Open Journal of Legal Science 法学, 2026, 14(10), 168-175
Published Online October 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.1410291

Hans汉斯

我国跨境数据流通的合规困境与机制完善

倪靖慧

宁波大学法学院，浙江 宁波

收稿日期：2026年9月16日；录用日期：2026年9月30日；发布日期：2026年10月27日

摘　要

数字经济时代，跨境数据流通成为数字贸易、跨国经营、国际科研合作的重要方式。我国已经建成由《网络安全法》《数据安全法》《个人信息保护法》为基础，配套部门规章共同构成的数据出境规范体系，确立安全评估、个人信息出境标准合同、个人信息保护认证三类并行合规路径，《促进和规范数据跨境流动规定》进一步细化豁免情形，力图实现安全前提下的数据有序流动。但从已公开司法裁判、网信与公安网安部门行政处罚案例观察，现行机制在合规路径边界识别、市场主体合规负担、个人信息主体跨境权利救济、国际规则对接层面，仍然存在机制落地的现实障碍。本文以已公开可溯源的司法、监管案例为实证样本，运用规范分析、案例实证、比较法研究方法，梳理机制运行中的真实矛盾，结合域外成熟治理经验，提出细化规则解释、实施分层分类监管、完善权利救济机制、参与全球数字规则对话等完善路径，谋求国家安全、个人信息权益保护与数字经济发展多重法益的动态平衡。

关键词

跨境数据流通，数据出境，安全评估，标准合同，合规困境

Compliance Predicaments and Institutional Improvement of Cross-Border Data Flows in China

Jinghui Ni

School of Law, Ningbo University, Ningbo Zhejiang

Received: September 16, 2026; accepted: September 30, 2026; published: October 27, 2026

Abstract

In the era of the digital economy, cross-border data flows serve as a vital vehicle for digital trade, transnational operations and international scientific research cooperation. China has established a

文章引用: 倪靖慧. 我国跨境数据流通的合规困境与机制完善[J]. 法学, 2026, 14(10): 168-175.
DOI: 10.12677/ojls.2026.1410291

data outbound regulatory system grounded in the Cybersecurity Law, Data Security Law and Personal Information Protection Law, supplemented by supporting ministerial rules. Three parallel compliance routes have been formulated, namely security assessment, standard contracts for outbound transfer of personal information, and personal information protection certification. The Provisions on Promoting and Regulating Cross-border Data Flows further elaborates exemption scenarios to pursue orderly data flows under security premises. Nevertheless, an examination of publicly available judicial judgments and administrative penalty cases issued by cyberspace and public security network security authorities reveals practical obstacles in institutional implementation, including ambiguity over the boundaries of compliance routes, heavy compliance burdens on market entities, inadequate cross-border remedy mechanisms for personal information subjects, and poor alignment with international rules. Taking publicly traceable judicial and regulatory cases as empirical samples, this paper adopts normative analysis, case-based empirical research and comparative law approaches to sort out real conflicts arising from institutional operation. Drawing on mature governance experience overseas, it proposes improvement measures such as refining rule interpretation, implementing tiered and classified regulation, perfecting right remedy mechanisms, and engaging in dialogue on global digital rules, so as to achieve a dynamic balance among multiple legal interests: national security, protection of personal information rights and interests, and development of the digital economy.

Keywords

Cross-Border Data Flows, Data Outbound Transfer, Security Assessment, Standard Contract, Compliance Dilemma

Copyright © 2026 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

数字技术的普及使得数据突破物理地域限制，跨境数据流通成为数字全球化的重要载体。跨国企业经营、跨境电商、跨境服务贸易、国际科研协作均高度依赖数据跨境传输行为。数据兼具财产价值与安全风险，无序跨境流动会带来国家安全风险、个人信息泄露、数据滥用等多重隐患，世界主要国家与地区均陆续构建本国的跨境数据治理机制。

我国逐步搭建层级完备的数据出境法律规范体系，形成基础法律联合部门规章的框架，确立安全评估、个人信息出境标准合同、个人信息保护认证三条并行合规通道。《促进和规范数据跨境流动规定》[1]进一步调整安全评估适用范围，增设多项豁免出境场景，降低市场主体运行成本，推动数据要素依法有序流动。虽然规则体系业已成型，但法律条文和实践落地之间始终存在鸿沟。司法领域出现《中华人民共和国个人信息保护法》[2](后文简称《个人信息保护法》)实施之后国内首例的个人信息跨境传输民事判决[3]；中央网络安全和信息化委员会办公室、公安部网安局等部门也公开多起企业违规出境个人信息的行政处罚案例，个案集中暴露出企业合规识别困难、法律概念模糊、权利救济渠道不畅等现实问题。

