数字贸易中跨境数据流动的国际法规制

谭观福*

摘　要：跨境数据流动是进行数字贸易的前提，但各国对于跨境数据流动的规制分歧难以弥合。WTO框架下的一些安排推动了数字贸易基础设施的贸易自由化，从而促进了跨境数据流动。新近FTA通过确立“原则+例外”的规制模式为跨境数据流动构建了相对自由的法律框架；FTA还针对特殊数据规定了专门规则，包括个人数据保护和政府数据开放规则。WTO成员可以在WTO中为数据保护达成一个基本框架，成员还可以依据GATS第7条通过互认机制来协调个人数据保护标准，并加强与APEC或OECD的合作。我国对跨境数据流动的规制坚持了以风险为基础的思路，初步形成了分级分类管理的顶层设计框架。我国的国内规制措施已经与国际接轨，但还应进一步完善有关立法和标准，并加强对外协调。

关键词：数字贸易；跨境数据流动；国际法；WTO；FTA；规制

跨境数据〔1〕流动通常意味着对跨越国界的数据进行读取、存储和处理的活动，包括数据的出境和入境两个方面。对数据入境的规制主要涉及互联网审查，包括互联网屏蔽和互联网过滤审查。本文探讨的跨境数据流动，主要指数据出境。〔2〕跨境流动的数据类型不同，需要法律予以调整的问题也不同。〔3〕商业数据的跨境流动通常涉及知识产权保护，个人数据涉及隐私保护，而政府数据涉及公共安全。

跨境数据流动是进行数字贸易的前提，但各国对于跨境数据流动的规制持有不同立场。形成于前互联网时代的世界贸易组织（以下简称“WTO”）没有规制跨境数据流动的专门规则，在过去的数十年中，自由贸易协定（以下简称“FTA”）成为了讨论数据治理问题的中心场所。FTA帮助克服了WTO多边体制的一些问题和矛盾，为数字贸易新议题制定了新规则，塑造了跨境数据流动的监管环境。〔4〕《全面与进步跨太平洋伙伴关系协定》（以下简称“CPTPP”）和《美国—墨西哥—加拿大协定》（以下简称“USMCA”）的电子商务/数字贸易章中的跨境数据流动规则代表了FTA数据治理规则的最新发展。

我国作为最大的跨境电子商务市场，在保障数据流动方面存在重大利益，因而不宜回避跨境数据流动问题。2021年以来，我国国内数据安全领域的立法进展迅速，跨境数据流动规则框架逐渐清晰。《中华人民共和国数据安全法》第7条明确了我国对数据流动规制的基本立场，即“保障数据依法有序自由流动”。我国于2020年11月签署的《区域全面经济伙伴关系协定》（以下简称“RCEP”）中的电子商务章

---

*　中国社会科学院国际法研究所助理研究员，《国际法研究》编辑部编辑，法学博士。本文系2020年度国家社会科学基金重大项目“中国特色自由贸易港国际法治研究”（批准号：20&ZD205）的阶段性研究成果。

〔1〕　为研究便利，本文不严格区分数据和信息，统一用数据来指代。

〔2〕　有关数据出境的概念及内涵，可参见全国信息安全标准化技术委员会发布的《信息安全技术 数据出境安全评估指南（征求意见稿）》第3.7条。

〔3〕　李思羽：《数据跨境流动规制的演进与对策》，载《信息安全与通信保密》2016年第1期，第97页。

〔4〕　Mira Burri, *The Regulation of Data Flows through Trade Agreements*, 48 Georgetown Journal of International Law 407, 407 (2017).

相较于之前签订FTA中的电子商务章新增了有关跨境数据流动的条款（第12.14条和第12.15条），总体上为跨境数据流动规定了“原则+例外”的规制模式。该条款借鉴了CPTPP中的跨境数据流动规则。随着数据监管方面的国内立法逐渐完善，我国在跨境数据流动问题上的立场渐趋开放，开始对接国际标准。我国于2021年9月正式申请加入CPTPP，于2021年11月申请加入《数字经济伙伴关系协定》（以下简称“DEPA”）。本文将从WTO规则出发，结合新近国际经贸协定中的数字贸易规则，探讨跨境数据流动与数字贸易的关联及规制分歧，国际经贸协定对数字贸易中跨境数据流动的规制模式，并在此基础上尝试探讨跨境数据流动规则的协调路径，提出我国立场。

一、跨境数据流动与数字贸易的关联及规制分歧

部分国家认为，跨境数据流动不属于贸易问题，不应通过国际经贸协定制定规则。之所以对跨境数据流动采取回避立场，是因为相关国家在国内基础设施和制度建设上还不完善。[5]数字贸易的一大特点是依赖于数据传输，跨境数据流动是数字贸易得以开展的前提，国际经贸协定可以成为规制跨境数据流动的规则框架。不同国家基于一系列国内政策目标的考量，对跨境数据流动的规制持有不同立场。对跨境数据流动的规制措施直接影响数字贸易的发展，不合理的限制措施（如数据本地化措施）将构成数字贸易壁垒。因此，跨境数据流动问题理应成为数字贸易规制中的重要议题。

（一）跨境数据流动与数字贸易的关联

人们通过挖掘数据来获取信息、指导实践，数据成为了一种重要的生产要素。跨境数据流动对于数字贸易至关重要，是进行数字贸易的前提。企业和客户依赖不间断的数据流动来交付数字产品和数字服务，甚至传统制造业和物流行业也都依靠数据自由流动来优化其运营并提高其生产力。跨境数据流动使企业能够实时沟通客户订单，作出有关生产计划的快速决策，并根据消费者需求的变化迅速调整设计。[6]从石油和天然气公司到制造业和零售公司的众多传统产业，都依赖于其在全球各地的数据来进行日常决策。现代经济中几乎每个部门的公司都依靠数据驱动的创新来开展业务，各种规模的公司都在共享数据创新的好处。如今，对于域外拥有业务、供应商或客户的公司而言，可能没有一家公司不依赖于跨境数据传输，无论是为了获得竞争优势还是作为正常业务运营的一部分。[7]

既然跨境数据流动是进行数字贸易的前提，那么，跨境数据流动议题是否应被纳入国际经贸协定？在20世纪80年代，包括美国和日本在内的一些国家的官员希望在贸易协定中纳入规制数据自由流动的条款。但其他国家出于主权的考虑，希望保留对跨境数据流动进行限制的能力，以保护隐私或国家安全。[8]当这些官员无法形成一致意见时，经济合作与发展组织（以下简称“OECD”）起草了自愿性原则，以平衡隐私、安全和数据自由流动。[9]随着数字贸易、移动电话和云技术的兴起，跨境数据流动问题再次引起广泛争议。

有学者认为，贸易决策过程与互联网治理过程完全不同，考虑到WTO和FTA等国际经贸规则谈判的保密性、缓慢、自上而下和封闭的特点，国际经贸协定并非规制跨境数据流动的主要场所。此外，国际经贸协定也不可能为隐私保护规定全面框架，因而也无权敦促缔约方为保护这些权利提供有利的监管环

〔5〕 徐程锦：《国际经贸协定中网络空间治理议题的新发展》，载《区域与全球发展》2018年第3期，第93—94页。

〔6〕 Joshua Paul Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 2 Asia & the Pacific Policy Studies 90, 92 (2015).

〔7〕 Daniel Castro & Alan Mcquinn, *Cross-Border Data Flows Enable Growth in All Industries*, The Information Technology and Innovation Foundation 1, 1–2 (2015).

〔8〕 Susan Ariel Aaronson, *Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security*, 14 World Trade Review 671, 672 (2015).

〔9〕 OECD Council, Recommendation on Principles for Internet Policy Making, December 2011.

