

跨境电商企业出海数据合规路径研究

李珂

浙江理工大学法学与人文学院, 浙江 杭州

收稿日期: 2025年6月12日; 录用日期: 2025年6月25日; 发布日期: 2025年7月25日

摘要

在全球数字化转型进程中, 各个国家均力求在维护数据管辖权与促进数据跨境流动之间寻求平衡。而现有国际条约和区域性协定虽已构建基础性规范框架, 但由于数据跨境流动规范体系的复杂性及各国立法的差异化, 实践中跨境企业仍然面临数据本地化义务泛化、合规标准碎片化、跨境协同机制缺失等多重制度挑战。而化解企业数据合规困境需从以下四个方面推进: 完善数据治理法律规范强化制度保障, 建立行刑衔接与合规互认的法定程序, 构建跨境监管协作框架明晰权责边界, 健全企业合规组织体系培育内生机制。通过“规范-程序-监管”三个层次的治理架构, 既可应对数字经济的复合规制需求, 又能为企业国际化发展提供制度保障, 最终实现治理效能与数据要素市场化的良性互动。

关键词

数据权益, 企业出海, 合规路径, 数据治理模式, 合规体系建构

Research on the Data Compliance Pathway for Cross-Border E-Commerce Enterprises Global Expansion

Ke Li

School of Law and Humanities, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: Jun. 12th, 2025; accepted: Jun. 25th, 2025; published: Jul. 25th, 2025

Abstract

During global digital transformation, sovereign states seek to balance data sovereignty protection and cross-border data flows. While existing international/regional agreements provide basic norms, cross-border enterprises face challenges like overgeneralized data localization obligations,

fragmented compliance standards, and lacking cross-border coordination mechanisms due to regulatory complexity and legislative disparities. Solutions require four steps: improving data governance laws for institutional support, establishing legal procedures for administrative-criminal enforcement linkage and compliance mutual recognition, constructing cross-border regulatory frameworks to clarify authority boundaries, and strengthening corporate compliance systems to foster internal mechanisms. A three-layer governance structure of “norms-procedures-regulation” can address digital economy regulatory demands, safeguard corporate globalization, and achieve positive interaction between governance efficiency and data element marketization.

Keywords

Data Sovereignty, Enterprise Global Expansion, Compliance Pathway, Data Governance Model, Construction of Compliance System

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

在全球数字经济迅猛发展的时代背景下，数据作为核心生产要素已深度嵌入全球经济治理体系。数据跨境流动作为数字经济的基础性运行机制，其法律权益配置体系的建构正在重塑国际经济秩序。权威研究显示，全球数据跨境流动对经济增长的贡献预计至 2025 年将达到 11 万亿美元[1]。这一趋势不仅凸显了数据要素在国际经济格局中的战略地位，更表明了数据要素跨境流动规则的法治建构必要性。而跨国企业作为数据跨境流动的核心主体，在全球化运营中正遭遇数据管辖规则冲突的严峻挑战：各国基于国家安全、经济发展等价值取向制定的数据跨境政策存在显著差异，例如欧盟 GDPR 构建的数据出境监管框架强调隐私权优位，美国 CLOUD 法案确立的数据管辖权长臂管辖原则侧重自由流通，我国《数据安全法》框架下的分类管理制度则注重风险防控，这导致企业陷入“合规标准冲突”与“法律适用竞合”的双重困境。深入研究企业出海合规路径，不仅关乎企业自身的生存与发展，对于我国在全球数据治理体系中争取话语权、推动数字经济健康发展也具有重要意义。

在理论研究层面，现有理论虽在数据治理与企业合规领域取得基础性突破，但仍存在体系性不足的局限[2]。现有成果多聚焦单一国家数据规制分析(如欧盟 GDPR、美国 CCPA)，却鲜少系统揭示主要经济体间数据权益博弈的互动机制；合规路径探讨亦多停留在规范解释层面，对企业全球运营中面临的合规成本控制、技术架构适配等实操问题缺乏回应。理论供给的滞后性，导致企业出海时频发制度性障碍：或因多国数据本地化要求导致运营成本过高，或因跨境传输规则模糊陷入法律风险。在此背景下，突破碎片化研究框架，构建兼具理论深度与实践价值的企业出海合规范式，既为数据管辖与治理理论体系化建构的必要路径，更是破解企业跨境合规困境的现实所需[3]。

