

【专题:跨境数据与国家安全】

FTA 数据跨境流动规制的三种例外选择适用

马 光

【摘 要】如同世界贸易组织协定,大多数自由贸易协定都设有安全例外条款,这些条款与一般例外条款及电子商务或数字贸易章节中的数据跨境流动限制条款一道形成了对数据跨境流动的限制依据。特别是国家安全例外规定,对数据的跨境流动有可能形成较大限制。国家安全例外中的“信息”,若包括个人信息,则有可能对数据跨境流动产生较大影响。此外,在电子商务或数字贸易章节中本身就有例外条款的前提下,再有一般例外和安全例外的选择适用,就会对数据跨境流动产生更大限制效果。

【关键词】自由贸易协定;一般例外;国家安全例外;个人信息;数据跨境流动

【作者简介】马光,法学博士,浙江大学光华法学院副教授。

【原文出处】《政法论坛》(京),2021.5.14~24

【基金项目】本文系国家社科基金重大专项“建立健全我国网络综合治理体系研究”(项目编号:20ZDA062)、浙江大学人工智能与法学专项课题“促进数字贸易国际规则研究”(项目编号:18ZDFX010)的阶段性成果。

引言

通过自由的数据跨境流动,利用大数据分析,一国可能对他国的社会状况进行精准画像,并有针对性地开展情报收集和研判等工作,威胁他国国家安全^{[1](P.93)},因而各国都或多或少地对数据跨境流动予以限制,2021年8月20日,第十三届全国人民代表大会常务委员会第三十次会议通过的《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)也要求任何组织、个人都不得从事危害国家安全、公共利益的个人信息处理活动。随着《全面与进步跨太平洋伙伴关系协定》(Comprehensive and Progressive Agreement for Trans-Pacific Partnership,以下简称“CPTPP”)、《美墨加贸易协定》(United States-Mexico-Canada Agreement,以下简称“USMCA”)、《区域全面经济伙伴关系协定》(Regional Comprehensive Economic Partnership,以下简称“RCEP”)等超大型自由贸易协定(Free Trade Agreement,以下简称“FTA”)的缔结,各国对通过电子方式跨境传输信息(即数据跨

境流动)问题的关注度逐渐加强。而在 FTA 中允许数据跨境流动的原则和特定情况下对其进行限制方面似乎已经达成一致,尽管其对例外的范围方面具有很大差异。FTA 中,对数据跨境流动的限制往往都包括三个部分,即来自电子商务或数字贸易^①章节下的限制、一般例外条款下的限制以及安全例外条款下的限制。现有的研究往往聚焦于第一种类型的限制,而基于一般例外条款,诸多的世界贸易组织(World Trade Organization,以下简称“WTO”)案例表明其不好援引。基于国家安全例外对数据跨境流动施加限制以及因此而对数据跨境流动产生的重大影响则尚未引起充分关注,况且,目前国家安全的范围正处于扩张的趋势。^②

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、地区间更容易进行个人数据跨境转移,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](P.100)}。CPTPP 和 USMCA 总体上对数据跨境流动设限采取

了较为严格的标准,而且两者中尤以USMCA对数据跨境流动采取了更高的保护标准,RCEP总体上虽然也采取支持数据跨境流动的态度,但同时也对各缔约方政府赋予了采取限制的权利,而这种权利有时可以避开其他缔约方政府的挑战。在FTA中同时规定了三种类型的设限途径,这就使得缔约方可以通过选择适用安全例外、一般例外条款以及电子商务或数字贸易章节下的限制措施,从而降低数据跨境流动自由化成果。这一情况似乎是此类FTA缔约方不曾预想到的,而这些条款的并存和交叉适用将会让数据跨境流动产生诸多不确定性。

2019年和2020年,《美日数字贸易协定》(U.S.-Japan Digital Trade Agreement,以下简称“DTA”)、《新加坡新西兰智利数字经济合作协定》(Digital Economy Partnership Agreement,以下简称“DEPA”)、《新加坡澳大利亚数字经济协定》(Singapore Australia Digital Economy Agreement,以下简称“SADEA”)等三个专门对数字经济或数字贸易做出约定的条约相继缔结。而这些条约对三种例外的援引做出一些调整,尽管在适用方面,这些数字贸易或数字经济协定和相对应的FTA在适用顺序方面可能会存在争议。^③

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^{[3](P.158)},本文的研究将以后者为重心。2021年6月和8月,我国相继出台《数据保护法》和《个人信息保护法》,再加上《网络安全法》,对数据跨境流动相关的国内法框架已告完成,但《个人信息出境安全评估办法(征求意见稿)》尚处于草案阶段。《个人信息保护法》要求国家积极参与个人信息保护国际规则的制定,促进个人信息保护方面的国际交流与合作,推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

一、FTA数据跨境流动规制三种例外选择适用可能性和特定例外分析

(一)FTA数据跨境流动规制三种例外选择适用可能性

越来越多的FTA开始对数据跨境流动做出专门

规定,这些专门规定中不乏对数据跨境流动施加特定限制的约定(电子商务或数字贸易章节或条款下的限制)。此外,一般例外和安全例外条款作为FTA中的普遍适用条款,也适用于电子商务或数字贸易章节或条款。换言之,特定例外限制、一般例外和安全例外条款下的例外限制有可能形成多重限制。甚至,在部分FTA中除了既有的安全例外条款,也设有电子商务或数字贸易章节下基于基本安全利益采取措施的权力,或许立法者在立法过程中出于便利将WTO协定的条款套用到FTA中,但这在无意间形成了对数据跨境流动的多重限制。

