国际经贸探索
International Economics and Trade Research
ISSN 1002-0594,CN 44-1302/F

《国际经贸探索》网络首发论文

题目：中国跨境数据流动规制体系的 CPTPP 合规性研究
作者：徐程锦
DOI：10.13687/j.cnki.gjjmts.20230217.002
收稿日期：2022-07-11
网络首发日期：2023-02-20
引用格式：徐程锦．中国跨境数据流动规制体系的 CPTPP 合规性研究[J/OL]．国际经贸探索. https://doi.org/10.13687/j.cnki.gjjmts.20230217.002

DOI：10.13687/j.cnki.gjjmts.20230217.002 网络首发时间：2023-02-20 11:14:42
网络首发地址：https://kns.cnki.net/kcms/detail//44.1302.f.20230217.1552.004.html

中国跨境数据流动规制体系的CPTPP合规性研究

徐程锦

摘　要：中国已正式申请加入CPTPP，但国内外始终存在质疑，认为中国的跨境数据流动制度不符合CPTPP规则。近年来，中国通过设立数据出境安全评估、网络安全审查、关键信息基础设施等机制逐步完善跨境数据流动制度框架。中国的跨境数据流动制度并非如外界一般认为的普遍设置数据本地化要求或禁止数据出境，制度总体符合CPTPP规则，或可以援引例外规则进行抗辩。与美欧相比，中国的重要数据和数据出境安全评估机制是对现行跨境数据流动制度的创新和必要补充。数据跨境安全网关对外国部分网站的整体屏蔽在加入CPTPP谈判中宜单独处理。

关键词：跨境数据流动；CPTPP；数字贸易
中图分类号：F743.1　　**文献标识码：**A　　**文章编号：**1002-0594（2023）02-0069-19

中国已正式申请加入《全面与进步跨太平洋伙伴关系协定》（CPTPP）[①]，但部分观点认为，中国在跨境数据流动问题上存在严重的贸易壁垒[②]，不可能符合CPTPP规则。这已成为学界公认的中国加入CPTPP的难点。同时，CPTPP的跨境数据流动规则已成为新一代数字贸易规则的范本，可能影响中国有意加入的任何多双边经贸协定[③]。因此，中国在跨境数据流动方面的国内规制体系能否符合CPTPP规则是当前亟需回答的重要问题，其实质是国内法的国际规则合规问题。此前学界难以回答该问题，主要是因为国内立法不完善，作合规分析时缺少必要支点。2021年以来，国内相关立法进展十分迅速，跨境数据流动规制体系的轮廓逐渐清晰。鉴于国内外对中国的跨境数据流动规制体系已产生较深误解，同时作为合规分析的逻辑起点，有必要先详细阐明中国国内法究竟如何规制跨境数据流动。只有先弄清“事实”，合规分析才有扎实依据；一旦弄清“事实”，对是否符合CPTPP规则的一些质疑也会自动消除。据此，本文分为四个部分，一是根据现行法律法规及重点征求意见稿，廓清中国对跨境数据流动的基本规制框架；二是从上述框架中提取对数据跨境流动的限制措施；三是针对跨境数据流动限制措施做CPTPP规则的合规分析；四是对完善国内跨境数据流动制度和对外谈判提出政策建议。

收稿日期：2022-07-11
作者简介：徐程锦（1986-），女，北京人，工业和信息化部国际经济技术合作中心经贸法律研究所副研究员，研究方向为国际经贸规则、数字贸易、中美经贸关系、产业政策。
感谢匿名审稿专家提出的修改建议，文责自负。

一、中国跨境数据流动的法律规制框架

（一）跨境数据流动涵盖哪些行为

中国现行法律法规中没有“跨境数据流动”概念。《数据安全法》的表述方式是数据“出境”，《个人信息保护法》《网络安全法》《汽车数据安全管理若干规定（试行）》的表述方式是“向境外提供”数据[④]。2017 年的《信息安全技术数据出境安全评估指南（征求意见稿）》（下称《指南》）对“数据出境”作出了定义，概括而言，指将在中国境内运营收集的数据提供给境外机构、组织或个人的行为[⑤]。从语义上看，数据“出境”和“向境外提供”应无本质区别。

但在逻辑上，“跨境”可以包括“出境”和“入境”两个方向。2021 年 11 月颁布的《网络数据安全管理条例（征求意见稿）》第五章规定了“数据跨境安全管理”，其中第四十一条针对的就是将来源于中国境外的信息传输至中国境内[⑥]，说明中国已将数据入境纳入了跨境流动管理范畴。尽管信息与数据在概念上有一定区别，但既然《网络数据安全管理条例》已作出明确规定，在分析中国的跨境数据规制体系时，就需要考虑境外信息向境内传输的情形。

（二）中国国内法如何规制跨境数据流动

综合已生效和正在征求意见的各项法律法规中的相关规定，可以从数据处理者（主体）、数据（客体）、数据流向三个维度，将中国国内法下的跨境数据流动规则归纳为五种情况。

1．一般数据处理者处理个人信息。

此时数据处理者为一般主体；客体为非重要的个人信息；数据流向为出境。对此，《个人信息保护法》规定[⑦]，因业务需要，在满足下列条件之一时，可以向境外提供个人信息：一是通过国家网信部门组织的安全评估；二是按照国家网信部门规定经专业机构进行个人信息保护认证；三是采用国家网信部门制定的标准合同与境外接收方订立合同。此外，一般数据处理者向境外传输个人信息还须满足两项叠加条件：一是数据处理者须采取必要措施保障境外接收方处理个人信息的活动达到中国个人信息保护法规定的保护标准[⑧]。此项规定采纳了很多国家和地区在个人信息保护法中要求的“同等保护”（equal protection）原则，但中国的同等保护只针对境外数据接收方，而不对外国整体法律环境提出要求[⑨]。二是数据处理者须向个人履行告知义务，并获得个人单独同意[⑩]。将个人单独同意作为个人信息出境的必要条件在其他国家的立法中相对少见[⑪]。

2．一般数据处理者处理重要数据。

此时主体为一般数据处理者；客体为重要数据；数据流向为出境。《汽车数据安全管理若干规定（试行）》第十一条规定，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。《数据出境安全评估办法》第四条规定，数据处理者向境外提供重要数据，

应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。上述规定中的数据处理者并非都是以关键信息基础设施运营者为代表的重要主体，多数只是一般数据处理者，但他们处理的数据均为重要数据。此时数据出境必须通过国家网信部门组织的安全评估。

此处出现的关键概念是重要数据，其核心特征是与国家安全和公共利益相关[12]。公众普遍关心的重要数据的范围目前尚未确定。2022 年 1 月发布的《信息安全技术重要数据识别指南》征求意见稿[13]仅提出了识别重要数据的基本原则和考虑因素，最终仍需各地方、各部门结合实际情况确定重要数据目录。根据工业和信息化部 2022 年 2 月公布的《工业和信息化领域数据安全管理办法（试行）》征求意见稿，重要数据的实际范围可能并非由政府部门强行划定，而是由相关领域的数据处理者按照办法提出的重要数据特征，自行确定本单位的重要数据目录，向地方工信主管部门备案[14]。若其他领域的重要数据认定也按此方式办理，则企业在确定重要数据范围过程中可能保有较高水平的自主权。

《数据安全法》还提出了“国家核心数据”概念，重要数据与国家核心数据可以理解为包含与被包含关系[15]。重要数据中特别重要，以至于关系国民经济命脉、重大公共利益的属于国家核心数据。因此，有专家评论称，重要数据的涵盖范围较大，广泛分布在商业领域，而国家核心数据的范围一定极窄，绝大部分组织并不掌握，并需要实施更加严格的管理制度[16]。现行法律并未明确规定核心数据是否能跨境流动。根据《工业和信息化领域数据安全管理办法（试行）》征求意见稿的内容推断[17]，核心数据的出境条件不会比重要数据更加宽松，至少需要经过数据出境安全评估，甚至可能在任何条件下均不得跨境传输。