本文将立足于国家数据权益保障与数字经济发展权协调的法益平衡框架，通过比较法维度解构企业合规实践中“规制冲突-激励不足-架构缺陷”的结构性矛盾，提出“治理模式转型-激励机制重塑-合规体系建构”的动态适配机制。在系统梳理域外数据合规制度范式的基础上，对我国企业数据合规制度开展顶层建构：建立多层次的合规激励机制，形成系统完备的合规规范框架，设立兼具独立性监管职能与穿透式管理权限的合规组织机构，最终形成契合我国治理需求并彰显制度优势的企业数据合规实施机制。

2. 跨境企业出海的多维数据合规困境

2.1. 全球数据治理模式的差异化格局与合规冲突

在数字经济全球化背景下，数据管辖权成为国家权力的重要延伸，各国基于不同价值取向形成差异化治理模式，加剧了企业出海的合规复杂性。围绕数据管辖权的争夺，全球逐渐形成了三种具有代表性的数据治理模式。

2.1.1. 美国：“数据自由流动 + 长臂管辖”模式

美国以《云法案》(CLOUD Act)为核心构建“数据自由流动 + 长臂管辖”治理框架，其核心特征是通过法律手段突破数据物理边界，实现对境外数据的控制权扩张。例如，2021年美国司法部依据《云法案》强制微软交出存储于爱尔兰的数据中心内的用户电子邮件数据，该行为引发欧盟及其他国家对数据管辖权归属的强烈质疑，凸显了美国治理模式中“经济利益优先”的导向[4]。在区域贸易协定层面，美国通过 CPTPP、USMCA 等协定推行“数据非本地化”原则，禁止缔约方强制要求数据存储于境内，但保留“国家安全例外”条款，形成“原则自由 + 例外管控”的双轨制。这种模式虽降低了企业合规成本，但“长臂管辖”的随意性易引发权力冲突，例如 TikTok 因美国《限制法案》面临业务剥离，折射出非对称治理格局下企业的合规被动性。¹

2.1.2. 欧盟：“数据权利保护 + 外严内松”模式

欧盟数据跨境治理以个人隐私保护为基础，将基本人权保障与内部市场建设作为核心目标，形成“外严内松”的监管模式：在欧盟内部通过《非个人数据自由流动条例》等规则破除数据流通壁垒，鼓励数据自由流动与共享，以推动数字经济一体化发展；在对外数据传输层面，则构建起以“一般禁止原则 - 充分性认定例外 - 标准数据保护条款补充”为核心的严格规制体系[5]。该模式以严格保护个人数据为导向，仅允许向通过“充分性认定”的国家(如 2023 年韩国)自由传输数据，其他国家的企业则需采用标准数据保护条款(SCCs)、约束性公司规则(BCRs)等工具满足“同等保护”要求。此举虽保障了人权，却也增加了企业的合规负担，例如 TikTok 因违反 GDPR 隐私保护义务被处以巨额罚款，凸显其严格治理逻辑[6]。

2.1.3. 新兴经济体：“数据管辖权优先 + 本地化”模式

对于中国、东盟、印度、俄罗斯等新兴经济体而言，维护国家安全与数据管辖权是跨境数据流动治理的逻辑起点，其在认可隐私保护与数据流动价值的同时，形成以安全为导向的差异化路径：中国构建“安全评估 + 分类分级 + 政府监管”机制，统筹发展与安全；东盟将数据安全确立为区域治理核心原则，平衡数据安全与数字贸易；印度、俄罗斯奉行数据保守主义，以数据本地化存储为核心手段。新兴经济体的治理实践体现了对数据安全的优先考量，既回应了数字霸权下的诉求，也为全球数据治理提供了多元样本，我国需在借鉴欧美经验的同时，加强与新兴市场的规则协同，探索安全与效率平衡的治理路径。

