我国跨境数据传输规则与国际规则的协调研究

马 光

【摘 要】关于跨境数据传输的全球性国际规则尚未确立，目前仅有部分区域性条约和软法对其作出规定，其中以FTA和数字经济协定为中心的经贸协定占据着重要地位。而这些FTA和数字经济协定对跨境数据传输的规定也不尽相同，大体已经形成了美国、欧盟及中国模式，三大模式各具特色，比如，美国模式注重跨境数据传输自由，欧盟模式强调个人数据保护，中国模式关注国家安全。而这些模式也不是一成不变的，随着FTA网络的不断交织，上述三种模式也呈现出一定程度的协调。在这一进程中，新加坡、新西兰、日本、韩国等国家起到了重要作用。目前我国已经正式申请加入DEPA和CPTPP，而这些协定中的跨境数据传输规定与我国模式有存在较大差异。在我国形成的各种数据出境模式中，数据出境安全评估制度要求最为严厉，其在我国的DEPA和CPTPP加入谈判中将会面临重大挑战。在此背景下，结合国际和外国的立法，重新审视我国的个人信息跨境传输规则及立场非常的必要。

【关 键 词】跨境数据传输；DEPA；CPTPP；RCEP；数据出境安全评估

【作者简介】马光(1975-)，吉林龙井人，现为浙江大学光华法学院副教授，研究方向为国际经济法学。

【原文出处】《中国政法大学学报》(京)，2024.2.227～239

【基金项目】本文系浙江省法学会2023年度法学研究课题“数字贸易高质量发展法治保障研究”(项目批准号：2023NA05)和2023年浙江大学“重要国家和区域研究”专项“亚洲主要国家数字贸易规则比较研究”的阶段性研究成果。

一、引言

全球跨境数据传输的法律、指南大体可以分为国际层面和国内层面，国际层面主要有经济合作与发展组织(OECD)的《隐私准则》、亚太经济合作组织(APEC)的《跨境隐私规则》(CBPR)、欧洲理事会的《108号公约》、包含跨境数据传输条款的自由贸易协定(FTA)和数字经济协定，国内层面则有各国国内法中的跨境数据传输规定。

目前，国际组织的跨境数据传输法律、指南和数字经济协定的数量非常有限，故要对其进行全面的深入研究。而与跨境数据传输有关的FTA和各国国内法的数量非常庞大，因此有必要对其进行筛选。美国和欧盟在跨境数据传输领域较早形成各自模式；新加坡则在主导数字经济协定的签订，包括《数字经济伙伴关系协定》(DEPA)、新加坡—澳大利亚数字经济协定(DEA)、新加坡—英国DEA和新加坡—韩国数字贸易协定(DPA)；日本是我国申请加入的《全面与进步跨太平洋伙伴关系协定》(CPTPP)的重要成员，同时也缔结了日本—美国数字贸易协定(DTA)，与欧盟就跨境数据传输条款纳入FTA开启了谈判，并于2023年10月28日就此达成了协议；韩国于2023年6月9日宣布已完成加入DEPA的谈判，从而将成为第一个通过加入成为DEPA缔约方的国家，对我国后续加入该协定有重要借鉴意义，同时也与新加坡缔结了DPA；新西兰为CPTPP、DEPA的缔约方，同时与欧盟缔结了带有实质性跨境数据传输条款的FTA。对这些重要国家和地区缔结的FTA和数字经济协定的跨境数据传输条款进行分析，并对其国内法中的相关规定进行比较非常重要。因为我国已经申请加入DEPA和CPTPP，将我国的数据跨境传输法律规定与这些FTA相关条款及各缔约方的国内法进行比较也将对我国提供帮助。

二、各国(地区)缔结的FTA和国内法中对数据跨境传输的规定

数字贸易治理存在着两类主流规制路径:数据规制与贸易规制。[①]不同的FTA对数据跨境流动采取了不同的标准,保护水平相同和相近的国家、地区之间更容易进行个人数据的跨境转移,而发达国家基于产业优势和国内立法完善,对于数据自由流动的需求更大。[②]数据本地化浪潮的兴起、数据贸易壁垒的形成,即昭示着良好数据保护、跨境数据自由流动和数据主权间的失衡困境。[③]尽管如此,从实践来看,国际社会目前的共识是:贸易协定是管理跨境数据流动的适当场所。因为当信息跨境流动时,这些流动似乎基本上与贸易相关。[④]

(一)美国缔结的FTA和国内法规定

截止2023年11月30日,在美国缔结的FTA中,美国—智利FTA、美国—多米尼加—中美洲FTA、美国—韩国FTA、美国—日本FTA和《美国—墨西哥—加拿大协定》(USMCA)中含有跨境数据传输相关条款。美国—智利FTA和美国—多米尼加—中美洲FTA仅在合作条款中提到努力保持信息的跨境传输,并认为这是营造充满活力的电子商务环境的基本要素。美国—韩国FTA进一步规定,缔约双方认识到信息自由传输对促进贸易的重要性,并认识到保护个人信息的重要性,应努力避免对跨境电子信息传输施加或保持不必要的障碍,但从措辞来看,其不具有强制约束力。而真正有约束力的规定来自USMCA和美国—日本FTA。USMCA和美国—日本FTA比继承TPP跨境数据传输条款的CPTPP更进一步对跨境数据传输提出了更高的要求,将"缔约方可以对通过电子手段传输信息提出自己的监管要求"这一内容予以删除,从而否定了缔约方具有的普遍监管要求,之前的跨境数据传输条款的结构是在第一款承认缔约方提出监管要求,第二款才是跨境数据传输自由。因为USMCA首次将上述内容的第一款替换成跨境数据传输自由的内容,对跨境数据传输的理念发生了质的变化。USMCA跨境数据传输条款的第二款规定了跨境数据传输自由的例外,即缔约方为了实现合法的公共政策目标,可以采取或维持对信息跨境传输的限制措施,而这种措施要符合:第一,不构成任意或不合理的歧视或变相的贸易限制;第二,对信息传输施加的限制不超过实现目标所需限度。可以概括为,要符合这种例外,应满足如下四个条件:第一,实现合法公共政策目标所需;第二,不构成任意或不合理的歧视;第三,不构成变相的贸易限制;第四,不超过实现合法公共政策目标所需限度。只要不符合上述四个条件之一,就会构成对该条款的违反。[⑤]而这里所规定的"合法公共政策目标"应包含个人数据保护、国家安全等。因此,为个人数据保护、国家安全等而对信息的跨境传输进行限制是正当的。但实际上要符合这种例外条件非常困难,这从WTO案例中对一般例外条款的援引成功比例中能够得到印证,因为"合法公共政策目标例外"的设计和WTO的一般例外非常相似。从此可以看到,美国FTA中的这些规定显然是贸易主导型的,且将缔约方对跨境数据传输的规制权逐渐予以弱化。美国在FTA中引入跨境数据传输条款的成功,也是其在全球性平台外,借助经济优势在缔约方相对较少的情况下主导规则制定的成果。