3. 重要数据处理者处理个人信息或重要数据。

此时主体为重要数据处理者；客体为个人信息或重要数据；数据流向为出境。重要数据处理者主要指关键信息基础设施运营者，在部分法律下也包括处理数据达到特定数量的企业和国家机关[18]。关键信息基础设施运营者在中国境内运营中收集和产生的数据原则上应当在境内存储，因业务需要确需向境外提供时，须按照网信部门会同有关部门制定的办法进行安全评估[19]。此时，无论客体是何种数据，出境条件均无区别。

此处的关键概念是关键信息基础设施（下称“关基”）[20]。成为关基需要满足三个属性：一是属于重要行业或领域，包括公共通信和信息服务、能源、交通、水利等，其中信息服务应主要指大型互联网平台；二是一旦遭到破坏、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；三是属性上是重要网络设施、信息系统。据此，关基的核心特征是与国家安全、国计民生和公共利益相关。一方面，产生关基的行业和领域本身是关系国家安全和国计民生的行业；另一方面，由于其被破坏后的严重危害，关基受到法律法规的特别规定和特殊保护。这些特征都凸显了关基与国家安全、国计民生、公共利益的联系。

4. 外国司法或执法机构请求提供数据。

此时主体为外国司法或执法机构，客体为所有数据，数据流向为出境。与前述情况的区别在于，此时数据出境的原因不是出于市场主体开展业务之目的，而是出于司法或执法目的。对此，《个人信息保护法》和《数据安全法》只提供了一种数据出境条件，即相关数据的主管机关根据中国缔结的国际条约、协定或平等互惠原则处理，经过主管机关批准后才能向外国司法或执法机构提供存储于中国境内的数据[21]。例如，中国政府将向美国证监会和美国公众公司会计监督委员会（PCAOB）提供中概股企业的审计底稿，视为向国外执法机构提供存储于境内的数据，必须通过监管合作渠道答复美方协查请求[22]。这与《个人信息保护法》和《数据安全法》规定的精神是一致的。

为司法或执法目的的数据跨境流动只是中国法律体系下诸多情形中的一种，但在美欧等西方国家，则是其法律重点规制的数据跨境情形[23]。欧盟 2022 年 2 月公布的《数据法》草案第 27 条和美国《澄清境外数据合法使用法》（CLOUD Act）都是规范司法或执法目的数据跨境的典型例子。

5. 境外向境内传输信息。

对于数据或信息入境，目前仅有《网络数据安全管理条例（征求意见稿）》有所规定。《网络数据安全管理条例》第四十一条称，国家建立数据跨境安全网关，对来源于中国境外、法律和行政法规禁止发布或者传输的信息予以阻断传播。所谓法律、行政法规禁止发布或传输的信息，《网络安全法》第十二条第二款有所概括，包括危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情的信息，及扰乱经济秩序和社会秩序的虚假信息，侵害他人名誉、隐私、知识产权和其他合法权益的信息等。对于此类不良信息，中国政府建立数据跨境安全网关，禁止跨境流动。

在上述五种情形中，第四种不属于 CPTPP 跨境数据流动条款规范的“为开展业务之目的”，后文不再作专门分析。其他四种情形对数据跨境的规制大体可分为三类：一是对于一般数据处理者处理的个人信息，可以通过国家网信部门规定的个人信息保护认证或国家网信部门制定的标准合同实现向境外传输；二是当数据处理主体或被处理的数据客体具有重要性时，只能通过国家网信部门组织的安全评估才能向境外传输数据；三是对于涉及国家安全、社会经济秩序或个人与组织合法权益的不良信息，国家直接通过数据跨境安全网关阻断输入，并无例外情形。除上述三种情形外，对于一般数据处理者处理的非个人信息、非重要数据、非不良信息的跨境流动，法律允许数据和信息自由出入境，并无限制措施。因此，不应认为中国的法律法规普遍限制数据跨境流动。

二、中国法律法规对跨境数据流动的主要限制措施

对数据出入境设置条件对数据跨境流动具有限制效果，属于 CPTPP 约束的措

施。根据第一部分的分析，并结合中国现行法律法规中的其他规定，可以梳理出 5 种对跨境数据流动的限制措施。此类措施是分析中国的跨境数据流动规制体系是否符合 CPTPP 规则的关键事实（material facts）。

（一）个人信息保护认证与标准合同

个人信息保护认证与标准合同是各国个人信息保护法中常见的个人信息出境时需满足的条件。在欧盟《通用数据保护条例》（GDPR）下，个人信息保护认证和标准合同是贯彻“同等保护”原则的手段[24]。中国也借鉴了 GDPR 相关规定。

根据《个人信息保护法》第三十八条，个人信息保护认证机制有 3 方面特征：其一，国家网信部门将为此制定专门规定；其二，由专业机构对企业作出个人信息保护认证，按照合格评定程序的一般惯例，此类有权作出认证的专业机构事先应获得政府主管部门对其专业资质和能力的认可；其三，需要获得认证的仅为中国境内的个人信息处理者，而不包括境外的个人信息接收者，相比之下[25]，GDPR 的个人信息保护认证范围延伸至境外个人信息接收者（王燕，2022）。

根据《个人信息出境标准合同规定（征求意见稿）》，标准合同机制具有 3 方面特征：其一，标准合同由国家网信部门制定；其二，个人信息处理者向境外提供数据前应开展个人信息保护影响评估，并与标准合同一并向省级网信部门备案；其三，标准合同的核心内容是约定个人信息处理者和境外接收方的义务[26]。依据标准合同实施个人信息出境，本质上属于境内外双方之间的民商事法律关系，政府部门的限制主要为限定了标准合同内容。就此而言，中国的标准合同机制与欧盟 GDPR 下的标准合同机制并无本质不同[27]。

（二）国家网信部门组织的数据出境安全评估

数据出境安全评估是中国现行法律法规中适用范围最广泛、重要性最高的数据出境限制措施，主要有以下特点。

一是安全评估适用于重要数据处理者或重要数据。根据《数据出境安全评估办法》规定，当数据出境涉及重要数据处理者或重要数据时，必须进行安全评估。其中，重要数据处理者包括关键信息基础设施运营者、处理个人信息达到 100 万人的个人信息处理者、自上年 1 月 1 日起（即连续 2 年以内）累计向境外提供 10 万人个人信息或 1 万人敏感个人信息的数据处理者[28]。

二是安全评估机制主要评估数据出境是否“确需”，以及数据出境后是否“安全”。对于数据出境是否“确需”的评估，体现在安全评估事项的第一点，即评估数据出境的目的、范围、方式的合法性、正当性、必要性[29]。根据 2017 年发布的《数据出境安全评估指南（征求意见稿）》的解释，合法性包括有无法律法规或主管部门明确禁止的出境情形，正当性包括是否满足获得个人同意或存在紧急情况等条件，必要性包括是否存在履行合同、业务需要、履行公务等实际情况[30]。如果合法、正当、必要在安全评估中的实际执行尺度确如《数据出境安全评估指南（征求意见稿）》的解释，则“确需”实际只是保证数据出境存在真实依据，且不会破坏法律

法规底线，而并非设置了如行政法“必要性测试”那样高的门槛。对于数据出境后是否“安全”，安全评估主要考虑数据接收方所在国家或地区的法律法规和政策环境、数据接收方的数据保护水平、出境数据的特征、数据出境后面临的风险、数据处理者和境外接收方是否充分约定了安全保护义务等因素[31]。总体来看，安全评估的结果应是基于对上述因素的综合评判，由于缺乏公开的实际评估案例，安全评估执行的严苛尺度，特别是任一单一因素是否能决定评估结果仍有待观察。

