

全球竞争格局下的中国特色数据跨境流动治理方案研究

许皖秀¹, 左晓栋^{2*}

(1. 中国科学技术大学管理学院, 合肥 230026; 2. 中国科学技术大学公共事务学院, 合肥 230026)

摘要: 当前, 围绕数据跨境流动为中心的 digital 权力博弈进入白热化阶段, 全球竞争格局已初步形成。我国高度关注数据跨境流动安全治理, 在经历迭代优化后, 目前已形成独具特色的平衡数据安全与发展的治理模式, 这将为破解全球数据治理难题提供中国方案。本文剖析了实现数据跨境安全可信流通面临的多重挑战, 从国际组织、经贸协定、主要经济体三个维度解构了现有的全球数据跨境流动治理竞争格局, 对我国平衡数据安全与发展的治理方案进行全局性的考察。这一方案以总体国家安全观为理论根本, 以“统筹安全与发展”为政策目标, 以安全可信流通为评判基准, 体现出浓厚的中国特色与创新色彩, 并服务于维护国家安全、促进数字贸易、扩大对外开放等战略目标。在此基础上, 本研究从全球视域出发, 提出我国治理方案的后续完善对策, 包括优化治理理念、推动国际合作、突出技术治理、强化人才培养、开展国际宣贯等。

关键词: 全球数据博弈; 数据跨境流动治理; 数据安全; 数字贸易; 中国方案

中图分类号: D92 文献标识码: A

China's Approach to Cross-Border Data Flow Governance in the Context of Global Competition

Xu Wanxiu¹, Zuo Xiaodong^{2*}

(1. School of Management, University of Science and Technology of China, Hefei 230026, China; 2. School of Public Affairs, University of Science and Technology of China, Hefei 230026, China)

Abstract: Currently, the digital power struggle centered around cross-border data flows has entered a critical phase, with the global competition landscape taking shape. China places high importance on the security governance of cross-border data flows and, after several iterations and optimizations, has developed a unique governance model that balances data security and development. This model offers a Chinese solution to the global data governance challenge. This study analyzes the multiple challenges in achieving secure and trusted cross-border data circulation, deconstructing the existing global governance competition from three perspectives: international organizations, trade agreements, and major economies. It provides a comprehensive examination of China's governance model that balances data security and development. Grounded in the overall national security concept, this model aims to “coordinate security and development”, with secure and trusted data circulation as the evaluation benchmark. It reflects strong Chinese characteristics and innovative elements, supporting strategic goals such as national security, digital trade promotion, and expanding opening-up. Based on this, the study offers policy recommendations for the further enhancement of China's governance framework from a global perspective. These recommendations focus on optimizing governance principles, fostering international cooperation, prioritizing technological

收稿日期: 2024-12-06; 修回日期: 2024-12-28

通讯作者: *左晓栋, 中国科学技术大学公共事务学院教授, 主要研究方向为网络空间安全治理; E-mail: xdzu@ustc.edu.cn

资助项目: 中国工程院咨询项目“关于统筹数据发展和安全的治理规则和策略研究”(2023-XBZD-20); 国家社科基金项目(23&ZD335)

本刊网址: sscae.engineering.org.cn

governance, strengthening talent development, and advancing international advocacy initiatives.

Keywords: global data competition; cross-border data flow governance; data security; digital trade; Chinese solution

一、前言

随着云计算、人工智能等新一代信息技术的快速发展，数据正超越传统的土地、劳动力、资本等生产要素，成为驱动新质生产力发展的基础性、决定性资源。全球经济生产活动、技术创新活动对数据要素的日益依赖，使得数据跨境流动需求呈现指数级的爆炸性增长，海量数据跨越国界的流动成为世界经济繁荣的新型指向标。美国布鲁金斯学会的相关研究显示，2014年数据跨境流动对全球经济增长的价值贡献超过2.8万亿美元，预计2025年有望突破11万亿美元^[1]。

随着“9·11”“棱镜门”等事件相继爆发后，数据跨境流动与国家安全、数据隐私保护等议题间的关联性得以被全球认知^[2]。在大国数字权力博弈的背景下，数据正被视为一种等同于石油的新型权力，围绕以数据跨境流动为核心的国际战略资源与话语权争夺使其属性呈现更为复杂的特征。统筹安全与发展，实现数据跨境流动安全可信流通，成为全球的关注焦点。

当前，有关数据跨境流动的研究更多关注的是全球数据跨境流动治理框架；具有典型性的数字贸易协定内容；美国、欧盟等各主要经济体的数据跨境流动法律规则；数据跨境流动合作战略博弈历程等^[3-6]。对于我国数据跨境流动治理方案，现有研究仍多数停留在《促进与规范数据跨境流动规定》（简称《规定》）《网络数据安全条例》（简称《条例》）出台前的旧有观点分析。因此，有必要在全球竞争格局下突出我国的独特贡献，对我国迭代后的平衡安全与发展治理理念及体系展开分析。本研究通过有机结合全球宏观视角与国内微观规则设计理念及治理逻辑，展现中国特色数据跨境流动治理方案的全球性贡献，并对方案的后续完善提出针对性的对策建议。

二、数据跨境安全可信流通面临多重挑战

一般来说，跨境数据流动所指的数据类型与所在国家的监管模式和监管重点有关。例如，欧盟语

义下的数据跨境多指个人数据，美国语义下的数据跨境多指个人数据与商业贸易相关的数据。根据我国的治理框架，本研究所指的跨境数据类型包括个人数据、商业数据以及与国家安全相关的数据等。

