RCEP数据跨境流动基本安全例外条款与中国方案

张晓君　刘泽扬

【摘　　要】数据跨境流动是促进数字经济发展的关键要素，数据跨境流动规则因此成为RCEP电子商务章节的重要条款。RCEP确立了数据跨境自由流动原则，同时规定了公共政策目标和基本安全例外。当前，中国“本地储存，出境评估”的数据跨境流动监管模式与数据跨境自由流动的要求还存在不尽协调的问题，在现有立法下，应充分考虑基本安全例外条款的适用，以满足RCEP对数据跨境流动监管的要求。为此，应推动数据立法完善，在明确例外条款适用标准的基础上，强调数据跨境自由流动原则，统一相关概念的界定，健全数据分级分类监管规则。

【关 键 词】RCEP；数据跨境流动；基本安全例外；适用；立法完善

【作者简介】张晓君(1969-)，男，云南永德人，西南政法大学国际法学院院长，博士生导师，中国—东盟法律研究中心主任，研究方向为国际经济法、数据治理；刘泽扬(1994-)，男，重庆人，西南政法大学国际法学院博士研究生，研究方向为国际经济法、数据治理(重庆 400044)。

【原文出处】《郑州大学学报》：哲学社会科学版，2023.4.36～42

【基金项目】教育部哲学社会科学研究重大课题攻关项目“对‘一带一路’沿线国家投资风险监测预警体系研究”(项目编号：19JZD053)；重庆市教育委员会人文社科重点研究基地项目“RCEP数字贸易争端解决机制研究”(项目编号：22SKJD036)；重庆市研究生科研创新项目“数据跨境流动规制中的例外条款研究”(项目编号：CYB22184)。

随着数字全球化发展，数据跨境流动成为数字经济发展的关键要素。《区域全面经济伙伴关系协定》(以下简称“RCEP”)《全面与进步跨太平洋伙伴关系协定》(以下简称“CPTPP”)《数字经济伙伴关系协定》(以下简称“DEPA”)等主要区域经贸协定中均规定了数据跨境流动规则。RCEP作为迄今为止中国参与的最重要的区域自贸协定，其中数据跨境流动规则充分兼顾了缔约国之间经济发展和法律制度的差异，在倡导数据跨境自由流动的同时，设置了公共政策目标例外条款和基本安全例外条款。公共政策目标例外在条文中作出了较为明确的适用标准，但基本安全例外的条文相对简单，具有较大的模糊性，既不利于协定的实施，也容易引发贸易争端。故本文主要针对基本安全例外条款进行研究。

基本安全例外条款最早规定于《关税与贸易总协定》(以下简称“GATT”)第21条和《服务贸易总协定》(以下简称“GATS”)第14条。基本安全例外有其独有的制度功能，可以让缔约国履行条约义务的同时，也能寻求到维护本国安全利益的合法性依据，这对于条约的履行以及条约的灵活性有着重要意义[1]。但长久以来，基本安全利益的范

围和“自裁决”属性等问题普遍存在争议。目前各大区域自贸协定要么直接引用了该安全例外条款,要么对其进行部分修改,这导致WTO安全例外条款既存的争议也出现在当前的区域自贸协定之中。

当前,我国越来越注重国内数字立法和参与国际经贸协定的谈判。数据跨境流动规则作为经贸协定中的重要条款,也是中国立法完善与经贸谈判的重点。然而,我国现阶段数据立法与RCEP有关规则不尽协调。如何充分适用基本安全例外条款为我国数据跨境流动监管规则提供合法性依据,成为我国推动RCEP在国内实施的关键。

一、RCEP数据跨境流动的规则要义

数据跨境流动在对全球经济增长做出重大贡献的同时,也引发了国家安全、网络安全、个人隐私等问题,尤其是2013年“斯诺登事件”爆发之后,各国普遍实施大量诸如数据本地化、数据出境安全评估等限制数据跨境流动的监管措施。此外,由于传统经贸协定对于数字贸易以及数据跨境流动没有明确规定,对数据跨境流动限制性措施的规制效力不佳,也难以保障缔约方行使合法的国家规制权。在这一背景下,RCEP通过确立数据跨境流动规则,在区域范围内达成了数据跨境自由流动的共识。RCEP第12章第14条和第12章第15条就数据本地化以及数据跨境流动作出了明确规定。