在法律上,美国并不限制将个人数据等转移到美国境外的行为。在其主导的双边和多边国际协定中,也都寻求美国境外数据对等的自由流入,反对本地化存储等对数据跨境流动进行限制的立法,尤其反对他国对数据出境的限制。[⑥]受此影响,从国内立法上看,虽然美国愈发重视加强通过立法保护个人信息,并且开始在州立法中得到体现,如《加利福尼亚消费者隐私法》,但这些立法对数据的跨境传输方面却并未规定。美国并没有针对个人数据的传输与保护进行单独立法,相关的规定散见于各行业的法律法规中,而且也更多依赖于企业的自我监管,比如要求美国企业通过自我申请与认证的方式加入美国与欧盟就个人数据传输作出的相关隐私保护安排。尽管美国主张彻底的数据跨境流动,但从其域内立法来看,都存在不少基于国家安全考虑来限制数据跨境流动的立法。[⑦]

(二)欧盟缔结的FTA和欧盟法规定

截止2023年11月30日,欧盟缔结的FTA中,欧盟—日本FTA首次对跨境数据传输做出规定,缔约双方约定应在该协定生效之日起三年内重新评估是

否有必要将有关跨境数据传输的规定纳入该协定。按此规定,双方在2022年10月24日正式开始对此进行谈判,并于2023年10月28日达成协议。欧盟—墨西哥FTA升级版的原则协定文本也有类似规定。欧盟—新西兰FTA在欧盟缔结的FTA中唯一就跨境数据传输问题做出较详细的规定,且该FTA的跨境数据传输条款有自己的特色,与CPTPP、RCEP、DEPA等FTA或数字经济协定中的跨境数据传输条款在结构和内容等方面有较大差异。该协定规定,缔约方致力于确保跨境数据传输,以促进数字经济贸易,并承认各缔约方在这方面可能有自己的监管要求。进而规定缔约方不得通过所列举方式限制缔约方之间在数字经济贸易范围内的活动中发生的跨境数据传输。缔约双方允许依据一般例外情况采取或维持旨在实现公共政策目标的措施。协定还特别规定,在相关情况下,对公共政策目标的解释应考虑到数字技术的演进性质,且不影响本协定其他例外条款的适用。除非缔约双方另有协定,否则缔约双方须在协定生效后三年内审议该条实施情况,并评估其成效,缔约一方亦可随时向另一方提出审议本条的建议。缔约双方应从善意,考虑有关的建议。虽然截止2023年11月30日,欧盟—新西兰FTA尚未生效,但其包含的跨境数据传输条款的内容与CPTPP和DEPA等条约的跨境数据传输条款不存在本质差异。这表明欧盟也逐渐开始将跨境数据传输纳入FTA条款中,尽管其还规定日后要重新对该条款进行审议。除此之外,2023年7月20日和10月31日,欧盟先后与新加坡和韩国启动了数字贸易协定的谈判,这也说明欧盟在数字贸易国际规则的制定中扮演着越来越重要的角色。

与美国不同,欧盟将人权的保护置于数据自由传输之上。[8]欧盟的《通用数据保护条例》(GDPR)第5章"对将个人数据传输到第三国或国际组织"做出相应规定,其规定,对于正在处理或计划进行处理的个人数据,将其传输到第三国或国际组织,包括将个人数据从第三国或国际组织传输到另一第三国或另一国际组织,控制者和处理者必须满足相应规定,而这些规定包括:基于认定具有充分保护的传输;符合传输所需要的适当安全保障;有约束力的公司规则;未经欧盟法授权的传输或披露;数据主体仍明确表示同意,为履行数据主体与控制者之间的合同,为实现数据主体的利益必要等特殊情形下的传输。欧盟数据的跨境传输采取"充分性决定+补充措施"的制度。[9]而基于GDPR第45条中的充分性认定要求,截止2023年11月30日,欧盟已对15个国家做出该认定。如,2020年1月23日,通过对日本的充分性认定;2021年12月17日,通过对韩国的充分性认定;2023年7月11日,通过"欧盟—美国数据隐私框架"的充分性认定。充分性认定允许欧盟和这三个国家之间的个人数据自由传输,这也意味着设有高标准个人数据保护要求的欧盟认可美日韩三国对个人数据保护的力度。尽管美日韩三国与欧盟之间未缔结FTA或所缔结的FTA对数据跨境传输问题未作具体规定,但美日韩与欧盟之间的数据跨境已经做到自由传输,即其效果与在FTA对此予以规定是相似的。欧盟—日本FTA后续谈判中就此达成的协议文本尚未公开,此处尚且认定双方FTA并未包含实质内容的相关条款。基于此,欧盟与这些国家在日后缔结FTA或升级FTA时对跨境数据传输做出相应规定也不足为奇。

