RCEP争端解决机制对数据跨境流动问题的适用与中国因应

赵海乐*

内容摘要:RCEP第12章“电子商务”原则上不适用RCEP争端解决程序,但允许缔约方选择适用。这引发了中国是否应当同意数据跨境流动条款具有可诉性的讨论。RCEP数据跨境流动条款中设置的“公共政策例外”与“基本安全利益例外”将为我国数据跨境流动规制措施提供政策空间,但我国仍须以非歧视的方式进行规制,同时对安全评估、关键信息基础设施等规则进一步澄清。此外,承认RCEP数据跨境流动条款可诉性,将有助于我国避免他国的制度性歧视。因此,承认RCEP数据跨境流动条款可诉性符合我国国家利益,但仍应以此承诺换取他国对等安排。

关键词:RCEP　数据跨境流动　公共政策例外　基本安全利益例外

一、引言

随着全球数字经济的蓬勃发展,与电子商务或数字贸易相关的自由贸易协定(Free Trade Agreement,FTA)谈判也同样飞速进行。在亚太地区,长期以来我国一直是区域数字贸易自由化规则制定的旁观者,但从2015年中韩与中澳FTA开始,我国逐渐积极参与区域数字贸易规则制定。[①]至今为止,我国参与的FTA中,最为复杂的数字贸易规则当属2020年底缔结的《区域全面经济伙伴关系协定》(Regional Comprehensive Economic Partnership,RCEP)。其中不仅包括电子签名、无纸化贸易等我国向来接受度较高的传统电子商务条款,还包括线上个人信

*　吉林大学法学院副教授。

本文系国家社会科学基金重大项目“中国参与制定国际劳工标准新规则研究”(项目批准号:19ZDA136)、吉林大学劳动关系专项研究课题“国际贸易规则重构对职工权益实现影响研究”(项目批准号:2021LD010)阶段性成果。

①　参见李冬冬:《亚太地区数字贸易自由化路径的演进、分歧与启示》,《亚太经济》2021年第4期,第23-32页。需要说明的是,当前主流FTA文本中并不明确区分“数字经济”与“电子商务”,以上述名称为章节标题的条约文本并无本质差异。本文因而对此不另做区分。

息保护、数据跨境传输、计算设施本地化等当前热点议题。不过，值得一提的是，由于RCEP缔约方经济发展水平差异过大，RCEP规则体系不得不坚持开放与包容性，[①]以保证不同发展水平的缔约方能就此议题达成一致，其中最典型的条款即为最不发达成员设定更长的过渡期。另一个体现RCEP开放性的制度设计，则是其中的争端解决机制。例如，RCEP第12章“电子商务”第17条第3款规定，“任何缔约方不得就本章项下产生的任何事项”诉诸第十九章争端解决程序，除非缔约方对此明确同意。这意味着，因RCEP电子商务章节产生的争议，仅会在两缔约方均在事前或事后明确同意的情况下才能提交争端解决程序；且缔约方的同意，可能基于该章特定事项、特定条款而非该章整体。某一缔约方甚至还可能仅仅同意与RCEP特定相对方而非全体缔约方开启争端解决程序。这因而引发了我国应思考的问题：我国未来是否应当承认RCEP电子商务章节诸条款的可诉性？鉴于RCEP电子商务章节内容颇为复杂，本文并不对此进行整体评述，而仅仅选择核心条款之一——数据跨境流动条款进行研究。

本文的分析将始于对RCEP第12章第15条的研究，剖析其对缔约方数据跨境流动权利义务的设定；在此基础上，分别结合我国国内立法与海外利益诉求，分析接受数据跨境流动条款可诉性将对我国国内法治造成的影响以及可能为我国海外利益带来的助益；最后，基于以上分析为我国未来对RCEP数据跨境流动条款的可诉性安排提出意见和建议。

二、RCEP数据跨境流动规则解析

（一）RCEP第12章第15条文本解读

RCEP第12章第15条，是对数据跨境流动的规定。其条款如下：

“一、缔约方认识到每一缔约方对于通过电子方式传输信息可能有各自的监管要求。

二、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。

三、本条的任何规定不得阻止一缔约方采取或维持：

（一）任何与第二款不符但该缔约方认为是其实现合法的公共政策目标所必要的措施，只要该措施不以构成任意或不合理的歧视或变相的贸易限制的方式适用；或者

（二）该缔约方认为对保护其基本安全利益所必需的任何措施。其

① 参见田云华等：《RCEP的开放规则体系评价：基于CPTPP的进步与差距》，《国际贸易》2021年第6期，第65-72页。

他缔约方不得对此类措施提出异议。”

第15条第3款第1项中的“必要”与第2项中的“必需”措辞虽有不同,但英文版表述均为“necessary”一词。从这一意义上讲,至少在RCEP第12.15条语境下,“必要”与“必需”应当不存在根本性区别。不过,条约文本仅仅在第3款第1项“必要”一词后以脚注的形式强调,就本项而言,缔约方确认实施此类合法公共政策的必要性应当由实施的缔约方决定。第3款第2项“必需”一词后则无此注释。

上述条约文本中,最核心的义务性规定当属第15条第2款,该款原则性禁止对数据跨境流动的限制。该条款并未明确“数据”的类型,因而既可能包括个人信息也可能包括非个人信息。此外,此处规制的数据跨境流动仅包括以“商业行为”为目的,政府或司法机关主导的数据跨境流动(如跨境取证)不受此条款规制。