(一)数据跨境流动规则的基本原则

RCEP第12章第14条规定,对于涵盖的人为进行商业行为,各缔约方不得强制要求其在境内设置计算设施或使用其领土内的计算设施。第12章第15条规定,缔约方不得阻止涵盖的人为进行商业行为通过电子方式跨境传输信息。可见,无论是对计算设施位置还是对跨境传输信息的规定,RCEP均作出了缔约方不得采取限制数据跨境流动措施的原则性规定。第12章第14条的规定也表明RCEP禁止“数据本地化”措施的态度。“数据本地化”措施通常会导致他国服务提供商在该国的运营成本大幅上升,形成贸易壁垒,从而影响数字贸易的发展。所以禁止“数据本地化”的要求是RCEP数据跨境自由流动原则对缔约国设定的核心义务。

值得注意的是,RCEP“金融服务”条款同样也要求缔约方不得阻止金融服务提供者为进行商业行为所必需的信息转移。“电信服务”条款规定,各缔约方须保证其境内的服务提供者信息转移的需求。由于金融、电信领域的敏感性,传统经贸协定均给予了缔约方较大的规制权。RCEP做出的数据跨境自由流动的原则性规定,体现出RCEP成员国积极推动区域范围内更加开放的态度。

(二)数据跨境流动规则的例外条款

RCEP数据跨境流动规则采取的是“原则+例外”的模式,即在明确数据跨境自由流动原则的同时,也为各缔约方出于特殊目的采取限制性措施设置了例外条款。RCEP第12章第14条第3款第1项和第12章第15条第3款第1项均明确了各缔约方可以出于实现其合法公共政策目标采取必要的措施。这一例外条款同样也被规定于CPTPP、DEPA之中。其主要功能是在数据跨境自由流动与各国维护公共利益之间寻求平衡。公共政策目标例外在条文中规定了较为明确的适用标准,即采取的措施应当满足不构成歧视和变相贸易限制的要求。与CPTPP和DEPA不同的是,RCEP在第12章第14条第3款第2项、第12章第15条第3款第2项进一步引入了基本安全例外。CPTPP、DEPA的数据跨境流动规则没有做此规定,而是在例外章节中引入了GATT第21条的安全例外规定。RCEP基本安全例外与公共政策目标例外不同,其目的是保证各缔约国维护其基本安全利益的需求,两者适用范围存在差异。由于RCEP基本安全例外的条文规定相对简单,既没有明确“基本安全利益”的范围,又没有罗列具体的适用情形,适用标准相对模糊。

RCEP在第17章第13条同样引入了GATT第21条的安全例外，相较于数据跨境流动规则中所规定的基本安全例外，其适用标准更为明确，也意味着该条款的限制性条件更多，缔约方援引第17章第13条的可能性较低。但该条款可能成为专家组解释数据跨境流动规则中基本安全例外的标准之一。此外，RCEP在数据跨境流动基本安全例外中强调其他缔约方不得对限制措施提出异议，进一步扩大了缔约方的自由裁量权。

二、RCEP数据跨境流动基本安全例外条款的解析

RCEP第12章第14条第3款和第12章第15条第3款明确规定各缔约方可以出于保护其基本安全利益采取措施，并且其他缔约方不能对此类措施提出异议。其中有三个关键性术语值得关注。其一是“基本安全利益”的范围；其二是“缔约方认为”的自裁决属性；其三是“其他缔约方不得对此类措施提出异议”的含义和适用该例外条款的影响。

(一)“基本安全利益”的范围

基本安全利益与一般安全利益最大的区别在于其涉及国家的关键职能，主要体现在国家内部确立法治或公共秩序，并采取某些措施以保护其领土或人民免受外来侵害。其中“基本”一词在文义上是指“绝对不可缺少的或必需的”。从GATT的历史谈判文献中也可以看到，大部分的成员方代表对于“基本安全利益”的理解均持保守态度[2]，主要是对其滥用后难以保证非歧视原则和贸易自由化的担忧[3]。所以，虽然各缔约方被赋予对“基本安全利益”的定义权，却也受到“善意原则”的限制[4]。从WTO实践案例来看，“基本安全利益”主要是以传统安全观为出发点，以维护国家政权、社会秩序稳定为重心。此“安全观”不同于美国式的将所有可能影响其霸权地位的事由均认定为对国家安全的威胁。当然，也不同于过于保守的数据防御主义，将任何数据的出境都视为对国家安全的威胁[5]。在乌克兰诉俄罗斯运输限制措施案(以下简称“俄罗斯过境运输措施案”)中，WTO专家组认为基本安全利益仅限于与国家根本性功能有关的权益。成员方虽然对于“国家根本性功能有关的权益”有着自裁权，但必须是真诚善意的，专家组也将通过“合理性测试”来判断措施与相关利益之间的关联。

