E-Commerce Letters 电子商务评论, 2026, 15(3), 343-351
Published Online March 2026 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2026.153280

Hans汉斯

跨境数据流动的安全监管困境与优化路径

张雨馨

贵州大学法学院，贵州 贵阳

收稿日期：2026年1月22日；录用日期：2026年2月10日；发布日期：2026年3月6日

摘 要

在数字经济背景下，跨境数据流动已成为驱动全球经贸发展的关键要素，其安全监管面临多重现实挑战。本文基于数据内在特性、经济安全需求及法律体系建设等驱动因素，系统分析了我国跨境数据流动安全监管的实践困境，主要表现为核心监管对象认定标准模糊、多重合规路径交叉导致企业策略保守化，以及新兴技术业态凸显制度滞后等问题。本文基于问题，提出了应通过制定可操作的“重要数据”与“关键信息基础设施”分类细则、构建基于风险分级的差异化监管流程，并建立面向技术创新的动态监管框架，从而在保障数据安全的前提下促进数据依法有序跨境流动，支持我国数字经济高质量发展与高水平国际经贸合作。

关键词

跨境，数据流动，数据安全，监管

Security Regulatory Dilemmas and Optimization Paths for Cross-Border Data Flow

Yuxin Zhang

College of Law, Guizhou University, Guiyang Guizhou

Received: January 22, 2026; accepted: February 10, 2026; published: March 6, 2026

Abstract

In the context of the digital economy, cross-border data flows have become a key driver of global economic and trade development, while their security regulation faces multiple practical challenges. This paper systematically analyzes the practical dilemmas in China’s cross-border data flow security regulation, based on driving factors such as data intrinsic characteristics, economic secu-

文章引用: 张雨馨. 跨境数据流动的安全监管困境与优化路径[J]. 电子商务评论, 2026, 15(3): 343-351.
DOI: 10.12677/ecl.2026.153280

rity needs, and legal system construction. The main issues include ambiguous criteria for identifying core regulatory targets, conservative corporate strategies caused by overlapping compliance pathways, and institutional lag in emerging technological sectors. Addressing these problems, the paper proposes establishing actionable classification guidelines for "critical data" and "critical information infrastructure", developing risk-based differentiated regulatory processes, and creating a dynamic regulatory framework oriented toward technological innovation. These measures aim to promote lawful and orderly cross-border data flows while ensuring data security, thereby supporting China's high-quality digital economy development and high-level international economic and trade cooperation.

Keywords

Cross-Border, Data Flow, Data Security, Regulation

1. 引言

在数字经济时代，跨境数据流动的规模与频率已远超传统货物与服务贸易，成为驱动全球经济增长的新兴力量。数据作为关键生产要素，凭借其强流动性、非实体性、弱稳定性、非消耗性与非均质性的核心特征，得以在数字空间中高效、广泛地传输与交换。面对数据资源的激增，政府、企业及个人对其跨境使用需求持续扩大，这也从内部催生了对数据跨境流动进行安全规制的客观要求。

与此同时，数据跨境流动正深度重塑全球产业分工与贸易形态。在传统生产要素边际效益渐趋饱和的背景下，主要经济体纷纷将跨境数据流通视为提升产业竞争力、促进数字贸易发展的战略领域，并积极参与构建相应的国际规则与标准框架。围绕数据跨境流动的规制模式，各国基于自身数字经济发展阶段、产业结构和商业利益考量，形成了不同的制度取向与实践路径，这些差异在客观上构成了跨境数据治理体系的多层性与复杂性。在此背景下，如何在保障数据安全的前提下促进数据依法有序自由流动，已成为推动全球数字贸易健康发展、维护各国核心经济利益的重要课题，而数据跨境流动也就此成为当代国际经济运行中不可忽视的常态与关键环节。

2. 跨境数据流动安全监管的驱动因素

基于前述背景，数据因其强流动性、非实体性等特征，得以在全球范围内迅速传播与交换。这一特性也对基于地理边界的传统管辖模式构成现实挑战，并引发各方对数据跨境流动过程中安全与合规问题的关注。数据内在属性、各国对数据资源的经济与安全考量，以及相应的法律体系建设，共同构成了跨境数据安全监管的主要动因。本章将依次对这些驱动因素展开分析。