三是安全评估考虑到了便利跨境业务往来的需求。其一，《数据出境安全评估办法》明确将“保障数据依法有序自由流动”作为基本原则[32]，说明制度初衷希望实现数据“自由流动”，但需“依法有序”。其二，安全评估并非完全由政府掌控、自上而下。根据《数据出境安全评估办法》，政府开展安全评估，很大程度上要基于境内数据处理者的自评估结果及其与境外数据接收方的合同约定。企业是实施数据跨境流动的主体，企业的自评估结果及合同约定成为政府安全评估的重要依据，体现了安全评估对企业跨境业务需求的考虑[33]。其三，安全评估并非对数据出境一事一议，一旦通过评估，结果有效期为 2 年，若不发生影响评估考虑因素的重大变化，在结果有效期内无需进行重复评估[34]。这为通过评估的数据跨境流动提供了比较稳定的预期。其四，安全评估只能由“国家网信部门”组织实施[35]。这意味着安全评估的标准和执行尺度将相对统一，有助于企业开展业务。

（三）网络安全审查

网络安全审查对数据能否出境有重大影响，也属于数据出境的限制措施。《网络安全审查办法》规定，网络平台运营者开展数据处理活动，影响或可能影响国家安全的，应当进行网络安全审查[36]。此处的“数据处理活动”在逻辑上应当包括数据出境活动，特别是“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”须强制申报网络安全审查[37]。此前，滴滴、货拉拉等互联网企业被实施网络安全审查，应与赴美上市引发的潜在数据出境风险有关[38]。

与数据出境安全评估相比，网络安全审查的适用范围不限于数据出境，但其关注点限定于国家安全风险。一方面，在数据出境问题上，网络安全审查关注的对象是核心数据、重要数据或大量个人信息，都是关系国家安全和重大公共利益的数据。另一方面，网络安全审查关注数据出境后被外国政府影响、控制、恶意利用的风险，这是一种典型的国家安全风险[39]。而数据出境安全评估除适用于与国家安全和公共利益相关的关键信息基础设施运营者和重要数据外，还可以适用于一般数据处理者实施的个人信息出境，此时安全评估关注的是个人合法权益是否会受到侵害，其保护利益不限于国家安全（赵海乐，2021）。由于其保护利益的特定性，网络安全审查不会像数据出境安全评估一样，在数据出境活动中普遍适用。

（四）禁止数据出境或要求数据在境内存储、处理

中国没有一般性禁止数据出境的规定，禁止数据出境多存在于具体行业的相关规定中，表述方式主要有两种。

一是禁止向境外提供或应在境内存储、处理。例如，2011 年《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第六条规定，“在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。……银行业金融机构不得向境外提供境内个人金融信息”。2012 年《征信业管理条例》第二十四条要求，征信机构在境内采集的信息的整理、保存和加工应当在中国境内进行。《网络安全法》创设安全评估机制后，针对同类数据的出境要求已开始有所变化。例如，同样是针对个人金融信息，2020 年发布的《个人金融信息保护技术规范》7.1.3.d 称，在中国境内收集和产生的个人金融信息，因业务需要，确需向境外机构提供的，应满足个人明示同意、出境安全评估、监督境外机构履行职责义务等要求。对于此类原则上要求数据在本地存储，但因业务需要确需出境且经安全评估后可以出境的，实质仍是允许数据出境，只是施加了安全评估的限制性条件。

二是要求服务器必须设在境内。例如，2014 年《人口健康信息管理办法（试行）》第十条规定，不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。2015 年《地图管理条例》第三十四条要求，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国境内。2006 年《电子银行业务管理办法》第十条规定，中资银行业金融机构的电子银行业务运营系统和业务处理服务器设置在中国境内；外资金融机构的服务器可以设置在境外；设置在境外时，应在中国境内设置可以记录和保存业务交易数据的设施设备，满足政府部门现场检查和调查取证的要求。上述两类规定反映出规则背后的两种不同考虑：一是认为数据出境后有重大安全风险，因此绝对不能出境，人口健康信息和地图数据属于此种情况。二是为监管机构保留管辖权，如电子银行业务运营系统应属于此种情况，只要满足监管机构的调查取证要求，在境内有备份，数据实质仍可以出境。

（五）数据跨境安全网关

根据《网络数据安全管理条例（征求意见稿）》的规定，数据跨境安全网关是对入境数据和信息进行阻断的限制性措施。根据其功能推断，数据跨境安全网关应指通常所称的“网络防火墙”，通过对互联网域名系统中的域名服务器进行技术设置，使境内互联网用户访问境外违法信息的请求无法获得正常域名解析[40]，进而实现拒绝境内用户访问特定网址或对网页上的特定内容进行过滤的目的。

综上所述，中国真正禁止数据跨境流动的只有两种情形。一是在数据出境方面，由于数据本身十分重要（如人口健康信息、地图数据）、可能被认定为国家核心数据，必须使用境内服务器。二是在数据入境方面，对于法律法规禁止发布或传输的信息，通过数据跨境安全网关予以阻断。上述两种情形属于绝对禁止数据跨境流动，没有例外。除此以外，对于其他数据出境情形，虽然法律法规有禁止数据出境或要求数据在境内存储的表述，但规则内在逻辑并非真正禁止数据出境，而是设置了一系列限制性措施，在一般情形下是个人信息保护认证和标准合同、数据出境安全评估等，在涉及国家安全的情形下还须通过网络安全审查。限制性措施的本质是为数

据出境施加了一定条件，当满足条件时，数据可以出境。这也体现了中国法律法规对于跨境数据流动问题的基本原则，即促进数据跨境安全、自由流动[41]。允许绝大部分情形下的数据出境体现了促进数据自由流动，为数据出境设置条件体现了保障数据跨境安全，即在数据跨境流动问题上，须在自由与安全间保持平衡。

三、中国跨境数据流动规制体系在 CPTPP 下的合规性分析

CPTPP 与跨境数据流动相关的规则主要有两条，即第 14.11 条和第 14.13 条[42]。第 14.11 条是总体规定跨境数据流动的条款；第 14.13 条规范了限制跨境数据流动的一种特殊情形，即要求使用本地计算设施（王中美，2021）。

（一）禁止数据跨境流动或要求数据境内存储的措施是否违反 CPTPP 规则

如前所述，中国真正禁止数据跨境流动、要求在境内存储的只有两种情形：一是人口健康信息、地图数据等可能被认定为国家核心数据的必须使用境内服务器；二是通过数据跨境安全网关阻断法律法规禁止发布或传输的信息。

1．可能被认定为国家核心数据的必须使用境内服务器。

第 14.11 条第二款要求成员国应当允许为商业目的跨境传输信息，第 14.13 条第二款要求成员国不得将使用或设置境内计算设施作为开展商业活动的前提条件。当中国的法律法规直接规定人口健康信息、地图数据必须存储于境内服务器时，可以认为此类措施明显违反了第 14.11 条和第 14.13 条第二款的规定。

