Dispute Settlement 争议解决, 2023, 9(5), 2364-2373
Published Online September 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.95321

Hans汉斯

DEPA数据跨境治理规则研究与我国的制度衔接

陈思莹，富灵琳，徐　钲

华东政法大学国际法学院，上海

收稿日期：2023年8月9日；录用日期：2023年9月3日；发布日期：2023年9月12日

摘　要

在数字经济时代，数据的战略地位越发凸显，世界各国和各区域贸易协定纷纷规定了符合自身利益的数据跨境治理规则，以规范和有序促进数字经济贸易的发展。随着RCEP、CPTPP和DEPA等的签署推进，我国也正积极推进加入DEPA。然而我国国内数据治理规则与DEPA相关的数据跨境治理规则有着一定出入，若要更顺畅地推进我国的加入签署进程，则我国需要明晰国家安全概念的内涵外延和规范表达，进一步构建系统性的数据管理制度和统一的中央数据监管机构，同时鼓励我国企业加入数据保护可信任标志体系并促进监管互认；如此将利于完善数字治理框架体系和关键性规则安排，建立健全数据要素市场规则、进一步打通数据资源要素的自由流动，更好促进我国数字经济贸易的高质量发展。

关键词

DEPA，数据跨境治理，数据监管，可信任标志

Research on DEPA Data Cross-Border Governance Rules and China’s Institutional Convergence

Siying Chen, Linglin Fu, Zheng Xu

International Law School, East China University of Political Science and Law, Shanghai

Received: Aug. 9th, 2023; accepted: Sep. 3rd, 2023; published: Sep. 12th, 2023

Abstract

In the era of digital economy, the strategic position of data has become more and more prominent,

文章引用: 陈思莹, 富灵琳, 徐钲. DEPA 数据跨境治理规则研究与我国的制度衔接[J]. 争议解决, 2023, 9(5): 2364-2373.
DOI: 10.12677/ds.2023.95321

and countries around the world and regional trade agreements have stipulated data cross-border governance rules in their own interests to regulate and orderly promote the development of digital economy and trade. With the signing of RCEP, CPTPP, DEPA, etc., China is also actively promoting its accession to DEPA. However, there is a certain discrepancy between China's domestic data governance rules and data cross-border governance rules of DEPA. If we want to promote our accession and signing process more smoothly, we need to clarify the connotation and standardized expression of the concept of national security, and further build up a systematic data management system and a unified central data regulatory body. At the same time, China may encourage Chinese enterprises to join the data protection and trust mark system to promote mutual recognition of regulation. This will be conducive to the improvement of the framework system of digital governance and the key rules and regulations, and to the establishment of sound market rules for the elements of data, further opening up the free flow of data resources and elements, so as to better facilitate the high-quality development of China's digital economy and trade.

Keywords

DEPA, Data Cross-Border Governance, Data Regulation, Trust Marks

1. 引言

数字经济时代，数据作为战略资源和关键生产要素，已经超越传统的跨国投资和贸易，成为推动全球经济发展的重要力量[1]。在此背景下，围绕数据跨境流动产生的国家利益博弈日益激化，TikTok 被美国封禁、滴滴出行赴美上市引发数据安全风险，日趋复杂的数据跨境流动趋势，难免对我国在跨境贸易、企业跨境上市中的数据流动造成困难[1]。为回应全球范围内崛起的跨境数字贸易、有序推动数字经济发展，《区域全面伙伴关系协定》(Regional Comprehensive Economic Partnership，简称 RCEP)、《全面与进步跨太平洋伙伴关系协定》(Comprehensive and Progressive Agreement for Trans-Pacific Partnership，简称 CPTPP)、《美墨加协定》(The United States-Mexico-Canada Agreement，简称 USMCA)等各类涉及数字经济贸易的国际协议如雨后春笋般涌现。由新加坡、智利、新西兰三国于 2020 年 6 月 12 日线上签署的《数字经济伙伴关系协定》(Digital Economy Partnership Agreement，简称 DEPA)是首个专门针对数字贸易规则进行规定的全球性数字经济协定规则，2022 年 8 月，中国加入 DEPA 工作组正式成立，全面推进中国加入 DEPA 的谈判。

而目前，我国保守的数据规则导向和分散的立法与 DEPA 所倡导的数据自由流动和限制国家自主监管权有所差距。本项目通过对 DEPA 协定第 4 章内容及 RCEP、CPTPP 两个协定中有关数据跨境规则的串联分析，比较国外代表性国家跨境数据治理模式，从国内现有法律、法规和规范性文件出发，研究数据治理和数据跨境规制在我国的兴起过程与发展趋势，从中寻找总结出国内规则与国际规则相衔接存在的现实问题，分析 DEPA 项下数据跨境的国家自主监管权权限问题、国家安全例外的适用问题，以及在实践层面现存制度碎片化、缺乏统一监督机构等问题；以期通过立法完善、有效监督、行业自律等方式，

[1]Kinsey Global Institute (MGI). Digital globalization: The new era of global flows. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.pdf, last visited at 17th Aug., 2023.

