生成式人工智能数据跨境流动的法律风险与规制路径

宋延敏
（中国人民公安大学　法学院，北京　100038）

摘　要：生成式人工智能作为前沿技术突破的重要载体，其高效运转离不开多模态海量实时更新的数据支持。随着生成式人工智能蓬勃发展，跨境数据流动频率日益增加。生成式人工智能数据跨境流动带来经济价值与社会效益的同时，也存在一些法律风险：一是个人信息在跨境传输中可能面临泄露与滥用风险，二是对生成式人工智能产业产生负面影响的风险，三是数据跨境流动所引发的国家安全与数字主权风险。然而，当前生成式人工智能数据跨境流动相关法律体系和政策框架尚不完善。基于现有的监管体系，针对上述风险，从国内层面和国际层面提出治理对策建议，在国内，应进一步构建生成式人工智能数据跨境流动监管制度体系；在国际，应加强合作，推动数据跨境安全标准的互认，以期促进生成式人工智能数据跨境流动的可持续发展。

关键词：生成式人工智能；跨境数据流动；数据主权；法律规制
中图分类号：TP18；D922.17　　**文献标志码**：A　　**DOI**：10.19358/j.issn.2097-1788.2026.03.011

中文引用格式：宋延敏. 生成式人工智能数据跨境流动的法律风险与规制路径［J］. 网络安全与数据治理，2026，45(3)：73-80.
英文引用格式：Song Yanmin. Legal risks and regulatory paths for cross-border flow of Generative AI data［J］. Cyber Security and Data Governance，2026，45(3)：73-80.

Legal risks and regulatory paths for cross-border flow of Generative AI data

Song Yanmin
(School of Law, People's Public Security University of China, Beijing 100038, China)

Abstract: Generative Artificial Intelligence (AI), as a cutting-edge technology, is only possible due to the continuous and rapid updating of vast amounts of data. However, as Generative AI becomes more prevalent, the volume of cross-border data flows is increasing. The cross-border flow of Generative AI data brings economic value and social benefits, but also poses legal risks. First, personal information may face risks of leakage and misuse during cross-border transmission. Second, there is a risk of negative impacts on the generative AI industry. Third, cross-border data flows pose risks to national security and digital sovereignty. However, the legal and policy frameworks for cross-border data flows are not yet complete. This paper proposes some solutions to address these risks, both domestically and internationally, to ensure the sustainable development of cross-border data flows. Domestically, we should further establish a regulatory framework for the cross-border flow of generative AI data; internationally, we should strengthen cooperation to promote mutual recognition of cross-border data security standards.

Key words: Generative Artificial Intelligence; cross-border data flow; data sovereignty; legal regulation

0　引言

生成式人工智能作为人工智能技术发展的前沿领域，具备强大的内容生成能力，能够依靠指令输出详尽全面的文本内容。中国国家互联网信息办公室（以下简称网信办）等七部门发布的《生成式人工智能服务管理暂行办法》规定，生成式人工智能技术是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术[1]。随着技术的不断发展与完善，生成式人工智能的出现对国内外技术创新产生了变革性影响。2022 年 ChatGPT 的突破性问世揭开了生成式人工智能技术革命的序幕，使这一领域迅速获得了人们的关注，随后全球科技企业竞相推出大模型，持续推动技术创新浪潮。2025 年 1 月，中国深度求索公司 DeepSeek 推出 R1 模型，对标 OpenAI 的 o1 模型，其凭借深度推理能力与低成本算法架构迅速占领市场[2]。

生成式人工智能的全球化发展深度依赖安全有序的跨境数据流动。在生成式人工智能的技术实现中，系统化的数据治理过程构成基础支撑体系，主要包括

数据收集、数据清洗、数据标记和转换等操作[3]。值得关注的是，随着多模态大模型技术的突破性发展，训练数据的需求呈现显著的全球化特征，既需要融合不同国家的语言样本，又需整合多元文化特征和行业数据，国际合作与地区间政策协调需求增大，这使得数据跨境流动成为技术迭代的必然选择。然而，生成式人工智能数据跨境流动一方面虽然有效促进技术创新，但其也会给国家、公共以及个人安全构成威胁，例如个人信息与隐私保护、产业安全，以及国家安全和数字主权等方面的风险。当前生成式人工智能与跨境数据流动研究均取得一定的进展，但在其交叉领域，研究相对还比较少，现有监管体系尚未有效回应其带来的新兴法律挑战。因此，本文基于现有的监管体系，针对上述风险，从国内和国际两个层面对生成式人工智能数据跨境流动提出具体建议，以期促进其可持续发展。

