

数据规则的国内构建、国际竞争和协调

邱 静

（中国社会科学院 世界经济与政治研究所，北京 100732）

关键词：数据规则；多因素平衡；规则构建；国际竞争和协调

摘 要：在数字时代，协调各国数据规范并形成国际规则的需求比较强烈。经济利益、价值理念、国家安全等因素在形成数据规则过程中发挥了重要作用。主要经济体尽力平衡各类政策因素，并基于优先考虑因素形成不同的制度特征。基于制度特征，主要经济体参与国际竞争和协调：通过域外适用的方式扩大国内规则的适用范围和影响力；与其他国家签订双边、区域协定以及建立相应合作机制，在一定程度上形成数据流动联盟；在 WTO 等国际平台上提出国际规则诉求。中国应当审慎研判数据规则竞争与合作的现状，基于国情和形势做好应对准备：借鉴他国有益经验，动态调整和完善国内规则，在以更加具有针对性和隐蔽性的方式保障国家安全的前提下，促进数据利用和流通，同时积极构建国际数据流动圈，参与国际规则建设。

一、导论

全球进入数字时代之后，各国之间的联系更加紧密。2019 年全球 47 个经济体的数字经济规模达到 31.8 万亿美元。数据不仅随着人、物、技术和资本在全球流动，而且数据本身作为标的物也需要全球流动。根据美国智库布鲁金斯学会的相关研究，2009—2018 年全球数据跨境流动对全球经济增长贡献度高达 10.1%。与此同时，数据泄露、数据滥用等问题凸显了数据保护的紧迫性。由于数据无国界传输的特征，数据保护、利用和流动成为国际热点问题。尤其是，全球存在多种数据跨境流动政策，数据跨境流动出现障碍，需要各国进行政策协调。目前数据领域规则竞争和合作交织进行，掺杂着国内外多种复杂因素，相关问题对于国家的发展和安

全十分重要，亟需深入研究和讨论。

国内针对数据问题的研究文章逐渐增多，从各个角度进行分析，给数据治理提供了学术贡献。

较多学者撰写了关于个人数据保护的文章。例如，王磊、贡绍海撰文指出，随着个人信息保护制度逐渐确立，需要进一步考虑个人信息主体、数据处理者和产业全链条各方的贡献，从促进数据利用的角度研讨个人信息保护制度的构建；孙登科对个人数据保护法律适用规则构建的基本逻辑，尤其是针对个人数据保护给传统法律适用规则带来的挑战进行了分析；姚佳撰文指出，数字时代令个人享有的权利呈现多维特征，需要致力于权利保护与权利救济并重，实现对个体权益的充分保护。

一些文章针对数据流动制度进行分析和研讨。例如，刘晨希针对“一带一路”建设中数据跨境流动的挑战进行分析，在强化数据跨境流动监管机制、促进数据自由流通方面提出了相关政策建议；金晶通过研究欧盟数据保护立法模式，认为应当谨慎对待充分性决定、标准数据保护条款等具有欧盟特色的复杂法律工具，以及全盘统筹个人数据与非个人数据流动立法方案；陈红娜通过定量分析，指出限制跨境数据流动有其合理性，且难以被消除，故需要通过专业化分工来降低限制流动带来的成本；蔡翠红、郭威梳理了中美两国跨境数据流动政策的演进历程和特征，认为两国的分歧是各自数字实力、认知理念和地缘政治共同作用的结果。

果。

一些文章针对数字竞争、数据主权撰写了相关文章。例如，叶成城认为，国家间地缘经济竞争模式随着生产方式的变革而变化，尽管数字技术革命在短期内加剧了中美科技竞争，但在长期仍会强化中美之间的相互依赖；阎学通、徐舟撰文分析了数字时代初期的中美竞争，指出冷战思维和数字思维将对数字时代的外交决策产生混合影响，国家间这种对外政策的互动将会塑造一种和平但很不安定的国际秩序；周念利、吴希贤指出，在中美科技博弈的大背景下，中美数字技术权力竞争已对现有国际产业分工与国际秩序造成了严重影响；张晓君通过对相关数据主权规则建设的模式进行介绍和分析，建议以主权平等、合作共治为原则，以网络命运共同体理念为指导，构建符合我国数据要求并兼顾各国利益的数据主权规则。

上述几类文章主要针对数字竞争、跨境数据流动、个人数据保护等方面进行研讨，提出了学术见解和政策建议。但是这些文章中，有的主要关注如何构建法律规则，有的主要从国际政治角度进行剖析，还未能针对数据规则建构背后的多因素进行分析，未能针对几种类型的建构模式进行全面的比较，也未能将国内规则构建与国际竞争和协调进行协同分析。规则构建包括两个阶段：一个阶段是国家和地区在平衡各类因素的基础上形成制度特征，继而形成国际规则诉求；另一个阶段则是国家和地区在国际上参与规则竞争和协调。本文在回顾数据规则的相关文献的基础上，以美国、欧盟和俄罗斯等国家和地区为代表，分析数据规则的国内构建及其形成原因，阐释数据规则的国际竞争、协调状况，针对中国情况提出政策建议。本文力求针对数据规则的国内构建和国际竞争、协调进行较为全面和深入的分析，以求对数据规则构建需要考虑的因素和分析框架、国际竞争和协调状况有更加清晰和全面的认识，进而从国内构建和国际竞争两个角度来科学认识和构建数据规则。

二、数据规则的国内构建

构建国内制度是一个复杂的过程，需要在知识和诉求的基础上评估多种因素并进行合理平衡。建构主义把规范定义为一个行为集体拥有的关于适当行为的期望，认为应当研究各个国家是如何发展和确定其利益的。规则的制定过程就是不同理念存在竞争的情况下平衡各种因素的过程。

经济利益在国家构建规则过程中始终占据重要地位。经济发展和繁荣是国家追求的关键目标，是民众提升福利水平和获取幸福感的必要途径，也是国家综合实力的重要体现。普遍的经济竞争已经成为国际关系的基础。国家实施对外战略过程中，经济利益因素是基本的出发点，政治、军事等政策在较大程度上为经济政策服务。

价值理念成为影响国家规则构建的重要因素。在不同的地域文化中，人们的社会实践不同，就会产生不同的社会表象体系，进而产生不同的知识体系、形成不同的价值理念。每个国家都有自己独特的历史、文化、国民性以及社会基本制度，在全球治理中形成了各自的治理价值偏好。

国家安全是国家构建规则过程中无法回避的重要因素。如果行为体之间的共同期望使其互相猜疑和对对方做出最坏的打算，双方都感到威胁，则形成了“安全困境”。维护安全利益就是维护有利于国家安全的现状，并改变对国家安全不利的状况。目前国家安全除了政治军事传统安全，还有全球性问题导致的非传统安全。

当今全球大多数国家都制定了相应的数据规则。由于议题的复杂性，各国基本上都需要平衡相关因素，以构建适当的国内数据规则，并在此基础上形成国际规则诉求。本部分重点分析以美国、欧盟和俄罗斯为代表的国家和地区的数据规则构建、影响规则构建的相关因素及其差异。