（一）数字主权博弈下国家安全风险激增

数据跨境流动与掌握面向未来的战略发展优势以及国家安全高度关联，并成为地缘政治与地缘经济博弈的工具之一^[7]。在数智化时代，数据作为一种等同于石油的生产性资源，拥有的数据数量与质量正成为一国未来发展实力的另一种表征。将马克斯·韦伯对于权力概念的經典定义应用至国际关系领域，行为体在权力关系中所占位置问题，变成了行为体掌握的权力资源种类和多寡的问题。而作为不等价交易和冲突性合作过程的权力关系问题也就转化成了谁拥有权力（权力资源）和由谁来行使权力（影响、控制或支配）的问题^[8]。正因如此，围绕数据资源的抢夺以及数据跨境规则话语权的争夺，正成为大国地缘政治博弈的战场之一。在数字主权意识的主导下，全球数据本地化政策兴起，各国的数据跨境流动圈正形成类似政治同盟圈的现象，以共同价值观排斥特定国家的加入成为圈层内的共识^[9]。但现有的国家间双边合作进程受到战略博弈等因素的影响，也并不全是一帆风顺。安全风险与资源争夺造就了数据跨境流动的政治属性，也塑造了全球数据跨境治理的碎片化趋势。

此外，由于数据广泛分散在多个行业，并且具有高低不同的精度，这也意味着与国家关键基础设施、军事布防等敏感领域相关的数据流动，一旦发生泄露与窃密，将产生严重的国家安全风险。在个人信息领域，正在形成一种新的国家安全风险，那就是当批量的跨境数据与智能化的数据分析技术相融合，将能够准确地掌握一国的公民特征与价值取向，形成民众操作的政治风险^[10]。数据跨境带来国家安全风险的另一来源，在于第三国政府的非法数据访问行为。现有的数据跨境传输主体多为个人与经济组织，数据跨境传输至他国境内后，受到第三国司法与领土的天然管辖，原有数据主体对数据安

全的掌控能力减弱。当第三国存在大量的国家安全与刑事执法目的数据调取法律条款时，便可以此为依据公开或秘密调取本国数据主体或企业的敏感数据，造成另一种维度的国家安全风险。

（二）数据跨境流动引发的数据安全问题趋严

信息科技以及智能化设备的普及改变了人们的工作、生活模式，使得标志个人特征的信息或数据越来越精细、准确化。而个人信息的肆意收集、大规模买卖以及无防护措施的多系统存储，使数字化时代下的每个人都承受着技术非法使用的负面阴霾^[11]。从维护公民数据与隐私的角度出发，以欧盟为辐射中心，全球正掀起轰轰烈烈的数字化时代下的个人数据保卫战。由于数据跨境流动涉及多个主体、多重传输介质，如数据发送方、接收方、中转方，数据所有权和处理权可能被分散至不同的司法辖区，传统以物理位置为基础的隐私保护框架难以覆盖整个数据生命周期。多方参与和传输环节的增加，也为数据在流动中遭受拦截、窃取和篡改提供了更多机会。苹果公司 2023 年发布的报告显示，2021 年和 2022 年，全球共泄露了 26 亿条个人记录^[12]。

基于对国家安全、数字贸易等不同利益的均衡，各国的数据跨境传输法律规则与技术标准呈现分散化的特征，这造成跨境数据的安全性难以通过法律与技术手段得到完全保障。例如，加密技术的标准差异可能导致数据传输过程中无法实现一致性的保护，而政策的不透明性进一步增加了用户隐私被滥用的可能性。在跨大西洋数据跨境传输中，美国和欧盟数据法律体系的非对称性以及美国情报监视法律的扩散，成为笼罩在双方合作历程中挥之不去的阴影。

（三）数据跨境自由流通受阻的负面经贸效应尽显

技术-经济范式理论认为，技术革命推动人类社会的发展，每一次重大技术变革都伴随着相应技术-经济范式的产生。信息科技的变革促使以数据为生产要素、数字服务为核心、数字交付为特征的数字贸易蓬勃兴起，全球贸易的生产链、价值链正有序转向数字化^[13]。数据是数字贸易的基础性资源，数据跨境流动规则作为支撑经济转型的基本载体与重要流通资源，在数字贸易中的地位不断提

升。基于数据跨境流动对数字贸易的重要影响，截至 2023 年年底，涵盖数字经贸规则专章的自贸协定和数字经贸专门协定数量达到 125 项。

在经济全球化的背景下，数据能否跨境自由流动，直接影响数字价值链相关市场主体的商业效率，以及数字市场与数字生态系统的建设。对于大型科技公司与中小型数字企业来说，数据跨境流动是构成其商业模式全球化运作的重要组成部分。通过依靠分布在各个国家的网点，企业可以获得来自用户、公开资源、传感器等的丰富数据，而这些数据在交互、物流、信息推送等方面的运用，可以产生成本降低、绩效提高、流程改善等效果。而在限制性的数据跨境流动政策下，企业参与国际化竞争的成本门槛将大大提高，正常的跨国业务流转也将面临停滞^[14]。对于这些提供数字产品或服务的企业来说，一国的数据跨境流动政策已经成为评估其营商环境的重要考量因素。

（四）以物理位置为判断基准的传统司法管辖模式失效

数据跨境流动的主体是由信息科技进步产生、汇聚的大量数据，但技术的进步正模糊化传统的领土、市场边界，带来新的技术治理困境。互联网技术使得全球进入互联互通的“零距离”时代，在云计算等技术的加持下，数据在物理空间上和经济主体间的转移需求与频率达到了极高的量级^[15]。技术营造的网络空间具有“非矢量同时性”的特征，数字化时代的交易可能会在多个“地点”一次性发生^[16]。随着各国数字基础设施的普及，数据在多国存在技术联结点的情况极为普遍。传统的国家边界与国家市场边界已经难以有效识别并阻挡数据的跨境流动，数据的跨区域流动也不再受到自然地理空间的限制。在大卫·科林格里奇看来，新兴技术的发展在推动社会进步的同时，可能带来“科林格里奇困境”^[17]。数据跨境流动的兴起虽然加速了全球技术的交流与进步，但也带来新的技术治理难题，传统以物理位置为判断基准的司法管辖模式已不再有效。出于数据控制权掌握、技术发展、人权保护等考虑，部分国家选择了具有扩张性的“长臂管辖”模式或保守的数据本地化政策，而这都将引发碎片化数据跨境治理模式的“蝴蝶效应”。