(二)FTA数据跨境流动规制特定例外分析

以美韩FTA为开端,美国开始在自己缔结或主导的FTA中加上数据跨境流动相关条款,这些条款呈现出逐步加强数据跨境流动自由化的态势。特别是到了CPTPP和USMCA,数据跨境流动相关内容已经相对完整。之后的DTA以及DEPA、SADEA等数字贸易或数字经济协定也对数据跨境流动做出约定,这些条约要么将数字贸易从一般贸易分离出来单独立法,要么对数字经济整体做出约定,这些都能说明各国对数字贸易或数字经济的关注度在逐渐增强。我国缔结的FTA中,虽然也有中国-澳大利亚FTA、中国新加坡FTA、中韩FTA、中国毛里求斯FTA对电子商务相关内容做出规定,但直接对数据跨境流动做出规定的则只有RCEP。

最早对数据跨境流动自由作出明确规定的FTA当属CPTPP,而之后的USMCA则对其进行了强化。CPTPP规定各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,尽管该条款在其它条款的限制下并未赋予缔约方实质性的规制权,但因其数据跨境流动条款的第一款,所以似乎也可以理解为其以类似于总则的形式赋予缔约方权利。在USMCA、DTA中,美国则将该款予以删除,这明显是其对数据跨境流动规制的严格限制贯彻在这些条约中,即无论缔约方是出于国家公共安全还是各自的监管要求,都不能妨碍在FTA中所定义的“跨境数据

自由流动”。DEPA 和 SADEA 这两个由新加坡所主导的数字经济协定也与大多数 FTA 一样,首先认可了缔约方对数据跨境流动的规制权。

CPTPP、USMCA、DTA、DEPA^④和 SADEA 均规定,缔约方要保障信息的跨境流动。但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流动的限制措施,同时这种措施要符合:(1)不构成任意或不合理的歧视或变相的贸易限制;(2)对信息传输施加的限制不超过实现目标所需限度,^⑤实际上缔约方的例外措施要符合这些条件非常困难^{[4]P.74}。

与上述 FTA 相比,RCEP 则采取了不同的方式。与 CPTPP、DTA、DEPA 和 SADEA 等类似,RCEP 第 12.15 条首先认可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。在此前提下提出不得阻止为进行商业行为而通过电子方式跨境传输信息的大要求,进而列出例外,即缔约方可以采取其认为是实现合法的公共政策目标所必要的措施(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),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。与 CPTPP 等相比,RCEP 的特定例外存在两个特点,第一是增加了“其认为”的措辞,第二则是直接明确此类合法公共政策的必要性应当由实施措施的缔约方决定。除此之外,RCEP 还允许缔约方采取其认为对保护基本安全利益所必需的任何措施,而其他缔约方不得对此类措施提出异议,该条就是在特定例外条款中额外加入了安全例外。RCEP 的特征是在类似于 CPTPP 或 USMCA 的条款设计下,通过对合法公共政策的必要性由采取措施的缔约方决定以及赋予缔约方在基本安全利益下的绝对权利,丰富了缔约方动用该条实现合法公共政策目标和维护国家利益,并对数据跨境流动采取限制的可能性。从这一点来看,两者可以说具有非常大甚至是根本性的区别。特别是对合法公共政策必要性由实施措施的缔约方决定以及基于保护基本安全利益所必需的任何措施其他缔约方不得提出异议的规定赋予采取措施的缔约方决定

性的权利。这其实是给对数据跨境流动进行限制留了一个大口子。

二、FTA 数据跨境流动规制一般和安全例外分析

(一)一般例外和安全例外条款的缘起和发展

从国际规则层面来看,一般例外和安全例外条款始于《关税与贸易总协定》(General Agreement on Tariffs and Trade,以下简称“GATT”)第 20 条和第 21 条,类似规定也出现在《服务贸易总协定》(General Agreement on Trade in Services,以下简称“GATS”)第 14 条和第 14 条之一、《与贸易有关的知识产权协定》(Agreement on Trade-Related Aspects of Intellectual Property Rights,以下简称“TRIPS”)第 73 条和《与贸易有关的投资措施协定》第 3 条。虽然内容各不相同,但以 CPTPP、USMCA、RCEP 为代表的 FTA 也往往包含有一般例外条款,而且均直接将 GATT(1994)第 20 条和 GATS 第 14 条作为 FTA 条款的一部分,只不过在电子商务或数字贸易章节适用 GATT(1994)下的一般例外条款还是 GATS 下的一般例外条款有所不同,这起因于各国对电子商务或数字贸易属性的分歧。多数的 FTA 要么直接引用了 WTO 安全例外条款,要么对其进行部分修改。

(二)一般例外条款在 FTA 数据跨境流动限制中的适用

CPTPP 第 29.1.3 条和 USMCA 第 32.1.2 条规定,电子商务或数字贸易适用 GATS 第 14 条的一般例外,但同时也在注释中说明该款规定不影响电子产品是否应归为货物或服务。DEPA 第 15.1.3 条、SADEA 第 3.1 条和第 3.2 条、DTA 第 3 条、RCEP 第 12 条则规定 GATT(1994)第 20 条和 GATS 第 14 条一般例外的适用。这些条款表明,对于一般例外,上述 FTA 均直接将 GATT(1994)或(和)GATS 的一般例外纳入到 FTA 之中予以直接适用,当然相互之间也存在差异,就是 CPTPP 和 USMCA 规定适用 GATS 的一般例外条款,而其他则规定同时适用 GATT(1994)和 GATS 的一般例外,即便如此,前者也通过注释的方