（一）强调“数据流动”的美国模式

美国是数字经济大国，数据已经成为其经济发展的重要生产要素。在数据治理方面，美国制定了多类规则平衡相关考量因素。

从经济利益角度来看，基于数据流动对于数字经济发展的必要性，美国十分强调促进数据利用和流动。2019年12月23日，美国白宫行政管理和预算办公室（OMB）发布了《联邦数据战略与2020年行动计划》，提供使用数据方面的指导，以促进和加速数据的利用，实现数据价值。美国主张跨境数据自由流动，没有做出限制数据流动的一般性规定，而且，在国际协定中强调成员方不应针对数据流动施加任意或者歧视性限制，主张禁止采用数据本地化条款来保证企业不需要在当地设立或者购买数字基础设施。

从价值理念角度来看，基于个人隐私和数据权利的重要性，美国制定了个人数据保护的相关规范。美国联邦贸易委员会（FTC）制定了有关隐私保护的各类规则，例如健康信息泄露通知规则、儿童在线隐私保护法执行规则、金融服务现代法隐私规则。《联邦贸易委员会法》管辖之外的银行、航空、保险以及电信公共运营，则主要适用专业性立法和自我监管措施。一些州制定了比较全面的法规，例如，加利福尼亚州制定了《消费者隐私保护法》。

从国家安全角度来看，基于数据与国家安全紧密相联，美国实施了数据安全保护措施。例如，美国《出口管理条例》中技术和软件的出口包括由美国境外通过互联网访问获取重要信息，从而可以通过出口管制来保护数据安全。美国制定的《外国投资风险审查现代化法》将对于国家安全造成威胁的高风险敏感数据界定为“敏感个人数据”，并明确将敏感个人数据列为外国投资安全审查时评估国家安全风险的要素之一。美国还颁布《受控非密信息》行政命令，建立和实施受控非密信息登记备案及标识管理制度，作为对国家秘密保护的补充，这类信息一般不允许出境。2016年美国税务局发文规定联邦机构必须将接收、处理税务信息的信息系统置于美国领土、大使馆区域内。美国参议院法案《2019国家安全和个人数据保护法案》明确中国和俄罗斯为特别关注国家，禁止向特别关注国家传输用户数据以及破译相关用户数据所需的密钥数据（包括间接通过第三方非特别关注国家传输）。

从上述规定可以看出，基于数据涉及经济利益、价值理念和国家安全，美国注重从这些因素的角度规范和管理数据。在平衡各因素的情况下，美国倾向于促进数据利用和流动，并形成了支持数据跨境自由流动的国际规则诉求。其一，美国的个人数据保护较为宽松，以保证企业合规成本维持在合理程度。美国联邦层面没有统一的数据保护法律，而采取了行业分散立法模式。美国个人数据保护主要以隐私保护状况为考核指标，其隐私保护标准有两个层级：在线隐私联盟公布的建议性指引以及由美国两大隐私认证企业制定的具有约束力的隐私保护计划。美国国会议员提出了关于制定个人数据保护的议案，但议案尚未通过审议，且普遍认为通过审议的难度较大。可见，美国的个人数据保护规定较为宽松，降低了数据跨境流动的门槛。其二，美国大力主张数据跨境自由流动。美国《2007年国家网络安全战略》明确指出，美国经济的成功与数据流动密不可分，美国将通过积极参与互联网名称与数字地址分配机构、互联网治理论坛等重要组织的活动促进数据自由流动。2010年《韩美自贸协定》首次纳入跨境数据流动的条款。2016年由美国主导的《跨太平洋伙伴关系协定》（TPP）将这一条款转变为具有相对约束力的条款。由美国主导的《美国-墨西哥-加拿大协定》（USMCA）要求各方拥有个人数据保护的法律制度，同时规定各方不得禁止和限制数据的跨境流动，除非是实现合法的政策目标，而实现政策目标不得构成武断或不合理的歧视、不得对贸易构成限制。USMCA重申了TPP中“实施数据存储非强制本地化”诉求，并且删除了缔约方监管例外的规定。

美国在平衡相关政策目标的基础上，强调数据自由流动，并不以限制数据流动的方式来实现数据安全和权利保护，表明其将经济利益作为政策制定的优先考虑因素。这种立场与美国一直重视信息流动的理念相关，更是源于美国强大的互联网经济实力和数据的掌控能

力。美国已连续几年位居全球数字经济竞争力榜首，在数字经济领域占据绝对优势地位。全球前十大互联网公司中有 6 个是美国公司。微软、谷歌等 4 个美国公司提供全世界超过一半的云服务能力。有数据表明，美国存储了全球约三分之一的数据。基于数字经济的强大实力，美国主张数据跨境自由流动和在数据保护上采取相对灵活、有效平衡的态度，从而进一步提高美国数字企业的国际竞争力，帮助美国数字企业进入他国市场，实现巩固和增强数字霸权的政策目标。

美国虽然优先考虑经济利益，但也重视个人权利保护和国家安全，尤其是在国家安全方面，美国采用了较为隐蔽的方式以实现在保障国家安全的同时不影响其关于数据跨境自由流动的立场。美国没有专门针对数据安全和限制数据流动的国内规范，而是通过其他规范来实现数据安全，例如，采取出口管制、外商投资安全审查、保密信息和受控非密信息管控以及针对特定国家加强数据管理。这类处理方式有以下优势：保护数据安全具有较强的针对性，主要针对需要采取出口管制、外商投资安全审查的领域和国家进行数据管制；信息管理侧重于保密和受控非密信息的管理，属于信息的统一管理，不针对数据出境专门规定；由于数据安全监管方式较为隐蔽，所以不影响美国基于经济利益支持数据自由流动的国际规则诉求。

除美国之外，日本也倾向于强调数据自由流动。在 2019 年 6 月的 G20 大阪峰会上，日本提倡建立允许数据自由流动的“数据流通圈”，强调数据对于创新和经济的重要性。日本并不认为在国际合作中个人数据保护问题不容谈判和妥协；提出为了促进跨境数据流动，可以在一定程度上降低个人数据保护标准，以促进“基于信任的跨境数据流动”。由日本主导的《全面与进步跨太平洋伙伴关系协定》（CPTPP）包含了与 USMCA 规定类似的促进数据流动和利用的条款。在 WTO 关于电子商务的谈判中，日本基本上支持美国的主张。日本积极提倡数据流动和促进数据利用源于其数字经济实力以及数字经济对国家发展的重要性。

《世界创新竞争力发展报告（2011～2017）》指出，美国、中国、日本位列全球数字经济发展总体规模前三。数据跨境自由流动对于日本实现经济社会目标至关重要，具有重振日本经济的潜力。如果全面开发日本人工智能和物联网的潜力，那么预计日本 2030 年的 GDP 可提高 40%；日本公司对大量公共云服务的需求会产生良好的溢出效应，尤其是对于远程办公的需求，可解决日本大量就业的问题。

（二）强调“权利至上”的欧盟模式

为了促进数字经济发展和保护数据权利，欧盟发布了若干关于数据的规则，从各个角度进行有效的数字治理，以确保实现预期目标。

从经济利益角度来看，欧盟促进数据利用和流动，提倡形成欧洲单一数据市场，改善数字经济较为落后的局面。欧盟制定了《非个人数据自由流动条例框架》（FFD），以保证数据在欧盟内部的自由流动。欧盟提出了商业对政府（B2G, business to government）和商业对商业（B2B, business to business）两种模式，以加强数据利用和分享。在限制数据流动措施方面，欧盟作出了禁止性规定，例如，明确不允许规定数据必须在本地计算设备上存储或将数据本地存储作为数据跨境流动的条件。2022 年 5 月 16 日，欧盟理事会批准通过《数据治理法案》，其重点旨在增进数据的可用性，促进各部门和各成员国的数据共享，推动企业间有偿共享数据，提供可信赖的数据环境以促进研究和创新服务。

