸边谈判的提案来看，无论融合GATT第20条和GATS第14条，抑或删除GATS第14条第d、e项，[②]皆将继续支持适用一般例外条款检验数据本地化措施，从而表明正当公共政策目标的说明性清单可作为数字信任原则的履行依据。

（二）规则完善：以多维协作为实质精神

1. 推动个人数据隐私的法治统筹

单凭一般例外条款保障个人数据隐私并不足够，WTO肩负统筹国际国内双层法治体系的现实任务。第一个子任务是在国际礼让的影响下锚定WTO法的内向化使命，“数据来源国不会接受对其隐私保护权的片面限制”（Mattoo & Meltzer，2018），源自对他国法律的礼让须以不损害本国及其国民权益为限。迫于个人数据隐私法律单边发展的不平衡，以及双边和区域贸易安排往往服务于推广发达经济体的监管偏好，WTO法理当承担就个人数据隐私法律法源作出基本规定的内向化使命。一个棘手的问题是，何种法律具备成为国际法法源的资格？

续前所论，美国、欧盟、澳大利亚的WTO电子商务诸边谈判提案，实际上与他们主导的自由贸易协定遵循同一价值观。譬如，《美墨加协定》（United States–Mexico–Canada Agreement）第19.8条第2款规定，“缔约方制定个人信息保护法律框架时，应参照《亚太经合组织隐私框

① World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, 2020.
② WTO Electronic Commerce Negotiations Text, INF/ECOM/62, 15 November 2023: Scope and General Provisions para. 6.

架》、2013年OECD《关于隐私保护和个人数据跨境流动指南的理事会建议》等国际机构的原则和准则”，该项引致条款的争议在于作为渊源的特定国际标准过于宽松（Greenleaf，2009）。同理，在宪法视野下加强隐私保护的欧盟自然反对贯彻消费者合同法进路的美国提案。而《欧韩自由贸易协定》（EU-South Korea Free Trade Agreement）第7.48条第2款仅规定，“缔约方同意电子商务的发展必须完全符合数据保护的国际标准”。该项引致条款与欧盟提案异曲同工，二者不顾缔约方的贸易承诺而全权授权其选择渊源，弊病在于增加产生变相数据保护主义措施的机会。《秘澳自由贸易协定》（Peru-Australia Free Trade Agreement）第13.8条第2款则规定，“缔约方应采用或维持用于保护电子商务用户个人信息的法律框架，其在制定时应参照相关国际机构的原则和准则”，该项引致条款与澳大利亚的提案均在一般合规的限度内保持授权限制的开放性，好处在于包容非任意和非歧视前提下的法律创新，以致不必就法源冲突组织针对性谈判。因此，笔者建议WTO法采纳这一介于欧美方案间的折中提案。

第二个子任务是挖掘WTO推动成员间不同个人数据隐私法律衔接的潜力。一方面，这需要依靠WTO的自主努力。一个前车之鉴是亚太经合组织的跨境隐私规则体系（CBPRs），其虽旨在“减少信息流动障碍、加强消费者隐私保护和提升区域间数据隐私制度的互操作性”，[①]但存在实施进展缓慢、束缚一国主权、偏重大国利益等局限。另一方面，这需要依靠WTO与其他国际组织、多利益相关方组织的共同合作。全球隐私大会、全球隐私执法网络、国际隐私专家协会等国际组织皆为保障个人数据隐私做出实质贡献，WTO可与他们在制定数据隐私标准、开展跨境隐私执法、举办专题会议等事宜上进行合作。多利益相关方组织在非正式制定和动态制定有关互联网政策问题的技术标准上颇有经验，为WTO将多利益相关方组织纳为合作对象提供必要性。