式明确本款不影响电子产品是否应归为货物或服务。只不过,在GATS项下的一般例外情景明显少于GATT(1994)项下的一般例外,而且WTO争端实践表明,成员在GATT(1994)和GATS项下首选的例外情形大不相同。在GATT(1994)中最常被引用的是保护公共健康和环境的例外,而在GATS中最常被援引的是公共道德例外^{[5](P.105-106)}。另外,仅将电子产品明示出来,似乎在暗示着除电子产品之外的电子商务或数字贸易则归属于服务贸易。因此,这些条款对电子商务或数字贸易属性确定方面其实存在不小的区别。

(三)国家安全例外条款在FTA数据跨境流动限制中的适用

大多数FTA要么复制WTO安全例外条款要么对其进行部分修改。CPTPP、USMCA、DTA、DEPA、RCEP等条约均包含有此类安全例外条款。

CPTPP第29.2条、USMCA第32.2条、DTA第4条、DEPA第15.2条均规定:本协定中任何条款不得解释为:(a)要求一缔约方提供或允许获得其确定如披露则违背其基本安全利益的任何信息;或(b)阻止一缔约方采取其认为对履行维护或恢复国际和平或安全义务或保护其自身基本安全利益所必需的措施。SADEA虽然没有设置安全例外条款,但构成其核心部分的附件A替换了新加坡-澳大利亚FTA的电子商务章节,并将其名称改为“数字经济”,而新加坡-澳大利亚FTA第17.2条的安全例外规定与CPTPP等的规定内容没有区别。依据这些条款的规定,缔约方的自决权较WTO的安全例外有所扩张,因为GATT(1994)第21条(c)项中的“根据《联合国宪章》(以下简称《宪章》)采取的维持国际和平与安全的行动”在这些协定中变更为“其认为有必要为履行维持或恢复国际和平与安全之义务而采取的行动”,这为这些国家采取非《宪章》下的维持和平行动创造了可能^{[6](P.108)}。RCEP第17.13条也规定了安全例外,该条除了增加“为保护包括通讯、电力和水利基础设施在内的关键的公共基础设施而采取的行动”“在国家

紧急状态”之内容之外,与GATT(1994)第21条非常相似。当然,上述内容的增加,为缔约方采取措施提供了更多可能性。

因为在RCEP中,已经在电子商务章节对限制措施的例外适用做出了较为宽泛或适用条件较低的规定,因此,缔约方就数据跨境流动施加限制而援引第17.13条国家安全例外的可能性不大,而且,RCEP在电子商务章节中已经含有内容宽泛的安全例外条款。相反,因为CPTPP、USMCA、DTA、DEPA下对数据跨境流动限制措施伴随着诸多前提条件,所以,反而导致在FTA中为数据跨境流动限制援引国家安全例外条款的可能性增加。

从上述条款可以看到,诸多FTA安全例外条款所保护的是国家的基本安全利益,因此,对什么是基本安全利益进行界定就非常重要。WTO专家组在“俄罗斯-运输限制措施案”(DS512)中所作出的裁定内容应该可以提供一些帮助,其认为基本安全利益显然是比安全利益更狭隘的概念,通常可以理解为与国家基本职能相关的利益,即保护其领土和人民免受外部威胁,以及内部维护法律和公共秩序。^⑥也有学者主张基本安全利益的范围应紧密限制在军事安全、领土安全的范围内^{[7](P.99)}。FTA特定例外所保护的往往是合法的公共政策,因而,可以理解为公共政策和公共秩序在选取所采取措施时是有区别的,即公共政策针对的是非基本安全利益,而公共秩序则针对基本安全利益。

要正确把握FTA条款中的国家安全例外,离不开对WTO相关规则的理解,特别是该例外在WTO争端解决案例中的援引情况。国家安全例外同一般例外一起构成WTO例外体系的重要组成部分,或许WTO协定中没有任何条款比国家安全条款更具政治敏感性。^⑦在WTO成立前,尽管该条在争端解决案例中有被援引,但尚无就此通过的专家组报告,^⑧即使在WTO成立后也是仅有两个专家组报告。这与一般例外条款在诸多WTO争端解决案例中得以援引相差甚远。但在国家安全普遍被泛化的情况下,

