全球数据跨境流动规则全景图

Global Cross-border Data Flows Rules Panorama

商务部国际贸易经济合作研究院

上海数据交易所

版权声明

编写组（排名不分先后）

林梓瀚、杜国臣、林丽颖、王荣、马有梅、杨辉

编写单位（排名不分先后）

商务部国际贸易经济合作研究院

中国图书进出口（集团）总公司

上海数据交易所

目录
Contents

报告要点

当前，数据跨境流动正在逐步超过贸易、投资全球化，成为驱动全球经济增长的新动能。本次报告，从国际组织、国际贸易协定、经济体三个层次切入，聚焦十大国际机制安排（五个国际组织与五个国际贸易协定）与十二大经济体，分析其关于数据跨境流动的规则与特点，并研判未来规则发展趋势，为我国参与全球数字经济规则的制定提供借鉴与参考。

研究发现，在国际组织层面，主要国际组织在全球层面推动数据跨境流动“软法”的构建，典型的如联合国（UN）建立数据跨境流动国际合作平台，经合组织（OECD）首创有关数据跨境流动与个人数据和隐私保护的基本原则，世界贸易组织（WTO）在电子商务谈判中推动数据跨境流动议题讨论等。在区域及双边框架层面，主要经济体通过加入或缔结区域或双边自贸协定及数字经济专项协定，如《美墨加协定》（USMCA）、《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《区域全面经济伙伴关系协定》（RCEP）、《数字经济伙伴关系协定》(DEPA)等，将数据跨境流动相关条款纳入相关协定中，旨在破除各国间数据跨境流动壁垒，促进全球数据自由流动。在主要经济体层面，包括中国、美国、欧盟、英国、韩国、印度、巴西、俄罗斯、澳大利亚、新加坡、日本等，出于维护自身数据安全的必要，纷纷进行立法规制，明确数据出境安全前提。

纵观纳入研究的十大国际机制安排与十二大经济体，发现在国际组织“软法”的影响下，国际贸易协议、主要经济体演变出其有关数据跨境流动规则的独有特点。本次报告将上述关于数据跨境流动规则的安排划分为三种类型，分别为开放进取型、严格监管型以及监管例外型。开放流动型主要表现为强调数据跨境的自由流动，典型的经济体如新加坡、东盟、美国等，国际经贸协定如 DEPA、USMCA 等。严格监管型主要强调数据跨境的事前监管，通过安全要求后方可进行数据出境，典型的代表为中国、俄罗斯、巴西等，国际贸易协定主要为 RCEP 等。监管例外型虽然强调数据跨境的监管，但是如若在白名单或者生态机制内则可以享有“监管例外”的权利。

未来，各国数据跨境流动的规则主张愈发倾向于“数据重商主义”，不过随着数据要素重要性的提升，未来数据跨境流动的规则亦会呈现出行业精细化的趋势等，同时数据主权、数据安全与个人隐私依然是数据跨境流动规则制定时关键考量。基于现有趋势，认为未来我国数字企业出海将面临更多的数据合规风险，我国数字贸易面临较高的政策不确定性，同时我国数字产业发展面临的数据壁垒有可能将继续提升等。因此，建议我国继续加强与 CPTPP、DEPA 等国际经贸规则的对接，并对 CPTPP、DEPA 中有关数据跨境流动的创新机制率先在上海等地进行探索试验，如 DEPA 中的监管沙盒机制、数字身份、数据保护可信任标志等。

一、数据跨境流动对经济全球化的影响

（一）数据跨境流动成为全球增长新动能

数据跨境流动是信息、知识、要素、商品的全球流动、传播与共享，数据跨境流动正在逐步超过贸易、投资全球化，成为驱动全球经济增长的新动能。长期以来，国际贸易和跨国投资一直充当了推动全球化快速发展的重要力量，全球贸易总额占 GDP 比重从 1986 年的 33.98%上升至 2006 年的 57.21%；其中，货物贸易总额占 GDP 比重从 28.63%上升到 47.29%。而 2008 年经济危机后，这种趋势出现逆转，全球贸易增速一直慢于全球 GDP 的增速，全球外国直接投资（FDI）也始终增长乏力。近年来受中美贸易战、俄乌冲突等影响，全球贸易增长速度放缓，全球直接投资流量下降。根据世界贸易组织（WTO）2023 年 4 月发布的《贸易统计与展望》，全球货物贸易量继 2022 年增长 2.7%之后，2023 年预计将增长 1.7%，最新预测进一步调低，预计 2023 年世界商品贸易量增长 0.8%。根据联合国贸发会议（UNCTAD）发布的《世界投资报告》，2022 年全球外国直接投资(FDI)流量下降了 12%，下降至 1.3 万亿美元。与之形成鲜明对比的是，全球数据流动对全球经济增长的贡献却显著增强。根据麦肯锡的研究报告，早在 2014 年，数据流动直接创造的价值就高达 2.8 万亿美元，预计到 2025 年，数据跨境流动对全球 GDP 的贡献价值将达到 11 万亿美元。“数字全球化”的作用日益超过贸易和投资全球化，数据跨境流动的重要性愈发凸显。此外，数据跨境流动将创造更加高效的全球市场，进一步降低全球化的参与门槛，全球化的包容性将进一步增强。如果说 20 世纪全球化是以贸易和投资的全球化为主要特征，那么 21 世纪的全球化将以数据跨境流动为主要驱动力量。

（二）数据跨境流动推动投资结构新变化

数据要素的重要性日益凸显，国际投资区位选择的决定因素发生变化，数字平台型跨国公司快速增长，推动国际投资发生结构性变化。一是数据成为新的生产要素，土地、人力和资金等传统生产要素的投资区位决定作用相对下降。在数字跨国公司的对外投资中，数据资源是否丰富、数字技术是否先进、数字基础设施是否完善、数据跨境流动是否便利成为跨国公司国际投资区位选择的重要因素，对国际投资流动的方向发挥着日益重要的作用。

二是数字跨国公司快速增长，数字跨国公司的平台化特征日益明显。根据 UNCTAD 发布的《2021 年数字跨国企业 TOP100》，自 2016 年以来，数字 100 强跨国公司的海外投资、海外销售、总利润持续上升。据普华永道(PwC)“2023 全球市值 100 强上市公司”排行榜显示，2023 年全球市值排名前 10 位公司中，数字平台型跨国公司占据了 7 位（苹果、微软、谷歌、亚马逊、英伟达、特斯拉、脸书），数字平台型跨国公司日益成为国际投资的主体。

表 1 “2023 年全球市值 100 强上市公司”排行榜（前十位）

排名	公司	总部所在地	领域
1	苹果(APPLE INC)	美国	信息技术
2	微软(MICROSOFT CORP)	美国	信息技术
3	沙特阿美(Saudi Arabian Oil Company)	沙特	能源
4	ALPHABET INC(谷歌母公司)	美国	通信服务
5	亚马逊(AMAZON.COM INC)	美国	非必需消费品

排名	公司	总部所在地	领域
6	英伟达(NVIDIA CORP)	美国	信息技术
7	伯克希尔(Berkshire Hathaway Inc.)	美国	金融
8	特斯拉(TESLA INC)	美国	非必须消费品
9	META PLATFORMS(脸书母公司)	美国	通信服务
10	维萨(Visa Inc)	美国	金融

资料来源：普华永道(PwC)“2023 全球市值 100 强上市公司”排行榜

三是数字跨国公司的国际投资模式发生显著变化，呈现出轻资产、低就业海外布局的特征。数字跨国公司通过在线平台市场而非商业实体进行海外销售，依托平台的数据和算法优势，通过复制其贸易模式为加快轻资产海外布局。据调研，中国跨境电商独角兽企业希音（Shein）布局海外 150 多个国家，年销售额约 300 亿美元，其海外员工总数仅有 6000 多名。据 UNCTAD 发布的《2021 年数字跨国企业 TOP100》，相较于传统跨国公司，数字跨国公司海外销售额与海外资产的比值更高，尤其是纯平台型公司及数字解决方案提供商[1]，该指标是传统跨国公司的 2 倍多，表明数字跨国公司以较少的海外资产实现了较大比例的海外销售。

（三）数据跨境流动重塑国际贸易新形态

数字时代的每一笔国际贸易都依赖数据跨境流动，数据跨境自由流动是开展数字贸易的基本前提条件。根据经合组织（OECD）、世界贸易组织（WTO）、国际货币基金组织（IMF）等国际组织对数字贸易的概念界定，从交易方式上分，数字贸易可以分为数字订购和数字交付的贸易，既包含以货物为载体的跨境电商，也包含以服务为载体的数字服务贸易，无论是跨境电商还是数字服务贸易，数字贸易的开展都离不开海量的数据跨境流动。根据交易方式的差异，广义的数字贸易可分为数字订购型(digitally ordered)、平台支持型(platform enabled)、数字交付型(digitally delivered)。其中，以数字形式订购的跨境交易指直接通过专门用于接收或下订单的计算机网络进行的商品或服务交易，其支付环节及货物或服务的交付通过线上或线下完成均可。该模式不包括以电话、传真等形式达成的交易，仅覆盖通过网页、外部网、电子数据交换达成的交易。平台支持型数字贸易指间接通过中介平台进行的商业交易，中介平台为供应商提供设施和服务，但不直接销售商品，例如阿里巴巴、亚马逊、淘宝、京东商城等。数字交付型数字贸易指直接通过信息及通信技术网络远程提供的服务产品，包括可下载的软件、电子书、电子游戏、流媒体视频、数据服务等，但不包括有形货物的交付。

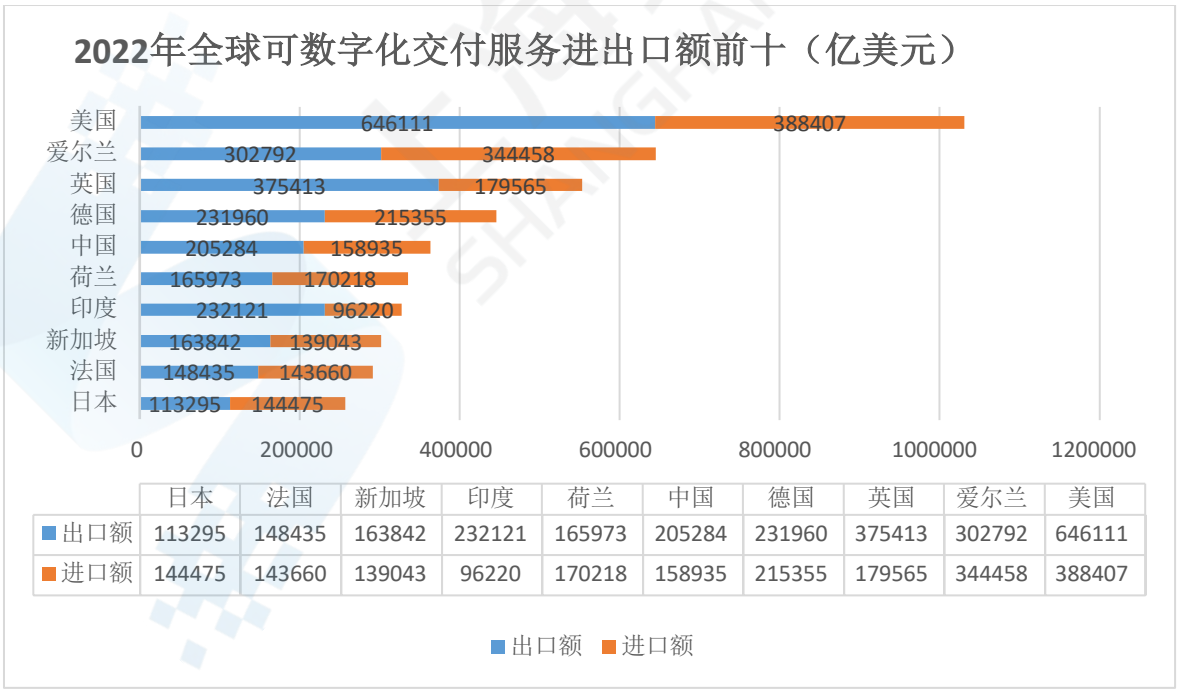
正如美国学者马修·斯劳特(Matthew J. Slaughter)和大卫·麦考密克(David H. McCormick)所说，当今的国际贸易是关于数据的“永动机”，贸易的过程消耗数据、处理数据、分析数据，又源源不断产生海量新数据，而云计算、5G 等技术又为大数据的存储、计算和快速处理提供了技术支撑。

国际贸易由跨国公司主导的大宗贸易模式转向数字平台主导的个性化、分散化数字订购模式，以货物、服务为载体的数字订购模式的数字贸易依托数字平台和数据跨境流动。跨境电商等贸易新业态兴起并成为国

[1] 榜单将数字跨国公司分为互联网平台（包括搜索引擎、社交网络、其他共享经济类平台）、数字解决方案（包括电子支付、数字金融、软件提供商、其他数字解决方案提供商）、电子商务（物流、互联网零售、其他电商）、数字内容（数字媒体、游戏、信息和数据）四类。

际贸易增长的新引擎，中小微企业甚至个人通过跨境电商平台和线上支付方式参与国际贸易，平台在国际贸易中发挥越来越重要的作用。2022 年，我国跨境电商进出口规模突破 2 万亿元，五年增长了近 10 倍，跨境电商主体超 10 万家，跨境电商贸易伙伴遍布全球，涌现出了阿里速卖通、Shein、Temu 等一批全球性数字平台企业，直连我国上万家中小微制造业企业与海外市场，高效组织供应链，带动数以万计的中小企业以数字化方式进入国际市场，重塑了我国贸易竞争新优势。

数据跨境流动支撑、拓展了可数字化交付的数字服务贸易增长，以服务为载体的数字交付模式的数字贸易依赖于数据跨境流动和数字技术的应用。跨境数据流动支撑、拓展了数字广告、数字营销、数字音乐、数字视频、游戏、动漫、软件研发、远程医疗、在线教育等数字服务贸易发展，5G、人工智能、大数据等数字技术的应用提高了服务的可贸易性。根据 UNCTAD 测算数据，2022 年全球可数字化交付服务出口额 3.94 万亿美元，在全球服务出口占比达到 55.3%。其中，发达经济体占主导优势，2022 年可数字化交付服务出口 3 万亿美元，占全球市场份额的 76.1%。发展中经济体可数字化交付服务出口 9460 亿美元，同比增长 12.6%，占全球市场份额的 22.1%。2022 年，我国可数字化交付的服务进出口额达到 2.51 万亿元，同比增长 7.8%，居全球第五位。其中，可数字化交付的服务出口 1.42 万亿元，同比增长 12.2%，我国数字交付的服务组织国际竞争力稳步提升，Tiktok 等社交媒体平台风靡全球。但总体而言，虽然我国数字服务贸易增长较快，数字服务贸易占服务贸易的比重从 2011 年的 36.2%提升至 2022 年的 48.4%。但横向对比来看，与发达国家仍存在较大差距。美国、英国、日本等发达国家数字服务贸易占服务贸易的比重超过 70%，而中国只有 48%左右。



	日本	法国	新加坡	印度	荷兰	中国	德国	英国	爱尔兰	美国
出口额	113295	148435	163842	232121	165973	205284	231960	375413	302792	646111
进口额	144475	143660	139043	96220	170218	158935	215355	179565	344458	388407

图 1 2022 年全球可数字化交付的服务进出口总额前十

数据来源：UNCTAD

表 2 数字贸易的分类

交易方式	交易对象	说明及举例
数字订购	货物	货物类跨境电商
	服务	网上订票、分时租赁
数字交付	数字产品或内容	游戏、动漫、短视频、数字音乐、数字影视等
	数据服务	搜索引擎、社交平台、数字广告等
	ICT 服务	软件服务、大数据服务、云计算服务、区块链服务、工业互联网服务
	其他可数字化交付的服务	远程医疗、在线教育、数字金融与保险服务、专业技术服务
平台支持	货物或服务	通过中介平台进行的商业交易，中介平台为供应商提供设施和服务，但不直接销售商品，如阿里巴巴、亚马逊、淘宝、京东商城等。

资料来源:根据 OECD、WTO、IMF 对数字贸易的定义整理

（四）数据跨境流动重构国际经贸新规则

数据的特殊属性、全球贸易投资形态的改变以及各国利益的再分配要求形成具有新的国际共识的经贸规则体系。

数据的特殊属性要求形成新的国际经贸规则。现有国际经贸规则不能解决跨境数据流动中出现的新问题，关于数据的定价和权属的制度缺失。当前国际经贸规则体系以世界贸易组织（WTO）及前身《关税与贸易总协定》（GATT）为主体框架，其运行和治理的依据是以贸易类型（商品或服务贸易）、贸易额、贸易地点（来源地和目的地）为主的统计数据。如商品贸易相较服务贸易而言，受到更多贸易规则的约束，产品的原产地则决定了该产品将适用怎样的关税和贸易限制政策。而这套规则体系不能适用于跨境数据流动，首先，以跨境数据流动驱动的贸易过程中商品贸易和服务贸易难以区分开。例如通过跨境电商平台购买实物商品，这个过程还包含了营销、跨境支付结算、跨境物流等一系列服务，很难将商品贸易和服务贸易区分开。其次是数据的价值难以确定。如个人网购记录及浏览记录，这是从个人活动和行为中收集的原始数据，伴随着交易其他商品和服务而产生，数据本身并没有产生直接的经济价值，但是经过分析处理可以产生价值，第三是跨境数据流动的“地域”问题即数据主权的问题难以确定。传统贸易中商品或服务生产、消费每个环节所在地点都可以由一个国家领土范围所决定，而数据因为无形、开放的特征，难以用以前的规则（如原产地规则）来适用于跨境数据流动，例如跨国公司云存储的数据属于哪个国家，数据产生、数据存储和数据开发的国家不同该如何确定。

以数据跨境流动为支撑的跨境电商、数字服务贸易快速发展，新的数字贸易形态要求形成新的数字贸易规则。传统国际经贸规则包括货物、服务的市场准入、待遇、关税、贸易投资便利化、知识产权规则。而在数字贸易形态下，转变为数字市场准入、数字产品待遇、数字税收、数字贸易便利化、在线消费者保护等规则。此外，数字贸易高度依赖于数字技术、数据流动、网络和数字平台，催生一系列新兴议题。如在数字技

术领域，催生出源代码保护、加密 ICT 产品、人工智能、金融科技等新兴议题；在数据流动方面，催生出数据跨境流动、个人隐私保护、计算设施位置等议题；在信息网络方面，催生出互联网接入、网络安全等议题；在数字平台方面，催生出平台责任、数字平台竞争等议题。

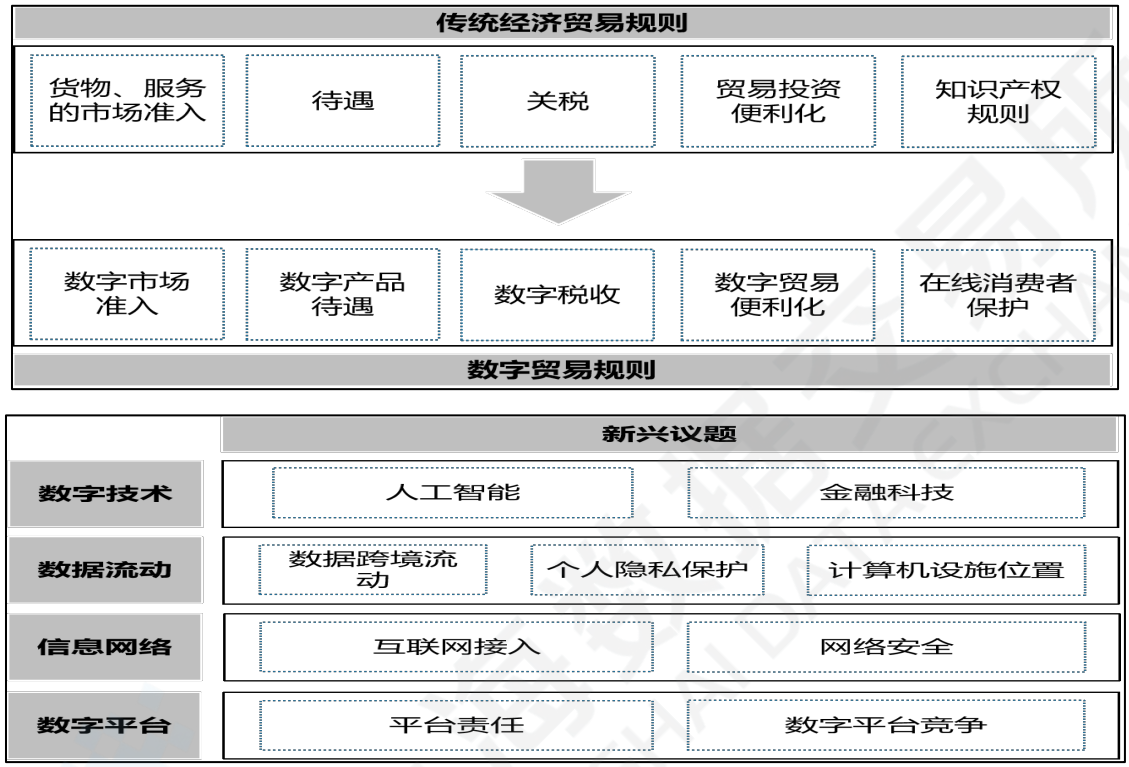


图 2 数字贸易规则主要议题

各国贸易利益的再分配必然导致国际贸易规则的再调整。数据跨境流动催生出以数据为关键要素的全球数据价值链，推动全球产业分工体系发生深刻变化，发达国家和发展中国家通过数据流动获益的能力存在显著差距，各国之间竞争合作的攻守利益因为技术和产业形态的变化而发生了根本性的改变，利益的再分配必然导致国际经贸规则的再调整。

（五）数据跨境流动催生全球数据价值链

数据跨境流动催生全球数据价值链，全球性数字平台在全球数据价值链中占据重要地位，各国在应用数据价值的能力方面差异巨大，拥有大型数字平台的国家通过数据价值链获益最多。数据价值链是以数据采集、存储、处理以及数据可视化等环节组成的价值链，其核心环节在于数据收集和处理能力并转化为数字智能，通过数据增值服务实现数据货币化，数据已经成为创造和捕获价值的新经济资源（UNCTAD，2019）。在传统贸易中，进出口产品的结构代表了一国的技术水平，出口产品的技能和技术含量的提高代表了国内附加值的增加，也表征着一国在全球价值链中的地位。而就跨境数据流动而言，在数据价值链的背景下，大多数发展中经济体是原始数据的出口国和增值数据产品的进口国，而那些拥有主要数据优势和处理原始数据能力更强的国家是原始数据的进口国和增值数据产品的出口国，位于数据价值链的中高端环节。

全球性的数字平台在全球数据价值链的各个环节中发挥日益重要的作用。一方面，大型数字平台以自身技术或服务换取来众多用户的海量原始数据，并借助网络效应、规模经济和范围经济，获得超强数据收集能力，并将原始数据转化为具有经济价值的数据产品。数字广告是数字平台实现数据盈利的主要方式之一，全球数字平台在数字广告市场的主导地位逐步增强，根据 eMarketer 数据，预计到 2022 年，数字广告支出预计将达到媒体广告支出总额的 60%，是 2013 年的两倍左右，前五大数字平台在数字广告总支出中所占份额预计将超过 70%。另一方面，全球性数字平台通过收购初创企业实现横向和纵向扩张，增强其在数据价值链中市场力量。如，处理海量数据的数字平台也越来越多地投资于人工智能（AI），而 AI 技术反过来又帮助平台企业更有效利用数据、改善用户体验并吸引新用户，进一步收集更多用户数据。从人工智能领域初创企业并购数来看，2016 年 1 月 1 日至 2021 年 1 月 22 日期间，共有 308 宗并购交易，价值 284 亿美元。按同期收购人工智能初创企业数量计算，全球排名前五的并购公司是美国的大型科技公司，其次是中国的百度（第六）和腾讯（第八）。其中苹果公司位居首位，谷歌和微软紧随其后。大型数字平台在人工智能方面的领导力将进一步增强其在全球数据价值链中的地位。

美国和中国参与全球数据价值链并从中受益的能力最强。根据 UNCATD 报告，中美两国拥有的超大规模数据中心约占全球 50%，两国的 5G 普及率最高，占全球初创人工智能企业融资总额的 94%，占世界顶尖人工智能研究人员的 70%，占全球最大数字平台市值的近 90%。中美两国的数字平台，如美国的苹果、微软、亚马逊、Alphabet(谷歌)、Facebook，和中国的腾讯和阿里巴巴，正越来越多地投资于全球数据价值链的每个环节。这些平台通过面向用户的平台服务进行数据收集；通过海底电缆和卫星进行数据传输；数据存储(数据中心)；以及通过人工智能等方式进行数据分析、处理和使用。这些数字巨头公司已经成为全球范围内的数据公司，拥有巨大的金融、市场和技术力量，并控制用户的大量数据。在疫情期间，这些公司的规模、利润、市场价值和主导地位进一步加强。例如，纽约证券交易所综合指数在 2019 年 10 月至 2021 年 1 月期间增长了 17%，但顶尖数字平台的股票价格的涨幅从 55%（Facebook）到 144%（苹果）不等。

二、国际组织推动数据跨境流动“软法”的构建

（一）UN 积极搭建数据治理国际合作平台

联合国发布《全球数字契约》推进数据跨境流动治理创新。2023 年 5 月，联合国发布《我们的共同议程政策简报 5:全球数字契约——为所有人创造开放、自由、安全的数字未来》（Our Common Agenda Policy Brief 5: A Global Digital Compact—an Open, Free and Secure Digital Future for All）。该简报建议制定一项《全球数字契约》，为推进开放、自由、安全、以人为本的数字未来制定原则、目标和行动，实现数字领域的可持续发展。在该简报中，联合国提出了迫切需要多利益相关方合作的八个重点领域，而数据保护和赋权是其中一个重点议题。

在数据保护和赋权方面，联合国建议制定多层次、可互操作的标准，以实现安全可靠的数据流动以及推动全球经济包容发展。该简报根据主体身份的不同，区分了成员国、区域组织和所有利益相关方应采取的行动措施。首先，对于成员国及区域组织，应注重法律对个人数据和隐私的强制保护，考虑通过一项关于数据的宣言以确保严格的数据驱动决策、互操作性和可移植性，防止行为操纵和歧视，通过全球数据契约,寻求数据治理原则共识。另外，对于所有利益相关方而言，应监控并执行通用定义和数据标准，加强人们对个人数据使用的影响和控制，由多利益攸关方制定全球数据契约。