从价值理念角度来看，欧盟尤其重视个人数据权利保护。欧盟于 2018 年出台了《通用数据保护条例》，条例明确法律适用的行为主体包括数据控制者和处理者；不断强化数据主体的各项权利，除了完善之前规定赋予的权利，还增设了一系列新的权利，如遗忘权、持续控制权、拒绝权等；对数据控制者和处理者提出了更加严格的要求，加重了他们的数据保护义务与责任。

从国家安全角度来看，欧盟强调数据安全和主权。2019 年 6 月，欧洲议会和欧盟理事

会发布了《关于欧洲网络与信息安全局信息和通信技术的网络安全》，2018年欧盟委员会提出了制定《网络安全法》的议案。2020年2月，欧盟委员会发布了《塑造欧洲的数字未来》《人工智能白皮书》《欧洲数据战略》等数字战略文件，提出了“技术主权”的概念，认为欧盟应当确保数据基础设施、网络和通信的完整性，摆脱对美国互联网大企业的依赖。

从上述可见，欧盟从数据利用、保护、安全和主权等多方面进行规范，然而，欧盟政策的鲜明特征是十分强调个人数据权利保护，权利保护是优先政策考虑因素。

欧盟制定的《通用数据保护条例》被称作全球最严格的个人数据保护法规，明确了数据主体的各项权利。欧盟将个人数据保护作为政策优先考虑的因素，其他政策目标都要让位于这个优先目标，即不会妥协个人数据保护来实现其他目标。为了有效保护个人数据，《通用数据保护条例》对欧盟数据出境规定了条件：充分性认定（数据可向被认定数据保护达到了与欧盟同样标准的国家流动）；适用于具体企业的约束性企业规范、标准合同条款、认证机制等；数据主体的明确同意。条例的严格规定让企业合规成本上升，但是欧盟认为，即使相关规定会提高企业合规成本，以致其失去商业发展机会，也应当坚定维护欧洲的核心价值理念。同时，在贸易协定谈判过程中，欧盟将个人数据保护置于不可妥协的位置，认为欧盟数据保护规则不能成为贸易协定谈判的对象，因为个人数据权利是基本权利，不是可以谈判的商品。

欧盟形成了“以权利为中心”的制度特征，尤其看重与个人尊严紧密相关的隐私权和个人信息保护，这具有历史、法律等方面的原因。

第一，欧洲关于基本权利保护的文化和法律制度已经根深蒂固。第二次世界大战以后，欧洲国家进行集体反思，加强了个人基本权利保护。1950年欧洲各国签署了《欧洲人权公约》，并于1959年成立了欧洲人权法院。2007年欧盟颁布了《欧盟基本权利宪章》，明确了若干基本权利保护。其中，《欧洲人权公约》第8条规定的个人和家庭生活权利包含了个人信息权利；《欧盟基本权利宪章》第7条和第8条分别规定了个人隐私权利和个人数据权利。在基本权利文化深厚的土壤中，史上最严的个人数据保护法规——《通用数据保护条例》应运而生。

第二，在权利保护方面，欧洲十分看重隐私保护，与美国具有一定的差异，两者在隐私保护理念上的差别导致在个人数据保护方面的价值优先次序不同。欧盟明确的个人数据权利是主动的个人自决权利，强调个人对数据拥有控制权。美国则主张从隐私权的角度进行保护，认为个人数据保护建立于隐私权的基础之上，而隐私权是一种偏向防御性的权利，其保护需要与商业利益、表达自由等权利进行平衡。欧美在个人信息保护上的差异体现了西方国家对待隐私的两种文化，即尊严和自由。欧洲国家认为隐私是人格尊严的体现，必须得到很好的保护，在权利保护体系中位居前列，处于优先位置。美国也注重隐私保护，但将其看作自由的一个方面，在复杂的权利体系中并不具有优先位置；主张隐私保护需要与言论自由等权利进行平衡，在较多时候可能需要让位于自由权利。

此外，欧盟数字经济相对落后，欧盟欠缺数字大公司和掌握数据的能力，数据跨境自由流动并不完全利好其数字经济发展，因此，欧盟欠缺大力促进数据跨境流动的经济内驱力。根据联合国发布的《2019年数字经济报告》，中国与美国占全球70个最大数字平台市值的90%，而欧洲的份额仅为4%。被誉为“互联网女皇”的玛丽·米克尔发布了2019年的《互联网趋势报告》，报告公布了全球前30大互联网公司，美国上榜的企业高达18家，而欧盟仅上榜了1家企业。美国公司在欧洲市场居于垄断地位，谷歌、亚马逊、爱彼迎等电子平台以及推特、脸书等社交平台占据了欧洲国家绝大部分市场。因此，欧盟强调“数字主权”，以增强自身数字技术能力。不过，即使美国大企业掌控欧盟数字市场，但是欧盟未采取数据本地化措施，而是强调在保护个人数据权利的前提下实现数据自由流动。虽然针对数据流动的限制措施被认为具有数据保护主义之嫌，但是严格的个人数据保护和跨境流动要求适用于

所有公司，也增大了欧洲本土企业的合规成本，对欧洲小企业的成长并不友好。从执法实践来看，欧盟模式虽然强调隐私保护和数据主权，但易导致数据交易成本和执法成本大幅增加，在一定程度上扼杀了大数据产业发展的活力。总之，“个人权利至上”的价值理念主导欧盟的政策制定过程，是欧盟政策制定的优先考量因素，决定了欧盟数据规则的基本面貌。

（三）强调“国家安全”的俄罗斯模式

与美国、欧盟一样，俄罗斯也从相关因素角度考虑，颁布了若干规范来进行数据治理。相较而言，俄罗斯模式体现了注重国家安全的特点。

从经济利益角度来看，基于数字经济不发达的情况，俄罗斯采取了相关措施发展数字技术和经济。2017年7月，俄罗斯联邦政府发布《俄联邦数字经济国家规划》，确定了立法规范、数字经济生态系统建设、数字教育和人才培养等数字经济发展方向。2019年2月，俄罗斯制定了新版规划，增大了数字经济投入。2019年10月，俄罗斯发布《2030年前俄罗斯国家人工智能发展战略》，旨在优先发展和使用人工智能。

从价值理念角度来看，俄罗斯制定了相关法规来保护个人数据权利。2006年俄罗斯加入了《个人数据自动化处理中的个人保护公约》。同年俄罗斯颁布了《关于信息、信息技术和信息保护法》，明确了信息拥有者、信息系统运营者的信息保护义务。2006年俄罗斯还颁布了《个人数据法》，明确了各项数据主体权利以及数据处理者的相关义务，并且规定数据处理者有义务保证数据跨境传输后能享有同等程度的保护。之后俄罗斯多次修改法律，保护个人数据的力度不断增强。俄罗斯根据公约明确了能够提供个人数据充分保护的白名单国家，允许向这些国家进行跨境数据传输。