2.1. 数据内在特性对安全监管的需求

数据的高流动性与无实体性使其能够轻易突破地理边界，这对建立在物理地域基础上的传统法律管辖与监管模式构成了直接挑战。数据跨境流动的瞬时性与隐匿性导致监管主体难以对其传输路径和存储位置进行有效追踪与实时控制。为了应对管辖权在实际执行中被稀释的风险，对数据出境节点实施安全监管成为必要的补偿性手段，由此构成了数据跨境安全监管的基础逻辑。

跨境数据的流动特性在催生监管需求的同时，也带来了具体的合规挑战，即数据跨境流动过程中，个人隐私与商业秘密泄露的风险无法完全避免，尤其是现阶段贯穿数据全生命周期的统一保护标准与可追溯机制尚未完善，一旦发生数据泄露，往往难以定位违规的确切环节与责任主体。加之，数据权利体系中的控制权、使用权等法律界定尚不清晰，权利归属的模糊性容易在数据跨境共享、加工与收益分配等后续环节中引发法律争议。

技术架构的演进则更凸显安全监管的必要性与复杂性。以云计算为代表的数字技术推动了数据量的爆发式增长与应用模式的革新，云环境固有的“资源池化”与“弹性扩展”特性，使得数据的物理存储位置处于动态变化之中，可能分散于不同的司法管辖区。这要求有效的监管机制不能仅依赖于锁定服务器物理位置的传统思路，而是需要具备穿透虚拟逻辑层、协调多方基础设施运营商的技术能力与法律依据，可见在技术实现的动态性与跨境性的情形下，简单化的属地监管模式已经难以适应现实需求。

2.2. 经济安全与产业发展驱动的监管需求

数据的高流动性与非实体性不仅冲击了传统属地管辖模式，也使得数据跨境流动过程中的安全与可控性问题凸显。在此背景下，对跨境数据流动实施监管，成为维护本国核心经济利益与保障数字产业健康发展的重要制度回应。

确保数据安全是维护整体经济安全的内在要求。数据跨境流动可能涉及一国的宏观经济运行、关键技术研发、企业经营信息等重要内容，一旦泄露或滥用，可能导致国家关键产业竞争力受损、市场秩序受到干扰，或企业商业秘密丧失。因此，通过监管措施对重要数据出境进行风险识别与控制，有助于防范因数据无序流动引发的系统性经济风险。

跨境数据流动的监管同样关乎一国在全球数字经济发展中的主动性与获益能力。数据持续、有序的跨境流动是数字技术迭代与产业创新不可或缺的条件，对此，主要经济体及相关国际组织均致力于构建有利于自身的跨境数据规则体系，例如欧盟通过《通用数据保护条例》确立其高标准保护模式，经济合作与发展组织长期推动隐私保护国际框架的协调。这些实践表明，跨境数据规则已成为影响国际数字贸易、产业布局与科技合作的关键变量。因此，探讨跨境数据监管制度的建立与完善，有助于国家在参与国际规则讨论、维护本国企业跨境经营权益、吸引高质量数据要素集聚等方面提升中国的制度性影响力，但若缺乏与之匹配的监管能力与法律工具，中国则可能在数据驱动的全球产业竞争中处于被动地位。

2.3. 中国跨境数据流动监管的法律体系概述

各国基于自身数字经济发展水平、产业结构和利益考量，形成了不同的跨境数据流动监管政策，其中，发达国家总体上倾向于推动数据自由流动，以服务于其全球数字贸易与服务业优势；而多数发展中国家则更注重在融入全球数据流通的同时，防范外部风险并维护本国对核心数据的控制能力。

中国作为数据资源规模庞大、数字产业快速发展的主要经济体，其监管路径则呈现出明显的复合型特征。中国既是数据生产与消费大国，也在部分核心数据处理技术与高附加值数字服务领域面临追赶压力，所以其双重身份决定了中国的监管框架需在促进数据要素有序流动、支持产业创新升级与防范重大数据安全风险之间寻求平衡。因此，中国的监管模式并非简单地趋同于发达经济体的高度自由化或部分发展中国家相对保守的管控，而是试图构建一种兼顾数据利用效率与安全保障的规则体系。

这一制度取向反映在近年来中国陆续出台并实施的一系列基础性法律中，初步形成了以“三法”为核心的跨境数据流动监管顶层架构。

《中华人民共和国网络安全法》作为该领域的先行立法，于 2017 年施行，其监管重点在于保障关键信息基础设施的安全稳定运行。该法第三十九条规定，关键信息基础设施运营者在境内收集产生的重要