中国就制定《全球数字契约》向联合国提交了相关意见，表明了坚持多边主义、坚守公平正义的数字治理立场。在数据保护方面，中方坚持以下观点。第一，应以事实为依据全面客观看待数据安全问题，促进数据依法有序自由流动；反对利用信息技术破坏他国关键基础设施或窃取重要数据，以及利用其从事危害他国国家安全和社会公共利益的行为。第二，各国应尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人调取位于他国的数据；各国如因打击犯罪等执法需要跨境调取数据，应通过司法协助渠道或其他相关多双边协议解决。国家间缔结跨境调取数据双边协议，不得侵犯第三国司法主权和数据安全。第三，信息技术产品和服务供应企业不得在产品和服务中设置后门，非法获取用户数据、控制或操纵用户系统和设备；产品供应方应承诺及时向合作伙伴及用户告知产品的安全缺陷或漏洞，并提出补救措施[2]。

联合国积极搭建数据治理国际合作平台。2006 年 11 月，联合国根据信息社会世界首脑峰会（WSIS）的决议，正式设立了联合国互联网治理论坛（Internet Governance Forum，简称 IGF）。该论坛致力于将集聚不同利益相关方，讨论与互联网相关的公共政策问题。2022 年 11 月 28 日至 12 月 2 日，第 17 届 IGF 召开，并集中讨论了《全球数字契约》中涉及到的五个重要主题。其中，在“数据治理和隐私保护”主题方面，会议认可了跨境数据流动对电子商务和数字贸易的重要性。同时，会议总结认为，有效的区域内贸易和供应链管理依赖于数据以及货物、服务和资本的顺畅流动，因此需要考虑复杂的交叉因素：监管的趋同性、法律框架的协调、互联网治理、信息和通信技术政策改革以及战略性区域基础设施实施。然而，目前多边、区域和双

[2] 《参见中国关于全球数字治理有关问题的立场》，http://newyork.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202305/t20230525_11083602.shtml，2023 年 10 月 23 日访问。

边贸易协定不能完全适用于当前和未来的跨境数据流动，国家法律制度之间几乎没有一致性，数据跨境流动都在基本不受监管的环境中运作。由于各国采用的方式不同，且各有背景，故容易造成贸易壁垒，许多国家目前没有足够的立法或执法能力。综上，制定和协调管理跨境数据流动的措施愈发必要。IGF 希望促进不同背景下的发展和经济价值创造，同时尊重国家主权和用户隐私[3]。2023 年 10 月 8 日至 12 日，第 18 届 IGF 在会议讨论中同样涉及了跨境数据流动有关内容。为了使数据效能促进发展，IGF 认为需要创建可信且安全的方法实现数据跨境共享。可信的数据自由流动现在被广泛讨论为国际数据管理和数据跨境流动的框架概念。需要制定原则和实际措施来发展“基于信任的数据自由流动”（Data Free Flow with Trust，以下简称“DFFT”）的概念，并为数据传输创建共同基础，以利用数据促进发展，同时解决各主体对数据隐私和数据主权的担忧。至关重要的是，发展中国家应充分参与有关跨界数据流动的讨论，反映他们的需要和关切。

此外，联合国还举办了联合国世界数据论坛（United Nations World Data Forum,简称“UNWDF”），至今已举办四届。UNWDF 以“可持续发展数据”为主题，是为落实“联合国可持续发展目标(简称 SDGs)”搭建的国际合作交流平台，旨在促进数据创新、培育伙伴关系、动员高级别政治、以及财政支持，为可持续发展建立更好的数据途径。2023 年 4 月 24 日至 27 日，第四届联合国世界数据论坛以“拥抱数据 共赢未来”为主题口号在杭州开幕。在《杭州宣言》中，联合国重申通过《数据战略》和《我们的共同议程》，为人类和地球建立更好的联合国数据生态系统和测度方法提出共同愿景，并呼吁利益攸关群体要加快行动，制定与《全球行动计划》相一致的数据管理方法。中国国家主席习近平向本届联合国数据论坛发贺信指出，中国愿同世界各国一道，在全球发展倡议框架下深化国际数据合作，以“数据之治”助力落实联合国 2030 年可持续发展议程，携手构建开放共赢的数据领域国际合作格局，促进各国共同发展进步[4]。

联合国多次发布政策研究报告推进数据治理。联合国近年来先后多次发布《数字经济报告》（Digital Economy Report）、《G20 成员国跨境数据流动规则》（G20 Members’ Regulations of Cross-Border Data Flows）等多份报告，从不同角度对各成员国的数字监管政策进行了调查，介绍了数据的多维性质以及各国相关政策和立法，讨论了多利益攸关方监管方法之间的共同点、差异和融合要素。联合国调查突出了跨境数据流动有关法律法规的多样性，认为目前成员国对跨境数据流动的监管存在不同政策，始终坚持力图促进成员国之间达成共识、建立协调的数据治理方法的立场[5]。

（二）WTO 电子商务谈判中关于数据跨境流动议题分歧较大

世界贸易组织(WTO)自 1995 年创立以来，为全球贸易自由化与便利化做出了突出贡献，是引领与制订多边贸易规则最重要的国际组织。早在 1998 年，WTO《电子商务工作计划》就开始启动关于电子商务议题

[3] See Addis Ababa IGF Messages, https://igf2022.intgovforum.org/en/content/igf-2022-outputs(last visited Oct. 24, 2023).

[4] 参见习近平向第四届联合国世界数据论坛致贺信，https://www.gov.cn/yaowen/2023-04/24/content_5752969.htm，2023 年 10 月 24 日访问。

[5] See Digital Economy Report 2021, https://unctad.org/publication/digital-economy-report-2021 (last visited Oct. 24, 2023)；G20 Members’ Regulations of Cross-Border Data Flows, https://unctad.org/publication/g20-members-regulations-cross-border-data-flows (last visited Oct. 24, 2023).

的讨论，早期侧重于对全球电子商务发展中出现的新议题的讨论，但并未取得实际进展。自 2015 年 12 月内罗毕部长级会议后，WTO 有关电子商务讨论的活跃度和参与度迅速上升，WTO 成员提交了大量电子商务提案和讨论文件，日本、新加坡、澳大利亚、加拿大、欧盟、美国、中国、俄罗斯、巴西等成员的提案数量较多。2017 年 12 月，在布宜诺斯艾利斯第十一次部长级会议（MC11）上，71 个 WTO 成员开创性发布了《电子商务联合声明》，推动 WTO 就贸易相关的电子商务议题进行谈判，这标志着 WTO 框架下关于电子商务问题探索由议题讨论进入了规则谈判的新阶段。2019 年 1 月，在瑞士达沃斯举行的电子商务非正式部长级会议上,包括中国在内的 76 个 WTO 成员发布了第二份《电子商务联合声明》，宣布正式启动与贸易相关的电子商务诸边谈判，号召更多成员国加入谈判，推进在现有协定和《电子商务联合声明》框架基础上构建高标准电子商务国际规则。截至 2020 年 12 月，共有 86 个 WTO 成员方加入电子商务谈判，贸易额占全球贸易总额比重超过 90%。2021 年 12 月，澳大利亚、日本和新加坡作为联合召集人发表联合声明，表明在电子签名和认证、在线消费者保护、未经请求的电子商业信息、开放政府数据、电子合同、透明度、无纸化交易以及互联网开放这 8 项条款的谈判中取得了实质性进展，同时将加强电子传输免关税、跨境数据流动、数据本地化、源代码、电子交易框架、网络安全、电子发票以及关于市场准入等领域加强谈判。2022 年 6 月，在 WTO 第十二届部长级会议（MC12）上，各方同意将电子传输临时免征关税的期限延长至下一届。此外，澳大利亚、日本和新加坡作为谈判的共同召集人发表联合声明，与瑞士一起启动电子商务能力建设框架，以加强数字包容性缩小数字鸿沟，帮助发展中国家和最不发达国家从数字经济发展中获益。该框架将提供广泛的技术援助、培训和能力建设，支持各国参与电子商务谈判。具体包括：成立一个新的数字咨询和贸易援助基金（DATA FUND）（澳大利亚和瑞士正在为该基金提供资金），日本通过日本国际协力事业团（JICA）和日本对外贸易组织（JETRO）提供数字能力建设支持，新加坡通过新加坡-WTO 第三国培训计划（TCTP）提供支持。2023 年 8 月，根据 WTO 电子商务谈判最新合并文本，目前 WTO 电子商务谈判的参与者基本就数字贸易便利化条款达成一致，但关于隐私和跨境数据流动、电子传输关税、数据本地化、源代码等议题分歧较大，谈判进展较为迟滞。

图 3 WTO 电子商务谈判演进

资料来源：根据公开资料整理

根据 WTO 电子商务谈判文本，WTO 电子商务谈判主要包括六个章节。第一节是电子商务便利化措施，主要包括电子交易便利化措施和数字贸易便利化，在电子交易便利化方面，包括电子交易框架、电子认证和电子签名、电子合同、电子发票和电子支付服务；在数字贸易便利化和物流方面，包括无纸化贸易、最低限度规则、海关程序、改善贸易政策、单一窗口数据交换和系统互操作性、物流服务、增强贸易促进、使用技术释放和清关货物、提供贸易促进和支持服务。第二节是开放与电子商务，主要包括非歧视待遇和责任、信息和数据流动、电子传输关税、以及互联网和数据访问，其中包括数据跨境流动，也是整个谈判最核心且分歧最大的议题。第三章是信任和电子商务，包括消费者保护、隐私以及商业信任，商业信任议题下就包含禁止将转让源代码或算法作为市场准入前提等议题。第四章是交叉领域的议题，包括透明度、国内监管与国际合作机制，网络安全，能力建设等议题。第五章是电信章节，包括更新 WTO 电信服务参考文件，以及与电子商务相关的网络设备和产品。第六章是市场准入，主要包括服务市场准入、与电子商务相关人员的暂时入境和逗留，以及商品市场的准入。

表 3 电子商务谈判的主要议题

A. 电子商务便利化措施
A.1 电子交易便利化措施：电子交易框架、电子认证和电子签名、电子合同、电子发票和电子支付服务。
A.2 数字贸易便利化和物流：无纸化贸易、最低限度、海关程序、改善贸易政策、单一窗口数据交换和系统互操作性、物流服务、增强贸易促进、使用技术释放和清关货物、提供贸易促进和支持服务。
B. 开放性和电子商务
B.1 非歧视和责任：数字产品的非歧视待遇、交互式计算机服务（限制责任）、交互式计算机服务（侵犯）。
B.2 信息与数据流动：跨境电子方式传输信息/跨境数据流动、计算设施位置、金融信息/覆盖金融服务供应商的金融计算设施位置
B.3 电子传输的关税
B.4 互联网和数据的访问：开放政府数据、开放互联网访问/有关电子商务的互联网访问和使用原则、在线平台访问/竞争
C. 信任和电子商务
C.1 消费者保护：在线消费者保护；未经请求的商业电子信息
C.2 隐私：个人信息保护；个人数据保护
C.3 商业信任：源代码；使用密码术的信息和通信技术产品
D. 交叉领域的议题
D.1 透明度、国内监管和合作：透明度；贸易相关信息的电子可用性；国内监管；合作；合作机制
D.2 网络安全
D.3 能力建设：能力建设和技术援助的选择
E. 电信
E.1 更新 WTO 电信服务参考文件：范围；定义；竞争保障；互连；普遍服务；许可和授权；电信监管机构；稀缺资源的分配和使用；基础设施；解决争端；透明
E.2 网络设备和产品：与电子商务相关的网络设备和产品
F. 市场准入
服务市场准入；与电子商务相关人员的暂时入境和逗留；商品市场准入

资料来源：根据 WTO 电子商务谈判最新发布的联合声明整理

数据跨境流动是 WTO 电子商务谈判中分歧较大的议题之一。2019 年 1 月,76 个 WTO 成员签署《电子商务联合声明》,确认启动与贸易有关的电子商务议题谈判,旨在制订电子商务/数字贸易领域的国际规则。在 WTO 电子商务谈判中，总共有 12 个成员的提案涉及数据跨境流动问题。此外，还有以中国为代表的一些成员，并未在提案中提及数据跨境流动，倾向于不将数据跨境流动列入谈判议程，而只将电子商务便利化相关议题纳入谈判议程。以成员对数据跨境流动的态度分类，可以分为三组。

以美国提案为代表，主张数据跨境自由流动，但近期美国贸易代表凯瑟琳·泰（Katherine Tai）在 WTO 谈判中放弃了数据跨境自由流动要求。2019 年由特朗普政府提出的美国提案中“通过电子方式进行的跨境信息转移”条款与《美墨加协定》第 19.11 条完全一致，体现了美国试图通过 WTO 谈判打破数据壁垒以维护其产业竞争优势的意图[6]。美国主张 WTO 成员之间不应对以商业为目的的数据跨境流动作出限制，但其提案支持设置合理例外条款。日本提案内容并未公开，通过相关文献和其之前提交的文件来看，其与美国立场基本一致[7]。新加坡和巴西提案基本沿袭 CPTPP 的规定，与美国、加拿大提案实质内容相同，但承认各成员在数据跨境流动方面的监管要求[8]。值得关注的是，2023 年 10 月 25 日，美国贸易代表凯瑟琳·泰（Katherine Tai）在 WTO 谈判中放弃了美国长期以来对数据跨境自由流动的要求，以便为国会提供调控、监管大型科技公司的空间。

以欧盟提案为代表，重视个人隐私和数据保护。欧盟在大方向上与美国持一致的立场，禁止成员通过四种方式限制跨境数据流动，包括要求使用本国计算设施处理数据，要求数据存储和处理本地化、禁止在其他成员境内存储或处理数据以及将使用本国计算设施或数据本地化作为允许数据流动的条件等[9]。但是，欧盟重视个人隐私和数据保护，并将其作为禁止限制跨境数据流动的例外情形，即“可以采取和维持其认为适当的保护措施，以确保对个人数据和隐私的保护，包括通过采取或适用个人数据的跨境传输规则”[10]。

[6] 石静霞：数字经济背景下的 WTO 电子商务诸边谈判：最新发展及焦点问题，p. 7

[7] 石静霞：数字经济背景下的 WTO 电子商务诸边谈判：最新发展及焦点问题，p. 5；〕WTO, Joint Statement on Electronic Commerce Initiative-Proposal for the Exploratory Work by Japan, INF/ECOM/4, 25 March 2019; 李墨丝: WTO 电子商务规则谈判：进展、分歧与进路；See WTO, Proposal for the Exploratory Work by Japan, Joint Statement on Electronic Commerce Initiative, JOB/GC/177 (INF/ECOM/4), 12 April 2018, pp.1-5; Communication from Japan, Joint Statement on Electronic Commerce Initiative, List of the Key Elements and Ideas on Electronic Commerce, JOB/GC/180 (INF/ECOM/7), 13 April 2018, pp. 1-2.

[8] 石静霞：数字经济背景下的 WTO 电子商务诸边谈判：最新发展及焦点问题，p. 7；WTO, Joint Statement on Electronic Commerce -Communication from Singapore -Text Proposal, INF/ECOM/25, 30 April 2019；WTO, Joint Statement on Electronic Commerce-Communication from Brazil, INF/ECOM/27, 30 April 2019.

[9] 石静霞：数字经济背景下的 WTO 电子商务诸边谈判：最新发展及焦点问题，p. 7；WTO, 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.

[10] 李墨丝：WTO 电子商务规则谈判：进展、分歧与进路，p. 9；WTO, Communication from the European Union, Joint Statement on Electronic Commerce - EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, INF/ECOM/22, 26 April 2019, para.2.8.2.

以中国提案为代表，不主张在 WTO 谈判中纳入数据跨境流动议题。中国在国内有关于数据跨境流动的法律规定，但在 WTO 谈判层面，中国、俄罗斯等国家回避该问题，基本谈判立场是以保障国家安全为前提，服务于网络强国的战略目标和数字经济发展的客观需要[11]。

（三）OECD 开创全球隐私保护和数据跨境流动规制的尝试

OECD 较早参与到隐私保护的全球规则探讨中。经济合作与发展组织（OECD，简称“经合组织”）最早于 1960 年由加拿大、美国及欧洲经济合作组织的成员国等 20 个初始国家成立，并签署《经济合作与发展组织公约》。由于信息技术、数据跨境流动与经济发展和国际经贸活动密不可分，而 OECD 的成员国均是科技和经济较为发达的国家，因此 OECD 也较早参与到隐私保护和数字经济发展的全球规则探讨中。OECD 最早于 1968 年在科学政策委员会下成立了计算机应用工作组(Group on Computer Utilization)，以调查计算机和通信等涉及的技术、经济和法律问题。1974 年 OECD 成立了资料库专门小组，考察计算机化的个人资料库涉及的政策问题。1977 年，工作小组召集政府、私人行业、国际资料传送网络的使用者、资料处理服务商和跨国组织的代表，召开跨境数据流动与隐私保护研讨会。1978 年，OECD 设立临时性的跨境数据障碍与隐私保护专家组，由其负责制定有关数据跨境流动与个人数据和隐私保护的基本原则，并促进与国内立法的融合。在充分研究讨论了与跨境数据流动和信息保护相关议题后，专家组于 1979 年提出了下述指南草案。OECD 于 1980 年发布《关于隐私保护与个人数据跨境流动指南》（以下简称“《OECD 隐私指南》”“《指南》”）（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data），并于 2013 年进行修订。此后，OECD 于 1985 年和 1998 年分别发布了“跨境数据流动宣言”（Declaration on Transborder Data Flows）（以下称“1985 宣言”）和“关于保护全球网络隐私的部长级宣言”（Declaration on the Protection of Privacy on Global Networks）（以下称“1998 宣言”），对数据跨境和隐私保护问题表明立场。

《OECD 隐私指南》是全球层面对数据跨境流动进行规制的首次尝试，也是全球个人信息保护法规的历史源头之一。《指南》明确了个人数据保护的八项基本原则，即限制收集、数据质量、目标明确、限制使用、安全保护、公开透明、个人参与以及问责，设定了个人信息保护的最低标准。《指南》确立了数据跨境流动的基本原则，即鼓励数据自由流动及对数据跨境流动的合法限制。《指南》针对数据跨境流动的规定集中于第四部分，其赋予成员国基于保护个人隐私对数据跨境流动采取合理限制的权力，但限制措施应尽量减少对数据自由流动的影响，不能超出必要限度，应当遵循比例原则，需要结合数据的类型、敏感程度、数据处理目的和范围等因素综合考量；《指南》明确数据跨境所带来的风险应当由数据控制者承担相应责任；《指南》规定了两种成员国应该避免设定数据跨境限制的具体情形，第一类是当其他国家已经充分的遵守了 OECD 的相关指南；第二类是数据传输目标国家已经具备了充足的安全防护，安全防护既包括强制执法机制也涵盖了数据控制者所采取的措施。

《OECD 隐私指南》成为全球各国及国际组织制定隐私保护与数据跨境制度的重要参考。《指南》虽然仅以指南形式制定，不具备强制效力。但 OECD 作为较早提出隐私保护制度的组织，以非强制方式为各国提供了包容各国不同情况的制度框架。一方面，《指南》成为 OECD 成员国制定国内个人数据保护法规的参

[11] WTO 电子商务规则谈判与中国的应对方案_徐程锦, p.10.

考。如 OECD 的成员国澳大利亚、新西兰、加拿大、韩国等在《指南》原则的基础上进行取舍和创新，纷纷开始加快国内个人数据保护的立法进程。另一方面，《指南》确立的八项基本原则还对许多非成员国国家、国际组织确立新的个人数据保护原则提供了指导。如欧洲委员会《个人数据自动处理中的个人保护公约》（简称《108 公约》）、亚太经合组织《APEC 隐私框架》中确立的隐私保护原则。

近年来，OECD 通过数字经济政策委员会（CDEP）及其数据治理和隐私工作小组(DGP)，致力于推动全球数据治理，促进数据跨境流动，发布了一系列关于数据跨境流动的建议和研究分析报告。OECD 对数据跨境流动的建议还包括：在隐私保护执法中开展跨境合作、增强数据访问和共享、加强数字安全等。

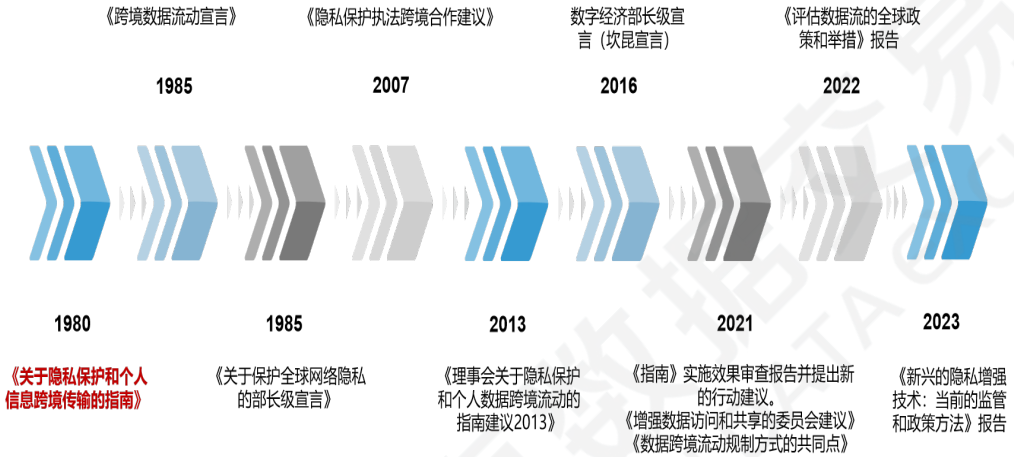


图 4 OECD 数据跨境流动相关的指南、建议及研究报告

资料来源：根据公开资料整理

OECD 及时总结全球前沿政策举措和规制方式。2021 年，OECD 发布《跨境数据转移的规制方式的共同点》（Mapping Commonalities In Regulatory Approaches To Cross-Border Data Transfers），该研究报告归纳总结了当前全球促进跨境数据流动的具体工具，并梳理了各种工具之内和之间的共同点，以帮助厘清跨境数据流动国际规制的现状，促进全球数据跨境流动。2022 年 10 月，OECD 发布《跨境数据流动——盘点关键政策和举措》（Cross-border Data Flows——Taking Stock of Key Policies and Initiatives），总结七国集团促进可信跨境数据流动的政策和举措。

根据 2021 年 OECD 发布的研究报告，可以将全球主流的规制数据跨境流动政策工具归纳为四类。一是单边机制，包括开放的保障机制和预先授权的保障机制。其中开放的保障机制不需要政府部门的事前审批，赋予私营部门更多自由裁量空间，如事后问责机制、合同、私营部门主导的充分性认定。而预先授权的保障机制需要政府部门的事前审批，如公共部门充分性认定和公共部门领导的事前保障机制，这两种方式都需要公共部门对另一司法辖区的隐私和数据保护水平进行评估，确保数据接收地的数据保护和执法水平与国内一致，单边的相关文本包括标准化的合同、有约束力的合同规则、或其他经批准的法律指令或计划（如行为准则、认证计划等）。OECD 对 46 个经济体使用的单边机制的统计显示，预先授权的保障机制是最常使用的单边机制。二是多边安排，多边安排往往通过区域组织来建立规则或达成共识，数据跨境数据流动的多边安排通常基于隐私和个人数据保护而制定。根据监管方式的可执行性，多边安排可以分为无约束力的多边安排和

有约束力的多边安排。无约束力的多边安排如《OECD 隐私指南》，通过设立具有共识的数据保护原则，提高成员国之间法律框架的互操作性，进而促进数据跨境流动的同时确保隐私保护。有约束力的多边安排如欧洲委员会的《108 号公约》和《108 号公约+》，国家承诺通过国内立法来对违反《公约》的行为进行制裁和救济。APEC 的 CBPR 系统也包含具有约束力的方面，当国家和公司均同意加入该系统时，公司需承担相应责任。多边安排中的原则和内容都逐步被成员国的国内立法所吸收，同一多边安排下各经济体的隐私和数据保护法规的重叠程度很高，如《108 号公约》成员国的监管条款重叠度高达 76%；《OECD 隐私指南》成员国的监管条款存在 71%重叠，而 APEC 系统的成员国由于多样性更强，因此其重叠程度相对较低为 68%。三是贸易协定及数字经济伙伴关系。由于 WTO 电子商务谈判中数据跨境流动等议题目前分歧仍然较大，各国探索通过自由贸易协定解决数据跨境流动问题。在目前的贸易协定中，按照对数据跨境流动的规制方式，可以分为三类：无约束力的数据跨境流动条款、有约束力的跨境数据流动条款，以及开放未来谈判的条款。协定大多规定不限制因商业活动而产生的数据跨境流动，但合法公共政策目标例外，且例外需要满足非歧视和必要原则。目前的自由贸易协定中的跨境数据流动规则越来越具有约束力，各国政府越来越倾向于利用贸易协定来实现促进数据跨境自由流动和保护隐私及其他公共政策目标双重目标。四是标准和技术工具。标准和技术工具通常由非政府和私营部门组织开发，以处理跨境数据流动带来的隐私和安全问题。标准工具包括，组织在监管数据跨境流动中保护隐私和安全的标准和原则，如 ISO 制定的与隐私和个人数据保护相关的标准；技术驱动工具指使用隐私增强技术（PETs），如密码学，可以用来防止或减少由于隐私和机密泄露所带来的风险；数据沙盒可以为加强数据控制和保护的能力。标准和技术驱动的规制工具是一个快速发展的领域，两者不互相排斥，公司既可以应用国际标准化组织（ISO）标准，也可以使用隐私增强技术来保护数据(有时后者是实现前者的一种手段)。虽然基于标准和技术的工具应用在组织层面，但提供标准和技术方面的示例可以帮助企业和组织选择合适的工具来建立基于信任的数据跨境流动。在 2022 年 OECD 发布的报告中，进一步将全球跨境流动的关键措施分为单边政策、政府间安排以及中介和组织措施，在技术和组织措施下，特别关注到数据空间、数据中介和隐私增强技术等举措。

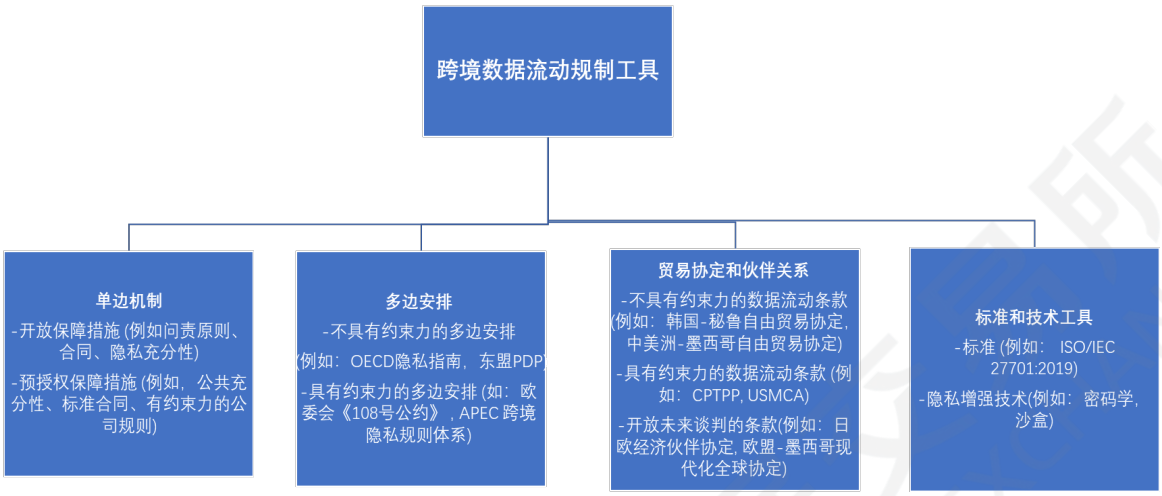


图 5 数据跨境流动的四种工具

资料来源：OECD《跨境数据转移的规制方式的共同点》，2021

图 6 可信跨境数据流动的主要政策及举措

资料来源：OECD 发布的《跨境数据流动——盘点关键政策和举措》

总体而言，OECD 是参与全球数据流动治理最主要的多边机制之一，多年来 OECD 通过理事会建议的形式，或以分析性研究的形式，致力于推动构建全球数据跨境流动的共同框架。其最早提出了全球隐私保护和数据跨境流动规制的原则，成为许多国家和贸易协定中制定规则的指南。近年来通过总结全球数据跨境流