三、全球视域下的数据跨境流动治理与竞争格局

作为全球数据治理格局的重要组成部分，数据跨境流动正成为国际组织、主权国家高度关注的重要议题。受到安全风险、经济发展、政治博弈等多重复杂因素交叉融合的影响，各主要经济体制定了差异化的数据跨境法律规则。对数据安全与发展等利益的分歧，致使全球数据跨境流动治理趋向碎片化。欧盟与美国正分别通过国际规则话语权优势的规范性力量以及强大的互联网技术实力优势，影响全球数据跨境流动治理的走向。

（一）国际组织：推动数据跨境国际合作的中坚力量，但缺乏强制约束力

目前，国际组织凭借自身的国际资源与组织优势，正成为推动全球数据安全治理与国际合作的重要主体。但由于联合国的数据治理作用较有限，多数国际组织形成或发布的协议、倡议并不具备强制约束性，全球数据跨境流动治理仍停留在缺乏统一强制性约束规则的碎片化阶段。

在国际组织中，联合国贸易和发展会议（UNCTAD）致力于推动全球数字贸易和数据治理，倡导强调多利益攸关方参与规则制定，在促进数据自由流动的同时实现可持续发展目标。七国集团（G7）聚焦“可信的数据跨境自由流动”，目前已形成“G7数字贸易原则”、《可信数据自由流动合作路线图》《可信数据自由流动行动计划》等国际合作协议与图谱，并宣布成立新的“伙伴关系制度安排”。经济合作与发展组织（OECD）则将个人数据和隐私保护等伦理问题延伸至跨境数据流动与网络安全领域，通过发布《跨境数据流动宣言》《关于隐私保护和个人数据跨境流动的指南》等文件，为全球跨境数据治理与协调提供“软法”支撑。亚太经济合作组织（APEC）通过跨境隐私规则（CBPR），在亚太地区推动数据跨境流动的自由化与隐私保护并行。该机制强调灵活性和互操作性，为区域内数据治理提供了非强制性的标准。

（二）经贸协定：助力全球数字贸易流动，但存在“政治分化”趋向

数字经贸规则对数字贸易发展兼具“加速器”

和“稳定器”作用。APEC研究报告显示，两个贸易伙伴之间每增加一项数字贸易规则条款，数字服务贸易流量就增加2.3%^[18]。但由于目前全球尚未就数据跨境流动治理形成统一的共识，现有的多边数字贸易规则制定由西方国家主导，故呈现出显著的“政治化”和“阵营化”特征。

在多边协定层面，世界贸易组织（WTO）电子商务谈判历经5年取得实质性进展。2023年12月20日，WTO电子商务联合声明倡议成员就若干全球数字贸易规则形成实质性结论；发布的协定案文包含38个条款和1个电信服务附件，涵盖数字贸易便利化、开放的数字环境以及企业和消费者信任三大领域。由于美国临时撤回一直支持的数据跨境自由流动主张，各成员国就数字贸易利益分歧较大，这一最新协定并未包含数据跨境流动、数字产品非歧视待遇等自由化议题。

在双边及区域协定层面，《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《区域全面经济伙伴关系协定》（RCEP）、《数字经济伙伴关系协定》（DEPA）等作为区域性的高水平经贸协定，均在数字贸易章节中纳入了关于数据跨境流动的条款，这为亚洲、澳洲、美洲等不同大洲的主要国家实现便利、自由的数据跨境流动奠定了基础。在双边或多边协定当中，《日本-欧盟经济伙伴关系协定》《美国-墨西哥-加拿大协定》（USMCA）和《英国-新加坡数字经济协定》（UKSDEA）等的签订，推动了国际数字经济发展的协作化趋势与规则构建。

（三）主要经济体：治理策略各有不同，关注数据主权与国际竞争博弈

数据跨境流动治理议题的多维属性，尤其是与数据主权的高度关联，促使各主要经济体形成了差异化的监管格局，而这一格局，反映出各国在数字时代下深层次的数据战略。

欧盟作为数据跨境流动监管的起源地，具有较高的人权、伦理属性，强调个人人权并防范非法隐形的数据监控。这一监管模式将人权视为实施数据本地化政策的合法理由，并通过输出价值观与规则掌握对全球的规范性权威。通过《数据保护指令》《通用数据保护条例》，欧盟逐步建立起数据跨境流动治理的全球话语权中心地位，确立了适用于不

同的主体、场景的数据跨境流动监管规则，如充分性认定、约束性企业规则、标准合同条款、数据保护认证等。目前，欧盟已通过数据保护充分性认定与全球 15 个国家或商业组织达成数据跨境流动合作。

与欧盟坚持强调基本人权保护的范式不同，美国对个人数据的跨境流动基本不设置监管规则，倡导数据跨境自由流动，依赖行业自律和州级法律进行数据治理。对于关键基础设施、金融、人工智能关键技术等重点领域，美国也施加了隐形的数据出境限制措施。这一监管模式植根于美国全球互联网霸主的技术地位，并凸显其欲通过硅谷科技巨头收割全球数据的野心。在美国国内，尚未建立统一的数据隐私法律体系，相关立法分散于州级以及电信、医疗等不同的行业。作为全球互联网科技巨头的聚集中心，美国掌握了汇聚全球数据的隐形权力，这成为其实施自由化监管模式的重要原因。这种松散、自由的监管模式，为美国的数据跨境流动国际合作赢得了比较优势。美国通过与世界上主要国家或地区建立双边协议、国际协议、数字贸易协定等途径构建起由其主导的数据跨境流动国际合作体系，如《欧盟-美国数据隐私框架》等。

