# RCEP 数据跨境流动规则与中国数据跨境流动立法研究

张学博　王智韬

**摘　要**：数据跨境流动已成为推动世界经济贸易高质量发展的新路径，数据跨境规则开始显现出双边、多边的治理模式，有效规制的关键是维持数据保护与数据自由的良好平衡。RCEP 作为中国加入的大型区域贸易协定，包含“合作共治”的数据跨境规则，其中“例外条款”“灵活监管”的具体设计与中国数据跨境立法中“欠缺明确的数据分级分类标准”“数据跨境监管形式单一”等问题产生了衔接上的冲突。中国作为 RCEP 的主要倡导国，应构建系统性的应对策略，舒缓二者间的冲突效果。文章提出建立数据出境分级审核体系；在推动 RCEP 数据跨境立法合作的同时，紧握住数据立法的国际话语权；加强 RCEP 技术安全保障，在数据跨境源头强化对数据的监管。

**关键词**：RCEP；中国数据跨境困境；重要数据分级分类；数据监管；数据保护

**中图分类号**：D922.16;D996　文献标识码：A 文章编号：1673-5706（2024）01-0098-08



## 一、问题的提出

伴随数字技术的快速发展，数据开始成为特殊生产力，具有十分重要的战略价值，数据资源成为推动全球经贸联动的关键因素，以数据跨境为媒介，数据的利用与处理已成为推动世界经济贸易高质量发展的新路径。2020 年 11 月，中、日、韩等 15 国正式签署《区域全面经济伙伴关系协定》（Regional Comprehensive Economic Partnership，以下简称 RCEP），于 2023 年 6 月 2 日全面生效[1]。RCEP 的全面生效标志着东盟经济一体化的进一步形成，使 RCEP 成为建设数字丝绸之路的重要环节。[2]针对数据跨境的监管，RCEP 已设专章进行规制，包括参与国对数据跨境的监管权利、义务、责任及例外规则，展现出不同于欧美范式的“折中性”数据跨境治理模式。但 RCEP 数据跨境规则的实际效果如何，是否可以有效平衡数据自由与数据安全的价值取向等问题结论并不明晰，需要在深入论证具体规则的基础上结合实践效果进行检验。

在数字经济时代，数据规则的国际化、协同化发展是数据治理的必由之路。当前，区域贸易协定已成为数据跨境规则发展的重要基石。RCEP 的全面生效为中国检视国内数据跨境立法、进一步完善数据跨境规则提供了有利机遇，也为中国输出数据跨境理念、掌握国际数据治理话语权提供了契机。分析 RCEP 数据跨境规则、梳理中国数据跨境立法现状，可有效审视二者之间的衔接

基金项目：文化和旅游部委托 2023 年度中央党校校级自筹课题“健全文化和旅游市场体系，推进治理体系和治理能力现代化”。

情况与不足。中国作为 RCEP 的主要倡议国，如何在“一带一路”的大环境下构建良好的数据跨境流动规制体系，并配套何种程序规则以平衡数据安全与经济发展？如何完善国内立法并增强与 RCEP 数据跨境规则的衔接性？这已成为当前中国建设数字“一带一路”、经营 RCEP 最需要思考的问题。当下，中国已正式申请加入《全面与进步跨太平洋关系协定》（CPTPP）、《数字经济伙伴关系协定》（DEPA）[3]。以 RCEP 数据跨境流动规则为导向，深入检视数据跨境立法，有助于积累国内立法与区域贸易协定有效衔接的立法经验，为中国后续加入 CPTPP、DEPA 等区域贸易协定注入新动力，并提高数据治理的高效化。

## 二、RCEP 数据跨境流动规则及困境

当前，RCEP 已形成合作共治的数据跨境模式，也面临各参与国间数据跨境治理理念差异大、RCEP 数据跨境规则设计涵括导致的数据闭塞现实困境，这将有可能造成与中国数据跨境立法衔接的不洽性，亟待探索解决思路。