在“俄罗斯-运输限制措施案”(DS512)中该例外曾得以援引。除此之外,“阿联酋-与货物、服务和与贸易有关知识产权措施案”(DS526)、“美国-对钢产品和铝产品措施案”(DS544、547、548、550、551、552、554、556、564)^⑩、“沙特阿拉伯-知识产权保护措施案”(DS567)、“卡塔尔-对从阿联酋进口货物措施案”(DS576)^⑪、“日本-有关向韩国出口产品和技术的措施案”(DS590)中,该例外也得以援引。^⑫“俄罗斯-运输限制措施案”(DS512)中被援引的安全例外是GATT(1994)第21条(b)项,其专家组裁定,WTO成员方总体上有权自行判断其“基本国家安全利益”以及相关措施是否是保护该利益“所必需的”,但行使该自判权应基于“善意原则”,专家组有权对其进行客观审查。这说明,专家组认为贸易自由化和多边主义精神与国家安全是相得益彰的。^⑬《沙特阿拉伯-知识产权保护措施案》中,被援引的是与GATT(1994)第21条(b)项内容完全相同的TRIPS第73条(b)项,该案中专家组的裁定与《俄罗斯-运输限制措施案》别无二致,而(c)项则很明确针对《宪章》下的制裁。笔者认为(a)项虽至今未得以援引,但就数据跨境流动而言,该条具有非常重要的地位,况且(a)项中还缺少类似(b)项的“必需性”要件。与上述FTA对(b)项和(c)项内容的不同程度引用相比,对(a)项内容则均采取全盘接受,即该项分别被CPTPP第29.2条的(a)项、USMCA第32.2条(a)项、DEPA第15.2条(a)项、DTA第4条(a)项、新加坡-澳大利亚FTA第17.2条(a)项和RCEP第17.13条(a)项原封不动地予以引用。各缔约方基于基本安全利益,可以对相关信息采取保护,这就意味着可以对相关数据的跨境流动予以限制,因为此类数据的跨境流动将会导致其被披露。而且,各缔约方对此可以自行判断,即“其认为”即可。虽然在货物贸易和服务贸易下此条款尚未被援引,使得各国对其认识不足,但随着数字贸易的进一步发展,此条是否有可能摇身一变成为限制数据跨境流动进而对数字贸易施加限制的杀手锏呢?

问题是,这里的信息是由缔约方政府直接掌握

的信息,还是泛指在其管辖权范围内存储的信息?^⑭通常,包含在贸易协定中的国家安全例外包含与个人数据直接相关的内容。因此,国家安全例外可能会针对限制数据跨境流动的其他措施,尤其是规范个人数据传输和存储设施位置的政府措施。可以说,援引这些国家安全例外的可能性是一个可以在现有数字贸易规范的讨论中带来重大变化的问题。这意味着当前的“原则-例外”框架缺乏对这一部分的考虑,存在固有的局限性,尤其是在对个人信息的海外转移保持保守或被动立场的国家将通过寻求国家安全例外来维持各种监管措施,其会认为贸易协定的国家安全例外中包括的与“信息”有关的规定也直接适用于“个人信息”。

三、FTA数据跨境流动规制三种例外选择适用问题解决方案

(一)FTA特定例外、一般例外和安全例外的适用顺序

在特定例外、一般例外和安全例外的适用顺序方面,可以首先尝试援引特定例外。如果特定例外的适用失败,则一般例外的适用也非常困难。不过,鉴于一般例外在贸易协定中的重要地位以及被援引的先例,许多国家还是会尝试援引该条。如在“韩国-对放射性核素的进口禁令和检测认证要求案”(DS495)和“澳大利亚-关于适用于烟草产品和包装的商标、地理标志和其他平装要求的某些措施案”(DS435、441、458、467)中,争端解决机构均认可了基于人的生命、健康保护而采取措施的正当性。一般例外保护包括公共政策、公共道德、生命和健康(在医疗个人信息的情况下)、环境(与消费环境侵权产品有关的个人信息)和自然资源(与有限资源消费有关的个人信息)保护所需采取的措施,因此其适用范围比特定例外和安全例外更加广泛。安全例外并没有“任意或不合理歧视或对国际贸易的变相限制”的禁止性规定,贸易限制措施的适用方式更为灵活,因此在适用方面也有优势^{[8](P.65)}。即对数据跨境流动采取限制的国家可能会先后援引特定例外、安全例外和

一般例外主张其措施的合法性,这种援引有可能是三种例外全部援引或援引其中的一部分。

(二) FTA 对三种例外条款进行的协调

数字贸易和个人信息的新时代需要在整个贸易协定中重新考虑和协调,而且在这方面,国家安全例外也需要被相应地予以纠正。这种平衡已朝着确保信息传输更多自由的方向发展,如在 USMCA 和 DTA 中删除了缔约方政府可以进行管制的原则声明,并已将援引特定例外的条件进行调整以适应一般例外。USMCA 和 DTA 中对禁止数据本地化并未设有类似 CPTPP 的特定例外,那么禁止数据本地化这一原则仅适用一般例外和安全例外,该条为通过海外服务器收集和使用个人信息提供了更加强有力的保护。想必 DTA 应该是考虑到了适用于整个协定的一般例外和国家安全例外,因此,在必要时可以通过证明与服务器位置有关的限制措施是合理的而免责。DTA 的这种新发展说明了一个基本问题,即关于数字贸易中已讨论的特定例外与一般和安全例外之间的关系存在选择适用的可能性。

(三) 警惕 FTA 国家安全例外适用的泛化

不仅是国际条约,各国的国内法对此也有类似的规定。例如,《通用数据保护条例》(General Data Protection Regulation,以下简称“GDPR”)序言规定, GDPR 不适用于国家安全事务,并且单独引入了国家安全例外条款。俄罗斯于 2015 年出台了《个人信息保护法》,原则上要求在俄罗斯境内存储个人信息,并限制向国外转移个人信息。在这里,国家安全考虑也起着重要作用。^⑩《美国 2019 年国家安全和个人数据保护法案》规定,基于国家安全考虑,重要信息(包括一些敏感的个人信息)不应存储在某些特定外国(中国、俄罗斯等)。韩国也认识到个人信息与国家安全之间的联系,2017 年制定的韩国《个人信息保护法》不适用于为国家安全而收集的个人信息以及为公共安全而临时处理的个人信息。