RCEP第12章第14条第3款和第12章第15条第3款规定缔约方可以根据其认为的基本安全利益而采取任何措施。条文中并没有对“基本安全利益”进行明确的范围划定。但在RCEP第17章一般条款和例外的第13条“安全例外”条款中规定，缔约方可以在几种情况下采取措施：一是缔约方可以拒绝披露违背其基本安全利益的信息；二是保护四类“基本安全利益”而采取的行动；三是可以根据维护国际和平与安全的义务采取行动。而这一系列规定中，第二款和第三款均进一步明确了“基本安全利益”的范围，其中包括与裂变和聚变物质有关的、与武器弹药和作战物资有关的、保护关键公共基础设施的以及在国家紧急状态或战时采取的行动。CPTPP、DEPA均未在电子商务章节中进行专门的“安全例外”规定，而是在条约的例外章节对“安全例外”进行了规定。CPTPP第29章第2条、DEPA第15章第2条规定相对一致，都引用了GATT第21条安全例外的形式，但进行了修改，取消了GATT第21条(b)款对基本安全利益三种情形的列举，使得从文本上来看，CPTPP和DEPA的基本安全利益的范围更为广泛。从整个条约来看，RCEP虽然在电子商务章节所规定的基本安全例外条款没有对基本安全利益的范围进行任何限制，但在最后的安全例外条款中做出了相较于GATT更为明确的规定，将基本安全利益的范围做了进一步的限制。而CPTPP和DEPA虽然在电子商务章节中没有作出基本安全例外的规定，但其最后章节的安全例外规定却给予了“基本安全利益”更大的解释范围。所以，在

实践中，RCEP基本安全利益例外的适用可能更为严格，并且还需要通过“合理性测试”才可以得以适用。

(二)“缔约方认为”的自裁决属性

“缔约方认为”的表述方式也出现在GATT、GATS的安全例外条款之中。部分国家表示“缔约方认为”的条文规定，赋予了成员方自决权和对条款解释的开放性[6]，是条款具有的自由裁量和弹性的体现。但部分国家在此基础上更为激进，认为该条款意味着出于维护基本安全利益目的而采取的措施不受WTO争端解决机构的管辖[7]。俄罗斯过境运输措施案中，俄罗斯认为专家组应当对成员出于维护基本安全利益而采取的措施予以承认，并不再进行评估。但最后专家组驳回了俄罗斯的观点，并对GATT第21条(b)中的“其认为”进行了明确，表示该形容词条款并不能覆盖成员方作出的所有决定，并且GATT第21条(b)第1-3项通过列举的方式明确了条款的适用情形，也从侧面证明了“基本安全利益”是有其自在范围的，成员方不能任意地适用。所以，成员方应当首先证明其所主张的“基本安全利益”符合第21条(b)中的规定，才可以进一步证明措施的合法性。

俄罗斯过境运输措施案专家组报告实际上对“自决权”明确了两点：其一，争端解决机构是有权管辖一成员方援引安全例外采取措施所引发的争议。其二，争端解决机构将要求缔约方证明其主张的“基本安全利益”符合第21条(b)款1-3项中的规定，进而证明其所采取的措施属于第21条(b)的范围。虽然RCEP数据跨境流动基本安全例外中并没有通过列举的方式明确具体的适用情形，但在RCEP17章13条中，“其认为”的措辞出现在第一款和第二款的条文中，并且第三款“出于维护国际和平与安全义务而采取的任何行动”并没有“缔约方认为”这一前提。所以，可以认为即使通过“缔约方认为”的自裁决方式进行适用RCEP基本安全利益例外也应当满足RCEP17章13条前两款的所规定的情形。值得注意的是，CPTPP和DEPA在其安全例外条款中删除了GATT第21条(b)款中所明确的适用情形，并规定了拒绝披露信息、维护国际和平以及自身基本安全利益的三种情形。与RCEP不同的是，CPTPP和DEPA将包括维护国际和平与安全义务而采取必需措施的例外情形在内的三种情形均增加了“其认为”的前缀，且没有针对“基本安全利益”的范围做出进一步明确。所以，CPTPP和DEPA虽没有在电子商务章节做出专门的安全例外规定，但在安全例外章节却做出了更为宽泛的安全例外规定。实践中，RCEP安全例外规定中的“缔约方认为”这一自裁决条款所受的限制可能更为严格。