综上所述，三大模式规则的差异性使我国企业面临出境安全评估与境外法律强制披露的合规义务冲突，增加了我国企业法律移植成本与市场准入障碍，需通过技术合规、区域协同及标准兼容等方法破解冲突、降低成本。

2.2. 我国企业面临的双重合规压力与制度冲突

我国企业“走出去”需同时应对国内法与东道国规则的双重约束，制度差异导致合规成本激增与决策风险上升。

¹2024 年 3 月 13 日，美国国会众议院以 352 票支持、65 票反对的结果通过了一项针对 TikTok 的法案，要求字节跳动剥离对 TikTok 的控制权。

2.2.1. 双重规制体系叠加导致的合规成本递增

我国企业在“走出去”时，面临本国与东道国数据监管制度的双重合规挑战。具体而言：在欧盟市场开展业务时，企业不仅需要按照 GDPR 要求在当地设立数据中心(由此产生的硬件建设成本通常增加 20%~30%)，²同时还需遵循我国《数据安全法》第三十一条的规定，对重要数据出境实施安全评估，这一双重合规要求显著增加了企业在人力、物力和时间方面的投入成本。另一方面，在我国吸引外资的背景下，由于现行法律对“重要数据”的界定标准尚缺乏具体实施细则，导致外资企业在实际操作中往往难以准确识别数据属性，约有 40%的非敏感数据被不必要地纳入严格审查范围，这不仅降低了数据跨境传输的合规效率，也增加了企业的合规成本，更带来了经营决策的不确定性。³上述情况充分表明，完善我国数据跨境流动法律体系具有现实的必要性和紧迫性[4]。

2.2.2. 规则碎片化引发的合规不确定性

当前，国内外数据合规规范体系呈现碎片化特征，层级关系紊乱且标准冲突显著，给企业跨境数据流动带来巨大挑战。在国内法层面，《个人信息保护法》与《信息安全技术个人信息安全规范》对敏感数据的认定标准存在分歧。由于法律规范与技术标准的衔接不足，导致企业在实际操作中难以明确适用规则，合规风险显著增加。在国际法层面，欧盟 GDPR 的“充分性认定”机制、美国 CCPA 的“长臂管辖”条款，与我国的数据出境“安全评估”制度形成鲜明差异。这些制度在数据存储、传输、使用等环节的要求各不相同，企业为满足不同市场的监管要求，不得不制定多套合规方案，由此导致管理成本平均增加 40% [5]。

在区域贸易协定领域，相关规则同样存在缺陷。以《数字经济伙伴关系协定》(DEPA)为例，其中“合法公共政策目标”条款表述模糊，赋予成员国过大的自由裁量权，在实际执行过程中出现“保护脱钩”现象[7]。由于各成员国对“重要数据”的解释存在分歧，企业在跨境数据流动过程中面临审查标准不统一的问题，不仅导致合规审查周期延长，还使企业难以制定稳定的发展战略，错失市场机遇。这种规范体系的碎片化状态，严重阻碍了企业跨境数据流动的顺利开展，亟需通过制度整合与协调加以解决。

2.3. 企业合规激励制度不足且缺乏有效衔接

我国企业数据合规激励机制在制度设计上存在明显不足，主要表现在三个方面：刑事领域的合规激励措施效果有限，行政监管的合规激励规则存在矛盾，以及刑事与行政合规机制之间缺乏有效衔接。这种多层次的制度缺陷严重影响了企业数据合规的实际效果。

2.3.1. 刑事合规激励的适用困境与程序缺陷

刑事合规激励受刑法谦抑性原则刚性约束，呈现“适用范围窄、程序风险高”的双重特征。一方面，刑法作为数据治理的终极手段，仅能介入《刑法》第 285 条(非法侵入计算机信息系统罪)、第 286 条(破坏计算机信息系统罪)等极少数严重数据犯罪，导致刑事合规激励的覆盖场景极为有限。另一方面，合规不起诉制度缺乏《刑事诉讼法》直接授权，存在三重程序隐患：其一，该制度突破刑法平等原则，可能形成“企业合规减刑特权”，如车浩教授在《合规不起诉的批判性反思》专题研讨会上指出，其“手段合理性与目的正当性缺失”可能引发权力滥用风险；其二，合规考察期与刑事侦查、审查起诉期限的衔接规则缺位，某科技企业数据滥用案因整改效果评估争议导致程序停滞 14 个月，凸显制度稳定性不足；⁴其三，数据合规整改的技术性评估指标(如数据分类分级的合规性)缺乏明确规范，导致检察机关量刑建议的司法接受度存疑[8]。