动对全球数据跨境流动治理的弥补了各国监管体系和机构设置之间的差异性，促进了不同国家监管框架的一致性，增进了跨境数据流动各方间的信任。

（四）APEC 推动 CBPR 认证体系便利数据跨境流动

APEC 电子商务指导小组以《OECD 隐私指南》为蓝本，于 2005 年发布《APEC 隐私框架》（APEC Privacy Framework）。早在 1998 年，APEC 就成立了电子商务指导小组（Electronic Commerce Steering Group，简称“ECSG”），其任务之一是推动亚太统一的法律和政策环境构建。2005 年，ECSG 发布了《APEC 隐私框架》（APEC Privacy Framework），并于 2015 年对其进行了更新[12]。《APEC 隐私框架》以原则和实施指南为核心，继承了《OCED 隐私指南》中的基本原则，提出信息隐私九大原则，即避免伤害、通知、收集限制、个人信息的使用、选择性原则、个人信息的完整性、安全保护、查询及更正、问责制。《APEC 隐私框架》旨在促进亚太地区对隐私和个人信息保护措施的一致性，指导亚太地区数据跨境自由流动。

建立 CBPR 跨境隐私规则体系（Cross-Border Privacy Rules, 简称“CBPR”），形成一套由政府背书、自愿、可执行的数据隐私保护认证机制。2007 年，APEC 批准了数据隐私探路者倡议（APEC Data Privacy Pathfinder Initiative），建立数据隐私探路者（Data Privacy Pathfinder），以促进亚太地区负责任的数据跨境流动[13]。2011 年，APEC 21 个经济体首脑共同建立了 CBPR 体系。CBPR 是对《APEC 隐私框架》的具体实施，是由隐私执法机构、问责代理机构和企业三方共同参与的数据隐私认证。具体而言，成员政府支持该规则的实施，企业可以加入该认证，以证明自己遵守国际公认的数据隐私保护，并据此可以在特定地区收集、传输和利用信息资源。而问责代理机构则负责对认证企业的行为进行监督和处罚，主要由违规企业所在国的隐私执法机构对企业进行法律制裁[14] 。CBPR 体系目前已有美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、中国台北和菲律宾共 9 个经济体或地区加入。

在 CBPR 体系下，APEC 建立针对数据处理者的认证体系——数据处理者隐私识别（Privacy Recognition for Processors，以下简称“PRP”）体系。由于 CBPR 体系的规制目标对象是数据控制者，并不适用于数据处理者。APEC 成员经济体和数据控制者希望建立一套针对数据处理者的认证体系。2015 年，数据处理者隐私识别（PRP）体系应运而生。CBPR 联合监督小组（Joint Oversight Panel）根据 CBPR 体系框架，采用类似于 CBPR 认证中的评估手段对数据处理者进行评估。数据处理者通过 PRP 体系认证可以证明自身的数据处理至少符合 CBPR 体系对数据控制者的数据处理隐私保护要求。这也帮助了数据控制者识别和选择合格数据处理者。

CBPR 建立了隐私执法机构和问责代理机构来确保企业隐私保护水平符合国际公认标准。为保证加入该体系的成员经济体能够按照隐私框架的最低要求约束本国企业，CBPR 体系设定的准入条件是：申请国至少有一个隐私执法机构加入跨境隐私执法安排（Cross-border Privacy Enforcement Arrangement，简称“CPEA”）。

[12] See APEC Privacy Framework (2015), https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015) (last visited Jul. 25, 2023).

[13] See https://www.apec.org/about-us/about-apec/fact-sheets/apec-privacy-framework (last visited Jul. 25, 2023).

[14] See What is the Cross-Border Privacy Rules System, https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system (last visited Jul. 25, 2023).

成员经济体向 APEC 提出加入 CBPR 的申请后，联合督导组将对申请国已加入 CPEA 的隐私执法机构进行调查，确定该机构在国内切实拥有针对隐私框架九大原则 50 项具体要求的执法权力。该审核制度保证了凡是获准加入 CBPR 体系的成员经济体能够按照隐私框架的最低要求对本国企业进行执法，保证了 APEC 隐私框架在加入国的法律效力，而隐私框架也为协调亚太各国隐私保护政策提供了一个法律平台[15]。此外，CBPR 还通过问责代理机构来衡量加入国认证企业的隐私保护水平。当一个成员经济体获准加入 CBPR 体系后，该国还要至少有一个 APEC 认可的问责代理机构（Accountability Agent)为该体系提供服务。问责代理机构的职责是:证明企业制定的跨境隐私保护政策符合 APEC 隐私框架并为其认证，为消费者提供渠道解决其对企业的隐私保护投诉。使用问责代理机构是 CBPR 体系的一大关键创新。问责代理机构通过提供独立的第三方认证证实某组织的隐私政策和做法符合 APEC 隐私框架，从而在 CBPR 体系中发挥着不可或缺的作用[16]。

表 4 APEC 及 CBPR 体系介绍

APEC 隐私框架	CBPR
2005 年发布，2015 年更新	2011 年
以原则和实施指南为核心，继承了《OCED 隐私指南》中的基本原则，提出信息隐私九大原则，即避免伤害、通知、收集限制、个人信息的使用、选择性原则、个人信息的完整性、安全保护、查询及更正、问责制。	CBPR 是对《APEC 隐私框架》的具体实施，是由隐私执法机构、问责代理机构和企业三方共同参与的数据隐私认证。

资料来源：根据公开资料整理

（五）G20/G7 框架下“基于信任的数据自由流动”影响力不断提升

日本在 G20 框架下启动“大阪轨道”，首倡“基于信任的数据自由流动”（Data Free Flow with Trust，以下简称“DFFT”）。2019 年 1 月，日本首相安倍晋三在达沃斯世界经济论坛上首次提出 DFFT 概念。同年，在 G20 大阪峰会茨城筑波贸易和数字经济大臣会议上，作为阶段性成果文件的部长级声明就 DFFT 的实施，提出了“尊重国内和国际的法律框架”“合作以鼓励不同框架之间的互操作性”“确认数据在发展中的作用”的主张。在 G20 大阪峰会领导人数字经济特别会议上，成员国宣布启动“大阪轨道”，并签署《大阪数字经济宣言》，重申 DFFT，建立运行数据跨境自由流动的“数据流通圈”，强调要在更好保护个人信息、知识产权和网络安全的基础上，推动全球数据自由流通并制定可靠的规则。但 G20 成员国中的印度、印尼与南非没有在宣言上签字。2020 年，G20 利雅得领导人宣言承认有信任数据自由流动和跨境数据流动的重要性，并提出“进一步促进数据自由流动，加强消费者和企业的信任”。2021 年，G20 集团罗马领导人宣言继续承认 DFFT 的重要性，表示“继续促进共识，努力确定现有监管方法和工具之间共同点、互补性，使数据能够信任地流动，以促进未来的互操作性”。

[15] 弓永钦,王健.APEC 跨境隐私规则体系与我国的对策[J].国际贸易,2014(03):31.

[16] 弓永钦,王健.APEC 跨境隐私规则体系与我国的对策[J].国际贸易,2014(03):31-32.

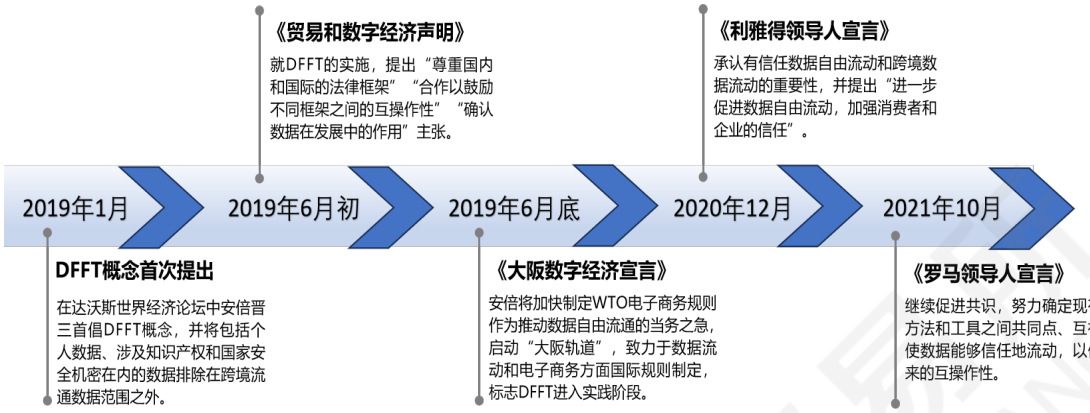


图 7 G20 框架下 DFFT 提出和演进过程

资料来源：根据公开资料整理

借助 G7 平台，DFFT 概念的推广和实施不断深化，影响力不断提升。由于 G20 成员国印度、印度尼西亚和南非拒绝加入“大阪轨道”倡议，日本继而选择缩小平台，在不包含新兴和发展中经济体的 G7 框架下推广和实施 DFFT。2021 年，G7 数字轨道和贸易轨道致力于 DFFT 问题的探索，在 4 月份的数字技术部长会议中，通过《DFFT 合作路线图》，内容包括数据本地化、监管合作、值得信赖的政府访问数据和优先领域的数据共享四个关键领域。强调释放数据在经济和社会力量中的重要性，试图利用“志同道合、民主、开放和外向型国家的共同价值观来支持一个工作计划，旨在实现数据自由流动和信任带来的益处”。同时，在 G7 贸易部长制定的数字贸易原则中强调了关于建立一个开放数字市场和基于信任的跨境数据自由流动的相关内容。在 2022 年德国担任 G7 轮值主席国期间，数字技术部长会议通过《促进 DFFT 行动计划》，行动计划重申了四个合作领域，表示致力于加强 DFFT 的证据基础，建立共同点，促进未来数字监管的互操作性、在数字贸易背景下促进 DFFT 以及分享有关“国际数据空间”（一种新兴互操作数据共享架构）建设构想等。2023 年 4 月在日本举行的数字技术部长会议则提出了更为详细的《DFFT 实施计划》，划定了 DFFT 落地的五项行动，即加强 DFFT 的证据基础并深入了解现有监管方法和工具，基于现有监管方法和工具促进可操作性，继续监管合作支持 G7 政策官员和监管机构之间的对话，在数字贸易的背景下推动 DFFT，以及共享关于国际数据空间前景的知识。宣言的附件中还涵盖了 DFFT 实施的更详细信息，包括从政策、工具、技术、法律层面促进 DFFT 具体实施，如开发兼容的政策、工具，增强隐私技术的研发，注重 DFFT 法律实践相关的探讨（模板合同条款和认证机制，国际隐私框架等）。此外，日本还寻求就 DFFT 建立专门平台支持，并启动“DFFT 伙伴关系机制性安排”（Institutional Arrangement for Partnership on DFFT，IAP）。日本希望在经合组织等国际组织的框架下，围绕 DFFT 成立秘书处以建立讨论、制定全球数据治理规则和框架的专门场合，并已启动“DFFT 伙伴关系机制性安排”，以促进更强有力的规则落实。

2022 年 G7 数据保护和隐私机构圆桌会议发表题为《通过信任和知识共享促进数据自由流动：国际数据空间的未来前景》的公报，突出强调个人隐私增强技术（Privacy-enhancing Technologies，PETs）对跨境数据流动的显著贡献。其应用不仅有助于确保数据共享的安全性和合法性，为数据跨境流动提供有力支持，还为

跨国创新者、政府部门以及广大公众提供了重大利益。因此，G7 数据保护和隐私机构将积极寻求推动 PETs 的创新应用，以确保跨境数据流动在安全、高效和可持续的基础上发展，促使国际数据空间的进一步发展。

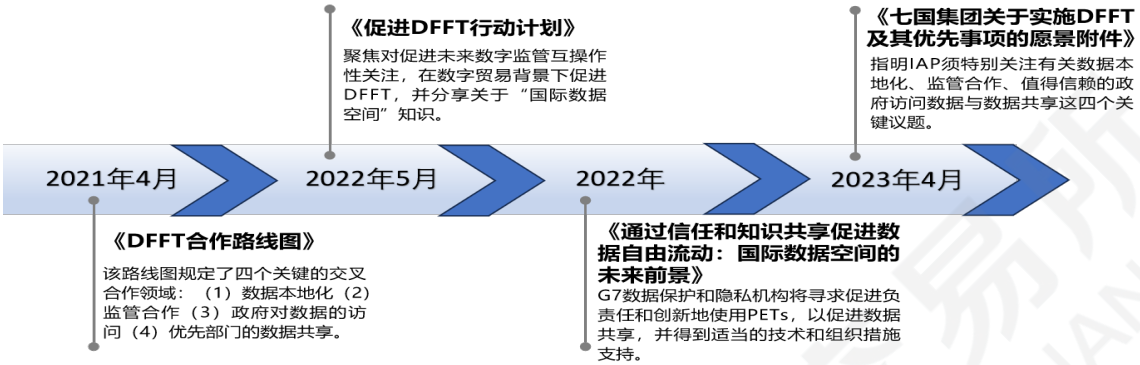


图 8 G7 框架下 DFFT 推进过程

资料来源：根据公开资料整理

总体而言，DFFT 在 G20 框架下由日本主导提出，在 G7 框架下不断发展并扩大其规则影响力，未来 OECD、G20 等国际组织可能进一步积极响应该倡议，并利用多边机制的广泛影响力，迅速达成相关协议，形成基于信任的数据自由流通圈。

三、国际贸易协定破除数据跨境流动壁垒

在区域及双边框架下，各国通过加入或缔结区域或双边自贸协定及数字经济专项协定，并在协定中纳入数据跨境流动相关条款，旨在破除各国间数据跨境流动壁垒，促进全球数据自由流动。目前纳入数据跨境流动相关议题的区域及双边贸易协定主要包括《美墨加协定》（USMCA）、《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《区域全面经济伙伴关系协定》（RCEP）等为代表的区域或双边自贸协定，以及以《美日数字贸易协定》（UJDTA）、《数字经济伙伴关系协定》（新加坡-智利-新西兰，DEPA）、《新加坡-澳大利亚数字经济伙伴关系协定》（SADEA）、《韩国-新加坡数字经济伙伴关系协定》（KSDPA）为代表的数字经济专项协定，相关议题主要包括“个人信息保护”、“通过电子方式跨境传输信息”、“计算设施的位置”等三类条款。同时，人工智能、5G、区块链等技术的发展推动全球数字经贸的相关议题与规则不断进行调整，全球经济体开始围绕新技术在数字贸易协定中打造新兴的规则。除数据跨境自由流动与数据存储本地化等传统原则性条款外，DEPA 等协定新加入了人工智能、开放政府数据、数字身份、数据监管沙盒等创新性条款。

在个人信息保护议题下，由于个人信息保护是制约数据跨境流动的主要因素之一，主要贸易协定均要求各缔约方在考虑国际组织关于个人隐私保护原则和指南的基础上，设立个人信息保护法律框架，基于非歧视原则为境外个人信息提供境内保护。此外，由于各缔约方可能采取不同的法律方式保护个人信息，各国个人信息保护制度的不兼容、不互认将限制数据跨境流动，因此，主要贸易协定均鼓励各缔约方建立促进各国个人信息保护制度兼容性和可互操作性的机制，便利跨境信息传输。

在“通过电子方式跨境传输信息”及“计算设施位置”议题下，目前主要区域及双边自贸协定基本采取“鼓励数据自由流动/禁止计算设施本地化+合法公共政策目标例外”的框架，即不得限制或禁止商业活动中的跨境数据流动、不得将计算设施本地化作为市场准入的条件，但可以为实现合理的公共政策目标实施例外措施，前提是例外措施不得构成歧视和变相贸易限制或超过必要限度（即限制措施需满足非歧视性和必要性原则），各协定对例外条款的限制程度有所不同。

不同

表 5 现有国际贸易协定中数据跨境流动相关议题

议题	CPTPP	USMCA	UJDTA	RCEP	DEPA	SADEA	KSDPA
个人信息保护	第 14.8 条	第 19.8 条	第 15 条	第 12.8 条	第 4.2 条	第 17 条	第 14.17 条
通过电子方式跨境传输信息	第 14.11 条	第 19.11 条+第 17.17 条金融章节	第 11 条	第 12.15 条	第 4.3 条	第 23 条	第 14.14 条
计算设施的位置	第 14.13 条	第 19.12 条+第 17.18 条金融章节	第 12 条	第 12.14 条	第 4.4 条	第 24 条	第 14.14 条、第 14.15 条

议题	CPTPP	USMCA	UJDTA	RCEP	DEPA	SADEA	KSDPA
争端解决	适用，部分给予马来西亚和越南 2 年过渡期	适用	不包含争端解决专章	不适用争端解决机制	适用	适用	适用

资料来源：作者根据协定内容自行整理

本次报告从贸易协定涵盖缔约国的广度、协定的国际影响力、相关条款的创新性三个维度综合考虑，最终选取 CPTPP、RCEP、DEPA、USMAC、UJDTA 等五个贸易或数字经济协定为代表，梳理各协定的历史演进过程，分析各协定中数据跨境流动相关条款，探寻各国通过加入或缔结贸易协定，如何在平衡国内监管要求的同时，破除数据跨境流动壁垒，以促进区域内的数据跨境自由流动。

（一）CPTPP 鼓励建立缔约国规则互操作机制

CPTPP 的前身是《跨太平洋伙伴关系协定》（TPP）。TPP 是自 2002 年开始酝酿的多边自由贸易协定，由新西兰、新加坡、智利和文莱四国基于《跨太平洋战略经济伙伴关系协议》（P4）率先发起。美国于 2008 年谈判加入 TPP，自此美国开始占据领导位置，发挥主导作用。2015 年，美国、日本及加拿大等 12 个国家达成 TPP，但未得到所有成员国立法部门的批准。2017 年，美国总统特朗普在就任当天正式宣布美国退出 TPP，称退出 TPP 有利于保护美国工人权益[17]。美国的退出增加了 TPP 的不确定性。为推动协议生效，日本与加拿大、新加坡、新西兰等其余十个国家，对协定内容进行了新的讨论，并签订新的自由贸易协定，新名称为 CPTPP。各方经过多轮磋商，于 2018 年 1 月完成 CPTPP 谈判，并于 3 月 8 日在智利举行新协定的签署仪式，CPTPP 最终于 2018 年 12 月 30 日正式生效[18]。2023 年 7 月 16 日，英国正式被批准加入 CPTPP，成为其生效以来第一次扩容的国家，也成为第一个加入 CPTPP 的欧洲国家。

目前中国正在全面推进加入 CPTPP 的议程。2020 年 11 月 20 日，习近平主席以视频方式出席亚太经合组织（APEC）领导人非正式会议并发表重要讲话。宣布“中方将积极考虑加入全面与进步跨太平洋伙伴关系协定”[19]。2021 年 9 月，中国商务部部长王文涛向 CPTPP 保存方新西兰贸易与出口增长部部长奥康纳提交了中国正式申请加入 CPTPP 的书面信函。在近期举行的商务部记者会上，商务部新闻发言人表示，目前我国已对 CPTPP 全部条款进行深入全面的分析、研究和评估，梳理可能需要采取的改革举措和修改的法律法规，并在有条件的自贸试验区和海南自贸港主动对照先行先试，我国正在全面推进加入 CPTPP 议程，以更大力度改革推进更高水平开放。

[17] 越南工贸部部长：11 国就跨太平洋伙伴关系协定达成框架协议[N]. 澎湃新闻, 2017.
[18] CPTPP：中国大步迈向全球化的阶梯[N]. 澎湃新闻, 2019.
[19] 第一观察 | 首次！习主席说中国将积极考虑加入这个协定[N]. 新华网, 2020.

CPTPP 是全球范围内较早生效的包含数字贸易规则的多边协定。CPTPP 在第 14 章节集中规定了数字贸易相关规则，其中关于数据跨境流动的三个核心条款为个人信息保护（第 14.8 条）、通过电子方式跨境传输信息（第 14.11 条）和计算设施的位置（第 14.13 条）。

在“个人信息保护”议题下，CPTPP 要求各缔约方在考虑国际组织关于个人隐私保护原则的基础上，建立个人信息保护法律框架，基于非歧视原则为境外个人信息提供保护。此外，由于各缔约方可能采取不同的法律方式保护个人信息，各国个人信息保护制度的不兼容、不互认将限制数据跨境流动，因此 CPTPP 鼓励建立促进各国个人信息保护制度兼容性和可互操作性的机制，包括对监管结果的互认、共同安排、更广泛的国际框架等，以便利数据跨境传输。

在“通过电子方式传输信息”议题下，CPTPP 采取了“鼓励数据跨境流动+合法公共政策目标例外”的基本框架。首先，CPTPP 肯定各国对跨境信息传输监管的权力，即各成员国有权设置不同的数据跨境传输监管要求。其次，CPTPP 要求数据跨境自由流动，但可以为实现合法公共政策目标对跨境数据流动实施限制，但该限制措施不能构成歧视或变相贸易限制，且不得超过必要限度（即限制措施需满足非歧视性和必要性原则）。

在“计算设施位置”议题下，CPTPP 采取了“禁止计算设施本地化+合法公共政策目标例外”的基本框架。首先，CPTPP 认可成员国基于通信机密和安全的需求，对其境内计算设施的使用具有监管权力。其次，CPTPP 要求各缔约方不得将计算设施本地化作为在其领土内开展业务的前提条件，但可以为实现合理的公共政策目标实施例外措施，前提是例外措施不得构成歧视和变相贸易限制或超过必要限度（即限制措施需满足非歧视性和必要性原则）。

总体而言，CPTPP 在促进数据跨境自由流动方面设置了较高的开放标准，它鼓励建立个人信息保护制度兼容性和可互操作性机制，支持数据跨境自由流动及计算设施非强制本地化，但 CPTPP 承认各国对于数据跨境流动、计算设施位置的监管要求，容许有条件的例外，但对例外条例的宽容度较低，仅允许有条件、有限度的例外。

表 6 CPTPP 数据跨境流动条款内容

协定	条款	条款内容
CPTPP	第 14.8 条	承认个人信息保护的价值，并将其纳入消费者的权益范畴而加以规制； 要求各方建立起个人信息的保护框架，并以现存的国际标准作为参考； 要求境外个人信息输入后享受非歧视的境内保护； 要求公开企业所应遵守的法律法规以及私人主体可获得的救济途径； 鼓励建立包含互认机制在内的兼容机制。
	第 14.11 条	认可“成员方关于跨境信息传输有其自身的规制要求”； 要求数据跨境自由流动； “公共政策目标例外”，为实现公共政策目标可对跨境信息流动实施限制，但该措施的实施方式不构成对贸易的任意或不合理的歧视或变相限制且是适度的，不超过实现目标所需的限制水平。
	第 14.13 条	承认各缔约方有各自监管要求，包括通信安全和保密要求； 不得以本地化作为开展业务条件；

		“公共政策目标例外”，可以为实现合理公共政策目标采取不符措施，但该措施的实施方式不能构成任意或不合理歧视或变相限制贸易，且不得超过实现目标所必需的限度。

（二）RCEP 允许 “例外规则”的高程度保留

RCEP 2012 年由东盟发起，由包括中国、日本、韩国、澳大利亚、新西兰和东盟十国共 15 方成员制定的协定。2020 年 11 月，第四次区域全面经济伙伴关系协定领导人会议以视频方式举行，会后东盟 10 国和中国、日本、韩国、澳大利亚、新西兰共 15 个亚太国家正式签署了《区域全面经济伙伴关系协定》。2021 年 3 月，商务部国相关负责人表示，中国已经完成 RCEP 核准，成为率先批准协定的国家。同年 4 月，中国向东盟秘书长正式交存《区域全面经济伙伴关系协定》核准书。2022 年 11 月，中国与东盟发布了《中国—东盟全面战略伙伴关系行动计划(2022-2025)》强调共同全面有效落实 RCEP，并加强在数字经济、网络和数据安全等的合作。

第十二章第八条规定的线上个人信息保护条款外，RCEP 数据跨境规则主要集中于第八章“服务贸易”中的附件一“金融服务”和附件二“电信服务”以及第十二章“电子商务”中。

RCEP 附件一“金融服务”第九条要求每一缔约方承诺不得阻止开展业务所必需的信息转移或信息处理，但是第九条同时承认每一个缔约方对其信息转移与信息处理的管理权利，强调上述规定不得阻止每一缔约方的监管需求与数据安全保护。附件二“电信服务”第四条则要求每一缔约方应当保证，另一缔约方的服务提供者可以使用公共电信网络和服务在其领土内或跨境传输信息。对于信息的安全性和机密性，附件二“电信服务”第四条同意每一缔约方可以采取必要措施进行保护，但是前提是不能阻碍服务贸易的进行。

第十二章“电子商务”第十四条对计算设施的位置进行规定，明确了数据存储非强制本地化的要求，但是第十四条第三款为该要求设置了前提，如果缔约方为了实现其合法的公共政策目标，以及为了保护其安全利益，则可以采取缔约方认为的必要措施。这里的合法公共政策的必要性应当由实施政策的缔约方决定，因此赋予了缔约方决定是否进行数据存储强制本地化的权利。第十二章第十五条“通过电子方式跨境传输信息”采取了与第十四条一样的规定方式。第十五条第二款对跨境传输电子信息的自由进行了强调，明确“一缔约方不得阻止涵盖的人为进行商业行为而通过电子方式跨境传输信息”，但是缔约方出于公共政策目标以及安全利益所需可以进行相应的阻止，对于公共政策目标的界定也由缔约方决定。

此外，由于缔约方国内数据相关立法水平不一，第十五条第二款对个别成员国适用该款进行了保留，如柬埔寨、老挝和缅甸在协定生效之日起五年内不得被要求适用该款等。第十二章第十四条、第十五条通过将数据存储本地化、数据跨境流动的决定权赋予缔约方，强调缔约方的“安全例外”，极大地维护了各缔约方的数据主权。