(三)“其他缔约方不得异议”的含义

RCEP数据跨境流动基本安全例外条款的最后，还附加了“其他缔约方不得对此类措施提出异议”的规定，扩大了缔约方的自由裁量权。部分学者认为，这一规定意味着其他缔约方不得对此类措施提起争端解决之诉，也即否定了争端解决机构的管辖权。但从上文对RCEP数据跨境流动基本安全例外条款赋予缔约方“自裁决”属性的分析来看，争端解决机构对于一缔约方援引安全例外而采取相关措施是具有管辖权的，而审查的重点是对援引例外的缔约方所主张的“基本安全利益”是否符合例外条款规定进行判断。而依据RCEP中规定的“其他缔约方不得对此类措施提出异议”，仅是赋予缔约方援引基本安全例外采取何种形式的措施的自由裁量权。所以，该条款也没有否定援引基本安全例外的“可诉性”，相对方依然可就采取措施一方所依据的“基本安全利益”不符合安全例外规定提起诉讼，只是相对方不得以措施的形式或程度为由提起诉讼。

根据前述条文来看，“缔约方认为”这一表述，实质上修饰了两个关键术语，一个是“基本安全利益”，另一个是“必需的任何措施”。在WTO实践中已经明确了争端解决机构对此类问题具有管辖

权,“缔约方认为”这一表述的“自裁决”属性因RCEP对“其他缔约方不得对此类措施提出异议”的强调,似乎明确了RCEP赋予缔约方自由裁量权的范围框定在其所采取的措施形式与程度上。而采取措施一方仍需要证明其援引该例外所主张的“基本安全利益”符合安全例外的规定以及采取措施与其主张利益的关联性。

三、RCEP数据跨境流动基本安全例外条款的适用

RCEP数据跨境流动基本安全例外的条文内容相对简单,赋予了缔约方“自裁权”,且未像公共政策目标例外一样要求采取的措施应当满足不构成歧视和变相贸易限制。但通过对条文解析可以看到,缔约国虽拥有“自裁权”,但并不影响专家组的管辖权,且审议的重点为对“基本安全利益”的判断以及采取措施与其主张利益的关联性。RCEP第19章第4条第2款规定,对于纳入了WTO协定的条款,专家组应当考虑WTO专家组及上诉机构作出的相关解释。所以,通过参考和借鉴WTO已有实践是对数据跨境流动基本安全例外条款适用进行分析的一条可行且重要的路径。

(一)WTO安全例外条款适用实践

基本安全例外对应到WTO规则中,主要包括GATT第21条、GATS第14条之二以及《与贸易有关的知识产权协定》(以下简称“TRIPS”)第73条等。其中GATT第21条是安全例外条款的立法渊源[8]。其明确了成员方在三种情况下可以实施背离条约规定的措施。其中包括:(a)披露相关信息会违背缔约国的基本安全利益;(b)缔约国采取其认为对保护其基本安全利益所必需的任何行动,并额外明确了此种情况下的三种适用情形;(c)缔约国出于维护国际和平与安全义务所采取的行动。由于兼具贸易与政治属性,各国存在争端解决机构对国家基本安全作出司法干预的担忧,也这是少有成员方就该例外提起争端诉讼的主要原因[9]。直至晚近WTO才于“俄罗斯过境运输措施案”和“沙特知识产权案”中对该条款作出较为明确的法律解释。“沙特知识产权案”涉及与贸易有关的知识产权,该案专家组遵循了“俄罗斯过境运输措施案”对GATT第21条的解释判理[10]。

俄罗斯过境运输措施案中,专家组认为安全例外的管辖权、基本安全利益的判定以及措施的必要限度为其中的重点。对于安全例外管辖权问题,由于《关于争端解决规则与程序的谅解》中没有规定涉及GATT第21条的特殊或附加程序,安全例外条款文本中赋予的“自由裁量权”并不影响专家组对于该案的管辖权[11]。对于基本安全利益的判定问题,专家组首先明确了每个成员都有对基本安全利益的定义权,且该内涵将随着特定环境和国家的变化而变化。客观上说,“基本安全利益”相较于“安全利益”的范围更小。这就意味着成员不能将其所关切的任何利益上升为“基本安全利益”,需要对成员所定义的“基本安全利益”进行一定标准的评估。该案中,专家组认为应当对成员所主张的“基本安全利益”根据《维也纳条约法公约》以下简称(以下简称“VCLT”)解释规则中的善意原则进行评估,也即成员方有责任阐明“基本安全利益”是源于国际关系中的紧急情况[11]。沙特知识产权案专家组表示,善意原则适用于确定“基本安全利益”范围的同时,也同样适用于措施行为与“基本安全利益”之间的关系。成员方应当遵循善意原则而采取相关的措施,同时成员方还需要善意地解读其所认为的基本安全利益,并证明其所采取的措施具有维护国家安全利益的充分性与紧急性[4]。不能以保护国家安全为名,却行贸易保护之实,从而违反其所承担的条约义务。