境。因此,贸易谈判的外交官不能轻易地在贸易协定中纳入诸如数据流动与隐私保护和监管之间关系的条款。〔10〕

国际经贸协定旨在为国际经贸治理提供一套规范体系,不可能为非贸易关切(如公共道德和公共秩序、隐私保护、国家安全)提供全面保护。很多国家基于国内政策目标而采取的贸易限制措施很可能构成贸易壁垒,因此,国际经贸协定需要对贸易价值和非贸易价值的协调作出回应。国际经贸协定成为了价值协调的工具,当贸易价值和非贸易价值产生冲突时,非贸易价值优先,但需满足一定条件。而对于如何保障非贸易价值,最终还是回到“上帝的归上帝,恺撒的归恺撒”。鉴于跨境数据流动对数字贸易的特殊重要性,而限制跨境数据流动的措施又很可能构成贸易壁垒,跨境数据流动议题应被纳入国际经贸协定中。技术发展带来的跨境数据流动问题成为贸易自由化和贸易管制的对象,导致传统规则的更新、修订或新规则的创制。〔11〕

(二)跨境数据流动的规制分歧

各国对于跨境数据流动的规制持有不同立场,各国的跨境数据流动政策在出台目的、适用范围和严格程度方面均存在较大差异,分歧难以弥合。美国未在法律层面对数据跨境传输作出限制性规定,对数据流动的规制长期依赖行业自律机制。美国在2018年4月向WTO提交的电子商务文件特别提到跨境数据自由流动的主张,指出:“贸易规则应当确保消费者和公司都能跨境移动数据而不受任意或歧视性限制;贸易规则应当确保公司无需在其服务的每个司法管辖区中建立或使用独特的、资本密集型的数字基础设施,从而可以更好地为客户提供服务;贸易规则,包括确保访问网络的规则,应当确保政府不会任意屏蔽或过滤在线内容,也不会要求互联网中间商这样做。”〔12〕

美国之所以坚持跨境数据自由流动的主张,一方面是因为美国的互联网企业具有先发和主导优势,另一方面是因为美国能够对本国数据实现有效管控。〔13〕日本也对跨境数据流动持有相同立场,其在2018年4月向WTO提交的电子商务文件也主张跨境数据自由流动和禁止数据本地化。〔14〕

欧盟对完全的跨境数据自由流动持保留态度,认为数据应该在安全的前提下流动,强调数据的监管和保护。个人数据的流动关涉个人隐私,个人隐私在欧洲被视为一项至关重要的人权。在跨境数据流动问题上,欧盟极力主张国际统一标准模式。〔15〕2016年4月,欧洲议会通过了《通用数据保护条例》(以下简称“GDPR”),该条例堪称是史上最严厉、最为翔实的一部保护用户个人数据安全的法律,把个人信息保护和监管提高到了一个前所未有的高度。2018年10月,欧洲议会通过了《非个人数据自由流动条例》,旨在消除欧盟内的数据本地化措施,促进非个人数据的自由流动。〔16〕欧盟在2019年4月向WTO提交的电子商务提案主张,在坚持保护个人数据和隐私的前提下,要求限制数据本地化措施,积极推动跨境

〔10〕 Susan Ariel Aaronson, *Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security*, 14 World Trade Review 671, 678–679 (2015).

〔11〕 韩立余:《自由贸易协定新议题辨析》,载《国际法研究》2015年第5期,第81页。

〔12〕 General Council, Joint Statement on Electronic Commerce, Communication from the United States, JOB/GC/178, 12 April 2018, para.2.1.

〔13〕 杨莜敏:《全球跨境数据流动国际规则及立法趋势观察和思考》,载CAICT互联网法律研究中心网站, https://www.secrss.com/articles/13744,访问时间:2022年4月25日。

〔14〕 General Council, Joint Statement on Electronic Commerce Initiative, Proposal for the Exploratory Work by Japan, JOB/GC/177, 12 April 2018, paras. 3.6–3.8.

〔15〕 彭岳:《贸易规制视域下数据隐私保护的冲突与解决》,载《比较法研究》2018年第4期,第187页。

〔16〕 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-personal Data in the European Union.

数据流动。[17]不过,欧盟主张的跨境数据流动规则还是要让位于个人数据保护措施。除欧盟外,还有很多国家都有因保护个人数据而限制跨境数据自由流动的国内立法,如澳大利亚、巴西、法国、印度、俄罗斯等。[18]很多国家的数据保护体系都受到GDPR的影响,GDPR事实上在数据保护模式方面发挥着规则引领作用。

对跨境数据流动的限制除了出于保护个人隐私的目的,还涉及金融、电信、国家安全等领域。对数据流动的限制措施可大致分为以下四类:(1)禁止将数据传输到国外(数据永远不会离开所在国家);(2)本地处理要求(数据可以离开该国,但主要处理必须在本地进行);(3)本地存储要求(数据副本必须存储在本地);(4)有条件的流动制度(数据只能在某些条件下才能被传输到国外,例如数据主体同意)。[19]

有条件的数据流动制度往往是根据保护数据隐私原则实施的,例如要求数据出境前征得数据主体同意的隐私法规,或要求对数据进行评估,达到要求后才允许出境。本地存储要求通常旨在促进执法时访问某些数据(例如记帐数据或元数据的情形)。在这种情况下,只要将数据副本保存在本地,数据就可以自由流出境外。要求在本地处理数据或完全禁止任何数据向境外传输的更严格的措施,通常是基于国家安全的理由。还有其他一些影响跨境数据流动的措施,例如对在线内容的屏蔽和过滤。这些互联网审查措施通常适用于特定网站、在线服务或政治内容,旨在审查某些信息和维护公共秩序,或者在其他情况下旨在保护本地公司。[20]对跨境数据流动的限制一方面有利于国家对数据进行监管,保障其国内政策目标,但另一方面也会限制企业在特定国家中可以进行交易或提供服务的类型,可能构成贸易壁垒。严格限制跨境数据流动也可能导致国内市场被孤立,相关的国内企业难以参与国际竞争。

二、跨境数据流动规制的多边法治环境

WTO没有规制跨境数据流动的专门规则,而通过规范以数据为基础的服务的提供来间接规范数据,例如数据处理和其他计算机服务。但WTO通过推动通信技术服务和信息技术产品的贸易自由化促进了跨境数据流动。

(一)通信技术服务的贸易自由化

通信技术服务的贸易自由化对跨境数据流动具有基础性作用。《服务贸易总协定》(以下简称"GATS")框架内有《基础电信协议》和《关于电信服务的附件》。《基础电信协议》也被称为《〈服务贸易总协定〉第四议定书》,只规定了生效时间等程序性事项,但其后所附的WTO成员关于基础电信的具体承诺减让表和GATS第2条豁免清单,则是该协议的主要内容。[21]《基础电信协议》要求WTO成员在客观公正的基础上非歧视地向其他成员开放国内的基础电信服务市场。《关于电信服务的附件》独立于各成员对电信服务市场作出的具体承诺,重点是要求所有WTO成员保证"以合理和非歧视的条款和

〔17〕 欧盟在提案中提出了四项要求:(a)不得要求使用成员境内的计算设施或网络元件进行数据处理,包括强制使用在成员境内认证或批准的计算设施或网络元件;(b)不得要求在成员境内对数据进行本地化存储或处理;(c)不得禁止在其他成员境内存储或处理数据;(d)不得要求数据的跨境传输取决于在成员境内使用计算设施或网络元件或在成员境内的本地化要求。*See* Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22, 26 April 2019, para. 2.7.1.

〔18〕 UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, April 2016, pp. 43–46.

〔19〕 Martina Francesca Ferracane, *Data Flows and National Security: A Conceptual Framework to Assess Restrictions on Data Flows under GATS Security Exception*, 21 Digital Policy, Regulation and Governance 44, 47 (2019).

〔20〕 Martina Francesca Ferracane, *Data Flows and National Security: A Conceptual Framework to Assess Restrictions on Data Flows under GATS Security Exception*, 21 Digital Policy, Regulation and Governance 44, 47 (2019).

〔21〕 Trade in Service, Fourth Protocol to the General Agreement on Trade in Services, S/L/20, 30 April 1996.

条件”接入和使用其公共电信传输网络和服务。《关于电信服务的附件》规定了服务提供商访问和使用公共电信传输网络和服务的基本权利，但其仅适用于成员已经作出承诺的部门，在很多对数字贸易发展至关重要的部门中承诺有限或没有承诺。[22]为确保《关于电信服务的附件》在各国国内法中得到遵守，以美国为主导的谈判专家提出了《电信服务参考文件》，为电信监管提出了基本的参考原则，其核心是竞争原则。但WTO成员对于《电信服务参考文件》并未达成共识，它没有成为WTO的正式法律文件。

受到《关于电信服务的附件》和《电信服务参考文件》纪律（disciplines）的影响，特别是有关访问和使用公共电信传输网络和服务以及竞争性保障的规定的影响，很多FTA的电子商务/数字贸易章纳入了“为电子商务而接入和使用互联网的原则”，例如《美国—韩国自由贸易协定》（以下简称“《美韩FTA》”）第15.7条。[23]《美韩FTA》第15.7条继承了前述协定中的原则，并将其修改以考虑到数字贸易的特性，其适用范围不仅包括互联网的硬件基础设施，还包括软件环境。该规定所带来的利益不仅扩展到网络提供商，还扩展到应用程序提供商、服务提供商和内容提供商。CPTPP和USMCA也有类似规定。[24]

美国向WTO提交的电子商务文件指出，实现竞争性的电信市场是任何国家克服数字鸿沟必不可少的第一步，《电信服务参考文件》仍准确地描述了进入市场的垫脚石，即多个公司在该市场进行投资并竞争以向消费者提供最佳服务。[25]欧盟特别强调了关于进一步开放电信服务市场的规则和承诺，并主张修改《电信服务参考文件》。[26]如果外国的互联网服务提供商无法访问国内的互联网基础设施，则很难实现自由的跨境数据流动。CPTPP建议其缔约方，允许寻求国际互联网连接的服务提供商在商业基础上与其他缔约方的服务提供商协商费用分摊。[27]