但是，由于人口健康信息、地图数据可能属于国家核心数据，上述违反 CPTPP 规则的措施可以援引基本安全例外进行抗辩。CPTPP 第 29 章的基本安全例外与 GATT 第 21 条相比存在很大区别，取消了 GATT 第 21 条 b 款中限制“基本安全利益”（essential security interests）的三种情形。在“乌克兰诉俄罗斯与转运有关的措施”（DS512）案中，专家组认为，设置裂变材料、武器运输、战争或其他国际关系紧急状态等三种情形，是为限制成员国对基本安全利益进行主观判断的权利[43]。三种情形是否存在，即成员国能否援引第 21 条 b 款进行抗辩，须由专家组根据实际情况做出客观判断；基本安全利益的内容也受到三种情形的限制，离典型的武装冲突或国内法律失序的情况越远，成员对于基本安全利益的举证责任就越重[44]。这导致 GATT 第 21 条的适用范围被局限在与军事安全相关的领域，很难适应当前国家安全新的发展形势。相比之下，CPTPP 第 29.2 条 b 款对“基本安全利益”未作任何限定[45]，即使参照 DS512 案专家组的法律解释，只要成员国在认定“基本安全利益”并采取限制措施时是“善意”的，就可以对“基本安全利益”的内容和所采取的限制措施拥有主观判断权[46]。CPTPP 第 29.2 条在措辞上的修改极大扩展了基本安全例外的适用范围和成员国的主观判断权，使其可以涵盖国家核心数据所涉及的安全利益。

国家核心数据是“关系国家安全、国民经济命脉、重要民生、重大公共利益”的数据。人口健康信息、地图数据大概率可以被认定为国家核心数据，因为人口健康信息是关系国民经济命脉的基础数据，地图数据更是直接关系国家军事安全，应

当属于“基本安全利益”。如前所述，由于 CPTPP 第 29.2 条 b 款对“基本安全利益”的内涵和援引例外的条件未做任何限定，只要中国本着“善意”认为人口健康信息和地图数据属于基本安全利益，且将人口健康信息、地图数据存储于境内服务器对于保护基本安全利益是必要的，就可以采取此类措施。由于有基本安全例外保护，要求此类可能属于国家核心数据使用境内服务器的措施不违反 CPTPP 规则。

2. 通过数据跨境安全网关阻断向境内传输违法信息。

一般意义上的跨境数据流动主要关注便利商业运营、保护数据安全，适用对象是计算机可处理的数据；而阻断违法信息传输主要关注意识形态安全，适用对象是自然人能理解的信息。CPTPP 第 14.11 条的措辞是跨境传输“信息”（information），而非跨境传输“数据”（data），可以涵盖阻断信息跨境传输的措施。

由于数据跨境安全网关对违法信息实施完全阻断，即绝对禁止信息跨境传输，该措施不符合第 14.11 条第二款关于“应当允许为开展业务跨境传输信息”的要求，因为至少一部分中国境内用户访问境外网站的行为属于业务行为，如在脸书、推特等社交媒体上投放广告。关键问题是，通过数据跨境安全网关阻断违法信息向境内传输是否能援引 14.11 条内设的例外或第 29 章基本安全例外进行抗辩。

如果按照《网络安全法》第十二条定义“违法”信息，被阻断的信息中，涉及“危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一”的信息属于涉及基本安全利益的信息；而暴力和淫秽色情信息、虚假信息、侵害他人名誉、隐私、知识产权和其他合法权益的信息则未必影响国家基本安全利益[67]。但中国在实施信息阻断时，并未区分信息内容，而是统一使用数据跨境安全网关对违法信息进行阻断。对于不涉及国家基本安全利益的被阻断信息，阻断措施需要符合第 14.11 条第三款的规定。第三款是比较典型的 WTO 一般例外条款（Mitchell & Mishra，2019），要求限制性措施在实现公共政策目标的同时，必须满足非恣意、非歧视和“必要性测试”，其中“必要性测试”要求在保证实现公共政策目标的前提下，对贸易的限制程度应保持最低水平。用数据跨境安全网关阻断违法信息可能难以满足第 14.11 条第三款的要求，主要原因是，当前的阻断措施既有对包含违法信息的特定链接的阻断，也有对部分网站的整体阻断。中国很难证明谷歌、推特、脸书等网站上的所有信息都属于中国法律法规认定的违法信息，因此也很难证明对此类网站的整体阻断满足非恣意和“必要性测试”要求。

（二）限制数据跨境流动的措施是否违反 CPTPP 规则

中国法律法规下对跨境数据流动的限制措施主要为个人信息保护认证和标准合同、数据出境安全评估、网络安全审查。这三种措施能否符合 CPTPP 规则，是决定中国能否接受 CPTPP 跨境数据流动条款的关键。

1. 限制数据跨境流动的措施是否违反 CPTPP 第 14.11 条第二款。

CPTPP 第 14.11 条第二款要求成员国应当允许为开展业务跨境传输信息。需要注意的是，该款在设定规则义务时使用的是“应当允许”（shall allow）；相比之下，

《美国－墨西哥－加拿大协定》和《美国－日本数字贸易协定》的对应条款在设定义务时使用的是“不得禁止或限制”（No Party shall prohibit or restrict），《区域全面经济伙伴关系协定》（RCEP）使用的是“不得阻止”（shall not prevent）[48]。以不同规则评价中国对跨境数据流动的限制措施可能得出不同的结果。如果以“不得禁止或限制”作为义务标准，或“不得阻止”被解释为包括“不得限制”，则中国对跨境数据流动施加限制明显违反规则。但 CPTPP 第 14.11 条第二款使用的是“应当允许”，既没有说不得对跨境数据传输设置任何条件，也没有要求允许“自由”传输。本文前两部分对中国现行跨境数据流动制度进行梳理后的重要结论是，除两种明确禁止数据跨境的情况外，中国并未不允许数据出境，而只是对数据出境设置了一些条件，只要满足条件，中国法律法规是允许数据出境的。因此，除非对 CPTPP 第 14.11 条第二款的措辞作变通解释，使其完全等同于《美国－墨西哥－加拿大协定》使用的“不得禁止或限制”的含义，否则，如果严格适用 CPTPP 的措辞，中国对跨境数据流动的规制不应被认为违反该款规定。

2. 个人信息保护认证和标准合同、网络安全审查是否满足 CPTPP 的例外规定。

即使中国对跨境数据流动的限制措施违反第 14.11 条第二款，也可以援引 CPTPP 中的例外条款对限制措施进行抗辩。

个人信息保护认证和标准合同是国际通行做法。欧盟 GDPR、亚太经合组织跨境隐私规则体系下的个人信息保护认证机制已运行多年[49]；在被欧盟法院判决无效前，美国和欧盟之间的“隐私盾”协议本质上也是一种个人信息保护认证机制（肖雄，2021）[50]；标准合同条款在欧盟已使用多年，2021 年刚经历更新，是欧盟众多企业选择的个人信息出境机制[51]。CPTPP 第 14.11 条第三款的核心要求是，限制跨境数据流动的措施须非恣意、非歧视、满足“必要性测试”。只要中国在个人信息保护认证和标准合同的实施中借鉴国际通行做法，并未歧视个别国家或提出超出必要限度的要求，则可以满足第 14.11 条第三款的要求。从目前公布的标准合同征求意见稿内容看，并无歧视特定国家和境外接收方的内容，所提合同义务也属于保护个人信息所必要的常规内容，与欧盟的标准合同条款内容并无实质区别。

网络安全审查适用于“影响国家安全”的情形。如前所述，CPTPP 第 29 章的基本安全例外大幅扩展了成员国自主认定基本安全利益和采取相应限制措施的权利，可以涵盖网络安全审查的适用情形。只要中国在实施网络安全审查时本着“善意”精神，不随意扩大审查的适用范围，或以安全为名追求贸易利益，就可以援引并满足 CPTPP 第29.2条的基本安全例外。以对滴滴适用网络安全审查为例，网络安全审查关注因在国外上市导致“核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险”。在审查启动前，滴滴出行的国内月活用户已超过 4 亿，年运送旅客量超过 100 亿人次[52]，并因此掌握了大量用户的个人信息和国内交通、地图数据，属于掌握重要数据甚至核心数据的企业。滴滴赴美上市后受到美国法律管辖，存在美国政府借管辖权控制滴滴并恶意利用其数据的风险，影响中国的