(二)RCEP基本安全例外适用限制

RCEP数据跨境流动规则虽引入了基本安全例外条款,但其具体规定与GATT第21条安全例外条款存在差异。首先,RCEP基本安全例外条款规定了GATT第21条安全例外条款中的(b)项的内容,但取消了(b)项后面的三种明确的适用情形,从

而使其适用范围更加宽泛[12]。此外，该例外条款中还进一步规定了其他缔约方不得对实施的措施提出异议。前文提到，该规定意味着措施相对方不能以采取行为一方所实施措施的方式和程度为诉讼请求。所以，基本安全利益的判定和措施必要限度是条款适用的关键。缔约国若援引RECP基本安全例外条款，需证明其主张的“基本安全利益”符合条文规定，以及其采取的措施与基本安全利益本身存在相应的联系。

1.主张的“基本安全利益”符合条文规定

俄罗斯过境运输措施案中，专家组基于善意原则对俄罗斯采取的措施进行评估后明确，限制商品入境的措施与俄罗斯和乌克兰边境安全问题有着直接关联，符合GATT第21条(b)款(iii)项“在战时或国际关系中的其他紧急情况下采取的行动”的规定。所以，即便是根据“善意原则”对成员方主张的“基本安全利益”进行判断，其标准仍然是条文中所明确的适用情形。根据专家组报告的内容，虽然GATT第21条明确赋予了成员方对根据基本安全利益和采取措施的必要性拥有“一定自由度”，但援引安全例外仍然受限于(b)款所明确的三种情形。并且，对于(b)款三种情形是否存在，成员方应当负有证明义务，而非自行判断的权利，否则成员很可能依其单方意愿采取措施，从而破坏WTO规则体系的整体稳定性与可预期性。

RCEP数据跨境流动基本安全例外条款取消了GATT第21条(b)款后面三项具体的适用情形，这也使得判断缔约方主张的“基本安全利益”是否符合例外条款规定缺乏标准。虽然RCEP取消了具体适用的情形意味着适用范围的扩大，但并不能理解为没有任何的限制。VCLT解释规则中明确，根据上下文进行解释的方法亦是可行的。所以，在判断缔约方所主张的“基本安全利益”是否符合要求，还可以寻求RCEP第17章一般条款和例外中的规定。该章的安全例外条款第2款规定了4项具体适用情形，其中包括了缔约方可以出于保护通信、电力或水利基础设施等关键公共设施采取相关措施。在RCEP数据跨境流动基本安全例外条款缺乏适用情形判断标准时，缔约方同样可以通过证明其主张的“基本安全利益”符合上述4项适用情形来援引该例外条款。

2.限制措施与基本安全利益之间的联系

根据WTO的实践来看，采取的措施与其主张的基本安全利益存在必要联系，是成员方能够成功援引例外条款的另一要素。俄罗斯过境运输措施案专家组表示，善意原则同样适用于判断措施与基本安全利益之间的联系，成员方需证明其采取的措施“并非全然无法服务于此目标”，也即证明其措施等是“最小合理性”的判断标准[13]。所以，即使缔约方采取的某项措施存在对贸易的限制性影响，但只要证明该措施与基本安全利益之间存在最小合理性的联系，该措施即具有合法性。而在一般例外条款在适用过程中，需进行更为严格的“必要性”测试[14]。在韩国牛肉案中，上诉机构提出“权衡与平衡”的评估方法①，进而判断相关措施的必要性以及与基本安全利益之间的关联度。在中国出版物案中，专家组表示如果起诉方提出存在更小程度上的限制措施，便可以认为争议措施不是“必须的”[15]，但被诉一方(援引例外条款的一方)可以通过证明即便存在替代措施的情况下争议措施仍是“必须的”的原因，从而援引例外条款。根据这一标准来看，援引基本安全利益例外所需满足的“最低限度标准”应当相较于一般例外的“必要性”测试更为宽松，且成员方无须证明措施的形式和程度的合理性，仅需证明相关措施与其主张的基本安全利益具有“表面合理性”即可，并且采取的措施不会因为存在其他可选的措施而失去合法性。

四、我国适用基本安全例外条款问题与立法完善

随着数字经济的不断发展，我国也愈加重视数字相关的立法工作。数据无国界的特性意味着

只有国内监管规则与国际立法具有高度的衔接性，才可以实现保障数据安全与促进数字经济发展的平衡。当前我国部分数据跨境流动监管措施与RCEP数据跨境自由流动的原则性规定不符，存在援引基本安全例外的需求。应当在梳理中国数据跨境流动监管立法的基础上，就我国适用基本安全例外条款的问题进行立法完善。

