统合法律理论视角下数据跨境流动的困境与因应

刘　建[1]，朱　沁[2]

（1. 中国农业大学 人文与发展学院，北京　100083；2. 清华大学 法学院，北京　100084）

摘要：在互联网时代，数据跨境流动在推动国际贸易、科技创新和文化交流的同时，也面临着国家安全、数据主权安全与个人隐私保护等多重挑战。立足于数据法治的价值多元性特征，构建三维统合的法律分析框架，深入剖析跨境数据流动的价值、规范与事实要素已成为协调数据安全与数据流动的重要议题。跨境数据流动是价值、规范和事实综合作用的结果，集中表现为价值维度经济利益与安全诉求的深层张力、规范维度自由流动与强力保护的制度冲突以及事实维度主权博弈与治理需求的实践错位。为了有效破除跨境数据流动壁垒，未来可以构建三位一体的治理体系，即在价值层面，建立经济利益与安全风险动态平衡的协同机制；在规范层面，形成法律协调与国际合作的双轮驱动框架；在技术层面，完善可操作性强的管理措施与实施方案，最终实现跨境数据流动的法治化和规范化发展。

关键词：数据跨境流动；统合法律理论；数据主权；数据自由流动；数据安全

[中图分类号]D922.29　[文献标识码]A　[文章编号]1002-4034(2025)06-0062-16

引　言

随着信息技术的迅猛发展，数字经济蓬勃兴起，数据跨境流动作为数字经济的重要组成部分，已成为推动全球经济增长的重要引擎。然而，不同国家对于数据跨境流动的法律规制存在显著差异，使得全球数据的自由流动和有效利用存在壁垒。中国作为数字经济大国，始终高度重视数据跨境流动问题。随着《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》(以下分别简称《网络安全法》《数据安全法》《个人信息保护法》)的出台和实施，中国

[收稿日期]2024-12-05

[基金项目]国家社会科学基金一般项目“老龄社会背景下数字治理与法治融合机制研究”(25BFX009)

[作者简介]刘建(1981—　)，男，山东莱芜人，中国农业大学人文与发展学院副教授、博士生导师，北京市习近平新时代中国特色社会主义思想研究中心研究员，博士，研究方向：民商法、数字法学、劳动与社会保障法；朱沁(1993—　)，女，浙江义乌人，清华大学法学院博士后，研究方向：行政法学、数据法学

已形成了以总体国家安全观为指导、具有中国特色的数据相关法律体系[①]。然而，在数据跨境流动的具体实践层面，仍存在着诸多亟待解决的问题。如何在保障国家安全和数据主权的前提下，制定和实施数据跨境流动的相关政策和法规？如何平衡数据流动与数据保护之间的关系，以提升中国在全球数据治理中的话语权？这些问题不仅关乎中国数字经济的健康发展，也影响着中国在全球数字经济竞争中的地位和影响力。

哲学家莱特(Brain Leiter)提出，互联网时代的人类认识论发生了显著转变，从早期的“本质因果”依赖逐渐转向对认知权威(epistemic authorities)的倚重(Leiter，2022)。在法学理论领域，围绕“回到哈特”(Back to Hart)命题的探讨更是将这种转变推向了高潮。自然法主义虽然具有一定的影响力，但在大数据语境下，难免存在时代局限性。有鉴于此，本文拟立足于巴西法学家莱尔(Miguel Reale)提出的统合法律理论框架，从价值维度、规范维度和事实维度对跨境数据流动壁垒进行系统分析(Lima，2008)。其中，价值壁垒体现为不同国家和地区在数据隐私、安全保护及个人自由等价值取向上的差异，规范壁垒源于现行法律规范在适应数据跨境流动需求时存在的滞后性与不足，事实壁垒则聚焦于数据跨境流动实践中所遭遇的技术瓶颈、经济成本与地缘政治等实际问题。总体而言，统合法律理论框架可以在综合考虑价值多元性、规范适应性和事实动态性的基础上，构建一个规范、包容、有序的数据治理框架，驱动全球数据资源高效、安全流通。

一、问题的提出：数据跨境流动的壁垒困境

在统合法律理论框架的视角下，法律不再被看作孤立的实体，它与社会价值、经济活动及社会行为紧密相连。同样，跨境数据流动壁垒也由此成为一个融合价值性、规范性与社会性的系统工程。

(一)价值层面的多维度冲突

理念是行动的先导。当今世界面临百年未有之大变局，考虑到各国国情不同，其对于数据跨境流动的态度也差别迥异，进而直接影响到了规范层面和实践层面的跨境数据流通治理。

1. 数据跨境流动中的多元价值导向

在数据跨境流动治理中，各国基于政治、经济及文化差异形成了多元化的价值立场。中国的数据跨境流动涉及数据治理、法律规制与政治考量等多维因素，其价值取向涵盖数据主权理论、道德主义理论以及现实主义理论。然而，这些不同维度的价值指向之间如何协调、冲突如何化解，目前仍缺乏系统性整合方案(尉明洋，2025)。有鉴于此，应对数据跨境流动过程中不同国家的价值立场进行类型化总结，进而系统分析不同价值之间的关联性。法律道德主义和法律形式主义是主要价

①关于数据安全的法律体系争议，参见翟志勇：《数据安全法的体系定位》，载《苏州大学学报(哲学社会科学版)》2021 年第 1 期，第 73-83 页。

值类型。前者强调在数据跨境流动中应当保证实质公平，后者则更加强调逻辑正义（尉明洋，2025）。但问题在于，其一，这种分类标准以特定国家的治理实践为范式基础，本质上属于价值负载型分类方法，未能实现理论建构所需的价值中立性。其二，这种分类标准过度聚焦公平与正义的二元价值维度，未能充分容纳数据跨境流动中多元价值的复杂谱系。这尤其体现在以美国为代表的立法实践中，其政策法规根本上体现了效率优先、市场自治等差异化价值取向。比如，《美墨加协定》《跨太平洋伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》中的数据保护条款，都在一定程度上强调数据跨境流动的自由价值。其三，其秉持的公平与正义价值本质上是一种国际关系视角下的分配正义观。这种观点将数据跨境流动治理简化为国家间规则与利益的协调问题，一定程度上忽视了对各国国情的差异化处置。