随着我国数据跨境立法体系不断完善，跨境数据流通成为重要研究领域，现有论文研究重点较多聚焦规范释义、制度比较和国际规则博弈，围绕安全评估、数据出境路径的研究引用量较高，但立足于我

[1]https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm
[2]http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html
[3]左某诉爱利琴商务咨询(上海)有限公司、雅高股份有限公司(ACCOR SA)个人信息保护纠纷案(一审：广州互联网法院(2022)粤0192民初6486号民事)。

国公开司法与监管处罚案例开展实证分析的研究仍相对有限，对法律落地实践中的真实合规摩擦的实证讨论尚有拓展空间。本文采用裁判文书网、人民法院案例库、国家网信办、央视网等公开可溯源的案例与规范文本。通过梳理跨境数据流动的规范框架，挖掘其运行中存在的合规困境，参考域外治理经验，以此完善我国跨境数据流通路径，为我国跨境数据流通治理优化提供学理参考。

2. 我国跨境数据流通现行规范框架

我国跨境数据流通治理坚持安全与发展并重，以维护国家数据安全、保障个人信息权益、促进数字经济对外开放为价值导向，形成法律、行政法规、部门规章多层级规范体系。

从法律层面上，《中华人民共和国网络安全法》[4](后文简称《网络安全法》)第 37 条率先确立关键信息基础设施运营者境内产生的个人信息、重要数据出境应当开展安全评估的规则，奠定我国数据出境监管的雏形。《中华人民共和国数据安全法》[5](后文简称《数据安全法》)确立数据分类分级保护，要求重要数据处理者强化出境风险管控，将国家安全、公共利益嵌入跨境数据治理全过程。《个人信息保护法》第 38~42 条系统搭建个人信息出境基础规则，明确安全评估、标准合同、个人信息保护认证三类法定出境路径，同时设置单独同意、个人信息保护影响评估等强制性前置义务。

同时，部门规章进一步细化可操作的实施机制。《数据出境安全评估办法》[6]划定安全评估申报触发阈值：处理 100 万人以上个人信息、当年累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息，以及出境重要数据的处理者，应当申报安全评估。《个人信息出境标准合同办法》[7]明确未达到安全评估门槛的个人信息出境，可以签署国家网信部门发布的标准合同完成备案，为中小企业提供相对简便的合规通道。《促进和规范数据跨境流动规定》厘清不同现实情况下的适用关系，增设大量免予履行前置出境程序的场景，跨境购物、机票酒店预订、跨境劳务管理等履行合同必要场景可以豁免安全评估、标准合同备案义务，同时发挥自由贸易试验区数据跨境负面清单试点功能，兼顾监管安全与市场便利需求。

并且，地方层面也在进行相应的立法尝试。上海现已形成以一部地方性法规、两部地方政府规章，配套多项行政规范性文件共同构成的数据治理体系。其中上海市出台的《上海市数据条例》[8]，以上海临港新片区为试点，推行低风险数据跨境流动目录管理机制。参考欧盟相关规制思路，对数据跨境流动实施分级分类管控，尝试设立跨境数据流动正面清单，同时强化常态化日常监管与事后监管。[1]但该试点机制与欧盟充分性认定在法律基础、适用范围上存在本质差异，不可等同。

整体来看，我国体制设计形成三条并行的合规通道：第一，数据出境安全评估，面向重要数据、大规模个人信息出境，侧重国家安全与公共利益风险防控；第二，个人信息出境标准合同，面向未达到评估阈值的个人信息出境，依靠标准化民事合同约束境内处理者与境外接收方；第三，个人信息保护认证，由专业机构开展第三方认证，作为数据出境合规选项。三条路径分别适配不同风险等级的数据出境场景，但路径之间的边界划分、衔接关系主要依靠规章抽象表述，面对复杂商业场景，企业在路径选择上极易产生认知困惑，机制落地的实际效果有待实践检验。

3. 从公开监管与司法实践看跨境数据流通的合规困境

随着监管执法常态化，企业跨境数据合规纠纷陆续进入司法与行政程序。本文选取人民法院案例库收录的左某诉爱利琴商务咨询(上海)有限公司、雅高股份有限公司(ACCOR SA)个人信息保护纠纷案 [9]、