(一)我国数据跨境流动监管的立法

我国数据跨境流动监管立法已初成体系。2017年6月实施的《网络安全法》针对关键信息基础设施运营者所产生收集的重要数据与个人数据明确要求本地存储，确需出境的应当进行安全评估。2021年9月实施的《数据安全法》，在《网络安全法》的基础上进一步细化了数据跨境流动的监管规则，该法第31条重申了关键信息基础设施运营者在境内收集和产生的重要数据的管理办法，并明确了其他领域数据由国家网信部门会同国务院有关部门监管。2021年11月实施的《个人信息保护法》第38条明确，个人信息数据的出境可以通过安全评估、专业机构认证以及标准合同等方式进行。该法第40条要求达到国家网信部门规定数量的个人信息与关键信息基础设施生成的数据一样本地存储，确需出境的由网信部门组织进行安全评估。此外，2022年9月实施的《数据出境安全评估办法》进一步明确了我国数据出境安全评估的具体内容，提高了规则的可操作性与透明度。其中明确规定了四种情形需要进行安全评估，包括重要数据[②]、关键信息基础设施运营者或达到100万人以上个人信息的处理者向境外提供的数据、自前一年起向境外累计提供超10万个人信息或1万敏感个人信息的处理者向境外提供的数据以及其他网信部门认为需要进行安全评估的情形。根据监管规则的不同形式来看，可以将我国监管立法中的数据类别分为三类，如表1所示。

(二)我国适用基本安全例外条款的问题

关键信息基础设施生成的数据和达到规定数量的个人信息要求数据存储在境内，一定程度上将会对国际贸易造成限制性影响，存在援引基本安全例外条款的需求。其他领域重要数据需要根据具体的法律法规分析是否存在引发争端的可能。对于一般的个人信息，我国法律明确规定了多种数据跨境流动方式，在保障此类数据安全和促进数字经济发展中实现了较好平衡。所以，我国在适用该例外条款时应当着重关注前两类数据是否符合RCEP的相关规定。

1.关键信息基础设施生成的数据

关键信息基础设施的上位概念“关键基础设施”的重要性在国际范围内已形成共识，美欧国家在其外资并购国家安全审查中均将涉及关键基础设施的并购直接纳入国家安全考量的范围。我国对于关键信息基础设施的定义本身已经明确包含了基本安全利益因素。2021年9月实施的《关键信息基础设施安全保护条例》中对“关键信息基础设施”作出的定义[③]，与RCEP第17章第13条第2款第3项中所包括通信、电力和水利基础设施在内的关键公共基础设施相符性较高，理论上就关

表1　　我国数据跨境流动监管立法中的数据类别、监管规则及法律依据

数据类别	监管规则	法律依据
关键信息基础设施运营者在境内收集和产生的数据；达到国家网信部门规定数量的个人信息	本地存储，出境评估	《网络安全法》第37条 《数据安全法》第31条 《个人信息保护法》第40条
其他数据处理者在中国境内收集和产生的重要数据	国家网信部门会同国务院有关部门制定	《数据安全法》第31条
非上述情形的个人信息	安全评估、专业机构认证或标准合同条款	《个人信息保护法》第38条

键信息基础设施生成的数据采取相关措施的争议不大。

2.达到国家网信部门规定数量的个人信息

“达到规定数量的个人信息”与“关键信息基础设施生成的数据”一样,均要求数据本地存储。由于RCEP第17章第13条第2款中列明的4种适用情形并没有直接涉及个人信息,故难以通过该条款证明这一类别的数据与“基本安全利益”的相符性。而“达到规定数量的个人信息”也即具有大数据特征的个人信息,比如“大型平台”涉及庞大的个人信息便存在“系统性的风险”[16],对其规定特殊的监管办法,立法目的已从人权保护转化为维护国家安全。从这一角度来说,RCEP第17章第13条第1款“缔约方可以拒绝披露违背其基本安全利益的任何信息”或许可以为采取措施维护具有国家安全属性的大数据提供依据。但这一条款也并不能完全为“达到规定数量的个人信息”提供合法性依据,《个人信息保护法》通过国内法的方式将“一般的个人信息”与“达到规定数量的个人信息”进行区分,实则是将保障个人隐私的公共利益上升为基本安全利益,其中虽有维护国家安全的目的存在,但并不能完全证明所有达到规定数量的个人信息均对国家安全造成威胁。暂且不论“规定的数量”是否可能引发争议,不同行业所产生的个人信息达到“规定数量”后均上升为基本安全利益可能成为争议焦点。故需要对不同行业领域进行细化分类分级,形成数据分级分类监管办法,才可以更好符合“基本安全利益”的标准。