转变消极“守夜人”角色，平衡和消解跨境数据流动中的紧张冲突[2]。

2. 世界各国与区域性协定的数据跨境治理规则概述

(一) 主要国家数据跨境治理规则

美国模式：基于美国强大的数字经济贸易地位、数据技术保障与其国内众多大型数据公司的强竞争力，美国范式极力强调数据跨境的自由流动，以更好地利用数据要素这一资源，促进数据资源在其国内经济发展中的优化配置作用。比如在其自身签订的贸易协定如早前的《跨太平洋伙伴协定》(TPP)、《美墨加协定》(USMCA)和 TPP 的接续发展《全面与进步跨太平洋伙伴关系协定》(CPTPP)中，美国都极力推崇数据跨境自由流动规则之设立，以促进数据要素在世界范围内的自由流动[3]。

欧盟模式：《通用数据保护条例》作为欧盟在个人数据保护领域的保护盾，被称作全球最严格的数据跨境治理规则；由此欧盟范式更为重视个人数据权利保护和欧共体的数据安全主权。然而欧盟也推崇数据跨境的自由流动，不过限于欧洲共同体领域范围内，倡导欧盟国家内部间的数据自由流动和欧盟公民的个人数据权利保护[4]。

中国模式：2012~2021 年，我国出台了《信息安全技术数据出境安全评估指南》《中华人民共和国网络安全法》《数据安全管理办法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等不同效力等级的规则，治理模式基于较为保守的数据治理政策导向，一方面欲积极融入全球数字经济贸易和数据治理规则，一方面也担忧国内数据安全主权和国家安全利益因此遭受负面影响，目前暂时处于一种尴尬境地。

俄罗斯模式：重视国家政治和安全问题，坚持将网络数据安全作为国家主权的核心地位，较大程度上限制了数据跨境流动，以保障其国家数据主权的不可动摇性。

印度模式：关注数据给国内行业经济发展带来的社会效益，却尽力避免国内数字经济发展遭受“数据殖民主义”，预防发达国家如美国、加拿大等国以数据流动自由理念攫取其本国的数据利益。

澳大利亚模式：采取了更为折中的政策导向和立场，一边设有统一的数据监管机构，确保国内数据的安全处理和自由流动，另一方面设置了明晰的数据分级分类制度，对不同等级、种类的数据之跨境治理做出了不同的对应安排[4]。

(二) 主要区域协定数据跨境治理规则

RCEP：作为东盟主导的《区域全面经济伙伴关系协定》(RCEP)，是全球范围内较为重要的区域自由贸易区协定，也是我国加入的一个重要协定，其对数据跨境流动规则有着自身独特的规制特点，即在尊重国家数据主权的基础上，允许数据跨境自由流动，同时设置了国家安全例外条款，与我国国内现行规则的政策导向较为吻合。

CPTPP：与美国模式较为接近，美国、日本等国在其中发挥着积极引领作用，倡导数据跨境自由流动，对国家的自主监管权有着一定程度限制，适用国家安全例外条款的情况较为严苛，与我国目前数据治理的政策导向有一定冲突，我国目前正处于加入 CPTPP 谈判中[5]。

DEPA：同时作为 CPTPP 加入国的新西兰、智利、新加坡三国，主导着首个也是暂时专门针对数字贸易规则进行规定的全球性数字经济协定规则《数字经济伙伴关系协定》(DEPA)，该协定同时吸纳了 CPTPP 中限制国家自主监管权的导向，意图倡导全球性数据跨境治理规则之体系构建，我国目前也正处于加入谈判中[6]。

以下表格是上述提到的世界若干代表性国家与区域性协定的数据跨境治理规则的整体概览(见表 1)。

Table 1. Data cross-border governance rules of some representative countries and regional agreements around the world
表 1. 世界若干代表性国家与区域性协定的数据跨境治理规则