表 7 RCEP 数据跨境流动条款内容

协定	条款	条款内容
RCEP	第八章 附件一	缔约方认识到，每一缔约方可就信息转移和信息处理设臵其管理要求。 一缔约方不得采取下列措施阻止：

协定	条款	条款内容
		其领土内的金融服务提供者为进行日常营运所需的信息转移，包括通过电子方式或其它方式进行数据转移；或者其领土内金融服务提供者进行日常营运所需的信息处理。 上述中的任何规定并不阻止一缔约方的监管机构出于监管或审慎原因要求其领土内的金融服务提供者遵守与数据管理、存储和系统维护、保留在其领土内的记录副本相关的法律和法规，只要此类要求不被用作规避一缔约方在本协定项下之承诺或义务的手段。以及不限制一缔约方保护个人数据、个人隐私，以及个人记录和帐户机密性的权利，包括根据其法律和法规进行保护的权利，只要此类权利不被用作规避一缔约方在本协定项下的承诺或义务的手段。
	第八章 附件二	每一缔约方应当保证，另一缔约方的服务提供者可以使用公共电信网络和服务在其领土内或跨境传输信息，包括此类服务提供者的公司内部通信，以及接入任何缔约方领土内数据库所包含的信息，或者以机器可读形式存储的信息。 尽管有上述规定，一缔约方可以采取此类必要措施，以保证信息的安全性和机密性，并且保护公共电信网络或服务终端用户的个人信息，只要此类措施不以对服务贸易构成任意的或不合理的歧视或者构成变相限制的方式实施。
	第十二章 十四条	缔约方认识到每一缔约方对于计算设施的使用或位置可能有各自的措施，包括寻求保证通信安全和保密的要求。 缔约方不得将要求涵盖的人使用该缔约方领土内的计算设施或者将设施路于该缔约方领土之内，作为在该缔约方领土内进行商业行为的条件。 “公共政策目标例外+安全例外”。 缔约方可以为实现合法的公共政策目标决定计算设施的位置，只要该措施不构成任意或不合理的歧视或变相贸易限制的。该缔约方可以为基本安全利益采取任何不符措施，且其他缔约方不得对此类措施提出异议。
	第十二章 十五条	各缔约方对电子方式传输信息有各自的监管要求； 一缔约方不得阻止为进行商业行为而通过电子方式跨境传输信息； “公共政策目标例外+安全例外”。 缔约方可以为实现合法的公共政策目标采取限制数据传输的措施，只要该措施不构成任意或不合理的歧视或变相贸易限制的。该缔约方可以为基本安全利益采取任何不符措施，且其他缔约方不得对此类措施提出异议。

（三）DEPA 提出数据跨境流动创新性条款

随着全球数字技术的快速发展以及全球数字贸易发展的形势变化，以新加坡为代表的小国家认为 CPTPP 容易造成新的贸易壁垒，同时 RCEP 由于例外规则的保留降低了规则的约束力，且 RCEP 所涵盖的数字贸易规则标准较低，因此 2019 年 5 月，在新加坡主导下，新加坡、新西兰和智利共同宣布开启《数字经济伙伴关系协定》（DEPA）谈判。经过多轮谈判，新加坡等三国于 2020 年 6 月签署 DEPA，并于 2021 年 1 月 7 日正式生效。同时，2020 年 8 月，新加坡与澳大利亚签订《新加坡-澳大利亚数字经济协议》（SADEA）。DEPA 与 SADEA 的签订标志着以新加坡为代表的小国成为亚太地区，乃至全球数字贸易规则制定的重要力

量，构建起数字贸易规则的“新式模板”，推动亚太地区数字贸易规则的多元化发展。2021 年 11 月 1 日，中国商务部代表中方向《数字经济伙伴关系协定》保存方新西兰正式提出申请加入 DEPA。

DEPA 关于数据跨境流动的原则性条款主要涵盖在第 4.2、4.3 与 4.4 条款中。作为数据跨境流动的重要前提，数据安全的保护，尤其是个人信息安全的保护日益引起全球范围内的关注。DEPA 第 4.2 条列举了缔约国国内个人信息保护法应该涵盖的内容，包括收集限制、数据质量、用途说明等，然而 DEPA 更强调各缔约国在个人信息保护体制之间的兼容性和交互操作性。DEPA 第 4.2.6 至 4.2.10 条规定各缔约国通过建立监管互认机制、认证框架互认、采用数据保护可信任标志等方式来进一步促进各缔约国的国际合作。在数据跨境自由流动与数据存储本地化规则方面，DEPA 第 4.3 条在强调数据跨境自由流动并将个人信息纳入可跨境传输范畴的同时，明确如果缔约方为了合法公共政策目标而阻碍数据跨境流动，则其所采取的措施必须控制在所需限度之内。第 4.4 条的计算设施位置规则采取与第 4.3 条相同的表述方式，要求数据存储非强制本地化，并将为实现合法公共政策目标而阻碍该要求的措施控制在必要范围之内。

除数据跨境自由流动与数据存储本地化等传统原则性条款外，DEPA 新加入了人工智能、开放政府数据、数字身份、数据监管沙盒等具象的创新性条款。

DEPA 同时关注政府数据的跨境流动以及跨境流动数据的应用，相关的内容主要集中在 DEPA 的第 8.2 条“人工智能”以及第 9.5 条“开放政府数据”中。第 8.2 条强调缔约方建立可信、安全和负责任的人工智能框架，同时考虑到“数字经济的跨境性质”，DEPA 旨在最终实现此类框架的国际一致性。第 9.5 条要求缔约方保证以开放数据形式向公众开放政府信息，并合作确定可扩大获取和使用公开数据的方式以及制定允许任何人进行访问、使用和修改的开放数据许可模式，从而增加和创造商业机会。而在数字身份、监管沙盒等数据监管方面，DEPA 旨在实现各缔约方的互操作性以及实现数据驱动的创新。DEPA 第 7.1 条要求各缔约方建立框架，实现数字身份制度的互操作性并建立共同的标准，同时规定缔约方将数字身份纳入各自的法律框架或互认数字身份的法律和监管效果。不过第 7.1 条也设置了实现“合法公共政策目标”的例外情形。对于数据监管沙盒，DEPA 第 9.4 条认为企业在数据监管沙盒机制下进行数据共享的有利于促进创新，以及可信的数据共享框架可以促进数据在数字环境中的使用，因此 DEPA 要求各缔约方在数据共享项目和机制、数据新用途的概念验证(包括数据沙盒)等方面开展合作。

表 8 DEPA 数据跨境流动条款内容

协定	条款	条款内容
DEPA	第 4.2 条	缔约方认识到保护数字经济参与者个人信息的经济和社会效益，以及此种保护在增强数字经济和贸易发展的信心方面的重要性。 每一缔约方应采用或维持为电子商务和数字贸易用户的个人信息提供保护的法律框架。在制定保护个人信息的法律框架时，每一缔约方应考虑相关国际机构的原则和指南。 缔约方认识到，健全的保护个人信息法律框架所依据的原则应包括:收集限制;数据质量;用途说明;使用限制;安全保障;透明度;个人参与;以及责任。 每一缔约方应在保护电子商务用户不受其管辖范围内发生的违反个人信息保护行为的影响方面采取非歧视做法。 每一缔约方应公布关于其为电子商务用户提供的个人信息保护的信息，包括:(a)个人如何寻求救济;及(b)企业如何遵守任何法律规定。

协定	条款	条款内容
		认识到缔约方可采取不同法律方法保护个人信息，每一缔约方应致力于制定机制，以促进不同个人信息保护体制之间的兼容性和交互操作性。这些机制可包括:对监管结果的承认，无论是自动给予还是通过共同安排更广泛的国际框架:可行时，对各自法律框架下的可信任标志或认证框架所提供的相当水平的保护给予适当承认;或缔约方之间个人信息转移的其他途径。 缔约方应就第 6 款中的机制如何在各自管辖区内实施交流信息，并探讨扩大这些或其他适当安排的途径，以促进它们之间的兼容性和交互操作。 缔约方应鼓励企业采用数据保护可信任标志，以帮助验证其 8 符合个人数据保护标准和最佳做法。 缔约方应就数据保护可信任标志的使用交流信息并分享经验。 缔约方应努力相互承认其他缔约方的数据保护可信任标志作为便利跨境信息传输的同时保护个人信息的有效机制。
	第 4.3 条	1.认可“成员方关于跨境信息传输有其自身的规制要求”。 2.义务款，要求数据跨境自由流动。 3.“公共政策目标例外”，为实现公共政策目标可对跨境信息流动实施限制，但该措施的实施方式不构成对贸易的任意或不合理的歧视或变相限制且是适度的，不超过实现目标所需的限制水平。
	第 4.4 条	1.认可“成员方关于有其自身的规制要求”。 2.任何缔约方不得要求一涵盖的人在该缔约方领土内将使用或设置计算设施作为在其领土内开展业务的条件。 3.“公共政策目标例外”，为实现公共政策目标可对跨境信息流动实施限制，但该措施的实施方式不构成对贸易的任意或不合理的歧视或变相限制且是适度的，不超过实现目标所需的限制水平。
	第 7.1 条	1.认识到缔约方在个人或企业数字身份方面的合作将增强区域和全球互联互通，并认识到每一缔约方对数字身份可能有不同的实现工具和法律方式，每一缔约方应努力促进其各自数字身份制度之间的可交互操作性。这可能包括：(a)建立或维持适当框架，以促进每一缔约方数字身份制度之间实现技术可交互操作性或建立共同标准；(b)每一缔约方各自法律框架为数字身份提供同等保护，或通过自动授予或共同协议方式相互认可其法律和监管效果；(c)建立或维护更广泛的国际框架；以及(d)就与数字身份相关的政策和法规、技术实现工具和保障标准以及用户采用的最佳实践交流知识和专业技术。 2.为进一步明确，本条中任何内容不得阻止一缔约方采取或维持与第 1 款不符的措施以实现一合法公共政策目标。
	第 8.2 条	1.缔约方认识到，在数字经济中人工智能(AI)技术的使用和采用日益广泛。 2.缔约方认识到为可信、安全和负责任使用人工智能技术而制定道德和治理框架具有经济和社会重要性。考虑到数字经济的境性质，缔约方进一步承认不断增进共同谅解并最终保证此类框架的国际一致性的益处，从而尽可能便利在缔约方各自管辖范围之间接受和使用人工智能技术。 3.为此，缔约方应努力促进采用支持可信、安全和负责任使用人工智能技术的道德和治理框架(人工智能治理框架)。

协定	条款	条款内容
		4.在采用人工智能治理框架时，缔约方应努力考虑国际公原则或指导方针，包括可解释性、透明度、公平性和以人为本的价值观。
	第 9.4 条	1.缔约方认识到，跨境数据流动和数据共享能够实现数据驱动的创新。缔约方进一步认识到，企业在数据监管沙盒机制下，根据缔约方各自法律法规共享包括个人信息 13 在内的数据，进一步增强创新。 2.缔约方还认识到，数据共享机制，例如可信数据共享框架和开放许可协议，可便利数据共享并促进其在数字环境中的使用，从而： (a)促进创新和创造；(b)便利信息、知识、技术、文化和艺术的传播；以及(c)促进竞争和培育开放高效的市场。 3.缔约方应努力在数据共享项目和机制、数据新用途的概念验证(包括数据沙盒)方面开展合作，以促进数据驱动的创新。
	第 9.5 条	1.缔约方认识到，便利公众获得和使用政府信息可促进经济和社会发展、竞争力和创新。 2.在一缔约方向公众提供政府信息(包括数据)时，应努力保证以开放数据方式提供此类信息。 3.缔约方应努力合作确定缔约方可扩大获取和使用公开数据的方式，以期增加和创造商业机会。 4.本条下的合作可包括下列活动： (a)共同确定可利用开放数据集、特别是具有全球价值的数据集促进技术转让、人才培养和创新的部门； (b)鼓励开发以开放数据集为基础的新产品和服务； (c)推动使用和开发通过可在线获得的以标准化公共许可证为形式的开放数据许可模式，此类模式允许任何人出于缔约方各自法律法规所许可的任何目的自由访问、使用、修改和分享开放数据，且此类模式依赖于开放数据格式。

（四）USMCA 强化与国际“软法”的衔接

USMAC 由北美自由贸易协定（NAFTA）演化而来。2020 年 1 月 29 日，美国总统特朗普签署USMCA，标志着实行 20 多年的 NAFTA”改名换姓”，并将其升级为新的版本[20]。

NAFTA 最早于 1992 年签订并于 1994 年生效，由此形成的北美自由贸易区曾是发达国家与发展中国组成自由贸易区、开展经济合作的典范。早在 20 世纪 80 年代，墨西哥开始推行市场化改革，1986 年加入关贸总协定，对外开放度显著提高，为北美自由贸易协定的谈判创造机遇和条件。1990 年，美国与墨西哥开始谈判。1991 年，加拿大加入谈判。1992 年 12 月 17 日，三国领导人签订了北美自由贸易协定。1994 年 1 月 1 日，北美自由贸易协定正式生效，北美自由贸易区宣布成立[21]。根据该协定，成员国相互之间的关税税率在 15 年内基本削减为 0；其中，汽车产业只要满足 62.5%的北美原产地标准，则在 5-10 年间减免成员国间的全部关税；各国之间减少投资障碍，对外商直接投资实行非歧视待遇，但与国家安全相关的产业、墨西哥的能源产业、加拿大的文化产业除外。不同于其他的关税同盟、自由贸易区等形式的区域经济组织，北美自由贸易区由两个属于七国集团成员的发达国家和一个发展中国家组成，三国在政治、经济、文化方面差距

[20] 曹永福.北美自由贸易协定的前世今生[J].经济,2020(Z1):152-154.

[21] 曹永福.北美自由贸易协定的前世今生[J].经济,2020(Z1):152-154.

很大。因此，北美自由贸易区主要通过垂直分工来体现美、加、墨三国之间的经济互补关系。具体而言，美国和加拿大以其发达的知识、技术密集型产业，通过商品和资本流动加强在墨西哥的优势地位，扩大墨西哥市场；墨西哥则可利用本国廉价劳动力，发展劳动密集型产业，将劳动密集型产品销往美国，同时可以获取美国的巨额投资和技术转让，促进本国产业结构调整。

在发达国家贫富差距不断扩大、低技能劳动者失业浪潮、以及数字贸易兴起的大背景下，美国主导了对 NAFTA 的修订及谈判。在 2016 年的美国总统竞选活动中，特朗普承诺将重新谈判或撤出 NAFTA，并且不止一次称 NAFTA 是“有史以来最糟糕的贸易协议”。此后在美国主导下，三国在 2017-2018 年就 NAFTA 的修订进行了谈判。2018 年 11 月，美国、墨西哥、加拿大三国领导人在阿根廷首都布宜诺斯艾利斯签署 USMAC，替代原来的 NAFTA[22]，USMAC 于 2020 年 7 月 1 日正式生效。值得关注的是，相较于 NAFTA，USMAC 除了在汽车原产地规则、劳工标准、环境保护、知识产权保护等方面发生变化以外,USMAC 还首次将“数字贸易”作为独立章节纳入自由贸易协定。在数字产业快速发展、数字贸易高速增长的背景下，USMAC 反映了美国在数字时代维护其贸易利益的主张，对未来全球贸易规则制定产生巨大影响。

USMCA 的总体目标是建立一个灵活的数字贸易框架，努力让缔约方在数字法规、政策、执法和合规方面加强相互合作，并在一定程度上依赖以 APEC 和 OECD 为代表的现有国际原则。USMCA 在第 19 章中集中规定了数字贸易相关规则，其中数据跨境流动相关的三个核心条款为个人信息保护条款（第 19.8 条）、通过电子方式跨境传输信息条款（第 19.11 条）、计算设施的位置条款（第 19.12 条）。另外，USMCA 在金融服务章节（第 17 章）中，也特别规定了金融领域的电子方式跨境传输信息条款（第 17.17 条）和计算设施位置条款（第 17.18 条）。

在“个人信息保护”议题下，由于个人信息保护是制约数据跨境流动的主要因素之一，USMCA 同其他主要贸易协定的基本态度相同，要求各缔约方在考虑国际组织关于个人隐私保护原则和指南的基础上，设立个人信息保护法律框架，基于非歧视原则为境外个人信息提供境内保护，并鼓励各缔约方建立促进各国个人信息保护制度兼容性和可互操作性的机制。具体而言，在要求各缔约国设立个人信息保护法律框架方面，USMCA 明确可以参考 APEC《亚太经合组织跨境隐私规则》(CBPR)体系和《经合组织隐私保护和个人数据跨境流动指南》。在鼓励各国建立促进个人信息保护制度兼容性和可互操作性机制方面，由于美国、墨西哥、加拿大均加入 APEC 的 CBPR 体系，因此 USMCA 承认 CBPR 系统是保护个人信息同时促进跨境信息转移的有效机制。这也反映出《OECD 隐私指南》和《APEC 跨境隐私规则》及 CBPR 体系对 USMCA 相关规则形成的影响力，以及美国正在着力推动 CBPR 体系作为区域性数据跨境流动的制度安排。

在“通过电子方式传输信息”议题下，USMCA 同其他主要贸易协定一致，采取了“数据自由流动+合法公共政策目标例外”的框架，即不得限制或禁止商业活动中的跨境数据流动，但可以为实现合理的公共政策目标实施例外措施，前提是例外措施不得构成歧视和变相贸易限制或超过必要限度（即限制措施需满足非歧视性和必要性原则）。在各主要贸易协定中，USMCA 最为严格地禁止实施数据自由流动的限制性措施。一方面，USMAC 删除了“各方可能有自己的监管要求”的表述，另一方面 USMAC 还将数据跨境流动的范围扩大至金融服务领域。

[22] 美墨加三国领导人在阿根廷签署新版贸易协定[N]. 新华网, 2018.

在“计算设施位置”议题下，目前主要区域及双边自贸协定基本采取“禁止计算设施本地化+合法公共政策目标例外”的框架，不得将计算设施本地化作为在其领土内开展业务的条件，但可以为实现合理的公共政策目标实施不符措施，前提是例外措施不得构成歧视和变相贸易限制或超过必要限度（即限制措施需满足非歧视性和必要性原则）。但是，USMCA 最为严格地禁止将计算设施本地化作为市场准入的前置条件，没有设置合法公共政策目标例外。此外，USMAC 还将禁止计算设施本地化的范围扩大至金融服务领域。而其他贸易协定均承认各方基于通信安全和保密要求，可能有自己的监管要求，且设置合法公共政策例外。

总之，USMAC 最大程度强调数据跨境自由流动、禁止计算设施本地化，并着力推动 CBPR 体系作为区域性数据跨境自由流动的一项制度安排,将 CBPR 体系作为增强各国个人信息保护机制兼容性的参照。

表 9 USMCA 数据跨境流动条款内容

协定	条款	条款内容
USMCA	第 17.17 条	任何一方均不得阻止传输信息。本条的任何规定均不限制缔约方采取或维持保护个人数据、个人隐私以及个人记录和账户机密性的措施的权利。
	第 17.18 条	一方可直接、完整和持续的访问金融监管机构获取相关人员的信息，并需要消除对该访问的任何潜在限制； 任何缔约方均不得要求使用或定位其领土作为在该领土开展业务的条件。
	第 19.8 条	缔约双方认识到保护数字贸易用户个人信息的经济和社会效益，以及保护其对增强消费者对数字贸易信心的贡献； 各方应考虑相关国际机构的原则和准则采用或维持一个法律框架，规定保护数字贸易用户的个人信息； 各方认识到确保遵守个人信息保护措施的重要性，并确保对个人信息跨境流动的任何限制都是必要的，且与所呈现的风险相称； 各方应努力采取非歧视性做法保护数字贸易用户； 各方应公布其向数字贸易用户提供的个人信息保护信息； 各缔约方应鼓励制定机制以促进这些不同制度之间的兼容性，认可 CBPR 体系是便利跨境信息传输、同时保护个人信息的有效机制。
	第 19.11 条	各方不得禁止或限制为开展商业活动而通过电子方式跨境传输信息；“公共政策目标例外”。为实现公共政策目标可对跨境信息流动实施限制，但该措施的实施方式不构成对贸易的任意或不合理的歧视或变相限制且是适度的，不超过实现目标所需的限制水平。
	第 19.12 条	任何缔约方均不得要求将计算设施本地化作为在该领土开展业务的条件。

（五）UJDTA 沿袭“美式模板”核心规则

继 USMAC 签署约一年之后，2019 年 10 月，美国和日本正式签署了 UJDTA。UJDTA 谈判以 TPP 为起点，是美日数字贸易治理博弈的最新产物，也是数字贸易规则“美式模板”的代表之一，其在数据跨境流动、数字产品待遇、源代码保护等核心议题上的标准较高[23]。

UJDTA 中的多数规则承袭了 USMCA 数字贸易章节中的相关规则[24]，但也基于美日两国贸易的实际情况作出了一定调整。总体而言，UJDTA 共包含 22 条内容，关于数据跨境流动相关的核心条款包括个人信息保护条款（第 15 条）、通过电子方式跨境传输信息条款（第 11 条）、计算设施的位置条款（第 12 条）。

在“个人信息保护”议题下，具体内容为“各缔约方应设立保护数字贸易用户个人信息的法律框架；各缔约方应公布其为数字贸易用户提供的个人信息保护的相关信息；各缔约方应鼓励创建机制，以促进不同制度之间的互操作性；缔约双方认识到遵守个人信息保护措施的重要性，且确保对个人信息跨境流动的限制是必要的且与所出现的风险相称。”可见，UJDTA 无论是在要求各缔约国设立个人信息保护法律框架方面，还是在鼓励各国建立促进个人信息保护制度兼容性和可互操作性机制方面，都基本承袭了 USMCA 的相关规定。

在“通过电子方式传输信息”议题下，UJDTA 基本沿袭了 USMAC 的相关规定，同样采取“数据自由流动+合法公共政策目标例外”的框架，且严格地禁止实施数据自由流动的限制性措施，同样删除了“各方可能有自己的监管要求”的表述。在“计算设施位置”议题下，UJDTA 也基本沿袭了 USMAC 的相关规定，严格禁止将计算设施本地化作为市场准入的前置条件，没有设置合法公共政策目标例外。不同于 USMAC 的是，UJDTA 禁止计算设施本地化的范围不适用于金融服务领域。

表 10 UJDTA 数据跨境流动条款内容

协定	条款	条款内容
UJDTA	第 11 条	任何一方均不得禁止或限制为从事商业活动通过电子方式跨境传输信息； “公共政策目标例外”。为实现公共政策目标可对跨境信息流动实施限制，但该措施的实施方式不构成对贸易的任意或不合理的歧视或变相限制且是适度的，不超过实现目标所需的限制水平。
	第 12 条	任何一方不得将本地化作为在该领土开展业务的条件； 不适用于第 13 条所涵盖的金融服务提供者。
	第 15 条	各缔约方应采用或维持一个法律框架，以保护数字贸易用户的个人信息； 各缔约方应公布其为数字贸易用户提供的个人信息保护信息； 各缔约方应鼓励创建机制，以促进这些不同制度之间的互操作性； 缔约双方认识到确保遵守个人信息保护措施的重要性，以及确保对个人信息跨境流动的任何限制必要且与所出现的风险相称。

[23] 周念利,吴希贤.美式数字贸易规则的发展演进研究——基于《美日数字贸易协定》的视角[J].亚太经济,2020(02):44-51+150.DOI:10.16407/j.cnki.1000-6052.2020.02.006.

[24] Matthew Pereira. U.S.-Japan Digital Trade Agreement and U.S.-Japan Trade Agreement Finalized [EB/OL]. [2019-10-11]. https://www.ustrademonitor.com/2019/10/u-s-japan-digital-trade-agreement-and-u-s-japan-trade-agreement-finalized/.