基本安全利益，对其启动网络安全审查并非是完全出于贸易利益而限制数据跨境流动，中国可以援引 CPTPP 第 29.2 条对滴滴的网络安全审查进行抗辩。

3. 数据出境安全评估是否满足 CPTPP 的例外规定。

数据出境安全评估是中国跨境数据流动规制体系中最核心、最独特的机制设计[53]，只有数据出境安全评估满足 CPTPP 的例外，中国的跨境数据流动规制体系才能符合 CPTPP 规则。如前所述，安全评估适用于重要数据处理者或重要数据。此处的“重要性”既涉及国家安全，也涉及非国家安全的公共利益、经济运行等[54]。因此，安全评估不能仅满足基本安全例外，还应满足第 14.11 条第三款内设例外。由于内设例外的合规标准高于基本安全例外，此处仅分析数据出境安全评估机制能否满足内设例外的要求。CPTPP 第 14.11 条第三款有三项核心规则。

一是要求限制数据出境的措施是为实现合理公共政策目标。关于合理公共政策目标的范围，CPTPP 第 14.11 条并未作出规定。考虑到性质类似的 GATT 第 20 条明确列出了可以援引例外的公共政策目标[55]，而 CPTPP 第 14.11 条第三款并未明确公共政策目标范围，从法律解释角度讲，中国可以主张此种省略是有意为之，即 CPTPP 第 14.11 条允许成员国根据实际情况确定本国的公共政策目标范围。根据前述梳理，需要进行数据出境安全评估的，或者属于主体重要，如数据处理者是关基运营者或国家机关，或者属于客体重要，如出境数据是重要数据，其目标都是为保障国家安全和重要公共利益，应属于第 14.11 条第三款所说的合理公共政策目标。

二是要求限制措施不恣意，非歧视，且不构成隐藏的贸易限制。根据《数据出境安全评估办法》的规定，安全评估由国家网信部门统一组织实施，有明确的评估程序、重点考察因素等。这些规则的设置都是为在安全评估过程中保持标准客观统一。至少从国内规则层面看，只要正常适用安全评估程序和标准，就不应存在恣意、歧视或隐藏的贸易限制问题。如果某些国家因为国内数据保护规则不完善等原因，在安全评估中处于劣势或未通过评估，则属于客观评估标准适用于具体国家时得出的结果，不应被认为是对该国的歧视。可能有观点认为，对数据出境专门设置安全评估，对数据在境内流动则不作此要求，本身就是对境外数据接收者的歧视和贸易限制。对此，一方面，数据出境确实存在一些数据在境内流动不存在的风险，包括境外整体法律环境、境外数据接收方的能力难以掌控等，确需进行专门规制。另一方面，安全评估程序是否构成歧视或贸易限制，关键应看对境外数据接收者适用的评估标准是否实质高于境内数据接收者，使境外数据接收者处于相对更加不利的竞争地位。事实上，中国相关法律法规对境内数据处理者也设定了相当严格的义务。例如，重要数据处理者在境内开展共享、交易、委托处理重要数据，也需要进行安全评估，评估内容与数据出境安全评估的内容并无实质区别[56]。只要在安全评估中没有专门针对境外设置不合理要求，开展数据出境安全评估就不应被认为是对境外数据接收者的歧视或贸易限制。

三是限制措施应满足“必要性测试”。CPTPP 第 14.11 条第三款未用 necessary 的措辞，但一般认为该条款就是客观必要性测试[57]。核心要求是限制措施应保持在最低水平，不应存在同样能实现合理公共政策目标但限制性更小的替代措施。相比之下，RCEP 相应条款最大的区别是将客观必要性测试改为主观必要性测试，并将基本安全例外直接纳入跨境数据流动条款，使成员国拥有较大的对基本安全利益、合理公共政策目标和限制措施必要性的主观判断权[58]。由于措辞区别，RCEP 跨境数据流动条款体现了更多对成员国的包容性（谢卓君、杨署东，2021），其合规门槛比 CPTPP 低得多。CPTPP 采用的客观必要性测试历来是例外条款中最难通过的一关，但数据出境安全评估机制仍有可能通过测试。首先，证明限制措施“不必要”需要举出能同样实现安全评估机制所保护的合理公共政策目标但限制性更小的替代措施。对重要数据处理者实施的数据出境和重要数据出境进行安全评估，是中国跨境数据流动制度中一项独特的机制创新。当前，美欧等国的数据出境监管集中于个人信息和因执法目的跨境调取数据，对于非个人信息或执法目的的数据出境则缺乏规制[59]。而重要数据处理者实施的数据出境和重要数据出境，恰恰是对个人信息和执法目的以外的数据出境情形作出了规范，其所保护的政策目标，如经济运行、社会稳定、公共利益等，也非人权、隐私权、执法权等政策目标所能涵盖。因此，当前其他国家尚无与中国数据出境安全评估机制所保护的公共政策目标类似的数据出境监管替代机制。从这个角度看，中国的数据出境安全评估机制不仅不是数据出境的壁垒，反而弥补了跨境数据流动监管中的一项制度空白，为非个人信息或执法目的，而与国家安全、公共利益相关的数据跨境流动提供了解决方案。其次，即使外国存在保护类似合理公共政策目标的替代措施，其对数据出境的限制性也未必比中国的数据出境安全评估更小。从欧盟的情况看，尽管其法规并未使用评估的措辞，但其个人信息出境的关键制度均在实质上基于评估机制。充分性认定是对外国整体法律环境进行评估[60]，自 GDPR 生效后，仅有日本、韩国等少数国家获得了充分性认定，说明该评估并不易通过；根据欧洲法院在 Shrems II 案件中的判决，在使用标准合同条款进行个人信息跨境传输的情形下，也需要欧盟境内数据处理者对标准合同条款是否能提供充分保护进行评估，评估内容包括合同条款是否约定充分、境外数据接收方的基本情况、境外数据接收国政府接触数据的可能性、接收国的法律制度等[61]，其评估的全面和复杂程度并不亚于中国的数据出境安全评估。从美国的情况看，尽管美国没有专门的数据出境监管规则，但事实上通过出口管制、外资安全审查等手段对其认为重要的数据实施严格监管（魏宁，2022）。2022 年 6 月，在美国外国投资委员会（CFIUS）的压力下，Tiktok 与甲骨文达成协议，将 Tiktok 美国用户的所有数据从 Tiktok 的服务器转移至甲骨文在美国境内的服务器，且专门设置隔离机制，使 Tiktok 的母公司字节跳动无法访问美国用户数据[62]。尽管 CFIUS 启动审查的理由是威胁国家安全，但 Tiktok 数据的本质是大规模个人信息，在中国法律下属于参照重要数据保护的类型，经安全评估后可以出境[63]。而美国采用外资安全

审查管理大规模个人信息出境引发的潜在安全风险，不仅审查标准更加恣意、不透明，最终结果也是强制数据在美国境内存储，与中国的数据出境安全评估相比，是更加严苛、更具有贸易壁垒性质的数据跨境监管机制。

四、对完善国内跨境数据流动制度和参加 CPTPP 谈判的建议

通过上述分析，本文的基本结论是：除数据跨境安全网关对部分外国网站的整体屏蔽外，中国的跨境数据流动规制体系可以满足 CPTPP 第 14 章的规则要求。但鉴于中国的跨境数据流动制度尚不完善，且国际社会在跨境数据流动问题上对中国的偏见已经形成，要实现这一结论，中国在国内和国际层面还需付出艰苦努力。