（二）信息技术产品的贸易自由化

跨境数据流动要大规模发展的另一个重要的基本条件是信息传输所必需的硬件设施，因而信息技术产品的贸易自由化对跨境数据流动的发展也有关键作用。《信息技术协定》（以下简称“ITA”）旨在分阶段将信息技术产品的关税削减至零。ITA的最初版本是1996年新加坡部长级会议通过的《关于信息技术产品贸易的部长宣言》，该宣言的产品范围涵盖了大量高技术产品，如自动数据处理设备、半导体制造与测试设备及其部件、计算机、网络设备等。[28]ITA的最终达成在很大程度上与美国信息技术行业施加的压力有关。作为WTO框架下诸边协定的新类型，ITA的成果在最惠国待遇原则的基础上适用于所有成员，每个成员都可以从ITA缔约方的市场准入承诺中受益。

ITA在2015年完成了扩围谈判，达成了《关于扩大信息技术产品贸易的部长宣言》，新增了201项产品。[29]扩围谈判的成功使ITA适应了技术发展的现实，扩围后的ITA涵盖了尖端技术产品，例如医疗磁

---

〔22〕 Farrokh Farrokhnia & Cameron Richards, *E-Commerce Products under the World Trade Organization Agreements: Goods, Services, Both or Neither?* 50 Journal of World Trade 793, 806 (2016).

〔23〕 《美韩FTA》第15.7条规定：“为支持电子商务的发展和增长，缔约各方认识到其领土内的消费者应能够：（a）访问和使用他们选择的服务和数字产品，除非该缔约方的法律禁止；（b）在符合执法机关要求的情况下运行他们所选择的应用程序和服务；（c）将他们选择的设备连接到互联网，前提是此类设备不会危害互联网且未被该缔约方的法律所禁止；以及（d）从网络提供商、应用程序和服务提供商以及内容提供商之间的竞争中受益。”

〔24〕 Art. 14.10 of CPTPP; Art. 19.10 of USMCA.

〔25〕 General Council, Joint Statement on Electronic Commerce, Communication from the United States, JOB/GC/178, 12 April 2018, para. 7.1.

〔26〕 Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22, 26 April 2019, paras. 3.1–3.11; Joint Statement on Electronic Commerce, Communication from the European Union, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce: Revision of Disciplines Relating to Telecommunications Services, INF/ECOM/43, 15 October 2019.

〔27〕 Art. 14.12 of CPTPP.

〔28〕 Ministerial Conference, Ministerial Declaration on Trade in Information Technology Products, WT/MIN (96) /16, 13 December 1996.

〔29〕 Ministerial Conference, Ministerial Declaration on the Expansion of Trade in Information Technology Products, WT/MIN (15) /25, 16 December 2015.

共振成像机、高端半导体、激光技术等。信息技术产品贸易的主要成员几乎都加入了该协定。ITA扩大了作为数字贸易基础的技术产品贸易，但ITA的规制局限于信息技术产品的关税削减机制，不包含任何形式的非关税壁垒的有约束力的承诺。〔30〕数字贸易壁垒更多涉及边境后的非关税措施，但ITA委员会在2003年通过的《非关税措施工作计划》〔31〕至今仍未取得成果。尽管如此，ITA为与信息技术相关的硬件贸易提供了非常自由的体制，极大地推动了信息技术在全球的普及和运用，促进了跨境数据流动。

三、新近自由贸易协定中跨境数据流动的规制模式

由于USMCA的数字贸易规则大部分移植了CPTPP的规则，而DEPA的跨境数据流动规则也和CPTPP基本相同，因此，本文主要以CPTPP为分析对象。CPTPP和USMCA的电子商务/数字贸易章为跨境数据流动规定了“原则+例外”的规制模式。跨境数据流动是一项原则性要求，这项义务的适用范围本身也有一定的限定条件。早期的美国FTA也有要求跨境数据流动的条款，但直到CPTPP时期才上升为一项有约束力的法律义务。跨境数据流动的例外包括“监管要求”例外和“合法公共政策目标”例外，后者部分借鉴了WTO一般例外条款的文本。

（一）跨境数据流动“原则+例外”的规制模式

1. 原则上要求跨境数据自由流动

美国是世界上最早考虑在国际经贸协定中纳入跨境数据流动规则的国家。〔32〕《美韩FTA》是世界上首个在电子商务章中纳入了数据自由流动规则的FTA。〔33〕该协定第15.8条规定：“各方应努力避免对跨境电子信息流动施加或维持不必要的障碍。”但该条款并未定义什么是必要的障碍或不必要的障碍，也未禁止使用此类障碍，并且未澄清信息自由流动的合法例外是否必要。一缔约方是否可以依据该款规定来质疑另一缔约方对此类壁垒的使用是不明确的，该条款不具有可诉性。

CPTPP跨境数据流动规则的措辞从《美韩FTA》中使用的“努力”改成了具有法律约束力的“应当”，从而加强了义务。CPTPP第14.11.2条规定：“当以电子方式进行跨境信息传输的活动是为了涵盖人的商业行为时，每一缔约方应当允许以电子方式进行跨境信息传输，包括个人信息。”这一条款的主要目的是削弱很多国家有关诸如数据本地化、保护本地技术以及阻止外国数字服务的政策。USMCA第19.11.1条的跨境数据流动规则使用了更强硬的否定陈述句，即“任何缔约方不得禁止或限制跨境信息传输”。

CPTPP第14.11.2条确定了跨境数据自由流动的原则性要求，但也要注意这一条款的适用范围。《美韩FTA》电子商务章中规定的信息并未作任何限定，可以理解为涵盖了所有信息，而CPTPP中的信息传输仅指“为了涵盖人的商业行为时”进行的跨境信息传输。根据CPTPP第14.1条，“涵盖人”是指：（a）第9.1条定义的涵盖投资；（b）第9.1条定义的缔约方的投资者，但不包括投资于金融机构的投资者；或（c）第10.1条定义的缔约方的服务提供者，但不包括第11.1条定义的“金融机构”或“缔约方的跨境金融服务提供者”。由于“涵盖人”的定义仅包括涵盖投资、投资者或服务提供者，其他当事方不能从该条款中受益。换言之，如果一缔约方选择不向其他缔约方开放某些服务贸易或投资部门，则可以限制该部门中的数据流动。涵盖人的定义排除了金融机构和跨境金融服务提供者，CPTPP第11章（金融服务）附件

〔30〕 Congressional Research Service, Digital Trade and U.S. Trade Policy, 11 May 2018, p. 31.

〔31〕 Committee of Participants on the Expansion of Trade in Information Technology Products, The Non-Tariff Measures Work Programme, Compilation of the Submissions by the Secretariat (Revision), G/IT/SPEC/Q2/11/Rev.1, 14 April 2003.

〔32〕 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页。

〔33〕 Susan Ariel Aaronson, *The Digital Trade Imbalance and Its Implications for Internet Governance*, CIGI Working Paper 1, 8 (2016).

11-B的B节规定了单独的数据传输要求。[34]根据CPTPP第14.2.3条，CPTPP第14.11.2条的跨境数据流动要求也不适用于政府采购和政府持有或处理的信息。

根据CPTPP第14.11.2条，涵盖人只能在为了其商业行为的活动中获益。何谓“为了涵盖人的商业行为”？如果广义地理解，大多数通过互联网传输的数据，包括通过社交网站进行的个人通信、电子邮件服务等，都有可能被认为是为了涵盖人的商业行为。“为了”（for）一词至少表明，数据流动（即活动）和涵盖人（即任何数字服务的提供者）的商业行为之间必须存在一定程度的因果关系。在实践中，要在数据传输和所涵盖的商业行为之间确立因果关系，从而将本条款所涵盖的“信息”与互联网流动的“一般数据”区分开来，不仅花费巨大，而且不可行。[35]如果狭义地解释“为了涵盖人的商业行为”，预售促销活动可能不被涵盖在内。[36]

为限制跨境数据流动而普遍采取的措施是执行数据本地化法规。数据本地化法规通常要求外国或国内服务提供商将一国居民的所有信息或某些类别的信息存储在该国境内的服务器中。数据本地化特别不利于云计算的高效增长，云计算的有效增长是以规模经济和全球信息的无缝传输为前提。数据本地化措施严重阻碍信息技术的重大创新，不仅影响云计算，还威胁大数据和物联网的发展前景。