因此，在划定不同类型的价值立场时，不仅需要考虑国家和国家之间的关联，更要考虑国家自身的追求。其一，就自由价值而言，自由价值强调在数据流动过程中，应当尊重个人、企业选择数字产品、服务的自由意志与自治能力。其二，就主权价值而言，在数据跨境流动过程中，主权价值体现为各国在数据管辖权上的分歧与冲突。数据管辖权是国家主权在数字空间中的延伸和体现（张晓君，2025）。在实践中，数据管辖权的典型例证是欧盟开展严格的数据保护立法，注重数据安全保护，并对违反者进行高额处罚。其三，就安全价值而言，数据跨境流动固然要追求自由流动，但同时应当注意数据流动的安全性。正是考虑到这一点，中国《网络安全法》才明确规定："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；法律、行政法规另有规定的，依照其规定。"

因此，对于数据跨境流动中的多元价值导向和冲突，有必要通过科学构建相关价值理论，实现对于数据跨境流动壁垒的有效因应，从而最大限度减少因价值观念存在张力而导致的数据跨境流动障碍。

2. 多元价值导向的必要性证成

需要说明的是，不同国家的立场不同，其对于自由价值、主权价值和安全价值的认知也差别迥异。与此同时，自由价值、主权价值和安全价值并非孤立存在，而是呈现出一种动态平衡的张力关系。三者既相互制约，又彼此依存，构成了数据跨境流动治理中的"三元悖论"（陈珍妮，2025）。其一，如果特定主权国家要享有充分的主权，维护其国家安全，那么往往会对数据跨境流动展开严格的数据立法。但由此会导致国家间立法严格程度不一致，进而为数据跨境流动的"制度壁垒"埋下隐患（龚六堂，2025）。其二，如果特定国家试图借助数据自由流动来实现经济价值，那么这些国家则会制定较为宽松的法律规范。其三，为了兼顾自由价值、安全价值及主权价值，可能的方案有两种：一是将数据主权或数据管辖权让渡给一个超主权的国际机构，由该机构进行价值平衡；二是通过本国制定层级性规定或分层保护策略，平衡数据自由流动与国家主权安全之间的关系（毕德旭，2025）。

以上第三种分级保护策略在中国的法律实践中有明显体现。立足于《网络安全法》《数据安全法》及《个人信息保护法》等法律规范，中国初步形成了涵盖数据收集、存储、流动和使用在内的全程规制方案。在此过程中，中国根据数据本身涉及的安全性进行不同类型的场景控制，充分体现了数据流动治理的场景性(许可，2021)。首先，针对关乎国家安全、和平和发展的数据，中国有权进行严格管制。比如根据《数据安全法》第 25 条，国家有权对符合条件的数据进行出口管制。其次，数据跨境流动的限制是附条件的。如《个人信息出境标准合同办法》第 4 条对个人信息出境范围作出了限定。最后，当数据自由流动所体现的自由价值成为主要考量时，主权价值和安全价值则相对弱化。如《促进和规范数据跨境流动规定》中明确划定的数据自由流动许可范围。

(二)规范层面的立法模式差异

在数据跨境流动过程当中，不同国家基于不同的价值立场，形成了差别迥异的立法模式。其中，重视安全价值的国家着重强化个人隐私与数据安全保护，秉持主权价值的国家则通过立法明确界定数据管辖范围，推崇自由价值的国家则致力于构建促进数据流动、释放经济潜能的制度框架。陈珍妮(2025)将各国的价值立场类型化为数据自由化模式和数据本地化模式，齐鹏(2025)将其概括为“美国优先”的美式进取范式、聚焦隐私保护的欧式规制范式、新加坡全球兼容的“新式”非约束性范式和数据跨境流动的“中国特色”方案，张晓君(2025)则认为欧盟的数据治理模式具有“强监管”“强规范”等典型特征。在此，立足于统合法律理论框架，可以将各个国家的立法模式类型化为安全保护模式、自由流动模式以及本地化模式三种。

第一，就安全保护模式而言，安全保护模式强调在数据跨境流动、储存和使用的过程中，政府应立足于数据安全观，严格限制数据跨境流动。以欧盟为例，早在 1980 年 9 月，欧洲经济合作组织便出台《关于保护隐私和个人数据国际流通的指南》，对个人数据跨境流动范围进行了严格限定。2018 年，欧盟发布了《通用数据保护条例》(General Data Protection Regulation，GDPR)，进一步构建了严密的个人数据保护体系。

第二，就自由流动模式而言，在科学技术加持下，自由流动模式更为注重数据的自由流转。以美国为例，近年签署的《美墨加协定》明确规定，缔约国不得限制数据跨境流动。然而，美国凭借其技术及经济优势，推行自由流动模式，实际上强化了其全球经济、技术和政治主导地位。

第三，就本地化模式而言，在采取本地化模式的国家中，俄罗斯和澳大利亚强调对于数据安全的保护，尤其是对于涉及国家安全的重要或敏感数据进行严格的监管。同时，还有一些国家采取较为温和的本地化模式，比如印度和印度尼西亚都要求在进行本地化处理之后才能够进行数据跨境流动(陈珍妮，2025；张晓君，2025)。

(三)事实层面的意识形态差异

数据跨境流动会加剧各国间在政治、经济、技术乃至文化上的分歧。其一，在政治层面，虽然国家安全是数据跨境流动的核心考量，但不同国家基于经济发展需

求可能对安全标准采取差异化界定，进而导致政策冲突。其二，在经济方面，数据作为新型生产要素，无法弥合各国在数据存储格式、“脱敏”标准等技术规范上的本质差异。更重要的是，技术鸿沟直接影响着国家安全。当前全球数据系统的开发和升级多依赖美国技术巨头公司，这种技术依附性可能演变为政治话语权的不平等。数据跨境流动的复杂性进一步凸显了意识形态差异，促使各国通过设置数据本地化等壁垒维护主权利益，形成以技术标准为表象、以国家安全和经济利益为实质的新型国际竞争格局。总体而言，由于历史、文化、政治体制等方面的差异，不同国家基于意识形态差异对数据跨境流动形成了差异化的价值立场。例如，部分国家可能强调数据自由流动的重要性，认为数据是数字经济时代的核心生产要素，应促进其在全球范围内的自由流动以推动经济发展和技术创新；另一些国家则可能更加注重数据安全和隐私保护，认为数据跨境流动可能带来严重的安全风险(胡俊宏和仲瑞洋，2024)，应当采取更为严格的监管措施。