数据和个人信息原则上应在境内存储，因业务需要确需出境的，须依法进行安全评估。此项规定确立了数据出境安全评估制度的雏形，但其初始适用范围限于特定运营者，且配套评估办法曾一度缺位。

2021 年相继生效的《中华人民共和国数据安全法》与《中华人民共和国个人信息保护法》，进一步扩展并深化了监管体系。《数据安全法》引入了覆盖全体数据处理者的数据分类分级保护制度，要求根据数据对国家安全、公共利益及个人、组织权益的危害程度实施差异化保护，并授权制定重要数据具体目录，标志着监管重心从特定的“关键设施”转向以数据重要性为核心的全面风险管理。《个人信息保护法》则系统规定了个人信息跨境提供的法定条件，明确安全评估、保护认证和标准合同成为三条主要的合规路径，并建立了个人信息保护影响评估制度，聚焦于个人权益保障。

总体而言，上述三部法律分别从网络运行安全、一般数据安全与个人信息保护三个维度，共同构建了中国跨境数据流动监管的基本法律框架，呈现出中国对监管对象逐步扩大、监管工具趋于多元、合规路径逐渐清晰的发展脉络，并体现了其在动态平衡数据跨境流动价值与安全目标过程中的立法探索。

3. 我国跨境数据流动安全监管的实践困境

3.1. 监管核心对象的认定标准模糊与执行困境

我国跨境数据流动监管的核心，在于对“关键信息基础设施运营者(CIIO)”、“重要数据”及“个人信息”三类对象实施重点管控，但现行立法对这些核心概念多采用“概括 + 授权”的定义模式，导致在实践中，哪些主体应被认定为 CIIO、哪些数据构成“重要数据”，均缺乏全国统一、清晰可操作的认定标准与目录[1]。这种根本性的概念模糊，已从理论争议具体转化为企业在司法实践、行业监管及国际合规三个层面面临的切实困境。

在司法层面，核心概念的缺失导致数据权益纠纷陷入“无法可依”的裁判困境。由于法律未明确企业数据的权利属性，法院在审理相关案件时不得不进行“造法性”解释。在“腾讯公司诉网智天元科技集团股份有限公司不正当竞争纠纷案”[2]中，对于腾讯公司投入巨资形成的新闻数据集合，法院也绕开了数据所有权的争议，最终依据《反不正当竞争法》的原则性条款，以违反商业道德为由认定被告构成不正当竞争。上述案例表明，在核心法律概念模糊的背景下，司法系统不得不借助政策或“兜底”条款来定分止争，这固然体现了司法智慧，但也使得企业数据活动的合法边界高度不确定，法律预期极不稳定。

在行业监管层面，数据类型认定的模糊性与多套监管体系的交叉，构成了企业难以操作的“合规迷宫”。对于同时可能受到《数据安全法》及《个人信息保护法》规制的数据类型，其出境审批路径如何衔接，目前缺乏明确细则。监管实践表明，一旦发生安全事件，相关数据极易被事后追溯认定为需严格管控的类型，如上海某医疗科技公司因其内部系统漏洞导致大量个人信息被境外窃取[3]，上海市网信办便依据《数据安全法》以未能采取有效安全措施为由进行了处罚，揭示了企业在“重要数据”目录缺失情况下面临的“事后认定”风险。

在国际合规层面，国内概念的模糊性被急剧放大，使中国企业面临严峻的“制度性话语权短板”。中国科技企业“出海”时，必须面对如欧盟《通用数据保护条例》(GDPR)等域外法规的严格审查，GDPR 要求向欧盟境外传输个人数据时，接收国必须能提供“实质等同”的数据保护水平。TikTok 爱尔兰公司曾因此被爱尔兰数据保护委员会处以高额罚款，核心原因之一便是监管机构认定，TikTok 未能充分证明中国法律能对传输至中国的欧盟数据提供“实质等同”的保护，特别是指出对中国法律框架下政府访问数据的权力范围、程序及监督机制缺乏清晰、可理解的阐释[4]。由此可见，当国内对“重要数据”的界定、政府数据调取的法律边界等关键问题缺乏与国际规则对话的清晰“术语表”时，国内制度的“解释留白”会直接转化为中国企业在国际合规中难以自证清明的被动局面[5]，对其全球商业模式的合法性构