那么，数据本地化措施是否需要专门的规则来规制？有学者指出，通过特定规则来禁止数据本地化要求并非绝对必要，禁止缔约方强加或维持对数据流动的不必要障碍的通用规则可以用作对抗非法数据本地化要求的一种手段。[37]通过更有针对性的规则规制数据本地化问题并无不妥，关键在于规则的设置能否在数据自由流动与国家规制权之间实现合理平衡。为确保跨境数据自由流动，CPTPP和USMCA都规定了禁止计算设施本地化的规则。CPTPP第14.13.2条规定：“任何缔约方不得要求涵盖人使用位于其境内的计算设施，或将计算设施置于其境内，作为在其境内从事商业行为的前提条件。”除非符合协定列明的例外，CPTPP明确禁止缔约方采取计算设施本地化措施。国际经贸协定中的禁止计算设施本地化条款一方面是为了实现跨境数据自由流动，另一方面也是为了扫除其他国家基于数据管辖权的考虑而实施的其他限制措施。[38]

2. 规定了跨境数据流动的例外情形

推动“跨境数据自由流动”是美式数字贸易规则最关键的诉求，因而美国在《跨太平洋伙伴关系协定》（TPP，即CPTPP的前身）谈判过程中坚定支持跨境数据自由流动。[39]但其他谈判方则基于各种国内政策目标要求对数据流动实施限制。例如，澳大利亚、新西兰和加拿大希望限制跨境数据传输以解决有关其公民数据的隐私关切；越南主张以国家安全为由限制互联网的使用和数据传输；新加坡提出以公共道德为由限制数据流动。[40]

---

〔34〕 即“每一缔约方应允许另一缔约方的金融机构在其日常业务过程中以电子形式或其他形式将信息传输入境或出境，以进行数据处理。本节的任何内容均不限制一缔约方采取或维持以下措施的权利：（a）保护个人数据、个人隐私以及个人记录和帐户的机密性；（b）出于审慎考虑，要求金融机构事先获得有关监管机构的授权，以指定特定企业为此类信息的接收者，但前提是该权利不得用作规避该缔约方在本节项下的承诺或义务的手段”。

〔35〕 Neha Mishra, *The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?* 20 Journal of International Economic Law 31, 38 (2017).

〔36〕 Henry Gao, *Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation*, 45 Legal Issues of Economic Integration 47, 68 (2018).

〔37〕 Mark Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, RTA Exchange, International Centre for Trade and Sustainable Development and the Inter-American Development Bank, 24 (2017).

〔38〕 徐程锦：《WTO电子商务规则谈判与中国的应对方案》，载《国际经济评论》2020年第3期，第43—44页。

〔39〕 当然，美国近年来也越来越多地把国家安全作为控制数据的理由，例如特朗普政府以国家安全为由针对TikTok发布行政禁令，相关分析可参见冯硕：《TikTok被禁中的数据博弈与法律回应》，载《东方法学》2021年第1期。

〔40〕 Neha Mishra, *The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?* 20 Journal of International Economic Law 31, 37 (2017).

CPTPP中的跨境数据流动条款本身限定了义务的适用范围，跨境数据流动的例外包括“监管要求”例外和“合法公共政策目标”例外。CPTPP第14.11.1条规定：“缔约方承认，每一缔约方可就以电子方式进行的信息传输规定自己的监管要求。”CPTPP第14.13.1条也规定：“缔约方承认，每一缔约方可就计算设施的使用制定自己的监管要求，包括为寻求确保通信安全和保密的要求。”这两项规定是对缔约方国家规制权的尊重，允许缔约方独立自主地对跨境数据流动和计算设施进行规制，其基础在于国家主权原则，而合法公共政策目标例外是这种“监管要求”的具体体现。因此，“监管要求”例外和“合法公共政策目标”例外是一个问题的两个方面，二者统一于国家主权的行使。不过，USMCA第19.11条直接删除了CPTPP第14.11.1条有关监管要求的规定，USMCA第19.12条有关禁止计算设施本地化的条款也剔除了监管要求的规定。

在合法政策目标例外方面，CPTPP第14.11.3条规定：“本条规定不得阻止缔约方为实现合法公共政策目标而采取或维持与第2款不符的措施，若该措施：（a）其实施并未构成任意或不合理的歧视或构成对贸易的变相限制；及（b）其对信息传输所施加的限制并未超过为实现合法目标所必需的限度。”CPTPP第14.13.3条也对计算设施的使用和位置设定规定了极为类似的例外。“采用”或“维持”的措辞包括了现有措施和未来措施。CPTPP电子商务章中的这一例外规定与GATT1994第20条和GATS第14条的一般例外条款在措辞上非常相似，但在编排结构上互为颠倒。〔41〕WTO一般例外条款的序言规定措施的实施方式，子项规定公共政策目标；而CPTPP第14.11.3条和第14.13.3条的序言规定公共政策目标，子项规定措施的实施方式。一般例外条款序言和子项编排结构的变化将对条款的适用步骤产生一定影响。在WTO实践中，争端解决机构在适用一般例外条款时，首先结合具体的公共政策目标对争议措施进行“必需性”（necessity）测试，然后再考察措施的实施方式。而CPTPP的上述条款很可能使得争端解决机构在适用该条款时，采取完全颠倒过来的步骤，即先考察措施的实施方式，再进行“必需性”测试。

WTO一般例外条款列出了一系列公共政策目标，如保护公共道德、公共秩序、人类、动物或植物的生命或健康，但CPTPP第14.11.3条和第14.13.3条却没有这样的列举，只是提到了“合法公共政策目标”。其缘由在于，CPTPP缔约方对何为合法公共政策目标未能达成一致。这一规定允许CPTPP缔约方对跨境数据流动和计算设施的规制享有更多的监管自主权，但也可能导致缔约方对该例外的滥用以及总体上的法律不确定性。例如，某些政策目标（例如互联网审查或言论自由限制）在某些缔约方国内是合法的，而在另一些国家中可能被认为是非法的。

为探究公共政策目标的范围，从法律解释的角度可以结合条约的目的和宗旨来理解。CPTPP序言规定：“承认缔约方固有的规制权，并决心保留缔约方在设定立法和监管优先事项、保障公共福利和保护合法公共福利目标方面的灵活性，如公共健康、安全、可用尽生物或非生物自然资源的保护、金融系统的完整性和稳定性以及公共道德。”可见，序言列举的公共福利目标与WTO一般例外条款涵盖的政策目标大体相同，并且CPTPP序言的列举并没有穷尽，仅仅是示例性的说明。在对跨境数据流动的规制中，隐私保护、在线消费者保护、公共道德、公共秩序等都有可能构成“合法公共政策目标”。如果发生相关的贸易争端，援引公共政策例外的缔约方负有责任证明其主张的国内政策目标符合上述例外条款的规定。

事实上，GATT1994和GATS中的一般例外条款在作了必要修改之后已经被纳入到CPTPP中。〔42〕那么，CPTPP第14.11.3条和第14.13.3条中的例外与CPTPP一般例外条款是何关系？ CPTPP第14章内置的例外条款和一般例外条款为合法公共政策目标的实现提供了双重保障。根据CPTPP第29.1条（一般例外），第14章（电子商务）适用于GATS第14条的（a）（b）和（c）款，即电子商务章的规则要受到整个协定的一般例外条款的约束。如果一项限制跨境数据流动的措施无法依据CPTPP第14.11.3条或第14.13.3条

〔41〕 彭岳：《数据本地化措施的贸易规制问题研究》，载《环球法律评论》2018年第2期，第188页。

〔42〕 Art. 29.1 of CPTPP.

正当化，还可以依据协定中的一般例外条款进行抗辩。

CPTPP电子商务章中例外条款非歧视性的条件类似于GATT1994第20条和GATS第14条确定的严格测试，其目的在于平衡贸易和非贸易利益。对于何谓“任意或不合理的歧视”或“对国际贸易的变相限制”，WTO丰富的案例实践可以提供非常有益的参考。在评估限制措施是否“未超过为实现合法目标所必需的限度”时，CPTPP仲裁庭可以采用类似于GATT1994第20条中的“必需性”测试。跨境数据流动的例外条款体现了最小限制原则和比例原则，基于合法政策目标对跨境数据流动的限制应考虑对数据流动影响更小的措施。〔43〕

USMCA第19.11条关于合法政策目标例外的规定增加了一个脚注，即“如果一项措施仅仅因为数据传输是跨境的就被授予不同待遇，从而改变竞争条件，损害另一缔约方的服务提供者，则不符合本款的条件”。该脚注的规定借鉴了国民待遇原则中“不低于”概念的法律解释，强化了非歧视的概念，特别强调不得因为改变竞争条件而对境外服务提供者造成损害。USMCA第19.12条有关禁止计算设施本地化的条款把CPTPP第14.13条内置的例外条款删除了。但这并不意味着，禁止计算设施本地化是一项绝对的义务而没有例外，它仍然可以适用USMCA第32章中的一般例外和安全例外条款。