（一）尽快完善跨境数据流动监管体系中的关键制度

中国的当务之急是尽快补齐跨境数据流动规制体系中的关键空白和短板，一是完成重要数据的认定，二是明确数据出境安全评估机制的细则和实施标准。这两项制度是中国跨境数据流动规制体系中的关键支柱，只有其细节明确，对中国跨境数据流动制度的评价才有基本准星。从参与国际规则谈判角度看，完善国内关键制度十分重要。其一，国内制度是一国参与制定国际规则的基础。只有国内关键制度的细节和标准明确，在国际谈判中才能准确判断是否能接受一项约束该制度的国际规则，否则谈判人员将陷入进退失据之中，遑论掌握规则谈判的主动权。其二，清晰的国内制度是澄清国际舆论的必要条件。中国的国内制度细节越不明确，国内外各方就越容易向最保守的方向理解。由于预期不稳，企业不敢实质开展数据出境业务，其他国家则可借题发挥，指责中国实施世界上最恶劣的数据本地化政策。所谓三人成虎，此类负面印象会给中国在加入 CPTPP 等国际规则谈判中营造非常被动的舆论氛围，谈判尚未开始，各方就已认为中国难以达到规则标准，这将大幅提升中国参与规则谈判的难度。

数据出境安全评估制度直至 2022 年中才发布、重要数据认定标准至今尚未出台的原因可能在于这两项制度过于重要，主管部门不得不十分慎重、反复论证。对于此类特别重要的制度，今后在制定规则过程中可考虑先由中央主管部门颁布试行制度，指定国内个别地方开展试点，而非让地方自行探索；并效仿产业技术创新中的快速迭代理念，在试点过程中不断发现问题、解决问题，实现关键制度在应用中的快速迭代创新，在基本成熟后再普遍推广适用。尽管在短期内，试点制度快速迭代会增加制度的不确定性，但与为了追求一次完美成型而付出制度长期无法出台的代价相比，试点制度快速迭代反而可能为市场提供更大的确定性。

（二）积极向国际社会解释中国跨境数据流动制度的合理性和创新性

在国内跨境数据流动制度基本成形后，应积极主动向国际社会解释中国的制度。

首先，中国需要坚信一个事实，即国际社会即使对中国有偏见，也希望听到中国人对自己的制度做出清晰的说明。本文作者曾在英文媒体上简要阐述过本文的核心观点，包括对国内制度的梳理结果。很快美国大使馆就与作者联系，希望就中国

的跨境数据流动制度进行深入讨论。不论外方是否同意我们的观点，当中国人主动解释自己的情况，且给出与通常看法不一样的观点时，至少会引起外方的重视，比将中国重要制度的解释权留给外国人更好。

其次，解释中国的跨境数据流动制度需着眼于制度的合理性和创新性。尽管中国的跨境数据流动制度不完美，但制度的关键核心要素是合理的。例如，外国攻击中国跨境数据流动制度的主要理由是中国要求数据本地存储，但只要仔细梳理中国的法律法规就可以发现，这种攻击并不符合事实。中国真正要求的是重要数据处理者处理的数据和重要数据出境需要经过安全评估，而非要求数据本地存储，且欧美各国均以各种形式实质存在类似的安全评估机制。从这个角度看，中国的制度并非比其他国家的制度更不合理。此外，评论中国的跨境数据流动制度不能只看限制性措施，还应看到对于绝大部分非个人信息、非重要数据、非重要数据处理者、非不良信息，中国是允许数据跨境自由流动的，并无限制措施。同时，中国的跨境数据流动制度还具有创新性，最典型的表现是中国的制度几乎涵盖了所有数据，而非像美欧一样主要规定个人信息和执法目的的跨境数据流动。在当今产业数字化的时代背景下，与产业相关的数据无论从规模还是重要性角度，都不亚于个人信息，中国的重要数据概念很大程度上涵盖了产业数据，并为产业数据跨境流动提供了规范。在此意义上，创立重要数据制度不仅不是数字贸易壁垒，反而是一种重要的制度创新。其他国家也需要对产业数据的跨境做出规范，如果将其中的创新性阐述清楚，这将成为中国给国际社会提供公共产品的难得契机。

（三）谨慎限缩基本安全例外的适用范围并在国内制度中作出相应适配

对于跨境数据流动的限制措施，既可以适用 CPTPP 第 14.11 条和第 14.13 条的内设例外，也可以适用第 29 章的基本安全例外。从中国的国家利益角度看，应尽量限缩基本安全例外的适用范围。首先，中国法律法规中强制要求数据本地存储的情形并不多，网络安全审查也并非时时审、事事审，中国对基本安全例外的需求是有限的。其次，中国企业目前遭遇了其他国家以国家安全为由实施的歧视性政策，Tiktok 是典型案例。随着中国企业国际化程度加深，此类情形可能越来越多。出于保护本国企业的目的，中国需要限制其他国家滥用基本安全例外。再次，中国需要借助跨境数据流动规则使其他国家的数据向中国流动。随着当前国际供应链重构，大量中国企业加强对外投资，在东南亚等地扩张生产线。在产业数字化的浪潮中，若此类企业的数据能回流中国，对于中国工业互联网、智能制造所需的算法、工业软件等技术的发展将是一笔巨大财富（周念利、姚亭亭，2021；陈寰琦，2020）。为防止其他国家滥用数据本地存储政策，中国需要限缩基本安全例外的适用范围（魏求月、洪延青，2022）。

为此，中国可主张仅在极为有限的情形下适用基本安全例外为限制跨境数据流动的措施进行抗辩，绝大部分限制措施均应满足 CPTPP 第 14.11 条和第 14.13 条的内设例外。即使限制措施是出于国家安全目的，也不应直接适用基本安全例外，只

要相关数据在其他国家被允许跨境流动，实施限制措施的国家就应优先援引第14.11条和第14.13条的内设例外，而非基本安全例外进行抗辩。事实上，对以国家安全为由实施的措施加以约束并非没有先例。2022年3月美国与欧盟签订的《跨大西洋数据隐私框架》就规定，美国情报部门为保护国家安全而获取欧盟数据的措施须满足必要性测试和比例原则[64]。

中国国内的跨境数据流动监管也应做出相应的制度安排。若某项数据确实不能出境，应明确其国家核心数据的属性。核心数据的范围划定应尽量审慎，限制在人口健康信息、地图数据等确需本地存储的有限范围内。其余重要数据出境则应统一到安全评估上来，明确数据经安全评估后可以出境。

（四）在国际规则谈判中单独处理数据跨境安全网关问题

数据跨境安全网关作为跨境数据流动限制措施，是中国符合 CPTPP 规则的主要障碍。该措施能否援引基本安全例外存在疑问，即使能援引，由于数据跨境安全网关的适用范围很广，也将与前述宜限缩基本安全例外适用范围的立场存在冲突。对中国而言，是否将基本安全例外进行扩大化解释，用于保护数据跨境安全网关；若扩大化解释后其他国家滥用基本安全例外损害中国企业利益，中国又将如何处理，此中的国家利益应如何平衡，是主管部门需提前考虑并妥善把握的关键政策决断。

适当的处理方案是将数据跨境安全网关问题从跨境数据流动议题中剥离出来，在加入 CPTPP 谈判或其他类似国际规则谈判中单独处理，争取获得豁免。其一，数据跨境安全网关的设置目的主要出于意识形态安全原因，与其他限制跨境数据流动措施的政策目标和措施性质均不相同，其屏蔽的是含有特定内容的信息，与出于商业目的的数据跨境属于不同情景；其二，接受 CPTPP 跨境数据流动条款对中国整体是有利的，宜尽早取得结果，在谈判中纳入数据跨境安全网关问题将使跨境数据流动规则的谈判复杂化，甚至不必要地陷入僵局。可考虑以脚注或加入议定书单独条款的形式，明确 CPTPP 跨境数据流动规则不适用于数据跨境安全网关。