除欧盟、美国之外，日本、印度、俄罗斯等国家也形成了完整的治理规则。日本采取了折中欧盟统一式立法与美国分散式立法的模式。日本国内层面通过《个人信息保护法》等基础法规构建数据跨境治理框架，国际层面则秉持“可信任数据自由流通”原则，积极参与双边、多边数据跨境治理合作，这种模式有助于在数据跨境流动治理中平衡隐私保护与数据自由流动^[19]。印度以数据本地化政策为核心，强调数据主权和国家控制。2023 年 8 月，印度发布第一部综合性个人数据保护法——《数字个人数据保护法》。该部法律将监管对象从敏感个人数据扩大到个人数据，淡化了绝对禁止个人数据跨境传输的立场，但由于缺乏个人数据跨境传输的法定情形，监管力度仍处于较为严苛的状态^[20]。俄罗斯的数据治理政策围绕数据本地化展开，通过《联邦个人数据保护法》对跨境数据做出了严格的规定，对个人信息保护实施严格的监管，针对国内、国外两个层次形成了“内外双严”保护数据主权的法律特征^[21]。

四、中国特色数据跨境流动治理方案的全局考察

相较于美国、欧盟，我国数据跨境流动治理方案的构建起步较晚。也正因如此，欧盟与美国的数据跨境流动管理制度与法律规则对我国治理方案的形成产生了一定影响。在经历了有序迭代的过程后，我国最终形成了体系化的数据跨境流动治理方案^[22]。相较于欧盟与美国，这一方案以总体国家安全观为核心理论基础，以统筹安全与发展为政策目标，以安全可信流通为评判基准，体现出浓厚的中国特色与创新色彩。对内，这一方案服务于维护国家安全、优化营商环境、促进数据要素流通利用的政策导向；对外，服务于扩大对外开放与国际合作、吸引外商投资、申请加入高水平经贸规则的国际战略。

（一）以总体国家安全观为理论根本

总体国家安全观是指导我国数据出境安全管理制度建立的理论根本。2014 年 4 月，习近平总书记创造性地提出了总体国家安全观。这是一个内容丰富、开放包容、不断发展的思想体系^[23,24]。在后期完善的过程中，这一理论正式将网络安全、数据安全等非传统安全确定为国家安全领域之一。《中华人民共和国国家安全法》的出台，明确将“国家建设网络与信息安全保障体系”等任务提升至法律义务的层级，将我国网络安全与数据安全建设正式纳入法治轨道。在总体国家安全观的指导下，数据安全成为我国战略布局的重点，强调保护个人信息权益与国家安全“双轨并行”的数据治理制度逐步建立^[25]。

（二）迭代形成统筹安全与发展的法律框架

国家对数据跨境流动的高度关注，使我国的治理方案处于逐步优化的过程。因此，与欧盟法典化的立法模式不同，我国数据跨境流动法律规则分散于法律、法规与多部门规章当中，并经过逐步迭代最终确立基本的法律框架。《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》4 部法律奠定了我国数据跨境流动规则的法律基础。

《中华人民共和国国家安全法》第八条明确国家安全工作应当统筹内部安全和外部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，这成为统领我国数据跨境流动规则制定的基本导向。《中华人民共和国网络安全法》第三十七条将关键信息基础设施运营者对个人信息和重要数据的境内存储义务予以明确，但依据“法无禁止皆自由”的原则，关键信息基础设施运营者之外的数据处理主体可自由开展数据跨境流动行为，该规定遗留了较大的安全敞口。《中华人民共和国数据安全法》第三十一条对这一缺陷进行了弥补，规定其他数据处理者开展重要数据出境也应当满足国务院与网信部门发布的文件要求。但这仍然存在一个问题，因为该条款并未对个人信息跨境流动的问题予以解答，《中华人民共和国个人信息保护法》的出台真正解决了我国数据跨境法律框架确立的基本问题，第三章以专章的形式对个人信息跨境提供的规则予以明确，规定了数据出境安全评估、标准合同条款、个人信息保护认证、国际条约、协定以及其他的数据出境合规途径。在这4部法律的支撑下，我国数据跨境流动的法律框架已初步明确。

在以上4部上位法逐步出台后，我国的立法重点进入一个新的阶段，即如何落实这4部法律当中对数据跨境流动安全治理提出的要求。基于此，首先相继出台《数据出境安全评估办法》《个人信息出境标准合同办法》《个人信息保护认证实施规则》，初步构建起我国数据跨境传输机制的操作细则。之后《规定》《条例》等高层级的法律文件相继颁布，对前一阶段存在的规则过于严苛、模糊等问题进行纠正。这些文件的出台，不仅落实了我国统筹安全与发展的数据跨境流动治理理念，也极大地增强了整套方案的细致性与可操作性。目前，我国针对重要数据与批量个人信息出境的数据跨境流动监管制度已走向成熟。

（三）行之有效、重点突出的治理体系

数据分类分级制度是我国数据跨境流动安全治理的重要抓手，这一制度除了充当科学管理分门别类的海量数据工具外，还在于在非国家秘密信息领域，识别、保护对国家安全产生重要影响的重要数据。这一治理制度顺应了国际趋势，借鉴自美国受控非密信息管理制度以及在商业领域提出的“受保

护信息”概念。《中华人民共和国网络安全法》首次提出重要数据，但在这一阶段，分类分级的思路和方案均站在组织内部的视角，目的是提升组织的数据安全管理能力和水平。《中华人民共和国数据安全法》第二十一条通过规定“国家建立数据分类分级保护制度”，将数据分类分级任务上升至国家层级，这将在构建我国“外向型”数据主权战略之中发挥重要作用^[26]。目前，我国已经形成核心数据禁止出境，重要数据经过安全评估后可以出境，一般数据可自由流动的基本规制思路。