总体而言，CPTPP第14.11条和第14.13条以及USMCA第19.11条和第19.12条通过确立“原则+例外”的规制模式为跨境数据流动构建了一个相对自由的法律框架。CPTPP和USMCA的上述规则可能是跨境数据流动监管合作形式的典范，它将在服务贸易中引发更广泛、更深入的承诺。〔44〕RCEP第12章（电子商务）中的数据流动规则也借鉴了上述模式，其中的例外条款还涵盖了国家安全例外的情形。〔45〕但“原则+例外”的规制模式依然存在局限性，其例外条款无法为限制数据流动的合法性提供足够的法律确定性。大量数据在全球范围内的不断流动，越来越多地涉及范围广泛的国内法规。由于缺乏统一的数字贸易治理框架，各国政府只能依赖宽泛的例外条款来限制数据流动。为了满足限制数据流动措施的“必需性”测试要求，通常需要各国在数据治理的国际标准和监管合作方面的共识作为支撑，而这恰恰是各国在数字贸易规制中所缺乏的。〔46〕

（二）特殊数据的专门规则

不同类型数据的跨境流动可能影响的政策目标不同，为了对不同国家特定政策目标的维护提供法律确定性，也为了更好地利用数据，促进数字贸易发展，FTA数字贸易章节除了对跨境数据流动规定了“原则+例外”的总体要求以外，还对特殊数据规定了专门规则。CPTPP和USMCA对跨境数据自由流动的要求包括个人数据，〔47〕因为个人数据也可能与涵盖人的商业行为有关，也可以被商业化。但个人数据的跨境流动直接关涉个人隐私保护，因此，CPTPP和USMCA还专门规定了个人数据保护条款。不过，CPTPP和USMCA的跨境数据自由流动要求均不适用于政府持有、处理或收集的数据。〔48〕政府数据关涉一国的公共安全或国家安全，因而对政府数据采取本地化措施不受自由流动的义务约束。但政府数据的开放和利用可以促进数字贸易的发展，因此USMCA规定了政府数据开放条款。〔49〕此外，前文述及的金融数据的单独传输规则亦属于此处的特殊数据的专门规则。〔50〕

---

〔43〕 孙益武：《数字贸易与壁垒：文本解读与规则评析——以USMCA为对象》，载《上海对外经贸大学学报》2019年第6期，第92页。

〔44〕 Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 Journal of International Economic Law 769, 784 (2018).

〔45〕 Art. 12.14 and Art.12.15 of RCEP.

〔46〕 Joshua P. Meltzer, *Governing Digital Trade*, 18 World Trade Review s23, s46–s47 (2019).

〔47〕 Art. 14.11.2 of CPTPP; Art. 19.11.1 of USMCA.

〔48〕 Art. 14.2.3 of CPTPP, Art. 19.2.3 of USMCA.

〔49〕 Art. 19.18 of USMCA.

〔50〕 相关分析可参见马兰：《金融数据跨境流动规制的核心问题和中国因应》，载《国际法研究》2020年第3期。

1. 个人数据保护

个人数据的流动关涉个人隐私保护。谷歌（Google）、脸书（Facebook）等大型互联网公司在提供数字服务的过程中侵犯用户个人隐私的事件时有发生。〔51〕由于不同国家在特定文化、宗教和政治背景方面的差异，人们对隐私和数据保护问题的看法往往截然不同，结果导致隐私保护要求在不同法域之间的差异，对于保护在线隐私的最佳方法尚无国际共识。欧盟强烈主张将隐私作为一项基本人权，我国数据保护法将隐私视为信息安全而非人权问题，美国将隐私视为一项消费者权利，但一些发展中国家尚未制定隐私或数据保护法。〔52〕不同国家对个人数据的监管差异通常会增加跨境服务提供商的合规成本，因为他们需要为客户量身定制其网站和数据收集方法等，此类要求还可能影响新技术的采用和使用。复杂的隐私保护要求也将阻止中小微企业从事数字贸易，因为合规要求对他们来说是一种沉重的负担。隐私法规可能成为歧视性贸易壁垒，但在另一方面，完善的隐私法规提高了互联网用户的信心，因为他们的数据被服务提供商安全地收集、使用和存储。〔53〕保护在线隐私日益成为数字贸易的基本要求之一。〔54〕加拿大在2019年向WTO提交的首轮电子商务提案中特别强调隐私保护，以增进人们对数字贸易的信心和信任。〔55〕

欧盟将个人数据保护置于优先位置，并坚持其高标准的要求，不容挑战。为保障欧盟个人数据安全，欧盟和美国于2000年签署了《安全港协议》，但2013年的“棱镜门”事件暴露了《安全港协议》执行中存在的问题。欧盟公民在政府访问其数据时缺乏救济权，因而《安全港协议》无法确保充分的隐私保护。2015年欧洲法院裁定《安全港协议》无效。2016年2月，欧盟和美国就数据传输达成了《隐私盾协议》。根据《隐私盾协议》，美国公司通过行业机构或单独向美国商务部自我证明，他们将保护欧盟公民的个人数据。《隐私盾协议》承诺提供比《安全港协议》更严格的隐私标准，将权利扩展到欧盟数据主体，并强化了监督和执法要求。〔56〕不过，由于美国的数据保护水平仍然未能达到“与欧盟基本等同”的标准，欧洲法院于2020年7月裁定《隐私盾协议》无效。

GATS第14（c）（ii）条仅将保护隐私作为一项例外，不能确保所有成员在个人数据保护方面采用统一框架，也没有解决因各国隐私框架的差异而导致的贸易壁垒。自TPP谈判的早期阶段以来，美国就一直希望通过一种灵活的机制来保护个人信息，允许建立用于数据传输的自我认证机制并采用自我监管框架。亚太经合组织（以下简称“APEC”）在2004年通过了类似的隐私框架，但澳大利亚和加拿大等国反对宽松的隐私框架，因为它可能会限制其基于隐私理由限制跨境数据传输的能力。澳大利亚则特别关注如何维护其居民的电子健康记录的隐私。〔57〕

CPTPP第14.8.2条要求每一缔约方“采取或维持保护电子商务使用者个人信息的法律框架”。在数字贸易时代，如果一个国家没有个人信息保护方面的国内规则，可能构成贸易壁垒。但该条款并未为法

〔51〕 戴龙：《论数字贸易背景下的个人隐私权保护》，载《当代法学》2020年第1期，第154页。

〔52〕 Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 Journal of International Economic Law 389, 392–393 (2019).

〔53〕 Neha Mishra, *The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?* 20 Journal of International Economic Law 31, 41 (2017).

〔54〕 Neha Mishra, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, 52 Vanderbilt Journal of Transnational Law 463, 503 (2019).

〔55〕 Joint Statement on Electronic Commerce, Communication from Canada, Concept Paper–Building Confidence and Trust in Digital Trade, INF/ECOM/29, 9 May 2019.

〔56〕 Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 Journal of International Economic Law 769, 783 (2018).

〔57〕 Neha Mishra, *The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?* 20 Journal of International Economic Law 31, 41–42 (2017).

律框架规定任何标准或基准，而是提出了一个更广泛和更普遍的要求，即缔约方应“考虑相关国际机构的原则或指南”。它承认隐私原则或指南正在发展，其他相关的国际机构也在处理这些问题。同时，该款的脚注允许缔约方采取自己版本的隐私法规来执行该款规定的义务。USMCA第19.8.2条在提及国际机构的原则或指南时专门列举了《APEC隐私框架》和OECD《关于隐私保护和个人数据跨境流动的指南（2013）》。这说明USMCA缔约方在规制个人数据出境方面接受APEC和OECD的相关原则作为统一的保护标准。USMCA第19.8.3条还强调对个人信息跨境流动的限制必须是必要的，并且与所面临的风险成比例。

一些国家的数据监管措施忽视了对数据的保护，当个人或企业数据被政府滥用时，缺乏有效的救济途径。CPTPP第14.8.3条规定：“缔约方在保护电子商务使用者在其管辖法域中免遭个人信息侵犯行为时，应尽力采取非歧视的做法。”保护互联网用户的隐私有助于建立消费者对互联网服务的信任，但CPTPP第14.8.3条使用的措辞却是“尽力”，因而不具有强制约束力。CPTPP第14.8.4条规定：“缔约方宜公布其向电子商务使用者提供的个人信息保护的信息，包括：（a）个人如何寻求救济；和（b）企业如何遵循相关法律要求。”这一条款体现了透明度原则的要求。