(三)日本缔结的FTA和国内法规定

截至2023年11月30日,日本缔结的FTA中,跨境数据传输规定包含在与欧盟、美国签订的FTA和以日本为缔约方的CPTPP、RCEP中。日本于2019年10月7日与美国缔结了数字贸易协定,该协定已成为日本—美国FTA的一部分。正如上文所述,日本—欧盟FTA中的跨境数据传输条款已经完成谈判。RCEP、CPTPP和日本—美国FTA的跨境数据传输条款虽然外形相似,但内容实际上差别较大。第一,RCEP和CPTPP的跨境数据传输条款在第一款认可了"每一缔约方对通过电子方式传输信息可设有各自的监管要求",而日本—美国FTA中该款就得以删除。第二,RCEP对"为实现合法公共政策目标采取或维持措施"的必要性明确授权由采取措施的缔约方决定,即,他方"不得提出异议",从而扩大了例外的适用范围及可能性。这与CPTPP和日本—美国FTA下跨境数据传输限制例外很难得以满足的情形形成鲜明对比。日本既与美国签订数字贸易协定,

又通过欧盟的个人数据跨境传输的充分性认定，对美式数字贸易规则和欧式数字贸易规则的协调做出了一定的贡献。同时，其作为CPTPP的重要缔约方，对我国加入该协定也有相当重要的作用。

《日本个人信息保护法》第24条规定："个人信息处理者向境外第三方提供个人数据的，应当事先取得本人就向境外第三方提供的同意。个人信息处理者欲依照前一款的规定取得本人的同意时，应当依照《个人信息保护委员会规则》的规定，事先将相关境外个人信息保护制度、第三方采取的个人信息保护措施及其他可供本人参考的信息提供给本人。个人信息处理者将个人信息提供给境外第三方后，应当依照《个人信息保护委员会规则》的规定，采取必要措施确保该第三方持续采取相当措施，并在本人要求后将该必要措施的相关信息提供给本人"。其还规定："以下情形则可不经过用户同意：向位于被日本个人信息保护委员会(PPC)认定为具有与日本同等个人信息保护水平的国家的第三方提供用户个人信息；符合PPC制定的规则中的以下标准：第一，基于信息提供方与接收方之间的合同，或者信息提供方与接收方属于同一集团且建立了适用于双方的内部规章、隐私政策等；第二，信息接收方已经取得关于个人信息处理的国际体系的认证"。

(四)韩国缔结的FTA和国内法规定

截至2023年11月30日，韩国与美国、新加坡缔结的FTA，其作为缔约方的RCEP和2023年6月9日宣布完成加入谈判的DEPA中具有跨境数据传输条款。韩国—美国FTA中的跨境数据传输条款并不具有明确的权利义务，而与新加坡缔结的FTA中已经包含了DPA，且已完成DEPA加入谈判。RCEP与DEPA、韩国—新加坡FTA相比有对合法公共政策例外的自主决定权，DEPA和韩国—新加坡FTA对跨境数据传输的规定则相同。韩国于2021年12月15日与新加坡缔结的DPA是目前最为详细的数字经济协定之一，共有34个条款。韩国受到美式数字贸易规则的影响较大，也是美国推广其数字贸易政策收效的第一个国家。但同时韩国也通过与欧盟完成跨境个人数据传输的充分性认定，在保护个人数据方面又满足了欧盟的严格要求。因此，与日本类似，其在这方面充当了美式数字贸易规则和欧式数字贸易规则的缓冲带，这也为全球数字贸易规则的协调起到了一定的作用。

《韩国个人信息保护法》第39条之12第4款规定："信息通信服务提供者等经个人信息所有人的同意，将个人信息传输到国外的，应当根据总统令规定采取保护措施"。但依据该法第15条第1款规定，在"以下例外情形中可不经个人信息所有人的同意：第一，法律另有规定或为遵守法定义务而不可避免；第二，公共机构为履行法定义务而不可避免；第三，保护数据主体或第三者的生命、身体或经济利益免受迫在眉睫的威胁；第四，法庭命令或者法官签发的令状另有要求；第五，对于履行信息通讯服务之合同和便利用户是必要的，但是要进行适当通知或披露；第六，计算与位置资料或定位服务之提供相关之费用所必需；第七，资料之提供是以一种无法确定特定主体的方式进行，且用于统计、科学研究或市场调查之目的。目前，总统令尚无明确规定应采取何种保护措施。

(五)新加坡缔结的FTA和国内法规定

截至2023年11月30日，新加坡缔结的FTA中，新加坡—斯里兰卡、新加坡—新西兰FTA有跨境数据传输规定，且其与澳大利亚、英国、韩国各自缔结的数字经济协定、《东盟电子商务协定》、RCEP、CPTPP、DEPA均有内容相同的跨境数据传输规定，这些规定基本上都沿用了CPTPP的跨境数据传输规则。除此之外，其还与欧盟启动了数字贸易协定谈判。

《新加坡个人数据保护法2012》第26条对于跨境数据传输作出了规定：第一，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。第二，新加坡个人数据保护委员会(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。第三，可豁免的情形可以由PDPC书面说明；豁免不需要在政府公报中公布，并且PDPC随时可撤销豁免。第四，PDPC可以随时增加、改变或撤销豁免的具体适用情形。数据的跨境传输需符合以下合规要求：第一，个

人同意或被视为同意将其个人数据传输给新加坡以外的国家或地区的接收方;第二,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;第三,传输方已采取合理的措施对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;第四,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;第五,传输的个人数据是已经处于传输状态中的数据,或者是该个人数据在新加坡是公开的。此外,新加坡要求数据的传输方必须采取适当的措施确保数据的接收方受到法定义务的约束。该法定义务包括以下对个人数据接收方施加的义务:第一,境外接收者所在国的数据保护法律;第二,与境外接收者签订数据传输协议;第三,具有约束力的公司规则;第四,任何其他具有法律约束力的文件。