### （一）RCEP 数据跨境流动规则：“有条件的数据跨境 + 合作共治”模式

数据跨境流动监管可归纳为三种方式：国家干预、本地化存储、数据本地化豁免 。RCEP 数据跨境治理规则主要是对国家干预及本地化存储两种规制方式的贯彻。具体而言，RCEP 在支持数据跨境流动自由的基础上，重视国家安全与公共利益的维护，不排除非歧视性数据本地化存储的措施，这一核心特点既体现了国家干预，又体现本地化存储规则。在数据本地化豁免方面，目前 RCEP 未参照欧盟 GDPR 制定“白名单机制”，这与 RCEP 参与国数字技术发展水平偏低有着密切关联。但在 RCEP“鼓励数据跨境流动自由”理念的影响下，也展现出数据本地化豁免的情形，例如第十二章第 14 条、第 8 章服务贸易附件一第 9 条等 [4] 。不过，RCEP 数据本地化豁免制度的适用多以“公共政策”“安全利益”等例外条款为补充，这将对数据跨境的实际效果造成影响。

当前，RCEP 数据跨境流动规则已形成“有条件的数据跨境 + 合作共治”的特有模式。主要体现在 RCEP 支持高度自由的数据跨境流动理念，但也接受参与国可以基于对公共政策或国家基本安全利益的保护而采取一定的数据流动限制措施，这是顺应数据自由流动趋势与国家自身利益保护的融合表现。例如 RCEP 第十二章第 14 条规定禁止以数据本地化作为贸易条件，第十二章第 15 条重申支持参与国为保护基本安全利益与实现公共政策对数据进行限制的例外情形。由此可知，RCEP 给予了参与国充分的管理数据的自主权。RCEP 未对参与国针对数据的非歧视性监管作出较多限制，通过例外条款的设置，使参与国对数据流动的监管与控制仍保留较大的权力。

### （二）RCEP 数据跨境流动规则的困境

现行 RCEP 跨境数据流动规则是区域贸易协定中数据跨境治理的新样态，有一定进步之处，但也使 RCEP 面临数据跨境规则与数字经济快速发展不适应的困境，究其缘由主要来自宏观数据理念与微观规则设计两方面。

宏观层面：各参与国数据治理理念差异造成数据跨境的实际障碍。由于各参与国科学技术发展水平、政策文化等具有差异，现已形成数据理念差别较大的事实，导致各参与国间制定和使用的数据跨境流动法律规则的差别显著，无法形成成熟一致的国际标准。此外，受不同数据理念的影响，参与国出于对国家安全、个人隐私安全、数字技术能力等多方面考量，对数据流动自由度标准也不统一，容易造成数据流动的闭塞，影响经济发展。

微观层面：RCEP 的数据跨境立法设计较为“涵括”，“例外条款”的模糊容易造成数据闭塞。RCEP 数据跨境规则在规则设计上的“涵括性”，虽给各参与国发展国内数据跨境立法留下了较大空间与法律接口，但 RCEP 在推进“有条件的数据跨境流动”的同时还设置“例外条款”，在赋予参与国基于“国家安全”等正当理由限制数据跨境自主决定权的同时，可能产生不当使用的风险。当前 RCEP 数据跨境例外条款已受到学界质疑，有学者指出 RCEP 数据跨境例外条款较为宽松的设置有可能造成该条款被滥用的后果 [5] 。例如 RCEP 一般例外中“合法公共政策”的表述就有待细化，RCEP 只规定各参与国可根据“合法公共政策”目的限制数据跨境，却欠缺针对“合法

公共目的”的定义。只设置例外条件而忽略对例外条件的必要解释，极易造成各参与国对条款解释的泛滥。虽然 RCEP 还对应设置“非歧视以及不超过必要限度”的补充规定，但鉴于例外条款的内涵不清，相关必要限度的要求也极易落空。

以上问题给形成统一、有效、稳定、适用性强的数据跨境法律规制体系造成障碍，逐渐使 RCEP 数据跨境流动进入治理困境、面临较多弊端。当前，中国作为 RCEP 的主要倡议国，已经丰富了数据跨境领域的国内立法，并不断做出动态调整，这为 RCEP 数据跨境规则提供了中国理念与完善思路。中国在数字立法领域的实践是输出中国数字理念的有效举措，以 RCEP 为视角科学审视中国数据跨境规则，是帮助中国后续加入 CPTPP 和 DEPA 等数字协定的有意义尝试。另外，将 RCEP 数据跨境规制与中国相关国内立法紧密对接，形成二者交互发展之势，是破解 RCEP 数据跨境困境的有益之策。