意识形态不仅影响数据跨境流动政策的方向和重点，还深刻塑造了相关法律规制的具体内容和实施方式。例如，在数据保护主义盛行的国家，可能会制定更为严格的数据跨境流动规则，如要求数据本地化存储、限制跨境数据传输等；在倡导数据自由流动的国家，则可能更加注重市场机制作用，强调通过行业自律和事后追责等方式来保障数据安全。在数据跨境流动实践中，意识形态差异的现实影响主要体现在以下具体维度：其一，政策冲突。不同国家基于各自意识形态制定的数据跨境流动政策可能存在冲突，导致跨国企业在数据运营过程中面临复杂的法律环境和合规要求，增加文化冲突和社会矛盾爆发的风险(卫志民等，2025)。其二，信任缺失与合作障碍。意识形态差异可能导致国家之间的信任缺失，进而阻碍数据的有效共享和利用。其三，法律执行与监管难度增加。意识形态差异引发的治理冲突与互信赤字，显著提升了数据跨境流动的合规成本与监管复杂度。跨国企业可能需要花费更多时间和精力来应对不同国家的监管要求，进而增加了运营成本和时间成本。

二、数据跨境壁垒的成因：以价值、规范和事实为基础

当前数据跨境流动壁垒的形成是多重因素交织的结果，从统合法律理论视角来看，这些壁垒根植于价值冲突、规范差异与事实博弈。基于“价值—规范—事实”的三层分析框架，可以将数据跨境流动壁垒的成因总结如下：其一，各国在经济利益与安全保障的价值追求中失衡；其二，自由流动与强力保护的规范构建存在结构性冲突；其三，主权博弈与具体国情差异导致了事实层面的实践障碍。

(一)价值维度：经济利益与安全诉求的深层张力

数据的全球化流动显著扩大了跨国生产者的国际市场份额，催生了新的经济增长点，提升了交易效率，有力推动了全球经济的多元化、高效益发展。然而，囿于不同国家对数据跨境流动所秉持的不同态度，数据的自由交易需求与法律规制之间产生了冲突，平衡经济利益与社会公共利益变得至关重要。若过度放任自由交易，将损害法律权威，难以保障个人信息安全和企业经济效益，甚至可能滋生信息侵

权、不正当竞争等乱象，阻碍法治化进程①。反之，若过度进行法律规制，则可能阻碍数据在国际市场的自由流通，影响数据要素的经济转化，制约数字经济的发展。

1. 追求经济利益时的自由流动需求

在经济利益的驱动下，数据跨境流动的自由化需求本质上是全球数字资本主义扩张的内在要求。这种经济动因深植于数据作为新型生产要素的独特属性——非排他性和可复制性，打破了传统生产要素的稀缺性逻辑，使得数据资源的价值实现高度依赖规模效应和网络效应(许可，2021)。当数据被纳入生产要素范畴时，实质上重构了数字经济时代的价值创造范式，数据跨境流动成为全球价值链重构的核心机制。其深层矛盾体现为数据自由流动的经济理性与主权控制的政治逻辑之间的根本张力。发达国家凭借先发优势，通过将数据规则嵌入国际贸易协定确立制度霸权，是数据殖民主义的体现。

制度性摩擦还与国际治理框架的代际落差有关。现行 WTO 框架下的《服务贸易总协定》(GATS)形成于前数字经济时代，其规则体系难以涵盖数据跨境流动衍生的新型议题。制度层面的缺位迫使各国转向区域性协定以寻求突破，但区域规则间的价值取向差异导致规则碎片化的问题。更深层的悖论在于数据要素市场化配置的天然张力，数据的非竞争性特征理论上支持完全自由流动，但其承载的隐私权等法益又要求施加必要限制。这一价值层面的冲突在制度层面具象化为流动自由与规制主权的持久博弈，不同国家差异化的制度选择本质上是对数据多重法律属性的价值排序差异。

2. 降低安全风险时的双轨多层机制

数据跨境流动安全风险的形成源自数字经济时代生产关系与生产力发展的深层错位。在制度层面，国际规则碎片化与国内治理能力代际落差形成“双重挤压”，美国与欧盟主导的数据自由流动规则体系与发展中国家的数据主权诉求存在着根本性对抗。例如，GDPR 第 45 条与《全面与进步跨太平洋伙伴关系协定》(CPTPP)第 14 章的规范冲突迫使跨国企业采取数据碎片化存储策略以应对差异化的合规要求。这种制度性权力博弈背后映射出的是数字殖民与反制防御的角力——发达国家通过将数据规则嵌入贸易协定以获取制度霸权，而发展中国家则是通过数据本地化立法构筑制度防线。

技术代差引发的结构性失衡进一步加剧了风险传导。全球数据基础设施呈现“中心—边缘”的分布格局，大多数的跨境数据路由节点集中于特定技术霸权国家，形成隐性的数据控制网络。平台通过算法黑箱、API 接口等技术手段实施市场准入控制，技术支配地位使得数据跨境流动天然带有权力的不对称性。

市场权力的结构性垄断源自数据要素的独特属性。平台经济的网络效应与规模效应形成天然垄断，头部企业构建“数据—算法—生态”三位一体的闭环系统，通

①实证的有关证据，可以参见 Patrick B. , Victor C. , Ali H. , et al. The Impact of Big Data on Firm Performance: An Empirical Investigation, AEA Papers and Proceedings, 2019.