不过,对数据跨境流动限制的原则性禁止,同时要受到第3款中两项例外的限制。在第一项公共政策例外中,援引例外一方实施的措施应当服务于“合法的公共政策目标”,但对于何为“公共政策目标”并未明示。鉴于第15条第1款载明,“缔约方认识到每一缔约方对于通过电子方式传输信息可能有各自的监管要求”,这暗示着,监管措施尽管在国家间存在差异,但其完全可能均服务于合法的公共政策目标。此外,“公共政策例外”的另一个特征是其“自裁决”属性。此例外措辞为,“缔约方认为是其实现合法的公共政策目标所必要的措施”。“缔约方认为”一词,足以保证措施实施者有权决定涉案措施的必要性。不仅如此,此例外文本还通过脚注特别强调,“缔约方确认实施此合法的公共政策的必要性应当由实施的缔约方决定”。“实施的缔约方”一词进一步表明,某措施的施行者同时也属于该措施必要性的最终判定者。与之形成鲜明对比的是,GATT第20条“一般例外”中就并未出现“缔约方认为……”字样。这也意味着,自裁决性是RCEP第12章第15条区别于GATT“一般例外”最明显的特征。当然,RCEP第12章第15条与GATT“一般例外”在设计上仍然存在相当的共性。缔约方实施某项数据跨境流动限制措施,不得构成任意或不合理的歧视,或者变相的贸易限制。

与公共政策例外相比,基本安全例外的设计更加简单。缔约方认为是保护其基本安全利益所必需的措施,均可豁免RCEP对数据跨境自由流动的要求。此处并未对措施是否应当以“非歧视”的方式施行、该措施是否构成对贸易变相限制进行额外要求,也并未像GATT第21条“安全例外”那样,要求保护该缔约方基本安全利益的措施必须与裂变材料、军火贸易或紧急情况相关。不仅如此,基本安全例外条款还要求,“其他缔约方不得对此类措施提出异议”。此处的“提出异议”对应的英文文本为“be disputed”。这意味着,“不得对此类措施提出异议”可能被解读为“不得对此措施提起争端解决之诉”。

（二）RCEP第12章第15条对成员方规制数据跨境流动权力的影响

从上述条款文本设计来看，不论是上述哪一款例外，较之于GATS或GATT一般例外、安全例外，RCEP均更加倾向于尊重、保护成员方规制数据跨境流动的权力。

1.RCEP第12章第15条基本安全例外对司法审查的排除

RCEP第12章第15条中的基本安全例外，不论是较之于GATT第21条、GATS第14条，还是RCEP第17章中的“安全例外”，均更加宽松。RCEP第17章“一般条款和例外”第13条“安全例外”适用于RCEP整体，其自然也适用于RCEP第12章。不过，鉴于RCEP第12章第15条中的“基本安全例外”规则是专门适用于数据跨境流动的特别规则，根据“特别法优于一般法”的法理，RCEP第12章第15条“基本安全例外”应当优先于RCEP第17章第13条“安全例外”。WTO判例表明，GATT“安全例外”可以提交司法审查，援引例外一方行为的合法性也因此可能被否决。而RCEP第12章第15条中的基本安全例外，则以十分肯定的措辞完全排除了司法审查空间。此种状况，即便在RCEP当中也同样是特例。RCEP的总体态度是严格限制缔约方援引“安全例外”的政策空间。具体来讲，RCEP第17章第13条“安全例外”仅规定缔约方有权采取“其认为对其保护其基本安全利益所必需的行动”，允许缔约方对行为必需性进行自裁决。至少在措辞上，第17章第13条并未强调不得依据此条款提起争端解决之诉；同时其对“基本安全例外”的界定也相对严格，缔约方必须证明其主张的基本安全利益属于法定事项才可援引此例外。

2.RCEP第12章第15条公共政策例外排除了“必需性”审查

RCEP第12章第15条公共政策例外的设计较之于GATT一般例外更加宽松。这首先体现为对“公共政策”一词的宽松界定。GATT“一般例外”中并无宽泛的“公共政策”例外，而仅仅包含公共道德、环境、健康等更加特定化的例外种类；GATS第14条例外虽允许成员方采取“为保护公共道德或维护公共秩序所必需”的措施，但是特别强调，此处的公共秩序例外仅能在“社会根本利益受到真正和足够严重的威胁”时方可援用。[①]对比而言，在RCEP第12章第15条语境下，援引例外的一方证明其政策目标系服务于公共政策考量显然更加容易。

不仅如此，不论是GATT还是GATS一般例外，均不允许缔约方自行认定涉案措施是否服务于某一目标所必需，此问题必须经由司法程序裁定。在RCEP第12章第15条项下，援引例外一方无须证明其行为的必需性。这就意味着，对数据跨境流动进行限制的国家无须证明其限制措施为对贸易损害最小、且别无其他合理替代措施——此种对“必需性”的解读，是从美国—博彩案到韩国—牛肉案以来一

① 对于数据跨境流动是否符合公共政策、公共道德等特定种类例外的讨论，参见张倩雯：《数据跨境流动之国际投资协定例外条款的规制》，《法学》2021年第5期，第90-102页。

贯坚持的,且在GATT与GATS项下完全一致。[①]正如世界贸易组织(WTO)上诉机构在韩国—牛肉案中总结的,对于某项措施是否具有"必需性",判断标准的一端是"有助于"某政策目标的实施即可;另一端则是"实现某政策目标不可或缺"。而"必需性"判断显然与"不可或缺"标准更加接近。[②]一项措施如果是其他措施绝对不可替代的,则该项措施必然符合"必需性"标准;但如果仍然存在其他替代措施,则还需要在个案中运用比例原则继续分析:这些措施对于实现上述目标的贡献大小;所保护的共同利益与价值有多重要;涉案措施对于贸易的影响多大,进而决定究竟是否应当采用替代措施。[③]从GATT到WTO,能够成功突破"必需性"要件援引一般例外的例子并不多见。在绝大多数案件当中,争端解决机构均认为存在同样有效、且对贸易影响更小的替代措施。对此,唯一的例外,或许是欧共体—石棉案;而此案的特殊性恰恰在于,涉案措施为贸易禁令而非贸易限制措施。在该案当中,上诉机构认定,石棉的毒性人所共知,因而除禁止其使用之外再无其他措施可以保护人类健康。[④]