## 三、中国数据跨境流动的法律规制框架及困境

现今中国有关数据跨境的立法包括但不限于《网络安全法》《数据安全法》《个人信息保护法》，在“三部法”中，以后两部法律为典型，并以《关键信息基础设施安全保护条例》《数据出境安全评估办法》等为补充，共同构成中国数据跨境规制的法律框架。以《网络信息安全管理条例（征求意见稿）》为先例，2023 年 9 月 28 日，国家互联网信息办公室（“网信办”）发布《规范和促进数据跨境流动规定（征求意见稿）》（以下简称《规定》），向社会公开征求意见。此举是中国在维护国家安全、个人信息权益的基础上对推进数据跨境自由做出的最新尝试。目前，中国数据跨境立法体系已基本形成。

### （一）中国数据跨境流动的规制模式与不足

当前中国数据跨境规制的法律框架针对不同类型、不同级别的数据设置了差异化的数据出境监管要求。数据的跨境规制正呈现出精细化、科学化的监管模式，形成了以重要数据、个人信息为基本分类，以安全评估、标准合同、专业认证等制度为具体规制方式的数据跨境流动监管体系。

1. 重要数据跨境流动的规制模式。中国对重要数据尚未给出明确定义，参考《个人信息和重要数据出境安全评估办法（征求意见稿）》《数据出境安全评估指南（征求意见稿）》《重要数据识别指南（征求意见稿）》等相关条款，重要数据的核心特征应与国家安全、公共利益密切相关。《网络信息安全管理条例（征求意见稿）》明确将数据分为核心数据、重要数据和一般数据三个基础类别[6]，重要数据与核心数据的关系应为包含与被包含关系，重要数据中特别重要、关系到国民经济命脉、重大公共利益的数据为国家核心数据，以此形成对个人信息和重要数据进行重点保护、对核心数据保护应更加严格的数据跨境监管理念[7]。这是数据分级分类保护体系的雏形。

依据数据处理者的不同，重要数据的跨境流动规制程度也有所区别。实践中，重要数据处理者主要分为一般数据处理者和关键信息基础设施运营者两种数据处理主体。针对一般数据处理者，《数据出境安全评估办法》第 4 条规定一般数据处理者若向境外提供重要数据，应当通过所在地省级网信部门申报数据安全评估。由此可知，中国已确立了适用于一般数据处理者的“以数据安全评估为前提”的重要数据跨境流动规制模式。针对关键信息基础设施运营者，《网络安全法》第 37 条、《数据安全法》第 31 条规定关键信息基础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，确因业务需要向境外提供时，需进行数据安全评估。由此可知，中国对于关键信息运营者的重要数据出境监管采用“原则上本地存储 + 跨境前数据评估”的规制模式，较一般数据处理者的重要数据跨境监管更为严格。

虽然重要数据跨境流动监管分类清晰，各自监管框架也较为明确，但现实中由于重要数据核心概念不清、重要数据清单不明已经导致政府部门的监管范围过大、企业数据跨境的合规压力较强等弊端。另外，针对重要数据的安全评估指标也应细化，为数据处理者的风险自检、相关部门的数据出境审核提供确切指引。《规定》第 2 条限缩了重要数据的出境限制，规定只有被明确标识为“重要数据”的数据，才需要进行数据出境安全评估。此举鼓励了非重要数据的跨境流动，也对尽快出台重要数据目录清单、重要数据安全评估细则提出了要求。

2. 个人信息跨境流动的规制模式。《个人信息保护法》为规制个人信息跨境流动提供了基本模板，《个人信息保护法》第 38 条确立了以信息主体同意为基础，以安全评估、个人信息认证、标准合同文本和其他举措四方式之一为跨境前提的个人信息跨境流动机制。在此基础上，该法第 40 条将关键信息基础设施运营者和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作为个人信息跨境的特殊主体，明确对于由两类特殊主体收集和产生的个人信息出境监管采用“原则上本地存储 + 跨境前数据评估”的规制模式。2022 年 9 月施行的《数据出境安全评估办法》第 4 条第 2、3 款对《个人信息保护法》上述条款进行细化，明确了以信息处理者重要性与处理个人信息具体体量为指标的特殊主体。规定关键信息基础设施运营者、处理 100 万人以上个人信息的数据处理者、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，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。同时，为避免个人信息处理者规避数据出境安全评估的强制性规定，《个人信息出境标准合同办法》专门规定个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。《规定》对个人信息的跨境设置了更为具体的监管豁免情形。