3.其他领域的重要数据

其他领域重要数据的监管规则与上述两种类别的数据不同,根据《数据安全法》第31条的规定,此类数据由国家网信部门会同国务院有关部门制定监管规则。其他领域的重要数据是除却关键信息基础设施生成的数据,并且其如果受到侵害也会对我国重大利益产生影响的数据,其范围可能会与“达到规定数量的个人信息”存在重合。实践中,“其他领域”多见于行政法规和部门规章之中,所涉范围广泛。如金融信息④、医疗信息⑤、地图数据信息⑥等具有特殊性质的数据,以及如“车联网”背景下超过10万人的个人信息、人脸信息⑦或赴国外上市的运营者掌握超过100万用户信息⑧等具有大数据特征的重要数据[17]。证明此类重要数据与“基本安全利益”的相符性并不困难,但由于《数据安全法》中并没有明确“其他领域”的具体范围,在实践中只能针对不同行政法规和行业规定进行具体分析,故应当在具体领域的立法过程中仔细比对“基本安全利益”的判断标准。

4.监管措施与“基本安全利益”的关联性

我国要求“关键基础信息设施产生的数据”以及“达到规定数量的个人信息”本地存储。数据本地化的监管措施在2013年“棱镜门”事件爆发之后,在世界各国得到普遍实施,以抵御他国监控和维护国家安全。数据本地存储的监管措施在保护数据安全、国家基本安全利益方面的作用得到绝大部分国家的接受。数据本地化措施即使存在对国际贸易的限制性影响,也并不影响其与维护重要数据安全之间的关联性。出境评估也是我国针对维护基本安全利益的监管措施,2022年9月施行的《数据出境安全评估办法》澄清了我国数据出境安全评估的具体事项⑨,可以有效证明出境评估措施与维护基本安全利益之间的关联性。其他领域重要数据的监管规则主要散见于各行政法规与部门规章,主要的监管措施同为本地存储、出境评估或仅需安全评估,故可参照上述的分析。

(三)我国数据跨境流动规则的立法完善

我国在积极推动RCEP实施的同时,也在申请加入拥有更高水平数据跨境流动规则的CPTPP和DEPA,因此,应重视例外条款的合理应用,表明中国在数字经贸规则领域的立场。鉴于目前我国数据立法与RCEP相关规则仍存在不尽协调的问题,应在充分运用例外条款的同时,完善国内立

法，统筹安全与发展，坚持数据跨境流动的自由化原则。

第一，强调数据跨境自由流动原则。无论是RCEP还是其他大型区域经贸协定中的数据跨境流动规则，均以数据跨境自由流动作为原则性规定，也是其促进贸易自由化宗旨的体现。当前我国数据跨境流动监管规则强调数据的“安全流动”[18](P201)，针对关键信息基础设施产生的数据、其他领域重要数据以及达到国家网信部门规定数量的个人信息采取“本地存储、出境评估”的监管措施，且立法文件中没有明确数据跨境自由流动的原则。这不仅影响我国推动RCEP的实施，还会影响我国申请加入更高水平的区域自由贸易协定。因此，有必要在数据立法中强调数据跨境自由流动原则，表明我国推动数字贸易发展的积极态度，这也是我国合理应用例外条款的前提条件。

第二，统一立法文件中相关概念的界定。RCEP例外条款中“缔约方认为”的规定虽给予了各缔约方对于“基本安全利益”内涵的自由裁量权，但专家组在审理贸易争端的过程中，仍然会根据“善意原则”对采取措施一方所主张的“基本安全”进行审查，而采取措施一方国内立法文件中的表述是否符合条约规定将成为考察的关键之一。当前，我国数据立法文件中对于“基本安全利益”主要采取了“国计民生”“国家安全”等措辞，与RCEP数据跨境流动规则例外条款中采取的“基本安全利益”的表述存在一定差异，并且各立法文件中的表述亦有不同。所以，有必要针对我国数据跨境流动监管立法中有关“基本安全利益”或相近含义的措辞进行统一，做出明确的界定。