过交叉补贴、生态捆绑等策略实施降维打击，更隐蔽的“数据虹吸效应”让新进入者难以获取有效训练数据集，市场创新活力受到系统性压制。

法律规制的内生性矛盾还体现为安全与发展价值的制度性错位。中国《数据安全法》确立的“重要数据”概念尚未形成明确目录，导致企业在申报合规时面临规则缺位。制度上的模糊性衍生出双重困境，即监管机构为避免安全风险倾向于从严解释法律，而企业因合规预期不确定被迫采取保守策略，最终形成高监管成本与低流通效率的恶性循环。除此之外，法律的滞后性在技术迭代中愈发凸显。区块链技术对数据主权的解构、去中心化学习对数据权属的模糊化使得传统属地管辖原则面临实施困境，进而形成监管套利空间。

（二）规范维度：自由流动与强力保护的制度张力

在规范维度，数据跨境流动的制度性冲突根植于不同法域对数据法律属性的差异化认知。美国将数据定位为“可交易商品”，基于其数字产业的全球竞争优势，在《美日数字贸易协定》第 12 条明确禁止数据本地化（蔡翠红和郭威，2022），这一制度设计本质上是将数据自由流动塑造为新型贸易壁垒拆除工具。与之形成鲜明对照，欧盟在 GDPR 序言第 101 段中将个人数据界定为“人格权的延伸”，构建起以充分性认定为核心的数据出境审查机制（周汉华，2018）。更深层的冲突源自数字主权主张的范式差异，美国通过《云法案》确立数据控制者管辖原则，突破传统属地管辖限制，构建起全球数据控制网络。而中国《数据安全法》第 36 条确立的数据分类分级制度实质上是通过技术标准重构数据主权边界。规范层面的制度竞争为跨国企业带来了合规困境，即平台可能同时面临欧盟 GDPR 的“被遗忘权”要求与中国《个人信息保护法》第 13 条的知情同意规则，双重合规成本会导致平台运营效率的下降。

规范冲突的激化还源自国际治理框架的制度性缺陷。现行 WTO 框架下的《服务贸易总协定》（GATS）未能涵盖数据跨境流动新型议题，导致各国转向区域性协定寻求制度突破。CPTPP 第 14 章确立的数据自由流动条款与《区域全面经济伙伴关系协定》第 12 章的安全例外条款形成规范断层，碎片化格局导致发展中国家陷入了制度选择困境，即加入高标准自贸协定可能被迫让渡数据主权，固守现有规则则会面临数字孤岛风险。

（三）事实维度：主权博弈与治理需求的实践错位

在数据跨境流动的过程当中，数据安全和国家安全是主权最鲜明的体现。数据跨境流动过程当中的事实控制体现了国家主权，但是数据的强流动性不可避免地造成了国家数据主权之间的博弈。比如，美国和欧盟作为数据跨境流动领域的强势者，双方对数据主权秉持截然不同的理念（徐玉梅等，2024）。美国强调数据流动的自由化，而欧盟则采取严格个人信息保护模式，主张个人隐私保护优于数据自由流动（李仁真和罗琳娜，2022）。然而，数据自由流动虽然能够促进经济发展，但是依然要考虑到数据所涉及的个人信息和隐私，否则跨境数据流动极易引发数据自

由流动和隐私保护之间的冲突。以美国企业 Facebook 为例，2022 年，因泄露涉及 106 个国家超 5 亿用户的敏感信息(如 Facebook ID、姓名、位置、生日、个人简介及邮箱等)，该公司被欧洲监管机构依据《通用数据保护条例》(GDPR)处以 2.65 亿欧元罚款①，深刻揭示了数据自由流动与隐私保护之间的根本矛盾。与此同时，强调本地化模式虽然能够实现数据流动安全，但在一定程度上会减少数据自由流动带来的经济效益，甚至形成新型数字威权主义。

三、跨境数据壁垒的因应方案：以价值平衡、规范融贯和技术协调为导向

随着数字技术进步与全球化趋势加强，跨境数据传输已成为企业运营和国际贸易的重要组成部分。因此，法律制度的设计和实施需要兼顾数据流动的特性，避免影响经济发展。另外，数字安全原则是审视跨境数据流动法律制度的核心考量，包括确保数据传输的安全性、保密性和完整性，以及防止非法获取或滥用数据。通过建立和完善跨境数据传输的法律机制，可以更好地平衡数据流动与数据安全之间的关系，确保数据流动既能促进经济发展，又能保护国家安全，实现跨境数据有序流动。这涉及建立多层次审查机制，以及在必要时对特定类型的数据实施更严格的管制。此外，构建完善的数据流动与保护体系，需要突破国内外的法律障碍，并有针对性地构建中国跨境数据流动的法律规制体系。

对于前述问题，有必要结合统合法律理论，对数据跨境流动的壁垒进行有效因应。所谓统合法律理论，是指在数据跨境流动治理过程中，秉持利益和价值多元化的理念，适度平衡自由价值、主权价值和安全价值之间的冲突，尊重各价值导向的差异，在规范与事实的基础上实现数据有效、高效、长效跨境流动机制的完善与优化，找到自由、主权、安全的最优平衡点。

(一)价值维度：平衡经济利益与安全风险的协同机制

世界银行发布的《2021 年世界发展报告：数据改善生活》数据显示，2022 年全球数据流动量将是 2021 年的 9 倍，超过 153 000GB/s，且流动量呈现逐年增长趋势(李梓鸿，2025)。在价值选择层面，需要考虑数据流动所产生的经济价值，同时防止因偏重经济效益而忽视数据安全，从而增加跨境数据流动风险。因此，有必要采取平衡经济利益与安全风险的协同机制，在保证国家安全和个人隐私安全的基础上，减少跨境数据流动的阻碍，从而有效提升数据流动的经济利益。

1. 以维护安全为基础

从世界各国的立法选择来看，美国和欧盟分别强调数据的自由流动和对于数据的安全保护。除此之外，大部分国家采取数据本地化策略。比如，巴西 2020 年通过了《通用数据保护法》(Lei Geral de Proteção de Dados，LGPD)，要求公民个人数据在其境内“物理存储和维护”。尽管这种大规模的本地化模式存在风险，但从实