成根本性质疑。

3.2. 多层监管路径交叉引发企业合规策略保守化

《个人信息保护法》构建了数据出境的“安全评估、保护认证、标准合同”三条主要路径，本意是为不同规模、风险的企业提供差异化选择，但由于各项路径的法律属性、适用场景与长期效力缺乏足够清晰的官方指引与权威释明，企业面对这一“选择题”时，往往陷入决策困境。该困境的核心是规则的不确定性迫使企业在“短期效率”与“长期风险”、“一次性成本”与“持续性责任”之间进行艰难博弈，难以形成稳定的合规预期。例如，标准合同路径因其相对明确的“备案即合规”特点，早期成为许多企业的首选，但随着《个人信息保护认证办法》等相关细则的出台，认证路径从理论走向实践，企业必须重新权衡，是选择标准合同这一看似便捷但可能需为每次业务变更重新备案的工具，还是投入更高昂的初始成本与时间建立一套获得三年有效期的内部管理体系？对于业务场景频繁变动或涉及多国数据传输的跨国企业而言，这种抉择尤为复杂。

在具体司法案件与企业实操中路径选择的模糊性会使企业合规风险与成本增加。在司法层面，企业对“履行合同所必需”等出境合法性基础的理解偏差可能导致路径选择错误。广州互联网法院在审理左某诉某跨国酒店集团一案中明确指出，企业将用户数据传输至境外关联公司用于“营销传播”等目的，明显超出了履行酒店预订合同所必需的范围[6]。此案表明，企业若未能精准评估出境目的与所选路径的匹配度，即便完成了形式上的合规手续，仍可能在诉讼中被认定为违法出境并承担赔偿责任。在实操层面，不同自贸试验区出台的“数据出境负面清单”存在内容与标准上的差异，例如上海侧重于国际航运与再保险，浙江则聚焦于电子商务，对于跨区域经营的企业，这种地域性规则差异进一步放大了路径选择的复杂性，企业可能为了寻求最宽松的清单而进行不必要的业务架构调整，增加了制度性交易成本。

最终，多层路径交叉且指引不清的直接后果，是诱发了企业普遍的合规策略保守化倾向。为了规避因路径选择错误而导致的监管处罚、诉讼败诉或业务中断风险，大量企业，尤其是风险承受能力较低的中小企业，倾向于采取“就高不就低”的防御性策略。一项针对企业的实务调研指出，许多企业因担心标准合同或认证无法完全覆盖其复杂的业务场景，或对“必要性”标准把握不准，即使其数据出境规模可能未达到法定门槛，也会主动寻求适用程序最严格、审查最全面的数据出境安全评估[7]。这种保守策略不仅导致国家网信部门等监管机构面临不必要的审核压力，造成行政资源挤兑，更重要的是其实质上构成了对企业正常数据跨境业务的无形抑制，与立法意图中“促进数据依法有序自由流动”的目标产生了一定张力。长此以往，这种因规则模糊而内生的“寒蝉效应”，可能阻碍我国企业在全球数字经济中的竞争力[8]。

3.3. 新兴技术业态暴露出既有制度的滞后与空白

以生成式人工智能、生物识别应用为代表的新兴技术业态，其数据处理模式已经超出了以《网络安全法》《数据安全法》《个人信息保护法》为核心的传统监管框架的预设场景，这三部法律在制定时主要针对的是相对静态、目的明确的个人信息收集与业务数据传输，难以有效覆盖人工智能模型训练所需的海量、动态、多源数据流转，以及全球性数字身份项目引发的生物识别数据跨境等全新议题，导致现行制度在面对技术快速迭代时，呈现出适用性不足和规则真空的双重困境。

技术的迭代速度远远超过了立法的更新周期，使得许多新型数据处理活动处于“无法可依”或“旧法套用”的灰色地带。一个突出矛盾在于，人工智能大模型的训练依赖于对巨量公开及非公开数据的收集与融合，这一过程是否符合“知情同意”、“目的明确”等传统个人信息保护原则，在司法与监管实践中存在巨大争议。例如，大型语言模型开发者常主张其对公开数据的训练属于“合理使用”，但数据主