由此可知，依据个人信息处理主体、出境原因的不同，对个人信息的跨境监管也呈现不同的标准。相较重要数据主要依托数据安全评估作为跨境前提，个人信息的跨境前提展现出多样化的特点。然而，特殊主体处理的个人信息跨境仍需经过数据安全评估，这更凸显了数据安全评估机制的重要性。在数据跨境传输领域，数据安全评估机制是以防御国家安全风险为目的、以监管机构的实质审查为主，对跨境数据进行的全面事前评估，其对数据跨境监管存在着特殊意义。数据安全评估机制应依托详细、科学的评估细则，为数据跨境的安全提供保障。目前，中国数据安全评估体系不断完善，但具体的指标亟待优化。

（二）中国数据跨境流动法律规制框架的现有困境

当前中国数据跨境立法已有新进展，有关数据跨境立法呈现渐进发展趋势。以“三部法”为基础，近年来《数据出现安全评估办法》《规定》等陆续出台，不断细化数据跨境的安全评估与监管规则。在数据跨境监管中，科学的数据分类分级模式是数据安全治理的前提，也是数据合规中最核心的部分，但目前中国在此领域的问题较为凸显。

首先，缺乏明确的数据分级分类标准。虽然《网络信息安全管理条例（征求意见稿）》将数据分为核心数据、重要数据、一般数据三个基础类别，但在实践中却以重要数据、个人信息作为基本监管指标，存在现实监管的冲突。为缓和重要数据不明确的问题，目前中国实行各行业地区自行确定重要数据等目录清单的方式，以满足不同行业对于数据的监管。但囿于上位法未清晰界定重要数据等概念，造成数据分类依据、分级标准并立的现状，使各地区、各行业的分类分级体系并不统一，使中国数据跨境监管更为混乱。

其次，面临由于数据安全评估的具体指标不明造成的数据跨境流动监管形式单一问题。《网络安全法》《数据安全评估办法》等虽然确立了数据本地化存储与数据出境安全评估相结合的监管方式[8]，但立法尚未能结合数据跨境流动的具体情形与种类等进行多层次、差异化的监管设置，没有具体的分类监管而将安全评估作为数据出境的必经程序，可能会极大压缩数据流动空间，难以满足企业日益增长的数据跨境流动需要，也不利于 RCEP 区域经济的联动发展。

## 四、RCEP 数据跨境规则与中国数据跨境立法的冲突

由于各国数据跨境理念差异和 RCEP 数据跨境规则中例外条款设计的“涵括”已形成 RCEP 数据跨境闭塞的现实困境，这与 RCEP 所提倡数据跨境自由的宗旨不相符。与之相对，伴随中国数据跨境立法的不断发展，中国数据跨境理念虽已逐渐从“保守型”转变为“开放型”，但仍欠缺以重要数据为核心的数据分类分级标准和数据安全评估指标，致使数据跨境流动监管形式单一，

实际监管效果不理想。由此可见，无论是中国还是 RCEP 数据跨境困境，其困境来源均是数据跨境理念和具体规则设计，本质属于现有规则与数据跨境理念的不适配。形式上，中国数据跨境理念已基本符合 RCEP 规则中所提倡的数据跨境自由，中国数据跨境监管规则也基本符合 RCEP 的数据跨境要求，部分数据的境内存储顺应 RCEP 规则中“例外条款”的适用。但实质上，RCEP 的数据跨境规则较同类其他区域贸易协定更加保守，RCEP 数据跨境的实际理念是较为封闭和折中的，这与中国逐渐确定的“开放型数据跨境理念”相冲突。此外，RCEP 并未形成统一的数据跨境监管方式，其规则设计非常简化，这与中国逐渐完善的数据跨境监管框架亦产生冲突。以上两方面共同形成了 RCEP 数据跨境规则与中国数据跨境立法衔接的具体冲突点，具体分析如下：