CPTPP第14.8.5条规定：“认识到各缔约方可采用不同方式保护个人信息，每一缔约方宜鼓励建立相应机制，以促进不同体系间的相互协调。这些机制可以包括互认规制结果，无论是自主承认还是通过共同安排承认，或通过更广的国际框架。为此，缔约方应尽力相互交换其管辖范围内适用的相关机制的信息，并探索相应的方法扩大这些机制或其他适当安排以促进机制间相互协调。”但对于个人信息保护问题，在国际上并没有公认的共识。CPTPP第14.8.2条中有关保护个人信息的“法律框架”是否存在最低标准，依然是不确定的。USMCA第19.8.6条提到，为实现保护个人信息的同时促进跨境信息传输，APEC的《跨境隐私规则体系》（CBPR）是有效的机制。在线隐私已在国际社会中日益被视为一项基本人权，因此基于保护隐私而限制数据流动的措施有可能构成CPTPP第14.11.3条和第14.13.3条中的合法公共政策目标之一。

2. 政府数据开放

政府通常是数据最大的拥有者，公民的很多信息都被数据化，被政府掌握。政府数据与公众的生产生活息息相关，关涉公共安全甚至国家安全，因而不适用自由流动的原则性要求。大数据建立在开放数据的基础上，开放政府数据供社会利用是实现大数据战略的重要前提。〔58〕开放数据不同于公开数据，开放数据往往是结构化、可机读、获得开放授权并得到良好维护的数据，而公开数据通常是非结构化的、混乱的、授权使用要求模糊的数据。〔59〕政府数据开放不同于政府信息公开，信息公开强调公众的知情权，而数据开放强调公众利用数据的权利。

政府数据开放有利于消除政府数据的垄断和不对称性，促进数据的运用，从而推动数字贸易的发展。日本在2018年4月向WTO提交的电子商务文件指出，为了促进电子商务/数字贸易的进一步发展，可以向公众开放由政府收集的数据，例如统计信息、公共交通数据和防灾数据。通过将这些数据提供给国内外公司，政府可以增加促进创新的机会。如果只允许国内公司访问此类数据，这将对外国公司构成国民待遇壁垒，使得外国公司无法进入相关市场。因此，各国政府收集的数据应当公开，并应在非歧视的基础上允许广泛获取。〔60〕美国在2018年4月向WTO提交的电子商务文件也指出，便利公众获取和使用政府信息可促进经济和社会发展，并鼓励对该信息进行创新利用。贸易规则应鼓励政府以机器可读和开

〔58〕 郑磊：《开放政府数据研究：概念辨析、关键因素及其互动关系》，载《中国行政管理》2015年第11期，第13页。

〔59〕 郑磊：《开放不等于公开、共享和交易：政府数据开放与相近概念的界定与辨析》，载《南京社会科学》2018年第9期，第87页。

〔60〕 General Council, Joint Statement on Electronic Commerce Initiative, Proposal for the Exploratory Work by Japan, JOB/GC/177, 12 April 2018, para. 3.11.

放的格式提供公共信息，并使信息可以被搜索、检索、使用、重复使用和重新分发。〔61〕

USMCA数字贸易章新增了政府数据开放条款，其第19.18条规定："1.缔约方承认，便利公众获取和使用政府信息可以促进经济和社会发展、竞争和创新。2.在某一缔约方选择向公众提供政府信息（包括数据）的范围内，应努力确保该信息采用机器可读和开放的格式，并且可以被搜索、检索、使用、重复使用和重新分发。3.缔约双方应努力合作，以确定各缔约方可以扩大对本方公开的政府信息（包括数据）的访问和使用的方式，以期增加和创造商机，特别是为中小企业创造商机。"但这一条款并无强制性，仅仅是鼓励性的，没有为缔约方创设具体义务。《美日数字贸易协定》规定了与USMCA几乎完全一样的政府数据开放条款。〔62〕政府数据开放需要满足一定的技术条件，政府在行使职能过程中收集的部分数据有可能是非结构化数据，无法机读，这将制约政府数据开放。

对特殊数据规定专门规则，是FTA规制跨境数据流动议题的一大特点。FTA对跨境数据自由流动的要求针对的是涵盖人的商业行为有关的数据，即商业数据。由于跨境数据流动是进行数字贸易的前提，因此FTA将跨境数据自由流动上升为一项原则性要求。个人数据的跨境流动可能影响个人隐私，CPTPP和USMCA的个人数据保护条款要求缔约方采取保护个人数据的法律框架，考虑相关国际机构的原则或指南，采取非歧视的做法，并促进个人数据保护不同体系间的相互协调。这一规则设置有利于实现个人数据跨境流动与隐私保护之间的平衡，防止隐私规则或隐私执法措施成为数字贸易壁垒。USMCA的政府数据开放条款将促进政府数据的合理利用和创新，推动数字贸易发展。总体而言，对特殊数据进行专门规制与数字贸易规制的多元目标相契合，是较为合理的规制路径。当然，不同规则之间应注意衔接和协调。例如，个人数据保护也可以成为跨境数据流动"例外"中的合法公共政策目标之一，如果发生实际争端，相关条款的适用应防止出现冲突。

四、跨境数据流动规则的协调

通信技术服务和信息技术产品的贸易自由化为跨境数据流动奠定了基础。理想的数字贸易规则框架应促进数据自由流动、数字创新以及在全球数字市场中的健康竞争，同时不妨碍一国基于正当理由监管互联网的权力。CPTPP和USMCA在电子商务/数字贸易章为跨境数据流动设定了"原则+例外"的规制模式，并对特殊数据规定了专门规则。

（一）在国际经贸协定框架下协调跨境数据流动规则的普遍困境

有很多FTA（尤其是含发展中国家的FTA）在处理跨境数据流动问题上仅规定了监管合作条款，要求缔约方"努力保持信息的跨境流动，将其作为营造充满活力的电子商务环境的基本要素"。〔63〕欧盟当前FTA中的数字贸易规则没有为跨境数据流动设定有约束力的义务，有些FTA仅强调了个人信息保护和隐私保护。〔64〕《欧盟—日本经济伙伴关系协定》第8.81条规定："双方应在本协定生效之日起三年内重新评估是否需要将数据自由流动条款纳入本协定。"这表明欧盟对跨境数据流动问题的讨论在不断发展，在未来的FTA中可能会有更多的具体行动和承诺。

在国际经贸协定谈判中，跨境数据流动问题往往成为谈判方争议的焦点。在《国际服务贸易协定》（以下简称"TISA"）谈判中，关于数据流动的条款有很多争论。美国、日本和加拿大建议，"任何一方

〔61〕 General Council, Joint Statement on Electronic Commerce Initiative, Communication from the United States, JOB/GC/178, 12 April 2018, para. 6.1.

〔62〕 Art. 20 of the Agreement between the US and Japan Concerning Digital Trade.

〔63〕 Art. 16.5(c) of the Canada–Honduras FTA; Art. 1507.1(c) of the Canada–Colombia FTA; Art. 13.7(c) of the Canada–Korea FTA; Art. 1508 of the Canada–Peru FTA; Art. 15.5(c) of the US–Chile FTA.

〔64〕 Art. 7.48.2 of the EU–Korea FTA; Art. 16.4 of the Canada–EU CETA; Art. 8.78.3 of the EU–Japan EPA.

都不得阻止另一方的服务提供者在该方领土内或领土外转移、访问、处理或存储包括个人信息在内的信息，前提是此类活动与服务提供者的业务行为有关”。〔65〕很多国家或地区考虑了该禁令的例外或条件，以允许更多的国内灵活性。例如，我国香港建议，跨境数据自由流动与保护个人数据之间应保持平衡，推进前者应不损害维护后者的权利。欧盟委员会公布的TISA第21轮谈判报告显示，有关数据流动和计算设施本地化的条款需要缔约方继续进行深入讨论。〔66〕在《跨大西洋贸易与投资伙伴关系协定》（以下简称“TTIP”）谈判中，跨境数据流动议题也面临同样的困境。2017年1月发布的《美国—欧盟关于TTIP进展的联合报告》提到，TTIP谈判中有关数字贸易的分歧在于如何建构数据流动承诺，以加强美欧经济关系中必不可少的电子商务和数字基础设施，同时尊重保护隐私的合法关切。〔67〕

（二）在WTO框架下为数据保护达成基本框架

跨境数据流动的国际规则协调所面临的一个重要分歧是在个人数据方面。为实现跨境数据自由流动，数据来源地国和目的地国都应具有有效的隐私框架。有学者曾在20年前主张在WTO主持下制定一项关于数据保护的国际条约，该条约侧重于建立规范发展的制度过程，旨在短期内促进不同制度的共存，并随着时间的推移促进信息隐私治理标准的统一。该学者指出，将该数据保护条约纳入WTO具有重要意义。首先，WTO框架提供了具有广泛成员资格的制度过程；其次，尽管WTO倾向于市场导向的规范，但将数据保护条约纳入WTO将把社会保护规范移植到贸易领域，将促进治理规范的融合。〔68〕但时至今日，WTO仍未形成这样的数据保护条约。各国如果要在跨境数据流动规制问题上达成综合性条约，需要协调好各主权国家之间在互联网的物理层、逻辑层、应用层和核心层的权力配置关系，以及主权与互联网、主权与人权、主权与多方治理等多维利益平衡和价值协调问题，这在短期来看不具有可行性。〔69〕