四、主要经济体围绕自身利益诉求提出规则主张

根据中国信息通信研究院 2022 年 12 月发布的《全球数字经济白皮书（2022）》显示，2021 年各国数字经济规模排名前 20 的国家分别为美国、中国、德国、日本、英国、法国、韩国、印度、加拿大、墨西哥、意大利、巴西、俄罗斯、澳大利亚、爱尔兰、西班牙、新加坡、瑞士、瑞典、荷兰[25]。由于欧盟《通用数据保护条例》（GDPR）适用于欧盟区域内国家，如法国、意大利、爱尔兰等，加之瑞士《联邦数据保护法》与 GDPR 的相似性以及 GDPR 在欧洲经济区内的适用力，因此对于欧洲区域内的国家数据跨境的规则统一为欧盟 GDPR 规则。同时，美国与墨西哥、加拿大签订了《美国-墨西哥-加拿大协定》，在其中美国一直强调数据跨境自由流动，“美国规则”占据主导地位。因此，通过调整，本次白皮书纳入研究的经济体包括中国、美国、欧盟、东盟、英国、韩国、印度、巴西、俄罗斯、澳大利亚、新加坡、日本等 12 个主要经济体。

（一）中国构建完善立法体系划下数据出境安全红线

继 2016 年《网络安全法》发布后，2021 年，中国陆续出台《个人信息保护法》《数据安全法》等法律，并基于三大法出台了《关键信息基础设施安全保护条例》《网络数据安全管理条例（征求意见稿）》等行政法规，构建起中国数据出境安全保护的顶层规则体系。

由于网络空间个人信息往往不可避免主动或被动地流出境外，因此《网络安全法》第 37 条首先强调进行“数据本地化”要求，规定关键信息基础设施的运营者应当在境内存储个人信息、重要数据。《网络安全法》第 37 条还明确了数据出境的安全评估要求，规定因业务需要，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；法律、行政法规另有规定的，依照其规定。《网络安全法》第 37 条的规定标志我国开始进入数据出境强监管的时代。

《数据安全法》关于数据出境的安全规则集中在第 24 条数据安全审查制度，第 25 条出口管制制度以及第 31 条重要数据出境安全管理等。其中，《数据安全法》第 31 条与《网络安全法》第 37 条规定的重要数据内容进行了衔接，其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重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定，进一步解决重要数据出境安全评估的法律效力问题。对出口管制数据的范围以及重要数据的界定，《网络数据安全管理条例（征求意见稿）》第 73 条进行了明确，并将出口管制数据纳入重要数据范畴。此外，《数据安全法》第 36 条明确基于国际条约、协议等缘由向外国司法或者执法机构提供境内数据的，须经主管机关批准。

《个人信息保护法》第三章建立了个人信息跨境流动的规则。第 38 与 39 条对于向境外提供个人信息设置了前置条件，包括出境安全评估、个人信息保护认证、订立标准合同以及出境事项告知并取得个人单独同意等。《个人信息保护法》补充了《网络安全法》第 37 条有关个人信息跨境流动管理的相关内容，主要体现在第 40 条个人信息出境安全评估条款。《个人信息保护法》第 41 条则与《数据安全法》第 36 条相呼应，明确即使基于国际条约、协议等缘由向外国司法或者执法机构提供境内个人信息的，也需要经主管机关批准。

[25] 中国信息通信研究院：《全球数字经济白皮书（2022）》，p15,http://www.caict.ac.cn/kxyj/qwfb/bps/202212/P020221207397428021671.pdf

除出台《网络安全审查办法》《数据出境安全评估办法》等部门规章外，我国针对个人信息出境制定了相应的国家标准，进一步保障数据出境安全，细化数据安全出境操作路径。

为落实《数据安全法》第 24 条关于数据安全审查制度的规定，国家对原基于《网络安全法》制定的《网络安全审查办法》进行修订。除保留原先的安全审查内容外，《网络安全审查办法》主要增加了网络平台运营者在国外上市的规定，强调“掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查”。《数据出境安全评估办法》细化《网络安全法》第 37 条、《数据安全法》第 31 条以及《个人信息保护法》第 40 条关于重要数据、个人信息出境评估的要求。《数据出境安全评估办法》明确了评估事项，评估所需材料、评估申请流程、评估所需期限等内容。至于哪些情形需要申请出境安全评估，《数据出境安全评估办法》明确了具体的范围，主要是包括：重要数据出境；关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息以及出于兜底需要的其他情形。

对于个人信息出境，目前有三种路径，除适用《数据出境安全评估办法》外，还可适用《个人信息跨境处理活动安全认证规范 V2.0》与个人信息出境标准合同。《个人信息出境标准合同办法》明确个人信息出境标准合同适用的是未达到安全评估门槛的个人信息出境情形并且由个人信息处理者自我审查决定，与《数据出境安全评估办法》有清晰的界限。同时，个人信息出境标准合同与东盟的 MCCs 类似，《个人信息出境标准合同办法》明确个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。《个人信息跨境处理活动安全认证规范 V2.0》则是依托第三方专业机构对个人信息处理者开展个人信息出境进行安全认证，不过与其他两种路径有清晰的适用范围相比，其缺乏较为具体的认证适用范围。

2023 年 9 月 28 日，国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》（下称“《规定》”），旨在保障国家数据安全，保护个人信息权益的基础上，进一步规范和促进数据依法有序自由流动。本次《规定》的重点内容主要包括重申需申报数据出境安全评估的场景；明确无需申报数据出境安全评估的情形；赋予自由贸易区制定“负面清单”的权利等。本次《规定》的出台与此前发布的法律法规构成我国数据出境更加完善的规则体系，在厘清数据安全红线的前提上，踩下了数据出境的“油门”。

（二）美国主张“有限例外”的自由流动规则

美国在与其他经济体签订的双边或者多边贸易协议中一直强调有限例外原则，旨在推动数据跨境自由流动，从而利用自身技术市场优势实现数据跨境流动的经济利益最大化。1997 年开始，美国基于有限例外原则在《全球电子商务框架》（The Framework for Global Electronic Commerce）中提出在尽量保障个人隐私的基础上，信息要尽可能自由跨境流动，如果各国在信息跨境流动方面采取不同的政策，那么有可能形成非关税贸易壁垒。此后，美国在 2000 年与欧盟签订《安全港协议》（U.S.-EU Safe Harbor Framework），允许网络运营商忽略欧盟各国法规差异，在美国与欧盟国家之间合法传输网络数据。在《安全港协议》的保护下，谷歌、脸书等多家美国公司频繁将欧洲用户数据输往美国存贮及分析。由于施雷姆斯案，2015 年 10 月，欧盟判决认定《安全港协议》无效。为弥补《安全港协议》失效后美欧数据跨境流动的限制，2016 年，美国与欧盟签署《欧美隐私盾协议》（EU-U.S. Privacy Shield）。美国强调在加强政府安全监管的基础上允许数据的自由流动。截至 2020 年，超过 5000 家美国企业根据该协定传输并处理其欧洲用户的数据。此后，欧盟认为美国的

数据保护未达到欧盟标准，最终于 2020 年 7 月宣布《欧美隐私盾协议》无效。2023 年 7 月，欧盟与美国在跨境数据流动领域达成第三份协议——《欧盟-美国数据隐私框架》（EU-US Data Privacy Framework）。通过近三年的长久谈判和强力的政治行政手段，欧美恢复了跨境数据流动的规制体系。

在其他双边、多边协议中，坚持有限例外原则下的数据跨境自由流动依然是美国的出发点。2012 年，美国与韩国签署《美韩自由贸易协定》（US-Korea Free Trade Agreement），提出双方应避免限制跨境数据流动，实现数据自由流动。在《美墨加协定》（USMCA）、《跨境隐私规则体系》（CBPR）、《全面且先进的跨太平洋伙伴关系协定》（CPTPP）等中，美国一直强调数据流动的全球属性，禁止数据与数字基础设施本地化，旨在打开推行数据本地化存储的国家的市场。

出于维护数据安全和数据霸权的需要，美国对数据采用严格的出口管制并适用长臂管辖。在出口管制方面，美国《出口管理条例》(Export Administration Regulations)限制特定领域的数据出口，受管制的技术数据若传输到位于美国境外的服务器，则需获得美国商务部产业与安全局（BIS）的出口许可。此外，2023 年 10 月 25 日美国贸易代表凯瑟琳·泰（Katherine Tai）在世界贸易组织（WTO）的谈判中放弃了长期的美国数字贸易要求，以便为国会提供监管大型科技公司的空间。美国正撤回 2019 年由特朗普政府提出的提案，这些提案坚决要求 WTO 电子商务规则允许自由的跨境数据流动，并禁止数据本地化和软件源代码审查的国家要求。此举目的在于为从严监管国内科技巨头做好政策铺垫，未来将继续要求科技巨头做好数据本地化，限制科技巨头的数据出境等。

在长臂管辖方面，美国则于 2018 年出台《澄清境外数据的合法使用法案》（CLOUD 法案），规定无论网络服务提供商的通信内容、记录或其他信息是否存储在美国境内，只要该网络服务提供者拥有、控制或监管上述内容、记录或信息，均需要按照该法令的要求保存、备份、披露。通过 CLOUD 法案美国将过去数据管辖的数据存储地原则转变为数据控制者原则，扩大了其获取海外数据的权力。此外，外国政府若想通过网络提供商访问调取储存在美国的本国数据，则必须是 CLOUD 法案所定义的符合条件的外国政府并满足其所要求的一系列条件。

（三）欧盟对外实行充分性认定规则

欧盟的数据跨境流动主要分为内部成员国之间的数据跨境流动，以及跨欧盟疆界的数据流动。《通用数据保护条例》（GDPR）规定的跨境指的就是跨越欧盟的疆界。在内部成员国之间，欧盟旨在推动数据的自由流动，构建欧洲单一数据市场[26]。欧盟身处数字经济边缘，几无大型数字平台，仅占全球 70 个大型数字平台市值的 4%（中美占 90%）[27]，而欧盟的大部分大型数字平台企业来自美国，因此，基于维护数据主权、保障数据安全的需要，欧盟构建了数据跨境流动的充分性认定规则框架。

在 1995 年的《关于个人数据处理保护与自由流动指令》（Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data）中，欧盟提出了充分性认定的要求，其第 25 条 A 款规定如果欧盟范围以外的其他国家能够对欧盟公民的个人隐私和数据提供充分的

[26] 林梓瀚.基于数据治理的欧盟法律体系建构研究[J].信息安全研究,2021,7(04):

[27] 金晶.欧盟的规则，全球的标准?数据跨境流动监管的“逐顶竞争”[J].中外法学,2023,35(01):

保护，那么欧盟公民的个人隐私和数据可以从欧盟境内转移到欧盟境外的其他国家。从那时起，欧盟将“充分性认定”作为数据（信息）跨境传输的基本准则。此后，对充分性认定的要求，GDPR 第 45 条第一款做了进一步规定，明确当欧盟以欧委会决定的形式认定某个国家、某个国家的特定区域或行业或者某个国际组织能够提供充分的数据保护水平时，个人数据即可向前述国家、区域或国际组织传输，而无需欧盟的额外授权。因此，如果数据要流出欧盟边境，得到欧盟的充分性认定是前提。目前，获得欧盟充分性认定的国家地区包括以色列、日本等，中国尚不在充分性认定名单之中。

如果达不到欧盟充分性认定的标准，则有另外两种方式，分别是约束性企业规则（BCRs）和标准合同条款（SCCs）。BCRs 是适用于在跨国公司内部进行个人数据跨境流动的规则。跨国公司如果具备欧盟成员国数据管理机构认可的 BCRs，则可以直接进行公司内部的数据跨境传输。不过，当跨国公司适用 BCRs 时，个人数据跨境流动仅限于跨国公司内部的数据传输，如果该跨国公司将个人数据传输至其他外部主体时，则不得适用 BCRs 模式，即使该外部主体也有资格适用 BCRs。SCCs 是个人数据跨境传输的标准合同文本，欧盟委员会通过制定强制性条款内容约束数据输出者和数据输入者以确保个人数据获得充分的保护。SCCs 主要包括数据输出者和数据输入者的义务，第三方受益人权利条款，以及责任分担条款。不过，SCCs 在适用方面存在较大缺陷，每一次个人数据的跨境流动都需要专门签订合同，因此，难以适用于大量的数据跨境流动，同时，大量的合同文本也会很容易造成合规风险漏洞。

除上述规则外，GDPR 第 42 条和第 43 条规定了个人数据跨境流动合规性认证的制度，由欧盟各国数据监管当局认可的认证机构对第三国数据接收方进行认证，通过认证获得认证证书后方可进行个人数据的跨境流动。2018 年，欧盟数据保护委员会发布《关于 GDPR 第 42 和 43 条规定的认证和认证标准的指南》（Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation）对认证规则进行了细化。不过，某个成员国的认证机构颁发的认证证书只对该国有效，除非第三国数据接收方申请欧洲通用级认证方可在欧盟境内通用。

（四）东盟落地施行“示范合同条款”机制

2016 年，东盟依托《东盟经济共同体蓝图 2025》和《东盟信息通信技术总体规划 2020》，出台《东盟个人数据保护框架》。该框架旨在统一东盟内的网络安全和数据流动标准,以东盟整体增强数据保护水平，同时为确保成员国的对该框架的适用，该框架在内容上灵活适应成员国在数据和隐私保护监管方面的不同的成熟度。此后，随着全球数字经济的发展，东盟寻求更加具有前瞻性以及有利的治理框架与政策以促进数字经济的增长，因此出台了《东盟数字数据治理框架》。《东盟数字数据治理框架》提出四大战略优先事项，分别为数据生命周期系统、数据跨境流动、数字化和新兴技术以及法律法规和政策，而为了支撑这四大战略优先事项的落地，该治理框架对应提出东盟数据分类框架、东盟数据跨境流动机制、东盟数字创新论坛、东盟数据保护和隐私论坛等四大倡议。其中，对于东盟数据分类框架，《东盟数字数据治理框架》明确制定一个宽泛的数据分类框架是比较有利的，而且这个分类框架也不意味着穷尽了数据的分类。而对于东盟数据跨境流动机制，《东盟数字数据治理框架》认为成员国进行数据跨境流动时须明确哪类数据可以流动以及数据流向的对象是谁，但同时在建立东盟数据跨境流动机制时也应该考虑成员国的发展水平与法律环境。

此后，鉴于对国际现有标准的适用，如美国 NIST 800-60《将信息和信息系统的类型映射到安全类别的指南》、ISO 27001《信息安全管理体系》、ISO 27701《隐私信息管理体系》等以及相关机构制定数据治理架构的需要，东盟将东盟数据分类框架调整为《东盟数据管理框架》，并在第一届东盟数字部长会议上正式发布。《东盟数据管理框架》提出了数据治理框架的六大组成部分，分别为治理与监管、政策与程序性文件、数据清单、影响与风险评估、控制、监控与持续性提升，其中数据清单的制定对使用、收集的数据进行识别和归类，而控制则是根据分配的类别和数据的全生命周期，在系统内设计和执行数据的保护性控制。在落实东盟数据跨境流动机制建设方面，东盟出台《东盟跨境数据流动机制的关键方法》，在其中建议东盟重点建设“东盟示范合同条款”和“东盟跨境数据流动认证”两个机制。

2021 年 1 月，东盟发布《东盟数据跨境流动示范合同条款》（MCCs）。MCCs 根据数据传输方式的不同，提供了“数据控制者到数据处理者”及“数据控制者到数据控制者”两种合同模板，在合同中通过必备条款、可选条款以及选择相关条款明确了数据跨境流动双方的责任、所需的数据保护措施和相关义务。与欧盟的 SCCs 相比，东盟 MCCs 缺少欧盟 SCCs 的另外两中场景的模板，即“数据处理者到数据处理者”和“数据处理者到数据控制者”。东盟的 MCCs 只是自愿性标准和指导性范本，东盟鼓励各成员国将 MCCs 作为数据跨境流动的最低标准。MCCs 的使用并不要求成员国将其直接内化为国内法或修改成员国现有的法律，仅仅将其作为最低要求的非约束性条款。对于 MCCs 合同条款的修订，合同双方可依据 2016 年《东盟个人数据保护框架》规定的原则或成员国法律的要求，通过书面协议修订 MCCs，同时，在不与 MCCs 相矛盾的情况下，也可以通过书面协议协商添加条款。尽管 MCCs 是为了东盟成员国之间的数据跨境流动而设计，但是东盟不排斥企业在东盟成员国以外适用 MCCs。除施行 MCCs 外，东盟也承认国际标准化组织有关安全和隐私技术的系列标准以及亚太经合组织跨境隐私规则、亚太经合组织数据处理者隐私识别体系等机制。

（五）新加坡适用多元规则强化与国际对接

从 2006 年开始，新加坡政府就开始致力于智慧国家的建设。其代表性事件是，新加坡在 2006 年启动了“智能国家 2015”计划，并在 2015 年升级为“智慧国家 2025”计划。而随着“智慧国家 2025”建设的推进，数据的流通与安全，尤其是个人数据的流通与安全日益引发重视。为此，2012 年新加坡制定了《2012 年个人数据保护法》，并针对个人数据的出境制定了基本要求。

新加坡《2012 年个人数据保护法》第 26 条明确，在新加坡境内，负责数据跨境流动的监管部门主要是个人数据保护委员会（Personal Data Protection Commission，PDPC）。对于具体的出境传输要求，第 26 条规定，对于跨境传输的数据，机构应当按该法律规定建立个人信息保护标准，确保被传输的数据得到与新加坡法律相当的保护，否则不得进行跨新加坡国境传输。第 26 条同时给予 PDPC 豁免的权利，规定 PDPC 可以根据机构的申请，通过书面通知豁免机构前述跨境合规义务。对于豁免的具体适用情形，PDPC 有权利可以随时增加、改变或撤销。此后，新加坡对《2012 年个人数据保护法》进行了补充修订，并于 2021 年出台了《2021 年个人数据保护条例》，进一步补充了新加坡数据跨境传输的规定。《2021 年个人数据保护条例》第三部分对《2012 年个人数据保护法》第 26 条进行了补充完善，除第 9 条再次强调其所指的数据跨境流动是指数据出境外，第 10 条细化了个人数据出境的相关要求。规定个人数据出境必须获得个人同意并遵循“出境必要论”与“目的纯粹论”，明确将个人数据传输给新加坡以外的国家或地区的接收方，对于保护数据主体利

益以及国家利益是必要的，同时传输机构确保数据接收方不会为除了数据处理目的之外的其它任何目的而使用或披露该个人数据。同时，第 10 条再次对《2012 年个人数据保护条例》第 26 条进行了回应，规定传输方应采取合理的措施，确保其对所传输的数据提供的保护不低于新加坡法律规定的标准等。

为强化与国际接轨，除适用本国的法律与东盟层面相应规则外，《2021 年个人数据保护条例》第 12 条明确承认《亚太经合组织跨境隐私规则体系》（APEC CBPR 体系）和《亚太经合组织处理者隐私识别体系》（APEC PRP 体系）在新加坡境内的有效性。数据的境外接收方通过 APEC CBPR 认证或者 APEC PRP 认证，则可视为满足新加坡法律对于数据传输接收方的合规要求。APEC CBPR 体系的目标对象是数据控制者而非数据处理者，数据处理者则可通过 APEC PRP 体系认证，证明自身的数据处理至少符合 APEC CBPR 体系对数据控制者的数据处理隐私保护要求。基于第 12 条，PDPC 建立了一项与 APEC CBPR 认证、APEC PRP 认证对接的认证，拟申请认证的企业需要向新加坡通信和信息部下属的新加坡信息通信和媒体发展局（IMDA）提交申请。通过申请评估后，企业即可通过 APEC CBPR 认证、APEC PRP 认证。每次认证的有效期为 1 年，企业需要至少在有效期届满的 3 个月前向 IMDA 再次申请认证。

（六）英国脱欧后推行“英国 GDPR”

英国脱欧过渡期结束后，可以自由决定自己的国际贸易政策，但同时也丧失了作为欧盟成员国的权利。自 2021 年 1 月 1 日起，欧盟法律（包括欧盟 GDPR）不再直接适用于英国。为了应对这一转变，英国修订了现行的《2018 年数据保护法》，将 GDPR 的要求和原则纳入其中，形成了英国 GDPR（United Kingdom General Data Protection Regulation）[28]。该法第五章允许个人数据在充分性认定、适当保障措施（如标准数据保护条款和有约束力的公司规则）或该法规定的其他条件的基础上从英国流向第三国。

英国 GDPR 第 45 条设立了“数据保护充分性认定”规则。英国 GDPR 规定的充分性检验标准是通过对第三国数据保护法律、实施、执行和监督的整体效果进行分析评估，确保当个人数据进行国际传输时，英国 GDPR 规定的保护水平不会受到削弱。除以上评估标准外，还应特别考虑第三国关于法治、尊重人权和基本自由、独立监管机构的存在和有效运作以及相关国际承诺。英国脱欧后，无法通过欧盟单一数据市场下成员国之间的自由流动机制实现数据跨境传输。双方需要一个长期解决方案以应对可能面临的个人数据跨境传输中断和企业合规成本高昂的风险。2021 年 6 月 28 日，欧盟委员会通过了两项将个人数据传输到英国的充分性认定的决定。这些决定意味个人数据可以从欧洲经济区流向英国，而无需适当的保障措施。然而，为防止未来出现分歧，欧盟委员会引入"日落条款"（sunset clause），将充分性认定有效期限制为四年，并受到定期监测和审查。此外，如果欧盟充分性认定决定被撤销或修改，将个人数据从欧盟转移到英国则需要遵循 GDPR 第 46 条规定的额外保障措施。目前，英国已制定了脱欧后充分性认定的评估方法、评估模板和相关指南。英国进行充分性评估的优先国家是韩国、美国、澳大利亚、迪拜国际金融中心和哥伦比亚，长期优先国家是印度、巴西、印度尼西亚和肯尼亚。英国已经通过与韩国的充分性认定，“英美数据桥”（UK-US data

[28] See United Kingdom General Data Protection Regulation, https://www.legislation.gov.uk/eur/2016/679/introduction

bridge）也将于 2023 年 10 月 21 日生效，届时将允许英美相关组织通过“欧盟-美国隐私框架的英国扩展”进行英美两国间的数据跨境传输。

当第三国未通过英国充分性认定时，公共部门和私营部门可以通过英国 GDPR 第 46 条规定的适当保障措施进行跨境数据传输。政府公共部门之间的数据传输可以通过政府机构之间的法律文书和行政安排进行。私营部门可以通过标准数据保护条款、约束性企业规则、数据保护行为准则（Data protection codes of conduct）和认证计划（Certification schemes）进行数据跨境传输。标准数据保护条款是双方在传输数据之前必须签署的现成的合同条款，旨在为向第三国组织传输个人数据提供适当的保障。2022 年 3 月 21 日，新的英国国际数据传输协议（IDTA）和新的 2021 年欧盟标准合同条款的附录（SCCs 附录）开始生效，取代了旧的欧盟标准合同条款（旧 SCCs），作为符合英国 GDPR 的传输工具。然而，由于英国在未脱欧前认可并使用的是欧盟 SCCs，因此，2022 年 9 月 21 日之前依据旧的欧盟 SCCs 签订的合同继续有效，直到 2024 年 3 月 21 日之后，适用旧欧盟 SCCs 的旧合同将需要根据 IDTA 进行修订。对于 2022 年 9 月 21 日或之后签订的新合同，组织必须使用 IDTA 或 SCCs 附录。

约束性企业规则是适用于跨国公司、企业集团或从事联合经济活动（如特许经营，合资企业或专业合伙企业）的企业使用的规则。申请者在满足英国 GDPR 第 47、48 条以及信息专员办公室（ICO）发布的准则和要求时可以将个人数据合法地传输到英国以外的其他子公司。此外，在 2020 年 12 月 31 日持有欧盟批准的具备约束性企业规则的公司，如果在 2021 年 6 月 30 日之前满足相关条件，经信息专员批准可得英国认可。数据保护行为准则是经 ICO 批准的规定了适当保障措施的特定行业准则，可由行业协会和其他代表机构制定。如果相关组织做出具有约束力和可强制执行的承诺、遵守准则并应用适当的保障措施，则可以依靠这些措施将个人数据传输到英国境外。认证计划是证明相关主体符合英国 GDPR 所规定的保护水平的机制。通过认证必须得到 ICO 的批准，并遵守 ICO 认证指南中规定的标准。但是数据保护行为准则和认证计划目前并未在数据跨境流通领域充分应用。

（七）日本在保护个人信息的基础上构建数据跨境生态圈

2003 年 5 月，日本通过《个人信息保护法》（Act on the Protection of Personal Information）（以下简称“APPI”）建构数据跨境传输规则[29]。该法在附则中规定，法律施行后，政府每三年就应当根据形势变化进行相应的修订。基于该规定，《个人信息保护法》历经数次修订，最近一次的修订案已于 2023 年 4 月 1 日正式实施。

APPI 确定了个人信息跨境传输以取得数据主体同意为原则，不同意为例外的出境规则。对于事前同意机制，APPI 第 28 条规定，当个人信息处理者向境外提供个人数据取得数据主体同意时，必需根据个人信息保护委员会（PPC）的规定，事先向数据主体提供有关外国个人信息保护的制度、第三方采取的个人信息保护措施以及其他可供参考的信息。

有三类情形可不需要取得数据主体的同意，分别是充分性认定规则、PPC 规定的充分的隐私保护标准和 APPI 第 27 条规定的七种例外情形。充分性认定规则是指 APPI 第 28 条所规定的在保护个人的权利利益方

[29] See Act on the Protection of Personal Information , https://www.ppc.go.jp/en/legal/

面与日本具有同等水平的个人信息保护制度的国家可以实现数据跨境自由流动，而不需要获得数据主体的同意。此前，为达成欧盟 GDPR 要求的充分性认定要求，日本修订了《个人信息保护法》以加强个人信息保护达到欧盟 GDPR 所要求的同等保护水平。此外，制定基于充分性决定处理从欧盟和英国转移的个人数据的个人信息保护法补充规则以弥合与欧盟在数据保护水平的差距。2019 年 1 月 23 日，日欧实现了数据保护充分性双向认定，数据传输方可以将个人数据从日本转移到欧盟，而无需采取特定数据主体同意或特殊合同条款等措施。

根据 APPI 的执行规则，“类似适当的隐私保护标准”是指经营者处理个人信息的做法至少与 APPI 规定的个人信息保护要求相等，或者经营者获得了有关个人信息处理的国际框架的认证。亚太经济合作组织（APEC）跨境隐私规则（CBPRs）可作为将个人数据传输给日本境外第三方的一种选择。亚太经合组织于 2016 年 1 月批准日本信息处理开发中心（"JIPDEC"）成为 CBPR 系统下日本的第一家责任代理机构。日本信息处理开发中心可向日本企业颁发证书，证书一旦颁发，即被视为在所有亚太经合组织国家有效，可保证经认证的实体已制定符合亚太经合组织隐私框架的程序。此外，APPI 第 27 条规定的七种情形，可作为未经数据主体同意将个人信息提供给第三方的例外。这七种情形分别是：①法令要求；②为保护人的生命、身体财产需要且难以取得本人同意；③为改善公共卫生或促进儿童发展需要且难以取得本人同意；④国家机关、地方人民政府或者受其委托的人员需配合执行法律规定的事务，征得本人同意，可能会妨碍该事务的执行；⑤信息处理者是学术研究机构且为公开学术研究成果或传授学术研究成果必需提供个人数据；⑥信息处理者是学术研究机构且出于学术研究目的需要提供个人数据；⑦第三方为学术研究机构且出于学术研究目的必需处理个人数据。

在保护个人信息安全的基础上，日本对外推动“可信赖数据自由流动倡议”（Data Free Flow with Trust，DFFT）以构建数据跨境流动生态圈。DFFT 是日本在 2019 年的达沃斯世界经济论坛上提出的倡议，其邀请邀请各国领导人建立一个可信赖数据自由流动的国际秩序，并将此倡议命名为“大阪轨道”。DFFT 的概念旨在促进数据的自由流动，同时确保隐私、安全和知识产权方面的信任。随后，在 G20 大阪峰会上，各国政府首脑对实现数据自由流动与信任（DFFT）愿景表示了赞同，确认了"大阪轨道"的价值。此后，日本积极通过多种途径推行 DFFT。

（八）韩国聚焦个人信息细化跨境传输规则

韩国《个人信息保护法》（Personal Information Protection Act，以下简称“PIPA”）和《个人信息跨境传输规定》（以下简称《规定》）建构了个人数据跨境的主要规则。PIPA 于 2011 年 9 月 30 日首次实施，后经历了多次重大修订，最新修订的 PIPA 于 2023 年 9 月 15 日生效[30]。新修正案在很大程度上简化了 PIPA 下有关海外个人数据转移的现行框架，设置了多元化数据跨境传输条件及处罚制度，并授予个人信息保护委员会（PIPC）强制停止跨境转移的权力。然而，值得注意的是，修订后的 PIPA 没有规定标准合同条款或具有约束力的公司规则作为跨境转让的法律依据。2023 年 7 月 26 日，PIPC 发布了《规定》的草案，2023 年 10

[30] See Enforcement Decree of the Personal Information Protection Act [Enforcement Date September 15, 2023] , https://www.pipc.go.kr/eng/user/lgp/law/lawDetail.do

月 16 日，《规定》正式生效[31]。该《规定》旨在更好地执行修订后的《个人信息保护法》以及《个人信息保护实施令》，该《规定》也将进一步完善韩国的跨境传输制度。

根据 PIPA，数据传输方在将个人数据转移给境外的第三方之前，必须事先取得数据当事人的同意。同样，在后续数据传输中，个人数据的第一个境外接收方将作为个人数据的转让方受到 PIPA 的约束。尽管有上述限制，如果传输被认为是出于签订、履行合同需要而"存储或委托处理的目的"所必需，数据控制者可在未征得数据主体/用户同意的情况下，将个人数据传输到韩国境外，前提是已经在隐私政策或通过电子邮件中披露了接受方的详细信息。