（一）在数据跨境治理中，RCEP 数据跨境理念与中国立法理念存在偏差

RCEP 实施“有条件的数据跨境 + 合作共治”模式，运用“例外条款”的立法设计突出各参与国在数据跨境流动领域的自主权。RCEP 模式针对数据跨境的规制本质上仍然依靠各参与国对“例外条款”的理解，虽也辅之“促进数据流动”的相关规则，但数据的实际流动效果却不显著。RCEP 依靠各参与国对数据跨境的妥协，极易导致数据的跨境结果具有相对性。当各参与国均寻求数据跨境的同等待遇时，那 RCEP 本身的数据跨境促进规则便形同虚设，使 RCEP 规则设计与旨在“促进区域数据流动与经济发展”的区域贸易协定理念存在矛盾。就中国当前数据治理理念而言，已较传统的“数据本地化存储 + 数据出境安全评估”的数据跨境监管模式更为开放。新发布的《规定》证明中国开始在数据跨境领域致力于促进“数据流动自由”、发掘数据背后的经济价值，这将与 RCEP 保守的数据跨境流动效果存在冲突。伴随 RCEP 的全面生效以及中国数据跨境规则的不断发展，理念的分歧带来的困境会更加突出。

（二）在数据跨境监管领域，RCEP 监管规则与中国数据监管框架不匹配

在 RCEP 数据跨境规则设计之初，在兼顾数据流动自由与数据安全理念指导下，RCEP 并未明确具体的数据跨境监管规则，仅创造性提出“安全例外条款”使参与国实际获取数据跨境的“自主权”以满足各国的国家安全需求。但综观现有区域贸易协定，对数据跨境的规制不宜太过简化，应设计能够舒缓“例外条款”适用弊端的灵活跨境监管方式，充分发挥自由贸易协定的便利性与高效性。考虑中国不断丰富数据跨境监管规则的事实，这本可为 RCEP 数据跨境监管的完善提供可行之策，但目前因缺乏国家层面清晰的“数据分级分类”标准与数据出境安全评估机制两个核心内容，致使中国与 RCEP 相衔接的数据跨境监管框架缺失，无法向 RCEP 各参与国输出可行、有效的数据跨境监管方案。这就造成了 RCEP 数据跨境制度与中国数据跨境立法缺乏衔接性，不利于 RCEP 数据跨境规制的完善。对于这一主要问题，应以细化中国国内的“数据分级分类”标准、健全数据出境安全评估机制为逻辑起点，重点建立适用于 RCEP 的数据跨境监管规则。

RCEP 作为大型区域贸易协定，考虑各参与国数据理念的差异，其数据跨境规则的设计较为保守、折中，目前已不适应数据自由流动的国际趋势。就中国国内立法而言，其数据跨境理念已呈现开放趋势，但现实规则无法满足数据跨境自由的要求，关键弊端在于数据跨境重要指标的不明确。RCEP 数据跨境规则的完善需要依附各参与国的共同努力，但更需要科学、精准的监管方式。中国作为 RCEP 的重要参与国，应积极创新自身数据跨境监管体系，并向 RCEP 输出数据治理方案，以缓解二者间在数据跨境规制领域的冲突。考虑目前中国的核心问题在于欠缺数据分级分类标准进而影响数据安全评估体系的运行，因此解决数据跨境规则的冲突需要从数据分级分类标准入手，建立有效运行的数据分级分类体系，并加以设计适用于 RCEP 的多元化、灵活性监管路径。

## 五、RCEP 视角下中国数据跨境规则的完善路径

在数字高速发展的时代背景下，数据跨境是世界经济发展的必然趋势，但如何有效促进数据跨境自由与安全的平衡，将是优化数据跨境规则的

重要思考路径。中国在面临 RCEP 的数据跨境规则时，如何解决二者立法衔接性不强这一问题是重中之重，不仅需要国内立法的完善，更需要 RCEP 数据跨境规制的改进。笔者认为，从中国角度审视 RCEP 数据跨境机制的完善方向，最关键的优化点是建立统一的数据出境分级分类机制，尽快明确数据的分级分类标准。尤其针对重要数据，需要中国尽快公布具体的评估指标，再配套监管机构督促实行[9]。随后中国应积极推动该监管机制适用到 RCEP 数据规制体系中，成为保障各参与国国家安全、个人隐私权利以及国家利益的有力举措。