[4]https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm
[5]http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html
[6]https://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm
[7]https://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm
[8]https://www.shanghai.gov.cn/nw12344/20211129/a1a38c3dfe8b4f8f8fcba5e79fbe9251.html
[9]广州市中级人民法院(2023)粤 01 民终 33217 号民事判决。

迪奥(上海)公司行政处罚案[10]、上海携程商务有限公司数据出境行政处罚案[11]三份公开可溯源的典型样本展开分析。

(一) 合规路径边界模糊，市场主体法律识别难度较高

现行法律设置安全评估、标准合同、认证多元路径，但部分核心法律概念仍然较为抽象，商业业务场景复杂多变，企业难以精准判断应当适用哪一条合规通道，容易出现路径选择错误。

“履行合同所必需”是跨境数据流通中重要的法定豁免事由，对“必需”的判断是指“客观上的必要”，处理个人信息“应符合合同相对人、社会公众的合理期待或者行业惯例”，必要性的判断要“兼顾实现合同目的和保护个人信息权益的比例性原则”。[2]坚持客观必要性与比例原则，以完成合同本身目的为边界，不能将营销推广、客户维护等衍生商业目的纳入豁免范围，但目前缺少细化可操作的指引，导致实践中容易出现豁免规则被不当扩张适用的风险。在左某诉爱利琴商务咨询、雅高股份个人信息保护纠纷案中，被告将用户预订酒店的基础信息传输至境外预订系统用于完成订房业务，该部分传输属于履行合同所必需；但同时基于营销目的，将用户个人信息传输至美国、爱尔兰合作机构，该部分传输超出合同履行客观必要，法院认定该出境行为不具备合法性基础，不能援引履行合同必要免除单独同意义务。该案暴露出司法实践中的现实难题：商业实践中业务场景高度复杂，区分“合同履行必要”与商业营销、客户维护等衍生目的，缺少可操作的细化指引，企业极易将营销类数据出境归入履行合同必要，进而省略单独同意、出境合规程序。

同时安全评估、标准合同之间的适用边界容易混淆。在实践中则“碎片化”严重，相互之间缺乏科学的逻辑设计。[3]法律规定达到特定数量阈值需要申报安全评估，未达阈值可以适用标准合同。但企业业务扩张过程中，出境个人信息数量处于动态变化，企业难以精准把握阈值计算时点。部分企业出于规避风险考量，未达评估门槛也主动申报安全评估，挤占监管资源；部分企业误判自身数据规模，本应申报安全评估却直接签署标准合同备案，埋下违法风险。重要数据识别同样存在现实难题，现行法律要求重要数据出境必须申报安全评估，但各行业重要数据识别指引仍在持续完善，市场主体对于何为重要数据判断标准模糊，容易出现应当申报而未申报的情形。迪奥(上海)公司行政处罚案中，企业直接向法国总部传输境内用户信息，既未申报安全评估，也没有签署标准合同。同时未取得用户单独同意，被予以行政处罚，反映跨国集团企业普遍存在的认知误区：默认集团内部可以自由流转境内用户数据，忽视我国法定前置出境程序义务。

(二) 市场主体合规负担不均衡，中小企业合规能力短板突出

我国跨境数据合规体系设置自评估、个人信息保护影响评估、备案、持续风险监测等多重义务。大型跨国企业可以组建专门法务、数据合规团队；大量中小企业存在跨境业务需求，却缺少专业合规人员，合规成本压力突出。

大型企业可依靠内部合规审计、外部律所咨询完成安全评估材料准备、标准合同备案等工作。但大量中小企业没有专职数据合规人才，无法完成复杂的数据出境风险自评估，难以区分哪些数据需要履行出境程序、哪些场景可以适用豁免。不仅要深入了解境外接收方所在国家或地区的数据安全保护政策与网络安全环境，还需将其与我国法律要求进行对比。[4]部分中小企业不清楚标准合同备案流程，无力承担高额外部合规服务费用，现实中分化为两种极端：一是过度保守，凡是涉及对外业务一律拒绝数据出境，抑制正常商业往来；二是漠视法律规定，直接将业务数据传输境外，埋下行政处罚隐患。

现行法律更加重视出境前的事前程序，出境完成之后的持续风险监督落地存在短板。标准合同备案

[10]央视网. 法国品牌迪奥发生数据泄露事件 公安网安部门: 予以行政处罚[EB/OL]. https://news.cctv.com/2025/09/09/ARTIrjKmL62MZk7XpFH50R7J250909.shtml, 2025-09-09.
[11]网信上海. 亮剑浦江丨网信部门依法严肃查处违法出境个人信息问题[EB/OL]. https://mp.weixin.qq.com/s/f1-b4qGK7sDNO7YErI8Low, 2026-06-13.