数据跨境治理规则之不同模式	规则特征
美国模式	强调数据自由流动
欧盟模式	重视个人数据权利保护
中国模式	较为保守的数据规则导向
俄罗斯模式	坚守国家数据安全主权
印度模式	避免“数据殖民主义”
澳大利亚模式	折中政策导向之利益保护
RCEP 模式	国家安全例外条款宽泛
CPTPP 模式	倡导数据跨境自由流动
DEPA 模式	承续对国家自主监管权的限制

3. DEPA 核心规则与我国相关规则之对比

DEPA 作为首个专门针对数字贸易规则进行规定的全球性数字经济协定规则，对于未来数字经济贸易发展具有深远重大意义；而我国正在积极申请加入此协定，故十分有必要对 DEPA 核心规则和我国相关规则进行分析研究，以更好为我国相关规则的完善提出建议，以更好地促进我国加入或融入该协定规则，促使我国数字经济贸易更好地衔接上世界步伐。

(一) “数据安全”的概念差异

我国国内法对于“数据安全”概念的界定，是以总体国家安全观为基本立场的。根据《数据安全法》及《网络安全法》的规定，数据安全指的是：在必要措施的保障下，保持相关数据被有效保护与可合法利用的状态。从规范构造的角度上看，我国“数据安全”的概念与 DEPA 第 15.2 条所谓“基本安全利益(essential security interests)”“维护或恢复国际和平或安全(international peace or security)”存在两层面的差异。

1) 国内法“数据安全”的定义界定范围大于 DEPA 第 15.2 条

《数据安全法》第 21 条根据数据的重要程度与遭受非法攻击时的危害程度来对数据进行分级分类。不难发现，我国对数据安全的基本态度是：如果数据“遭到篡改、破坏、泄露或者非法获取、非法利用”，就会“对国家安全、公共利益或者个人、组织合法权益”形成危害，也正是为了维护上述个人、组织合法权益、公共利益与国家安全，我国立法建构了数据安全制度。易言之，在我国立法框架下，不同于单纯的“国家安全”含义，以数据为载体的“安全利益”还包括除“国家安全”以外的其他主体的安全利益，比如私主体的合法权益以及公共利益中的数据安全；而上述其他利益(尤其是私主体的合法权益)并非完全能被“合法公共政策”这一概念所囊括。

然而，相比于 RCEP 电子商务章节第 15 条明确在其数据跨境自由流动部分设置专门的安全例外条款，DEPA 沿袭 CPTPP 的立法模式，仅规定了一般安全例外，使其框架下的安全概念更加限缩。同时，在内容上，作为安全例外条款的 DEPA 第 15.2 条似乎并未将私主体的安全利益纳入其框架下。就其立法表达而言，私主体的数据安全很难称得上足以影响一国国家安全利益的“基本安全利益”，也很难涉及“国际和平与安全”。因此，我国监管机构对于私主体数据权益及涉及公共利益数据的安全监管似乎与 DEPA 相关规则存在差异，国内立法的监管权范围与 DEPA 协定框架下的概念范围并非完全对应。

2) DEPA 第 15.2 条对传统国际法意义上的安全概念进一步限缩

早在数据贸易兴起以及“数据安全”概念诞生之前，国际法的理论与实践已经对贸易法意义上的“国家安全”作出了划分与界定。DEPA 在很大程度上移植了传统国际法意义上的安全概念，但在借鉴的同时，DEPA 通过相关规则的调整对数据保护视阈下的“国家安全”做出了三个层次的限制：

一是 DEPA 没有赋予缔约方国家安全例外措施的自决权。虽然 DEPA 在定义一般安全例外的位置也使用了“其认为(it determines)”进行修饰，但上述规定也只能产生 WTO 现行规则的效果，即争端解决机制仍有权对一国的管制措施进行审查。与之相反，RCEP 第 15.3 条明确规定各缔约方不得对其他缔约方为保护国内基本安全利益所必需采取的措施提出异议。易言之，DEPA 框架下各缔约方有权对我国采取的限制数据自由流动的安全例外措施提出异议，这一受到争端解决机制管辖与审查的可能性对我国的监管与执法提出了挑战。如若其他缔约方对我国无涉国家安全的数据出境监管措施也提出异议，我国则需要承担关于个人、组织合法权益与公共利益构成“基本安全利益”的举证责任。