（一）标准层面：推动建立重要数据出境分级审核体系

《网络安全法》从数据的重要性着手，规定只要涉及国家数据就属于重要数据[10]，并明确了重要数据本地化的要求。参考中国《网络信息安全管理条例（征求意见稿）》分类标准，结合《关键信息基础设施安全保护条例》等相关规定，可知中国对重要数据、个人信息两类需要被重点监管的跨境数据已有初步认定标准。尤其在个人信息领域，中国以数据处理者的量级、数据处理者的种类作为数据安全评估的认定标准，较重要数据的界定更为明确。因此笔者将着重选取重要数据进行立法完善，对相应审核机制予以构思。

1. 确立重要数据分级分类标准。重要数据是指具有高度关键性，对国家安全、个人隐私等方面极易造成威胁的数据类型，它不仅包括重要商业数据、个人敏感数据、国防数据、政府数据、特种行业等，还应包括可以推断和计算出国家安全、科技、军事、社会等现状的敏感数据。当下这样的涵括使重要数据的范围泛化，但也是必要的考虑。伴随中国数据跨境理念向着更为开放的方向发展，这使缺乏重要数据目录清单和具体认证标准成为阻碍数据跨境高效监管的突出问题，需要被解决。虽然国家网信办在《规定》第 2 条中明确只有被标识为“重要数据”的数据，才需要进行数据出境安全评估，以此缓解由于重要数据界定不清造成的合规压力，但本质上仍是治标不治本。针对重要数据的认定，中国目前采取分地区、分行业的自行认定规则，但参考美国缺乏统一隐私法造成各州、各行业监管标准混杂化的历史经验[11]，笔者认为应尽快统一重要数据认证标准，制定国家层面的目录清单是优化之策。笔者认为当下成立重要数据安全评估中心十分必要，以此为契机推动中国尽快明确重要数据跨境流动安全评估的流程与具体标准，运用多因素评价、计算等方式预测何种数据会给国家安全、公共利益造成潜在的风险与威胁，以此为依据有效监管重要数据的跨境流动。此外，还可根据风险等级对重要数据进行分级排序，为国家网信部门的数据出境安全评估提供指引。

数据自由跨境需要以“充分保护”作为前提，如果一味推崇数据跨境的自由会给国家安全造成极大风险。美国一贯崇尚数据流动的自由理念，但对国家安全的维护也是颇为重视，对于可能影响国家安全的重要数据严格限制出境。由此可见，数据跨境的自由与国家安全的维护并不冲突，国家安全必须高于数据跨境的自由度。当前，针对重要数据的跨境流动规制，中国应继续坚持严格管理的政策理念，伴随数据安全评估机制的建立，同步推行重要数据分类明细出台。在此基础上，才能将成熟的重要数据分级分类机制逐步推广到 RCEP 体系中，为各参与国提供统一参考，也将在一定程度改善参与国数据限制标准不统一的情况。

2. 建立灵活的数据跨境监管体系。考虑重要数据在跨境过程中面临的复杂影响因素，中国可根据数据安全评估机构的设立，出台重要数据分级审核监管体系并推广到 RCEP 数据跨境规则中。首先，可参考欧盟 GDPR 的“白名单机制”，以 RCEP 为视角对数据跨境流动设置前提性条件，明确重要数据双向流动的前提是相对国家或地区的数据保护水平达到中国认定的标准。但是，以 RCEP 为视角审视中国化的“白名单机制”便会发现一个问题，即中国为 RCEP 所设定的跨境流动前提性条件能否适用于全部参与国。考虑到 RCEP 参与国数据保护水平不统一的现实因素，这一潜在风险尤为突出。如果中国针对 RCEP 设计的“白名单机制”无法对所有参与国适用，就无法形成 RCEP 统一的数据跨境规制机制，最终不可避免使该标准流于形式，事倍功半。所以，中国针对 RCEP 数据流动“白名单机制”的设计不可简单罗