与"安全例外"类似,上述公共政策例外,在RCEP文本中同样具有特异性。RCEP第17章虽有第12条"一般例外",但该条款仅仅重申了GATT第20条例外与GATS第14条例外对RCEP的适用,而未对其要件进行任何修改。

与此同时,"歧视"与"变相限制"两要件的存在,意味着缔约方规制权仍要受到一定限制,以保证涉案措施不至于构成贸易保护。RCEP第12章第15条与GATT第20条、GATS第14条类似,均要求涉案措施不得构成"任意或不合理的歧视"。这要求行为方涉案措施必须以国家间平等、产品间平等的方式加以实施。而此种平等,不仅仅包括法律上的平等,还包括事实上的平等——即相同法律在具体实施过程当中必须给予各方同等待遇。在WTO判例中,曾将此种平等演绎为"平等进行谈判的权利"。在美国—虾案中,专家组认为,美国有义务善意、尽可能努力地与相关国家进行谈判,以达成贸易限制措施之外的解决方案;而对于"善

① 援引WTO判例对RCEP文本进行解读之所以具有正当性,一方面是由于WTO规则在国际经济法领域具有"宪法"性地位,因而足以对FTA解释提供指引;另一方面是因为RCEP第19章第4条明确规定,"WTO争端解决机构通过的WTO专家组报告和 WTO上诉机构报告中所作出的相关解释",在审理纳入RCEP的《WTO协定》的条款相关争议时应当进行考量。参见杨署东、谢卓君:《跨境数据流动贸易规制之例外条款:定位、范式与反思》,《重庆大学学报(社会科学版)》2021年第4期,第1-15页。

② See WTO, Korea-Measures Affecting Imports of Fresh, Chilled and Frozen Beef, Appellate Body Report, WT/DS161/AB/R, para.161.

③ See WTO, Korea-Measures Affecting Imports of Fresh, Chilled and Frozen Beef, Appellate Body Report, WT/DS161/AB/R, para.162.

④ See WTO, European Communities-Measures Affecting Asbestos and Products Containing Asbestos, Appellate Body Report, WT/DS135AB/R, para.172.

意”和“尽可能努力”的评判标准，则应当比照美国此前完成谈判的中美洲国家所获得的待遇进行。而且，谈判过程必须考虑到各国实际情况，不得“一刀切”地以单一标准取代协商谈判。[①]除此之外，此种“任意或不合理的歧视”还可能产生于贸易措施过于模糊、行政机关裁量权过于宽泛的情形之下。在欧共体—海豹制品案中，上诉机构认为，此种过于宽泛的立法可能导致某些商业捕猎被划归“土著居民例外”，进而在商业捕猎行为之间造成歧视性待遇。[②]

除“任意或不合理的歧视”这一要件之外，“对贸易的变相限制”要件同样会对缔约方产生一定限制。尽管此标准的内涵与歧视要件存在一定重叠，当前通过WTO判例确立的法律标准，包括“涉案措施是否对外公布”“措施的实施过程是否存在任意或不合理的歧视”“措施是否具有保护主义目的”等要素。[③]

上述诸要件的设置如何对数据跨境流动产生影响，下文还将具体论述。但上文分析至少能够阐明的是，RCEP数据跨境流动条款通过对数据跨境自由流动的原则性规定和宽泛的例外设定，为缔约方确立了对数据跨境流动进行规制的政策空间。此种政策空间能否有效维护我国数据流动国内法律规制的合法性空间、是否会对我国海外利益的维护产生负面影响，将共同决定我国是否应当承认RCEP数据跨境流动条款的可诉性。

三、我国数据流动规则在RCEP项下的合法性

（一）我国数据跨境流动法治现状

目前，我国已形成了较为完善的数据跨境流动法律框架。我国法律在界定某些情形须进行数据出境审查的同时，原则上允许数据跨境流动。

首先，我国数据出境审查的一个重要方面，是对关键信息基础设施境内运营数据出境的安全审查，这其中可能同时涉及个人信息、公共秩序与国家安全三方面利益的维护。例如，我国2017年《网络安全法》第37条规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估”。《网络安全法》第31条将关键信息基础设施界定为“国家对公共通信和信息服务……重要行业和领域，以

① See WTO, United States-Import Prohibition of Certain Shrimp and Shrimp Products (Article 21.5), Panel Report, WT/DS58/RW, paras.5.67-5.74.

② See WTO, European Communities-Measures Prohibiting the Importation and Marketing of Seal Products, Appellate Body Report, WT/DS400/AB/R, para.5.328.

③ 对此的阐述与批评，参见Chang-Fa Lo, *The Proper Interpretation of "Disguised Restriction on International Trade" under the WTO: The Need to Look at the Protective Effect,* 4 Journal of International Dispute Settlement 111-137 (2013).

及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”。这其中就同时包含了公共秩序要素与国家安全要素。而关键信息基础设施引发安全评估的,又恰恰是个人信息出境,这不可避免地会涉及个人信息保护问题。2021年《个人信息保护法》第40条、《数据安全法》第31条、《网络安全审查办法(修订草案征求意见稿)》第2条也均有类似规定。

其次,我国信息出境安全审查的又一重要方面,体现在《个人信息保护法》第40条的规定: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,其信息出境应通过国家网信部门组织的安全评估。此规定在《网络安全审查办法(修订草案征求意见稿)》第6条中,被细化为掌握超过100万用户个人信息的运营者赴国外上市,须首先提交网络安全审查。二者措辞虽有差异,但共性在于,均认可处理个人信息达到一定数量即可引发数据出境安全审查义务,而非特定数量个人信息实际出境时才需要提交安全审查。这无疑表明,我国法律对数据出境可能引发国家安全问题防患于未然,而非基于实际、确定的风险对数据出境进行限制。

再次,重要数据的跨境流动同样会引发安全评估。2017年《网络安全法》第37条规定,关键信息基础设施的重要数据原则上应当境内存储,其跨境传输应当通过安全评估;2021年《数据安全法》第31条也作出了类似规定。2021年《汽车数据安全管理若干规定(试行)》第11条在强调重要数据出境安全评估义务的同时,对重要数据进行了定义。其中,既包括与个人信息保护相关的内容(如涉及个人信息主体超过10万人的个人信息、人脸信息),也包括非法利用将危害国家安全或公共利益的数据,如车流物流数据等。