重要数据安全管理制度是确保我国数据治理方案安全目标实现的重点。在最新发布的国家标准中，重要数据被描述为特定领域、特定群体、特定区域或达到一定精度和规模的，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、公共健康和安全的的数据，而仅影响组织自身或公民个体的数据一般不被识别为重要数据。值得注意的是，重要数据的识别仍然以总体国家安全观为核心，其目标在于识别军事、经济、科技等领域中关系国家、社会、公民的具有特殊安全影响的数据^[27]。在此基础上，围绕重要数据目录、重要数据处理者的特别义务和责任、重要数据处理前的风险评估等，我国通过《条例》建立了完整、细化、可操作的具体规则，这表明我国这一具有创新性的重要数据安全管理制度已基本成熟。

基于总体国家安全观中的网络安全与数据安全，我国设立了网络安全审查与数据安全审查制度，目的在于防范可能产生的网络安全、数据安全风险。我国原有的网络安全审查制度针对关键基础设施运营者采购网络产品和服务的安全风险防范而设立，但随着网络平台日益掌握大量重要数据与批量个人信息，其业务与关键信息基础设施相关联。在某种意义上，大型网络平台已经成为新的关键信息基础设施运营者，滴滴全球股份有限公司在美国上市触发了我国改革网络安全审查制度的进度。2022年修订后的《网络安全审查办法》第二条、第七条，将网络平台运营者开展数据处理活动以及赴国外上市的活动纳入审查范围，防范核心数据、重要数据或大量个人信息可能产生的安全风险。这体现出我国网络安全审查制度的不断向前发展态势。相较于网络安全审查制度，《中华人民共和国数据安全法》第二十四条设立的数据安全审查制度适用

范围与实施机制并未明确。但可以肯定的是，网络安全审查制度并不等同于数据安全审查制度，前者只是后者在网络数据领域的实施，而更完备的数据安全审查制度仍待建立。

为了避免监管主体设立过多造成的冗杂，我国在原有监管体制基础上迭代形成了多主体、体系化的协同治理制度。一是从数据与国家安全高度关联的战略高度，由中央国家安全领导机构设置国家数据安全协调机制，负责推动国家数据安全战略和有关重大方针政策的落实落地，指导各地区、各部门加强协作与配合，推进数据安全领域全局性、基础性、关键性工作。二是在数据安全具体监管事项层面，由国家网信部门统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。根据数据所涉及的保护、利用情形，以及由数据引发的行政监管、产业开发、刑事犯罪、政治安全等不同性质的事件，形成由国家网信部门、国家数据管理部门、公安机关与国家安全机关“三足鼎立”的监管格局。三是将治理层级细化至基层，我国将数据跨境监管的权力部分下放至自由贸易区。自由贸易区可自行指定需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单。在公布负面数据清单之外的数据，可自由跨境流动，这赋予了自由贸易区更大的开放力度与自主权，也与我国对自由贸易区“开放排头兵”的定位相符合。

（四）开放便利的数据跨境流动传输机制

以安全、便利为导向，我国目前形成了3种有效的数据跨境流动传输机制。数据出境安全评估继承了我国对国家安全、数据安全的战略性考量，是现有3种机制中的创举。相较于其他两种机制，数据出境安全评估的启动条件具有强制性，并且与其他机制不属于并列关系，可理解为在符合条件前提下企业开展数据出境活动的“必选题”。根据《规定》，这一机制的适用主体为关键信息基础设施运营者，以及自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息的普通数据处理者。在实践当中，随着各省数据出境安全评估申报指引与相关程序的建立，已有包括海康威视数字技术股份有限公司、

支付宝（中国）网络技术有限公司等不同类型的企业顺利通过数据出境安全评估。

个人信息保护认证机制与标准合同条款主要借鉴于欧盟，并充当数据出境安全评估的补充性角色，与国内的衔接性较高。个人信息保护认证制度囊括个人信息处理活动与个人信息跨境提供两种情形的安全认证，该机制的实施细则由《信息安全技术 个人信息跨境传输认证要求》（征求意见稿）补充。但由于这一机制仍在建设当中，公开披露的认证案例较为稀少，并不能成为国内企业首选的数据跨境传输合规机制。相较于个人信息跨境传输认证，标准合同条款这一传输机制在我国逐渐成熟，已有多家企业通过这一机制实现数据跨境传输。这一机制采用的“自主缔约与备案管理相结合”的原则，适用于少量、批次的数据出境行为。在香港和澳门地区，我国专门发布了《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》，通过发挥粤港澳大湾区的先行先试作用，率先实现了机制的创新应用。

在优化、创新上述传输机制的应用外，我国还通过明确多种豁免监管的情形，突出已有数据跨境流动监管规则的明确性与合理性。在商贸、生产、学术交流等数据跨境流动最为频繁的领域，《规定》补充了多项豁免情形，这将为跨境人员交流与商贸往来提供便利。《条例》通过围绕《中华人民共和国个人信息保护法》第十三条构建的个人信息处理合法性基础框架，规定了便利化数据跨境流动的要求，在已有的数据出境安全评估3种途径之外明确了其他合法流动的豁免情形。例如，为订立或履行个人作为一方当事人的合同所需、实施跨境人力资源管理、履行法定职责或者法定义务等5种情形。这与欧盟发布的《通用数据保护条例》中规定的克减条件基本保持一致。

（五）顺应国际趋势的数据跨境合作规则

在全球数字化转型的背景下，数据跨境流动国际合作有助于降低数字贸易壁垒与合作成本，创造繁荣的贸易市场。也正因如此，创建与国际接轨、便利操作的合作通道成为我国数据跨境流动治理方案的重点之一。在《中华人民共和国数据安全法》中，第十一条就明确规定：国家积极开展数据安全