在国家安全方面,国家适用免责例外限制个人信息的跨境传输以及服务器的域外设置,实际上有

三种选择。一种是利用 FTA 中有关电子商务(数字贸易)一章中包含的特定例外,另一种是可以选择适用于整个 FTA 的一般性例外,最后一种方法是在国家安全例外情况中寻找解决方案,该例外作为替代方案也适用于整个 FTA。即使选择第一个或第二个例外,也有可能同时使用第三个例外作为补充。现在讨论的数字贸易不仅限于现有贸易的电子方法(传统意义上的电子商务),还指具有新形式和新内容的交易。在现有贸易协定的框架下定义和管理这些新交易存在根本的局限性。想必因为这些理由,才出现了 DTA 以及 DEPA、SADEA 等数字贸易或数字经济协定。

从个人信息和信息的关系来看,信息应是包括个人信息的概念。在 CPTPP、USMCA、RCEP 等大型 FTA 中都有国家安全例外条款,而这些条款或许可以成为缔约方对数据跨境流动采取限制的依据。更值得关注的是,这些规定给了缔约方对披露是否违背其基本安全利益的认定权,尽管在程度上各异,但至少关于披露将会引发基本安全利益受损这一项,上述条约几乎采取了相同的规定。

(四) 对数字贸易(经济)另行订立协定的可行性分析

将数字贸易从现有 FTA 中分离出来并缔结专门适用于数字贸易的协定也可以被视为解决结构性问题的一种方式。它认识到数字贸易的特征,为协定的应用准备一个新的框架,并通过它来规范数字贸易,DTA、SADEA、DEPA 等就是此方面作出的较好尝试,新加坡和韩国、英国间也已启动相关谈判。当然,即使在这种情况下,现有的相关贸易协定仍将适用于与数字贸易有关的一般贸易,因此如何协调应用这两个协定的问题仍然存在。如新加坡和澳大利亚、新西兰之间既有 FTA,又有数字经济协定,而美日两国间,也同时具有 FTA 和数字贸易协定。

SADEA 第 3 条(a)项将新加坡-澳大利亚 FTA 的电子商务章节予以修订,即替换为附件 A 的数字经济章节。新加坡与韩国和英国推动的数字经济协定

也极有可能采用这种做法。美日贸易协定第2条也规定了其与DTA之间的关系,即每一缔约方确认其在WTO协定和双方均加入的其他协定项下相对于另一缔约方的现有权利和义务,此条也意味着DTA的内容优先适用于美日贸易协定。与SADEA的替换不同,美日之间则采取了有顺序的重复适用。DEPA则因为是新加坡、新西兰、智利三国间的多边协定,而三国间又没有签订FTA,因此并无类似条款,仅在第1.2.2条规定:如果一缔约方认为DEPA的条款与其和至少一个其他缔约方作为缔约方的另一协定的条款不一致,应请求另一协定的相关缔约方协商以达成双方满意的协议。新加坡和新西兰之间签有FTA,因此,如果新加坡-新西兰FTA的电子商务章节以及与数字经济有关的条款与DEPA不一致的话,就会出现如何适用的争议。

四、我国的数据跨境流动规制实践及完善建议

(一)明确FTA数据跨境流动限制例外条款模式

我国需明确数据规制的目标^[9],欧美对数据跨境流动采取不同的模式,欧盟通过GDPR影响他国的立法,而美国则通过FTA推行其政策。鉴于我国既是数据大国也是对外投资大国,例外条款的构建可考虑以数据跨境自由流动为原则,以限制流动为例外^{[10][P.100]}。在此方面,RCEP中的例外条款模式还是提供了较好的模板,因为其较好地处理了在国家安全等核心方面继续保留较大范围限制的同时,又很好地贯彻了数据跨境流动总体自由的大方向。以后在与他国商定新的FTA或对既有FTA进行修订时,就数据跨境流动问题,可以考虑将RCEP的相关条款作为模板,在此基础上进行适当调整。

(二)关注FTA中三种例外对数据跨境流动的选择适用问题

当前,就FTA的结构而言,最紧迫的问题是澄清电子商务(数字贸易)一章中包含的特定例外与适用于整个FTA的例外之间的关系。现在,一般例外和国家安全例外适用于整个协定,因此它们当然也适用于电子商务(数字贸易)部分,允许在同一情况下存

在多个例外情况的做法将会造成混乱。特别是,如果没有像现在这样提及重复适用的可能性,并且没有关于以何种顺序和以何种方式适用这些例外的规定,最终,援引例外条款的国家和反对国之间将出现争议。

另外,在互联网领域,国家安全不存在统一认识。如在我国,数据(信息)安全亦与政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、生态安全、资源安全、核安全并列且相互交错,共同组成综合安全体系^{[11][P.31]}。俄罗斯在“俄罗斯运输限制措施案”中主张国家有权就采取的措施是为保护其基本安全利益所必要作出决定,而美国也在该案中披露了与俄罗斯相同的观点。对美国而言,GATT(1994)第21条(b)项的自我判断性质使争端“不可审理”,即认为专家组无权审查成员援引该条的权利。欧盟、中国、巴西、澳大利亚、日本和其他第三方则认为专家组有权审查此案,不同意对涉及国家安全的争议不可审理的观点。^⑤甚至,美国在针对我国抖音和微信采取限制措施时曾主张个人信息的海外流露会影响国家安全。即应该注意个人信息与国家的外交、安全、经济和社会领域中关键国家职能的执行有关。我国要警惕美国泛化基本安全利益的范畴,特别是试图将经济安全也纳入到基本安全利益,从而打压我国企业;也要考虑有关个人信息的泄露是否会导致基本安全利益受损的问题。对此,建议对个人信息应采取区分,即警惕将个人信息泄露直接与国家安全联系起来,也不要将两者完全剥离。或许在此方面,网络安全审查办公室于2021年7月2日和7月5日分别对滴滴出行和运满满、货车帮、BOSS直聘展开的网络安全审查可以提供思路。