²欧盟数据保护委员会(EDPB):《2022 年跨境数据合规成本调研报告》，2022 年。

³商务部国际贸易经济合作研究院:《数字贸易合规环境研究报告》，2023 年，第 12 页。

⁴最高人民法院第四检察厅:《企业合规典型案例(第二批)》，2022 年案例编号 2。

2.3.2. 行政合规激励的归责冲突与制度空白

行政合规激励受制于传统归责逻辑与数据治理需求的内在矛盾,呈现“事前激励难证明、事后激励难豁免、和解机制难适用”的三重困境。事前激励方面,《行政处罚法》第33条虽引入“主观过错”要件,但数据合规体系的完备性与“无过错”的关联性证明缺乏技术标准。例如,某企业因未标注敏感数据边界,即便构建合规体系仍被认定存在过失,反映出传统客观归责惯性对执法实践的深层影响。事后激励层面,免于处罚需满足“行为轻微+及时纠正+无危害后果”的严格条件(《行政处罚法》第33条第1款),但数据违规常伴随不可逆后果,合规整改仅能作为减轻处罚情节,而行政机关对“减轻处罚”的裁量缺乏量化标准。行政和解制度则因数据领域立法授权空白,导致某跨境电商因数据跨境违规被调查时,执法机关无法参照证券期货领域“当事人承诺制度”促成整改,且现行模式仅关注事后整改,事前预防效能不足[9]。

2.3.3. 数据合规行刑衔接的协同失灵

数据合规的行刑衔接机制存在系统性缺陷:一是案件移送标准模糊,行政机关与司法机关对“数据违法”与“数据犯罪”的界分存在争议(如“个人信息”认定的“关联说”与“识别说”分歧),导致2023年某省数据领域行政案件刑事移送率不足15% [10];二是合规激励的跨法域冲突显著,企业通过刑事合规获不起诉后,仍可能面临吊销许可证等严厉行政处罚[11];三是数据犯罪的技术性特征要求行政机关深度参与刑事合规考察,但现行制度未明确行政机关在第三方监督评估机制中的角色,技术标准认定等关键环节缺乏专业支撑。此类制度性障碍导致企业“合规投入与法律收益失衡”,亟待通过《数据安全法实施条例》立法明确激励标准,并在《刑事诉讼法》中增设数据合规特别程序。

2.4. 组织架构失位与合规执行断层

我国企业数据合规的组织架构缺陷集中体现为制度供给不足与执行体系断层的双重困境。从规范层面看,《网络安全法》《数据安全法》《个人信息保护法》虽要求企业设立数据保护相关负责人(如网络安全负责人、数据安全负责人、个人信息保护负责人),但对设立条件、选任标准及职责边界的规定极为模糊。例如,《个人信息保护法》第52条仅原则性要求“对个人信息处理活动进行监督”,未明确其是否需具备专业资质、能否兼任业务部门职务等关键问题。实践中,多数企业将数据合规职能并入法务或技术部门,甚至由法定代表人、总经理等兼任负责人,导致合规监督缺乏独立性。

在组织架构设计层面,数据合规委员会、合规部门等专门机构的缺失或虚置,导致企业内部治理与外部监管难以衔接。一方面,传统合规组织架构(如审计委员会)未纳入数据合规的技术性要求,在处理跨境数据分类、传输风险评估等事务时,缺乏跨部门决策中枢,容易形成合规漏洞。例如,某跨境电商因未设立独立数据合规委员会,在数据出境安全评估中因业务部门与技术部门协调失序,被监管部门责令暂停数据传输业务;⁵另一方面,中小微企业受制于成本压力,常以“合规专员兼职化”“制度文本形式化”应对监管要求,导致数据分类分级、风险应急预案等制度难以落地。