除知情-同意外，还有两种替代性传输机制，分别是数据跨境传输认证和充分性认证。跨境传输认证是对数据接收方所提供的处理及保护措施是否符合 PIPA 规定的保护水平进行的认证，包括个人信息保护认证和个人信息跨境传输认证。个人信息保护认证是指个人信息保护委员会就海外接收方的数据处理及保护措施是否符合 PIPA 的规定进行认定。个人信息跨境传输认证是指根据《规定》，由个人信息保护认证机构和跨境转移专家委员会就个人信息保护水平以及对个人信息主体权利的保护是否充分进行评估和审查，并提交 PIPC 审查认定。针对两项认定的优先级，《规定》明确，PIPC 在进行跨境传输认证审查时，应同步确定跨境转移认证的隐私保护水平是否符合《个人信息保护法》第 32-2 条规定的个人信息保护认证。如果 PIPC 经审查确认该跨境转移认证的隐私保护水平未达到第 32-2 条规定的个人信息保护认证的隐私保护水平，该跨境传输认证应同时适用个人信息保护认证结果。在达到认定标准时，海外接收方还采取必要措施保护个人数据安全和数据主体权利，并采取个人信息移转所在国的数据保护认证规定的必要措施进行数据处理。

PIPA 规定的充分性认定框架与 GDPR 充分性认定机制一致。根据 PIPA 第 28-8 条，个人信息可以跨境转移到 PIPC 认可的具有基本等同于 PIPA 要求的数据保护水平的国家或国际组织。欧盟委员会于 2021 年 12 月 17 日通过了一项针对韩国的充分性决定，承认韩国对个人数据的保护水平基本相当，规定向韩国的数据可以转移到欧洲经济区（EEA）国家，而无需额外的转移工具或条件，也无需获得欧洲经济区数据保护监管机构的授权。随后，2022 年 7 月 5 日，英国和韩国就跨境数据传输原则上达成了充分性协议，该协议于 2023 年 11 月 23 日生效。

（九）俄罗斯以数据本地化存储作为数据跨境流动必要前提

根据 2015 年 9 月 1 日生效的数据本地化相关法律第 242-FZ 号联邦法（Federal Law No. 242-FZ）的规定，数据控制者收集的与俄罗斯公民有关的个人数据必须在俄罗斯境内的数据库中进行操作[32]。早在 2015 年 8 月 3 日，俄罗斯联邦通信与大众传媒部（Minsviaz）就发布了关于数据本地化存储的书面指南，说明了第 242-FZ 号联邦法实施的新的个人数据本地化要求。指南表明，只要遵循俄罗斯关于个人数据的其他法律，就可以将有关俄罗斯公民的个人数据转移出俄罗斯。但是，俄罗斯公民的个人数据必须首先在俄罗斯数据库中“记录、系统化、累积、存储、修改、更新和检索”，随后才可以转移到俄罗斯以外的其他数据库。

[31] See South Korea: PIPC publishes draft regulations on overseas transfer of personal information for public comment, https://www.dataguidance.com/news/south-korea-pipc-publishes-draft-regulations-overseas

[32] See Primer on Russia’s New Data Localization Law, https://www.natlawreview.com/article/primer-russia-s-new-data-localization-law

满足数据本地化存储的要求后，个人数据在符合《俄罗斯个人保护数据法》和《为保护公民道德、健康和合法利益而禁止或限制个人数据跨境传输的个人数据主体权利保护授权机构决策规则》[33]（以下简称《授权机构决策规则》）构建的个人数据跨境传输规则下可以进行国际传输。

《个人数据保护法》根据境外第三方对个人数据的保护程度，制定了差异化的个人数据跨境流动规则。根据《个人数据保护法》和《授权机构决策规则》的规定，如果目的地国为俄罗斯联邦通信监管局（Roskomnadzor）认定的对个人数据提供充分性保护的国家，则可以在通知 Roskomnadzor 后进行传输。充分性认定标准包括第三国是否具备有效的个人信息保护法律、是否设立了个人信息保护机构，以及是否针对违反个人信息保护法律的行为建立了有效的惩罚措施等。《个人数据保护法》修订时将《关于个人数据自动化处理的个人保护公约》（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data，简称《108 号公约》）缔约国及处理个人数据时保证数据保密性和安全性方面符合该公约规定的非缔约国认定为提供充分性保护的国家。然而，自 2022 年 9 月起，Roskomnadzor 将独立决定哪些国家在跨境数据传输方面被认定为充分。因此，Roskomnadzor 可以决定是否将《108 号公约》缔约国列入充分国家名单。2022 年 8 月 5 日，Roskomnadzor 发布第 128 号命令将中国、印度、吉尔吉斯共和国等国纳入充分性认定名单中。若目的地国为非通过充分性认定的国家，除为保护个人数据主体或其他人的生命、健康和其他切身利益而必须进行个人数据跨境传输外，个人数据传输主体向 Roskomnadzor 通报并通过审查后方可进行传输。在特殊情况下，如果个人数据跨境传输会使国防、安全或宪法秩序的基础受到威胁，Roskomnadzor 会做出限制或禁止传输的决定。在做出禁止或限制决定后，数据传输主体应确保数据接收主体销毁此前接收的个人数据。

（十）澳大利亚以“合理措施”规制数据跨境流动

澳大利亚《隐私法》（Privacy Act）[34]和澳大利亚信息专员办公室发布的《澳大利亚隐私原则指南》（Australian Privacy Principles Guidelines，以下简称《指南》）构成了其数据跨境流动的基本框架[35]。根据《隐私法》和《指南》的规定，除非适用某些豁免，否则数据传输方只有在采取合理措施（reasonable steps）确保海外接收者不会违反与信息有关的隐私原则时才可以进行个人数据跨境传输。《指南》指出，何为"合理措施"取决于个案情况，包括个人信息的性质(如是否为敏感信息)、数据传输方与海外接收者的关系、信息处理不当对个人造成伤害的风险以及采取特定措施的可行性等。通常，数据传输方会与海外接收方会通过合同安排，加入要求实体遵守《隐私法》相关的条款及明确规定关键要求。

[33] 俄罗斯联邦政府 2023 年 1 月 16 日发布的第 24 号命令 Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан，于 2023 年 3 月 1 日生效。

[34] See Privacy Act 1988, https://www.legislation.gov.au/Details/C2023C00347

[35] See Australian Privacy Principles Guidelines, https://www.oaic.gov.au/__data/assets/pdf_file/0009/1125/app-guidelines-july-2019.pdf

《隐私法》和《指南》规定了 3 种合理措施豁免的情形。第一，澳大利亚法律或法院/法庭命令要求或授权披露信息。这一豁免仅涵盖有限的情况，例如，根据澳大利亚法律（如反洗钱法或有关刑事互助的法律）必须向外国当局披露个人信息的情况。第二，获得数据主体对披露信息的“知情同意”。数据传输方要明确告知个人（通过明确的口头或书面声明），如果个人同意将其数据传输到境外，那么数据传输方将不再需要采取“合理措施”来确保海外接收者遵守《指南》。第三，存在允许披露“一般情况”。这些情况包括：①有理由相信，为减轻或防止对任何个人的生命、健康或安全，或对公共健康或安全的严重威胁，且征得个人同意不合理/不可行，有必要进行此类披露；②有理由怀疑，已经、正在或可能发生与本组织职能或活动有关的非法活动或性质严重的不当行为，且本组织有理由相信披露信息对于本组织就该事项采取适当行动是必要的；③有理由相信有必要披露信息，以协助任何组织或实体查找所报告的失踪人员。对于以上例外，组织应保留审计线索，以证明其决定符合"合理相信"或"合理步骤"要求的依据。除保留审计线索外，数据传输方还必须在收集个人信息时或之前（如不可行，则在收集之后尽快）通知被收集个人信息的个人一些事项，包括数据传输方是否可能向海外接收者披露他们的个人信息，并在可行的情况下说明这些接收者可能位于哪些国家。除“合理措施”规则及豁免外，数据传输主体还可以根据澳大利亚加入的国际条约和标准认证进行数据跨境传输。

除需遵守《隐私法》和《指南》的规定外，医疗健康、金融及税收等领域的数据传输还需符合数据本地化存储等额外要求。如医疗健康领域，2012 年《我的健康记录法》（My Health Records Act 2012,MHR）规定，受 MHR 管辖的操作者不得将记录持有或带出澳大利亚，与消费者或 MHR 系统参与者的个人信息或者与身份识别无关的的记录不受此限制。在金融领域，根据强制性综合信用报告制度，信用机构有义务将所有综合信用信息保存在澳大利亚境内或符合澳大利亚信号局公布的适当云平台上。而受监管的金融实体，除需要遵守《隐私法》及《指南》中有关个人信息跨境传输的固定外，还需要满足澳大利亚审慎监管局(APRA)或澳大利亚证券和投资委员会(ASIC)关于数据跨境传输的要求。

（十一）巴西调整数据跨境流动规则强化“ANPD”角色

此前，巴西关于数据跨境流动的规则主要体现在《通用数据保护法》（General Data Protection Law，LGPD）中[36]。LGPD 第 33 条明确了巴西个人数据跨境传输的法律机制：（1）第三国或国际组织提供的个人数据保护水平达到了 LGPD 规定的充分性程度。（2）当控制者提供和证明符合 LGPD 规定的原则、数据主体权利和数据保护制度的保证文件时，其形式为：用以传输的具体合同条款；标准合同条款；全球性的公司规则（类似于欧盟有约束力公司规则，即 BCR）；定期发布的印章、证书和行为准则。（3）根据国际法律文书，政府情报，调查和警察机构之间的国际法律合作需要传输；（4）为了保护数据主体或第三方的生命或身体安全；（5）巴西数据保护局(ANPD)授权传输；（6）通过国际合作协议承诺传输；（7）履行公共政策或法定公共服务职责之必要；（8）数据主体明确同意，且传输目的可清楚地区别于其他目的；（9）遵守法律或监管义务；合同程序；司法、行政、仲裁中正常行使权利。

[36] See General Data Protection Law , https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

巴西数据保护局（“ANPD”）于 2023 年 8 月 15 日发布了《个人数据跨境传输条例（草案）》（简称《条例草案》）和配套标准合同条款以征求公众意见[37]。一旦条例草案获得批准并生效，公司将有 180 天的时间将 ANPD 的版本纳入其现有的个人信息跨境传输协议或根据 ANPD 发布的配套标准合同条款起草新的协议。《条例草案》是对现有数据跨境传输机制的细化。《条例草案》明确其适用于两类数据跨境传输方式，一类是提供符合 LGPD 充分保护水平的国家或国际组织；一类是“提供并保证遵守 LGPD 规定的原则、权利和数据保护制度”，包括标准合同条款、全球性企业规则等。《条例草案》规定，ANPD 将确定具有充分保护水平的国家或地区名单，以允许个人数据在巴西与这些国家或地区之间自由流动。《条例草案》明确，ANPD 将优先评估保证巴西互惠待遇的外国或国际组织的数据保护水平。

ANPD 在评估国家或国际组织个人数据保护水平时将考虑以下内容：现行立法的一般规则和部门规则；数据的性质；遵守 LGPD 中规定的保护个人数据和数据主体权利的一般原则；采取适当的安全措施，尽量减少对持有人（holder）公民自由和基本权利的影响；是否存在尊重个人数据保护权的司法和制度保障；与跨境传输有关的其他具体情况。与欧盟标准合同条款有 4 个模块不同，《条例草案》只规定了一种模式。根据《条例草案》，标准合同条款不得做任何修改，任何附加条款或其他规定不得直接或间接排除、修改或反驳条款规定。但是，经 ANPD 审查批准后，其他国家的标准合同条款可以视为《条例草案》标准合同的有效替代方案。全球性公司规则适用于同一经济集团的组织之间的数据传输，对该集团的所有成员都具有约束力。《条例草案》规定，通过此种方式跨境传输个人数据则公司必须建立和实施隐私治理计划，并概述了该计划的最低要求，如采取内部流程和政策确保遵守个人数据保护相关规则和良好实践。全球性公司规则制定后，需交由 ANPD 进行审批。

（十二）印度适用“通知限制”规范数据跨境流动

印度议会于 2000 年 10 月 17 日颁布 IT 法案，并于 2008 年 12 月 23 日颁布了《信息技术（修正）法案》（Information Technology (Amendment) Act, 2008）[38]。IT 法案及其修正案是印度处理网络犯罪和电子商务相关事项的主要法律。该法案及其修正案适用于在印度境内外处理以下个人信息的个人和组织：（1）在印度境内的个人信息；和（2）个人信息在印度境外，但使用位于印度的计算机、计算机系统或计算机网络处理的个人信息。虽然该法案及其修正案中的部分条款规定了针对网络上个人信息使用的保护，但主要侧重于信息安全，而不是数据保护。法案第 69A 条赋予了政府基于特定目的，禁止公众访问任何形成、传输、接收、存储或托管在任何计算机资源中的数据的权力。其中，该条所规定的特定目的包括，保护印度主权及保护国家安全与公共秩序，维持与外国友好关系，以及防止煽动实施与前述有关的任何可识别罪行等。这一条款为印度限制或禁止向境外传输的数据类型提供了一定的弹性空间，即任何类型的数据只要被政府认定为有损害

[37] See Aberta Consulta Pública sobre norma de transferências internacionais de dados pessoais, https://www.gov.br/anpd/pt-br/assuntos/noticias/aberta-consulta-publica-sobre-norma-de-transferencias-internacionais-de-dados-pessoais

[38] See Information Technology Act , https://www.meity.gov.in/content/information-technology-act；Information Technology (Amendment) Act, 2008, https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf

以上目的的风险，都有可能被禁止访问。实践中，印度信息电子与技术部曾援引 IT 法案 69A 条禁止用户在印度境内访问 59 款中国 APP，理由在于这些 APP 以非法方式收取用户数据并传输至境外的服务器，可能损害印度的主权以及国家安全与公共秩序。《信息技术（合理的安全实践和程序及敏感个人数据或信息）规则》（Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011）（以下简称"SPDI 规则"）由印度通信和信息技术部于 2011 年 4 月 11 日颁布[39]。SPDI 规则是 IT 法案项下的具体实施规则。该规则定义个人信息和敏感个人数据或信息，规定法人团体（或代表法人团体的个人）收集和处理敏感个人数据或信息时应遵守的具体要求，并界定了法人团体（或代表法人团体的个人）是否遵守合理的安全实践和程序的判定标准。SPDI 要求数据接收实体要确保与数据传输实体在 SPDI 规则下所遵守的相同数据保护水平。对于敏感个人数据或信息的跨境传输需履行数据传输实体和数据提供者之间的合法合同所必需；以及数据提供者同意。根据 SPDI 规则，收集和处理敏感个人数据或信息的任何实体（包括印度境外的实体）都必须实施合理的安全实践和程序。目前，SPDI 规则项下的合理的安全实践和程序包括：(1)国际标准 IS/ISO/IEC 27001；或(2)经印度中央政府批准和通知的行业协会最佳实践规范。上述合理的安全实践和程序还需经中央政府正式批准的独立审计师定期认证或审计。审计师应每年至少一次或当相关实体对其流程和计算机资源进行重大升级时进行审计。对于敏感个人信息以外的其他个人信息和非个人信息的跨境传输，印度目前尚无具体限制。

印度个人数据保护立法从《2018 年个人数据保护法案》开始，因法案过于严格等问题经反复修改、撤回以及更名，于 2022 年 11 月方才形成了第四版的《2022 年数字个人数据保护法案》。在《2022 年数字个人数据保护法案》的基础上，印度对立法进行相应的调整，并形成《2023 年数字个人数据保护法案》（Digital Personal Data Protection Bill，DPDP），2023 年 8 月 9 日，DPDP 最终在印度上院通过并于 8 月 11 日获得印度总统批准颁布于公报。在数据出境方面，DPDP 修改了《2022 法案》中较为严格的仅在中央政府进行必要因素评估后通知数据受托人方可个人数据出境的规定，改为中央政府可通知限制相应的个人数据出境行为。然而，DPDP 也指出其较为宽松的规定并不限制印度现行有效的任何法律的适用性，如该法律在与任何个人数据或数据受托人或其类别相关的方面为在印度境外的数据受托人转移个人数据提供更高程度的保护或限制。

[39] See Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, https://www.wipo.int/wipolex/en/text/338328

五、全球数据跨境流动规则特点与制约因素

（一）规则特点

1.多边机制推动数据跨境流动原则共识形成

多边机制和国际组织高度重视数据跨境流动的跨国协调问题，联合国、WTO、OECD、APEC、G20、G7 多年来致力于协调各国监管要求、提升各国监管一致性、促进数据跨境安全有序流动，成为推动共识形成的重要平台。联合国发布了《全球数字契约》，以开放、自由、安全为共同原则，针对成员国、区域组织和所有利益相关方等主体就数据保护和赋权这一议题提出了相应要求，致力于实现数字未来可持续发展。另一方面，联合国先后举办了联合国互联网治理论坛（IGF）和联合国世界数据论坛（UNWDF）以深化在全球发展倡议框架下的国际数据合作。IGF 致力于协调不同利益相关方形成具有一致认同和有效监管的跨境数据流动公共政策，发展“基于信任的数据自由流动”（DFFT）的概念，在利用数据传输创造经济价值的同时，解决各主体对数据隐私与主权的担忧。UNWDF 则更侧重于数据的可持续发展，通过促进数据创新和培育伙伴关系，营造更好的联合国数据生态系统。WTO 作为贸易协定的管理者和贸易立法的监督者，自创立以来便十分关注电子商务规则与数据跨境流动。2015 年至 2023 年八年间，不同成员国在多届部长级会议上相继发表《电子商务联合声明》，由此开启与贸易相关的电子商务多边谈判，推进制定高标准电子商务国际规则和搭建电子商务能力建设框架。但截至目前，WTO 电子商务谈判针对数据跨境流动议题分歧较大。OECD 开创了全球隐私保护和数据跨境流动规制的首次尝试。在成立相关工作组和专家组、召开研讨会等一系列早期准备的基础之上，OECD 于 1980 年发布《OECD 隐私指南》，明确了个人数据保护和数据跨境流动的基本原则，成为全球制定隐私保护与数据跨境制度的重要参考。近年来，OECD 通过数字经济政策委员会及数据治理和隐私工作小组发布众多研究报告，及时总结整理全球前沿政策和规制方式，弥补各国监管体系和机构设置之间的差异性。同样是区域性经济组织的 APEC 也积极投入到数据跨境流动治理中来。从 2005 年起，APEC 发布了《APEC 隐私框架》，并建立 CBPR 跨境隐私规则体系。一方面，CBPR 面向数据处理者建立了数据处理者隐私识别体系；另一方面，CBPR 创新性地建立了隐私执法机构和问责代理机构来衡量加入国认证企业的隐私保护水平，促进亚太地区个人信息保护措施的一致性和负责任的数据跨境流动。G20 主要围绕“基于信任的数据自由流动”的概念，不断推动各成员国形成共识，使数据能够信任地流动。《大阪数字经济宣言》标志 DFFT 进入实践阶段，《利雅得领导人宣言》《罗马领导人宣言》继续承认 DFFT 的重要性。此后，借助 G7 平台，通过《DFFT 合作路线图》《促进 DFFT 行动计划》《DFFT 实施计划》，DFFT 概念得到不断推广和深化。

表 11 多边机制和国际组织关于数据跨境流动的主张

主要主张		数据治理相关组织机制	相关研究报告
联合国	《全球数字契约》 《全球行动计划》	联合国互联网治理论坛 联合国世界数据论坛	《数字经济报告》 《G20 成员国跨境数据流动规则》
WTO	《电子商务工作计划》 《电子商务联合声明》	部长级会议 非正式部长级会议	
OECD	《关于隐私保护与个人数	跨境数据流动与隐私保护	《跨境数据转移的规制方

	据跨境流动指南》 “跨境数据流动宣言” “关于保护全球网络隐私的部长级宣言”	研讨会 跨境数据障碍与隐私保护专家组 数字经济政策委员会 数据治理和隐私工作小组	式的共同点》 《评估数据流的全球政策和举措》报告 《新兴的隐私增强技术：当前的监管和政策方法》报告
APEC	《APEC 隐私框架》 CBPR 跨境隐私规则体系	电子商务指导小组	
G20/G7	“基于信任的数据自由流动”		

2.全球数据跨境流动规则呈现三大模式特征

目前 WTO 电子商务谈判中，各成员方针对数据跨境流动等核心议题仍然存在较大分歧，规则共识在短期内难以达成，全球数据跨境流动规则呈现碎片化特征。而区域性贸易协定或数字经济专项协定成为促进数据跨境流动的主要方式，这种灵活性能够消除数据跨境流动障碍，从而为数据跨境流动治理提供有益示范，各国政府也越来越倾向于利用贸易协定来实现促进数据跨境自由流动，同时平衡和兼顾隐私保护及其他公共政策目标。据统计，截至 2023 年 5 月，已有 70 多个国家或地区都对数据跨境流动有所规制，已有超过 180 个区域贸易协定中增设了包括数据跨境流动在内的数字贸易规则专门章节或专门条款。例如以《美墨加协定》《全面与进步跨太平洋伙伴关系协定》《区域全面经济伙伴关系协定》为代表的区域或双边自贸协定，以及以《美日数字贸易协定》《数字经济伙伴关系协定》等为代表的数字经济专项协定，都将数据跨境流动治理、数据隐私保护等相关议题纳入了协定条款。

而在主要经济体层面，互联网技术的发展催生了与物理空间相对应的网络空间，数据跨境流动极大冲击了基于国家疆界的传统国家主权，尤其是一国的司法执法管辖权。对此，“信息主权”“数据主权”等概念被学者们相继提出。各国也纷纷出台维护数据主权的政策举措，但部分国家容易滥用数据主权，这些举措构成了对数据跨境流动的限制。

因此，通过归纳总结纳入研究的十大国际机制安排与十二大经济体，发现在国际组织“软法”的影响下，国际贸易协议、主要经济体演变出其有关数据跨境流动规则的独有特点。本次报告将上述关于数据跨境流动规则的安排划分为三种类型，分别为开放流动型、严格监管型以及监管例外型。

开放流动型主要表现为强调数据跨境的自由流动，典型的经济体如新加坡、东盟、美国等，国际经贸协定如 DEPA、USMCA 等。不过新加坡与美国所表现的方式有所不同，新加坡以及以新加坡等国家为主的 DEPA 体现的是外流特点，既是以新加坡为重要轴点向东南亚、亚太甚至全球流动。美国以及以美国为主导的 USMAC 体现的是内流特点，美国在与其他经济体签订的双边或者多边贸易协议中一直强调有限例外原则，旨在推动数据跨境自由流动，将全球数据流向美国境内，从而利用自身技术市场优势实现数据跨境流动的经济利益最大化。不过美国在主张数据自由流动的同时通过“长臂管辖”扩张其数据主权。如上文所述，美国的《澄清域外合法使用数据法案》（CLOUD 法案），提出了管辖“数据控制者”的新模式，即规定无论通信、记录或其他信息是否位于美国境内，美国的电子通信服务(ECS)或远程计算服务(RCS)提供者都有义务按照法定要求，保存、备份或者披露其拥有、监管或控制的用户或订户的通信内容以及任何记录或其他信息。

CLOUD 法案赋予美国执法机构访问和调取存储于美国域外数据的权利，其他国家对境内数据的控制权被削弱。

严格监管型主要强调数据跨境的事前监管，通过安全要求后方可进行数据出境，典型的代表为中国、俄罗斯、巴西、印度等，国际贸易协定主要为 RCEP 等。中国、俄罗斯、巴西等国家目前尚强调数据满足要求后才可出境，更加严格的如印度。2018 年 4 月，印度要求所有支付系统提供商应确保其系统运营相关的全部数据，包括端到端交易的完整详细信息，存储在印度境内的系统中，以便印度中央银行可以“不受限制地监管访问这些系统提供商存储的数据，以及他们的服务提供商/中介机构/第三方供应商和支付生态系统中其他实体存储的数据”。而 RCEP 虽然强调数据的自由流动，但是赋予了缔约国以“合法公共目的与安全例外”终止数据跨境流动的权利，事实上也强调了缔约国的事先监管权利。监管例外型虽然强调数据跨境的监管，但是如若在白名单或者生态机制内则可以享有“监管例外”的权利。典型的经济体如欧盟、英国、日本、韩国，国际贸易协定为 CPTPP 等。欧盟利用 GDPR 进行数据出境的监管，但是存在充分性认定的白名单，日本建立保护个人信息出境的监管机制，但是推动数据跨境生态圈与充分性认定规则。

3.标准和技术驱动的规制工具提供数据跨境安全传输新路径

一方面，部分国家和国际组织探索制定和出台了监管数据跨境流动的标准和原则以处理隐私保护与数据安全问题。美国国家标准与技术研究院（NIST）发布了 SP 800-66《隐私权利和数据泄露通知标准》；国际标准化组织（ISO）制定了 ISO/IEC 27701 全球性隐私信息管理体系标准，为数据跨境流动中的隐私保护和数据安全制定标准。另一方面，近年来，区块链、隐私计算等技术的发展和数据中介的出现为数据跨境传输提供了新的范式。国际数据空间协会提出利用数据空间，基于开放、透明和标准的数据共享系统，以实现安全可信的数据访问和共享传输。此外，隐私增强技术（PETs）、数据监管沙箱等也为数据跨境流动的应用实践提供了新的选择，如联合国 PET 实验室通过隐私增强技术为符合隐私保护的跨境数据传输提供技术解决方案。

在国际数据空间建设方面，欧洲已有国际数据空间组织（IDSA）、Gaia-X、Open DEI、FIWARE、My Data 等相关研究并推进数据空间的组织。目前，IDSA 是欧洲数据空间建设的重要推动者，其取得的成效也最为显著。根据 IDSA 数据统计，截止到 2023 年 10 月，共有 64 个使用 IDSA 技术标准的案例，以及 43 个使用 IDSA 技术标准的国际数据空间，合计 107 个应用场景。IDSA 将 107 个应用场景划分为移动交通、制造业、绿色协议、能源、供应链、汽车、跨领域、智慧城市、健康以及农业等十大类。

按照 IDSA 定义，数据空间是指“基于共同约定原则进行数据共享流通的可信任分布式数据生态系统基础设施”。在数据空间中，重要的不再是集中存储所有的数据，而是确保应用程序（如深度学习算法）能够以正确的方式接收和使用正确的数据。数据空间将提供能够实现数据互操作性的软基础设施。软件基础设施由技术中立的协议和标准组成，规定了组织和个人参与数字经济的方式，以及根据共同同意的规则和指令进行行事和行为的方式。由于所有参与者实施了相同的最小功能、法律、技术和运营协议和标准，因此无论他们处于哪一数据空间，他们都可以用相同的方式进行交互。构成软件基础设施的元素是互补关系，因此从一开始就整体设计这些协议和标准将使数据空间具备耦合性。为了建立符合特定行业的数据空间，需要用行业特定的措施来补充软件基础设施。