除了RCEP外,我国缔结的FTA中对电子商务作出规定的主要有《中韩FTA》和《中澳FTA》,我国缔结的FTA主要还是以直接适用WTO协定的一般例外和安全例外为主。《中韩FTA》和《中澳FTA》均未对数据跨境流动做出规定,所以,在FTA中并不存在电子商务章节下的特定例外。当然,从另外一个角

度来看,就因为对数据跨境流动做出明确的规定,即没有就此承担相关条约下的义务,所以,也没有必要通过例外条款来对其进行限定。

从目前的情况来看,我国加入CPTPP可能会是一个漫长的过程,在加入中会遇到的一系列难点中也将包括数据跨境流动问题。从我国缔结的FTA文本不难发现,RCEP是对数据自由跨境流动做出最开放态度的协定,尽管如此,其还是受到很大限制,CPTPP和RCEP的相关条款具有很大区别。而恰好CPTPP中一般例外和国家安全例外条款的存在和适当运用将会对我国具有很大启发,或许通过这些条款的援引,可达到数据跨境流动自由和国家安全利益的最佳协调。特别是对基于基本安全利益所适用的不披露任何信息这一条款,我们可以主张,除非另有协议,否则同一协定中包含的相同词语原则上应解释为相同。如果是这样的话,同一FTA中包含的“信息”一词应在整个协定中得到相同的解释。目前似乎没有理由对FTA中出现在不同条款中的信息这一措辞进行不同解释。并且,“信息”的词典含义涵盖了包括子概念“个人信息”在内的广泛内容,这也从上述FTA安全例外条款使用了“任何信息”的措辞中得到证明。但与RCEP第12.17.3条规定任何缔约方不得就电子商务章项下产生的任何事项诉诸争端解决不同,CPTPP等FTA则未将电子商务排除在争端解决之外。这也将是我国加入CPTPP时要谨慎的问题,即电子商务方面适用FTA争端解决机制^{[12](P.180)},换言之,在CPTPP、USMCA等FTA下,对基于基本安全利益而采取的限制数据跨境流动措施将面临FTA争端解决机制的审查,且与WTO具有上诉机制不同,在FTA中的争端解决机制仅有专家组程序,较目前WTO上诉机构缺位相比较,裁定做出和生效将会更加迅速和有效。

(三)完善我国国内法对数据跨境流动的规定

我国国内法对数据跨境流动的规定主要包含在《网络安全法》《数据安全法》和《个人信息保护法》中。但是因为这些立法所制定的年份各不相同,里

面的具体条款也存在部分不够明确、相互不衔接等情况。

1. 数据跨境流动适用法律问题

就数据出境问题,《网络安全法》《数据安全法》与《个人信息保护法》之间的适用关系问题值得探讨。《数据安全法》第31条规定,关键信息基础设施的运营者在我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《网络安全法》的规定;其他数据处理者在我国境内运营中收集和产生的重要数据的出境安全管理办法,由国家网信部门会同国务院有关部门制定。因为《网络安全法》也规定由国家网信部门会同国务院有关部门制定关键信息基础设施的运营者在我国境内运营中收集和产生的重要数据的出境安全管理办法,因此,所有重要数据的出境安全管理办法是统一的还是割裂的也不明确,目前对重要数据出境能够适用的安全评估尚无章可循,也未见有相关立法草案。

至于个人信息出境,则应适用《个人信息保护法》,《个人信息保护法》第38条规定的能够向境外提供个人信息的情况,包括:通过国家网信部门的安全评估;经专业机构进行认证;用标准合同与境外接收方订立合同;法律、行政法规或者国家网信部门规定的其他条件。这些情况与GDPR第5章下欧盟对第三国或国际组织传输个人数据所需的基于认定具有充足保护的转移,符合转移所需要的适当安全保障,有约束力的公司规则等要求非常相似。除此之外,我国缔结或者参加的国际条约、协定对向我国境外提供个人信息的条件等有规定的,可以按照其规定执行。尽管对个人信息的出境列举了上述五种方法,但同时也要求个人信息处理者应当采取必要措施,保障境外接收方处理个人信息的活动达到《个人信息保护法》规定的个人信息保护标准,从而对这五种方法设置了限制。当然,至于个人信息处理者是否以及如何能保障境外接收方符合我国法定标准的问题值得进一步探讨。另外,《个人信息保护法》第39条还要求就个人信息出境向个人告知和取得个人

单独同意。

《个人信息出境安全评估办法(征求意见稿)》尚处于草案阶段,随着《个人信息保护法》的出台,该安全评估办法应以《个人信息保护法》为依据,而非《网络安全法》。换言之,在目前《网络安全法》《数据安全法》和《个人信息保护法》均已出台的情况下,这些法律和下位法之间的关系都要予以适当调整。