列认证标准，需将刚性与活性标准配合施行，此为因应之策。具言之，一方面可在综合考察所有RCEP 参与国实际情况的基础之上明确统一的“最低标准”，另一方面可配合“标准合同”等形式，根据不同国家的不同数据监管情形，补充设置其他前置性条件[12]。具体监管方式设计如下：以保障国家安全与公共利益为前提，对相对国的数据保护水平等事宜进行具体化考察与评估，将数据跨境的前提性标准分为“刚性标准”“活性标准”两类。其中，刚性标准是综合 RCEP 全部参与国数据安全发展的基本情况，包括数据安全维护能力、国内法政策等综合制定完成，对 RCEP 的各参与国通用。相对应，活性标准则是综合分析国与国间的单个数据跨境因素，包括跨境数据的性质与类型、数据跨境原因等予以确认，只对跨境相对国适用，具有特定性，也较刚性标准灵活。其中，对于具有特定性的“活性标准”，笔者认为可给予企业较大的数据跨境自由。基于此举措的落实，在 RCEP 数据跨境机制运营中，中国可尝试应用以企业自治为主、国家监管为辅的数据规制模式，更好释放 RCEP 经济活力。但是，此种方式需要对数据跨境标准进行综合评估，考虑到活性标准的相对性与不确定性，这一问题的最终解决还需依靠 RCEP 各参与国间的实际交流与经验总结。

最后，数据跨境的充分性条件与数据审查的衔接仍是当前需要重点关注的部分。对于重要数据的审查是分级审核制的重要步骤，工作繁杂，体系庞大。因此中国有必要允许第三方专业机构的适度参与，对数据出境进行安全评估与详细论证，为网信等有关部门提供参考。此外，第三方机构还可以行业规制为基础，对企业内部的数据安全定期开展考察评估，督促企业的数据治理能力提升。以第三方机构的适度参与协助网信部门完成数据的分级和审核一体化内容。为缓解工作压力，有关部门在监管过程中可以行使审查与实质审查结合的方式完成对非重要数据的审核，其中实质审查可以具有随机性，但应贯彻数据跨境的全过程。

（二）立法理念：借鉴域外立法理念，推进 RCEP 立法统一

当前，针对数字时代下的数据跨境，中国已开始形成法律规制体系，但仍存在立法较为分散的情况。未来伴随数据保护水平的继续提升，中国可以考虑借鉴欧美立法经验，如美国国内立法与国际法的高度衔接性以及欧盟立法的创新性特点[13]。一方面，就美国数据立法模式来说，其最大特色就是国内法与国际法的高度衔接性。例如，美国自由主义数据理念表现在诸多方面，就美国互联网企业的发展模式而言，国内立法对互联网企业约束限制较少，对接国际规则便表现为美国政府主张的数据跨境流动自由，也正是国内、国际立法的完美对接，才使得美国互联网行业得到飞速发展。因此，中国可以适当借鉴美国立法经验，努力与国际立法相衔接。在 RCEP 数据跨境体系的完善中，中国应充分考察 RCEP 的数据跨境环境，形成与之相适应的国内立法。对于数据的国内立法不能仅局限于泛而空的指导性规定，更应细化落实，并与 RCEP 数据跨境背景相统一。

而欧盟的立法的及时性也成为欧盟数据立法的显著特征，2016 年，欧盟率先通过 GDPR，以此统一欧盟市场的数据准入标准，随后 GDPR 也推动世界数据立法的潮流。近年来，欧盟通过多个数字法案，强化针对数据跨境的治理以发展自身数据立法。正是欧盟及时立法创新的举措，使得欧盟率先确立数据流动“充分性保护”的评估权，通过区域贸易协定不断拓展数据流动的范围，在一定程度上扩大了欧盟在国际社会的影响力。综上，中国可借鉴美国、欧盟的立法经验，以完善 RECP 数据法律规制为契机，积极探索国内立法与 RCEP 立法的结合，以国内立法导向推动 RCEP 数据规则的完善。当前正处于数据跨境流动规则制定的关键期，已基本形成以欧盟和美国各自引领的数据立法，但这两种数据立法体系均是以发达国家为主导的，对于发展中国家并不适用。而 RCEP 却是以发展中国家为首，这与欧美式贸易环境截然不同。对于 RCEP 的数据立法也正是中国需要重点把握的良好契机，通过推动 RCEP 数据立法的统一，把握世界数据发展方向，扩大中国在数据立法上的世界影响力。