2. 厘清线上消费者信任模型

经济学上将信任分为算计性信任、个人信任与制度信任（威廉姆森，2016），后两者由人际互动形成或延伸而实在影响消费者维权效果，可随之确定线上消费者保护国际造法的双重维度。其中，个人信任是源自社会关系的非正式制度安排。鉴于其供给的非正式激励对软法实践的依赖性，理当创设并反复适用以国际合作为要旨的维权监管习惯。申言之，须区分国际公私合作和国际公共合作的监管习惯，前者对私营部门、民间消费者保护组织、行政性消费者保护机构等利益相关方产生效力，后者则对WTO和其他政府间组织产生效力。WTO可继续以做出实质贡献为标准选择合作对象，合作事宜诸如出台政策指引文件、部署联合执法行动等。以软法为先导便于动态调整上述监管习惯的细节要求，使之伺机变为WTO法自动接受的硬法规则。

制度信任是维系社会关系的正式制度安排，WTO电子商务诸边谈判提案可依托其强制力量成为WTO法的硬法规则。目前，源代码和算法开放禁令的适用范围和豁免仍有争鸣。以有无禁令适用除外为中心，加拿大、日本、韩国、墨西哥、秘鲁、乌克兰、新加坡、英国和沙特阿拉伯支持强制性义务，即不得将“要求转让或访问个人软件源代码或其表现的算法”充作“在其境内进口、分发、出售或使用该软件或含该软件的产品”的条件。而欧盟、中国建议补充“在商业基础上自愿转让或授权访问源代码”作为不适用禁止开放源代码和算法的除外情形。[②]以禁令的适用豁免情况为中心，第一种意见是豁免事由包括在“遵守防止未经授权披露的保障措施”条件下的“调查、检查、审查、执法行动或司法程序”，以及“根据缔约方/成员法律实行或执行救济措施”；第二种

① 2011 Leaders' Declaration. (2011-11-04)[2026-01-15]. https://www.apec.org/Meeting-Papers/Leaders-Declarations/2011/2011_aelm.
② WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023, C.3. (1)(2); C.3. (1)(3).

意见是豁免事由包括“执法行动”和出于合规目的的“调查、检查、审查或司法程序”。[①]

本文认为，措辞广泛的源代码和算法开放禁令会在多边范围内产生矛盾。一则，因为其有违数字服务质量保障的需求，数字服务背后的算法和技术代码有可能是歧视性的，抑或特许某些国家或团体未经授权访问数据。二则，因为其无益于改善信息技术的“巴尔干化”。在供应链全球化之际，确保IT设备和IT升级的完整性仍需设立区域审查站检查所有提供者的随机硬件或软件样本。[②]另外，源代码审查不等于强制以技术转让换取市场准入。西方普遍认为，IBM和微软同意中国政府进行源代码审查，标志着“中国将重启强制向中国企业转让技术的行动的大门”（Moran，2015）。然而，将遵从商业自愿原则的源代码审查视为强制技术转让实属偷换概念，且拒绝开放源代码的行为可招致扼杀创新、减少消费者选择等后果。[③]就禁令豁免而言，第一种意见的合理性在于，其对豁免事由的拓展并未突破比例原则的限制，可在最大限度内服务于数据安全流动的价值取向。

3. 切实探索网络空间治理边界

WTO电子商务诸边谈判看似就网络空间治理问题达成结论，实则仍有不少讨论空间。首先，在WTO法框架下，适用网络安全治理准则的可能问题耐人寻味。问题一是以风险为本准则适用依据的可行性。Mitchell和Mishra（2019）认为，在WTO框架内适用风险管理最佳实践“更困难和不可取”。然而，诸多实务人士则肯定了存在网络安全风险管理的最佳实践（Boehm et.al，2019；Knowles，2024）。问题二是合作最优准则适用效果的能动性。强制WTO成员间就网络安全监管进行国际合作并不贸然，WTO贸易与环境委员会是WTO成员就与贸易有关的环境政策加强国际合作的产物，应明确要求WTO成员和多利益相关方组织开展国际合作。其实，WTO已然突破不与多利益相关方组织联络的藩篱，其在2017年就已协同世界电子贸易平台推出了《世界电子贸易平台倡议》（Electronic World Trade Platform Initiative）。一言以蔽之，拟定网络安全治理准则的合理性确有提升空间。