(六)新西兰缔结的FTA和国内法规定

截至2023年11月30日,新西兰缔结的FTA中,新西兰—英国FTA、新西兰—新加坡FTA、新西兰—欧盟FTA包含跨境数据传输规定,新西兰还是CPTPP、RCEP和DEPA的缔约方,其中与欧盟的FTA尚未生效。新西兰缔结的FTA既有RCEP型较为宽松的例外规定,又有CPTPP和DEPA等相对严格的例外规定,更有与欧盟签订的具有较大特色的跨境数据传输规定。特别是与欧盟签订的FTA开创了欧盟FTA中具体跨境数据传输条款之先河。

《新西兰隐私法2020》第三部分第一节规定了十三项信息隐私原则,其中的第十二项原则专门规定数据跨境问题,称为"向新西兰境外披露个人信息"。按其规定,只有在某个国家的隐私保护水平与新西兰相似,或者在某个人已完全知悉并同意的情况下,新西兰的企业或机构才能将此个人的信息传输到该国。企业或机构将负责确保他们向新西兰以外的组织披露的任何个人信息得到充分保护。在进行跨境披露之前,企业或机构必须能够证明他们已经进行了必要的尽职调查。"跨境披露"的条件具体如下:该组织受《新西兰隐私法》约束,因为其在新西兰境内经营生意;该组织受其他《隐私法》的约束,该法提供了与《新西兰隐私法》类似的保障措施,或者同意以这种方式保护信息,例如使用合同范本条款;该组织受具有约束力的计划的保护,或受新西兰政府规定的国家隐私法的约束。另外,允许在维护公众健康和安全、防止对他人的生命和健康造成严重威胁以及维护法律的前提下,进行跨境披露。

(七)我国缔结的FTA和国内法规定

截至2023年11月30日,我国缔结的FTA中只有与港澳缔结的《更紧密经贸关系安排》(CEPA)和RCEP中包含跨境数据传输规定。《〈内地与香港关于建立更紧密经贸关系的安排〉经济技术合作协议》和《〈内地与澳门关于建立更紧密经贸关系的安排〉经济技术合作协议》规定"加强两地在跨境数据流动方面的交流",前者还规定"组成合作专责小组共同研究可行的政策措施安排"。而RCEP对数据跨境传输规定了较为宽泛的规制例外。因此,目前我国在数据跨境传输方面作出的对外承诺标准尚且不高。但随着我国于2021年10月13日和11月1日分别申请加入CPTPP和DEPA,如果要完成这两个协定的加入,就会面临着对上述例外进行限制。

我国对数据跨境传输的规则分散在《网络安全法》《数据安全法》和《个人信息保护法》中,对重要数据和符合一定条件的个人信息则要求较为严格的数据出境安全评估。其中,《个人信息保护法》确定了个人信息出境的三条路径:通过网信部门组织的安全评估,经专业机构进行个人信息保护认证,以及与境外接收方订立国家网信部门制定的标准合同。自2022年以来,《数据出境安全评估办法》(简称《办法》)《个人信息跨境处理活动安全认证规范》以及《个人信息出境标准合同办法》相继发布,对这三条路径进行了进一步细化。整体上,目前我国的数据跨境传输规则可概括为"安全评估+补充措施"制度,[10]个人信息出境之前的安全评估规则,在一定程度上加剧了"数据出境的合规负担"。[11]相比日本、新加坡等国家针对个人信息的跨境传输设置了"同等保护"的标准,我国现有规定和立法趋势更加严格,对国际数字贸易造成的影响和负担可能更大,在未来参与相关谈判时,需要证明我国的相关要求不会对贸易形成实质性的限制,难度较大。[12]2023年9月28日,国家网信办发布了《规范和促进数据跨境流动规定(征求

意见稿)》(简称《征求意见稿》)。

三、全球跨境数据传输规则的趋势及特点、存在的主要问题

(一)全球FTA下跨境数据传输规则的四种主要类型

结合上述FTA和数字经济协定下的跨境数据传输规定来看,全球跨境数据传输规则大体分为四种类型。

第一种类型为RCEP型,此类协定数量非常有限,目前只有RCEP,其赋予缔约方较为宽泛的规制权,即基于合法的公共政策目标,缔约方可以对跨境数据传输采取限制措施,且对何为"合法的公共政策目标",仅采取措施的缔约方有决定权,其他缔约方无权过问。因为我国对该模式引入RCEP作出很大贡献。所以,此种类型也可被称为FTA跨境数据传输规则的中国模式。

第二种类型是FTA跨境数据传输规则的欧盟模式,表现在欧盟—新西兰FTA中,也是欧盟首次在FTA中具体规定跨境数据传输条款。此种类型对例外条款进行了梳理,不像其他的FTA那样可以将一般和安全例外与跨境数据传输条款中的合法公共政策目标例外予以叠加适用,而是在适用一般和安全例外的前提下对一般例外中的"公共道德"保护条款扩展到"公共道德、公共秩序和公共安全"的保护。同时,此种类型采取了对国家管制和跨境数据传输自由保障一并重视,且就后续对跨境数据传输条款进行审议乃至修订专门予以规定,这也说明欧盟对引入该条款是非常谨慎的。从该FTA开始,想必日后欧盟缔结的FTA中类似跨境数据传输条款会越来越多。

第三种类型也非常有限,可以称之为美国模式,目前仅出现在USMCA和美国—日本FTA中,此类协定删除之前协定中允许缔约方对跨境数据传输具有规制权的规定,仅设定了严格限制下的例外,而此类例外的具体条件却很难满足,形同虚设,此为目前最严格的跨境数据传输条款,基本上不认可缔约方的规制权。

第四种类型是最普遍,也是目前我国应最为关注的模式,典型的协定就是CPTPP和DEPA。此类协定允许缔约方的规制权,但该规制权例外同样受到严格的限制,同时,例外的满足条件也很苛刻。[13]尽管在CPTPP和DEPA中包含了个人信息保护相关规定,但其并不要求旨在高水平保护个人信息的规范统一,允许各缔约国维持各自的相关法律体系。未将个人信息保护水平的差异视作一种壁垒可能对部分缔约国来说是有益处的。[14]这些协定对缔约方采取多种方式履行监管义务的认可,也即不限于制定法律,而"兼容性"的促进则是暗含寻求APEC隐私框架作为标准,达到较低限度的保护水平即可跨境传输数据。[15]因为我国申请了加入CPTPP和DEPA,在加入谈判中避不开该条款下的争论,这也是我国日后需要努力达成的标准,想必上述的《征求意见稿》也是在较为严格的《办法》基础上为逐步靠拢CPTPP和DEPA的要求做准备。