治理、数据开发利用等领域的国际交流与合作。在《中华人民共和国个人信息保护法》中，数据跨境流动国际合作的重要性被再次提及，第三十八条明确提出中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和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。这相当于从法律角度正式明确国际条约作为数据跨境流动国际合作的合法通道之一。截至2024年10月，我国已明确与德国、新加坡、欧盟等国家或地区达成建立数字政策对话机制的共识，为我国后续与其他国家开展数据跨境流动合作奠定基础。

同时，为了严防境外司法、执法机构以数据调取活动为名实施“长臂管辖”等非法行为，反抗以国家安全为名变相实施歧视性的数据安全监管，我国建立了跨境数据司法调取审批制度与对等反制制度。《中华人民共和国数据安全法》第二十六条、第三十六条对这两种制度的主要内容分别进行了概述。跨境数据司法调取审批制度的设置体现了对于合法合规向外国司法或者执法机构提供数据的重视，明确了我国处理外国司法或者执法机构关于提供数据请求的一般原则，同时也是依法应对少数国家肆意滥用“长臂管辖”，防范我国境内数据被外国司法或执法机构不当获取。对等反制制度以维护国家安全和利益为出发点，明确了我国解决外国在数据领域投资、贸易领域实施歧视的立法主张，体现了平等、公正维护网络空间数据主权的立法思想。

五、对策建议

相较于欧盟与美国，我国探索出了新型的平衡数据安全与发展的治理路径，这是对全球数据治理的创新性贡献。面向未来，为扩大我国数据跨境流动治理方案的全球影响力，需要针对方案本身及其应用等开展新一轮的工作。具体来说，可从优化治理理念、扩大国际合作、强化技术治理、开展国际宣贯等角度展开。

（一）优化治理理念，构建与国际并轨的数据跨境传输机制

目前，我国治理方案重点关注数据单向出境，对数据入境情形的规制理念与方法缺乏。同时，对比国际通行的欧盟数据跨境管理制度，我国增强规

制的国际互操作性仍然存在一定的差异。基于此，优化现有数据跨境传输机制，提高治理方案的完备性与科学性很重要。

首先，应以数字经济全球化布局为规划重心优化治理理念，同步考虑现有规则对我国企业数据入境的影响，优化建立客观公正的数据跨境监管规则与实践。其次，考虑到我国落地实施个人信息跨境传输认证机制还存在认证对象、认证主体资质不明确等问题，有必要通过严格规定认证对象、逐步放开认证机构准入、明确主管部门职责、强化对认证机构的监督等途径推动该机制的落地。在针对跨境电商、金融科技等重点行业，率先实现认证机制的应用。最后，可借鉴欧盟的制度设计，依据《中华人民共和国个人信息保护法》第三十八条，探索引入新的数据跨境传输机制，如数据保护充分性认定、约束性企业规则。通过优先对欧盟、东盟等主要经济体进行试点，逐步建立规则完善的实施机制，建立中国版本的新型数据跨境传输通道。

（二）注重“以点带面”，逐步扩大数据跨境流动国际合作

在已有的法律框架下，我国可发挥自贸区在对接高水平经贸规则中的作用，加快数据清单机制的建立与完善，探索在粤港澳大湾区等跨法域、拥有海量数据跨境流动场景的地区开展先行先试，推动可信数据跨境流动空间的建立。同时，依托与德国、新加坡、欧盟等国家或地区达成建立数字政策对话机制共识的契机，率先在这部分地区达成数据跨境流动国际合作，突破现有的国际数据联盟包围圈层。通过“以点带面”式的推进策略，开展涵盖数据流动的多边协定谈判，形成高水平数字贸易规则框架。目前，我国已完成中国-秘鲁、中国-新加坡自由贸易协定的升级，中国-东盟协定升级谈判已实质性结束。下一步，可在RECP以及现有升级贸易协定的基础上，加快对接CPTPP、DEPA等高水平经贸规则。

数字基础设施对于构建开放共赢的全球数字合作格局具有基础性作用，应成为我国扩大国际合作的“破局”关键点之一。为此，我国可率先通过与“一带一路”共建国家着手建设面向全球的数字贸易数据基础设施，打造国际化数据服务网络、建立国家级数字贸易数据枢纽以及跨境数据传输专用网

络和安全节点，为跨境电商、云计算和数字服务提供高效、安全的数据流动支持。完善的国际性数字基础设施以及运作良好的区域性数据跨境流动合作框架，为我国赢得数据跨境国际合作实践优势，并助力新一轮的对外扩大开放。

（三）突出技术治理，加快新兴数据安全技术的研发应用

数据跨境流动具有虚拟性等特征，且涉及不同的软硬件技术载体，单纯的法律规则与政府监管已经难以全面覆盖数据跨境流动的治理难题。随着跨境数据流动的不断增加，技术治理工具的研发与统一的技术标准显得尤为重要，特别是在数据传输协议、加密技术、安全性验证等方面。安全技术治理工具的应用有助于实现数据安全与隐私保护，保障数据的合规性与可追溯性，同时提升跨境数据流动的效率与灵活性。我国虽已形成完备的治理方案，但现有方案中对技术治理的关注度并不够高，需要进一步优化。