从国家安全角度来看，当俄罗斯发现数据直接关联国家安全，俄罗斯就十分重视维护数据安全。“棱镜门事件”后，俄罗斯意识到数据跨境流动的风险，通过修改法规确立了数据本地化存储的规则。俄罗斯修改《关于信息、信息技术和信息保护法》，要求信息拥有者、信息系统运营方有义务将记录俄罗斯联邦公民个人信息的数据库存放在俄罗斯境内；修改《个人数据法》，要求收集个人数据（包括使用互联网手段）时，运营商需要保证使用位于俄罗斯境内的数据库，还要求数据处理者在处理数据前告知数据保护机关包含俄罗斯公民数据的数据库所在地的信息，并规定为了保护公民权利和国家安全，可以中止或限制个人数据跨境转移。俄罗斯根据法律对企业进行执法检查，例如，2019年对美国企业推特（Twitter）和脸书（Facebook）做出了相关处罚。随着俄罗斯与美国等西方国家的关系日益紧张，俄罗斯持续强化数据主权，开始发展独立的网络通信技术，加强对网络的整体控制。

俄罗斯从各个角度进行数据治理，但其严格的数据本地化存储制度最为鲜明和突出，成为其数据治理的一大特征。与美欧通过长臂管辖扩张执法不同，俄罗斯等新兴经济体实行的数据本地化等主权战略，体现了保守型特征。虽然数据本地化存储规定会增加数字企业的成本，不利于吸引数字企业的投资，可能导致部分数字产业离开俄罗斯，阻碍俄罗斯对接世界数字经济发展的机遇，进而影响数字经济发展，但是，俄罗斯坚持制定和执行这一制度，将直接关联国家安全的数据安全作为优先考量因素。俄罗斯之所以高度重视数据安全，与其国情、特点和现实发展相关。

俄罗斯是一个非常重视国家安全的国家，这与其地缘政治现实相关，也是俄罗斯历史推动形成的国家特点。俄罗斯历史上一直具有大国雄心，是世界大国竞争的重要参与方。俄罗斯战略文化的精髓之一是安全观大于发展观，即使遭受严厉的制裁，也要追求战略缓冲区。冷战后，俄罗斯融入西方世界的努力宣告失败，北约国家仍然将俄罗斯视作战略威胁，北约东扩不断挤压俄罗斯的战略空间。基于地缘政治现实，俄罗斯认为国家安全是其最重要的国家利益，是必须优先考虑的因素。

俄罗斯意识到数据安全逐渐成为大国博弈的重要领域。一直以来俄罗斯十分重视国防、

军事等传统安全领域。随着网络全球普及，数据利用和流动成为信息交流和经济发展的重要支撑，网络空间和数字领域逐渐成为大国竞争的重点领域，而且其战略重要性会日益突出，深刻影响国际关系。俄罗斯具有大国雄心和实力，时刻处于地缘政治斗争的漩涡之中，意识到掌握数据对于其国家安全和参与大国竞争的重要作用。

俄罗斯面临较为紧迫的数据安全风险。“棱镜门事件”让俄罗斯意识到跨境数据流动带来的国家安全风险，让俄罗斯逐渐从放任网络自由转向管控网络来维护安全。而且，俄罗斯长期遭受大量网络攻击，存在数据泄露等较多安全隐患。据统计，俄罗斯国家机构遭受的网络袭击每天达 1 万多次，俄罗斯的网络安全风险在全球居于前列。因此，俄罗斯认为其必须高度重视网络安全，尤其是保证数据安全。

俄罗斯将数据安全作为数据流动的前提，并认为只有将数据风险降到最低，才能保证数据安全，即使相关措施制约了数据流动带来的经济和社会效益。随着地缘政治竞争日趋激烈，俄罗斯不断加强数据安全措施，从地域管控演变为有时特定条件下强制性地断网，以保障国家数据安全和网络安全。尤其是 2022 年 2 月俄乌冲突爆发后，由于俄罗斯面临不断恶化的国际环境，遭受更大的网络风险，俄罗斯会不断加强数据安全措施。

一些新兴经济体也侧重保障数据安全，如印度。印度制定了较多数据规范，数据安全和管辖是其尤其强调的维度。印度主张重要数据本地存储，要求外国公司在当地建设数据中心，数据受托人在印度境内或者数据中心存储个人数据的副本，并且绝对禁止关键个人数据出境。2019 年印度的《国家电子商务政策》草案阐明了这一立场：“印度及其公民对其数据享有主权，这种权利不应扩展到非印度人。”2020 年，印度电子和信息技术部以《信息技术法案》第 69A 条“禁止访问规则”为依据，以秘密传输用户数据至印度以外服务器为由，封禁 59 款具有中国背景的手机应用程序。印度未参与关于数据跨境流动方面的谈判和国际协作，例如，未参与发表 WTO 关于电子商务的两份联合声明。在 2019 年 6 月的 G20 大阪峰会上，印度、南非等国家未签署《数字经济大阪宣言》。

印度注重数据安全和管辖的主要目的在于保障国家安全、保护和发展本国数字产业。印度数字产业相对落后，来自美国和中国的科技巨头掌控互联网，印度广大人口则提供了发展数字产业的丰富资源。脸书旗下即时通讯应用 WhatsApp 是印度人手机上最流行的应用，YouTube 是印度最受欢迎的视频平台，亚马逊是印度第二大在线零售商。中国的抖音、微信等应用程序在印度也曾拥有大量用户。印度认为外国企业掌控本国数据危及数据安全、经济安全，尤其是中国与印度存在领土纠纷和大国竞争关系，印度也不信任美国，因此，印度将维护数据安全和对数据的管辖作为首要政策目标。而且，印度认为数据跨境自由流动不利于本国数字企业发展。咨询公司预测，如果印度拥有其产生的数据，到 2050 年它可能会成为数据中心市场的第二大投资者和全球第五大数据中心市场。

三、数据规则的国际竞争和协调

为了适应全球化的需求，国家之间需要协调制度以消除障碍，并进一步形成国际规则。在这个过程中，基于制度特征的差异，就会出现规则竞争，在竞争中有效协调。各个行为体宣称其规则的合理性和科学性，宣传规则蕴含的价值观和利益诉求，并以影响力、共同利益和共同认知等方法形成朋友圈，增强规则竞争的力量。同时，基于合作解决国际问题的需要，各国会努力在差异中寻求共识。全球治理以制度建设和协调为主，形成具有影响力的规则是获取和维护利益的重要途径；如何设计并推广符合自身利益和价值观的规则成为国内和国际规则建构的主要内容。国际规则竞争在很大程度上也是设计合法性的竞争，主导国必须通过权力让渡和利益分享来不断增强国际规则的合法性。

国际规则建构具有以下特征。第一，建构主体多元化。美国、欧盟、中国、日本等主要

经济体拥有较强的科技实力、生产能力和较大规模的市场，俄罗斯、印度等国家凭借发展能力、国土面积或者人员数量拥有一定的国际影响力。这些经济体在国际舞台上具有不同程度的话语权，可以影响国际规则设计。第二，建构理念多样化。由于国情、文化、法律等方面不同，各国设计规则的理念和关注点不同，因此，形成的国际规则诉求有所差异。第三，建构方法多样化。主要经济体努力推广国内制度并影响国际规则构建。例如，设定赋予国内法律域外管辖效力的条款；与相关国家形成协定或者合作机制，局部实现国际规则建构；在国际组织等全球性平台积极参与国际规则设计，试图主导国际规则制定过程。