数据合规的技术性特征,要求治理主体兼具法律素养与数据技术能力,但现行制度未建立“技术+法律”的复合型人才选任机制也未明确合规组织对业务部门的穿透式监督权。例如,金融行业数据合规需同时满足《金融数据安全数据分类分级指南》与《个人信息保护法》,但多数企业合规部门缺乏金融业务知识,导致制度执行与业务场景脱节[12]。由此产生的合规漏洞,不仅增加企业法律风险(如行政处罚或刑事追责),还可能因跨境数据流动障碍丧失市场机会,形成“合规成本高企-治理效能低下”的恶性循环。

⁵韩国个人信息保护委员会(PIPC):《关于 Temu Korea 数据跨境传输违规的行政处罚决定书》(第 2025-03 号),2025 年 5 月 15 日。

2.5. 我国数据治理模式的本土特色与衔接难题

我国形成以《数据安全法》《个人信息保护法》为核心的“安全评估 + 分类分级”治理模式，强调“国家安全优先、兼顾数据流动”，但与国际规则衔接存在三重矛盾。

2.5.1. 治理理念冲突

我国数据治理以国家安全为逻辑起点，通过《网络安全审查办法》《数据出境安全评估办法》等制度，对关键信息基础设施数据、重要数据实施强制本地化与出境管制。这种“安全优先”的治理理念，与美欧“数据自由流动”“人权保护”的理念直接冲突。有研究指出，这种理念差异导致我国企业在跨境数据流动中面临“合规悖论”——遵循本土安全要求可能触发境外监管制裁，而迎合境外规则则可能违反国内法律[13]。

2.5.2. 标准体系差异

我国“重要数据”定义呈现“范畴宽泛、行业标准碎片化”特征。《数据安全法》第 21 条将“关系国家安全、国民经济命脉”的数据界定为重要数据，但缺乏统一技术判定标准，企业需同时参照《金融数据安全分类分级指南》《工业数据分类分级指南(试行)》等 20 余项行业规范，合规效率显著降低。相比之下，欧盟《非个人数据自由流动条例》对金融数据、工业数据实施分级管理，美国《国防生产法》附件直接列明 12 类“受管制数据”，规则清晰度显著高于我国。这种标准模糊性，使得企业在跨境传输中难以精准识别风险，甚至面临“过度合规”与“合规不足”的双重风险[14]。

2.5.3. 协同机制缺失

我国缺乏类似欧盟的“认证互认”机制，企业需重复通过不同法域审查。在争议解决领域，我国尚未建立专门数据仲裁机制，跨境数据纠纷需通过传统司法程序解决，周期长达 12 个月以上，远高于欧盟数据仲裁庭的 3 个月平均处理周期。

综上所述，这一困境的本质其实是数据的非物理属性与属地管辖的内在冲突。如既有研究指出，数据的跨国流动特性与国家管辖权的物理边界形成“天然悖论”，我国“安全优先”的单向度治理框架，尚未充分平衡国家管辖权的刚性与企业全球化需求。例如，《数据跨境流动规定》虽提出分类分级治理思路，但在实践中仍面临“重要数据目录模糊”“技术剥离标准缺失”等操作瓶颈。如何通过技术赋能(如区块链存证、隐私计算)破解主权管辖与流动效率的矛盾，成为学界与实务界共同关注的焦点[15]。

3. 企业出海合规的法理重构：从零散应对到体系化治理

3.1. 治理模式转型：构建“自治 - 问责”双轮驱动体系

面对数据跨境流动的复杂挑战，我国需突破传统“命令控制”治理模式的局限，构建以企业为主体的“自治 - 问责”双轮驱动体系。这一模式的核心在于将企业从被动监管对象转化为治理参与者，通过内部合规体系建设与外部责任约束的协同，实现数据治理效能的提升。

在自治机制构建方面，企业需以数据分类分级为基础实施差异化治理。依据《数据安全法》第 21 条，对可剥离的非敏感数据(如用户行为数据)，可建立“合规白名单 + 快速备案”机制，通过 APEC 跨境隐私规则(CBPRs)认证或签订欧盟标准合同条款(SCCs)实现高效流动，减少重复性安全评估流程[16]。对于涉及国家安全或重要商业利益的数据(如设备传感器数据)，则需实施“动态评估 + 合规积分”制度，企业通过定期风险评估、加密技术升级等积累合规积分，以抵扣审查时长或简化审批流程。