（通讯作者 徐程锦电子邮箱：xucj@cietc.org.cn）

注释：

① “中方正式提出申请加入《全面与进步跨太平洋伙伴关系协定》（CPTPP）”，http://www.mofcom.gov.cn/article/ae/bldhd/202109/20210903199707.shtml。

② See United States Trade Representative Office，2022 National Trade Estimate Report on Foreign Trade Barriers，March 31，2022，at p109，https://ustr.gov/sites/default/files/2022% 20National% 20Trade% 20Estimate% 20Report% 20on% 20Foreign% 20Trade% 20Barriers.pdf；Nigel Cory，Cross－Border Data Flows：Where Are the Barriers，and What Do They Cost?，May 1，2017，at https://itif.org/publications/2017/05/01/cross－border－data－flows－where－are－barriers－and－what－do－they－cos。

③ 如《数字经济伙伴关系协定》（DEPA）第4.3条基本完全采用了 CPTPP 第14.11条的文本。

④ 见《数据安全法》第三十一条；《个人信息保护法》第三十八条；《网络安全法》第三十七条；《汽车数据安全管理若干规定（试行）》第十一条。

⑤《信息安全技术数据出境安全评估指南（征求意见稿）》第3.7条，2017年8月25日。

⑥《网络数据安全管理条例(征求意见稿)》第四十一条第一款原文为:“国家建立数据跨境安全网关,对来源于中华人民共和国境外、法律和行政法规禁止发布或者传输的信息予以阻断传播。”

⑦《个人信息保护法》第三十八条第一款。

⑧《个人信息保护法》第三十八条第三款。

⑨ 可资对比的是欧盟《通用数据保护条例》(GDPR)。GDPR 是最早对个人数据出境提出“同等保护”原则的重要立法之一。其与中国《个人信息保护法》的区别在于,GDPR 对证明“同等保护”提供了多种渠道,其中部分渠道是证明境外数据接收方满足“同等保护标准”,如标准数据保护条款、约束性公司规则等,见 General Data Protection Regulation, Article 46;部分渠道是证明国外整体法律环境符合“同等保护标准”,如欧盟委员会做出的充分性认定,见 General Data Protection Regulation, Article 45, https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX%3A02016R0679-20160504&qid=1532348683434.

⑩《个人信息保护法》第三十九条。

⑪ 欧盟 GDPR 对待个人单独同意的方式是多数国家此类立法的典型模式,即将个人单独同意作为无法满足“同等保护”条件时,仍可以进行个人信息跨境传输的减损条件,见 General Data Protection Regulation, Article 49, https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX%3A02016R0679-20160504&qid=1532348683434;但仍有部分国家与中国类似,将个人单独同意作为个人信息跨境传输的必要条件,如韩国《个人信息保护法》第 39-12 条, https://privacy.go.kr/cmm/fms/FileDown.do? atchFileId=FILE_000000000830758&fileSn=4&nttId=8186&toolVer=&toolCntKey_1=。

⑫ 见《汽车数据安全管理若干规定(试行)》第三条第六款、《数据出境安全评估办法》第十九条。尽管《汽车数据安全管理若干规定(试行)》将个人和组织合法权益相关的数据也作为重要数据,但总体来看,重要数据的特征是与国家安全和公共利益相关。

⑬ 根据业内专家披露的信息,《重要数据识别指南》将更名为《重要数据识别规则》,在 2022 年 4 月修改后,对重要数据的定义为:“特定领域、特定群体、特定区域或达到一定精度和规模的数据,一旦被泄露或篡改、损毁,可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。”该定义的核心内容与《数据出境安全评估办法》对重要数据的定义基本一致。见“小贝说安全”,“国标《重要数据识别指南》又有重大修改了”,2022 年 4 月 26 日, https://mp.weixin.qq.com/s/KD1UtgdUcarUDtiw3VS31A。

⑭《工业和信息化领域数据安全管理办法(试行)》征求意见稿第十二条。

⑮《数据安全法》第二十一条第二款。

⑯ 小贝说安全,“9 月 1 日生效日期临近,《数据安全法》当如何落实?”, https://mp.weixin.qq.com/s/Mjx-bkg0Jkd83S3Fpy-ML9w。

⑰《工业和信息化领域数据安全管理办法(试行)》征求意见稿第二十一条。

⑱《中华人民共和国个人信息保护法》第四十条。

⑲《中华人民共和国网络安全法》第三十七条;《中华人民共和国个人信息保护法》第四十条;《中华人民共和国数据安全法》第三十一条。

⑳《关键信息基础设施安全保护条例》第二条。

㉑《中华人民共和国个人信息保护法》第四十一条;《中华人民共和国数据安全法》第三十六条。

㉒ 证监会有关部门负责人就美国总统金融市场工作组发布《关于保护美国投资者防范中国公司重大风险的报告》事宜答记者问,2020 年 8 月 8 日, http://www.csrc.gov.cn/csrc/c100028/c1000720/content.shtml。

㉓ 从西方国家现行立法内容看,其法律规制的数据跨境情形主要有两种,一是个人信息的跨境,二是为司法或执法目的的数据跨境。

㉔ General Data Protection Regulation, Article 46 para. 2(c),(d), and(f), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:32016R0679&from=EN.

㉕ General Data Protection Regulation, Article 42 para. 2, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:32016R0679&from=EN.

㉖《国家互联网信息办公室关于＜个人信息出境标准合同规定（征求意见稿）＞公开征求意见的通知》，2022 年 6 月 30 日，http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm。

㉗ 欧盟 GDPR 也要求境内外双方须使用经欧盟委员会批准的标准合同条款，并对合同条款内容进行了限定，合同条款主要涉及个人信息出境范围符合最小化原则、采取必要安全保障措施、告知数据主体必要信息、限制再传输等，见 COMMISSION IMPLEMENTING DECISION（EU）2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation（EU）2016/679 of the European Parliament and of the Council，https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN。

㉘《数据出境安全评估办法》第四条。

㉙《数据出境安全评估办法》第五条、第八条。

㉚《信息安全技术 数据出境安全评估指南（征求意见稿）》，2017 年 8 月 25 日，http://std.samr.gov.cn/gb/search/gbDetailed?id=625516672A96BD9BE05397BE0A0A265C。

㉛《数据出境安全评估办法》第八条；《数据出境安全评估申报指南（第一版）》第三部分“拟出境活动的风险评估情况”，http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm。

㉜《数据出境安全评估办法》第三条。

㉝《数据出境安全评估办法》第五条、第六条、第八条。

㉞《数据出境安全评估办法》第十四条。

㉟《数据出境安全评估办法》第十条。

㊱《网络安全审查办法》第二条。

㊲《网络安全审查办法》第七条。

㊳ 有网络安全领域专家在评论《网络安全审查办法（修订草案征求意见稿）》和滴滴被审查事件时指出，修订草案中相关上市要求条款是为落实中办、国办《关于依法从严打击证券违法活动的意见》中关于“完善数据安全、跨境数据流动、涉密信息管理等相关法律法规”的精神，滴滴等这些企业存在的网络安全风险主要是数据安全风险，且因企业赴美上市而引发。见“中国信息安全研究院左晓栋：《网络安全审查办法》为何这样改”，2021 年 7 月 12 日，https://m.thepaper.cn/baijiahao_13545028。

㊴《网络安全审查办法》第十条。

㊵ The Great Firewall: A Technical Perspective, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/great-firewall-technical-perspective/index.html.

㊶《数据出境安全评估办法》第一条。

㊷ CPTPP 第 11 章“金融服务”附件 11-B“具体承诺”的 B 节规定了金融服务中的跨境数据流动规则。由于该规则仅适用于金融服务，含有金融监管的特定考量，对分析中国的跨境数据流动规制体系整体上是否符合 CPTPP 规则不产生决定性影响，本文不再做专门分析。

㊸ Russia-Measures Concerning Traffic in Transit, Report of the Panel, WT/DS512/R, 5 April 2019, at para. 7.65.