当今世界，技术发展强劲推动全球化发展。在数字时代，新兴事物竞相出现，具有较强的国际化特征。在此领域的规则设计比较复杂，一是新事物随着互联网蓬勃发展而兴起，没有国际规范可以学习和借鉴；二是相关议题涉及价值理念、经济发展以及国家安全等重要因素，协调各国立场比较困难。如上所述，主要国家和地区在数据领域形成各类规范，尽力平衡多种因素，以保护数据权利、促进数据利用和维护数据安全。基于国情、文化和政治等方面的差异，不同国家和地区形成了自己的制度特征，并且在国际上参与规则竞争。同时，这些国家和地区互相借鉴和学习，在规则竞争中进行协调和融合。

（一）扩大国内制度的影响力

一些国家通过设定相关条款让其法规具有域外管辖的效力，从而扩大国内制度的国际影响力和竞争力。

欧盟制定的 **GDPR** 产生了较大的国际影响力。其一，**GDPR** 适用于获取欧盟公民数据的境外企业，这让 **GDPR** 具有域外管辖的效力，促使不在欧盟境内的企业改变行为方式，采取相应的合规措施。例如，数据泄露丑闻发生后，脸书公司就直接表态全公司都会遵守欧盟 **GDPR** 的规定。**GDPR** 的域外适用，让个人数据保护规则的全球建构具有实践基础。而且，《联合国宪章》《世界人权公约》以及区域性人权公约的实施，促使不少国家制定了保护基本权利的法规，注重个人权利保护的全球意识已经形成。其二，由于 **GDPR** 具有充分性认定的规定，巨大的欧盟市场促使其他国家努力达到欧盟设定的保护水平。鉴于权利意识的普遍建构、**GDPR** 的域外适用以及与欧盟成员国进行数据流动的需求，越来越多的国家参考 **GDPR** 的规定，提高本国个人数据保护水平。有学者认为，**GDPR** 造成了“布鲁塞尔效应”，强迫欧盟主要的贸易伙伴采用与欧盟同样或者类似的规则。

随着数据保护的重要性得到越来越多的认同，各国立法也出现了趋同性。一是数据保护的基本原则逐渐趋同。数据保护的几大原则，如公开透明、限制处理、数据质量、安全责任等得到了很多国家的认同，并成为法律原则。二是越来越多的国家采用统一立法的模式。日本、韩国等国家制定了个人信息保护法律；中国于 2021 年制定了《个人信息保护法》。三是不断强化数据主体权利和数据控制者的责任。

2018 年 3 月，美国制定了《澄清域外合法使用数据法》（云法案，**Cloud Act**）。该法明确，为了执法需要，互联网企业应当向美国政府披露其控制的存储于境外的数据，同时授权美国与符合条件的外国政府达成双方可以互相调取对方境内数据的协定。此法使得美国扩大了数据管辖范围，延伸至其他主权国家境内。2019 年 10 月，美国与英国正式签署历史上首份双边数据分享协议，允许执法部门直接向对方国家的科技企业获取数据。基于美国的规定，一些国家也制定法规扩大获取国外数据的能力。

俄罗斯、印度等国家基于数据安全、经济安全，明确了管控跨境数据流动的措施，主要通过国内立法进行管控，并以形成异于欧美国家的模式来影响类似国家的规则设计。主要的本地化要求包括在本地建设数据中心、实现数据本地化存储和处理，最低要求则是在境内实现特定数据的容灾备份等。一些发展中国家采取了相似的举措。例如，越南在 2018 年通过《网络安全法》，要求脸书、谷歌等外国公司在越南设立办事处、将越南用户资料存储在越南当地，以及明确数据跨境流动之前必须进行安全评估；巴西于 2013 年开始制定相关

政策，要求数字公司在境内建立数据中心，并于 2018 年出台了《通用数据保护法》，对数据跨境流动提出了新要求。

（二）构建数据流动联盟

数据流动问题的国际性特征要求国际合作和制定国际规则。但是，关于数据的冲突日趋增多，形成统一规则、在所有国家之间实现数据自由流动并不现实，因此，相关国家发展各种机制，在特定国家之间实现数据流动，形成一定的“数据流动联盟”。

美国等国家通过双边、多边协定明确数据保护和流动事宜。美国与韩国、澳大利亚和新加坡等国家达成的双边协定中有条款明确不设定限制双方数据流动的措施。由美国主导的《美国-墨西哥-加拿大协定》（USMCA）、由日本主导的《全面与进步跨太平洋伙伴关系协定》（CPTPP）都明确提出，在协定参与成员之间实现数据跨境自由流动。美国和日本通过区域性机制推动制度建构，其中之一便是在亚太经济合作组织（APEC）平台上设立了 APEC《隐私框架》和《跨境隐私规则》（CBPR）。APEC《隐私框架》反映了美国的政策主张，即最大限度地通过市场问责机制来保护个人信息，而不是设定个人信息保护的高门槛。CBPR 是 APEC 根据其隐私框架建立的促进成员经济体之间跨境数据流动的机制，目前已有美国、日本等 9 个经济体参与。一旦信息处理机构被认证加入 CBPR，那么机构申请时所承诺遵守的规则都对其具有约束力，并可以被其国家管理机构强制执行。目前已有 43 个企业获得了 CBPRs 标章。《APEC 跨境隐私执行合作安排》（CPEA）则设立了一个自愿共享跨境隐私执行信息和相互传送协助条款的框架，为成员国隐私执行机构在跨境隐私执行方面提供了多边法律机制。

欧盟力图通过双边协定明确数据流动问题，但是由于存在分歧，协定中关于数据流动的规定最后基本上都是愿景性的语言。欧盟主要通过充分性认定机制来扩大数据跨境流动的范围，GDPR 详细列举了个人数据充分性保护的标准，例如，法治状况，即对人权和基本自由的尊重程度、相关综合性立法和专门行业立法以及立法的实施状况；具有专门规制机构。目前获得欧盟充分性认定的国家和地区有 14 个。其中与美国是通过建立隐私盾机制（EU-US Privacy Shield）来实现数据流动。2020 年隐私盾机制被终止后，美国和欧盟一直就此议题加强谈判，并于 2022 年 3 月再次达成跨境数据流动协议。

美国支持将 CBPR 和 GDPR 形成的数据流动圈进行联通，响应日本提出的建立“基于信任的数据流动圈”倡议，欧盟也表示同意。但是鉴于 GDPR 的保护标准明显高于 CBPR，两者之间实现联通的可能性较小。不过，欧盟的“约束性公司规则（BCR）”和美国主导下的 CBPR 具备一定的兼容性，因此，2012 年欧盟与 APEC 形成了联合工作小组。该小组比较两者的异同点，制定相应文本，以促进数据在两个组织成员之间的自由流动。2014 年 APEC-EU 工作委员会联合制定了“BCR 规则体系和 CBPR 规则体系共同参考”，重申了两者的规则体系，并指出需要满足的共同标准和认证要求。