问责机制的关键在于技术手段与法律确权的深度融合。企业可运用匿名化、区块链存证等技术，实现个人数据与公共数据的属性剥离，避免因数据混同导致的责任错配。对于混合数据集，需依据数据敏

感程度分层适用规则：含个人信息部分遵循 GDPR “单独同意” 机制，含重要数据部分履行我国《数据安全法》规定的安全评估程序。同时，建立独立于业务部门的数据合规官制度，明确其需具备法律与技术复合资质，并直接向董事会汇报，以避免职责混同引发的监督失效[17]。

3.2. 合规激励机制：构建“事前预防 - 事中监控 - 事后救济”体系

现行合规激励机制的不足，本质上是法律刚性约束与企业商业需求的失衡。刑事合规领域需坚持刑法谦抑性原则，有限度引入责任减免机制。对于轻罪案件，可探索将企业建立 ISO 31700 数据安全认证体系、完成整改验收等作为量刑考量因素[18]。例如，某科技企业因过失违规传输数据，通过合规整改获检察机关建议缓刑，成为数据刑事合规的典型案列。需注意的是，该机制适用范围应严格限定于非故意违规且未造成重大后果的情形，避免突破罪刑法定原则。

行政合规层面需突破传统客观归责框架，建立“合规认证 - 责任减免”的法律关联。依据《行政处罚法》第 33 条，企业通过数据安全认证(DSMC)等第三方认证，可主张“无主观过错”以减免处罚。同时，引入“行政和解 + 合规承诺”机制，允许企业以制定并履行整改方案替代部分行政处罚。某金融机构在数据跨境违规案件中，通过承诺 6 个月内建立合规体系，成功获暂缓处罚决定，体现了激励机制的灵活性([16] p. 42)。市场激励维度需将合规水平转化为商业竞争力。通过建立“数据合规示范企业”名单、将合规认证纳入政府采购评分体系等方式，引导市场资源向合规企业倾斜。

3.3. 规范体系整合：构建“国内 - 行业 - 国际”协同规则框架

针对国内外数据合规规则碎片化问题，需以“法律定原则、标准细操作、国际促协同”为路径，构建三级规范体系。

在法律层面，以《数据安全法》《个人信息保护法》为核心，明确“重要数据”的边界与分类规则，并授权国务院制定行业目录。例如，在《金融数据安全分类分级指南》基础上，进一步细化金融交易数据、客户信息的分级标准，解决与 GDPR “敏感数据” 认定的差异。同时，保持法律弹性，为新兴技术应用预留治理空间。

行业标准层面，需发挥行业协会的协同作用，制定细分领域合规操作指南。针对《个人信息安全规范》与《个人信息保护法》的冲突(如“明示同意”与“单独同意”的差异)，建议在医疗数据等敏感领域统一采用“单独同意”标准，并允许通过隐私设计(PbD)技术实现合规。推动《数据跨境流动安全认证实施规则》与国际标准对接，降低企业重复认证成本[19]。

国际协同层面，积极参与 WTO 电子商务谈判，推动“合规激励互认”条款纳入多边规则，争取我国 DSMC 认证与欧盟数据保护印章、美国隐私盾的等效性认可。在“一带一路”范围内开展双边试点，如中老铁路数据合作中，对一般运营数据适用“跨境脱敏传输”，对涉及国土空间的数据实施本地化存储，实现管辖权要求与业务需求的平衡[20]。

综上所述，企业出海合规的体系化重构，本质是在数据主权博弈中寻求安全与发展的动态平衡。通过“自治 - 问责”模式激活企业自律效能、以分层激励破解制度壁垒、用标准协同打通跨境堵点，不仅为企业“走出去”提供操作指南，更通过市场主体的合规实践反哺国家治理规则的完善。

4. 合规体系建构的实施保障与趋势展望

4.1. 技术赋能：智能合规管理系统的构建与应用

依托人工智能技术构建智能合规管理系统，是落实“自治 - 问责”治理模式的技术基石。在跨境数据管理中，企业可以借助人工智能技术开发一套智能合规管理平台，就像给数据治理配了一个“智能管