(二)传统的美欧中模式区别还在,但得到部分协调

传统意义上美国更为注重跨境数据传输自由,而欧盟更加注重个人数据保护问题,我国则较为注重国家安全问题。目前从各方的FTA实践来看这种趋势还继续存在,如我国仅在RCEP中对跨境数据传输做了承诺,但同时又设定了对合法公共政策目标的决定权;虽然欧盟已经开始与日本就跨境数据传输展开谈判,与新西兰缔结了相关条款,但整体上对跨境数据传输议题不积极,是一种被动的参加。另外,其还通过双边协议对美日韩作出充分性认定,从而使得欧盟数据可向美日韩进行传输。就是说,尽管未与这些国家缔结FTA或所缔结的FTA、数字经济协定中未规定跨境数据传输议题,但实际上通过双边充分性认定已经达成了相同的结果。

尽管三方的立场分歧尚且存在,但各方立场也在不断得到协调。特别是随着CPTPP、RCEP、DEPA等重要多边协定的出现和不断拓展,再加上新加坡、新西兰、日本、韩国等国不断与美欧中缔结复杂的FTA网络,这些国家和地区的跨境数据传输政策和立场分歧也在逐渐得到磨合和协调。如,欧盟与日本谈判跨境数据传输问题及与新西兰缔结相关条款,我国申请加入CPTPP和DEPA等都是这些新形势下的最新进展。

我国于2023年6月开始实行的《个人信息出境标准合同办法》便是对国际数据跨境传输规则调整的积极回应。该办法采取与欧盟类似的做法，强制合同双方事先约定权利义务等特定内容，确保个人信息在跨境过程中得到充分保护，客观上提升了我国在数据跨境传输过程中的保护水平。[16]

(三)存在的主要问题

上述的各大FTA和数字经济协定，对跨境数据传输自由的整体方向似乎已经形成一致意见，但对缔约方是否有规制权，及规制权和跨境数据传输自由之间的先后问题尚存分歧。不仅如此，就合法公共政策目标采取限制时何为合法公共政策目标及对此如何确定存有较大分歧。这其实就是跨境数据传输自由和设限之间的关系问题，即是一般和例外的关系，以及对例外的范围及例外范围是否恰当的决定权问题。

四、当前我国跨境数据传输规则的现状、问题与国际规则的协调

我国已经基本完成针对跨境数据传输的国内立法体系，并对外也基本形成了中式FTA跨境数据传输条款范式。整体上，我国对于数据跨境流动制定了以数字主权为出发点的较为严格的监管政策，在融入CPTPP和DEPA时，势必遭遇监管权条款范围难以衔接的困境，也即我国监管政策在条约所赋予的缔约方监管权下的合法性问题。[17]

如同上述，我国对跨境数据传输主要采取三种类型的规制，即，标准合同、认证和安全评估。因为标准合同和认证是多数国家在普遍采取，也不太会被认为阻碍跨境数据传输，因而在我国的CPTPP和DEPA加入谈判中被搬上谈判桌的可能性不大，下面将集中对数据出境安全评估制度及其存在的问题予以阐述。

(一)数据出境需要安全评估的情形和除外规定

结合相关法律、行政法规和部门规章的规定来看，如下数据和个人信息的出境需要进行安全评估；第一，重要数据；第二，关键信息基础设施的运营者收集和产生的个人信息；第三，国家机关处理的个人信息；第四，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；第五，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；第六，国家网信部门规定的其他需要申报数据出境安全评估的情形。“自上年1月1日起”这样的限定为不同时期数据出境需求存在动态变化的中小企业设置了科学合理的条件。但从上述的情形中可以推断要求数据出境进行安全评估的限制情况实际上涵盖了实践中的很多场景。[18]在《办法》征求意见阶段，这一规定曾经引起较大争议，认为其评估门槛过低，可能导致评估的泛化。[19]基于我国数字经济规模和数据处理的量级，可能相当数量的常见跨境数据处理活动都会落入《办法》的调整范围。[20]从而限制企业因业务目的的数据出境和跨境业务的开展。[21]

进行数据出境安全评估的主要对象是重要数据和个人信息，其中除了关键信息基础设施的运营者收集和产生的个人信息外，其它需要数据出境安全评估的个人信息范围还是比较明确的。那么，重要数据和关键信息基础设施的范围就对数据出境安全评估具有举足轻重的地位，对于这一部分的内容，将在下面进行详细阐述。

针对上述6种需要进行数据出境安全评估的情形，《网络安全法》和《个人信息保护法》也规定了除外情形。这些除外规定可以理解为如果法律和行政法规有相反规定，则不进行重要数据出境安全评估，而对于个人信息，除外规定的范围扩张到了国家网信部门的规定。而且相比对重要数据的“依照其规定”之规定，对个人信息则更为明确地表示“可以不进行安全评估”，此处，“依照其规定”是否包含“可以不进行安全评估”以及如果另有规定，是“应当不进行安全评估”还是“可以不进行安全评估”也不明确。《办法》虽在第7条规定了强制适用的情形，但在这些情形之外的“可选择”模式下，“安全评估”和“标准化合同”之间的逻辑关系究竟应当如何理解尚未得到正面回复。[22]

除此之外，《个人信息保护法》规定，可以按照我国缔结或者参加的国际条约、协定之规定执行向我国境外提供个人信息的条件。尽管此处用了“可以”，而非“应当”，但基于我国对国际法的尊重，如相关条约有相反规定，相信将会予以遵守。即，如果相