2. 适时出台相关细则

《网络安全法》《数据安全法》《个人信息保护法》规定,关键信息基础设施的运营者在我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。确需向境外提供的,应当进行安全评估。《个人信息保护法》还规定,国家机关、具有管理公共事务职能的组织为履行法定职责处理的个人信息应当在我国境内存储;确需向境外提供的,应当进行安全评估。而存储和提供并非相同概念,所以两者并非原则和例外的关系,境外存储是不被允许的,仅在确需并经过安全评估时,才能向境外提供,上述条款将数据本地化和数据跨境流动这两个不同的概念混为一谈,而往往在FTA中将这两个内容放在不同的两个条款,这种明确区分法值得我国的立法借鉴。出境之后的数据是否也构成境外存储,以及两者之间的关系也需要进一步明确。如果将个人信息转移到境外并对其进行处理,并符合以向境内自然人提供产品或者服务为目的或分析、评估境内自然人的行为,则应在我国境内设立专门机构或指定代表。目前,对关键信息基础设施、重要数据等的概念或范围并不明确^{[13][P.97]}。尽管《关键信息基础设施安全保护条例》第2条对关键信息基础设施做出定义,但该条涵盖的关键信息基础设施的范围是否过于宽泛有待进一步论证,而对于“严重危害国家安全、国计民生、公共利益”等相对模糊的部分有待进一步细化标准,否则就会导致企业无法遵从。虽然《数据安全法》第20条要求建立数据分类分级保护制度,确定重要数据目录,但因各部门和各地区都可设置重要数据目录,从而可能会导致重要数据目录体系较为复杂,这在

具体执行中会导致一定的困扰。如《汽车数据安全 管理若干规定(试行)》第3条对汽车重要数据作出规定,其它产业也有可能制定类似目录。而且何为数据分类分级保护制度,也需要进一步明确,因为重要数据目录的制定显然与此具有密切关联。《个人信息保护法》第40条规定,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,应当将在我国境内收集和产生的个人信息存储在境内。确需向境外提供的,应当通过国家网信部门组织的安全评估;法律、行政法规和国家网信部门规定可以不进行安全评估的,从其规定。而此处的“国家网信部门规定数量”“国家网信部门规定可以不进行安全评估”等内容有待进一步明确。《个人信息出境安全评估办法(征求意见稿)》尚未包含这些内容,^⑥仅在《汽车数据安全 管理若干规定(试行)》第3条中将涉及个人信息主体超过10万人的个人信息包含在重要数据范围之内,而这显然是不够的。

数据出境时的安全评估主体和办法等也并不明确。而且,即使属于需要安全评估的个人信息,因目前《个人信息出境安全评估办法》尚未出台,也缺乏可操作性。非个人信息的其他重要数据之安全评估办法也有待确立。即仅从现行法还无法得知跨境数据转移安全评估的具体标准,这样会存在一定的不确定性^{[14][P.153]}。除了安全评估之外,个人信息保护认证、标准合同以及其他条件等也需要在日后逐步予以明确,欧盟GDPR及其配套规定中的细节内容可以提供较好的借鉴。

3. 进一步完善应对外国制裁的法律体系

《数据安全法》和《个人信息保护法》均对司法或执法层面的数据或个人信息跨境流动进行了设限,非经我国主管机关批准,不得向外国司法或者执法机构提供存储于我国境内的数据或个人信息。不过,如果因此导致在国外有相应业务的国内企业受到外国相关机构的制裁该如何应对?这一问题值得思考。虽然我国也可以依据《反外国制裁法》予以反制,但其效果将会如何有待进一步观察。与《网络安

全法》和《数据安全法》在整体范围内设置反制条款不同,《个人信息保护法》在第三章个人信息跨境提供规则中规定了应对外国歧视做法的对等措施采取权利,并专门引入限制或者禁止个人信息提供清单制度,而如何使用好这一清单制度,尚待具体细则的出台。当然,后续也应规定如何从该清单中删除的要件和程序规则。依据《反外国制裁法》应可就外国对我国个人信息保护方面歧视性做法采取反制裁措施。

(四)适时推动数字贸易(经济)协定的谈判

随着数据驱动社会的复杂性上升,加强监管合作似乎是向前发展不可或缺的,因为数据问题不能被贸易谈判中的“降低关税、更多承诺”的立场所涵盖,而是需要协调不同的利益和需要监督。^⑦

如前所述,美国、新加坡、日本、澳大利亚、新西兰等国均已签订了数字贸易(经济)协定,而后续也有不少国家跃跃欲试,数字贸易(经济)协定似乎成为在数字经济和数字贸易的大背景下一个新的选择。我国作为数字经济和数字贸易大国,也应适时推动数字贸易(经济)协定,通过数字贸易(经济)协定的谈判,也可将我国对网络安全和数字贸易的相关理念融入其中,试图制定数字贸易(经济)协定的中国模板。这是一个新的领域,处于起步阶段,我国不应输在起跑线上,在数字贸易(经济)协定的谈判中,可以尝试先与新加坡开始推进,不仅因为其已经具有多个成功的模板,也因为两国共为中国-新加坡 FTA、中国-东盟 FTA、RCEP 等多个 FTA 的缔约国,具有成功合作的较大可能性。

结语

因为大多数 FTA 的数据跨境流动条款本身带有例外限制规定,而同时在 FTA 中又含有一般例外和安全例外条款,这就使得三种例外条款的选择适用具有可能性,从而对数据跨境流动构成了较大的制约。安全例外条款中的“不得要求任何缔约方提供其认为如披露则违背其基本安全利益的任何信息”之规定和数据跨境流动具有表面上的联系,这就使

得在数据跨境流动中选择适用特定例外和安全例外具有现实可能性。因此,在签订 FTA 时有必要对数据跨境流动之三种例外条款的适用进行调整,可以采取在电子商务或数字贸易章节中明确规定排除适用一般和安全例外的规定,也可以采取另行制定数字贸易或数字经济协定的方法。虽然我国的数据跨境流动相关三法已经完成,但因其制定时间相差较远,三法在适用方面会面临重合适用及细则不完善等问题,所以,有必要尽快出台《个人信息出境安全评估办法》等相关细则。

注释:

①不同的 FTA 分别选用了电子商务和数字贸易的不同用词,在国际贸易法层面,这两个用词有开始混用的迹象,基于此,本文也将对两者不予区分。

② Tatiana Lacerda Prazeres, Trade and National Security: Rising Risks for the WTO, World Trade Review, Vol. 19, No. 1 (2020), pp. 137-148.