最后,对于不包含在上述任一情形之内的个人信息跨境传输,我国目前并未要求一概进行安全评估。根据我国2021年《个人信息保护法》第38条,个人信息出境仅在涉及关键信息基础设施、处理个人信息达到某一数量的两种情形下才需要通过安全评估;除此之外,“按照国家网信部门的规定经专业机构进行个人信息保护认证”、采纳“国家网信部门制定的标准合同与境外接收方订立合同”均可成为合法性来源。不过,后两种情形需要履行向个人告知的义务并取得其单独同意(第39条)。这明显有别于我国《个人信息出境安全评估办法(征求意见稿)(2019年版)》原则上要求个人信息出境均应进行安全评估的严格态度。当然,该征求意见稿随后并未获得通过。这也侧面证明,我国数据出境并不是有些学者所主张的“凡出必审”,[①]而是仅有少数几种信息出境须以安全评估为前提。

① 参见薛亦飒:《多层次数据出境体系构建与数据流动自由的实现——以实质性审查制变革为起点》,《西北民族大学学报(哲学社会科学版)》2020年第6期,第64-74页。

（二）我国数据出境管理政策在RCEP第12章第15条项下的合法性

我国数据出境管理政策的合法性问题，从2017年起就曾屡次在WTO遭到美欧质疑。其中，最为详细的一份质疑文件，是美国2017年9月26日提交至WTO的《来自美国的通讯——中国与其〈网络安全法〉相关的已采取和起草中的措施》。从文件名称可知，美国此份质疑文件主要针对我国《网络安全法》，且质疑内容不仅包括我国已采取的措施，还包括对我国未来可能采取措施的预判。[①]美国表示，中国《网络安全法》对于重要信息和个人信息出境的特别要求会严重影响数据跨境流动；经营者必须满足严苛的条件才能将数据传输至境外，这对经营者而言负担过重，数据控制者必须证明数据出境的必要性，而且个人信息出境还要获得数据主体的单独同意，这同样为经营者施加了过重的负担，且此措施本身无助于隐私保护。美国在此基础上主张，除“安全评估”和“单独同意”之外，中国可以采取其他足以实现隐私保护目标且使企业负担更小的措施，例如，遵从跨境隐私保护规则（Cross-Border Privacy Rules，CBPR）、承认网络运营者与第三方数据接收者之间的合同安排、进行第三方认证（third-party accreditation）等。除此之外，美国还主张，中国数据出境管理法律措辞过于空泛，例如，对于何种情形下会导致数据跨境传输危及国家安全、社会公共利益，未作详细说明，这将导致涵盖范围过广，进而构成对跨境数据流动的直接禁止。此后，美国与欧盟陆续于2018—2019年向WTO提交类似文件，[②]截至目前，最后一份质疑文件发布于2019年4月。这些文件在重复上述内容的同时，还提出了关键信息基础设施界定不清晰、《网络安全法》内容须细化等问题。

美国与欧盟并非RCEP缔约方，但上述质疑的内容却很可能在RCEP数据跨境流动争端解决程序中重现。美国上述质疑，很大程度上涵盖了我国数据出境管理政策的合法性争点。对我国数据跨境流动现行规则与上述质疑内容进行分析，有助于揭示我国数据出境管理政策未来可能面临的合法性之争。

1.我国数据出境安全评估符合RCEP第12章第15条“基本安全例外”

考虑到RCEP第12章第15条“基本安全例外”的规定最为宽松，我国如能够

---

① See The United States, Communication from the United States, Measures Adopted and under Development by China Relating to its Cybersecurity Law, S/C/W/374.

② See EU, Statement by the European Union to the Committee on Technical Barriers to Trade - 21 and 22 March 2018, G/TBT/W/509; The United States, Communication from the United States - Measures Adopted and under Development by China Relating to its Cybersecurity Law - Questions to China, S/C/W/378; EU, Committee on Technical Barriers to Trade - China - Cybersecurity Law - Statement by the European Union to the Committee on Technical Barriers to Trade - 14 and 15 November 2018, G/TBT/W/590; EU, China - Cybersecurity Law - Statement by the European Union to the Committee on Technical Barriers to Trade, 6 and 7 March 2019, G/TBT/W/637.

证明数据出境安全评估符合此项例外,则其他缔约方可能难以对我国数据出境安全审查制度在争端解决机制项下提出质疑。根据RCEP第12章第15条,“基本安全例外”得以适用的条件,是涉案措施为该缔约方认为保护其基本安全利益所必需的措施。虽然此条款的“自裁决”属性意味着,我国无须证明上述数据出境安全审查措施具有“必需性”,但根据WTO相关判例,我国仍须证明另外两个要件:存在受保护的基本安全利益;涉案措施与保护基本安全利益之间存在关联。

具体而言,根据RCEP第19章第4条,“WTO争端解决机构通过的WTO专家组报告和WTO上诉机构报告中所作出的相关解释”,在审理纳入RCEP的WTO协定条款相关争议时应当进行考虑。尽管RCEP第12章第15条中的“基本安全例外”与GATT第21条安全例外不完全相同,但至少“该缔约方认为对保护其基本安全利益所必需的措施”这一表述,完整地从GATT第21条纳入了RCEP第12.15条。因此,以俄罗斯—过境措施案为代表的WTO判例对GATT第21条进行的解释,也能够对RCEP第12章第15条“基本安全例外”进行解释与补充。在俄罗斯—过境措施案专家组报告中,专家组虽然承认“基本安全例外”的自裁决性,但同时认为,WTO争端解决机构仍然有权对“基本安全利益”是否存在以及涉案措施与基本安全利益是否存在关联进行判断。