二是 DEPA 未在电子商务章节设置安全例外条款。不同于 RCEP 在电子商务和例外规定章节中都设置了安全例外条文的做法，DEPA 仅在其例外章节规定了安全例外条款。可见在规则取向上，DEPA 认为缔约方的数据储存强制本地化与出境安全监管不一定可以构成安全例外，二者之间没有必然的联系[7]。反映到程序层面，我国并不能同 RCEP 一样援引数据跨境流动条款和数据本地化条款中的专门安全例外条款，而需转而论证监管措施与一般安全例外之间的相符性，这在一定程度上表明了 DEPA 对数据跨境流动限制措施的进一步收紧。

三是 DEPA 所规定的“基本安全利益”的具体内涵仍有待进一步廓清，尤其是其与“安全利益”的界分。从规范内容上看，DEPA 第 15.2 条(b)款未如 GATT 以及 RCEP 一样列举国家安全的例外情形。有学者认为 DEPA 不列举例外的具体情形使 DEPA 语境下的国家安全并不限于 GATT 限定的情形，是对 WTO 视阈下国家安全外延的扩张[6]，这也符合国际政治中部分国家泛化安全概念的现实做法。但也有学者提出相反意见，指出对原本 GATT 限定的情形进行模糊处理的规则反而会限缩国家安全的范畴[5]。学界的共识在于，应当加强对 WTO 争议解决制度下 DS512 等一系列涉国家安全的争端研究，明确“善意原则”对国家安全例外的限制原理与国内监管措施必要性的认定路径。

(二) 国内基础：规制的分散与监管的无序

当前我国对跨境数据规制的规范性文件覆盖了多层级、多方面，出台了有关法律、规章、司法解释近 70 余部，涉及网络数据安全、个人信息保护等全方位或专项的数据治理领域。从表面来看，以《个人信息保护指南》为开端，到《网络安全法》与《数据安全法》的出台，再到《个人信息保护法》的面世，我国数据规制体系不断完善，但是不同文件有不同的定义、表现形式、规制内容、执行方式，立法规章错综交杂，难以适用[8]。以数据跨境国内监管的数据本地化和出境监管两方面为例。在数据本地化要求方面，《个人信息和重要数据出境安全评估办法(征求意见稿)》第 2 条对数据跨境确立的宗旨是以境内存储为原则，向境外提供为例外，但《数据出境安全评估办法》基于中国的数据战略转向，在第 3 条中注入了“保障数据依法有序自由流动”的目标，对本地化原则有所松动，而在《个人信息保护法》第 36 条中，针对“国家机关处理的个人信息”却仍然要求境内存储。在数据出境监管的评估标准方面，根据《数据出境安全评估办法》第 4 条、第 8 条规定，是否需要申报的评估标准为数据量级、数据是否与国家安全和社会公共利益领域相关、是否是重要数据或敏感信息。《个人信息和重要数据出境安全评估征求意见稿》规定含有 50 万人以上个人信息即不再属于自评估范畴，《数据出境安全评估办法》则将这一数值规定“10 万人以上”，在实践中过高量级会导致数据安全评估的目的落空，过低量级则致使中小企业负担过重义务。概而言之，我国在数据跨境规则制度的建设上仍然处于初始阶段，现行的法律法规整体而言较为庞杂且过于碎片化，缺乏体系性和实践可执行性。

除了数据跨境治理规则的分散、重叠，我国目前还缺乏统一的数据分类标准和权威的中央数据监管机构。当前我国数以万亿计的跨境贸易规模带来了巨大的数据流动需求，商业数据、个人数据、公共数据等重要性不同的数据相互交错，立法未对数据进行有效识别而施以同等的保护，在一定程度上抑制了市场运行效率。而在法律、部门规章相互交错和缺乏统一的中央数据监管机构的情况下，不同的行政机构和管理部门在其跨境数据流动规制中所设定的管理机构多有错位，阻碍数据流动的“管多了”和应管不管的“没人管”成为潜在问题，相关管理机构的权力边界有待进一步厘清。比如在处罚机制方面，《个人信息保护法》第 66 条[2]所保护的“个人信息”和《数据安全法》第 45 条[3]针对的“开展数据处理活动组织所处理的信息”显然在范围上有所重叠，在二者效力位阶相同的情况下，适用哪一条规则、由哪个部门主导监督处罚、如何避免不同部门间的相互推诿也成为一个现实难题。又如在救济机制方面，《个人信息保护法》第 50 条虽然规定信息主体可以向人民法院提起诉讼，但将诉讼权利的行使限定在“个人信息处理者拒绝个人行使权利的请求”的情形中，而其他规章或规范性文件亦缺少可适用的救济途径，这样的救济机制显然不甚完善。