㊹ Russia-Measures Concerning Traffic in Transit, Report of the Panel, WT/DS512/R, 5 April 2019, at paras. 7.79, 7.98, 7.134-7.135.

㊺ CPTPP 第 29.2 条 b 款的相关规定是：“本协定中任何条款不得解释为：（b）阻止一缔约方采取其认为对……保护其自身基本安全利益所必需的措施。” http://images.mofcom.gov.cn/sms/202101/20210111155757853.pdf。

㊻ Russia-Measures Concerning Traffic in Transit, Report of the Panel, WT/DS512/R, 5 April 2019, at paras. 7.132-7.133, 7.138.

㊼ 根据既往 WTO 争端解决案件中的法律解释，基本安全利益比安全利益的范围更窄，应指与国家根本职能，如保护本国领土和人民免受外部威胁或维护国内法律和公共秩序相关的利益。Russia-Measures Concerning Traffic in Transit, Report of the Panel, WT/DS512/R, 5 April 2019, at paras. 7.130-7.131.

㊽ 见 CPTPP 第 14.11 条第二款；《美国-墨西哥-加拿大协定》第 19.11 条第一款；《美国-日本数字贸易协定》第 11 条第一款；《区域全面经济伙伴关系协定》第 12.15 条第二款。

㊾ 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.

㊿ Guide to the EU－US Privacy Shield, at p8, https://ec. europa. eu/info/sites/default/files/2016－08－01－ps－citizens－guide_en. pd_. pdf#: ~: text = This% 20is% 20where% 20the% 20EU－U. S. % 20Privacy% 20Shield% 20comes, whether% 20you% 20are% 20an% 20EU% 20citizen% 20or% 20not.

(51) Standard Contractual Clauses(SCC), https://ec. europa. eu/info/law/law－topic/data－protection/international－dimension－data－protection/standard－contractual－clauses－scc_en.

(52) 经济参考报，“滴滴国内月活用户突破 4 亿”，2020 年 11 月 4 日，http://www. jjckb. cn/2020－11/04/c_139489450. htm? from = groupmessage。

(53) 根据本文第一部分的梳理，数据出境安全评估可以适用于除执法或司法目的跨境调取数据以外的所有数据出境情形，且是某些情形下唯一可以实现数据出境的机制，在中国的跨境数据流动制度体系中具有核心地位。其他国家的跨境数据流动制度（如欧盟 GDPR）提供了不同的数据出境机制，但尚未见到哪个机制在本国制度中的地位和重要性与数据出境安全评估类似。

(54)《信息安全技术 重要数据识别规则（征求意见稿）》第 3. 1 条，2022 年 3 月 16 日，见“小贝说安全”，“国标《重要数据识别指南》又有重大修改了”，https://mp. weixin. qq. com/s/KD1UtgdUcarUDtiw3VS31A；《关键信息基础设施安全保护条例》第二条。

(55) 第 20 条(a)－(j)款均提出了具体的公共政策目标，如保护公共道德、保护人类和动植物生命健康、确保法律法规得到遵守等，见 General Agreement on Tariffs and Trade, Article XX, https://www. wto. org/english/docs_e/legal_e/gatt47_02_e. htm#articleXX。

(56)《网络数据安全管理条例（征求意见稿）》第三十二条第四款。

(57) 除了“required”的措辞与一般“必要性测试”中常用的“necessary”不同外，CPTPP 第 14. 11 条第三款在逻辑结构、规则中的关键词等方面与“必要性测试”并无差别。目前尚不清楚美国在 TPP 谈判时为何将 necessary 改为 required，但可资对比的是，后来的《美国－日本数字贸易协定》第 11 条又将“required”改为“necessary”。

(58)《区域全面经济伙伴关系协定》第 12. 15 条第三款(a)项。

(59) 尽管欧盟制定了《非个人数据在欧盟境内自由流动框架法规》，但由于欧盟在数据立法上相对独立，对境内成员国和境外国家在数据跨境方面有明显区别对待，故欧盟对非个人数据的相关立法更类似于美国或中国的国内立法，数据在欧盟成员国之间的流动类似于在中国不同省份之间的流动，并非典型意义上的非个人数据在不同国家之间的跨境流动。

(60) See Questions & Answers on the adoption of the adequacy decision ensuring safe data flows between the EU and the Republic of Korea, 17 December 2021, https://ec. europa. eu/commission/presscorner/detail/en/qanda_21_6916.

(61) European Court of Justice, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems(Shrems II), at paras. 104－105, Case C? 311/18, 16 July 2020, https://curia. europa. eu/juris/document/document. jsf;jsessionid = CF8C3306269B9356ADF861B57785FDEE? text = &docid = 228677&pageIndex = 0&doclang = EN&mode = req&dir = &occ = first&part = 1&cid = 9812784.

(62) Reuters, TikTok moves U. S. user data to Oracle servers, June 18, 2022, https://www. reuters. com/technology/tiktok－moves－us－user－data－oracle－servers－2022－06－17/.

(63)《数据出境安全评估办法》第四条（二）、（三）。

(64) European Commission, Trans－Atlantic Data Privacy Framework, March 2022, https://ec. europa. eu/commission/presscorner/api/files/attachment/872132/Trans－Atlantic% 20Data% 20Privacy% 20Framework. pdf. pdf.

参考文献：

陈寰琦，2020. 签订“跨境数据自由流动”能否有效促进数字贸易[J]. 国际经贸探索(10)：4－21.

王燕，2022. 跨境数据流动治理的国别模式及其反思[J]. 国际经贸探索(1)：99－112.

王中美,2021. 跨境数据流动的全球治理框架：分歧与妥协[J]. 国际经贸探索(4):98-112.
魏宁,2022. 美国数据出境管理体制及中国因应[J]. 国际经济法学刊(4):25-44.
魏求月,洪延青,2022. 数据跨境流动之国家安全例外条款:制衡、边界与建构[J]. 国家安全研究(4):101-120.
肖雄,2021. 美欧《隐私盾协议》之无效及中国应对路径[J]. 信息安全与通信保密(7):76-84.
谢卓君,杨署东,2021. 全球治理中的跨境数据流动规制与中国参与[J]. 国际观察(5):98-126.
赵海乐,2021. RCEP 争端解决机制对数据跨境流动问题的适用与中国因应[J]. 武大国际法评论(6):39-55.
周念利,姚亭亭,2021. 跨境数据流动限制对数字服务进口的影响测度及异质性考察[J]. 国际商务(2):1-15.
Mitchell A.,Mishra N.,2019. Regulating Cross-Border Data Flows in a Data-Driven World:How WTO Law Can Contribute[J]. Journal of International Economic Law. 22(3):389-416.

China's Legal Framework on Cross-border Data Flow and its Compliance with the CPTPP Requirements

XU Cheng-jin

Abstract: China has officially applied to accede to the CPTPP. Suspicions abound, however, inside and outside China, that its institution on cross-border data flow is unable to pass muster the CPTPP requirements. Based on the recently promulgated rules and regulations, this paper attempts to lay out the big picture of the institution on cross-border data flow in China, summarize the restrictive measures therein and analyze its compliance with the CPTPP legal requirements. The conclusion is, in general, China does not require data localization and China's institution on cross-border data flow does not contradict to the CPTPP. Moreover, the new mechanisms on the important data and security assessment of data export are innovative and complementary to the current institutions on cross-border data flow as applied in the United States and the European Union. The measure with cross-border data gateway that blocks foreign websites is advised to be addressed separately in the CPTPP accession negotiation.

Key words: cross-border data flow; CPTPP; digital trade

（责任编辑　罗远航　责任校对　袁群华）