①资料来源：澎湃新闻，https://m.gmw.cn/baijia/2022-11/29/36196713.html(访问日期 2025-06-05)。

践角度上反映了对于国家安全和个人隐私安全的重视。事实上，这种价值选择有其合理性。谢谦和金才淇(2024)认为，国家数据安全风险防范是跨境数据流动规则的首要关切。首先，这种价值选择能够有效地应对信息泄露、数据垄断等问题。在数据流动过程中，不法分子可能会利用技术漏洞实施不法行为，从而致使数据泄露或者被篡改。其次，这种价值选择具有坚实的实践基础。除了上述本地化模式之外，世界各国在数据安全方面均进行了详细的规定。《跨太平洋伙伴关系协定》(TPP)和 CPTPP 第 11.11 条、第 13.4 条以及第 14.13 条均规定，缔约方可采取必要的手段使信息安全和保密性得到充分保障(谢谦和金才淇，2024)。同时，尽管 CPTPP 追求跨境数据流动的高度自由性，但是依然规定了有关的自主监管和合法公共政策目标，从而通过必要的监管保证数据流动安全(葛平原等，2025)。2021 年澳大利亚通过《个人控制的电子健康记录法案》(Personally Controlled Electronic Health Records，PCEHR)，禁止除特定例外情形外的个人健康记录出境(陈咏梅和张姣，2017)。

国际实践表明，建立量化评估机制是平衡数据价值与风险的有效路径。对此可以参照欧盟 GDPR 中的“数据保护影响评估”制度(DPIA)，构建包含“数据类型—应用场景”双维度的风险评估矩阵(见表 1)。该矩阵将数据类型细分为个人数据、商业数据和国家安全数据三类，分别对应的是跨境贸易、技术合作和公共服务三种流动场景，通过算法模型量化风险等级。2022 年 Meta 公司因未完成 GDPR 要求的 DPIA 评估被欧盟罚款 3.9 亿欧元的案件[①]印证了风险评估机制的必要性。

表 1　数据风险评估矩阵

数据类型	跨境贸易	技术合作	公共服务
个人数据	中	高	低
商业数据	低	中	低
国家安全数据	高	高	高

在区分数据类型和数据流动场景的基础上，借助量化模式评估，能够划定不同类型的风险规制手段，以此形成治理合力，从而实现在跨境数据流动过程中对国家数据安全和隐私安全的保护。

2. 以发展经济为要求

差异化治理需要制度创新。对此可以借鉴中美欧经验建立双轨并行机制：将通过等效性认定的国家(例如 RCEP 成员)纳入白名单，适用简化备案程序；针对金融、医疗等特定行业推行安全港协议，允许经同态加密或者匿名化处理的数据自由

①European Data Protection Board Decision 01/2023, January 2023.

流动[①]。中国—东盟“数字丝绸之路”试点项目已经验证了这一模式的有效性。2023 年，南宁国际金融数据枢纽通过白名单机制促使跨境支付数据处理时效提升 40%，合规成本下降了 30%(广西社会科学院，2023)，由此为《区域全面经济伙伴关系协定》第 12 章电子商务条款的落地提供了实践样本。

同时，在数据流动监管过程中，需要对规制手段进一步细化和类型化。比如，可以通过确定监管者所面临的风险和责任，结合数据的重要性，最终确定不同类型的规制举措。其一，在数据监管标准确定过程中，可以区分出以地理区域为基准和以组织机构为基准的规制路径。两者的差别在于规制原则，前者体现了充分性原则，而后者强调问责制原则(胡炜，2018)。以组织机构为基准的方案有助于精准确定企业风险，而以地理区域为基准的方案则容易忽视数据流动性。因此，在合规层面，后一方案便于企业进行风险评估。其二，在数据监管中，需要确定不同类型的数据分类。根据数据的重要性，区分出涉及国家安全和个人安全的数据、重要数据以及能够自由流动的数据等数据类型。数据分类既要避免分类琐碎，也要避免分类模糊，以便精准确定相关主体的责任。

此外，为了缓解中小企业的合规压力，国家可考虑修订《数据安全法》第 36 条，增设国家数据安全基金。基金来源可以包括跨境数据服务企业年度营收的 0.5%专项计提、数据交易所手续费分成，以及财政部数字化转型专项拨款。此外，还可以参照德国联邦数据保护局的做法，设立中小企业数字化扶持基金[②]，用于补贴企业采购隐私计算技术、培养数据合规官(DPO)以及跨境数据传输的基础设施建设。清华大学数字经济研究院(2023)研究表明，该机制可以帮助中小企业降低 25%~30%的跨境数据合规成本。

(二)规范维度：构建法律协调与国际合作框架

法律协调，很大程度上是价值的协调。统合法律理论要求构建法律协调与国际合作的有效框架。在跨境数据流动的实践中，欧盟和美国均有较为成熟的规制体系。黄宁和李杨(2017)指出，中国通过独立发展规制体系的方式尽快提升影响力，既缺乏基础也缺少实践，尤其是在隐私保护和经济发展两个目标上难以轻易作出权衡，最佳的途径是学习借鉴欧盟与美国的规制方法，分步骤推进国内规制实践，进而根据实践效果确立最合适的规制模式。

基于此，从一般层面来看，要实现本土化的规范建构，需要同时完善本国的立法规定并且深度参与国际合作，在此过程中要保证本土法律规定和国际规定之间的协调。其一，本土化的规范构建和国际规定之间相互影响。比如，包括本地化在内的各类数据跨境流动政策，会对依赖全球数据聚合的业务带来影响(王融，2018)。换言之，本土化的政策和法律规定会在金融、文化等方面影响国际政策。反过来，国际政策或者协议同样能够因其广泛接受性而对各个国家的本土规范施加影响。其

①ISO/IEC 20889：2018 Privacy-enhancing technologies 标准。

②参见 German Federal Ministry for Economic Affairs and Climate Action. 2022 Annual Report，2022.