(三) 我国缺乏与 DEPA 衔接的数据保护可信任标志体系(DPTM)

DEPA 中 4.2 条的 6~10 款规定：要求促进不同缔约方不同的个人信息保护体制之间的兼容性和交互操作性，要求承认其他缔约国(对于数据的)监管结果、适当承认各自不同法律框架下的可信任标志或认证框架所提供的相当水平的保护、缔约方之间的个人信息转移的其他途径，且让缔约方鼓励各自的企业采用数据保护可信任标志，以促进缔约方之间的数据监管互认，以更符合 DEPA 促进数据自由流动的宗旨。然而可惜的是，我国暂无此数据保护可信任标志体系，只是有着自己国内的处理标准，并没有大范围鼓励我国企业加入数据保护可信任标志的认证体系。

作为 DEPA 创始国之一的新加坡，有着较为完备的、在全球范围内影响力较广的数据保护可信任标志体系，即 DPTM 认证体系。数据保护信任标记(DPTM)是企业范围内的一项自愿性认证，用于企业展示负责任的数据保护实践。DPTM 认证框架是根据新加坡 PDPA (《个人数据保护法案》)并使其与之相适应并结合国际基准和最佳实践的要素而制定的，这无疑也会极大程度地影响着 DEPA 的运作实践。我国目前尚无此独立的数据保护可信任标志体系，国内许多跨国企业也并未加入此认证体系；但华为最近获得了 DPTM 的认证标志，“该标志的取得，印证了华为对保护客户隐私保护的承诺，向客户展现了华为健全和负责任的数据保护措施，增强了客户对华为收集、使用和披露个人数据过程的信赖。”[4]因此我国可以鼓励国内企业使用数据保护可信任标志，或者是积极加入 DPTM 认证体系，为日后加入 DEPA 与其他缔约方的协商统一机制做好衔接准备，日后可以更高效、便捷地促进缔约方之间的数据安全自由流动。

[2]第六十六条：违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

[3]第四十五条：开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

[4]《华为获新加坡资媒局授予数据保护信任标志》，https://www.huawei.com/cn/news/2022/3/singapore-imda-award-huawei-data-protection-cert，最后访问日期：2023 年 8 月 18 日。

4. 我国加入 DEPA 之衔接对策

(一) 我国宜对“数据安全”具体外延作进一步的解释与调和

在我国对相关规定的解释与适用不够清晰的情况下，部分国家便有空间恣意解释乃至污蔑我国规则的立法本意。美国向 WTO 提交的《美国来文——中国就〈网络安全法〉已采取和起草中的措施》认为，我国监管政策扩大了数据跨境的监管对象，对于国家利益与社会公共利益解释过于模糊，并通过安全评估对数据跨境的自由流动设置了不当限制[5]。因此，在充分肯定 DEPA 赋予我国监管权和坚持数据主权原则不动摇的同时，有必要厘清数据安全概念，进一步解释我国数据安全评估流程与 DEPA 数据自由流动原则的相符性，以达成国家监管权与数据流动自由之间的范式平衡。

首先，应当对自由与开放的数据跨境价值理念予以重视和关切，处理好国内监管自主权与贸易自由化之间的互动关系。一方面，考虑到 DEPA 缔约方目前仅有新西兰、智利和新加坡，可以考虑设立“动态白名单”机制，通过互惠与认证制度同上述国家推动 DEPA 规则的实际落地，在遵守条约义务的同时保持我国现有数据出境安全审查监管的整体机制不做改变，避免相关监管措施构成不当限制。另一方面，中国应当进一步细化数据分类监管规则。《数据出境安全评估办法》第 19 条所指的“重要数据”，指的是一旦遭到篡改、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，往往涉及我国国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等国家安全事项[6]。我国国内法上的“核心数据”与“重要数据”都涉及国家安全，这种范围重叠、内涵模糊的分类方式极易使人产生扩大监管解释权的误读。故将非传统安全领域的所有内容全都解释为国家安全是不可行的，应将其分门别类地归入个人隐私、个人信息、商业秘密、公共利益的范畴进行区分保护，适用不同的规则。所以，应尽快出台更加细致的数据安全分级目录，允许普通数据的自由多元化的跨境传输，采取谦抑、克制的监管立场为境内企业开展跨境业务保驾护航。