关条约就数据出境安全评估有不同规定的，可以执行。但CPTPP和DEPA对数据出境传输的要求是否与数据出境安全评估不同需要进一步进行探讨，即数据出境安全评估是否符合DEPA的规定尚不明确。[23]我国在推进CPTPP和DEPA加入谈判的同时也应将DEPA放在优先地位，因为其具有更大的可行性，而加入CPTPP则应是较为漫长和艰难的过程，因此，下面只针对我国数据跨境传输规则中数据出境安全评估制度与DEPA的合规性进行探讨。

(二)形成以RCEP为中心的中式FTA跨境数据传输模式

RCEP是我国缔结的唯一带有跨境数据传输规定的FTA，且该FTA有鲜明的特色，就是关于措施是否为合法公共政策目标而必需由采取措施的缔约方决定。这被称为是中方意见的反映，所以可被称为跨境数据传输的中国范式。

但随着申请加入CPTPP和DEPA，该模式可否继续保留面临抉择。因为CPTPP和DEPA对合法公共政策目标的认定权并非专属于采取措施的缔约方，所以，为了加入CPTPP和DEPA，该模式就面临要放弃的地步。当然，从另一角度来看，我国的数字贸易发展越来越快，尽早对跨境数据传输合理地松绑，会对日后的数字贸易进一步发展有好处。因此，是时候考虑接受CPTPP和DEPA的跨境数据传输条款，尽管有些难度，但通过叠加适用跨境数据传输条款下的“合法公共政策目标”例外及一般和安全例外，想必可以对有限但对国家安全重要的数据予以保护。

(三)存在的问题

随着我国申请加入DEPA和CPTPP，这些FTA的跨境数据传输条款与RCEP有重大区别，而在我国的加入谈判中以数据出境安全评估为中心的管制也会被其他缔约方不断提起。有学者指出，在某种意义上，我国笼统的数据出境管理要求可能构成限制数据跨境流动的因素。[24]例如，“关键信息基础设施”的内涵与外延还是具有较大不确定性，这可能导致争议数据本地化措施的涵盖对象过广、造成的贸易限制范围较大。[25]重要数据管控的确定性与重要数据外延的模糊性也形成了鲜明对比。[26]

CPTPP和DEPA不是新的尚在谈判的协定，而是既有协定，这就意味着我国为了加入这两个协定，不得不对现有国内法和政策进行相应调整。换言之，对RCEP的合法公共政策目标自决权是否要放弃是一个重点。且我国的数据出境安全评估制度是以政府为主导的范围非常广泛的数据出境审查制度。与他国普遍采取的认证和标准合同等制度存在较大区别，整体上是最为严格的管制，不仅与CPTPP和DEPA不符，与上述多个国家的做法也有区别。虽然《征求意见稿》试图对安全评估制度进行限制，但数据出境安全评估制度的存在及其包含的模糊概念和要素，导致上述问题不能根本上加以解决。

五、完善我国跨境数据传输法律制度及与国际规则协调的建议

(一)完善数据出境安全评估制度

我国应以数据跨境自由流动为原则，以限制流动为例外。[27]在此前提下，关键信息基础设施、重要数据范围过宽的问题有待解决。尽快厘清重要数据的范围，以明确我国数据出境的“负面清单”。[28]应当尽量缩小对关键信息基础设施和重要数据界定的范围，减少商业性个人数据传输的阻碍，减轻企业的运营成本。《数据安全法》要求各地区、各部门确定重要数据具体目录。这对重要数据的确定有益，但也要防止由此导致各地区重要数据存在较大差异，特别是相同数据在不同地区所属不一的现象。适时考虑地方数据分级是否具有必要性，相同的数据在不同的地区不应属于不同分级。所以，保留部门或行业对数据分级的权限，地方的分级权限有必要再行斟酌。

另，《征求意见稿》规定，自由贸易试验区可自行制定本自贸区需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单，报经省级网络安全和信息化委员会批准后，报国家网信部门备案。这里的数据清单将包括重要数据和个人信息，并赋予自由贸易试验区在此方面的较大自主权。截止2023年11月30日，我国的自由贸易试验区多达22个，涉及22个省、自治区、直辖市，那么，有可能出现22个省的自由贸易试验区范围内实施与我国其他地区不同的重要数据范围，且相

互之间也不相同。这可能会导致重要数据范围的混乱,且有可能导致各个自由贸易试验区竞相“瘦身清单”的情形,这对数据安全是否反而是不利呢?虽然这种放权总体效果是积极的,但也要明确“瘦身”的底线。关于个人信息,《征求意见稿》是否意味着自贸试验区可以调高100万以上个人信息必须要进行安全评估这一底线要求也要予以明确,目前《征求意见稿》的规定可能会就此产生不同的解释。

此外,目前除了数据出境安全评估,还同时存在标准合同和认证的模式进行数据出境,因此要明确监管制度安全评估、标准合同和认证的适用范围和功能定位,并对三个条款的逻辑内容进行紧密的衔接。[29]

(二)逐步完成与DEPA、CPTPP等国际规则的协调

《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。[30]因为我国陆续缔结包含跨境数据传输条款的国际条约,因此,《办法》的实施也应考虑与这些国际条约下我国将承担义务的协调,也为加入CPTPP和DEPA等国际条约进行协调做相关前瞻性研究。尽管DEPA的模块化安排允许缔约方选择特定模块加入,就特定义务作出承诺,但我国在加入谈判中仍有可能面临跨境数据流动与国内相关法律法规衔接的问题。[31]其实,在CPTPP和DEPA缔约方法律中并无类似我国数据出境安全评估的制度,所以,其是否构成过度的数据出境规制有必要事先考证其在这些条约下的正当性。虽然我国《个人信息保护法》规定:“可以按照缔结或参加的国际条约、协定的规定向境外提供个人信息”,但CPTPP和DEPA仅是原则性规定,不具有可操作性,且我国法院原则上拒绝国际贸易协定在我国的直接适用。