二，各个国家在制定法律规范时，需要积极吸纳国际规范，并且进行本土化处理。原因在于，法律规则是跨境数据流动治理的前提和基础，可为治理实践提供依据原则(郭海玲等，2024)。国内本土法律规范建构应当平衡主权价值和安全价值，从根本上维护国家利益。

在具体举措上，首先，明确各利益相关方的权利、义务和法律责任，包括但不限于数据主体、数据控制者、数据处理者以及数据接收方。明确各方权利义务，有助于构建清晰的跨境数据流动法律框架，为各方提供明确的指引。同时，建立以个人数据、商业数据以及特种行业数据为基础的数据分类审核制度(马其家和李晓楠，2021)。个人数据是指和个人信息有关的可鉴别身份要素，其中包括自然人的姓名、住址以及行为偏好等各类能够识别其身份的信息。商业数据是指具有经济价值的企业内部数据。特种行业数据主要是与社会安全、国家安全紧密相连的行业数据。明确跨境流动的数据类型能够为跨境数据流动的合理性和合法性提供判断根据，也能够增强跨境数据流动行为的可预期性。总之，通过区分不同类型的数据，既能针对不同数据的属性和价值进行结构化监管，也能为法律制度的建构提供基础。其次，指定主管机关并明确其职责。跨境数据流动关涉国家安全、经济发展以及个人隐私等重要价值，首要原则是维护数据安全(王中美，2021)，因此应当明确合规审查的监管主体。监管主体要对划定的不同数据类型采取差异化管理和监督方式。比如，针对涉及国家安全的数据需要设定严格的监管标准，而针对企业数据或者和经济发展相关的数据应柔性限制，满足一般的安全评估要求即可。针对个人数据，以允许自由流动为原则，在例外情况下可以进行干预。主管机关应负责监督跨境数据流动的合法合规性，查处违规行为，同时为各方提供政策指导和咨询服务。明确主管机关的职责，有助于提高跨境数据流动的监管效率。此外，拓宽跨境流动的程序性和监督性渠道，包括建立跨境数据流动的审批制度、风险评估机制和应急预案等。通过完善程序性和监督性渠道，可以确保跨境数据流动的合法合规性，降低数据泄露、滥用的风险。

在此过程中，中国可以借鉴欧洲、美国等地区在跨境数据流动法律规制方面的立法经验和制度模式。例如，GDPR 对个人信息保护提出了较高要求，美国的《加利福尼亚州消费者隐私法案》(CCPA)提供了有益的借鉴。同时，在互联和开放时代，国际层面的合作和交流不可或缺。这意味着中国不仅要学习域外的立法经验，还要和这些域外国家共同制定行之有效的国际规范。许多奇(2018)认为，中国需要对跨境数据流动的全球规则做前瞻性思考，提早部署研究，争取做国际规则的参与制定者，而不应成为规则的被动接受者。通过借鉴国际上的先进做法，可以丰富和完善自身的跨境数据流动法律体系，既能有效保护个人信息安全，又能促进数据的有序流动和数字经济的健康发展。这样的立法策略有助于中国在全球化背景下从根本上维护国家利益和公民权益，更好地融入国际数据治理体系。

以法律规定完善为例，中国可以以《促进和规范数据跨境流动规定》为基础，制定《跨境数据流动管理条例》，构建“分类分级—安全评估—负面清单”三位一体的监管框架。可以依托《数据安全技术 数据分类分级规则》(GB/T 43697-2024)

将数据划分为“核心”“重要”“一般”三个级别，核心数据(例如高精度测绘数据、生物基因序列)禁止出境，重要数据(诸如人口健康统计、跨境金融交易日志)应当通过年度安全评估，一般数据(例如跨境电商交易记录)适用标准合同或者认证机制。可以细化“安全评估—认证—标准合同”三重机制的操作细则，明确高风险数据处理者应当每年强制评估，认证机构要具备 ISO/IEC 27001 信息安全管理体系认证及中国合格评定国家认可委员会(CNAS)认可的实验室资质。此外，可以借鉴《中国(上海)自由贸易试验区及临港新片区数据出境管理清单(负面清单)(2024 版)》引入“数据流动负面清单”的经验，禁止生物识别原始数据、未“脱敏”医疗影像等 12 类数据出境。在立法衔接方面，建议在《个人信息保护法》第 38 条增设紧急豁免条款，允许突发公共卫生事件中医疗机构临时跨境传输患者诊疗数据，但应当在 72 小时内补交备案说明，以实现安全与效率的平衡。

(三)事实维度：落地技术与管理措施破解实操障碍

根据统合法律理论，跨境数据流动依托互联网的发展，不仅会造成网络风险和隐患，也会通过数据权利和数据主权争夺而影响国家的独立和自主(叶开儒，2020)。造成此种困境的重要原因在于技术的发展及其特性，需有效平衡主权与安全的价值导向。因此，从技术层面强化数据安全是克服跨境数据流动壁垒的重要环节，需要重视跨境数据标准的互操作性以及和国际标准的对接关系(孙冉，2024)。

第一，从技术产业发展的角度而言，可以促进数字产业关键技术的创新和技术标准的对接。其一，此项举措能够提升中国技术产业在全球数据价值链中的分工地位。具体举措包括：增加科研经费，制定相关政策培育技术发展的环境；加强域外学习，通过技术学习和技术合作，实现从学习域外技术到超越域外技术的转变；加强数据产业基础设施建设(王小林和兰松，2025)。其二，从一般层面来看，跨境数据流动的技术底线在于数据之间的格式、接口等方面的对齐。事实上，可以结合云技术和区块链等技术，明确数据格式、“脱敏”方式等标准，在跨境数据的收集、分析、传输等各个阶段确立可靠的行为标准和运行逻辑，从而保证数据流动的畅通和真实。通过提升数字技术发展水平、加强数字基础设施建设和完善数据流动的互操作性，形成跨境数据流动整体上的管理合力。

第二，技术标准的统一是构建可信跨境数据流动体系的基石。对此，可以全面推广中国自主可控的 SM 系列商用密码算法(其中包括 SM2 非对称加密、SM3 哈希算法、SM4 对称加密)。目前 SM2/SM3/SM4 算法已经纳入 ISO/IEC 国际标准体系(ISO/IEC 18033-3: 2021)，与欧盟 TLS 1.3 协议和美国 AES-256 算法形成互认框架①。具体实施路径包括如下方面：要求跨境数据处理平台接入国家区块链服务网络(BSN)，依托 SM3 算法实现数据流转全生命周期上链存证，确保哈希值不可篡改。在粤港澳大湾区试点“密码互认中心”，建立中欧、中美算法转换网关，以此

①国家密码管理局《商用密码管理条例》。

实现 SM2 与 ECDSA 算法[①]的密钥自动转换机制。杭州互联网法院“司法链”平台为该模式提供了典型范例，其存证的跨境电子证据超 100 万条，验证时间从传统司法鉴定的 3 天缩短至 5 分钟[②]，未来可以在《区域全面经济伙伴关系协定》(RCEP)框架下推动 SM 系列算法成为亚太区域跨境数据加密的参考标准。