对于何为基本安全利益,专家组在俄罗斯—过境措施案中认为,基本安全利益区别于一般性的“安全利益”,所指代的利益必然与国家典型职能紧密相关,即保护其领土和人民免受外来威胁;保护境内法治与公共秩序。专家组同时表明,虽然每个国家理论上都有权决定何为其基本安全利益且各国对此的界定必然存在区别,但是各国仍然需要依照《维也纳条约法公约》第31条中的“善意原则”进行定义。[①]《维也纳条约法公约》第31条规定的“善意原则”要求各国不得适用“安全例外”以规避其在GATT项下的义务,如将贸易利益包装为基本安全利益。[②]上述分析意味着,虽然GATT第21条安全例外并未承认一国对何为“基本安全利益”拥有最终决定权,但WTO争端解决机构仍然充分尊重当事国的自行裁量。当事国理论上仍须对“基本安全利益”进行善意定义,但“善意”的程度仅为“不规避条约义务”即可。

对于涉案措施与基本安全利益的关联,专家组同样运用善意原则进行了分析,并认为涉案措施必须具有“服务于基本安全利益的最低限度的可行性”,即“并

① See WTO, Russia - Measures Concerning Traffic in Transit, Report of the Panel, WT/DS512/R, para.7.59.

② See WTO, Russia - Measures Concerning Traffic in Transit, Report of the Panel, WT/DS512/R, paras.7.130-7.133.

非全然无法服务于此目标”。[①]此标准明显低于“必需性”标准，即涉案措施并不需要是实现该基本安全利益不可或缺且对贸易损害最小的措施。

基于以上分析，我国数据出境安全评估完全可以符合上述两项要求。从基本安全利益一词的定义来看，我国关键信息基础设施、达到一定数量的个人信息与重要数据出境，所服务的目标完全可以是狭义的国家安全。毕竟，关键信息基础设施的定义即为“一旦数据泄露就可能严重危害国家安全、国计民生与公共利益”的重要网络设施、信息系统，其与国家安全的关联是毋庸置疑的，且至少不是“伪装下的贸易利益”。即便某关键信息基础设施更多地关联“国计民生”“公共利益”而非“国家安全”，我国也可以援引上文国家安全定义的“保护境内法治与公共秩序”部分进行辩护。而个人信息、重要数据与国家安全的关联，则是它们作为“情报”的价值。[②]例如，“运满满”汇总的物流信息则可能反映我国物流基础设施现状。对这些信息进行出境审查，将有助于保护我国自然、人文地理信息不被他国情报机关获取，因而具有重要的国家安全价值。

关于我国数据出境安全评估与“国家安全”这一目标之间的关联，我国仅须证明数据出境安全评估并非完全无助于维护国家安全即可。鉴于韩国曾将地图信息的本地化存储作为维护国家安全的重要举措，[③]美国也曾在行政命令中认为应用程序可能造成个人身份信息和基因信息等敏感数据泄露、进而对美国数据隐私和国家安全构成风险[④]，数据出境与国家安全的“最低限度的关联”在国际上并不缺乏实践基础。

2.我国数据出境安全评估可能符合“公共政策例外”

即便RCEP争端解决机制将数据出境安全评估进行分解、将其中与公共利益和个人信息保护相关的管理措施与涉国家安全的管理措施区分对待，这些管理措施经进一步完善也很可能符合RCEP第12章第15条“公共政策例外”。

一方面，与公共利益相关的数据出境管理措施可以基于RCEP第12.15条“公共政策例外”的要求获得合法性认定。该项例外允许缔约方自行认定某项数据出境管理措施的必需性。因此，相对方不得以“数据出境管理会导致经营者负担过重、且存在同样服务于隐私保护但负担更小的替代措施”为由，要求中国采取其

① See WTO, Russia - Measures Concerning Traffic in Transit, Report of the Panel, WT/DS512/R, para.7.138.

② 参见李晓楠、宋阳：《国家安全视域下数据出境审查规则研究》，《情报杂志》2021年第10期，第74-82页。

③ 参见人民网：《担心威胁国家安全 韩国再拒谷歌地图“输出申请”》，http://world.people.com.cn/n1/2016/1120/c1002-28881646.html，2021年10月1日访问。

④ 参见新华网：《拜登撤销对TikTok和微信等中国软件禁令》，http://www.xinhuanet.com/world/2021-06/10/c_1127549552.htm，2021年10月1日访问。

他替代措施。不过,要符合“公共政策例外”,我国还须证明,涉案措施不构成任意或不合理的歧视、也不构成对国际贸易的变相限制。因为WTO判例表明,如果一项法律文本过于空泛、导致行政机关具有过于宽泛的自由裁量权,这就可能导致个案中的不平等对待,进而构成任意或不合理的歧视;而且,我国数据出境管理措施也曾被美欧指责为“不够清晰”。

目前来看,我国法律中“关键信息基础设施”一词可能过于空泛,[①]但这一问题未来必然会得到补救。我国2021年《关键信息基础设施安全保护条例》列举了能源、交通等一系列行业,规定这些行业的“重要网络设施、信息系统”构成关键信息基础设施;不仅如此,其中还规定“一旦遭到破坏、丧失功能、数据泄露就可能严重危害国家安全、国计民生、公共利益的其他重要网络设施、信息系统”同样属于关键信息基础设施,但数据控制者同样无从预计其具体内容,也无法预知自己掌控的数据是否应当基于此条例进行出境审查。对此,该条例第8条至第10条作出了具体规定:重要行业和领域的主管部门、监督管理部门需组织认定本行业、本领域的关键信息基础设施,及时将认定结果通知运营者,并通报国务院公安部门。这意味着,运营者至少能够清晰地获知自身是否应当受到信息出境安全评估的约束。

另一个相对模糊的概念,则是“安全评估”的具体方式。这同样是美欧在我国《网络安全法》公布后提出质疑的内容之一。对此,我国目前已发布若干征求意见稿但尚未获得通过。为保证安全评估清晰、公开、具有可操作性,此方面的立法工作无疑要加速进行。[②]