家”。这个平台能自动扫描企业传输和存储的数据，比如用户信息、交易记录等，快速识别其中的敏感内容，比如身份证号、医疗记录等。同时，它内置了全球主要国家的数据法规，比如欧盟的《通用数据保护条例》(GDPR)、我国的《数据出境安全评估办法》等，能自动匹配不同国家的监管要求，生成直观的风险报告，并给出具体的合规建议。例如，过去企业靠人工检查数据合规漏洞，往往需要 3 天时间，现在用智能平台最快 2 小时就能完成，而且准确率更高[21]。平台还会实时跟踪全球法规变化，比如某个国家新出台了数据本地化存储政策，平台会立即更新规则，提醒企业调整数据传输策略，避免因政策滞后导致违规。这种智能化的管理方式，既能减少人工操作的失误，又能大幅提升合规效率，降低企业的管理成本。

4.2. 组织能力建设：培养懂法律、技术和国际规则的复合型人才

数据合规工作需要既懂法律、又懂技术，还了解国际规则的“多面手”。为了解决这类人才短缺的问题，需要建立一套“数据合规师”认证体系。构建专业化合规人才体系，需以“法律素养 + 技术能力 + 国际视野”为核心标准。依据《企业合规师职业标准》，认证体系应覆盖三大模块：一是数据法律实务，包括《数据安全法》与 GDPR 的比较适用、跨境合规风险识别；二是数据技术操作，涵盖数据分类分级、隐私计算等技术工具的应用；三是国际规则实践，通过模拟 APEC-CBPRs 认证流程、WTO 电子商务规则谈判等提升实务能力[22]。

4.3. 趋势展望：合规能力向核心竞争力的转化路径

在全球数据治理规则日趋严格的背景下，合规能力正从企业运营成本转变为核心竞争优势。从市场准入角度看，通过 GDPR 认证的企业在欧盟市场可获得更高的用户信任度，获客成本平均降低 15%；符合我国“数据二十条”要求的企业，在“一带一路”国家政府项目投标中更具竞争优势，充分体现合规体系对业务拓展的促进作用[23]。从风险防控层面分析，具备完善合规框架的企业能够快速适应各国法规变化，减少因规则差异导致的业务风险。

未来，合规管理的价值将进一步拓展：领先企业可将自身合规体系转化为行业解决方案，通过输出数据分类指南、跨境传输操作手册等标准化成果，形成“合规即服务”的新型商业模式；在金融、医疗等数据敏感行业，合规达标企业可组建跨境数据联盟，共享经过安全评估的数据资源，降低行业整体合规成本。这种从“被动合规”到“主动引领”的转变，不仅有助于企业提升在全球价值链中的话语权，还能推动我国数据治理规则与国际标准的深度对接，为数字经济国际竞争构筑制度优势。通过技术支撑、人才培养与价值转化的协同推进，企业能够构建覆盖风险识别、应对与增值的全链条合规体系，实现合规成本向制度红利的有效转化[24]。

5. 结语

数据跨境流动犹如双刃剑。从积极层面看，其能够激活数据资产价值，显著增强国际贸易企业的经济效益；但从消极角度而言，存在侵犯个人隐私，甚至对国家安全构成威胁的潜在风险。以 CPTPP、DEPA、RCEP 为代表的自由贸易协定(FTA)纷纷纳入了跨境数据流动条款，以期解决国际贸易中跨境数据治理的关键问题。在数字经贸规则的架构内，各缔约国努力在发展与安全之间寻找平衡点，依据本国实际情况制定了各具特色的跨境数据监管模式。遵循上述思路，本文从治理范式、困境剖析、应对策略三个维度，对企业跨境数据合规的基础问题展开探讨，为企业提供参考，助力企业在出海过程中稳健前行。可以预期，世界各国的跨境数据治理规则将不断走向完善。无论是注重人权隐私保护的欧盟模式，还是强调数据自由流动的美国模式，亦或是重视数据主权安全的新兴经济体模式，均对国际贸易企业的合规管理体系提出了更高层次的要求。未来，国际贸易企业必须直面跨境数据合规难题，沉着应对跨境数据风险与