第三，在技术方面形成破除跨境数据流动壁垒的合力。技术进步带来了便利和效率，但也需要始终警惕潜在风险(潘晨子，2024)。具体来说，其一，细化数据分类，满足合规要求。《数据出境安全评估管理办法》规定，在数据出境过程中，需评估企业出境数据相关情形，比如出境数据的规模、范围、种类、敏感程度。然而，伴随着数字时代的发展和企业数据资产规模的扩大，需从技术上推进数据分类标准落地，从而满足企业安全合规的要求。其二，借助“脱敏”技术保证数据安全。数据信息的去标识化或者数据“脱敏”是指通过特定的技术手段并且依赖“脱敏”规则，实现对敏感或者重要信息的变形，以实现对敏感或重要的隐私数据的可靠保护。一般来说，包括个人信息在内的数据去标识化或者“脱敏”通常涉及数据预处理、打磨，再到数据去标识化，以及去标识化结果评级等阶段。数据预处理阶段可以采用数据抽样的方式，缩小数据集的规模，减少结果集中的个人信息。数据去标识化阶段可以应用统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术、数据合成技术等。其三，进行数据安全网络监管。企业数据跨境流动制度主要由数据出境安全评估、个人信息保护认证和数据出境标准合同三项内容构成(李晶晶，2025)。在此过程当中，境外系统可能通过 API 接口的方式访问境内数据中心。为了保证企业跨境数据流动的合法合规，一般需要引入数据安全网关对接口进行监管。数据安全网关能够识别多处敏感数据流量接口，并动态防护敏感数据接口。通过实施“脱敏”、拦截、限流、限频等事中控制措施，实现对于个人隐私数据、企业内部重要数据以及涉及社会安全数据的安全保障。其四，借助其他技术手段保证数据安全。比如，隐私计算是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析、处理与计算的一系列信息技术，以保障数据在流通与应用过程中“可用不可见”。由于其技术特性，隐私计算可在跨境数据场景中提供原始数据不出域的解决方案。此外，借助技术手段的责任要求不容忽视。比如，国家权力机关的算法应用在一定程度上建立起了“技术知识壁垒”，对此应要求算法系统使用机关主动承担算法解释责任(刘甜甜，2024)。

第四，在规则建构上，加强国际合作，推进跨境数据流动的规则统一。规则的统一不仅意味着国家需要对技术标准采取相同的规定，还需要契合技术标准背后所反映的价值理念。以中国为例，不仅需要在参考国外有关标准的前提下建立跨境数据流动的规范体系，实现跨境数据流动的规范和标准化效应，从而实现数据安全传

①ECDSA(Elliptic Curve Digital Signature Algorithm)，椭圆曲线数字签名算法。ECDSA 是一种高效且可扩展的公钥密码算法，其能够为密钥转换相关操作提供信任基础，检验相关操作是否正确且合法。

②杭州互联网法院《司法区块链存证操作指引》。

输和隐私保护等目标，同时还需要在价值理念上和其他国家的价值观念相协调。通过探索各类新型数据传输模式，扩展跨境数据流动边界，实现数据安全价值和数据经济价值之间的平衡。除此之外，在国际合作过程中，需要根据不同领域的数据流动所呈现的不同效应，制定不同技术标准和规制举措。跨境数据自由流动一方面会对数字贸易产生正向促进作用，另一方面会呈现出差异化的贸易效应(陈寰琦，2020)。具体来看，跨境数据流动过程中涉及企业数据、个人数据以及其他类型数据的传输，其传输方式包括物联网数据传输和“本地—云端”传输等多种类型。在这些不同类型的数据传输过程中，其采取的标准可能未必相同，比如可能采取 FTP(File Transfer Protocol 文件传输协议)、SFTP(SSH 文件传输协议)等类型技术或者协议。事实上，这种标准上的差异性增加了跨境数据流动的复杂性，需要国家分别进行规制，必要时还需要开展国际合作。比如，中国积极和其他国家签订互信互认的双(多)边协议，如《关于中德数据跨境流动合作的谅解备忘录》等。同时需要注意，在规则制定过程中，要充分地保证政策空间。比如，鉴于中国跨境数据流动规制措施与 RCEP 服务贸易核心义务存在某些冲突，为了避免在援引例外条款时可能存在的争议和不确定性，中国在未来 RCEP 服务贸易负面清单的拟定和谈判过程中应为此类措施争取足够的政策空间，注重国家安全、公共利益、个人信息权益与贸易自由化目标之间的平衡(宋俊荣，2025)。

四、结 论

跨境数据流动是数字时代全球经济发展的重要驱动力，但其背后涉及的国家安全、数据主权和个人隐私等问题，使得各国在规制路径上呈现出显著差异。本文基于统合法律理论，从价值、规范和事实三个维度系统分析了跨境数据流动壁垒的成因，并提出相应的消除路径。首先，自由价值、主权价值和安全价值之间的相互冲突构成了跨境数据流动的核心矛盾，而这种价值冲突具体表现为各国法律规范的差异。同时，受技术、政治等现实因素影响，跨境数据流动的障碍进一步加剧。面对这一复杂挑战，单一维度的解决方案难以奏效，必须采取多层次的协同治理策略。在价值层面，各国需通过国际对话形成共识，平衡经济利益与安全需求；在规范层面，应推动国内立法与国际规则的衔接，减少制度性摩擦；在事实层面，技术创新和国际合作是破解实际操作困境的关键。中国作为数字经济大国，应在坚持总体国家安全观的基础上，积极参与全球数字治理规则的制定，推动构建开放、包容、安全的跨境数据流动体系。

[参考文献]

[1]毕德旭．CPTPP 高标准数据跨境流动规则的中国因应[J]．北方法学，2025，19(2)：50-63.

[2]蔡翠红，郭威．中美跨境数据流动政策比较分析[J]．太平洋学报，2022，30(3)：28-40.

[3]陈寰琦．签订“跨境数据自由流动”能否有效促进数字贸易——基于 OECD 服务贸易数据的实证研究[J]．国际经贸探索，2020，36(10)：4-21.