另一方面,对于与国家安全、公共政策考量无关的、以个人信息保护为目标的信息出境限制,在RCEP第12章第15条项下的合法性同样能够得到保证。根据我国2021年《个人信息保护法》第38条,个人信息出境如不涉及关键信息基础设施且处理数量未达法定上限,则仅须获得个人信息保护认证或适用标准合同即可。这两种方式本身未必会为个人信息处理者施加过重负担,至少美国2017年、2018年10月向WTO提交的两份文本,都是承认上述两种方式作为合理替代措施的价值的。此处真正应当讨论的问题是,我国《个人信息保护法》第39条规定的个人信息处理者在信息出境前要向个人履行告知义务并且取得其单独同意,这是否符合RCEP第12章第15条公共政策例外?此问题同样出现在美国2019年文件中。我们认为,上述“告知同意”规则公开、透明且并不区分个人信息处理者或个

① 对此的质疑,参见欧盟2019年在WTO发表的声明。See EU, China - Cybersecurity Law-Statement by the European Union to the Committee on Technical Barriers to Trade, 6 and 7 March 2019, G/TBT/W/637.

② 参见曾磊:《数据跨境流动法律规制的现状及其应对——以国际规则和我国〈数据安全法(草案)〉为视角》,《中国流通经济》2021年第6期,第94-104页。

人信息接受者国籍、规模、所有制形态，因此，此规则显然不构成“歧视”，更无所谓“任意”与否；同时此规则并非以公共政策为由掩盖其贸易保护目的，因而，其同样不会构成对国际贸易的变相限制。或许唯一难以证明的是“告知同意”规则是否为保护个人信息所必需。不过，由于“必需性”问题在RCEP第12章第15条公共政策例外项下并不具有可诉性，因此，这很难对我国政策的合法性形成挑战。

综上，我国现行的数据出境管理体制，在其必需性免受质疑的情况下，可以在RCEP第12章第15条项下获得合法性认定。只不过，为满足第12章第15条例外的具体要求，我国未来还须对数据出境安全评估的具体方式、标准合同条款的具体内容、个人信息保护认证的具体方式加以澄清与完善，以保证规则本身的公开与透明；在具体实施过程中，应尽量保证相同情形的国家获得同等待遇。

四、RCEP第12章第15条可诉性对我国海外利益维护的意义

在确定RCEP第12章第15条不会根本影响我国数据跨境流动合法性的基础上，我国还须考量的是，此条款的可诉性，能否为我国企业海外利益的维护提供便利？换言之，我国与RCEP其他缔约方进行数字贸易可能遭遇的阻碍，究竟能否根据RCEP第12章第15条提起诉讼进而化解争端？

对于这一问题的分析，将始于对RCEP缔约方数据跨境流动规制现状的分析。首先，某些RCEP缔约方要求个人信息的跨境流动必须以目标国通过个人信息保护充分性为前提。例如，日本2017年《个人信息保护法》第24条规定，个人信息传输至第三国，如未获得数据主体同意，则该第三国必须获得日本个人信息保护委员会的“充分性认定”——确保该国个人信息保护水准与日本等同。此种“充分性认定”可构成数据从日本流动至中国的限制措施。[①]又如，澳大利亚1988年《隐私法》同样要求，受到该法律约束的企业如要将个人信息转移至澳大利亚境外，信息接收方要遵循的法律为个人信息提供的保护必须至少等同于或高于澳大利亚隐私原则的保护水平，该企业必须保证境外接收方能够遵循澳大利亚隐私原则，且对接收方违反隐私原则的行为承担责任。[②]泰国《2019年个人信息保护法》

① 参见张晓磊：《日本跨境数据流动治理问题研究》，《日本学刊》2020年第4期，第85-108页。

② See Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, Chapter 8: APP 8 — Cross-border Disclosure of Personal Information, https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information/#when-does-an-app-entity-disclose-personal-information-about-an-individual-to-an-overseas-recipient, visited on 13 October 2021.

第28条也有类似规定。[①]

其次,某些RCEP缔约方以国家安全为由拒绝特定信息出境,其中最为典型的就是韩国对于地理信息出境的限制。2016年,韩国政府就曾以国家安全为由,拒绝谷歌地图将韩国地图数据带出境外,谷歌地图如需在韩国提供服务则必须将数据存储于韩国境内。[②]

再次,有的RCEP缔约方虽然实际上限制信息出境,但并未将国家安全作为合法性来源。例如,印度尼西亚于2019年以行政命令的方式,要求"公共领域电子服务提供者"必须在印度尼西亚境内建立数据中心。这可能构成了变相的数据出境限制。[③]不过,考虑到"公共领域电子服务提供者"在该行政命令中被定义为"为政府机关提供电子服务的人",因此,上述命令视政府机关种类不同或可视为分别服务于国家安全或公共政策考量。

综上,对数据跨境流动的限制措施,在RCEP缔约方中并不罕见。尽管,这些国家未必存在类似于中国的"重要数据"概念,其规定的个人信息出境审查也未必是国家安全审查,而很可能是数据接收国的个人信息保护充分性审查。鉴于安全审查可以在RCEP第12章第15条项下豁免司法审查,但公共政策例外则未必如此,因此,有必要探讨的是,上述对于数据跨境流动的限制措施在RCEP项下是否具有合法性?

结合上文对于RCEP第12章第15条的分析可知,上述限制措施最有可能引发合法性质疑的,当属对数据接收国个人信息保护"充分性"问题的审查。此种"充分性"审查并不是RCEP缔约方所首创,欧盟此前早已开展过类似实践,学界早已对此在WTO与FTA项下展开合法性讨论。

个人信息保护充分性审查可能引发的第一个问题是,审查机关是否给予了对方国家或企业充分的机会参与认定。有学者曾在对欧盟实践研究后表示,一旦欧盟在隐私盾协议项下认可了美国个人信息保护与欧盟实质相同,则欧盟有义务至少给予其他国家同等机会与欧盟进行谈判、或由欧盟进行评估,以达成类似的安排。否则,将违反GATT第20条中对于"任意或不合理歧视"的要求。此种义务可

---

① See Thailand, Personal Data Protection Act, B.E. 2562 (2019), https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf, visited on 13 October 2021.