完成不等于合规义务终结，处理者需要持续评估境外接收方所在国家法律环境变化、数据泄露风险。实践中境内企业很难对境外接收方形成有效约束，境外接收方所在国法律发生变动或者发生数据泄露事件，境内企业很难及时发现、处置，事后监督义务容易流于形式。

上海携程商务有限公司被处以 1000 万元罚款的行政处罚案显示，即便是具备完备合规团队的大型互联网平台，同样会出现后端数据出境管控漏洞。监管通报认定其未落实数据出境安全评估要求、违法出境个人信息。监管通报指出，部分企业存在“后端处理数据合规能力不足、数据出境合规审计不严”问题，企业前端业务部门与合规部门脱节，后台数据流转脱离合规审计，造成违法出境后果。大型企业尚且存在管控漏洞，中小企业合规落地难度进一步放大。

(三) 个人信息主体权利救济机制存在现实短板

跨境数据流通场景之下，个人信息传输至境外之后，信息主体维权面临举证难、追责难、执行难三重现实障碍。

举证层面，普通用户很难知晓自身个人信息是否被企业传输境外、传输给哪些境外机构、境外接收方如何处理数据。完整的数据处理日志掌握在处理者手中，信息主体获取证据能力有限。用户甚至无从知晓侵权行为已经发生，更难以证明侵权方存在过错。鉴于大数据技术的隐蔽性和复杂性，令信息主体证明数据处理行为的违法性，其难度不亚于要求其证明信息处理者有过错。[5]在雅高酒店集团个人信息跨境侵权案中，原告需要依靠被告提交的境外接收方传输列表，才得以证明数据被传输至美国、爱尔兰机构；普通用户在一般场景中几乎无法获取此类证据材料，维权举证负担较重。

追责层面，当境外接收方发生泄露、滥用个人信息行为，信息主体追责境外机构，会遭遇涉外司法管辖、域外送达、准据法适用等多重障碍，维权成本极高。虽然法律规定境内处理者承担相应责任，但司法实践中，境内处理者与境外接收方责任划分缺少细化裁判指引。一旦数据出境发生损害，用户维权周期长、成本高，实际获得有效救济的案例数量有限。

(四) 国内规则与国际数字规则存在衔接壁垒

当前全球跨境数据流动规则呈现碎片化格局。欧盟以充分性认定、SCC 标准合同为核心，强调高水平个人信息保护；美国依托双边框架、行业自律推进数据流动；《区域全面经济伙伴关系协定》[12](RCEP)、《数字经济伙伴关系协定》[13](DEPA)等区域贸易协定设置专门跨境数据流动条款，不同治理模式价值取向差异明显。

我国已经加入 RCEP，正式申请加入 DEPA。区域协定则对跨境数据流动提出原则性要求。国内数据出境规则与贸易协定规则之间仍存在协调问题。一方面区域贸易协定倡导减少不必要的数据本地化限制，推动数据跨境流动；另一方面我国基于国家安全设置安全评估制度，部分境外主体对安全评估制度存在误解，简单将其等同于数据贸易壁垒。我国尚未与其他国家达成数据保护充分性互认机制，国内企业的出境合规文件，在境外很难直接获得监管机构认可，企业开展跨境业务，需要同时满足我国法律与业务所在国法律，承受双重合规压力。

同时域外司法机关经常依据本国法律，通过证据开示要求，直接要求境内企业提交存储在中国境内的数据，绕开我国的数据出境安全评估程序，形成跨境数据管辖冲突，对我国数据安全与跨境数据机制实施形成外部挑战。

4. 域外跨境数据流动的经验借鉴

全球主要经济体已经形成各具特色的跨境数据流动治理模式，分析域外实践，结合我国本土国情，

[12]https://www.sicsi.org.cn/Upload/ueditor_file/ueditor/20201117/1605580240660904.pdf
[13]https://gjs.mofcom.gov.cn/cms_files/oldfile//gjs/202303/20230314172358489.pdf