此外，一些国家还形成了专门针对数字经济的伙伴关系协定，例如，新加坡、智利、新西兰三国于 2020 年 6 月 12 日共同签署了《数字经济伙伴关系协定》（DEPA）。虽然这个协定只有三个国家签署，且三个国家的经济体量较小，但这是针对数字经济单独签署的协定，是全球第一个关于数字经济的重要规则安排，为全球数字经济提供了规则模板。DEPA 的数据跨境流动规则沿用了美国模式，与 CPTPP 的规定相近，但加强了个人数据保护，试图在数据跨境流动与隐私保护之间做出平衡。目前这个协定的参与方还较少，产生的实际影响相对较小，但作为第一个数字经济协定，在国际上受到较大关注。

由于在法律文化、价值认同、政策目标上的差异以及缺乏足够的信任，短期内形成全球共识而采用统一数据流动规则的想法并不现实，所以各国达成双边协议、区域协议，对特定国家的企业附条件地同意其数据跨境传输的要求。在拥有信任的国家之间完成数据自由流动，同时给隐私保护、数据安全及其他政策因素提供很小的例外空间，具有一定的现实条件，

也就是形成数据流动联盟。虽然这种途径可以部分解决问题，但也容易导致更多的分裂，尤其是被排除在外的国家可能形成竞争性的数据流动联盟。那么今后可能出现的情况就是，不同类型的数据在不同的数据流动联盟中实现流动。这也导致一些国家在各种类型的制度安排中不得不进行取舍。

（三）尝试形成国际规则

与数字经济快速发展形成鲜明对比的是，国际数据规则明显滞后。不少国家认同在国际层面进行制度协调很重要，否则各个国家都设定管辖范围很广的规则，容易导致管辖权冲突，而且跨国企业需要遵从不同的规范，导致企业经营成本上升。

目前虽然很多国家都相继立法提高个人数据保护水平，但是相关国际规则构建会遇及障碍，达成数据保护和流动的统一实体法规则并不现实。一是虽然各国基本上都认同个人基本权利保护，但是保护基本权利的程度和方式因各国发展阶段、国情、文化等因素而有所不同，而且如何解决基本权利之间的冲突、个人权利与公共利益的冲突也存在差异。二是欧盟高标准的数据保护规定会增大企业合规成本，拥有较多互联网企业的美国担心企业难以承受高成本的发展中国家并不愿采取过高的标准。明确哪种个人数据规范居于优先位置比较困难，因为这本来就是国内规范和治理的议题。三是国际社会信息技术发展不平衡导致不同国家的国际规则话语权失衡，意味着与跨境数据流动相关的利益分配本来就存在不公平的情况。因此，目前没有关于数据保护和流动的国际规则，但是尝试构建国际规则的努力一直存在。

经济合作与发展组织（OECD）于 1980 年制定了《关于隐私保护与个人数据跨国流动指南》，并于 2013 年进行了修订。指南内容虽然不及 GDPR 的规定严格，但明确了数据主体权利，影响了很多国家的立法。2011 年 OECD 发布的《1980 年 OECD 关于个人信息保护和跨境流通指南发布三十年检视——不断发展的隐私保护图景》指出，在加强个人信息和隐私保护的同时，如何协调各国关于个人信息和隐私保护的规定，避免其成为新的贸易壁垒，成为一个重要的政策议题。国际标准化组织也在努力制定相关标准，例如，已经制定了关于网络和信息安全的标准，正在尝试制定隐私标准。但是，即使制定了相关国际标准，各国执行也会存在差异，互操作性机制仍然相对欠缺。

2022 年 4 月 21 日，美国、加拿大、日本、韩国、菲律宾、新加坡、中国台湾共同发布全球跨境隐私规则声明（Global Cross-Border Privacy Rules Declaration），正式对外宣告成立 CBPR 论坛，致力促进数据自由流通与有效的隐私保护。这一举动实质上是这些经济体力图将 CBPR 独立于 APEC，达到排除中国和俄罗斯的目的，同时将这个框架转变为其他地区的经济体都可加入的全球性框架。CBPR 论坛旨在建立 CBPR 和处理者隐私识别（Privacy Recognition for Processors, PRP）系统认证，这是同类首创的数据隐私认证，并在共同的数据隐私价值观基础上承认国内保护数据隐私方法的差异，以促进国际贸易和国际数据流动。该声明称 CBPR 论坛的目标包括在 APEC、CBPR 和 PRP 系统的基础上建立国际认证体系，定期审议成员的数据保护和隐私标准，促进与其他数据保护和隐私框架的互操作性。

随着数字经济发展，WTO 开始关注和重视数字贸易规则建构中的数据保护和流动问题，但是，由于利益、价值理念和地缘政治等方面的因素，形成有效的国际规则困难重重。WTO 的几个协定都未涉及数据流动。1999 年服务贸易理事会认定较多的电子商务属于服务贸易总协定（GATS）的范畴。按照 GATS 的规定，成员国可以基于公共健康和道德、隐私、国家安全等原因限制贸易，只要限制合理和合乎比例，并且没有造成歧视。随着电子商务日益重要，一些成员国要求对电子商务做出明确清晰的规定，其中包括关于数据的规则。

WTO 于 1998 年成立“电子商务工作计划”。2016 年 7 月美国率先在 WTO 提交了全面讨论电子商务议题的提案。该提案以 TPP 中的数字规则为核心内容，首次将数据跨境流动等议题引入 WTO。在 2017 年 12 月举行的 WTO 第 11 届部长级会议上，43 个 WTO 成员发表了第一份《电子商务联合声明》。2019 年 1 月，包括中国在内的 76 个 WTO 成员发表了第

二份《电子商务联合声明》，确认将启动与贸易有关的电子商务谈判。2021年3月16日，WTO举行了电子商务谈判全体会议，对相关议题进行了较为充分的讨论。在数据规则方面，美国要求针对允许跨境数据自由流动、禁止采取过度严苛的网络安全措施等议题建立具有约束力的国际规则，从而为美国企业清除可能遭遇的“数字贸易壁垒”。日本基本上支持美国的主张。欧盟强调个人数据保护是基本权利，可以基于个人数据保护限制数据流动。发展中成员普遍将国家安全置于优先地位，为此可能采取限制数据跨境流动的措施，或将计算设施本地化、披露或转让源代码作为在本地开展业务的前提条件，因此，它们的提案中或未涉及相关内容，或强调保留政策空间。

总之，国际上一直尝试形成关于数据保护和流动的国际规则，但是由于议题涉及较多复杂问题，在国家安全、个人权利保护上较难协调立场，所以，虽然形成统一数据保护和流动规则并促使全球数据流动的需求较大，形成国际规则对于全球数字经济发展具有重要意义，但是，形成统一规范的希望仍然渺茫。各国的隐私保护规范存在差异，实践中的保护水平也参差不齐，而且基于国家安全和管辖的需求，尤其是地缘政治竞争导致国家之间缺乏信任，也就无法给数据流动营造信任和安全的环境。即使在相关协定中提及促进数据跨境流动，但也大多是原则性表述，一般都给各国留下了基于国家公共管理需要限制数据跨境流动的政策空间。

四、中国的数据治理及政策建议

从上述分析可见，美国、欧盟、俄罗斯等主要经济体都认识到数据议题的多个维度，尽力平衡各个因素，同时这些经济体基于国情、文化和价值理念等，形成了一定的制度特征。作为重要的数字经济大国，中国也通过制定规范进行有效的数据治理。