从国际趋势来看，隐私增强技术（PETs）的研发与应用正得到更多的关注。2023年，美国发布的“推进隐私保护数据共享和分析的国家策略”中，多次引用PETs。2024年10月，欧洲政策研究中心（CEPS）发布的报告中认为，PETs可在跨大西洋数据跨境传输中发挥关键作用。在这之后，英国政府科学、创新和技术部（DSIT）的责任技术采用小组（RTA）与英国信息专员办公室（ICO）合作创建并联合发布了PETs成本效益意识工具，加强PETs的基础研究和技术突破。基于此，PETs应成为我国推动技术治理工具开发的首要突破点。我国可通过加大对同态加密、差分隐私、联邦学习、多方安全计算等核心技术的研发投入，解决现有技术在计算效率、扩展性和适用场景上的瓶颈问题。选择数据密集型行业（如医疗、金融、人工智能）开展PETs应用示范，验证技术在跨境数据共享、隐私保护和安全计算中的实用性，推进PETs在实际场景中的应用示范，构建跨境数据传输的互操作性框架。

（四）强化人才先行，建立高水平治理人才的选拔与培育机制

全球数据跨境流动带来了多重属性交织的复杂治理议题，使得加快建立高水平治理人才的选拔与

培育机制愈发重要。要实现这一目标，需要构建融合国际政治、经济、法律，以及网络与数据安全技术的跨学科教育体系。课程设计应突出全球数据治理法律法规、技术标准、网络安全技术（如加密与区块链）等内容。通过建立合规与技术并重的培养模式，帮助学生掌握政策法规、解决数据安全与隐私问题的技术能力及跨领域综合能力。

在人才选拔层面，应采取多维度评估机制。通过建立学习与问题解决能力、学术成绩、国际视野、批判性思维等方面的综合考核标准，确保候选人能够应对跨境数据治理中的复杂挑战。在评估过程中，可结合案例分析、模拟场景等实践型评价方式，检验学生的创新能力与问题解决能力。同时，选拔标准应结合全球数据治理的最新发展，检测其对数据流动治理的理解与应对能力，以便为参与国际合作与政策制定提供支持。

进一步而言，实践导向的培养机制是人才培养成功的关键。高校应加强与国内外顶尖企业、国际组织的合作，开展联合培养和实习计划，为学生提供真实的国际实践机会，增强跨文化沟通与合作能力。课程设置中应融入实训项目，通过技术实验、合规模拟、国际法律案例等环节，让学生在实际操作中掌握数据跨境流动中的关键技术与法律规范。此外，高校可建立学术与行业双向反馈机制，通过“产学研”结合、国际标准更新等方式，不断完善人才培养体系。

鉴于全球数据治理的快速发展，人才培养必须具备动态适应性。应构建终身教育体系，为现有从业人员提供继续教育机会。通过结合国际、国内数据跨境流动法规更新和新兴技术进展，推动持续的技能提升，培养学生在全球视野下的政策应对能力，使其能够在日益复杂的全球数据治理环境中，发挥关键作用。

（五）开展国际宣贯，重塑我国国际话语权与影响力

欧盟与美国通过前期的规则、技术地位，赢得了国际话语权优势。对比之下，我国数据跨境流动治理的全球影响力仍有待提高，这不利于治理方案的应用与普及。有必要在方案的后期优化中，将重塑我国国际话语权与规则影响力提上日程。

首先，我国需要在国际社会加强对中国特色数

据治理方案的解读,推动“平衡安全与发展”模式的宣贯。通过联合其他国家共同起草涵盖数据保护、跨境传输规则、风险应对机制等的新型数据规则,提升中国方案的适用性和吸引力。其次,以《全球数据跨境流动合作倡议》的发表为契机,积极参与多边组织框架下的规则谈判,推动我国主导的议题进入国际组织的数据治理框架中,强调公平、包容的跨境数据规则,确保发展中国家的利益得到兼顾。最后,提高我国在全球数据技术标准的领导力。推动国内企业和科研机构深度参与国际标准化组织、国际电信联盟等国际组织的技术委员会工作,以数据格式兼容性、传输协议安全性和隐私保护技术为重点,形成具有国际竞争力的技术标准体系。通过与东盟、亚洲、拉美等国家与地区合作,建立区域化技术标准对接机制,推进区域标准互认,形成国际化技术标准生态圈,扩大我国标准的影响范围。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: December 6, 2024; **Revised date:** December 28, 2024

Corresponding author: Zuo Xiaodong is a professor from School of Public Affairs, University of Science and Technology of China. His major research field is cyberspace security governance. E-mail: xdzuo@ustc.edu.cn

Funding project: Chinese Academy of Engineering project “About Coordinating Data Development and Security Comprehensive Research on Governance Rules and Policies Investigate” (2023-XBZD-20); National Social Science Fund Project (23&ZD335)