③美国和日本、新加坡和澳大利亚、新加坡和新西兰同时缔结有 FTA,在两国间同时签有两个以上条约时,除非在条约中明确约定条约适用顺序的约定,则会发生适用顺序相关的争议。除这些数字经济协定,新加坡-韩国数字合作协定、新加坡-英国数字经济协定的谈判也已启动。

④该协定的附件 1 约定,各方承认该条不会在各方之间或在本协定项下产生任何权利或义务,想必该条款充分考虑了智利的立场,因为尚未发现智利签订的 FTA 中含此类条款。

⑤ CPTPP 第 14.11 条, USMCA 第 19.11 条, DTA 第 11 条, DEPA 第 4.3 条, SADEA 第 23 条。

⑥ WTO, Russia-Measures Concerning Traffic in Transit: Report of the Panel, WT/DS512/R, 5 April 2019, para. 7. 130.

⑦ Tatiana Lacerda Prazeres, Trade and National Security: Rising Risks for the WTO, World Trade Review, Vol. 19, No. 1 (2020), p. 137.

⑧ Petros C. Mavroidis, The Regulation of International Trade, Vol. I, Cambridge: MIT Press, 2016, pp. 479-487.

⑨2021年2月4日,本案的专家组主席通知争端解决机构:由于全球新冠疫情大流行造成的延误,专家组预计不早于2021年下半年向各方发布最终报告。

⑩在2019年8月8日的函件中,阿拉伯联合酋长国要求争端解决机构主席分发函件,其中表示由于卡塔尔公开撤回有关措施,其认为不再有必要继续提出申诉,即因此没有必要组成专家组,并请求终结此案。

⑪如在“美国-对钢产品和铝产品措施案”中,美国将采取措施的依据放在GATT(1994)第21条;在“阿联酋-与货物、服务和与贸易有关知识产权措施案”中,阿联酋也主张了国家安全例外,但该案在即将做出专家组报告之前被阿联酋和卡塔尔双方协议暂停专家组审议;在“沙特阿拉伯-知识产权保护措施案”中沙特阿拉伯援引了TRIPS第73条下的国家安全例外;在“日本-有关向韩国出口产品和技术的措施案”中,日本主张基于国家安全的顾虑而采取正当的出口管制措施,并试图援引GATT(1994)第21条。梁咏:“论国际贸易体制中的安全例外再平衡”,载《法学》2020年第2期,第143页。

⑫Daria Boklan & Amrita Bahri, The First WTO's Ruling on National Security Exception: Balancing Interests or Opening Pandora's Box?, World Trade Review, Vol. 19, No. 1(2020), pp. 123-136.

⑬Lee Jaemin, National Security Exception's Untested Terrain-Scope and Problems of a 'Refusal to Furnish Information' Clause-, Korean Journal of International Law, Vol. 65, No. 1 (2020), pp. 137-138.

⑭Alexander Savelyev, Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction?, Computer Law & Security Review, Vol. 32, No. 1(2015), p. 141.

⑮WTO, Russia-Measures Concerning Traffic in Transit: Report of the Panel Addendum, WT/DS512/R/Add. 1, 5 April 2019, Annex D.

⑯该草案之前的《个人信息和重要数据出境安全评估办法(征求意见稿)》第9条第1款第(一)项的规定,含有或累计含有50万人以上的个人信息,网络运营者应报请行业主管或监管部门组织安全评估。

⑰Mira Burri, Big Data and Global Trade Law, Cambridge: Cambridge University Press, 2021, p. 41.

参考文献:

[1]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。

[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。

[3]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。

[4]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。

[5]谭观福:“数字贸易规制的免责例外”,载《河北法学》2021年第6期。

[6]刘美:“论WTO安全例外对单边贸易制裁的有限治理——基于‘俄罗斯过境限制案’的分析”,载《国际经贸探索》2020年第1期。

[7]李文卿、郑玲丽:“WTO国家安全例外条款的合理适用”,载《海关与经贸研究》2021年第2期。

[8]谭观福:“WTO国家安全例外视角下的网络安全”,载《中国高校社会科学》2018年第2期。

[9]单文华、邓娜:“欧美跨境数据流动规制:冲突、协调与借鉴——基于欧盟法院‘隐私盾’无效案的考察”,载《西安交通大学学报(社会科学版)》2021年第5期。

[10]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。

[11]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。

[12]时业伟:“跨境数据流动中的国际贸易规则:规制、兼容与发展”,载《比较法研究》2020年第4期。

[13]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。

[14]张金平:“跨境数据转移的国际规制及中国法律的应对——兼评我国《网络安全法》上的跨境数据转移限制规则”,载《政治与法律》2016年第12期。