② 参见人民网:《担心威胁国家安全 韩国再拒谷歌地图"输出申请"》, http://world.people.com.cn/n1/2016/1120/c1002-28881646.html,2021年10月1日访问。

③ See Government Regulation of the Republic of Indonesia No.71 of 2019 ("GR 71/2019") 10 October 2019. 对此的阐述参见US Department of State, 2020 Investment Climate Statements: Indonesia, https://www.state.gov/reports/2020-investment-climate-statements/indonesia/, visited on 13 October 2021.

以类比为美国在海虾—海龟案中的善意谈判义务。[①]

个人信息保护充分性审查的第二个问题是,“充分性”审查必须遵循非歧视原则,对于同等情况的国家应当给予同等对待,以免造成任意或不合理的歧视。此处的“同等情况”并不代表两国必须完全相同才能获得同等待遇,而是就某公共政策目标而言条件相同。例如,在美国—虾案中,美国希望达成的公共政策目标是保护海龟,因此,“捕虾海域中没有海龟生活”的国家就属于同等情况下的国家,其待遇必须一致;又如,在欧共体—海豹案中,涉案公共政策目标为保护海豹,因此,“土著居民能够将狩猎海豹商业化”的国家和地区(如格陵兰)与“土著居民无法将狩猎海豹商业化”的国家(如加拿大)对欧盟而言就应当属于不同类国家,此时给予二者相同待遇反而会构成歧视。[②]这意味着,对他国个人信息保护充分性审查需实现的政策目标为个人信息保护,因此,对第三国的审查也仅应当包括这一内容,不得基于国际关系、国家经济互补性等原因给予某些国家更加宽松的待遇。[③]在此问题上,欧盟已经招致了一定批评。例如,有学者对欧盟给予新西兰的个人信息保护充分性认定进行分析后指出,欧盟的认定结果过于“务实”(pragmatic),过多关注于给予新西兰“充分性”认定能够对双边贸易产生何种影响。因此,即便新西兰具有透明度不高、缺乏数据跨境流动基本原则、对数据主体“选择退出”权利规定不足等问题,欧盟仍然对此一笔带过。但是在欧盟对澳大利亚的个人信息保护充分性评估当中,欧盟则明显更为严格。此种行为无疑是对澳大利亚的歧视。[④]

欧盟固然不是RCEP缔约方,但欧盟实践与国际法学界对此的批评足以为我国面对他国“充分性审查”提供参照。在RCEP第12章第15条项下,由于“公共政策例外”的存在,我国固然无法质疑他国的个人信息保护充分性审查是否必需,但我国完全可以关注此种审查在具体实施中是否对我国国家或企业造成了歧视。目前,RCEP缔约方中,有据可查的仅有马来西亚推出了个人信息保护充分性认定“白名单”,[⑤]且中国已在名单中。澳大利亚、日本等国虽有类似制度,

---

① See Aaditya Mattoo & Joshua P Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution,* 21 Journal of International Economic Law 769-789 (2018).

② See Emily Lydgate, *Do the Same Conditions Ever Prevail ? Globalizing National Regulation for International Trade,* 50 Journal of World Trade 971-995 (2016).

③ See S. Yakovleva & K. Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection,* 2 European Data Protection Law Review 191-208 (2016).

④ See Anna Donovan, The Adequacy Requirement: Selectively Flexible or Unjustifiable Discrimination? A Critical Analysis from an Australian Perspective, Master Thesis, University of Oslo, 2013.

⑤ See Malaysian Personal Data Protection Commissioner, Public Consultation Paper (PCP) No. 1/2017, http://www.pdp.gov.my/jpdpv2//en/pengumuman/871-public-consultation-paper-no-1-2017, visited on 13 October 2021.

但“充分性认定”开展得极其有限,且未作出对中国的歧视性认定。因此,目前尚无法对此进行实证研究。不过,基于国际法学界对于欧盟“充分性认定”的批判,未来我国一旦与他国达成了RCEP第12章第15条可诉性安排,且该国要对我国进行“充分性审查”,则我国至少可以主张:该国应当给予我国不低于第三国的程序性权利;对我国个人信息保护法律体系的评估应当基于公开、透明的标准进行;对我国个人信息保护水准的要求可以将评估国自身作为参照系但不得超出评估国自身的水平;评估内容应当仅关注个人信息保护问题,尤其不得掺杂贸易利益、经济发展水平因素,更不得基于双方经济竞争性或互补性之差异而对我国提出更高要求。

除此之外,另一个可能影响我国海外利益的问题,是他国出于公共利益考量而施加的数据跨境流动限制措施。对于此类措施,由于并未区分电子服务提供者的国籍、数据传输目的地等,因此,在无法对其“必需性”进行质疑的情况下,以“歧视”或“变相限制”为由质疑其合法性并不容易。不过,对我国企业而言,此种强制性的数据本地化政策的合法性同样未必需要质疑。这是因为,目前我国互联网企业的国际竞争力较之于谷歌、亚马逊等稍显落后,但诸如阿里巴巴、腾讯、字节跳动等中国企业,在云存储、数字金融、社交领域仍然占有重要地位。[①]不过,这些企业当前的经营策略却未必在于以中国为数据中心,反而更加倾向于更彻底的国际化经营。以字节跳动为例,近年来陆续有新闻表示其在新加坡投资建设数据中心、在美国租用数据中心,且此前曾有消息表明其拟在印度建设数据中心。如抖音/Tiktok、微信国内版与国际版等业务的分离也正在进行中。此种基于不同经营策略的“入乡随俗”,恰恰是谷歌、亚马逊等美国互联网巨头未必愿意进行的。在这一进程当中,我国企业的海外利益未必在于数据自由输出,反而在于寻求非歧视待遇,以避免承受较之于他国企业更高的负担。从这一角度来讲,即便我国无法就数据本地化措施的必要性提起争端解决之诉,以“非歧视”为由,为我国企业进入他国数字市场创造公平环境同样有其实际意义。