体及监管机构可能认为这侵犯了个人权益[9]。欧盟《人工智能法案》已明确要求对具有系统性风险的通用人工智能模型实施严格监管，包括训练数据的可追溯性与透明度。反观国内，尽管《生成式人工智能服务管理暂行办法》有所涉及，但其法律效力层级较低，且缺乏对训练数据跨境流动、模型透明度的具体操作细则，难以应对类似 DeepSeek 这样服务全球用户的中国 AI 企业所面临的实际挑战。该企业在欧洲市场遭遇的监管质疑，部分原因正是其数据实践与欧盟在数据本地化、算法透明度等方面的高标准要求直接冲突，而国内制度未能提供与之衔接的清晰合规指引[10]。

新兴业态也催生了全新的监管议题，例如生物识别数据的跨境治理。传统的跨境数据监管框架主要基于“个人信息”和“重要数据”的分类，但人脸、虹膜等生物识别数据具有高度人身依附性、唯一性和不可更改性。一旦此类数据在跨境流动中泄露或滥用，所造成的危害远非普通个人信息泄露可比，可能对个人权益造成永久性、不可逆的损害，并可能引发大规模的社会信任风险。然而，我国现有监管框架对于此类特殊数据的跨境流动，尚缺乏区别于普通个人信息的、系统性的特殊风险预防机制和专门的管理目录，在司法实践中也缺乏针对新型技术手段的明确认定标准。这种制度上的精细化不足，导致监管在面对利用新技术进行全球范围生物特征采集的项目时，往往缺乏前瞻性的规制工具，只能进行事后应对。

4. 跨境数据流动安全监管的优化路径

4.1. 明确数据分类标准：制定可操作的“重要数据”与“关键信息基础设施”细则

为解决因核心概念模糊所引发的监管与合规困境，当务之急是推动“重要数据”与“关键信息基础设施”的认定标准从原则性框架转化为具备高度可操作性的具体规则，并以建立一套全国统一、行业适配、动态更新的分类分级管理体系为核心目标，以稳定企业预期，降低制度性交易成本。

首要工作是构建并发布国家层面的《重要数据基础目录框架》与《关键信息基础设施认定指南》。这要求国家网信部门会同各行业主管机构，超越当前宽泛的定性描述，转而采用“属性定义 + 列举示例 + 负面清单”相结合的方式。对于“重要数据”，目录框架应明确其识别核心要素，例如是否关乎国家经济命脉、涉及大规模个人隐私、或一旦泄露可能引发系统性金融或产业风险。同时，须提供金融、医疗、交通等不同行业的具体数据示例作为参考，并对已公开且无法关联到个体的统计信息此类明显不构成重要数据的类型予以排除。对于“关键信息基础设施”，认定指南需细化其运营者(CIIO)的判定流程，明确以“业务中断或数据泄露后的危害影响范围和程度”[11]作为量化评估的关键指标，并设定清晰的申报与评审程序，使企业能够自主进行初步评估，避免因范围不清而盲目承担严苛的合规义务。

在统一框架下，必须同步建立高效的行业细则制定与动态更新机制。国家基础目录应明确授权并责成金融、卫生健康、工业制造等重点行业的主管部门，在给定框架内，于特定期限内制定并发布本行业的《重要数据具体目录》与《关键信息基础设施细分类型》。例如，证券监管部门需明确上市公司未公开财报、核心持仓数据等是否及如何纳入重要数据管理；卫健部门则需对临床实验数据、人群基因数据等制定分级标准。此机制应包含常态化的跨部门协同与专家评审程序，确保细则的科学性与一致性，同时要建立目录与指南的年度或定期复审修订制度，根据人工智能新应用等新兴技术演进和新型产业发展及时增补或调整范围，确保监管规则与技术、商业实践同步进化，避免再次出现制度滞后。

通过“国家框架定基线、行业细目明规则、动态机制保更新”一系列规则标准化的措施，构成跨境数据流动安全监管的闭环体系，可以从根本上将监管要求从不可预见的“原则”转化为可预判的“规则”，从实质上减轻企业在数据分类上的合规负担，为其数据出境决策提供稳定锚点，更能将监管资源精准聚焦于真正的高风险领域，实现安全与发展的有效平衡，这亦是提升我国跨境数据流动监管效能、

优化数字营商环境的奠基性一步。

4.2. 构建分级分类的差异化监管流程模型

为解决企业因合规路径交叉而普遍采取的保守策略，必须将《个人信息保护法》中并列的三条出境路径，重构为一套基于风险等级、前后衔接、功能互补的“评估–认证–合同”三级分流监管流程模型，并利用该模型建立标准化的风险评估前置程序，将不同的数据出境场景精准匹配至最适配的合规路径，从而实现监管资源的优化配置与企业合规负担的合理减轻。