1 生成式人工智能数据跨境流动的多维法律风险

全球数字经济和生成式人工智能技术蓬勃发展，跨境数据流动频率日益增加，为各国带来了诸多红利，但这一过程也伴随着一定的安全隐患。相较于传统的数据跨境流动，鉴于生成式人工智能技术应用涉及更大规模的数据量和更快的传输速度，再加上受到全球数据监管碎片化等多重因素的影响，生成式人工智能在数据跨境流动方面呈现出更为复杂且隐蔽的特征[4]。另外由于生成式人工智能数据通常具备多维属性，且跨境数据流动不受国家和市场边界的制约，这种特性让治理面临更大的挑战和困境[5]。概而言之，生成式人工智能数据跨境流动的法律风险主要包括以下几个方面。

1.1 个人信息安全与隐私风险

生成式人工智能在开发部署与数据采集过程中，因数据跨境流动与多模态数据无界性，个人信息安全和隐私保护面临着巨大挑战。首先，在生成式人工智能的开发和部署阶段，开发者和部署者若未严格依照数据跨境流动的评估要求、标准合同以及个人信息保护认证等规定加以落实，可能会带来潜在的风险[6]。目前，大多数国内生成式人工智能服务提供商依赖于接入生成式人工智能技术支持者的 API 接口或调用其深度学习模型等技术来提供服务。然而，由于这些技术支持者的服务器大多设于境外，数据在传输与交换过程中难以避免地涉及跨境流动，从而增加了安全隐患[7]。其次，在数据采集阶段，由于多模态训练数据的无边界性，使生成式人工智能数据较难规范治理。多模态（Multimodality）的概念起源于计算机人机交互领域信息表示方式的研究[8]，多模态数据是指包含多种类型（模态）的数据，如文本、图像、音频、视频、3D 模型等。例如，GPT-4V 可同时处理图文输入，Sora 需要海量数据进行训练，支持文本到视频、图像到视频的生成。无论是 GPT-4V 还是 Sora，都需要海量的训练数据作为基础，而训练数据的来源体现出较明显的无界性，在大量收集数据的过程中由于透明度不足，用户可能未被告知信息会被传输，或是使用目的不明确，知情同意不充分，可能会侵犯个人隐私，给个人信息安全带来风险[9]。同时，数据在传输过程中可能会被监控、拦截、窃取，尤其在网络传输过程中，若安全措施不足，比如对于未加密的传输链路，可能会被黑客通过网络嗅探[10]等手段进行攻击，对个人隐私和安全造成损害。

1.2 产业安全风险

生成式人工智能产业风险是指在生成式人工智能产业的发展、应用和推广过程中，可能面临的一系列对产业自身发展、社会经济、法律法规等产生负面影响的因素和问题，分为开发者或部署方自身所承受的产业风险和受生成式人工智能影响的相关企业所面临的产业风险[7]。

首先，生成式人工智能开发者或部署者自身所承受的产业风险，主要集中在数据传输、数据存储过程中的安全隐患，以及相关的管辖权争议上。具体而言：一是在数据跨境传输过程中，终端设备、通信链路、数据库、应用系统以及开放 API 等多个环节均可能成为网络攻击的目标，存在数据泄露、篡改或遭受破坏的潜在风险[11]。例如，在通信链路方面，数据在跨境传输过程中可能会受到黑客或其他机构的窃听、劫持或篡改。2013 年“棱镜计划”曝光，显示某些政府机构能够直接截取互联网服务提供商（ISP）的数据流量，并在数据跨境传输过程中进行深度包检测（DPI），导致全球范围内的大规模隐私泄露，暴露了政府和机构可能对数据流进行监控，使生成式人工智能开发者或部署者在数据收集或使用时面临着更严格的隐私保护与合规要求。同时，生成式人工智能数据在跨境流动过程中，需要遵守各国的数据法规和隐私政策。若存在违反监管要求的行为，可能会面临高额罚款与行政处罚，甚至可能会承担刑事责任，对企业产生不良的影响，影响相关数据产业的发展。二是在数据存储阶段，企业若将数据保存在境外服务器内，虽然可能会提高处理效率，但是可能面临数据泄露或