五、结语

从我国对数据跨境流动的限制措施来看,现行措施多出于真实的国家安全目的,与关键信息基础设施、重要数据、“大数据”个人信息以外的商业数据并未纳入国家安全考量。即便RCEP第12章第15条“基本安全利益”例外仍具有可诉性,上述考量也仍然会满足对国家安全的定义。对于基于个人信息保护目标的数据

① 参见李冬冬:《亚太地区数字贸易自由化路径的演进、分歧与启示》,《亚太经济》2021年第4期,第23-32页。

跨境流动限制，不论是“数据主体同意”“标准合同条款”，还是“第三方认证”，只要其以公开、透明、非歧视的方式实施，且具体实施方式有法可依，规则明确，就能够满足“公共政策例外”的要求。并且，以上要求同样是我国依法行政的题中之意，未来对此的细化符合我国国家利益。

另一方面，从我国应对他国跨境数据流动限制措施来看，在他国将此种限制措施“非安全化”的情况下，承认RCEP第12章第15条可诉性，有助于在两个方面维护我国企业海外利益：第一，在设置数据接收国个人信息保护充分性评估制度的国家，可诉性有助于我国企业避免制度性歧视。如他国对我国个人信息保护充分性拒绝给予评估或评估标准过于苛刻，我国政府可以根据美国—虾案确立的法理对此提出质疑，要求得到公平对待；此诉讼未必意在要求裁定违法，也可以“以斗争求和平”，以此推动双边谈判，促进与邻国的个人信息保护充分性互认。[①]第二，他国跨境数据流动限制措施的公平性问题。我国充分尊重他国数据主权、无意于效法美国干预他国个人信息保护等国内立法的具体实施方式。我国企业的海外投资也愿意遵循东道国法律，在当地设立数据中心。[②]然而，一旦当地法律以歧视性方式对我国企业实施，则RCEP第12章第15条同样有助于维护企业正当权利。

综上，鉴于承认RCEP第12章第15条并不必然损害我国规制权，因此，如时机成熟，我国可以在RCEP项下宣称愿意接受该条款相关问题的可诉性。此种态度将有助于我国展示大国担当，在区域内促进数据跨境流动，进而促进我国在数字经济领域的中长期利益。[③]当然，为保障我国当前数据跨境流动法治体系能够完全符合RCEP第12章第15条中的例外条款，我国仍须进一步细化当前法律，例如，对关键信息基础设施、重要数据等概念进一步明晰，尽量使用清单方式而非交由行政机关自由裁量。[④]对于安全评估如何进行、考量因素的具体内容等，也同样有待进一步明确。

我国对RCEP第12章第15条可诉性的承认，应当以进一步双边谈判为基础、以对等为条件，不宜以单方面报价的方式率先作出。我国并不是国际关系意义上的霸权国，也无意愿为维护区域稳定而率先提供公共产品以换取他国对合作的信心。博弈论同样表明，只有在主从博弈当中，处于领导者一方才能从先手行动当

① 参见牛哲莉：《个人数据跨境流动——中日韩合作规制进路探析》，《山东科技大学学报(社会科学版)》2021年第4期，第55-63页。

② 参见张渝：《数据本地化措施兴起下国际投资保护规则的适用困境及其纾解》，《武大国际法评论》2021年第4期，第139-157页。

③ 参见王中美：《跨境数据流动的全球治理框架：分歧与妥协》，《国际经贸探索》2021年第4期，第98-112页。

④ 参见马其家、李晓楠：《国际数字贸易背景下数据跨境流动监管规则研究》，《国际贸易》2021年第3期，第74-81页。

中获益。我国在国际合作中向来倡导人类命运共同体理念,在追求本国利益时兼顾他国合理关切。因此,我国即便有能力率先承诺实现数据跨境流动问题的法治化,也同样应当以国家利益为先,争取以此承诺换取他国对等安排。例如,我国完全可以与一个或多个RCEP缔约方展开数据跨境流动谈判,并以双边可诉性安排彰显我国履行承诺的诚意。而且,如果能够在几国间达成数据跨境流动充分性互认机制则更好。数据跨境流动的国际法问题仍处于发展之中,如果我国担心目前的可诉性承诺会掣肘未来的政策空间,则我国可以对可诉性问题进行限制性安排,例如,使用正面清单的方式列举数据跨境流动中的部分问题可提交国家间争端解决程序。此种安排在双边投资协定项下并不少见。再如,我国如认为某些措施与国计民生密切相关、不愿其合法性遭到任何形式的审查,也可效法《美墨加协定》第十九章"数字贸易"中的"祖父条款"安排,明示某些法律或措施是符合例外措施的条款。[①]

The Application of RCEP Dispute Settlement System to Cross-border Data Transfer and Its Implication for China

Abstract: RCEP dispute settlement shall not be applied to Chapter 12 Electronic Commerce in principle but member States may opt-in nonetheless. This consequently leads to the discussion about whether China shall acknowledge the adjudication of cross-border data transfer under RCEP. RCEP cross-border data transfer rules provide for public policy exceptions and essential security exceptions, which may allow for policy space for China's domestic regulation. Meanwhile, China ought to apply its regulation in a non-discriminating manner and clarify such rules as security evaluation and critical data infrastructure. Moreover, acknowledging the judiciability of RCEP cross-border data transfer clause may contribute to the avoidance of institutional discrimination. Consequently, acknowledging the judiciability is in accordance with China's national interest, but it is still advisable to do so under the theme of reciprocity.

Key words: RCEP; cross-border data transfer; public policy exception; essential security exception

(责任编辑:漆彤)

① See United States-Mexico-Canada Agreement, Annex 19-A, Article 4.