第三，健全数据分级分类监管规则。适用RCEP数据跨境流动例外条款需证明主张的“基本安全利益”与条约所规定的适用情形相符。我国目前没有明确的数据分级分类监管规则，这一方面不利于我国在适用例外条款时证明主张利益符合条约规定，另一方面也导致国内企业难以根据现有立法判断其掌握的数据是否需要本地存储或出境安全评估。2022年9月实施的《数据出境安全评估办法》明确了数据出境安全评估的具体内容，提高了规则的可操作性与透明度，有利于证明安全评估措施与措施所要维护的目的之间的合理关联。但评估办法中仍未对重要数据、关键信息基础设施生成的数据做进一步细化分类，导致我国需要证明主张的“公共政策目标”或“基本安全利益”符合RCEP条文规定的困难依然存在。所以，健全数据分类分级监管规则应是我国数据立法下一阶段的重点。应从我国数据主权、国家安全和发展利益出发，在现有数据立法的基础上，根据不同数据在各行业、领域的重要性进行分级分类，形成“重要数据目录”，并针对不同级别和类别的数据适配不同的安全保护规则以及出境监管办法，从而澄清我国对“基本安全利益”的界定，为适用例外条款提供明确的国内法依据。

注释：

①上诉机构指出在进行措施评估时至少有三个因素需要考虑：涉案措施对实现目标贡献度；所追求目标的重要性；涉案措施对国际贸易的限制性影响。

②《数据出境安全评估办法》中明确“重要数据”是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

③《关键信息基础设施安全保护条例》第2务规定，本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以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、公共利益的重要网络设施、信息系统等。

④国务院发布的《关于银行业金融机构做好个人金融信息保护工作的通知》第6条：在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

⑤国务院科学技术部发布的《人类遗传资源采集、收集、买卖、出口、出境审批行政许可服务指南》第2.2条：人类遗传资源出境需获得审批，如对我国国家安全、国家利益或公共安全存在可能的危害性则不予批准。

⑥根据《中华人民共和国测绘法》制定的《地图管理条例》第34条：互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并制定互联网地图数据安全管理制度和保障措施。

⑦《汽车数据安全管理若干规定(试行)》第3条：涉及个人信息主题超过10万人的个人信息为重要数据；第11条：重要数据应当依法在境内存储，因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估。

⑧《网络安全审查办法》第7条：掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

⑨《数据出境安全评估办法》第8条：数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：(一)数据出境的目的、范围、方式等的合法性、正当性、必要性；(二)境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；(三)出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；(四)数据安全和个人信息权益是否能够得到充分有效保障；(五)数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；(六)遵守中国法律、行政法规、部门规章情况；(七)国家网信部门认为需要评估的其他事项。

参考文献：

[1]马光.FTA数据跨境流动规制的三种例外选择适用[J].政法论坛，2021，(5).

[2]United Nations. Report of the Drafting Committe of the Preparatory Committee of the United nations Conference on Trade and Employment[R]. New York: UN, 1947.

[3]彭德雷，周围欢，杨国华.国际贸易中的“国家安全”审视——基于美国“232调查”的考察[J].国际经贸探索，2018，(5).

[4]World Trade Organization. Suadi Arabia- Measure concerning the Protection of Intellectual Property Rights- Report of the Panel[R]. Geneva: WTO, 2020.

[5]刘金河，崔保国.数据本地化和数据防御主义的合理性与趋势[J].国际展望，2020，(6).

[6]Ji Yeong Yoo, Dukgeun Ahn. Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security[J]. Journal of International Economic Law, 2019, (2).

[7]李巍.新的安全形势下WTO安全例外条款的适用问题[J].中国政法大学学报，2015，(3).

[8]张丽娟，郭若楠.国际贸易规则中的“国家安全例外”条款探析[J].国际论坛，2020，(3).

[9]黄志瑾.论国家安全审查措施在WTO中的可诉性[J].河北法学，2013，(12).

[10]何华.知识产权保护的安全例外研究由《TRIPs协定》第73条展开[J].中外法学，2019，(3).

[11]World Trade Organization. Russia- Measures Concerning Traffic in Transit[R], Geneva: WTO, 2019.

[12]谭观福.数字贸易规制的免责例外[J].河北法学，2021，(6).

[13]张晓君，屈晓濛.RCEP数据跨境流动例外条款与中国因应[J].政法论丛，2022，(3).

[14]张乃根.国际经贸条约的安全例外条款及其解释问题[J].法治研究，2021，(1).

[15]Panel Repor, China-Publications and Audiovisual Products, para. 7.

[16]姚志伟.大型平台的个人信息“守门人”义务[J].法律科学(西北政法大学学报)，2023，(2).

[17]吴汉东.数据财产赋权的立法选择[J].北京：法律科学(西北政法大学学报)，2023，(4).

[18]马长山.数字法治概论[M].北京：法律出版社，2022.