未经授权访问的风险，黑客可能通过各种手段获取存储在服务器上的数据[12]。三是生成式人工智能数据在跨境流动过程中还面临着管辖权冲突的合规问题。训练数据可能会涉及多个区域进行收集、处理以及存储，对于生成式人工智能开发者或部署者来说，如果缺乏对不同司法管辖区数据法规的全面理解，可能会在数据流动过程中面临法律责任与合规风险。

其次，受生成式人工智能影响的相关企业的产业风险主要体现在企业商业秘密的非法公开方面。一是在数据跨境传输过程中，可能会涉及一些企业的商业秘密，如果这些数据遭到非法攻击、泄露等，可能会使企业丧失竞争优势，甚至带来致命的打击。二是大模型也存在泄露用户输入数据风险。若用户输入的数据被用于模型训练，一些敏感信息可能会被存储，在后续的生成结果中可能会被泄露。一旦被泄露，用户可能会对企业产生不信任感，无疑会对企业产生不良的影响。例如，三星在启用 ChatGPT 的 20 天内就发生 3 起员工泄露数据事故，泄露内容包括半导体设备测量、产品良率、内部会议内容等敏感信息[13]，对企业自身产生不利的影响。

1.3 国家安全与数据主权风险

生成式人工智能数据跨境流动引发的数据主权风险正在成为国家安全领域的新兴威胁。所谓数据主权，是指一个国家或地区对其境内生成、存储和传输的数据拥有法律、技术和政策上的控制权，包括对数据的管辖权、所有权和使用权的管理[14]。这一风险主要表现在对技术、文化以及法律的影响三个层面。一是在技术层面，数据跨境流动在一定程度上会增加网络攻击的潜在目标，挑战国家对数据的防护管辖权。一些境外组织或黑客可能会利用生成式人工智能技术分析并滥用某一国家的数据，对其实施网络攻击甚至操纵舆论，对国家安全稳定产生极大的影响；同时，生成式人工智能训练数据可能会包含地理信息、生物信息等国家基础性数据，也有可能涉及国家机密等信息，在跨境传输过程中一旦被境外情报机构抓取，可能会对国家安全产生严重影响。二是在文化层面，依赖于全球语料库的多语言模型中的训练数据，在数据采集阶段可能会倾向于本国的文化意识形态，其输出内容可能会影响文化认同，从而对数据主权中的文化控制权产生影响。三是在法律层面，生成式人工智能技术的发展依赖于大规模数据支撑，为满足多语种覆盖和消除算法歧视的技术要求，其数据采集范围已扩展至跨国界和多语言领域。部分数据已被各国整合并公开，而另一部分尚未经过系统整理和发布。如果缺乏法律的有效监管和保护，可能对国家数据安全产生影响，甚至演变成新型地缘政治风险[3]。而不同的国家对数据以及隐私政策的规定有所差异，这种法律冲突可能会影响国家对本国数据的有效监管。比如欧盟《通用数据保护条例》要求较为严格的数据监管模式，而美国更倾向于自由的市场模式。

2 生成式人工智能数据跨境流动规制的立法考察

2.1 域外立法镜鉴

当前，国外关于数据跨境流动治理的规制尚未针对生成式人工智能形成专门立法，主要仍适用跨境数据流动的通用规定，包括以欧美为主的法律框架，以及促进全球数据保护合作的国际协作与多边机制三个类别。

第一，欧盟以隐私保护优先，具有严格的数据保护标准与跨境数据管控限制。2018 年 5 月，欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）正式生效，其中第 5 章专门规定了数据跨境流动的法律框架，旨在为欧盟境内的数据转移至非欧盟国家提供一系列多层次的法律保障机制[7]。同时，GDPR 对于欧盟区域外的国家也产生了重要影响，形成了布鲁塞尔效应。所谓布鲁塞尔效应，指欧盟可借助其单方面的市场规制能力，在无需其他国家或地区协作的情况下，通过多种渠道向外输出欧盟规则与标准，进而对全球市场秩序产生示范性规则引导[15]。例如，根据 GDPR 第 45 条关于跨境数据流动的要求，只有在接收国的数据保护水平获得欧盟的“充分性认定”后，个人数据才能合法地进行跨境传输。目前，只有少数国家，如日本、韩国和加拿大，已经获得了这一充分性认定。如果接收国未获认定，则必须通过标准合同条款（SCCs）或约束性公司规则（BCRs）等其他合规机制来确保数据传输的安全和合规。