由于欧洲数据空间的实践，国内以中国信通院为代表的智库参考欧洲数据空间的建设，正在基于特定行业与公共数据积极推动国内可信数据空间的构建。按照中国信通院定义，可信数据空间是数据要素流通体系的技术保障，通过在现有信息网络上搭建数据集聚、共享、流通和应用的分布式关键数据基础设施。可信数据空间以体系化的技术安排确保所签订的数据流通协议能够履行和维护，解决数据要素供方、使用方、服务方、监管方等主体间的安全与信任问题。因此，可信数据空间在平衡规模经济效益和竞争效益方面具有天然优势，它可以搭建安全可信的数据流通环境，构建共同认可的规范及价值，在空间内实现数据集聚，发挥数据乘数效应，实现数据赋能全行业发展。未来，基于数据空间的数据跨境流动将成为数据跨境流动新范式。

（二）制约因素

1.各经济体在数据价值链中的利益冲突制约数据跨境流动

数据跨境流动催生全球数据价值链，带来巨大的经济价值，但各国由于收集处理分析数据的能力、数字技术水平等方面的差距，从数据跨境流动中的获益能力也存在显著差异。在数据价值链背景下，拥有先进数字技术和大型跨国数字平台的国家处于数据价值链的中高端位置，是原始数据的进口国和增值数据产品的出口国，从数据跨境流动中的获益能力最强。而大多数发展中国家和最不发达经济体是原始数据的出口国和增值数据产品的进口国，位于数据价值链低端环节，这些国家不仅少从数据跨境流动中获益，其数字产业甚至部分传统产业还可能受到发达国家跨境电商和数字产品的冲击。这意味着数据跨境流动将不可避免带来新的利益冲突，而各国为了维护自身利益对数据跨境流动采取不同态度，如何协调各国利益冲突成为制约数据跨境流动国际规则形成的主要因素。

具体而言，美国凭借其全球领先的数字技术、竞争力最强的跨国数字平台和全球领先的数字服务贸易，在全球数据价值链中收益能力最强，因此主张数据跨境自由流动和计算设施非强制本地化存储。美国拥有苹果（Apple）、微软(Microsoft)、亚马逊(Amazon)、元（Meta）等数量最多、影响力和竞争力最强的跨国数字平台，根据联合国贸发会议发布的《数字经济报告 2021》，截至 2021 年 5 月，全球百家数字平台中有 41 家来自美国，市值占比为 67%，远高于其他国家。美国在云计算等数字服务贸易方面领先，美国的云计算提供商如亚马逊云服务（AWS）和微软 Azure 也占据了全球云计算市场的主导地位，它们通过提供全球性的数据存储和处理服务而产生巨大经济价值。根据 Gartner 发布的 2021 年全球云计算 IaaS 市场追踪数据，亚马逊和微软分别占全球云计算 IaaS 市场 38.92%和 21.07%的市场份额。美国数字服务贸易全球领先，根据联合国贸发会议（UNCTAD）测算数据，2021 年，美国可数字化交付服务贸易出口额为 6130.12 亿美元，居全球首位。美国是全球数字内容产业领域最先起步发展的国家，其中数字动漫、网络游戏、数字音乐以及网络视频是美国数字内容产业中发展最为迅速的部分。数据跨境自由流动给美国带来的利益最多，而本地化要求会给美国数字企业全球化经营带来额外负担。因此，基于其在数字经济和数字技术领域的领先优势，美国不断谋求在 OECD、G20、APEC 等有关数据流动的国际讨论中发挥主导作用，还通过缔结贸易协定占据国际规则制定的先机，强调数据跨境自由流动，以便破除数据流通壁垒，实现他国数据流动向美国的流动。

欧盟数字经济的幼儿、数字规则的巨匠。欧盟身处数字经济边缘，缺乏大型数字平台，因此欧盟以“保障基本权益+构建单一市场”为主要诉求，实施“内松外严”的数据保护政策致力于构建欧盟单一数字市场，进

而通过单一数字市场优势引领全球数据规则和标准的制定。根据联合国贸发会议发布的《数字经济报告2021》，截至 2021 年 5 月，全球百家数字平台仅有 12 家企业来自欧洲，市值占比仅为 3%，远低于美洲和亚洲。欧盟于 2018 年正式生效实施《通用数据保护条例（GDPR）》，在欧盟内部统一实施单一的个人数据保护法令，推动欧盟范围内数据自由流动，打造单一数字市场。而此后 2019 年《非个人数据自由流动框架条例》则补充了对非个人数据传输的法律规制，欧盟的基本立场是禁止数据本地化，确保除个人数据以外的数据在欧盟内自由流动[40]。对于欧盟境内个人数据向欧盟境外传输，欧盟树立了高标准数据保护规则，即个人数据只可以流向数据保护水平和欧盟相同的国家或地区。在具体实施路径上，通过欧盟委员会“充分性认定”[41]，确定数据跨境自由流动白名单国家，而非获认定地区的各类组织和企业可以根据欧盟认可的标准合同条款、约束性公司规则、行为规范、认证机制等进行数据跨境传输。近年来，欧盟凭借其市场优势，不断将数据保护的“欧洲标准”上升为“全球标准”，产生数据治理领域的“布鲁塞尔效应”，对世界范围内的数据治理变革发挥引领作用。以 GDPR 为例，不仅越来越多的国家以 GDPR 为范本制定数据保护规则，而且诸多大型跨国企业基于 GDPR 进行数据和业务合规。

新加坡作为一个小而开放的国家，是亚太地区数据中心、各类先进数字技术试验地和各类新兴业务的发源地，是全球数据汇聚与流动、数字技术应用创新的重要枢纽和节点，高度依赖数据跨境流动促进数字经济增长和数字技术创新发展。新加坡自 2000 年完全放开电信市场，解除国外企业以直接或间接投资方式进入本国电信产业的限制，有力推动新加坡数字基础设施建设，成为亚太地区数据中心。Salesforce、Digital Realty、Equinix、Meta、脸书、谷歌、字节跳动和中国移动、腾讯等大型跨国科技企业均在新加坡投资建设数据中心，微软 Azure、亚马逊 AWS、谷歌云、阿里云、腾讯云、金山云等云计算公司均将新加坡作为区域运营中心。此外，新加坡以鼓励投资和创新为导向，对加密货币、金融科技、人工智能等领域持开放包容的监管态度，构建数字技术创新发展生态。因此，新加坡致力于寻求区域内的数据自由流动。新加坡于 2018 年加入了 APEC 跨境隐私规则系统（CBPR）和处理器隐私识别系统（PRP）。此外新加坡主导与多个主要经济体签订多双边数字经济规则协定，破除数据跨境流动壁垒。2022 年以来，新加坡与智利和新西兰签订《数字经济伙伴关系协定（DEPA）》，与澳大利亚签订《新加坡-澳大利亚数字经济协定（SADEA）》，与英国《英国—新加坡数字经济协定（UKSDEA）》，与韩国签订《韩国-新加坡数字经济协定（KSDPA）》；2023 年 2 月，新加坡与欧盟签订《欧盟——新加坡数字伙伴关系协定》，下一步将推动与欧盟之间的数据跨境流动。

中国在数字技术和数字平台竞争力方面仅次于美国，我国数字贸易比较优势集中在以货物为载体的跨境电商方面，数字服务贸易增长迅速。中国拥有数量和市值仅次于美国的跨国数字平台，根据联合国贸发会议发布的《数字经济报告 2021》，截至 2021 年 5 月，全球百家数字平台中有 45 家来自中国，市值占比为

[40] 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 (Text with EEA relevance) Article 1 Subject matter This Regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localization requirements, the availability of data to competent authorities and the porting of data for professional users.

[41] 截至 2023 年 7 月 10 日，欧盟官网公布的通过数据保护充分性认定的国家或地区共计 15 个：安道尔公国、阿根廷、加拿大（限于商业组织）、法兰群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、韩国、瑞士、英国、乌拉圭、美国。

29%，仅次于美国。中国跨境电商优势明显，2022 年，我国跨境电商进出口规模突破 2 万亿元，五年增长了近 10 倍，跨境电商主体超 10 万家，跨境电商贸易伙伴遍布全球，涌现出了阿里速卖通、Shein、Temu 等一批全球性数字平台企业。中国数字服务贸易增长迅速，根据联合国贸易和发展会议（UNCTAD）测算，2011-2022 年中国数字服务出口年平均增速为 9.88%。中国是全球数字内容产品进出口大国，目前是仅次于美国的全球第二大网络游戏出口国。由于中国数字贸易发展优势仍集中于以货物为载体的跨境电商，因此近年来中国在 WTO 电子商务谈判中主要诉求集中在电子商务便利化方面。而在数据跨境流动方面，对外主张以保障国家安全、尊重各国监管要求为前提，对内则构建基本完善的数据出境安全管理框架，总体而言，我国数据跨境流动监管制度较为严格。2023 年 9 月 28 日，国家网信办就《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见，有望在数据跨境流动方面迎来新突破。

而对发展中国家和最不发达经济体而言，数字经济发展进一步加深了发达国家同发展中国家、最不发达经济体之间的数字鸿沟，数字不平等问题日益严重。与发达国家主张数据自由流动、促进数字贸易全球发展不同，发展中国家、最不发达经济体由于在数字经济发展中的滞后性，当前主要关注如何改善数字鸿沟、提升数字能力建设的问题，坚持保留国内产业政策空间，要求数字经济增长不仅要关注效率还需兼顾公平。如尽管在 2019 年的 G20 峰会上 24 个国家签署了日本主导的“大阪数字经济宣言”，发展“基于信任的数据自由流动”，但印度、南非、印尼等发展中国家并未签字。在 WTO 电子商务谈判中，发展中国家主张不将数据跨境流动议题纳入谈判议程。

2.数据安全风险阻碍数据跨境流动

数据跨境流动给全球带来发展机遇的同时也产生了新的安全风险。伴随数字技术的快速发展，数据安全问题日益凸显，自 2013 年“斯诺登”事件后，各国日益重视数据跨境流动引发的国家安全风险。个人信息的泄露容易导致国家公民的个人信息被境外所窃取、利用，造成对个人隐私的侵害，甚至引发针对个人的网络诈骗与电信诈骗，严重危害公民个人财产与人身安全。国家重要数据、核心机密数据的泄露将导致国家秘密的外泄，容易被境外不法分子、恐怖主义所利用，对国家的政治安全、经济安全等构成巨大威胁，严重侵犯国家主权和安全利益。例如，2022 年，国家计算机病毒应急处理中心在西北工业大学遭遇美国国家安全（National Security Agency, NSA）网络攻击事件的调查报告中指出，NSA 下设的“特定入侵行动办公室”近年来对我国开展恶意网络攻击高达上万次，通过控制各类网络设备先后窃取了超过 140GB 的高价值数据，对我国国家安全和数据主权造成了严重侵害。再如，据《2020 年中国互联网网络安全报告》，境外“白象”“海莲花”“毒云藤”等 APT 攻击组织以“新冠肺炎疫情”“基金项目申请”等相关社会热点及工作文件为诱饵，向我国重要单位邮箱账户投递钓鱼邮件，诱导受害人点击仿冒该单位邮件服务提供商或邮件服务系统的虚假页面链接，从而盗取受害人的邮箱账号和密码。据《2020 年中国互联网网络安全报告》，2020 年，中国共发现国内基因数据通过网络出境 717 万余次，流向境外 170 个国家和地区。

数据流动与数据安全之间存在天然冲突，各国高度重视数据跨境流动带来的安全风险。目前各国都存在不少基于国家安全考虑限制数据跨境流动的立法，即使是数据安全保护能力最强、主张数据跨境自由流动的美国也不例外。以美国为例，2010 年，美国建立了受控非密信息清单（Controlled Unclassified Information，简称“CUI”）。美国《信息安全纲要》规定，需要保护和控制传播的非密信息均属于 CUI，需采取严格的管理

措施。近几年，美国政府大幅提升了对CUI 清单的管控力度，CUI 包括关键基础设施、国防、金融、移民、情报、国际协议、税收、核等 20 大类、124 子类，按照风险程度予以不同管控。我国在《网络安全法》及特殊敏感行业规定中确立了数据跨境流动管理的要求，确立了分级分类管理制度，如针对金融、交通、健康、保险、征信、地图、网络出版等特定行业数据，均设置了“禁止出境”或本地化存储的要求。

3.个人隐私保护制约数据跨境流动

个人隐私保护问题是数据跨境流动规则制定最早也是最核心的关切。个人隐私保护和促进数据流动二者相悖，个人隐私保护需要以舍弃数据流动性为代价，而数据流动往往会导致隐私泄露[42]。OECD、APEC 等国际组织早期关于数据跨境流动规制的尝试均围绕个人隐私保护问题展开，即如何在保护个人信息的前提下促进数据跨境流动。如 OECD 于 1980 年发布的《隐私指南》是全球层面对数据跨境流动进行规制的首次尝试，即明确了个人数据保护的八项基本原则，成为各国及其他经济体制定个人信息保护法律制度的重要参考。

隐私保护问题是美欧长期以来在数据跨境流动问题上最大的冲突点。欧盟将个人数据保护视为基本权利，并予以严格的高标准保护。欧盟认为其境内个人数据只能流向保护水平与其等同的国家或地区，不能流向保护水平不如欧盟的“洼地”，并通过 GDPR 在全球范围内推行。而美国在隐私保护方面更强调市场驱动，并未将个人隐私视为基本权利，只是将其纳入市场经济中消费者保护的范畴。在联邦层面，美国没有统一的个人信息保护立法，只是由美国联邦贸易委员会(FTC)确保消费者对其信息数据的使用有知情和同意的权利。因此美国实际上反对个人信息保护欧盟的“高标准”，而是主张各国可以按照自己的方式予以保护，并促进各国个人信息保护制度的兼容性，提出限制个人信息跨境流动应该是“必要的且与所面临风险成比例”。围绕个人信息保护问题，欧美之间从《安全港协议》到《隐私盾协议》的破产,再到 2023 年 7 月 10 日欧盟委员会通过《欧盟-美国数据隐私框架》的充分性认定,欧美双方围绕隐私保护问题产生多次冲突与摩擦，不断推翻原有协议，终于再次建立起稳定的跨大西洋数据流动安排。

[42] 专访 方滨兴：破解数据要素流动与隐私保护相冲突的局，2023 年 05 月 07 日.

六、全球数据跨境流动规则的趋势研判及对我国的影响

（一）趋势研判

当前,全球数据跨境流动规则尚未达成最终共识，全球数据治理呈现碎片化特征，各国家基于国家安全、产业发展等情况,构建了特征不同的数据跨境流动监管制度与治理模式。美欧基于自身利益诉求形成较为明晰的规则主张，并致力于在全球范围内构建基于信任的数据跨境流动自由圈，同时，数据主权、安全、隐私问题仍是全球数据跨境流动治理的核心关切。

1.数据跨境流动规则主张趋向“数据重商主义”

各经济体数据跨境流动规则主张建立在自身经济利益基础上,呈现“数据重商主义”趋势。何一种规则主张的本质都是各国基于发展实际和国家利益而做出的“数据重商主义”选择。例如,开放流动型的美国基于自身数字技术、数字平台发展优势,在国际上高调呼吁推动数据跨境自由流动,但同时也通过制定重要数据清单对一些涉及安全或关键技术的数据进行出境限制,呈现出“宽入严出”的特点。监管例外型的欧盟所推行的数据跨境自由流动则是以高标准的个人数据保护为前提。欧盟对内以《非个人数据自由流动条例框架》《数据治理法案》等促进数据在各成员国之间自由流动;对外则是通过设立高标准个人数据保护壁垒对内部数据流出进行严格限制,呈现出“内松外严”的特点。严格监管型的俄罗斯、印度则以数据本地化政策要求数据回流,以保护主义政策推动本国 IT 产业发展。中国和新加坡所主张的数据跨境自由流动则是以维护数据主权和保障国家安全为前提。各国根据实际利益制定形形色色的跨境数据流动规则来保护本国数字产业发展,全球数据跨境流动规则与治理呈现“数据重商主义”趋向。

同时，在“数据重商主义”的驱动下，以美国、欧盟、日本为代表的国家基于信任关系或意识形态趋同推动构建数据跨境流动圈,全球数据跨境流动规则制定呈现出“政治泛化” 特征。美国正在通过强势的外交政策拉拢其盟友推动基于信任关系的数据自由流动，并针对中国、俄罗斯等“敌对国家”实行数据封锁,印度等国家和地区也在跟进对我国实行数据跨境流动限制。经合组织(OECD)的数字经济政策委员会(CDEP)在 2020 年 12 月声称:“努力实现政府对私营部门持有的个人数据的可信任的访问,是一个紧迫的优先事项”,而“缺乏受信任的政府访问个人数据的共同原则,可能会导致对数据流动的不适当限制,造成有害的经济影响”。美国与欧盟、日本、韩国意识形态和政治利益趋同,是传统的政治、军事盟友,美国正在拉拢盟友将所谓“缺乏受信任”的国家政府排除在数据自由流动圈子之外。首先，美国在 OECD、APEC、G20、G7 等国际组织中谋求主导地位。美国于 2015 年主导建立 APEC 的 CBPR 体系，目前共有 9 个国家或地区加入。近年来美国寻求将 CBPR 体系独立于 APEC 框架外，允许更多非 APEC 成员加入，此举被认为是为了排除中国加入 CBPR 体系。其次，美国及其盟友通过区域贸易协定或数字贸易专项协定，已经基本打通数据跨境自由流动圈。欧盟与美国 2022 年在已废除的隐私盾协议基础上建立了《欧美数据隐私框架》，欧盟委员会于 2023 年 7 月投票通过了《欧美数据隐私框架》的充分性认定，美欧之间继《安全港协议》《隐私盾协议》之后再次建立起稳定的数据跨境流动框架。此外，《日本-欧盟经济贸易协定》、《美国-韩国自由贸易协定》、《美国-日本数字贸易协定》等区域贸易协定或数字贸易协定均已生效,且都专门设定了包括数据跨境流动在内的数字贸易规则章节或条款。此外，美国与欧盟成立美欧贸易与技术委员会(U.S.-EU Trade and Technology Council,以下简称“TTC”)，主导与

澳大利亚、日本等 13 国启动“印度太平洋经济框架”（IPEF），建立更多合作机制，与盟友在政策上寻求协调，在规则上寻求共识，将在包括关键技术数据出口、数据跨境流动等方面采取更多努力，遏制竞争对手。

表 12 主要经济体达成的数据跨境流动先关协议、协定

国家、地区		框架	签订时间
美国	欧盟	《跨大西洋数据隐私框架》	2022.03.25
		《欧盟-美国数据隐私框架协议》	2023.07.10
	英国	《大西洋宣言：二十一世纪美英经济伙伴关系框架》	2023.06.08
新加坡	欧盟	《欧盟——新加坡数字伙伴关系协定》	2023.02.01
	英国	《英国—新加坡数字经济协定（UKSDEA）》	2022.02.25
	智利、新西兰	《数字经济伙伴关系协定（DEPA）》	2020.06.12
欧盟	阿根廷	《欧盟数据保护充分性认定》	2021.04 前已通过
	日本		
	安道尔公国		
	加拿大		
	法罗群岛		
	根西岛		
	以色列		
	马恩岛		
	泽西岛		
	新西兰		
	瑞士		
	乌拉圭		
	韩国		2021.12.17
	英国		2021.04.13
	美国	2023 年 7 月	
欧盟 GDPR 国家和地区		奥地利、比利时、保加利亚、克罗地亚、塞浦路斯、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰人、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典；挪威、列支敦士登、冰岛；亚速尔群岛、马提尼克岛、圣马丁岛等	
APEC 数据隐私框架国家和地区		美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、菲律宾、中国台湾	

2.数据跨境流动规则呈现行业精细化趋势

各国数据跨境流动规则针对重要行业数据进行精细化分级分类管理,数据跨境流动规则呈现行业精细化趋势。欧盟、美国等都根据本国产业实际需要确立了重要数据目录清单并制定了具体细则,构建了数据跨境流动分级分类监管模式，旨在对涉及国家战略、商业秘密、国家安全、高科技等敏感数据的出境进行限制。如美国制定CUI（非密受控信息）清单，对关键基础设施、国防、金融、移民、情报、国际协议、税收、核等20 大

类、124 子类，按照风险程度予以不同管控。美国还通过限制重要技术数据出口以及特定领域的外国投资进行数据跨境流动管制。2018 年 8 月签署生效的《美国出口管制改革法案》规定，出口管制不仅限于“硬件”出口，还包括“软件”，如科学技术数据传输到美国境外的服务器或数据出境，必须获得商务部工业和安全局（BIS）的出口许可。在外国投资审查方面，2018 年 8 月，美国通过了《外国投资风险评估现代化法案》（Foreign Investment Risk Review Modernization Act，简称“FIRRMA”），并建立了与 ECRA 之间的联动机制[43]，进一步收紧了对外国投资的国家安全审查程序。该法案规定了外商投资中的数据出境行为。根据 FIRRMA 第 1703 条，涉及敏感个人数据、关键基础设施和关键技术的美国企业的其他投资（包括非控制性外商投资）也要受美国外商投资委员会的审查，以防止外国投资者通过投资来获取美国的个人数据或关键技术。我国也在《网络安全法》以及相关行业规定中确立了数据跨境流动管理要求,以数据出境安全评估制度和数据分级分类管理机制为主,以国家安全为导向,对金融、交通、健康、保险、征信、地图、网络出版等特定行业数据、科研性质的特殊数据等核心数据严禁出境。

3.主权与安全隐私仍是规则制定的核心考量

数据主权、数据安全、隐私保护问题仍是未来数据跨境流动治理面临的核心关切，如何协调各国监管要求、贸易利益同时促进数据跨境流动是未来须应对的难题。一方面，目前许多国家和地区都在推进数据主权战略部署，尤其针对重要数据、敏感数据、核心机密数据、特定行业数据出境进行严格管制。如美国虽然基于其经济利益主张数据跨境自由流动，但同时也是全球最早部署数据主权战略建设的国家,其长臂管辖尤为突出。俄罗斯的数据主权战略囊括在其严格实施的数据本地化政策框架之下,颁布一系列法案对数据主权进行保护。我国则出台了《网络安全法》《数据安全法》《个人信息保护法》等顶层法律、配套细则办法以及特定行业规制，构建数据出境安全管理框架，旨在对重要数据出境进行安全评估和管理,维护我国数据主权。未来随着大数据、云计算、人工智能等新一代信息技术越来越广泛应用于经济社会、军事国防等各个领域，数据作为基础性、战略性资源的重要性将日益凸显，“数据主权”成为继边防、海防、空防之后的另一个主权空间。另一方面，数据安全面临新技术冲击。5G、大数据、云计算、人工智能、物联网等数字技术的发展及应用，给数据安全、隐私保护带来新的威胁，隐秘在新技术外衣下的数据泄露、数据贩卖、数据侵权等数据安全事件频发。如在使用 ChatGPT 的过程中，可能涉及个人信息、重要数据出境行为，如果使用不当，将对个人隐私、商业秘密、国家安全造成严重威胁。再如，大量数据通过各类传感器或终端采集，包括人脸数据、基因数据等个人敏感信息，及关键基础设施分布等关系国家安全的重要数据。相关机构估算，一辆自动驾驶测试车辆每天产生的数据量最高可达 10TB[44]。随着数字技术的深入发展和应用，数据主权、数据安全、隐私保护等核心问题将更加突出，未来如何协调各国监管要求、贸易利益同时促进数据跨境流动成为难题。

[43]刘瑛,孙冰.与外资安审联动的美国技术出口管制制度及中国应对[J].国际贸易,2020,(06):

[44]八位两会代表委员建言智能汽车数据安全：黑匣子要掌握在自己手中
https://auto.ifeng.com/qichezixun/20210308/1544217.shtml

（二）对我国的影响

当前，各国加快构建符合自身发展利益的数据跨境流动制度体系，各国数据跨境流动规则主张趋向“数据重商主义”，全球数据跨境流动规则呈现多样化、复杂化、差异化、行业精细化特征。一方面，美西方国家正在基于信任关系构建排除我国的数据跨境流动自由圈，数据主权、数据安全、隐私保护等核心问题仍然制约着数据跨境流动全球治理与规则形成。在此趋势下，我国数字企业出海将面临越来越多的数据合规风险，我国数字产业发展面临数据封锁困境，我国数字贸易面临较高的政策不确定性。另一方面，我国于 2021 年正式申请加入 CPTPP 和 DEPA,目前正在积极推进谈判进程。加入 CPTPP 和 DEPA 将为我国数字企业出海、数字产业合作、数字贸易发展营造稳定制度环境。但 CPTPP 和 DEPA 在数据跨境流动议题上的开放标准较高，我国仍需进一步借助自贸试验区、自贸港等高水平开放平台，对标高标准规则，开展先行先试和压力测试。

1.我国数字企业出海将面临数据合规风险

当前，我国数字企业正处于加速成长、出海拓展的关键时期，阿里速卖通、Shein、Temu、Tiktok 等一批数字平台企业加速出海，数据合规成为未来数字企业拓展海外市场的“必修课”。

一方面，美西方国家泛化安全问题，我国出海数字企业面临越来越多的数据合规风险。当前美西方国家正在主导建立基于信任关系的数据跨境流动自由圈，而我国作为“不受信任国家”被排除在外。近年来，美国针对我国应用程序的数据安全性审查持续不断。2023 年 4 月 14 日，美国美中经济安全审查委员会(US China Economic and Security Review Commission，简称“USCC”）[45]发布《Shein, Temu 和中国电商：数据风险、货源违规和贸易漏洞》专项调查报告，提出 Shein 利用用户数据和搜索历史，通过 AI 算法预测时尚趋势，但 Shein 缺乏有效的用户数据保护措施。纽约州于 2022 年对 Shein 的母公司 Zoetop 处以 190 万美元的罚款，原因是个人数据处理不当导致 3900 万个账户的用户数据泄露。中国出海社交媒体平台 TikTok 更因数据存储安全和算法推荐操纵的问题受到美国制裁，目前美国蒙大拿州众议院已通过全面禁止 TikTok 的法案。在欧洲方面，自 2018 年欧盟 GDPR 正式落地实施以来，欧盟针对跨国数字平台企业数据合规的执法力度正在逐步加强，据统计 2021 年欧盟数据保护监管机构针对 GDPR 违规的罚单总金额约 10 亿欧元，2022 年 GDPR 罚单总金额达到 16.4 亿欧元。如近年爱尔兰数据保护委员会对 Meta 分别处以 4.05 亿欧元、3.9 亿欧元、12 亿欧元的巨额罚款，卢森堡数据保护委员会对亚马逊平台处以 7.46 亿欧元罚款。而目前我国不在欧盟 GDPR 数据保护充分性认定白名单中。我国出海数字平台均涉及大量用户数据，随着我数字平台企业在欧美市场的竞争力和影响力逐步增强，未来美欧势必不断泛化数据安全问题，对我国数字企业进行打压，未来我国数字企业出海如何规避数据合规风险成为亟需解决的难题。