相较于制定一项数据保护国际条约，在WTO中为数据保护达成一个基本框架的难度更低一些，但什么样的隐私框架可以作为基本的监管框架是一个极其复杂的问题。USMCA第19.8.2条列举了《APEC隐私框架》和OECD《关于隐私保护和个人数据跨境流动的指南（2013）》，但在多边体制下将APEC和OECD的原则作为基准可能会引起争议，因为与GDPR及其类似框架相比，这些原则被认为是过于宽松的。〔70〕欧盟FTA在数据保护方面虽然也要求与国际标准兼容，但通常不规定任何具体的数据保护框架。例如，《欧盟—加拿大全面经济贸易协定》第16.4条规定：“每一缔约方应采取或维持法律、法规或行政措施，以保护从事电子商务的用户的个人信息，并且在这样做时，适当考虑双方都是成员的相关国际机构的数据保护国际标准。”

（三）通过互认机制协调个人数据保护标准

GATS第7条规定了相互承认“服务提供者获得授权、许可或证明的标准或准则”的机制。欧盟和美国签署的《安全港协议》和《隐私盾协议》是通过互认机制来协调个人数据保护标准的典型。GATS第7条允许这种选择性的、针对特定国家的承认协议，但该条要求数据来源国不得在存在类似条件的国家之间构成歧视，并给予其他国家加入该协议的机会。由于数字鸿沟的存在，通过互认机制来协调数据保护标准的实践主要发生在数字贸易大国之间，发展中国家和最不发达国家缺乏实践基础。但这种务实

〔65〕 Wikileaks, Trade in Service Agreement (TISA) Annex on Electronic Commerce, 3 June 2015, p. 2.

〔66〕 European Commission, Report of the 21st TISA Negotiation Round, 2–10 November 2016, p. 3.

〔67〕 Executive Office of the President of the United States & European Commission, US–EU Joint Report on TTIP Progress to Date, 17 January 2017, p. 3.

〔68〕 Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stanford Law Review 1315, 1360–1362 (2000).

〔69〕 彭岳：《数字贸易治理及其规制路径》，载《比较法研究》2021年第4期，第167页。

〔70〕 Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 Journal of International Economic Law 389, 409 (2019).

的双边互认机制会产生溢出效应和示范效应，从而影响其他国家之间的跨境数据流动规则协调。

GATS第7.5条规定："只要适当，承认即应以多边议定的准则为依据。在适当的情况下，各成员应与有关政府间组织和非政府组织合作，以制定和采用关于承认的共同国际标准和准则，以及有关服务行业和职业实务的共同国际标准。"该规定表明，WTO法有可能促进不同隐私框架的互操作性，从而协调跨境数据流动规则。根据该规定，成员可以通过纳入从事隐私标准和相关问题工作的相关跨国机构或多利益相关方机构，使相互承认的对话（例如在服务贸易理事会中的对话）更为有意义。WTO可以与从事国际合作以制定隐私规则/标准和跨辖区隐私执法的机构保持联系，如数据保护与隐私专员国际大会。该机构在采纳有关数据保护最佳做法的国际准则方面发挥着关键作用，并且在进一步制定数字隐私问题的规则和建立国际共识方面可以发挥至关重要的作用。〔71〕

（四）加强与APEC或OECD的合作

APEC和OECD在制定通用的隐私标准和原则方面做了很重要的工作。2013年，OECD发布了《关于隐私保护和个人数据跨境流动的指南》，对1980年版的隐私指南进行了更新。该隐私指南规定了管理个人数据的收集、存储和使用的最低要求，以指导OECD成员发展国内隐私保护制度，其中的很多原则都反映在GDPR中。关于个人数据流动的规制，OECD纳入了基于欧盟GDPR路径和美国"行业自律"路径的两种方式，要求数据收集者对个人数据负责。〔72〕APEC在2004年通过的APEC隐私框架类似于OECD的隐私指南。APEC隐私框架具有更强的可操作性，可以指导国内隐私法规的发展。APEC在隐私框架的基础上于2012年制定了《跨境隐私规则体系》，以促进APEC成员之间的个人数据流动。《跨境隐私规则体系》是一个自愿的、基于问责制的系统，可促进"尊重隐私"的跨境数据流动。《跨境隐私规则体系》并不改变各国有关个人数据的国内立法，它认识到，对于隐私保护，没有一种一刀切式的规制方法，因为不同国家在该问题上具有不同的法律和社会价值观及路径。鉴于互联网全球分布的特性，每个国家的数据治理机制都必须具有互操作性，以便同时实现隐私保护和数据流动。〔73〕WTO成员可以通过与APEC或OECD合作，促进成员之间隐私标准的互相承认，从而协调跨境数据流动规则。

2022年4月21日，美国、加拿大、日本、韩国、菲律宾、新加坡和我国台湾地区共同发布《全球跨境隐私规则声明》，〔74〕宣布成立全球跨境隐私规则论坛，以促进数据保护和隐私的互操作性并帮助弥合不同监管方式之间的差距。声明的基本目标包括建立基于APEC《跨境隐私规则体系》和《处理者隐私识别体系》（Privacy Recognition for Processors）的国际认证体系，定期审议成员的数据保护和隐私标准，促进与其他数据保护和隐私框架的互操作性等。声明还规定了其活动范围、运作模式、参与和组织规则。原则上，全球跨境隐私规则论坛旨在向接受本声明所体现的目标和原则的司法管辖区开放，本质上是将《跨境隐私规则体系》转变成一个所有国家或经济体都可以加入的体系。

鉴于不同类型数据的跨境流动涉及的政策目标不同，有学者提出先对数据进行归类，然后对不同类型数据的市场准入和国民待遇分别作出承诺，例如对公司数据的开放采取负面清单模式，对个人数据采取正面清单模式。〔75〕还有学者建议，在国际经贸协定谈判过程中，可以在对数据进行分类的基础上，再

〔71〕 Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 Journal of International Economic Law 389, 411–412 (2019).

〔72〕 Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 Journal of International Economic Law 769, 784 (2018).

〔73〕 Nigel Cory, *Why China Should Be Disqualified from Participating in WTO Negotiations on Digital Trade Rules*, Information Technology and Innovation Foundation Working Paper 8 (2019).

〔74〕 Global Cross-Border Privacy Rules Declaration, official website of U.S. Department of Commerce, Apr. 21, 2022, https://www.commerce.gov/global-cross-border-privacy-rules-declaration (accessed Apr. 25, 2022).

〔75〕 Nivedita Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?* 21 Journal of International Economic Law 323, 347 (2018).

借鉴服务贸易部门开放或货物贸易关税减让谈判的形式，由谈判方就数据的流动自由进行谈判。[76]上述学者建议的规制路径借鉴了WTO框架下传统服务或货物贸易的市场开放模式。国际经贸协定作为利益博弈的场所，国家在决定数据流动开放程度时需要平衡数字贸易自由化水平与国内政策目标，这一博弈过程有助于实现跨境数据流动规则的协调。上述建议的总体思路可行，但在具体操作过程中可能面临一定的障碍，因为数据的归类就像数字贸易的归类一样，本身又是一个悬而未决的难题。[77]不同种类数据的范围可能存在重叠，彼此之间并不存在泾渭分明的界限。

五、跨境数据流动规制的中国立场

（一）我国对跨境数据流动的国内规制实践

我国对跨境数据流动的规制坚持了以风险为基础的思路，目前初步形成了数据分级分类管理的顶层设计框架。[78]根据我国数据安全法、个人信息保护法、网络安全法、关键信息基础设施安全保护条例等相关立法，可以从数据处理者和数据两个角度，将我国的跨境数据流动规则大致分为四种情形。[79]

第一种情形为一般数据处理者处理个人信息（主体为一般主体，客体为非重要的个人信息）。借鉴GDPR等规定，我国个人信息保护法形成了个人信息多元化跨境提供的合法路径，确保实现同等保护水平。我国个人信息保护法第38条和第39条规定了个人信息跨境提供需要满足的基本要求。同时，由于向境外提供个人信息属于个人信息处理活动的一种类型，因此个人信息跨境提供还应当遵循我国个人信息保护法有关个人信息处理的一般规定。

第二种情形为一般数据处理者处理重要数据（主体为一般主体，客体为重要数据）。根据《汽车数据安全管理若干规定（试行）》第3条，重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益的数据。现行立法未对该种情形作出明确规定，根据我国数据安全法第31条，应由国家网信部门会同国务院有关部门制定相应的出境安全管理办法。《汽车数据安全管理若干规定（试行）》针对此种情形规定了一种数据出境条件，即原则上应将数据存储在境内，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。