（三）技术层面：加强 RCEP 数据安全技术保障

由欧盟、美国的最新立法进展以及区域贸易协定中数据治理的强化可知：加强数据安全的技

术保障是数据跨境流动自由的又一前提。数据安全技术的加强有利于国家通过相应技术手段预防、限制数据的非法跨境并且充分应对突如其来的网络攻击，以防数据泄露。对于RCEP数据跨境来说，中国应重点强化网络安全技术，以有效应对网络安全事件的发生，防止数据的泄露、丢失和损坏。并且在数据威胁发生后，能够积极采取补救措施用以阻断或者拦截数据的传播，通过有效措施降低数据丢失的损害和风险[14]。其实，数据跨境保护的最主要举措还是从源头以及跨境传播过程中强化对数据的监管。中国应鼓励RCEP参与国网络安全技术或者信息的共享，全面提升参与国的网络技术水平，这也能够在技术源头推动数据的自由流动，以实现RCEP经济协同发展的目的。

数字科技的发展孕育数据传播的新形式，提升了数据跨境的效率与速度，在缩短国与国间贸易距离的同时，为世界经济发展注入了新鲜动力。如何达到数据保护与数据自由的良性平衡是当今世界共同的难题。针对数据跨境的法律规制，近年来中国以保障数据安全为前提，在重要数据、个人信息出境规制领域不断创新，但尚欠缺数据分级分类监管的具体标准、缺乏详细的数据安全评估细则，导致与RCEP数据跨境规则的接洽性不足。RCEP作为中国参与的大型区域贸易协定，为中国建立适用于发展中国家的数据立法提供了条件与思路，是中国紧握数据立法国际话语权的重要契机。未来，RCEP数据规制体系有望成为数字丝绸经济建设的重要部分甚至“风向标”。但就目前来说，RCEP数据跨境规则与中国数据跨境立法均需完善，以欧美数据跨境立法范式为参考，以衔接RCEP与中国数据跨境立法为目标，从数据标准、立法理念、技术保障等方面提升数据安全性、扩展数据跨境流动自由度，是完善国内数据跨境立法体系进而推进RCEP数据跨境治理的合理进路。以此为契机，有助于中国持续向世界展示数据治理“中国智慧”与“中国方案”。

**参考文献：**

[1] RCEP对15个签署国全面生效[EB/OL]. 载中国商务部自由贸易区服务网，http://fta.mofcom.gov.cn/article/fzdongtai/202306/54037_1.html，2023-06-05.

[2] 习近平.携手推进“一带一路”建设——在“一带一路”国际合作高峰论坛开幕式上的演讲[N].人民日报，2017-05-15.

[3] 商务部.将积极推进加入CPTPP和DEPA[EB/OL].中国一带一路网站，https://www.yidaiyilu.gov.cn/p/0V7DADBD.html，2023-10-10.

[4] 徐伟功，贾赫.RCEP背景下跨境数据流动治理规则比较研究与中国方案[J].广西社会科学，2022，（12）：62-69.

[5] 杜玉琼，罗新雨.RCEP数据跨境流动规则例外条款的适用及中国应对[J].四川师范大学学报（社会科学版），2023，（5）：75-83.

[6][7] 网络数据安全管理条例（征求意见稿）[Z].2021：第5条，第37条.

[8][10]《中华人民共和国国家安全法》[Z].2016：第37条，第35条.

[9] 王志杰.论我国跨境数据流动的监管完善——基于数据安全性与数据开放性的利益平衡视角[J].福建金融，2021，（7）：9-16.

[11] Joshua M. Wilson, Cross-Border Data Transfers: A Balancing Act through Federal Law, 6Bus. Entrepreneurship & Tax L. Rev. 150 (2022).

[12] 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[J/OL].重庆大学学报（社会科学版）：1-15[2023-10-16].http://kns.cnki.net/kcms/detail/50.1023.C.20210826.1451.002.html.

[13] 翁国民，宋丽.数据跨境传输的法律规制[J].浙江大学学报(人文社会科学版)，2020，(2)：38-53.

[14] 朱扬勇，熊赟.数据跨境监管初探[J].大数据，2021，（7）：135-144.

作者：张学博，中共中央党校（国家行政学院）政治和法律教研部民商经济法室副主任、教授
王智韬，中共中央党校（国家行政学院）博士研究生

责任编辑：钟晓媚