欧美对跨境数据传输采用了不同的规制路径,欧盟是“以地理区域为基准”,依据“充分性”原则,进行事前防范的规制路径;美国则是“以组织机构为基准”,依据“问责制”原则,进行事后问责的规制路径。[32]相比在FTA中已自成体系的数字贸易规则“美式模板”,欧盟数字贸易专门章节的构建进程是比较滞后的。[33]目前,我国则在美国模式的文本中加入了强有力的国家安全保障,即涉及合法公共政策目标可由采取限制措施的一方决定。

我国数据跨境流动规制在国际上承受着诸多压力。[34]特别是由于其评估程序的启动门槛设置较低,或将导致相当一部分本不具有可阻却事由的数据处理者被预先纳入企业风险自评估环节,造成个人信息跨境传输效率受阻,影响数字贸易业务的对外开展。[35]

因为RCEP等我国所加入的FTA对跨境数据传输并未明确限制缔约方的规制权,所以,当下我国的数据出境安全评估制度尚与我国所承担的国际义务相符。但因为我国已经正式申请加入CPTPP和DEPA等开放内容更多的FTA或数字经济协定,所以,伴随着我国加入这些条约的过程,有必要逐步使得国内法与这些条约相协调。有学者提出我国的数据出境安全评估制度可能通不过“合法公共政策目标”的必要性测试,因为被质疑APEC的《跨境隐私规则》等成为对贸易限制更小的替代方案。[36]也有学者认为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。[37]这也充分表明我国的数据出境安全评估制度是否能够符合DEPA的要求将会产生较为激烈的争论。

DEPA共包含16个模块,主要特点为约束性规则较少。[38]且各国政府可以选择直接与DEPA协定对接,从而扩大与新成员的协议,也可以决定在不同的环境中选择和使用模块的全部或部分,如考虑将DEPA协定条款直接纳入其他贸易协定,或选择使国内政策与DEPA协定相关内容一致。[39]

《征求意见稿》对不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的跨境数据传输情形做了明确规定,从而整体上对跨境数据传输是有利的。从数据出境安全评估的角度来看,《办法》规定的是自上年1月1日起累计向境外提供10万人个人信息的数据处理者向境外提供个人信息需要申报数据出境安全评估。而按照《征求意见稿》的规定,预计一年内向境外提供1万人以上、不满100万人个人信息,与境外接收方订立个人信息出境标准合同并向省级网信部门备案或者通过个人信息保护认证的,可以不申报数据出境安全

评估。上述两个规定的时间计算节点是存在区别的,《征求意见稿》的计算时间更短,因此,如果按照《征求意见稿》指示的时间内向境外提供10万人以上个人信息的,也会符合《办法》中的申报要求。从这一点来看,《征求意见稿》可以理解为大大提高需要申报数据出境安全评估的条件,即,从10万人以上的信息提高到100万人以上,100万人以下的,订立个人信息出境标准合同或经过认证即可。虽然《征求意见稿》大大缩小数据出境安全评估的范围,但其是否符合CPTPP和DEPA的要求并不明确,在加入谈判中既有缔约方也会经常对此发难。所以,在加入DEPA和CPTPP的谈判中,除了逐渐减少数据出境安全评估的情形之外,还要说服既有缔约方我国的数据出境安全评估制度是符合"合法公共政策目标"和一般、安全例外条款。同时,也要明确如何履行我国缔结或参加的条约中跨境数据传输规定,特别是当其与数据出境安全评估有不同规定时的处理方法。在现有安全评估、个人信息保护认证、标准合同管理措施的基础上,可以考虑将"同等保护"作为一项独立的数据出境合法性事由。[40]

(三)引入白名单机制及自贸试验区的先行先试

白名单机制是根据数据流入国的政治法律环境,将部分国家和地区纳入可自由传输的国家和地区,形成白名单国家(地区)。我国也可以推动白名单机制,同时也要求我国针对白名单中的国家建立定期评估机制。[41]我国也可以进行双边数字经济协定谈判试点,寻找相似保护水平与发展诉求的数字经济体开展合作,形成较为合理的区域网格化布局,争取形成更加符合我国国家和企业利益的数字贸易或电子商务规则。[42]可以借鉴欧盟的个人信息保护充分性认定机制,同时,也要特别考虑数据传输到这些白名单国家和地区可能存在的国家安全风险。既要考虑拟列入白名单国家和地区的个人信息保护规则是否符合我国的个人信息保护标准,也要考虑国家层面的安全问题。在此方面,可以考虑在上海合作组织内开展相关讨论,尝试着从上海合作组织的成员中选取符合上述要求的国家进行试点合作,待条件成熟时再逐步扩大范围。我国可优先选择与我国具有较高政治互信度和经贸关系联结的国家进行数据跨境传输的合作尝试。[43]

我国目前在部分地区试点的白名单企业选定也应继续向全国普及,并且逐步将备选企业的数量限制放开,毕竟目前所试点的企业数量过少。对那些个人信息保护内部规定完善并能够充分保护个人信息的企业,逐步放开个人信息出境的管制,将其纳入白名单企业。这样,在充分调动企业和行业协会积极性的前提下,可以营造出企业自主积极保护个人信息的氛围。自贸区(港)可尝试申请国家授权建立"同主体同类数据高频出境白名单制度",即数据第一次出境时仍须完整执行安全评估流程,同时对数据处理者、数据接收方、数据条目、数据出境频次和数据用途等进行备案,后续同主体同类数据再次出境时,可省去繁琐的评估流程。[44]

我国可以利用容错机制在自贸区先行先试,充分发挥自贸区的制度试验性功能。[45]数据出境监管属于国家事权,自贸区(港)进行制度创新探索的视角"不是使不能出境的数据出境",而是"让可以出境的数据出境时更为便捷"。[46]

注释:

①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158页。

②张舵:《略论个人数据跨境流动的法律标准》,载《中国政法大学学报》2018年第3期,第100页。

③黄宁、李杨:《"三难选择"下跨境数据流动规制的演进与成因》,载《清华大学学报(哲学社会科学版)》2017年第5期,第179页。

④ See Susan Ariel Aaronson, Data Is Different, So Policymakers Should Pay Close Attention to ItS Governance, in Mira Burri ed., Big Data and Global Trade Law, Cambridge University Press, 2021, p.342.