其次，在WTO法中主张网络主权、数据主权的正当性有待验证。由中国学者联合发布的《网络主权：理论与实践（2.0版）》[④]指出，“倡导与实践网络主权，并不否定网络空间的互联互通性、必要秩序基础上的信息自由流动性和创新性”，这种开放的主权观念证明互联网的开放性和国家主权的现实性的矛盾并非不可调和。同理，如下论说不足以推翻数据主权的理论基础：第一，数据全球公域说以“为广泛的独立利益相关方提供数据访问”为意旨（Shkabatur，2017），实则是美国立足商业优先信仰树立数据霸权地位的新表现，忽视了数据是承载人格利益、商业利益、国家利益等多元利益的动态概念；第二，数据自由流动说断定“数据主权政策是数据保护主义的一种形式”（Elms，2021），其输送的新自由主义意识形态隐含西方数据霸权的工具理性，即在逐利动机的驱使下追求数据资本的完全市场化，最终方便大型跨国公司的寡头游戏侵蚀他国数据主权。总而言之，网络主权和数据主权皆有资格作为正当公共政策目标。

最后，由WTO法调整网络主权若干具体问题的可行性值得商榷。兹认为，WTO应对是否改变网络主权治理的既有法律格局持谨慎态度。比如，虽然“各成员因理论、法律及文化差异而倾向自行规范互联网”（May et al.，2004），导致由WTO法确定跨境数据在线内容审查的通行模式不切实际，但WTO谈判和决策机制可为就有关法律适用达成共同理解保驾护航。再如，巴西曾建议

① WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023, C.3. (1)(4).
② PIIE, Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers, 2013.
③ Commission Decision of 24 May 2004 relating to a proceeding pursuant to Article 82 of the EC Treaty and Article 54 of the EEA Agreement against Microsoft Corporation (Case COMP/C-3/37.792 — Microsoft), 2007/53/EC, 6 Feb. 2007.
④ 网络主权:理论与实践（2.0版)[EB/OL].(2020-10-15)[2025-10-15]. https://cn.wicinternet.org/2020-10/15/content_36225577.htm

“不得以缺乏国家管辖权为由拒绝访问执行国内法所必需的信息和数据”，且所有数字服务供应商向监管机构提供数据以遵守国内法，不论数据位于境内或境外。[①]该提案同《网络犯罪公约》第32条较为相似，二者欲确立以部分让渡属地管辖权为互惠条件的数据跨境调取多边合作机制，区别在于后者另区分境外公开和非公开数据的调取条件。《网络犯罪公约》第32条尚且遭遇适用瓶颈，[②]遑论更为粗放地处置数据跨境调取管辖冲突的巴西提案，WTO电子商务诸边谈判后续未予采纳有迹可循。

4. 强化执行特殊与差别待遇

作为以数据本地化措施贯彻数字产业政策的发展中成员代表，印度、南非以削弱贸易政策空间为由拒绝参与电子商务诸边谈判。然而，数字产业政策的单边制约因素无视内部竞争能力对搞活数字初创企业的决定作用，将阻碍发展中成员以经济可持续性的方式实现数字发展权。因此，不宜对发展中成员保留电子传输关税壁垒的权宜之计予以让步。相较而言，中国首倡的电子传输关税禁令暂时化方案受阻的可能性最小，其便于寻求最大程度地凝聚跨境电子商务合作共识。当然，不宜完全依赖发展中成员的单方进步弥合南北数字鸿沟，WTO法也要保障发展中及最不发达成员的特殊与差别待遇（S&DT）。