其次，以最佳实践(best practice)交流为契机，坚持完善并审慎优化跨境数据流动安全监管体制。晚近自由贸易协定重视国内监管良好实践(good practice, better practice)在消除不必要障碍、减少各国监管差异以及促进监管合作与对等方面的积极作用[9]。DEPA 协定文本在多处提及了对于最佳实践的分享与交流，涉及无纸贸易、跨境物流、电子发票、数字身份、竞争政策合作、中小企业、数字包容性以及数据保护可信任标志八个方面。在我国整体上以坚持数字主权、维护数据安全为由进行安全审查的前提下，更应当提高监管实践措施的透明度，使我国的数据处境安全审查制度具备适用的可预测性与可操作性。在优化监管的同时，中国应当观测各缔约方国内监管措施对数字经济造成的消极或积极影响，考虑相关措施的成本与维护数据安全的效用，考量他国做法的借鉴意义。

最后，在遵守 WTO 相关案例“必要性标准测试”原则的同时，中国应当以利益平衡为基本观点，积极推动 GATS 安全例外规则适用的进一步发展与明晰。既然承认 DEPA 等数字经济协定的安全例外规则承继自 WTO 法律制度，就应当更加重视目前 WTO 安全例外规则的模糊性与不确定性，安全例外这一贸易法规则将为我国所实施的监管措施提供法理上的内在支撑；或避免部分国家利用安全例外条款适用的模糊性，不顾国际法规则地损害中国企业在数字贸易上的利益。但上述两项好处是难以兼得的，这就涉及到利益平衡与立场面向的现实问题：在解释国家安全例外的时候，是选择扩张主义还是限缩主义？考虑到数字贸易规则的国际国内情况，赞同大部分学者在这一问题上的主张，即中国应当更积极地推动国家安全例外向限缩适用的方向发展。在国家安全被泛化并被作为攫取非正当利益的武器的情况下，对

[5]See The United States Communication from the United States, Measures Adopted and under Development by China Relating to Its Cyber-security Law, S/C/W/374, last visited at 17th Aug., 2023.
[6]中华人民共和国国家质量监督检验检疫总局《信息安全技术数据出境安全评估指南》附录 A，https://www.tc260.org.cn/ueditor/jsp/upload/20170527/87491495878030102.pdf，最后访问日期：2023 年 8 月 15 日。

其概念的严格、精准解释才是中国维护自身利益的现实需要。而在恪守 DS512 和 DS567 等一系列案件所确立的“善意”“最低限度”“必需性”要件的基础上，我国于国际舞台上提出贸易自由化利益与国家基本安全利益之间的平衡方案，不将经济和商业目的裹挟入基本安全利益的范畴，也是中国参与国际法规则制定和领导全球治理的历史使命。

(二) 我国宜设置统一的中央数据监管机构、形成更系统化的管理体系

1) 以数据监管母法带动分类制度建设

在《民法典》出台之前，个人信息的定义、内涵以及法律意义在学术界和实务界争论不休，这样的争论也影响了司法实践，同案不同判的现象屡有发生[10]。因此，要解决概念混淆、模糊的问题，必须通过高位阶法律的阐释。在上位法中确定一个“母概念”，向下分支出“子概念”，“母概念”内涵广泛，“子概念”则包含在“母概念”之中，通过法律汇编的方式对“子概念”进行整理。具体而言，可以将《数据安全法》作为保障数据安全的母法，总结并扬弃现有规则中的“关键信息”、“重要数据”、“核心数据”等概念。从横向角度，将数据根据应用领域分为商业数据、个人数据、公共数据等。商业数据是无关国家安全、公共利益的数据类型，采取行业自查的方式、事后追责的方式出境，推动行业自律制度建设[11]；个人数据进一步分为敏感数据与非敏感数据，根据个人授权、数据评级等前序操作来判定不同的监管方式；公共数据则根据其与社会利益、社会秩序的关联度进行安全评估，确定关联度阈值，对未达到阈值的数据允许出境。从纵向角度，将数据根据重要程度分为一般数据、重要数据、核心数据。以重要数据为基准，建立评估体系，在此基础上建立核心数据的名录，对二者予以明确并依次增加重点评估事项的数目、评估的审查严格程度、数据发送者和接收者所要承担的责任义务以及履行责任义务的技术措施标准要求，综合决定是否允许数据出境[6]；由此形成我国数据出境的动态评估体系。在面对定义泛化、评估流程繁琐、传输必要性负担等质疑时展现有力回应，更表明我国的数据跨境监管不存在限制贸易或阻碍数据自由流动的意图。