“评估–认证–合同”三级分流监管流程模型运作的起点，是建立一套强制性的“数据出境风险自评估”标准化框架。国家网信部门应发布具有约束力的《数据出境风险自评估指引》，要求所有数据处理者在选择具体合规路径前，必须依据统一量表完成此项评估。评估量表需包含可量化的核心维度，例如：出境数据的性质，即是否包含敏感个人信息或重要数据；出境规模与频次；境外接收方的法律环境与安全保障能力；数据出境后可能面临的再转移风险等。依据评估结果，数据出境活动将被划分为高、中、低三个基础风险等级。企业完成自评估并生成等级结论，是进入后续正式合规程序的前置条件与法定义务[12]。

基于风险评估等级，可基于模型设计清晰、排他的路径匹配与分流规则。高风险的出境活动，如涉及重要数据、大规模敏感个人信息或向数据保护水平未被认可的国家和地区传输，必须强制适用数据出境安全评估，该路径定位属于事前行政许可，监管机构进行实质性审查。中等风险的出境活动，例如持续向法律环境稳定的合作伙伴提供个人信息的业务，应导向个人信息保护认证，该路径定位为持续合规证明，由经认可的第三方机构对数据处理者的管理体系进行审计与背书，认证有效期内同类出境活动可反复适用，无需重复审批。低风险的出境活动，例如仅为履行单一合同而进行的、不涉及敏感信息的必要数据传输，则适用标准合同路径，该路径定位应当是标准化法律责任工具，企业按要求备案标准合同范本即可，监管负担最轻。通过此种刚性分流，可以根本上杜绝企业因无法预判而盲目涌向安全评估的现状。

为确保模型的动态有效性，还需配套建立路径间的状态转换与升降级机制。获得认证的企业在有效期内若发生重大数据安全事件或业务场景发生根本变化，其风险等级可能上调，需重新进行安全评估；反之，长期通过安全评估且合规记录优良的企业，其同类业务在续期时，可考虑适用简化的认证程序。在跨境数据流动案件中，针对多层监管路径交叉的困境，利用“评估–认证–合同”三级分流监管流程模型将抽象的路径选择，转化为基于量化风险评估的标准化作业流程，既能显著提升监管的精准性与效率，也能为企业提供稳定、可预期的合规导航，最终促进数据跨境流动在安全底线之上的健康发展。

4.3. 建立面向新业态的动态监管框架

为应对人工智能、生物识别等新技术业态带来的规则滞后与空白，需构建一个具备前瞻性、适应性和实验性的动态监管框架，并以建立一套能够快速识别新风险、容纳技术探索、能将有效的地方实践转化为成熟规则的制度化流程作为该框架的核心目标，以此来弥合技术迭代与法规更新之间的速度差，确保监管既能防范风险又不扼杀创新。

首先，设立常态化的“新兴技术数据合规评估与响应机制”。建议由国家网信部门牵头，联合科技、工信等主管部门及行业专家，组建“新兴技术数据合规专家委员会”，主要负责跟踪全球技术前沿，定期发布《新技术业态数据安全风险评估指引》，针对如通用人工智能模型训练、自动驾驶数据回传、生物特征跨境识别等特定场景，委员会应进行专项研究，提前界定其中涉及的训练数据、提示词、生物模板等数据类型，评估其跨境流动可能产生的算法偏见输出、深度伪造滥用、生物特征不可逆泄露等新型

风险，并在此基础上，迅速制定针对性的《数据出境安全评估要点》或《合规指南》，为监管和企业提供即时、具体的操作依据，改变当前被动应对的局面。

在此基础上，框架需创新监管工具，推行“监管沙盒”与“弹性清单”相结合的管理模式。对于技术路径尚未稳定、商业模式处于探索阶段的新业态，应在国家数据跨境安全管理试点区域(如自贸区)内，设立“数据跨境流动监管沙盒”[13]。允许入围企业在满足数据加密、可审计、风险隔离的底线安全要求以及承诺消费者权益保护的前提下，在限定的业务范围、时间段和数据规模内，试点其创新的数据跨境方案，例如特定的模型训练数据出境协议或去标识化生物特征传输技术。沙盒运行期间，监管机构与企业紧密合作，持续监测风险，评估成效，通过实践证明安全可控的模式，经标准化后便可通过动态更新的《自贸区数据跨境流动负面清单》或《特别管理措施》在一定区域乃至全国范围内推广。但需注意，此清单的调整应有明确的程序与周期，确保其灵活性。