一个前置问题是，S&DT是否具有有效性？疑点一为S&DT能否帮助发展中成员履行贸易承诺。譬如，美国质疑某些发展中成员通过自我宣示不当谋利，“一些最富有的WTO成员……坚持被视为发展中成员，并可酌情适用S&DT条款。”[③]疑点二为S&DT能否真正维护发展中成员利益。一项访谈调查显示，发展中国家的利益相关方大多提及“传统的S&DT在电子商务领域并不足够”（Angeles et al.，2021）。由此引出以下反驳或启示：一是发达成员不能忽视S&DT的实质不平等性，中国等部分发展中成员不同程度地放弃和丧失S&DT；二是发展中成员期待S&DT支持其把握数字商业机会，而非单纯帮助其履行贸易承诺。

在WTO电子商务诸边谈判中，科特迪瓦为有关S&DT条款的最新提案贡献了智慧。简言之，该提案融合《贸易便利化协定》（Trade Facilitation Agreement, TFA）第二部分与电子商务便利融资机制（E-Commerce Facilitation Funding Facility, ECFFF），以期WTO法从以自由化为中心转向以发展为中心。其中，TFA基于逐项处理的办法创设兼具系统性和灵活性的S&DT机制，发展中和最不发达成员在提交通知的前提下自主决定A、B、C三类承诺的履行时间，以及取得C类承诺履行能力所需的能力建设和技术援助。[④]ECFFF通过“管理与公开”支持WTO贸易便利化委员会协助发展中及最不发达成员实施TFA，优先开展“负责捐款方案”“回应发展中及最不发达成员关于能力建设和技术援助的请求”“参与附件D并同发展伙伴互动”“维护网站”等活动。[⑤]

诚然，TFA接受贸易承诺的分阶段履行，将令受惠成员在受到完全约束前有更多时间启动内部监管改革。ECFFF征集强制性捐款的权力，更将令履行C类承诺的受惠成员获得特别的物质支持。根据TFA数据库最新数据，完成TFA国内核准程序的发展中成员共90名、最不发达成员共35名，宣布同援助成员达成能力建设和技术援助安排的发展中成员、最不发达成员各16名，[⑥]但该数字与认

① Joint Statement Initiative on E-commerce, Communication from Brazil, INF/ECOM/17, 25 March 2019, Section XIII.
② Cybercrime Convention Committee, Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY, 2014.
③ WTO General Council, An Undifferentiated WTO: Self-declared Development Status Risks Institutional Irrelevance, Communication from US, WT/GC/W/757, 16 January 2019, para.4.4.
④ WTO Electronic Commerce Negotiations Text, INF/ECOM/62/Rev.5, 15 November 2023:D.5. para.1.
⑤ 附件D指向《多哈工作计划》的贸易便利化谈判。
⑥ 数据来源于TFA 数据库，https://tfadatabase.org/en/groupings/.

捐用于贸易便利化援助的资金调集数额不甚匹配。据估计，2006~2019年约有4090亿美元用于“帮助发展中国家建设贸易能力”。[①]扭转援助进展滞后局面的着力点是防止援助成员凌驾于受惠成员之上。对此，建议WTO引入公私伙伴关系协助实施TFA并就此进行预先规划，既有经验表明其可支持受惠成员通过两种方式实现规划目标，即将贸易便利化改革纳入国家发展计划[②]、绘制贸易便利化的阶段性路线图。[③]