另一方面,我国申请加入 CPTPP 和 DEPA 等高标准数字经济协定，将为我国数字企业开拓海外市场降低数据合规成本、提供稳定的制度保障。2021 年，我国正式提出申请加入 CPTPP 和 DEPA。目前，在我国签署的贸易协定中，仅 RCEP 涉及“电子方式跨境传输信息”规定，代表了我国在数据跨境流动议题上最高开放

[45] USCC 是美国国会创立的一个独立政府机构，直接向美国国会和总统提供政策建议，虽然其发布的内容没有法律约束力，但是有可能对美国联邦立法产生深刻影响。

水平。DEPA 和 CPTPP 比 RCEP 在数据跨境流动方面标准和要求更高，这要求我国对标高水平数字经济规则，依托自贸试验区、自贸港等高水平开放平台进行先行先试和压力测试。近期，国家网信办就《规范和促进数据跨境流动规定（征求意见稿）》，向社会公开征求意见。该意见赋予自贸试验区可自行制定“负面清单”的权力，我国数据跨境流动监管将迎来新突破。从我国数字企业在全球数据价值链中的地位来说，我国拥有阿里巴巴、腾讯、滴滴、拼多多、TikTok 等全球性数字平台，在全球数据价值链中占据重要地位。加入 CPTPP 和 DEPA 将为我国数字企业进入东盟、日本等特定市场提供良好的制度保障和便利的数据跨境流动机制，将降低数字企业数据合规成本，符合我国数字企业的发展诉求。

2.我国数字产业发展的数据壁垒可能加深

目前我国关键数字产业面临着核心技术受制于人的困境，高端芯片、操作系统、工业设计软件等均是我国被“卡脖子”的短板。而我国关键数字产业实现突破创新将面临数据封锁困境。

一方面,数据跨境流动规则的政治化、阵营化和行业精细化趋势，使我国数字产业发展面临数据封锁困境。芯片作为现代工业的基础、数字经济的引擎，已经深深嵌入到汽车、通信、能源、国防等许多行业的数字化进程中，也影响着人工智能、5G、边缘计算等关键数字技术的发展，决定了数字产业发展的未来。而芯片行业是资本、知识、技术密集型行业，是高度全球化和各国发挥比较优势分工协作的结果。全球芯片供应链具有高度复杂性、如欧盟在芯片设计环节的核心知识产权领域和制造环节的生产设备领域具有优势，但在先进芯片制造环节依赖亚洲（如韩国等），芯片设计工具依赖美国。欧美等国基于产业利益和数据主权制定“数据重商主义”色彩浓厚、附带意识形态偏见、针对高科技敏感行业进行封锁的数据跨境流动规则，将阻碍我国融入全球开放创新生态和贸易投资网络，切断我国重要数字产业的供应链，可能会阻碍我国数字产业升级发展,导致关键数字产业难以突破底层核心技术,数字产业安全风险增加。

另一方面,我国申请加入 CPTPP 和 DEPA,有利于同东盟国家探索数字产业合作机会。当前我国积极参与 WTO 电子商务谈判,同时申请加入 CPTPP、DEPA 等区域贸易协定,正在为构建一个凝聚更多共识、尊重各方利益的数字贸易治理规则框架而努力。东盟是我国第一大贸易伙伴,同时包括新加坡在内的东盟大部分国家都是 RCEP、CPTPP 成员国,新加坡是 DEPA 的主要成员。加入 CPTPP 和 DEPA，有利于我国数字产业在被欧美打压的情况下，同新加坡为代表的东盟国家开展更多有益合作,挖掘新的产业增长点。如新加坡是亚太地区数据中心、各类先进数字技术试验地和各类新兴业务的发源地，是全球数据流动、数字技术应用创新的重要枢纽和节点。此外，新加坡以鼓励投资和创新为导向，对加密货币、金融科技、人工智能等领域持开放包容的监管态度，构建数字技术创新发展生态。未来我国可以同新加坡在人工智能、金融科技、数字货币等领域探索开展更多数字产业合作和政策对接，形成互惠互利的合作模式，打造中新数字产业开放创新生态。

3.我国数字贸易面临较高的政策不确定性

当前，数据跨境流动规则所呈现出的碎片化、动态化、政治化、阵营化等趋势,导致出口企业面临的贸易政策不确定性显著增强,制约我国数字贸易创新发展。

一方面,数据跨境流动规则所呈现的碎片化、动态化、多样化等趋势,导致出口企业面临的贸易政策不确定性增强。目前各国基于自身利益诉求及监管目标制定本国数据跨境流动规则。如美国对数据跨境流动保持

“宽入严出”的政策。欧盟制定“内松外紧”政策,在个人隐私和个人权益得到保证前提下允许数据自由流动。目前欧盟 GDPR 构建了多层次的个人数据跨境传机制(充分性认定、SCCs 与 BCRs 等其他额外数据保障措施),但大多数国家并未制定与之互认的传输机制。我国基在《网络安全法》《个人信息保护法》《数据安全法》顶层立法及配套实施细则、指南的规制下，建立了严格的数据出境安全制度。虽然我国一定程度上借鉴了 GDPR 的 SCCs 和认证机制等,但仍坚持着严格的事前监管原则(数据出境安全评估机制等)。严格且具有差异性的数据出境安全管理制度一定程度上造成了数字贸易发展壁垒，给数据密集型的跨国数字企业带来高昂的制度成本。主要国家对数据跨境流动监管的差异性将带来数字贸易政策的不确定性,监管政策的动态发展也会扰乱出口企业对未来收益与损失情况的权衡,提高企业面临的不确定性,阻碍我国数字贸易发展。

另一方面,我国申请加入 CPTPP 和 DEPA,对标高标准数字经济规则，在区域内探索形成便利的数据跨境流动机制、可互操作的贸易便利化措施、以及稳定的数字贸易环境，将有利于我国数字贸易发展。就数据跨境流动议题而言，CPTPP 和 DEPA 均强调促进各国个人信息保护制度的兼容和可互操作。如 CPTPP、DEPA 列举了可能的兼容性机制：对监管结果的互认、更广泛的国际框架、对各自法律框架下数据保护可信任标志或认证框架的互认。由于新加坡国内建立了数据保护可信任标志，因此在 DEPA 中推进数据保护可信任标志的互认。目前我国在数据保护可信认证方面尚处于探索阶段，通过对标高标准数字经济规则，加快推进我国数据保护可信认证落地实施并与主要经济体互认，将有利于构建便利化的数据跨境流动机制，促进我国数字贸易发展。

七、思考建议

当前，全球数据跨境流动治理与规则正处于形成过程中，美欧等大国围绕数据跨境流动的规则博弈不断加剧，我国初步构建了较为严格的数据出境安全管理制度，尚未形成具有全球约束力的数据跨境流动全球治理和规则体系。下一步我国应统筹安全与发展，试点探索数据跨境流动安全管理便利化机制，增强数据跨境流动安全保障能力，推广数据跨境流动治理中国方案，提升全球数据治理话语权。同时，鼓励我国境内企业在数据出境时按照我国相关法律做好出境安全合规，在将数据引入我国时，遵守数据来源国的相关法律要求，并利用利用上海数据交易所国际板探索数据跨境流动新模式。

（一）探索数据跨境流动安全管理便利化机制

目前我国依托自由贸易试验区、自贸港等高水平开放平台探索数据跨境流动安全管理试点，如上海自贸试验区临港新片区、北京自贸试验区、海南自由贸易港、雄安新区片区等都加快推出了包括实施国际互联网数据跨境安全有序流动、促进数字产业开放发展等制度突破创新等举措。2023 年 9 月 28 日，国家网信办就《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见，赋予自贸试验区制定数据出境“负面清单”的权利。下一步应充分发挥开放平台制度创新优势，在数据出境安全评估、个人信息保护认证、标准合同备案等方面率先探索，逐步探索形成数据跨境流动便利化路径，形成可复制、可推广的经验。支持北京、上海、粤港澳大湾区等地在实施数据出境安全评估、个人信息保护认证、个人信息出境标准合同备案等制度过程中，试点探索形成可自由流动的一般数据清单。支持各自贸试验区统筹安全与发展，结合企业数据出境的实际需求，探索制定数据出境“负面清单”。依托上海数据交易所等数据交易平台，提供数据跨境流动合规服务，如设立数据安全与治理公共服务平台，吸引一批有数据跨境需求的企业以及优质数据合规的服务机构入驻，为数据出境企业提供政策咨询、风险评估、安全培训、自评估报告完备性审查等数据安全合规服务。

（二）推进数据保护可信认证试点与新技术应用

数据保护可信认证是很多国家和区域及数字贸易协定中常用的数据跨境流动机制，其本质是对数据保护水平达到一定标准的“白名单”认证。如新加坡建立了数据保护可信任标志，并在 DEPA 中推进成员国对数据保护可信任标志的互认，促进数据跨境流动。上海作为跨国公司集聚地，可结合企业数据出境实际需求，率先探索推进数据保护可信认证便利化试点，为已部署数据保护措施并达到数据合规标准的企业提供便利化认证方式，并探索与主要经济体实现数据保护可信任标志的互认，实现在国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的非重要非敏感数据跨境自由流动。同时，近年来，区块链、隐私计算等技术的发展和数据中介的出现为数据跨境传输提供了新的范式。如欧盟基于盖亚云（Gaia-X）建立的欧洲公共数据空间、日本数据社会联盟建立的数据交换平台（Data-EX）等。此外，隐私增强技术（PETs）、数据监管沙箱等也为数据跨境流动的应用实践提供了新的选择。下一步，应支持和鼓励各地数据交易所加快新技术新模式的研究，应用数据空间、数据监管沙箱等新工具，探索数据跨境安全流动新方式。

（三）增强数据安全保障能力

数据跨境流动将会带来一系列安全风险，如数据泄露、数据滥用等，对国家安全构成威胁。因此推进数据跨境流动必须增强数据安全保障能力。一方面，支持建设数据安全监测系统。如支持上海数据交易所等平台建立智能化数据安全监管系统，加强数据安全风险评估、信息共享、监测预警等技术能力建设。支持政府部门与数据安全企业协作，建设数据跨境流动安全威胁感知和监测预警基础设施，统筹数据安全威胁信息的获取、分析、研判、预警工作，强化数据安全事件日常监测、通报预警、快速响应、追踪溯源恶意行为等技术能力。另一方面，强化前沿数据安全技术研发。支持上海数据交易所等平台强化数据安全技术研发，针对数据跨境流动过程中可能的数据泄露、个人隐私风险、数据滥用等一系列安全风险，支持差分隐私、零知识证明、同态加密、多方计算、联邦学习等前沿数据安全技术研究，支持安全产品研发及产业化应用，为数据跨境流动安全提供切实可行的技术方案，降低数据跨境流动安全风险。

（四）推广数据跨境流动中国治理方案

目前全球数据跨境流动治理与规则正处于形成过程中，美欧等西方国家正在基于信任关系加速构建将我国排除在外的数据跨境流动自由圈。而我国尚未明确提出我国数据跨境流动治理方案，也尚未与世界主要经济体、我国主要贸易伙伴建立数据跨境传输便利化机制，参与数据跨境流动全球治理不足。一方面，我国应以“一带一路”建设为契机，基于互利互惠、安全便利等原则，提出有利于我国发展的数据跨境流动治理方案，推动形成可互认的数据保护认证、标准合同条款等机制，实现区域内数据跨境自由流动。另一方面，我国应积极推进 CPTPP、DEPA 谈判议程。新加坡作为亚太地区重要数据枢纽，是 CPTPP 发起成员，也是 DEPA 的主要推动方。我国应加强同新加坡在数据跨境流动方面的对接与合作，探索数据跨境流动可操作路径，进而将相关经验推广至 CPTPP、DEPA 其他成员。

（五）企业做好“出境”与“入境”的合规

目前，《网络安全法》《数据安全法》《个人信息保护法》等立法以及《数据出境安全评估办法》等规章构建了我国数据跨境流动的安全规则体系，因此企业在数据出境时需按照现有法律要求做好数据出境安全合规，如进行数据分类分级，涉及核心数据、重要数据等需进行数据出境安全评估等。数据跨境流动不仅涉及数据出境，还有数据入境，当前全球主要经济出于保障数据主权的需要对本区域内的数据出境进行立法规制，典型的如欧盟的 GDPR 等。因此企业在将境外的数据引入中国境内时，需按照数据来源国的法律要求做好安全合规，在满足数据来源国合规的要求的前提下，将数据流入中国境内。

（六）利用上海数据交易所国际板探索数据跨境新模式

上海数据交易所已经开设运行国际板，建设国际化数据交易平台，探索形成便捷、高效、安全的数据跨境流动规则体系，积极赋能我国国际数字贸易的发展，为我国参与国际数字贸易规则制定贡献探索实践的经验，同时服务于企业数据“走出去”与“引进来”。企业在开展数据跨境流动时，可利用上海数交所国际板开展数据产品合规评估审查，提高数据产品交易效率，同时依托上海数据交易所，加快企业向全球进行数据产品推介的步伐。

专栏：案例研究

学术数据跨境流动

——基于中国图书进出口（集团）有限公司的实践

一、企业背景

中国图书进出口（集团）有限公司（下称“中图”）是一家与共和国同龄的大型国有文化企业。中图始终坚持引进国际先进科技文化成果服务社会经济建设，持续推动中华文化“走出去”。目前，公司拥有国内外分支机构 28 家，服务全球 170 多个国家和地区上万家图书馆、大学、科研机构，已成为我国规模大、实力强的出版物进出口贸易企业、数字资源提供商和国际性书展服务机构。

近年来，中图完成了由传统贸易商向内容服务商的第一次数字化转型。进入新时代，踏上新征程，中图公司正在加快推进由内容服务商向数据运营商的第二次数据化转型和国际化再布局，努力构建“智慧中图”，为国家“科技强国”“文化强国”“数字中国”建设做出新的更大贡献。

二、在上海数据交易所国际板挂牌数据产品的实践

自 2023 年 7 月起，中图作为数据供应方数商，实现在上海数据交易所国际板挂牌数据产品。以中图独家代理的美国 IPDataLab 公司的系列数据产品为例，7 月 7 日，挂牌“美国药品专利链接”，“日本药品专利链接”，类型为数据服务；7 月 28 日，挂牌“药品专利链接”，类型为数据应用；10 月 18 日挂牌“标准必要专利 SEP”，类型为数据集。

中图公司完成在上海数据交易所数据交易系统的用户注册和实名认证，包括线下签署《上海数据交易所供需方服务协议》并上传至平台，在数据交易所开通账号后，便可进行数据产品的登记和挂牌。

中图公司挂牌 IPDataLab 公司的数据产品包括以下程序：

1. 产品登记：在【登记管理】中的【系列产品登记】处，完成产品系列新建；在产品系列下的【登记产品】处，完成数据产品基本信息、内容说明、使用描述、来源证明等信息填写并提交交易所进行初审和复审；审核通过后系统生成数据产品说明书，完成产品登记。

2. 产品挂牌：填写挂牌申请需要的信息，包括选择应用板块、产品挂牌描述、使用案例，和交易信息等，提交审核通过后，生成《可交易数据产品说明书》，产品即挂牌成功。

中图建立了 Pharmspot 数据服务产品系列，其下登记挂牌“日本药品专利链接”、“美国药品专利链接”；PharmspotTM 数据应用系列，其下登记挂牌“药品专利链接数据库”；SEP-Express 数据集系列，其下登记挂牌“标准必要专利 SEP”。

在产品登记过程中，根据《上海市数据条例》以及上海数据交易所的相关规定，数据产品和服务的形成以“实质性加工”和“创新性劳动”为前提，中图重点从以上两个方面对数据产品和服务进行认定。

1. 实质性加工方面：1）Pharmspot、PharmspotTM 系列产品。提升了药品数据和专利数据的颗粒度，药品数据增加了药物靶点、适应症等信息，对药品新适应症-获批日期以表格化视图做了呈现；专利数据增加了 Claim Chart 对照表，增加了药品专利到期日字段，并精准计算出最准确的药品专利到期日。产品并对美国、日本两国的数据字段进行了标准化处理，并提供清晰的对照表格，方便用户使用，例如美国药品申请号和日本药品批准号在 Pharmspot 中统一为同一字段。2）SEP-Express 系列产品，数据加工上的主要精力投入到了专利号的核实和标准化方面，以人工智能+手动核对的方式标准化了权利人向 15 个标准制定组织（Standard Setting Organization，SSO）所声明的专利。

2. 创新性劳动方面：1）Pharmspot、PharmspotTM 系列产品，建立了药品数据和专利数据之间的链接，链接的发现与建立需要基于 know-How 的专业技能，是一种创新性劳动。本数据产品全面考虑到药品专利到期日的影响因素，以 AI 算法结合人工核对的方式计算出了药品的精确专利到期日，提升了药品信息和专利信息的透明度并促进了用户对信息及数据的轻松获取，目前还没有同类型产品能做到列出专利到期日字段并精准计算。2）SEP-Express 系列产品，该产品使用人工智能+手动核对的方式标准化了权利人向 SSO(Standard Setting Organizations)所声明的专利。数据产品“标准必要专利 SEP”中，对所有声明专利的申请和公开号，并通过家族信息对重复声明的专利（就同一个发明专利的多个家族成员向 SSO 多次声明）予以去重，该产品中使用的标准化方法为自行开发，属于创新性劳动。

三、中图数据产品的使用场景与合规性

（一）使用场景

专栏：案例研究

根据上海数据交易所秉承“不合规不挂牌、无场景不交易”的原则，是否具有明确的使用场景是认定产品是否可交易的条件之一，中图对挂牌产品使用场景的描述，来源于真实使用场景。

1. Pharmspot、PharmspoTM 药品专利链接使用场景：1）医药公司查询所关注的美国药品，日本药品，获得其专利情况及各专利到期日，用于自身药品研发、上市的商业决策。2）行业分析公司查询所关注的医药企业，获得其美国药品、日本药品、及专利整体情况，用于市场预测、企业评级等。3）准确的专利到期日有助于辅助仿制药上市决策，有助于原研药厂制定专利策略。据此，用户获取到透明的药品对应专利信息，准确的专利到期日，从药品的专利图景中，可以实现原研药专利策略概览，展开药品竞争态势预测和分析，识别出药品的核心专利信息，外围专利信息，对市场进入开展壁垒分析，为药品研发提供技术情报。

2. SEP-Express 标准必要专利 SEP 使用场景：1）通信、物联网等行业公司获取全球标准必要专利最全面的数据，用于市场竞争、企业专利资产、技术演变分析等，并辅助相应的商业决策。2）作为 SEP 许可费率谈判的数据依据，以及专利的标准必要性法律分析的数据基础。这些是实施某标准技术时不可规避的专利。

（二）合规评估与质量评估

产品信息登记的一个重要环节是提交包括“数据产品合规评估报告”、“数据产品质量评估”等信息。数据产品的合规评估，需要评估数据来源的合法性、数据产品的可交易性、数据产品的流通风险等要点。

1. 数据来源的合法性：数据来源于官方机构或标准制定组织。

2. 数据产品的可交易性：数据产品的底层数据的更新与官方同步，数据产品有固定的更新频率，也可以根据用户的需求进行定制化更新。中图已经证明了 Pharmspot、PharmspotTM、SEP-Express，具有明确的使用场景，可定价。

3. 数据产品的可交易风险：主要考察 Pharmspot、PharmspotTM、SEP-Express 数据产品中，是否包含个人数据、不能够进行交易和禁止交易的重要数据、核心数据等。

4. 数据产品的流通风险：无场景不交易这一原则体现在流通过程中，中图根据场外的市场推广经验，预设适用场景，主要从是否有特殊限制、跨境数据流动过程是否安全等方面评估。

关于数据产品质量评估：按照定量指标和非定量指标两个方面进行评价，定量指标包括数据的规范性、完整性、准确性、一致性、时效性、可达性；非定量指标包括固有特性、说明性质量、可访问质量、环境性质量等。

根据上述指标，对挂牌数据产品进行了质量评估：

Pharmspot、PharmspotTM 药品专利链接：数据来源于官方，客观可靠，规范标准化程度高，数据内容覆盖全面，无空值，具备实体、引用、完整性，域完整性，例如在药品专利到期日计算上，充分考虑了影响变量，当对应变量字段的输出内容发生变化时，Expiry Date 专利到期日也会重新计算，得出新的输出数值。每个字段均有清晰的格式标准，对美国、日本不尽相同的数据字段做了标准化处理，能够满足数据分析要求和用户使用需求。在数据处理加工的环节，对数据质量、格式、输出、做了多重一致性检查，保障数据一致性。同一数据元素的类型和含义在不同的需求方、使用者的系统和不同数据处理环节上保持了一致与清晰。时效性上数据及时性很高，每月更新，包括药品信息更新和专利信息更新。数据容量较低，收录了美国和日本获批药品 25400 以上，获批药品核心专利信息 9200 以上，20 万件以上全球专利同族，可嵌入传统的医药数据库亦可嵌入专利数据库，数据的可达性满足市场需求。“药品专利链接”提供的药品相关专利及其准确的到期日，从药品专利图景中进行原研药专利概览，提供商业策略依据，具有极高的价值密度。

SEP-Express 标准必要专利 SEP：收录了 15 个标准制定组织 SSO 的专利权人声明的 SEP，每一条 SEP 记录都包含三个数据字段：1）专利号；2）对应的标准；3）声明公司。15 个标准制定组织为：ETSI 欧洲电信标准化协会，IEEE 电气电子工程师协会，ISO 国际标准化组织，CCSA 中国通信标准化协会，OMA 开发移动联盟，IMT 国际移动通信，OneM2M 物联网，TIA 美国通信工业协会，ATIS 世界无线通信解决方案联盟，ITS-T 国际电信联盟-电信标准化部门，ITS-R 国际电信联盟-无线电通信部门，IEC 国际电工委员会，IETF 国际互联网工程任务组，ANSI 美国国家标准局，TTA 韩国电信技术协会。产品提

专栏：案例研究
取的数据，如果在提取时该专利已经被授权，提供授权的专利号，如果仍在申请过程中，提取专利的申请号，当申请专利已获批，会在数据更新时更新为授权专利号。 总体而言，在上海数据交易所国际板完成国际数据产品的挂牌，是中图在推动国际数字资源到数据要素市场聚合，以数据要素流通促进数字经济发展的创新实践。未来，中图将围绕科研学术服务，在数据跨境流通标准化服务等方面，参与到推动数据要素流通的多主体、多层次、多场景建设之中，为我国科研学术发展提供更安全、更高效、更智能的产品和服务，更好助力数字中国、科技强国建设。

参考文献

[1] 林梓瀚,游祎,史渊.基于生物识别技术的全球个人信息安全治理研究[J].世界科技研究与发展
[2] 林梓瀚.基于数据治理的欧盟法律体系建构研究[J].信息安全研究
[3] 林梓瀚,黄丽华.全球主要经济体数据跨境流动规则研究[J].中国信息安全
[4] 林梓瀚.东盟数据跨境流动制度研究：进程演进与规则构建[J]世界科技研究与发展
[5] 吴沈括,胡然.数字平台监管的欧盟新方案与中国镜鉴——围绕《数字服务法案》《数字市场法案》提案的探析[J].电子政务
[6] 吴沈括,崔婷婷.欧盟委员会 2020 年《欧洲数据战略》研究[J].信息安全研究
[7] 洪延青.数据跨境流动的规则碎片化及中国应对[J].行政法学研究
[8] 洪延青.数据竞争的美欧战略立场及中国因应——基于国内立法与经贸协定谈判双重视角[J].国际法研究
[9] 洪延青.推进“一带一路”数据跨境流动的中国方案——以美欧范式为背景的展开[J].中国法律评论
[10] 胡海波,耿骞.数据跨境流动治理研究：溯源、脉络与动向[J/OL].情报理论与实践
[11] 林梓瀚,计丽娜.浅析我国金融业数据出境安全规则[J].中国金融电脑
[12] 冉从敬,郭潇凡,何梦婷.国际跨境数据流动治理合作：机理、困境与变革[J/OL].图书馆论坛
[13] 张相君,易星竹.数字贸易中跨境数据流动的国际法挑战与中国因应[J].福州大学学报(哲学社会科学版)
[14] 梅傲,李淮俊.数字贸易中数据跨境流动规则的新发展——基于《数据出境安全评估办法》与 DEPA 的比较[J].企业经济,2023,42(04):153-160.
[15] 朱勤,刘玥.数字贸易发展背景下跨境数据流动国际治理及我国的探索[J].科技管理研究
[16] 梅傲,李淮俊.论《数据出境安全评估办法》与 DEPA 中数据跨境流动规则的衔接[J].上海对外经贸大学学报
[17] 丁晓东.数据跨境流动的法理反思与制度重构——兼评《数据出境安全评估办法》[J].行政法学研究
[18] 王丽颖,王花蕾.美国数据经纪商监管制度对我国数据服务业发展的启示[J].信息安全与通信保密
[19] 翟军,李昊然,孙小荃,李剑锋.美国《开放政府数据法》及实施研究[J].情报理论与实践
[20] 赵丽莉,郑蕾.美国数据与隐私安全保护制度进展述评[J].重庆理工大学学报(社会科学)
[21] 金耀.数据产业法律规制路径研究——以美国数据经纪人制度为视角[J].司法改革论评
[22] 金晶.个人数据跨境传输的欧盟标准——规则建构、司法推动与范式扩张[J].欧洲研究
[23] 金晶.欧盟的规则，全球的标准? 数据跨境流动监管的“逐顶竞争”[J].中外法学
[24] 吴希贤.东盟数据治理：全球背景、规制框架与中国合作[J].亚太经济
[25] 刘箫锋,刘杨钺.东盟跨境数据流动治理的机制构建[J].国际展望
[26] 谢谦.全球数字经济规则议题特征、差异与中国应对[J/OL].改革

[27] 郭丰,林梓瀚,胡正坤.基于全球网络空间稳定进程的“国际软法”建构与演变[J].信息通信技术与政策
[28] 《全球数字治理白皮书 2022》[R].中国信息通信研究院
[29] 《全球数字治理白皮书 2021》[R].中国信息通信研究院
[30] 《全球数字经济白皮书 2021》[R].中国信息通信研究院
[31] 《跨境数据流动：相关政策和举措的盘点》[R] .经合组织（OECD）
[32] 《G20 成员国跨境数据流动规则》[R].联合国贸易和发展会议
[33] 《全球数字贸易发展趋势报告 2022》[R].商务部国际贸易经济合作研究院
[34] 《数字贸易发展与合作报告 2022》[R]. 国务院发展研究中心
[35] 《数字化新外贸趋势发展报告》[R]. 中国国际经济交流中心