可以提炼可借鉴的治理经验。

欧盟《通用数据保护条例》[14](GDPR)构建起以充分性认定为核心的跨境数据传输。欧盟委员会评估第三国法律保护水平，达到欧盟标准即作出充分性认定，来自该国家的传输无需额外审批。对于未获得充分性认定的国家，企业可以采用标准合同条款 SCC、约束性公司规则等工具完成跨境传输。“Schrems II 案”[15]之后，欧盟法院明确要求企业在使用标准合同时，必须自行评估接收国法律环境，如果评估存在风险，需要补充额外保护措施，不能仅仅依靠签署合同完成合规，强化企业动态风险评估义务。[6]欧盟的经验启示，跨境数据流动不能静态依赖合同文本，必须建立动态风险评估机制，持续关注境外接收地法律环境变化。但欧盟充分性认定门槛极高，全球仅有少数国家和地区获得认定，该模式不能直接照搬至我国。

RCEP、DEPA 代表区域层面治理路径。RCEP 尊重成员国监管数据，允许成员国基于国家安全、公共利益设置数据跨境的例外限制，鼓励各方推动数据流动。DEPA 进一步细化数字贸易规则，倡导避免不必要的数据本地化，推动成员国之间开展监管合作。区域协定坚持促进流动和安全例外的平衡思路，为我国参与全球数字规则谈判提供参考。

综合域外治理实践，可以总结三点启示：第一，坚持风险导向的分类分级治理，根据数据风险等级匹配不同强度监管工具，拒绝一刀切；第二，兼顾大企业与中小企业差异化需求，为中小企业提供简化合规路径，降低合规门槛；第三，平衡事前监管与事后救济，在设置出境前置程序的同时，完善个人权利救济渠道，强化企业持续风险管控义务。

5. 完善我国跨境数据流通的具体路径

立足于我国国家安全、数字经济发展现实，结合国内司法与监管实践暴露的问题，应当从规则细化、分层分类监管、权利救济、国际规则对接四个层面完善跨境数据流通。

(一) 细化法律规则解释，厘清合规路径适用边界

针对司法实践暴露出法律概念模糊的问题，网信部门应当出台配套行业指引，对“履行合同所必需”作出类型化解释，通过发布指导案例明确边界，区分纯粹履行合同必要的传输与商业营销、客户拓展等衍生性数据出境，降低企业法律不确定性。进一步细化重点行业重要数据识别指南，推动金融、医疗、交通等行业出台清晰的重要数据目录，解决企业识别难的现实困境。

厘清安全评估、标准合同、个人信息保护认证三者之间的适用关系，明确触发安全评估的法定情形；对于未达到评估阈值的个人信息出境，优先适用标准合同或者认证路径，减少企业盲目申报安全评估的现象。细化阈值计算规则，明确累计数量统计口径，对于业务扩张后数据规模动态超过阈值的企业，设置合理缓冲期，给予企业整改过渡空间，避免企业因为业务增长瞬间触发违法风险。同时细化豁免出境场景的适用条件，明确豁免不等于免除告知、单独同意等个人信息保护义务，防止市场主体滥用豁免条款逃避个人信息保护义务。通过确立统一的豁免程序原则，优化豁免适用的次序和流程，构建起规范明晰、运转高效的审查豁免运行程序[7]。

(二) 推行分层分类监管，减轻中小企业合规负担

落实分层分类监管思路，区分大型企业和中小企业，实施差异化合规要求。针对大型跨国企业，强化全流程监管，压实企业内部数据合规审计义务，督促企业建立内部跨境数据流转管控机制，防范内部业务部门脱离合规管控私自传输数据。针对中小企业，完善标准合同备案线上化流程，简化备案材料，发布跨境电商、跨境服务等高频场景化合规指引，提供风险自评估简易参考模板，降低中小企业专业门槛。

[14]https://gdpr-info.eu/
[15]See Schrems II, Case C-311/18.