参考文献

[1] 翟志勇.数据主权的兴起及其双重属性[J].中国法律评论,2018(6):196–202.
[2] 郭丰,刘碧琦,赵旭.多利益相关方机制国际实践研究[J].汕头大学学报(人文社会科学版),2017(9):53–64.
[3] 贺小勇,刘真宇.源代码条款的碎片化困境及中国因应[J].上海对外经贸大学学报,2026 (1):82–97.
[4] 姜伟,龙卫球.数字法学原理[M].北京:人民法院出版社,2023.
[5] 刘晗,叶开儒.网络主权的分层法律形态[J].华东政法大学学报,2020(4):67–82.
[6] 刘影.世界贸易组织改革进程中数据跨境流动的规制与完善[J].知识产权,2023(4):108–126.
[7] 马光,卜小翠.自由贸易协定金融信息传送规则构建[J].财经法学,2022(6):111–124.
[8] 彭岳.跨境数据隐私保护的贸易法维度[J].法律适用,2022(6):16–28.
[9] 邵宏华.贸易数字化:打造贸易新动能新业态新模式[M].北京:机械工业出版社,2022.
[10] 宋云博.DEPA个人信息跨境流动的规则检视与中国法调适[J].法律科学,2024(1):135–144.
[11] 谭观福.数字贸易中跨境数据流动的国际法规制[J].比较法研究,2022(3):169–185.
[12] 威廉姆森.治理机制[M].石烁,译.北京:机械工业出版社,2016.
[13] 许多奇.治理跨境数据流动的贸易规则体系构建[J].行政法学研究,2022(4):50–60.
[14] 张成岗,阿柔娜.智慧治理场景下的数字信任构建:机制、挑战及趋向[J].社会治理,2024(1):10–19.
[15] 张晓君,屈晓濛.RCEP数据跨境流动例外条款与中国因应[J].政法论丛,2022(3):109–119.
[16] Aaronson, S. A., *Handbook of the International Political Economy of Trade*, Cheltenham: Edward Elgar, 2014.
[17] Angeles, F., R. Roy, and Y. Yulia, Shifting from Consensus Decision–making to Joint Statement Initiatives: Opportunities and Challenges, WTO Capstone Project Paper, April 2021.
[18] Badran, M. F.,“Economic Impact of Data Localization in Five Selected African Countries”, *Digital Policy, Regulation and Governance*, 2018, 20(4): 337–357.
[19] Ben–Shahar, O., and L. S. Levitz,“Contracting Over Privacy: Introduction”, *Journal of Legal Studies*, 2017, 45(3): S1–S12.
[20] Boehm, J., N. Curcio, P. Merrath, et al., The Risk–Based Approach to Cybersecurity. (2019–10–08)[2026–01–15]. https://www.mckinsey.com/capabilities/risk–and–resilience/our–insights/the–risk–based–approach–to–cybersecurity.
[21] Box, S., Internet Openness and Fragmentation: Toward Measuring the Economic Effects, GCIG Paper, No. 36, May 2016.
[22] Carr, M.,“Power Plays in Global Internet Governance”, *Journal of International Studies*, 2015, 43(2): 640–659.
[23] Chander, A., and P. U. Le,“Data Nationalism”, *Emory Law Journal*, 2015, 64(3): 677–739.
[24] Córdoba, S. F., Trade and the MDGs: How Trade Can Help Developing Countries Eradicate Poverty. (2008–03–01)[2026–01–10]. https://www.un.org/en/chronicle/article/trade–and–mdgs–how–trade–can–help–developing–countries–eradicate–poverty.
[25] Drake, J. W., G. V. Cerf, and W. Kleinwächter, Internet Fragmentation: An Overview, World Economic Forum Future of the Internet Initiative White Paper, January 2016.
[26] Elms, D., Digital Sovereignty: Protectionism or Autonomy?. (2021–09–28)[2026–01–15]. https://www.hinrichfoundation.com/research/wp/digital/digital–sovereignty–protectionism–or–autonomy/.
[27] Greenleaf, G.,“Five Years of the APEC Privacy Framework: Failure or Promise?”, *Computer Law & Security Review*, 2009, 25(1): 28–43.
[28] Hirsch, D. D.,“In Search of the Holy Grail: Achieving Global Privacy Rules through Sector–based Codes of Conduct”, *Ohio State Law Journal*, 2013, 74(6): 1029–1070.