⑤蔡宇姬:《数据出境的界定及监管制度》,载《中国政法大学学报》2023年第3期,第195页。

⑥马光:《数据跨境流动国际规则的发展与我国的应对》,载《国际法学刊》2020年第2期,第87页。

⑦刘金瑞:《迈向数据跨境流动的全球规制:基本关切与中国方案》,载《行政法学研究》2022年第4期,第77页。

⑧赵骏、向丽:《跨境电子商务建设视角下个人信息跨境流动的隐私权保护研究》,载《浙江大学学报(人文社会科学版)》2019年第2期,第61页。

⑨徐伟功、张伟华:《中欧跨境数据流动治理合作机制:从非合作博弈到合作博弈》,载《河南财经政法大学学报》2023年第4期,第71页。

⑩徐伟功、张伟华:《中欧跨境数据流动治理合作机制:从非合作博弈到合作博弈》,载《河南财经政法大学学报》2023年第4期,第71页。

⑪马其家、李晓楠:《论我国数据跨境流动监管规则的构建》,载《法治研究》2021年第1期,第92页。

⑫何波:《中国参与数据跨境流动国际规则的挑战与因应》,载《行政法学研究》2022年第4期,第95页。

⑬马光:《FTA数据跨境流动规制的三种例外选择适用》,载《政法论坛》2021年第5期,第16页。

⑭马光:《论国际法上网络安全的定义和相关国际规则的制定》,载《中国政法大学学报》2019年第3期,第74页。

⑮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》,载《国际法研究》2021年第6期,第76页。

⑯梅傲:《数据跨境传输规则的新发展与中国因应》,载《法商研究》2023年第4期,第66页。

⑰马光、毛启扬:《数字经济协定视角下中国数据跨境规则衔接研究》,载《国际经济法学刊》2022年第4期,第49页。

⑱何波:《中国参与数据跨境流动国际规则的挑战与因应》,载《行政法学研究》2022年第4期,第95页。

⑲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〉》,载《行政法学研究》2023年第1期,第74页。

⑳张凌寒:《论数据出境安全评估的法律性质与救济路径》,载《行政法学研究》2023年第1期,第44-45页。

㉑洪延青:《数据跨境流动的规则碎片化及中国应对》,载《行政法学研究》2022年第4期,第63页。

㉒赵精武:《论数据出境评估、合同与认证规则的体系化》,载《行政法学研究》2023年第1期,第79页。

㉓关于我国的数据出境安全评估制度,请参考马光:《论我国数据出境安全评估制度构建》,载《上海政法学院学报》2023年第3期,第126-137页。

㉔孙南翔:《CPTPP数字贸易规则:制度博弈、规范差异与中国因应》,载《学术论坛》2022年第5期,第7页。

㉕鄢雨虹:《数据跨境流动规制中的正当公共政策目标例外及中国因应》,载《兰州学刊》2022年第2期,第116页。

㉖许可:《自由与安全:数据跨境流动的中国方案》,载《环球法律评论》2021年第1期,第34页。

㉗张倩雯:《数据跨境流动之国际投资协定例外条款的规制》,载《法学》2021年第5期,第100页。

㉘刘金瑞:《迈向数据跨境流动的全球规制:基本关切与中国方案》,载《行政法学研究》2022年第4期,第86页。

㉙蔡宇姬:《数据出境的界定及监管制度》,载《中国政法大学学报》2023年第3期,第205页。

㉚谭观福:《数字贸易中跨境数据流动的国际法规制》,载《比较法研究》2022年第3期,第184页。

㉛石静霞、陆一戈:《DEPA框架下的数字贸易核心规则与我国的加入谈判》,载《数字法治》2023年第1期,第119页。

㉜许多奇:《个人数据跨境流动规制的国际格局及中国应对》,载《法学论坛》2018年第3期,第134页。

㉝周念利、陈寰琦:《数字贸易规则"欧式模板"的典型特征及发展趋向》,载《国际经贸探索》2018年第3期,第96页。

㉞王楚晴:《申请加入DEPA背景下中国数据治理的相容性审视及优化路径》,载《太平洋学报》2023年第3期,第9页。

㉟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》,载《国际商务研究》2023年第3期,第66页。

㊱徐莉:《跨境数据流动规制之"合法公共政策目标例外"与中国实践》,载《求索》2023年第4期,第164页。

㊲谭观福:《数字贸易中跨境数据流动的国际法规制》,载《比较法研究》2022年第3期,第184页。

㊳周念利、于美月:《中国应如何对接DEPA——基于DEPA与RCEP对比的视角》,载《理论学刊》2022年第2期,第56页。

㊴赵旸頔、彭德雷:《全球数字经贸规则的最新发展与比较——基于对〈数字经济伙伴关系协定〉的考察》,载《亚太经济》2020年第4期,第66页。

㊵何波:《中国参与数据跨境流动国际规则的挑战与因应》,载《行政法学研究》2022年第4期,第100页。

㊶李晓楠、宋阳:《国家安全视域下数据出境审查规则研究》,载《情报杂志》2021年第10期,第81页。

㊷张正怡:《论数字经济协定的造法"再平衡"走向及中国回应》,载《法商研究》2022年第6期,第68页。

㊸梅傲:《数据跨境传输规则的新发展与中国因应》,载《法商研究》2023年第4期,第70页。

㊹周念利、于美月、柳春苗:《我国自贸区(港)数据跨境流动试点制度创新研究》,载《国际商务研究》2023年第4期,第10页。

㊺徐莉:《跨境数据流动规制之"合法公共政策目标例外"与中国实践》,载《求索》2023年第4期,第167页。

㊻周念利、于美月、柳春苗:《我国自贸区(港)数据跨境流动试点制度创新研究》,载《国际商务研究》2023年第4期,第5-6页。