为确保该动态框架的成果，则在于建立从“地方试点”到“全国规则”的标准化转化通路。国家层面需制定《数据跨境流动创新试点成果评估与推广办法》，明确试点成果转化为全国性政策或行业标准的具体条件、评估指标和审批流程。例如，某个自贸区内经过两轮沙盒测试、被证明能有效平衡自动驾驶数据出境需求与安全风险的分类管理方案，在经由专家委员会评估并公开征求意见后，可被吸纳入全国性的汽车数据安全管理规定。通过这一闭环机制，动态监管框架方能将前沿地区的创新实践，及时、有序地转化为支撑全国数字经济高质量发展的稳定规则，系统性解决制度滞后问题。

5. 结语

数字经济的发展使得跨境数据流动成为常态，其安全监管亦面临概念模糊、路径交叉与规则滞后的现实挑战。对此，本文提出应通过制定可操作的分类细则、构建基于风险的差异化监管流程，以及建立容纳技术创新的动态监管框架予以系统回应。这些路径旨在将原则性要求转化为稳定、可预期的规则，从而在筑牢安全底线的同时，有效降低企业合规成本，促进数据依法有序跨境流动，服务于我国数字经济的高质量发展与高水平参与国际经贸合作。

参考文献

[1] 王厚双, 汪海峰. 数据跨境流动规制与制造业全球价值链前向参与: 来自跨国数据的经验证据[J]. 世界经济研究, 2025(7): 31-45+135-136.

[2] 福建省福州市中级人民法院. 腾讯公司诉网智天元科技集团股份有限公司不正当竞争纠纷案民事判决书[(2024)闽 01 民初 689 号] [Z]. 福州: 福建省福州市中级人民法院, 2024.

[3] 央视网. 上海发布 5 起不履行个人信息保护义务的典型案例[EB/OL]. 2025-12-01. https://news.cctv.cn/2025/12/01/ART1kuxwLMZNbHxvPy0fXtG251201.shtml, 2025-12-01.

[4] 柳学信, 李花倩, 孔晓旭. 海外数据监管政策对中国企业数据安全信息披露的影响: 机制分析与效应检验[J]. 现代财经(天津财经大学学报), 2025, 45(7): 40-55.

[5] 刘益灯, 梁倩. DEPA 数据跨境流动例外条款的限度与因应[J]. 上海对外经贸大学学报, 2025, 32(4): 98-111.

[6] 广东省广州市中级人民法院. 左某与某某公司、某某有限公司网络侵权责任纠纷二审民事判决书[(2023)粤 01 民终 33217 号] [Z]. 广州: 广东省广州市中级人民法院, 2023.

[7] 王一楠, 万千惠. 个人信息出境认证新规落地, 企业如何破局“二选一”难题? [EB/OL]. 2025-12-01. https://www.ctils.com/articles/23469, 2026-02-01.

[8] 代丽华, 周灵灵, 陆静雯. RTAs 框架下跨境数据流动规则对数字服务贸易的影响研究[J]. 国际贸易, 2024(3): 72-85

[9] 宗绍昊, 罗世龙. DeepSeek 类生成式人工智能的新型数据安全风险治理[J]. 科学学研究, 2025(1): 1-19.

[10] 中国发展研究基金会课题组, 王路, 丁孟宇, 钟新龙, 王聪聪, 龙海波. 人工智能发展的全球形势、我国态势及“十五五”政策着力点[J]. 经济纵横, 2026(1): 19-30.

[11] 陈颖, 薛澜, 高宇宁. 数据跨境流动监管的三重逻辑——基于全球监管演进的跨国实证研究[J]. 经济社会体制比较, 2025(6): 132-143.

[12] 陈思, 马其家. 数据跨境流动监管协调的中国路径[J]. 中国流通经济, 2022, 36(9): 116-126.

[13] 林梓瀚, 刘羿鸣, 袁千里. 自贸区数据跨境流动监管沙盒机制: 理论证成与制度建构[J]. 中国科技论坛, 2025(5): 30-39+71.