第二，美国以市场自由化为导向，注重商业利益，立法政策整体上呈现“双重标准”：一方面鼓励数据流入美国，另一方面则对数据出境施加较多限制。与欧盟不同，美国关于数据的法律规制整体上更为分散和碎片化，没有统一的全国性数据治理框架，而是依赖联邦以及州各自的法律及政策组合管理数据。首先，在联邦层面，2018 年《云法案》（CLOUD Act）突破数据存储地域限制，授权执法机关可直接调取网络服务商控制的境外数据，该法案规定“电子通信或远程计算服务提供商应遵守本章的义务，保护、备份或披露有线或电子通信以及该提供商所拥有、保管或控制的

与用户或订阅户有关的任何记录或其他信息，无论此类通信、记录或信息是否位于美国境内或境外”[16]，开辟了执法机关可以直接向网络服务提供者调取境外数据的取证新途径[17]。然而该法案授权美国获取他国数据的同时，又通过一定的方式阻碍他国获取美国境内的数据，以维护美国的数据主权[18]。2024 年 12 月，美国司法部（DOJ）发布第 14117 号《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》的最终实施规则，旨在防止包括中国、俄罗斯、古巴等六个“受关注国家”及相关主体获取美国公民的大量敏感数据和美国政府相关数据，显示出在维护国家安全框架下的防御性立场。此外，美国较为依赖双边协议。如与欧盟之间的合作经历了多个阶段，从 2000 年的《安全港协议》（Safe Harbor Agreement），到 2016 年的《隐私盾协议》（Privacy Shield），再到 2023 年签署的《欧盟 – 美国数据隐私框架》（EU-U. S. Data Privacy Framework，DPF）。这些协议不仅为跨境数据流动提供了制度保障，也加强了数据和隐私保护，延续与欧盟之间的数据跨境合作，确保数据自由流入美国。其次，在州层面，最具代表性的是加利福尼亚州在数据隐私方面的立法，主要包括 2018 年颁布的《加利福尼亚消费者隐私法》（CCPA）和 2020 年实施的《加利福尼亚隐私权法》（CPRA）。尽管这两部法律对跨境数据流动的实质性限制相对较少，但它们强调了企业在收集和处理加州消费者个人信息时必须提供透明度，并给予消费者控制其个人信息的权利。概而言之，美国主要通过国家安全逻辑严格约束敏感数据的外流，同时依靠分散化、多层级的立法模式维持数据自由流入与商业利益最大化。

第三，国际协作与多边机制主要包括双边协议和多边框架。双边协议主要有比如上述提到的 DPF。多边框架主要有《区域全面经济伙伴关系协定》（Regional Comprehensive Economic Partnership，RCEP）、APEC 跨境隐私规则（Cross-Border Privacy Rules，CBPR）以及《全面与进步跨太平洋伙伴关系协定》（Comprehensive and Progressive Agreement for Trans-Pacific Partnership，CPTPP）。此外，还有《数字贸易伙伴关系协定》（Digital Economy Partnership Agreement，DEPA）以及 G7《数据自由流动与信任伙伴关系》（G7 Data Free Flow with Trust Partnership，DFFT）。首先，较为典型的是 RCEP。RCEP 是区域经济合作的重要成果，我国于 2020 年 11 月 15 日完成协定签署程序，2022 年 1 月 1 日正式生效。RCEP 更侧重于区域经济合作需求，倡导数据跨境流动自由，但允许成员国基于公共利益及国家安全利益设置例外。其次，CBPR 对于跨境数据采取问责制，要求通过认证的企业建立内部隐私管理体系，指定“问责代理机构”负责监督，设立了 Data Privacy Pathfinder，旨在建立一套跨区域的数据隐私规则系统[19]。CBPR 同时对数据流向有一定的控制，企业应确保数据接收方具备与 CBPR 体系要求相当的保护水平。再次，CPTPP 在第 14 章“电子商务”中设定了数据跨境流动规则的相关条款，其中第 14. 11 条规定通过电子方式跨境传输信息，对缔约方提出相关数据传输要求。相较于 RCEP，CPTPP 对数据跨境自由流动的态度更加宽容，主要体现在例外条款设置上[20]。