① OECD, Aid for Trade at a Glance 2019: Economic Diversification and Empowerment, 2019.
② Republic of South Sudan, Developing Capacities for Trade Integration and Economic Diversification, 2014.
③ UNCTAD, Roadmap for Building a Trade Single Window, 2023.

[29] Knowles, M., Cybersecurity Risk Management: Frameworks, Plans, & Best Practices. (2024-01-22)[2026-01-15]. https://hyperproof.io/resource/cybersecurity-risk-management-process/.
[30] Kokott, J., and C. Sobotta, "The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, 2013, 3(4): 222-228.
[31] Kuner, C., *Transborder Data Flows and Data Privacy Law*, Oxford: Oxford University Press, 2013.
[32] Mattoo, A., and J. P. Meltzer, "International Data Flows and Privacy: The Conflict and Its Resolution", *Journal of International Economic Law*, 2018, 21(4): 769-789.
[33] May, B. E., J. C. V. Chen, and K. W. Wen, "The Differences of Regulatory Models and the Internet Regulation in the European Union and the United States", *Information & Communications Technology Law*, 2004, 13(3): 259-272.
[34] Mishra, N., "Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation", *World Trade Review*, 2020, 19(3): 341-364.
[35] Mitchell, A. D., and N. Mishra, "Regulating Cross-border Data Flows in a Data-Driven World: How WTO Law Can Contribute", *Journal of International Economic Law*, 2019, 22(3): 389-416.
[36] Moran, T. H., Should US Tech Companies Share Their "Source Code" with China?. (2015-10-28)[2025-11-15]. https://www.piie.com/blogs/china-economic-watch/should-us-tech-companies-share-their-source-code-china.
[37] Palfrey, J., and U. Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems*, New York: Basic Books, 2012.
[38] Ramesh, V., Data Protection Principles around the World. (2018-10-08)[2026-01-15]. https://voelkerrechtsblog.org/de/data-protection-principles-around-the-world/.
[39] Richards, N., and W. Hartzog, "Privacy's Trust Gap: A Review", *Yale Law Journal*, 2017, 126(4): 1180-1224.
[40] Shkabatur, J., "The Global Commons of Data", *Stanford Technology Law Review*, 2017, 22: 354-411.
[41] Waz, J., and P. Weiser, "Internet Governance: The Role of Multistakeholder Organizations", *Journal on Telecommunications and High Technology Law*, 2012, 10(2): 331-350.
[42] Winn, J. K., and M. Webber, "The Impact of EU Unfair Contract Terms Law on U.S. Business-to-Consumer Internet Merchants", *The Business Lawyer*, 2006, 62(1): 209-228.
[43] Zhang, Q., and A. Mitchell, "Data Localization and the National Treatment Obligation in International Investment Treaties", *World Trade Review*, 2021, 21(4):1-20.

【作者简介】任妍姣：中央财经大学法学院博士研究生。研究方向：数据法、金融法。

Regulation of Cross-border Data Flows under the WTO Law

REN Yan-jiao

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

Abstract: The regulation of cross-border data flows constitutes a fundamental issue in the governance of global digital trade. WTO law stands out as the most appropriate framework for reconciling the disparate norms on cross-border data flowing across jurisdictions. The regulatory orientations of cross-border data flows fall into two categories: free data flow and secure data flow, while the regulatory approaches include two types of data localization measures, namely strict data localization requirements and conditional data flow mechanisms. Policy objectives such as data privacy protection, online consumer protection, cyberspace governance, and digital industrial policy can serve as the primary basis for judging the compatibility between WTO law and data localization measures. Normatively speaking, WTO law ought to encompass data localization measures that serve legitimate public policy objectives; further, it should refine its regulatory rules by closely aligning with the respective policy objectives underlying these measures, guided by such principles as hybrid regulation and digital trust.

Keywords: digital trade; cross-border data flow; WTO; GATS; joint statement initiative on e-commerce

（责任编辑：马莹）