（一）中国的数据治理

从经济利益来看，中国强调促进数据利用和流动。中共中央、国务院连续发文要求加快培育数据要素市场，将数据界定为第五大基本生产要素，要求完善数据权属、数据共享等方面的标准，开展数据交易，发挥数据资源价值。上海、天津、贵州等地已经出台地方条例或者规章来促进数据开放共享，尤其是《深圳经济特区数据条例》明确了相关主体对数据产品和服务享有财产权益。2022年12月19日，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》，进一步促进数据的利用和流通。

从价值理念来看，中国日益重视保护个人数据权利。中国《民法典》采用专章的形式保护个人信息和隐私权，针对个人信息的类型、收集、更改或者删除进行了规定。2021年8月《个人信息保护法》顺利出台，强调全面规范个人信息的收集、处理和利用，明确了与个人信息保护相关的若干权利类型。中国主管部门严格执法，对于侵犯个人信息权益的行为采取了多项执法行动，以实现有效保护个人数据权利的目标。

从国家安全来看，中国十分重视保障数据安全。中国于2016年制定了《网络安全法》，2021年又出台了《数据安全法》。基于数据安全的考虑，中国《网络安全法》第37条规定：“关键信息基础设施的运营者在中华人民共和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。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。”《数据安全法》侧重于对数据实行分级分类保护，强调开展数据活动必须履行数据安全义务、承担社会责任；明确国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查，而且要求重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估。

中国积极参加国际数字治理。中国于2019年签署《G20大阪数字经济宣言》，回应了其中“基于信任的数据自由流动”的倡议。中国参与了WTO的电子商务谈判，并参与发表

了第二份《电子商务联合声明》。在关于跨境数据流动议题上，中国认为应当尊重各国的政策主张和发展途径，允许各国根据本国的公共政策目标采取相应的规制措施，基于国情平衡不同政策目标。中国参加了《区域全面经济伙伴关系协定》（RCEP），协定明确要求除维护合法公共政策、基本安全利益等特殊原因外，各方不得阻止业务数据和信息跨境传输。RCEP 尊重国家数据主权，在数据跨境传输规则中未对各缔约方设定强制义务，对缔约方内部监管体系始终抱持包容的态度，缔约方不需要大规模调整数据法律体系就可顺利融入 RCEP 下的数据跨境体系。2021 年 9 月，中国正式提出加入 CPTPP 的申请；2021 年 11 月 1 日，中国还正式提出加入 DEPA 的申请。这些表明中国认同数据跨境自由流动的相关规定以及积极参与数字经济国际合作的意愿。

国际上一般认为，中国在数据保护上侧重保障国家安全。中国制定的《网络安全法》和《网络空间国际合作战略》将维护网络主权作为核心目标，《网络安全法》等法规明确了关键信息基础设施运营者收集的个人信息和重要数据应当本地存储的规定。中国颁布了《数据安全法》，对数据安全责任进行全面规范，明确了“总体国家安全观”对数据安全的统领作用，提出了数据跨境的“安全、自由流动”原则。《数据出境安全评估办法》于 2022 年 9 月生效施行，对数据出境评估作出了较为严格的规定，明确了数据出境需要安全评估的范围，包括数据处理器向境外提供重要数据、关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理器向境外提供个人信息、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器向境外提供个人信息、国家网信部门规定的其他需要申报数据出境安全评估的情形。总体而言，与一些发展中国家一样，中国认同在某些特定情况下适用数据本地存储的必要性，也强调数据跨境流动需要以数据安全为前提，对数据出境秉持较为审慎的态度。

（二）相关思考

中国注重保障数据安全，有以下原因。第一，基于国际形势，中国十分看重数据安全和管辖以维护国家整体安全。美国对互联网具有较强的控制能力，而且基于地缘政治、意识形态等原因，美国与中国之间缺乏充分的信任。美国政府禁止中国公司参与 5G 网络建设，在《网络安全战略》《国家安全战略》报告中将中国列为国家安全领域最重要的对手之一。尤其是，网络商业窃密等一系列网络安全事件发生，使得中美双方都将对方视作网络安全方面的主要威胁。美国是数字经济大国，具有超强的数据掌控能力，又与中国具有大国竞争关系，这些都客观上加剧了中国国家安全方面的威胁。

第二，中美在数据领域的竞争较为激烈，中国保持和扩大数字竞争力需要维护和增强数据掌控能力以及保持数据资源优势。中国人口众多，拥有发展数字产业的大量数据资源，数字经济发展迅速。与美国相比，中国的强势仍是以货物贸易为主要特征的电子商务，在数据产业领域中国相对落后。因此，为了充分利用数据资源优势，中国重视维持数据管控能力。

第三，中国注重保护民众安全权利，并且注意平衡权利保护与国家安全、经济发展之间的关系。一方面，中国等亚洲国家认同权利保护的重要性，不断完善权利保护体系，但同时强调，对于基本权利的保护需要考虑各个国家的不同情况；基本权利保护并不具有绝对性，基于国家安全、公共利益等因素可以对权利进行一定程度的限制。另一方面，中国民众十分看重安全权利，当安全权利与隐私权等权利存在冲突时，更加强调保障安全的重要性。

可见，中国倾向于保障数据安全具有国际政治、本国国情等方面的原因。上述分析表明，主要经济体制定数据规则时都努力平衡各类因素，因为各项政策目标都具有重要性，在此基础上主要经济体具有各自的制度特征，并且在国际上致力于扩大制度影响力，以及提出国际规则诉求。在以上分析的基础上，下面对于中国规则的国内构建和国际竞争提出以下思考。

第一，从经济利益来看，需要更加重视数据利用和流动，促进数据跨境流动。根据 2017 年数字经济的规模，第一世界是美国和中国，美国为 11.50 万亿美元，中国为 4.02 万亿美元。

2021 年，全球 47 个主要国家数字经济增加值规模达到 38.1 万亿美元，其中，中国数字经济规模达到 7.1 万亿美元，位居世界第二。据估计，如果充分利用数字贸易，2030 年中国的数字出口价值将比 2017 年增长 207%，达到 5 万亿元。来自美国、日本和中国三国的数字企业几乎占到 100 强的 70%~80%。然而，虽然中国数字经济实力较强，但中国数字经济的规模与美国相比还有较大的差距。麦肯锡数据显示，中国数字贸易规模位居全球第二，但跨境数据流动量却位居世界第八位，只有美国的 1/5。加强数据出境管控有利于将数据资源留在国内，从而增强国内企业利用数据的能力，但与此同时，中国从跨境数据流动获取的收益也会大大降低，难以获取和利用其他国家和地区的数据，在一定程度上会影响中国数字企业扩大国际市场的能力，不利于数字经济的长远发展。数字领域的资本天然具有国际化的需求和特征，而数据跨境流动则是国际化发展的现实要求。基于中国数字企业具有较大规模、中国数字经济发展态势良好，中国企业在获取和利用数据上具有既有优势和潜在能力。为了增强数字经济实力和国际竞争力，需要采取更多措施促进数据利用和流动：进一步形成促进数据利用和分享的机制，借鉴欧盟于 2022 年 5 月通过的《数据治理法》中相关措施，如在保障个人权利的前提下使得公共部门数据可重复利用、推动企业间有偿共享数据、允许个人在数据中介帮助下使用数据、促进以公共利益为目的的数据使用；审慎考察数据出境安全评估机制，对数据跨境流动进行分级分类管理，如针对关键特定行业、个人的敏感和关键数据加强管理，对其他数据则放松管理，可考虑设定数据出境安全评估的豁免机制，形成数据跨境流动的白名单，以及简化企业数据出境风险自评估环节。