2.2 我国规制现状与问题解析

近年来，全球数字经济迅猛发展，尤其是在生成式人工智能技术广泛应用的背景下，我国对于数据跨境流动监管需求显著增强。我国在积极寻求加入 CPTPP 和 DEPA 等新型国际规则的同时，也在不断推进与完善相关立法。

我国已初步建立起以《中华人民共和国网络安全法》（以下简称《网络安全法》）、《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）为基础的数据跨境流动监管体系，并通过配套文件如《数据出境安全评估办法》《个人信息出境标准合同办法》进一步细化具体实施路径。尤其是 2023 年出台的《生成式人工智能服务管理暂行办法》，首次在生成式人工智能领域提出训练数据处理要求“来源合法”，涉及个人信息需取得同意或符合法定情形，明确训练数据来源需符合《数据安全法》的三级分类标准[21]，标志着生成式人工智能数据跨境流动开始纳入监管框架。在既有制度基础上，2024 年 3 月实施的《促进和规范数据跨境流动规定》对于数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行做出了优化调整[22]。此外，2024 年 11 月国家网信办发布的《全球数据跨境流动合作倡议》体现了我国在推动数据跨境流动相关技术与安全保障能力评价标准国际互认方面的积极立场[23]，尝试在“安全”与“发展”之间找到动态平衡。

然而，面对生成式人工智能数据跨境流动的复杂性，现行法律规制体系也暴露出碎片化与适应性不足等问题。

第一，关键信息基础设施（CII）数据本地化与安全评估制度的适用存在不确定性。虽然《网络安全法》第37条规定了关键信息基础设施数据本地化与安全评估制度[24]，但是该制度以关键信息基础设施的运营者作为适用标准，在界定模糊以及执行弹力较大的情况下，生成式人工智能数据跨境流动是否纳入适用范围存在不确定性。

第二，数据类型识别模糊，适用标准不清晰。生成式人工智能通常调用非结构化、多模态数据[25]，可能会引发大规模数据调用以及训练数据来源合法性问题，而现行的《数据安全法》规定的数据分类分级管理制度更偏向传统结构化数据，对于生成式人工智能海量数据如何定性，如何划归保护级别，仍缺乏较为清晰的适用标准。

第三，个人信息出境制度的适用存在困境。2021年11月施行的《个人信息保护法》第38～40条规定个人信息跨境流动要经过“告知—同意”原则以及安全评估、认证、标准合同三重路径。然而在实践中，生成式人工智能数据来源通常较为复杂，往往无法逐一取得明确授权或明示同意要求，且其出境是否触发评估机制也存在较大的争议。此外，《数据出境安全评估办法》和《个人信息出境标准合同办法》虽进一步完善了个人信息出境制度，但对于技术更新以及数据流动速度较快的生成式人工智能数据，保持合规与效率之间的平衡问题亟待解决。

第四，在跨境数据调用成为训练数据常态的背景下，单一国家的数据合规规则难以回应生成式人工智能跨境数据流动下的治理挑战。尽管我国提出了《全球数据跨境流动合作倡议》，但其更多强调的是较为宏观的规则与政治主张，在生成式人工智能数据跨境流动的法律实践中，尤其是数据合规、信息出境以及责任认定等具体层面尚未形成具有普遍约束力的机制，难以有效回应生成式人工智能数据跨境治理提出的新挑战。《促进和规范数据跨境流动规定》虽通过“负面清单”“面向典型跨境业务情形豁免安排”等规定向国际规则靠拢，但对于生成式人工智能跨境训练数据类型复杂性与治理特殊性缺乏针对性规范。

总之，我国在数据跨境流动治理方面初步构建了以数据分类分级管理为核心的框架，但由于生成式人工智能技术在跨境调用以及数据规模上具有独特性，现有制度在数据类型分级、跨境场景适用以及国际标准衔接等关键环节仍需通过专项立法进一步健全规则体系。