规则模糊冲突的数据合规困境，在数据处理基本原则的指导下内外兼修，做到完善内部数据合规体系和构建外部交流合作机制的动态结合[25]。

参考文献

- [1] 文铭, 李星熠. “自由-规制”框架下跨境数据流动治理及中国方案[J]. 中国科技论坛, 2024(4): 106-116.
- [2] 唐巧盈, 杨嵘均. 跨境数据流动治理的双重悖论、运演逻辑及其趋势[J]. 东南学术, 2022(2): 72-83.
- [3] 罗云开. 数据跨境流动的欧美政策演进及启示——基于数据保护与数字经济发展权衡视角[J]. 当代经济管理, 2024, 46(10): 27-37.
- [4] 王燕. 跨境数据流动治理的国别模式及其反思[J]. 国际经贸, 2022, 38(1): 99-112.
- [5] 梅傲. 数据跨境传输规则的新发展与中国因应[J]. 法商研究, 2023, 40(4): 58-71.
- [6] 刘天骄. 数据主权与长臂管辖的理论分野与实践冲突[J]. 环球法律评论, 2020, 42(2): 180-192.
- [7] 张凯, 苏秋蕙. DEPA 视角下数字企业数据出境治理——兼论“公共政策目标”标准之厘清[C]//《法律研究》集刊 2024 年第 2 卷——制度型开放的实现路径研究文集. 2024: 30-37.
- [8] 刘品新. 论数据刑事合规[J]. 法学家, 2023(2): 89-107+193-194.
- [9] 黎桦, 吴庆洁. 企业数据合规的法律构建[J]. 武汉理工大学学报(社会科学版), 2025, 38(1): 62-71.
- [10] 解志勇. 行政法上企业合规治理制度体系的建构思路[J]. 法律科学(西北政法大学学报), 2023, 41(3): 103-114.
- [11] 齐英程. 数据合规协同激励体系的构建与完善[J]. 东方法学, 2024(2): 98-108.
- [12] 李本灿. 企业合规改革试点中的程序衔接[J]. 东方法学, 2022(6): 99-112.
- [13] 雷定美. 数据治理视域下企业数据合规的困境与路径[J]. 内蒙古民族大学学报(哲学社会科学版), 2024, 50(6): 96-104.
- [14] 张云蔚, 郭德忠. 数据主权视角下数据跨境流动规制路径探索[J]. 湖南人文科技学院学报, 2025, 42(2): 15-21.
- [15] 邵怿. 跨境数据流动规制的自由化与本地化之辩[J]. 政法论丛, 2023(5): 139-148.
- [16] 鄢浩宇. 企业数据合规的困境纾解与体系构建[J]. 华中科技大学学报(社会科学版), 2024, 38(4): 36-45+71.
- [17] 孙跃. 数字经济时代企业数据合规及其构建[J]. 湖北社会科学, 2022(8): 119-128.
- [18] 李迎寒. 合规视野下暂缓起诉制度的功能反思与体系重构[J]. 法律方法, 2023, 43(2): 300-318.
- [19] 袁康, 鄢浩宇. 数据分类分级保护的逻辑厘定与制度构建——以重要数据识别和管控为中心[J]. 中国科技论坛, 2022(7): 167-177.
- [20] 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.
- [21] 赵精武. 论数据出境评估、合同与认证规则的体系化[J]. 行政法学研究, 2023(1): 78-94.
- [22] 洪延青. 数据跨境流动的规则碎片化及中国应对[J]. 行政法学研究, 2022(4): 61-72.
- [23] 李凡. 商业数据跨境流动的规范重塑及合规治理[J]. 中国流通经济, 2023, 37(5): 71-80.
- [24] Cherciu, N. and Chirvase, T. (2020) Non-Personal Data Processing—Why Should We Take It Personally? *European Journal of Privacy Law & Technologies*, **20**, 183.
- [25] Somaini, L. (2020) Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability. *European Data Protection Law Review*, **6**, 84-93. <https://doi.org/10.21552/edpl/2020/1/10>