[4]陈咏梅，张姣．跨境数据流动国际规制新发展：困境与前路[J]．上海对外经贸大学学报，2017，24(6)：37-52.
[5]陈珍妮．数据跨境的自由流动与安全保护[J/OL]．科学学研究，2025-01-14[2025-05-20]．https://doi.org/10.16192/j.cnki.1003-2053.20250114.002.
[6]葛平原，陈永强，郭伟豪，等．数据跨境流动规制综述[J]．信息安全研究，2025，11(2)：164-172.
[7]龚六堂．以制度型开放推动贸易强国建设[J]．社会科学文摘，2025(3)：5-7.
[8]广西社会科学院．中国—东盟数字经济合作年度报告(2023)[R]．广西社会科学院，2023.
[9]郭海玲，刘仲山，卫金金．我国数据跨境流动协同治理现实困境及纾解路径研究[J]．现代情报，2024，44(9)：142-153.
[10]胡俊宏，仲瑞洋．数据安全治理的经济法理念分析与制度构建[J]．北京师范大学学报(社会科学版)，2024(5)：134-142.
[11]胡炜．跨境数据流动立法的价值取向与我国选择[J]．社会科学，2018(4)：95-102.
[12]黄宁，李杨．“三难选择”下跨境数据流动规制的演进与成因[J]．清华大学学报(哲学社会科学版)，2017，32(5)：172-182+199.
[13]李晶晶．总体国家安全观下企业数据跨境流动制度的检视与优化路径[J]．河北学刊，2025，45(3)：181-189.
[14]李仁真，罗琳娜．欧盟数据跨境传输标准合同条款新发展及启示[J]．情报杂志，2022，41(5)：146-153.
[15]李梓鸿．我国数据跨境流动事后规制研究[J]．山东社会科学，2025(2)：184-192.
[16]刘甜甜．智能刑事司法中算法解释的实践原则与具体路径[J]．法理——法哲学、法学方法论与人工智能，2024，10(1)：195-213+382.
[17]马其家，李晓楠．论我国数据跨境流动监管规则的构建[J]．法治研究，2021(1)：91-101.
[18]潘晨子．司法类案裁判中的 ChatGPT 应用——可能与限度[J]．法理——法哲学、法学方法论与人工智能，2024，10(1)：149-166+380-381.
[19]齐鹏．中国与 DEPA 数据跨境流动：规制差异及制度对接探究[J]．法学评论，2025，43(3)：30-43.
[20]清华大学数字经济研究院．中小企业数据合规成本研究报告[R]．清华大学，2023.
[21]宋俊荣．我国数据跨境流动规制措施与 RCEP 服务贸易规则相符性及应对[J]．当代法学，2025，39(2)：147-160.
[22]孙冉．粤港澳大湾区数据跨境流动的逻辑构造与优化进路[J]．地方立法研究，2024，9(5)：87-104.
[23]王融．数据跨境流动政策认知与建议——从美欧政策比较及反思视角[J]．信息安全与通信保密，2018(3)：41-53.
[24]王小林，兰松．“数字丝绸之路”数据跨境流动机制：逻辑框架与路径选择[J]．人文杂志，2025(3)：46-56.
[25]王中美．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，2021，37(4)：98-112.
[26]尉明洋．中国数据跨境流动安全的类型化法律规制研究[C]//《法治文化》集刊2025 年第 1 卷——部门法的数字化进路研究文集．北京：外交学院国际法系，2025：65.
[27]卫志民，杨梦，向晖蓉．跨境数据流动治理：理论逻辑、潜在风险与规制路径[J]．行政管理改革，2025(2)：51-60.
[28]谢谦，金才淇．跨境数据流动的共同关切、面临挑战与中国应对[J]．学习与探索，2024(8)：114-125.
[29]徐玉梅，杨柳，吕微．“自由”与“主权”：数据跨境流动治理模式的动态博弈——基于全球数字贸易规则视角[J]．行政论坛，2024，31(6)：157-167.
[30]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.
[31]许可．自由与安全：数据跨境流动的中国方案[J]．环球法律评论，2021，43(1)：22-37.
[32]叶开儒．数据跨境流动规制中的“长臂管辖”——对欧盟 GDPR 的原旨主义考察[J]．法学评论，2020，38(1)：106-117.

[33]张晓君．论数据管辖权的冲突与协调[J]．政法论丛，2025(1)：95-109.
[34]周汉华．探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向[J]．法学研究，2018，40(2)：3-23.
[35]LEITER B. The Epistemology of the Internet and the Regulation of Speech in America[J]. Georgetown Journal of Law & Public Policy，2022(20)：903-935.
[36]LIMA A C. A Brazilian Perspective on Jurisprudence：Miguel Reale's Tridimensional Theory of Law[J]. Oregon Review of International Law，2008(9)：77-148.

The Dilemmas and Countermeasures of Cross-border Data Flow from the Perspective of Integrated Legal Theory

LIU Jian，ZHU Qin

(1. College of Humanities and Development Studies，China Agricultural University，Beijing，100083；
2. School of Law，Tsinghua University，Beijing，100084)

Abstract：In the era of Internet plus，cross-border data flow，while promoting international trade，technological innovation，and cultural exchange，also faces multiple challenges such as national security，data sovereignty security，and personal privacy protection. Based on the value diversity characteristics of data law，it is necessary to construct a three-dimensional integrated legal analysis framework. In-depth analysis of the value，norms，and factual elements of cross-border data flow has become an important issue in coordinating data security and data flow. Cross-border data flow is not a sourceless water or a tree without roots，but rather the result of the combined effects of value，facts，and norms. This is mainly manifested in the deep tension between economic interests and security demands at the value dimension level，institutional conflicts between free flow and strong protection at the normative dimension level，and practical dislocations between sovereignty games and governance needs at the factual dimension level. To effectively remove barriers to cross-border data flow，a three-in-one governance system should be established in the future. At the value level，a collaborative mechanism for dynamic balance between economic interests and security risks should be established；at the normative level，a dual-driven framework for legal coordination and international cooperation should be formed；at the technical level，highly operable management measures and implementation plans should be improved，ultimately achieving the legalization and standardization of cross-border data flow development.

Keywords：Cross-border Data Flow；Integrated Legal Theory；Data Sovereignty；Free Flow of Data；Data Security

(责任编辑　祝子白　刘建昌)