第二，从价值理念来看，可以做好宣传阐释工作，加强与他国制度协调，进一步规范政府使用个人数据行为。中国制定的《个人信息保护法》较为全面地规范了个人信息事项，明确了信息主体的各项权利、信息处理者的义务和责任，但是西方国家仍然认为中国的个人信息保护水平较差。目前的法律既保护个人权利，也较符合中国实际，中国不宜完全向欧盟规定看齐，给企业设置的合规成本不能过高。建议从以下方面做出努力：将法律规定落到实处，真正实现个人信息权利保护；注意收集法律实施过程中的信息，做好法律适用评估工作，可根据《个人信息保护法》等法律制定更加明确且可操作的具体规范；做好增信释疑的宣传工作，表明中国高度重视权利保护的态度，纠正“数字威权主义论”对中国的不实指责；基于其他国家忌惮中国政府获取、使用数据，除了宣传新法律已经规范政府获取、使用数据的行为，还可以制定更加具体的规范，进一步增强政府使用数据的透明度和法律救济力度。

第三，从国家安全来看，坚持重视数据安全的立场，但可借鉴美国的做法，以较为隐蔽的方式保障数据安全。美国在国际上大力主张跨境数据流动，被认为是数据自由流动立场的旗手。与有些国家相比，美国确实倾向于促进数据流动以扩大数字经济效益，但实际上美国也重视数据安全，只是相关措施具有一定的隐蔽性和针对性，例如，主要通过出口管制、外商投资安全审查、国家秘密、受控非密信息、行业规范等措施管控数据安全，并未专门制定管理数据流动的规范，而是在相关机制中进行规范，而且主要对重要公共信息进行管控，针对部分特定国家加强数据管控，以及在某些特定行业规范中做出相关规定。目前中国数据规则重视国家安全，但存在以下问题：对于重要数据的管理要求十分严格，但是重要数据的范围仍不明晰，已有规定仍然较为宽泛和模糊；数据出境安全评估的范围似过大且不明晰，数据出境安全评估实行“一事一议”的行政审查，企业自评估报告在内容方面的制度设置略显冗杂，这可能导致企业合规成本上升、负责安全评估的网信部门承担过重的工作任务，以致影响数据跨境流动的实际效果；同时，数据出境后缺乏有效监管措施，没有形成数据出境活动的事中事后监管机制，而且欠缺责任分配与追究制度。在数字领域需要追求相对安全，即安全价值仅具有首要和基础地位，而不具有终极和最高地位，安全只是发展的基础和前提，需要努力摒弃追求绝对安全的行为。鉴于中国数字经济实力与美国接近，具有与美国进行数字竞争的潜在实力，可借鉴美国做法，采取更具针对性和隐蔽性的措施来保障国家安全，例

如，主要针对特定国家加强数据管控、在相关特定机制和行业规范中明确数据管控措施、使需要管控的公共信息范围更加具体和明确。

第四，从国际规则竞争和协调来看，积极参与数据规则竞争，构建数据流动朋友圈，推广国际规则诉求，并加强与其他制度的协调和融合。目前协调各国数据规则并形成国际规则的需求比较强烈。在需求强烈而又难以形成国际规则的情况下，多种制度的建构会平行持续一段时间，并可能出现以下几种情况：一是各国继续扩大国内制度的影响力，并做好不同制度之间的互操作性工作；二是继续通过双边、区域协定进行合作，扩大现有合作机制的影响范围，并尝试建立新的合作机制，以促使数据在数据流动联盟之间自由流动；三是尝试联通不同的合作机制，扩大数据流动联盟范围；四是不断推动 WTO 等多边平台制定国际数据规则。基于此，中国可做出以下努力：在保障国家安全的前提下，继续积极申请加入《数字经济伙伴关系协定》以及其他涵盖数字经济内容的协定，避免被长期排除在相关数据流动联盟之外；根据国家安全、权利保护以及对等原则，形成并动态调整跨境数据流动的白名单，加强与“一带一路”沿线国家的数字合作和制度协调，从而形成以中国为中心的数据流动圈；基于欧盟在国际上的重要性以及欧盟不寻求遏制中国，应当努力与欧盟形成相对固定的数字合作交流形式，例如欧盟与印度于 2022 年 4 月宣布成立了贸易与科技理事会，称将共同应对贸易、技术安全等领域的挑战，同时还可与欧盟开展关于数据保护水平认定的充分性谈判；在 WTO 等多边平台积极参与国际数据规则的讨论，提出中国方案，贡献中国智慧。

总而言之，中国可以借鉴他国模式，根据本国实际情况和战略需要，动态调整和完善数据规则，在以更加具有针对性和隐蔽性的方式保障国家安全的前提下，促进数据利用和流通，支持数字经济发展，并且积极构建国际数据流动圈，参与构建国际数据规则，扩大各领域的国际化发展。

五、结语

经济利益、价值理念、国家安全等因素在国家形成数据规则和国际规则诉求过程中发挥了重要作用，是形成国家共同观念和相应制度的主要推动力。国家在尽力平衡政策目标的基础上，基于国情、文化和政治等因素形成不同的制度特征。没有哪一个单一因素能够解释所有问题，多种因素助推观念的形成；不同因素成为不同制度特征的主要推动力。制度特征说明某一因素或者某种政策目标居于优先位置，也代表了国家经过平衡和选择而形成的观念体系。这种选择显现了国家的经济实力、价值理念以及国际环境和竞争状态。同时，这种制度特征是相对而言的，国家和地区都在尽力平衡各类政策目标，而且，制度特征也会随着形势变化而改变。可以说，国内制度和国际规则诉求的形成是多种因素推动观念建构并有效平衡的过程，也是明确优先政策目标并有所体现的过程。

一些国家和地区平衡各类因素，确定了优先政策目标并形成国内制度之后，便在此基础上努力影响国际制度构建。它们通过国内法律域外适用的方式扩大国内规则的适用范围和影响力，与其他国家签订双边、区域协定以及建立相应合作机制，在一定程度上形成数据流动联盟，而且在 WTO 等国际平台上提出规则诉求。在这个过程中，主要经济体的国际规则诉求存在差异，形成一定程度的国际竞争，同时在不断谈判和借鉴的过程中进行制度协调和融合，形成相应合作机制来解决共同面临的问题，并朝形成普遍有效的国际规则方向努力。在这个过程中，保护和追求国家利益始终是国家行为的重要目标；形成共同观念是建构国际制度的重要途径；权力政治在国际制度建构中扮演着重要的角色；通过国际协调和合作才能最终形成国际制度。

数据规则与经济利益、权利保护、国家安全等重要问题紧密相关，与各国的社会文化观念存在密切联系，各个国家一般不会轻易改变制度偏好，目前还没有形成广泛的国际共识。

在以上认识的基础之上，中国应当积极面对现状，认真研究和借鉴各国模式及其背后考量因素，根据本国实际情况动态设计和完善国内规则，积极参与国际合作和国际规则构建，从而不断促进中国数字经济发展，服务于中华民族伟大复兴的战略目标。

（本文发表于《安徽师范大学学报》（人文社会科学版）2023 年第 1 期。注释从略。）