第三种情形为重要数据处理者处理个人信息或重要数据（主体为重要主体，客体为个人信息和重要数据）。重要数据处理者主要是关键信息基础设施运营者，根据我国个人信息保护法，还包括处理个人信息达到国家网信部门规定数量的个人信息处理者和国家机关。此种情形的数据出境条件为，原则上应当在境内存储，确需向境外提供的，应当通过国家网信部门组织的安全评估。

第四种情形为外国司法或执法机构请求提供数据。我国数据安全法第36条和个人信息保护法第41条对此均有规定，数据出境的条件是依据国际条约、协定，或者按照平等互惠原则，且经过主管机关批准，该规定旨在从司法和行政执法层面阻却境外机构对境内机构和个人实施的长臂管辖。

（二）我国的国内规制措施已经与国际接轨

我国立法对跨境数据流动设定了一定的条件，此种限制可以构成国际经贸协定中的“限制措施”。

---

〔76〕 陈咏梅、张姣：《跨境数据流动国际规制新发展：困境与前路》，载《上海对外经贸大学学报》2017年第6期，第48页。

〔77〕 关于数字贸易归类问题的探讨，可参见谭观福：《国际贸易法视域下数字贸易的归类》，载《中国社会科学院研究生院学报》2021年第5期。

〔78〕 国家网信办2021年11月发布的《网络数据安全管理条例（征求意见稿）》第5条规定：“国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。”

〔79〕 参见徐程锦：《中国能否接受CPTPP版本跨境数据流动规则》，载微信公众号“顾小徐的随笔”，https://mp.weixin.qq.com/s/Fe2ZT8gMg0_s0vqyfZFsfg，访问时间：2022年4月25日。

那么，此种限制措施能否通过国际经贸协定中的压力测试？下文将以CPTPP为参考对象，对该问题稍作分析。CPTPP第14.11.2条是关于跨境数据流动的核心义务，具有强制性。我国立法允许为业务等需要进行跨境数据流动。我国对跨境数据流动的限制措施，如出境安全评估、个人信息保护认证或标准合同，本质上是对跨境数据流动规定了“监管要求”，与CPTPP第14.11.1条的规定相契合，并非不允许数据出境。因此，我国对跨境数据流动的国内规制措施不违反CPTPP第14.11.2条。至于CPTPP第14.13条规定的计算设施本地化问题，在一些特定行业（如互联网地图、网络出版）的立法中，确实存在计算设施本地化的要求，〔80〕但由于这些行业具有特殊性，此类要求往往可以援引协定中的例外条款免责。

假设我国的规制措施违反了CPTPP第14.11.2条，我国还可以援引CPTPP中的例外条款进行抗辩。我国对于跨境数据流动特别强调“安全、有序”，安全是首要价值。有少数关涉国家安全的核心数据可能被禁止出境，数据出境安全评估和数据安全审查措施都可能需要援引基本安全例外条款。CPTPP第32章的安全例外可以涵盖网络安全和数据安全的需要。当然，在具体适用时需要满足必需性的要求。〔81〕因此，接受CPTPP中的跨境数据流动规则时，需要对安全例外作出相应安排。

CPTPP第14.11.3条还规定了合理公共政策目标例外。个人信息保护认证和标准合同是其他国家普遍使用的机制，应该不会遭致违反CPTPP第14.11.2条的质疑。CPTPP第14.11.3条有三项核心义务：第一项义务是要求限制措施是为实现合法公共政策目标。数据出境安全评估是我国相对独特的机制，评估的目的是为了保障国家安全、公共利益、个人或者组织合法权益。CPTPP第14.11.3条的合法公共政策目标没有明确列举，外延很广，可以涵盖数据出境安全评估的前述目的。第二项义务是要求限制措施的实施不构成不合理的歧视或对国际贸易的变相限制。国家网信办已经起草了《数据出境安全评估办法（征求意见稿）》，规定了安全评估的情形、重点评估事项、评估程序等，相关的制度和标准正在形成过程中。由国家网信部门统一组织的安全评估只要适用客观标准，就不会造成不合理的歧视或对国际贸易的变相限制。第三项义务是限制措施应满足“必需性”测试要求，即不存在同样能实现合法政策目标，但对贸易的限制性影响更小的合理可行的替代性措施。我国的数据出境安全评估制度针对的是关键信息基础设施运营者或处理个人信息达到国家网信部门规定数量的个人信息处理者，或者重要数据的出境，在其他国家很少有类似的制度实践，因而也较难提出合理可行的替代性措施。〔82〕总体上，我国对于跨境数据流动的国内规制措施已经与国际接轨。

（三）完善跨境数据流动规制的建议

我国对跨境数据流动规制的制度逐渐走向完善，但其他国家对我国的规制措施仍有猜疑或不甚了解。跨境数据流动议题本身具有涉外性，各国是在国内规制的基础上进行国际规则的协调。只有不断完善国内制度，才能准确把握对外谈判立场，并引领国际规则。个人信息保护认证在我国还处于制度设计阶段，哪类机构可以进行认证，怎样确定该专业机构的专业资质和可信性，如何认证等问题有待后续立法加以明确。标准合同条款也还处于制定过程中。数据出境安全评估办法应细节明确，标准客观、一致，并考虑国际规则的合规问题（例如，应符合《关于进一步加强贸易政策合规工作的通知》的要求），避免造成歧视性后果。通过加强国内规制和国际经贸规则的协调，提高国内治理水平，营造良好的营商环境。在时机成熟时，我国可以发布跨境数据流动白皮书，以宣传阐释我国的跨境数据流动政策。我国并非反对跨境数据流动，也没有过于强调数据本地化，而是要求保障数据依法有序自由流动。

在对外协调方面，我国还可以依据GATS第7条，与相关国家就数据保护标准进行互相承认的谈判并

〔80〕 例如，《地图管理条例》第34条规定，“互联网地图服务单位应当将存放地图数据的服务器设在中国境内”。根据《网络出版服务管理规定》第8条，图书、音像、电子、报纸、期刊出版单位从事网络出版服务，必须将相关服务器和存储设备存放在中国境内。

〔81〕 相关分析可参见谭观福：《数字贸易规制的免责例外》，载《河北法学》2021年第6期。

〔82〕 徐程锦：《中国能否接受CPTPP版本跨境数据流动规则》，载微信公众号“顾小徐的随笔”，https://mp.weixin.qq.com/s/Fe2ZT8gMg0_s0vqyfZFsfg，访问时间：2022年4月25日。

签订数据出境的相关协议,以促进跨境数据流动。我国可以借鉴美国和欧盟在处理跨境数据流动问题上的经验,从双边层面开始探索。我国还应尽快加入APEC的《跨境隐私规则体系》,以提升数据传输便利性。〔83〕从欧盟对跨境数据流动的规制历史来看,建构跨境数据流动的全面机制是一个长期动态调整的过程。开展个人数据跨境流动的国际合作需要以基本的政治互信为基础。欧盟委员会在批准个人数据保护的充分性认定资格时,一国的人权和法治状况是其评估的重要因素。〔84〕欧盟的对外贸易政策是欧盟对外人权政策发挥作用的主要领域。为全面贯彻人权主流化目标,欧盟不断强化贸易与人权的联结。〔85〕鉴于欧盟和我国在人权等关键价值观上仍存在一定的分歧,我国和欧盟如果就个人数据保护的充分性认定展开谈判,将面临一定的障碍。

Regulation of Cross-Border Data Flows in Digital Trade through International Law

Tan Guanfu

Abstract: Cross-border data flow is the prerequisite for digital trade, but is faced with divergent regulations in different countries, and is hard to be coordinated. Currently, it is facilitated through some arrangements under the framework of WTO that promote the liberalization of digital trade infrastructures. It is also regulated through the newly concluded FTAs, which have established a relatively freer legal framework by adopting a regulatory model of "principle plus exception." The FTAs have also set down special rules for cross-border flow of particular data, including the rules for protecting personal data and for opening government data. Thus, the WTO members may negotiate a basic framework for data protection within the multilateral trading system, or they may also coordinate national standards for personal data protection through the mutual recognition mechanism under article 7 of GATS, and strengthen their cooperation with APEC or OECD. China, having sticked to risk control in the regulation of cross-border data flows, has formed a basic top-level regulatory framework that rate and classify data. Such a framework, though geared to international rules, still needs to be further improved through legislations and establishment of relevant standards, and be coordinated with that of the other countries.

Keywords: digital trade; cross-border data flows; international law; WTO; FTA

(责任编辑:倪鑫煜)

〔83〕 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33—35页。

〔84〕 杨莅敏:《全球跨境数据流动国际规则及立法趋势观察和思考》,载CAICT互联网法律研究中心网站, https://www.secrss.com/articles/13744,访问时间:2022年4月25日。

〔85〕 蒋小红:《贸易与人权的联结——试论欧盟对外贸易政策中的人权目标》,载《欧洲研究》2016年第5期,第79页。