2) 以合理高效的监管体系推动数据跨境评估

首先，要完善跨境数据流动当中的行业监管体系。要在进一步的立法环节当中，逐步去除“一刀切”的监管制度，逐步从静态的数据内容监管转向动态的流动过程监管。将监管机关的权限列明，为受监管企业的合规工作提供指引和帮助，重点强化跨境数据流动的事前监管和渠道监管。具体而言，可以将国家主体相关的数据和公民个人相关的数据进行分类监管，设立宽严相济的两套监管体系。从监管制度上落实数据分类，使不同数据获得不同程度的保护，在保证数据安全的前提下以监管促进产业繁荣。

其次，除了通过完善立法和加强政府监管外，规制跨境数据流动还应依靠行业自律制度。企业是社会的主要组成单元，企业对数据、信息安全法规遵从义务履行的成熟度是衡量社会整体数据、信息安全保障水平的重要标尺。由于企业在经营过程中产生、涉及、处理的大量数据会涉及到国家安全、基础设施状况和个人隐私等信息，掌握数据的企业有义务保障其控制范围内的数据安全，防止数据泄漏而损害国家利益及侵犯个人隐私。在跨境问题上，企业还面临国内外公权力机关依本国法所提出的数据要求，如欧盟通过标准合同或约束性企业规则要求数据转移者承担数据转移安全的直接责任。在这一背景下，企业应从构成 IT 社会一员的立场出发，从公司法人治理的高度，将数据、信息安全注入企业文化，形成企业内部人员上至总裁下至普通员工，都以自觉遵从保护个人数据、信息安全的国家法律法规以及企业规章制度为荣；以不履行保护义务的行为为耻的良好风气。

(三) 我国宜鼓励企业加入 DPTM 体系以促进数据监管互认

作为首个专门针对数字贸易规则进行规定的全球性数字经济协定规则，DEPA 区别于其他协定内容之一是鼓励使用信任标志，承认其在数据安全中所起到的重要作用[12]。DEPA 规则要求各国对于数据的保护水平应为“各自法律框架下的可信任标志或认证框架所提供的相当水平的保护”，然而，我国国内

并无与 DEPA 衔接的数据保护可信任标志体系，在这方面的规则构建与 DEPA 存在一定的差距。

信任标志作为一种资质认证的标记，有效使用信任标志至少可起到以下作用：对持有信任标志的内容、服务提供者提供便利化措施，提高数据跨境处理的效率；同时可以借此构建一个统一且稳定的安全监管体系，有助于实施国家数据安全的相应政策，为数字贸易发展营造良好的体系化环境[12]。作为 DEPA 创始国之一的新加坡，有着较为完备的、在全球范围内影响力较广的数据保护可信任标志体系，即 DPTM 认证体系。数据保护信任标志(DPTM)是面向企业的一项认证，用于认证已部署数据保护措施的企业，以证明其业务合规遵从了新加坡个人数据保护法(PDPA)。截至目前，仅有超过 80 家企业获颁该认证。同时，在数字经济贸易竞争愈发激烈之时，全球领先的 ICT (信息与通信)基础设施和智能终端提供商华为在新加坡的子公司华为国际(Huawei International)也于 2022 年 3 月就获得新加坡资讯通信媒体发展局(IMDA)授予的数据保护信任标志(Data Protection Trustmark，简称 DPTM)[7]。由此可见，主动积极地融入世界规则体系，才能更好地运用规则进行世界游戏和竞争。

因此，在以数据作为新生产要素的经济新时代，在愈发重视数据跨境安全处理的时代，要想使得本国企业在愈发激烈的数字贸易竞争中脱颖而出或是不受到沉重一击，我国就需要更加重视数据监管的便利化和效率化；同时随着今年我国国内数据出境安全评估的落实推进，国内企业申报效率低下的现状也亟需政府“搭一把手”。除了企业内部需要加强对数据出境的合规审查，国家层面也可以鼓励国内企业加入 DPTM 体系以促进数据监管互认，提高数据出境安全评估的效率和安全性；当然前提是国家层面需要认可 DPTM 体系下企业的数据合规性和可信任度，认可 DEPA 创始国之一的新加坡的该认证体系在我国的合法合理性。