充分发挥自由贸易试验区创新价值，依托自贸试验区负面清单开展试点，总结可复制经验向全国推广。改变“重事前备案、轻事后监督”，建立备案之后常态化抽查机制，重点核查企业是否落实境外接收方风险持续评估义务。发挥行业协会作用，开展面向中小企业的数据合规公益培训，缓解中小企业专业人才不足困境。

(三) 完善个人信息主体的跨境权利救济机制

针对跨境场景举证难问题，适度减轻个人信息主体举证负担，探索举证责任部分转移路径：当用户主张个人信息被违法跨境传输，由数据处理者就出境行为已经履行法定程序承担举证责任，降低普通用户举证压力。明确相关行为人权利与义务。同时，个人信息出境务必要征得信息主体同意，否则不允许个人信息出境。此外，个人信息运营者需要承担信息保护责任，明确境内数据处理者的兜底责任。即便损害由境外接收方造成，境内处理者依然需要就境外接收方违约、侵权行为承担相应民事责任。[8]

司法机关可以发布跨境个人信息保护指导性案例，统一裁判尺度，明晰境内外主体责任划分、单独同意司法认定标准，为同类案件提供裁判指引。畅通线上投诉举报渠道，完善行政投诉与民事诉讼衔接，降低个人维权成本，真正落实跨境场景下个人信息权益保障。

(四) 积极对接国际数字治理规则，推动监管互认

我国应当依托 RCEP、DEPA 平台深度参与全球数字规则谈判，坚持维护国家数据安全前提下，输出兼顾安全与发展的中国治理方案。积极开展跨境数据监管双边对话，探索与其他国家开展监管互认，推动合规结果跨境认可，减少企业双重合规负担。面对域外司法机关绕过我国法律直接调取境内数据的管辖冲突，用好现有法律阻断机制，维护我国数据安全。长远来看，要在区域互认的基础上，联合相关国家、地区，积极推动有关标准的国际化，主动参与个人信息保护认证国际互认规则的制定，推动国际数据跨境流动治理，用中国方案服务世界经济发展[9]。

在对外经贸谈判中，阐释我国数据出境安全评估的风险防控属性，厘清安全评估并非贸易壁垒，减少国际社会对我国跨境数据机制的误解。推动国内制度规则与国际高标准数字贸易规则良性对接，守住国家安全底线的同时助力我国数字产业高水平对外开放。

6. 结语

跨境数据流通承载多重价值目标，既要守住国家安全、个人信息权益的底线，又要顺应数字经济全球化，释放数据要素流通价值。我国已经搭建起完整的跨境数据流通法律体系，安全评估、标准合同、认证并行的机制设计回应数字时代数据治理现实需求。透过已公开的司法裁判与行政执法案例可以看到，制度文本落地实践过程中，仍然存在合规边界模糊、中小企业合规压力大、个人救济不足、国际规则衔接不畅等现实困境。

完善我国跨境数据流通治理，要立足于本土实践，细化法律解释，推行分层分类监管，健全权利救济渠道，积极参与全球数字规则构建。在国家安全、个人权益保护与数字经济发展之间寻求动态平衡，推动数据实现安全前提下的有序跨境流通，为高水平数字对外开放提供坚实法治保障。

参考文献

[1] 平凡. 域外跨境数据流通规制路径的启示[J]. 中国外资, 2024(7): 90-93.

[2] 杨合庆, 主编. 中华人民共和国个人信息保护法释义[M]. 北京: 法律出版社, 2022: 46.

[3] 叶传星, 闫文光. 论中国数据跨境制度的现状、问题与纾困路径[J]. 北京航空航天大学学报(社会科学版), 2024, 37(1): 57-71.

[4] 王永杰, 潘娅丽. 我国数据出境安全评估事项的立法不足与完善[J]. 浙江理工大学学报(社会科学), 2026, 56(3): 348-357.

[5] 宋伟锋. 限缩与扩张: 个人信息跨境流动中的标准合同[J]. 西华大学学报(哲学社会科学版), 2023, 42(5): 36-46.

[6] 杨帆. 后“Schrems II 案”时期欧盟数据跨境流动法律监管的演进及我国的因应[J]. 环球法律评论, 2022, 44(1): 178-192.

[7] 张晓君, 赵佳慧. 数据跨境流动中安全审查豁免制度的适用困境与纾解路径[J]. 厦门大学学报(哲学社会科学版), 2025, 75(6): 93-106.

[8] 钟鸣. 数字贸易时代个人信息跨境流动的法律保护路径[J]. 人民论坛·学术前沿, 2021(6): 108-111.

[9] 甘杰夫. 推动个人信息保护认证国际互认促进个人数据合规高效跨境流通[J]. 中国信息安全, 2022(12): 46-49.