参考文献

- [1] Manyika J, Lund S, Bughin J, et al. Digital globalization: The new era of global flows [EB/OL]. (2016-02-24)[2024-11-25]. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>.
- [2] Burri M. Cross-border data flows and privacy in global trade law: Has trade trumped data protection? [J]. *Oxford Review of Economic Policy*, 2023, 39(1): 85–97.
- [3] 茶洪旺, 付伟, 郑婷婷. 数据跨境流动政策的国际比较与反思 [J]. *电子政务*, 2019 (5): 123–129.
Cha H W, Fu W, Zheng T T. International comparison and reflection on cross-border data flow policies [J]. *E-Government*, 2019 (5): 123–129.
- [4] 陈兵, 徐文. 数据跨境流动的治理体系建构 [J]. *中国特色社会主义研究*, 2021, 12(4): 67–75.
Chen B, Xu W. Establishing a governance system of the flow of data across borders [J]. *Studies on Socialism with Chinese Characteristics*, 2021, 12(4): 67–75.
- [5] 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 [J]. *西安交通大学学报(社会科学版)*, 2021, 41(5): 94–103.
Shan W H, Deng N. Conflict, coordination and reference of trans-border data flow regulation between the EU and the U.S.: Comment on the “schremsii” of CJEU [J]. *Journal of Xi'an Jiaotong University (Social Sciences)*, 2021, 41(5): 94–103.
- [6] 冯硕. 美国数据霸权的建构与法律应对 [J]. *太平洋学报*, 2023, 31(8): 45–58.
Feng S. Construction of the U.S. data hegemony and China’s legal responses [J]. *Pacific Journal*, 2023, 31(8): 45–58.
- [7] O’Hara K, Hall W. *Four internets: Data, geopolitics, and the governance of cyberspace* [M]. Oxford: Oxford University Press, 2021.
- [8] Timasheff N S. The basic concepts of sociology [J]. *American Journal of Sociology*, 1952, 58(2): 176–186.
- [9] Cory N, Dascoli L. How barriers to cross-border data flows are spreading globally, what they cost, and how to address them [EB/OL]. (2021-07-19)[2024-11-25]. <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>.
- [10] 孙宝云, 李艳, 齐巍. 网络安全影响政治安全的微观分析——以“剑桥分析”事件为例 [J]. *保密科学技术*, 2020 (4): 27–34.
Sun B Y, Li Y, Qi W. Micro-analysis on the influence of network security on political security—Taking “Cambridge analysis” as an example [J]. *Secrecy Science and Technology*, 2020 (4): 27–34.
- [11] University D, Li W, Leung A, et al. Where is IT in information security? the interrelationship among IT investment, security awareness, and data breaches [J]. *MIS Quarterly*, 2023, 47(1): 317–342.
- [12] Apple. Report: 2.6 billion personal records compromised by data breaches in past two years—Underscoring need for end-to-end encryption [EB/OL]. (2023-12-07)[2024-11-25]. <https://www.apple.com/newsroom/2023/12/report-2-point-6-billion-records-compromised-by-data-breaches-in-past-two-years/>.
- [13] Perez C. Technological revolutions and techno-economic paradigms [J]. *Cambridge Journal of Economics*, 2010, 34(1): 185–202.
- [14] 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, 146(2): 34–44.
Chen B. The legal approach to compliance governance of cross border data flow in digital enterprises [J]. *Research on Rule of Law*, 2023, 146(2): 34–44.
- [15] World Economic Forum. *Agile governance: Reimagining policy-making in the Fourth Industrial Revolution* [R]. Davos Kloster: World Economic Forum, 2018.
- [16] Kobrin S J. Territoriality and the governance of cyberspace [J]. *Journal of International Business Studies*, 2001, 32(4): 687–704.
- [17] Mayne A J, Collingridge D. The social control of technology [J]. *The Journal of the Operational Research Society*, 1982, 33(8): 771.
- [18] 中国信息通信研究院. 全球数字经济规则年度观察报告 (2024年) [EB/OL]. (2024-09)[2024-11-25]. <https://www.caict.ac.cn/kxyj/qwfb/bps/202409/P020241212359348707348.pdf>.
China Academy of Information and Communications Technology. Annual observation report on global digital economic and trade rules (2024) [EB/OL]. (2024-09)[2024-11-25]. <https://www.caict.ac.cn/kxyj/qwfb/bps/202409/P020241212359348707348.pdf>.

- ac.cn/kxyj/qwfb/bps/202409/P020241212359348707348.pdf.
- [19] 薛志华, 曾德华, 孟奇勋. 日本跨境数据流动监管的制度实践及中日合作展望 [J]. 国际贸易, 2024 (6): 24–31.
Xue Z H, Zeng D H, Meng Q X. Institutional practice of cross-border data flows regulation in Japan and prospects for Sino-Japanese cooperation [J]. *Intertrade*, 2024 (6): 24–31.
- [20] 范婴. 印度数据本地化的范式评述及其对中国的启示 [J]. 中国科学院院刊, 2023, 38(8): 1177–1186.
Fan Y. Paradigm review of data localization in India and its implications for China [J]. *Bulletin of Chinese Academy of Sciences*, 2023, 38(8): 1177–1186.
- [21] 王超. 数据安全视角下国际数据跨境流动模式分析 [J]. 保密科学技术, 2023 (1): 14–19.
Wang C. Analysis of international data cross-border flow mode from the perspective of data security [J]. *Secrecy Science and Technology*, 2023 (1): 14–19.
- [22] Xu W X, Wang S, Zuo X D. Global data governance at a turning point? Rethinking China–U.S. cross-border data flow regulatory models [J]. *Computer Law & Security Review*, 2024, 55: 106061.
- [23] 刘跃进. 非传统的总体国家安全观 [J]. 国际安全研究, 2014, 32(6): 3–25, 151.
Liu Y J. Non-traditional concept of overall national security [J]. *Journal of International Security Studies*, 2014, 32(6): 3–25, 151.
- [24] 许皖秀, 左晓栋. 关于借鉴欧盟政策加强个人信息跨境传输安全认证制度建设的建议 [J]. 网络安全与数据治理, 2022, 41(12): 40–44.
Xu W X, Zuo X D. Suggestions on learning from EU policies to strengthen cross-border transfer of personal information for the construction of a security certification system [J]. *Cyber Security and Data Governance*, 2022, 41(12): 40–44.
- [25] 梅傲, 陈子文. 总体国家安全观视域下我国数据安全监管的制度构建 [J]. 电子政务, 2023 (11): 104–115.
Mei A, Chen Z W. System construction of data security supervision in China from the perspective of overall national security concept [J]. *E-Government*, 2023 (11): 104–115.
- [26] 洪延青. 国家安全视野中的数据分类分级保护 [J]. 中国法律评论, 2021 (5): 71–78.
Hong Y Q. Data classification and hierarchical protection in the vision of national security [J]. *China Law Review*, 2021 (5): 71–78.
- [27] 左晓栋. 我国数据安全法治治理体系建设的回顾与展望 [J]. 国家治理, 2023 (23): 32–37.
Zuo X D. Review and prospect of the construction of data security governance system by law in China [J]. *Governance*, 2023 (23): 32–37.