5. 结语

党的二十大报告指出：“加强重点领域、新兴领域、涉外领域立法，统筹推进国内法治和涉外法治，以良法促进发展、保障善治。”在数字经济贸易蓬勃发展的当下，构建与数字生产力发展相适应的法规体系是数字贸易高质量发展的迫切需要。

明晰国家安全概念的内涵外延和规范表达，构建系统性的数据管理制度和统一的中央数据监管机构，鼓励我国企业加入数据保护可信任标志体系并促进监管互认，将有利于完善促进数字治理框架体系和关键性规则安排，并对建立健全数据要素市场规则、打通数据资源要素的自由流动具有深远的制度保障意义。

目前，我国仍处于 DEPA 的加入谈判阶段。如能同全球领先的数据经济协定规则衔接得当，从而进一步提升我国在全球数字贸易中数据治理规则体系中的地位，更利于进一步促进我国的数字经济贸易的高质量发展，真正实现《数字中国建设整体布局规划》的美好愿景。

致　谢

在完成这篇论文的过程中，我们要向许多人表达我们最诚挚的感谢与敬意。首先，我们衷心感谢我们的导师，他的悉心指导和宝贵建议在整个研究过程中对我们产生了深远的影响，他在国际法以及国内立法方面的专业知识和无私支持使我们能够克服了许多困难，不断进步并最终完成这篇论文。

同时，我们也要感谢学校为我们提供的学术平台和资源。学校的支持使我们能够充分发挥自己的创造力和研究能力，为本论文做出了重要的贡献。

我们还要感谢所有在研究过程中给予帮助和支持的其他同仁以及所有在背后默默付出的师友。他们的鼓励、讨论和建议都对我们的研究产生了积极的影响，使我们能够不断完善和改进论文内容。

[7]《华为获新加坡资媒局授予数据保护信任标志》，https://www.huawei.com/cn/news/2022/3/singapore-imda-award-huawei-data-protection-cert，最后访问日期：2023 年 8 月 18 日。

这篇论文的完成离不开大家的共同努力和支持，在此向各位致以最衷心的谢意。

基金项目

华东政法大学 2023 年校级研究生创新项目之硕士研究生学术研究及社会调研项目，校内项目编号：2023-3-047。

参考文献

[1] 陈兵. 数字企业数据跨境流动合规治理法治化进路[J]. 法治研究, 2023(2): 34-44.

[2] 许多奇. 治理跨境数据流动的贸易规则体系构建[J]. 行政法学研究, 2022(4): 50-60.

[3] 张正怡. 数字贸易规制构建及中国的因应[J]. 江淮论坛, 2022(1): 131-139.

[4] 王娜, 顾绵雪, 伍高飞, 张玉清, 曹春杰. 跨境数据流动的现状、分析与展望[J]. 信息安全研究, 2021, 7(6): 488-495.

[5] 张明. 面向 CPTPP 的数据跨境流动: 规则比较与中国因应[J]. 情报杂志, 2022, 41(11): 144-150.

[6] 马光, 毛启扬. 数字经济协定视角下中国数据跨境规则衔接研究[J]. 国际经济法学刊, 2022(4): 45-62.

[7] 李佳倩, 叶前林, 刘雨辰, 陈伟. DEPA 关键数字贸易规则对中国的挑战与应对——基于 RCEP、CPTPP 的差异比较[J]. 国际商务, 2022(12): 63-71.

[8] 易永豪, 唐俐. 我国跨境数据流动法律规制的现状、困境与未来进路[J]. 海南大学学报(人文社会科学版), 2022, 40(6): 135-147.

[9] 孟夏, 孙禄, 王浩. 数字服务贸易壁垒、监管政策异质性对数字交付服务贸易的影响[J]. 亚太经济, 2020(6): 42-52+147.

[10] 石佳友. 个人信息保护的私法维度——兼论《民法典》与《个人信息保护法》的关系[J]. 比较法研究, 2021(5): 14-32.

[11] 许多奇. 个人数据跨境流动规制的国际格局及中国应对[J]. 法学论坛, 2018, 33(3): 130-137.

[12] 陈寰琦, 陆锐盈. DEPA 数据安全规则解析及对中国的启示——基于和 CPTPP/USMCA/RCEP 的比对[J]. 长安大学学报(社会科学版), 2022, 24(2): 22-31.