3 生成式人工智能数据跨境流动法律规制路径构建

在全球人工智能治理尚未形成统一法律体系的背景下，我国应立足本国国情，探索符合本国实际的发展路径，发展具有中国特色的治理对策。由于生成式人工智能数据跨境流动涉及个人信息、企业利益以及国家安全等多个方面，且人工智能技术快速迭代较为复杂，在短期内难以形成全球统一的法律体系来进行全面规范和监管，但国际规范的协同仍然是促进人类福祉的重要方向[26]。因此，我国应立足自身实际，一方面，在国内层面应构建完善的监管制度体系，助力我国生成式人工智能产业向上向善发展；另一方面，在国际层面应推动国际规则协同与合作，以增强我国在生成式人工智能领域的话语权和竞争力。

3.1 构建生成式人工智能数据跨境流动监管制度体系

在现有数据分级分类的基础上，应进一步完善数据治理机制，建立针对生成式人工智能数据特点的跨境流动监管体系。围绕该目标，具体可从细化数据分类标准、构建安全评估体系、推动数据流动可追溯管理以及探索“监管沙盒”机制四方面入手，构建科学透明的治理框架。

一是应进一步细化数据分类标准，明确生成式人工智能数据在不同应用场景下的敏感程度，确保监管措施精准适配。首先，对于涉及个人隐私、企业机密或国家安全的数据，应严格限定其跨境传输条件，并通过技术和法律手段强化保护。其次，我国已逐步完善了个人信息处理应当遵循的各类原则、数据分级分类制度和重要数据保护制度，同时充实了数据出境安全管理的相关规定[27]。但对于基于生成式人工智能所形成的动态数据和合成数据的分类依据仍存在不足，应进一步完善分类依据。应依据数据的重要性、敏感性、商业价值及应用场景，对训练数据进行分级管理，并相应设立访问控制、使用审批及监管机制，同时制定差异化的存储标准、使用权限与安全防护措施[28]。

二是构建针对生成式人工智能的跨境数据安全评估体系，以适应人工智能模型训练的特点。首先，在使用公共数据资源时，应当建立多维度的评估机制，重点考察数据体量、信息属性及其涉及的法律权益，合理评估其风险等级。第一，对于涉及国家安全的数据应严格禁止跨境流动，严格监管关系国家安全的数据跨境流动作为生成式人工智能的训练数据，应避免将此类数据作为输入语料。第二，对于企业数据，可采用“包容审慎”原则，包容审慎规制要求“政府不

以包容的名义放弃必要的审慎监管，也不因市场出现了一些问题而立即转向过度监管，其主张的并非先发展后规范或者先规范后发展，而是在发展中规范、在规范中发展”[29]。在保护企业数据隐私的同时，尽可能地为技术创新留有空间[30]。其次，针对涉及民生关键领域及社会公共利益核心范畴的敏感数据，在基础层面应避免将其直接纳入机器学习模型的训练数据集，在应用层面也不宜人为干预或输入，以确保数据的合理使用与安全合规[28]。

三是应推动数据流动全流程可追溯管理，借助隐私计算[31]等技术，实现跨境数据访问记录的透明化和可审计性，提高监管效率。在生成式人工智能数据开发、训练、部署过程中，针对跨境数据流动带来的个人信息隐私安全风险，采用覆盖全链条数据可视化、可审计、可追责监管机制。一方面，可利用隐私计算、区块链等技术手段，实现对数据访问的全过程记录与权限控制；另一方面，在数据跨境流动过程中，对数据接收方可设立合规责任约束机制，对个人信息等敏感数据进行定期合规审查，如发生泄漏可溯源追责。

四是可探索“监管沙盒”机制，在风险可控范围内进行小规模试点，测试生成式人工智能数据跨境流动规则的可行性。面对生成式人工智能产业在跨境数据传输与存储中面临的技术风险、法律冲突与商业敏感信息泄露风险，可建立“监管沙盒”机制，以小规模、低风险场景进行测试和评估。可由相关监管部门牵头，选择具备代表性的企业或平台，设定明确的试点范围和对象，在可控环境下对生成式人工智能数据跨境流动进行“实景测试”，以在实际操作中不断优化监管体系。

3.2 推动生成式人工智能数据跨境流动国际规则协同与合作

我国可基于互惠原则减少生成式人工智能数据跨境壁垒，深化与其他国家在数据治理方面的合作与规则对接，积极参与全球数据治理体系建设。当前，国内治理方案重点关注数据单向出境，而对数据入境情形的规制理念与方法都相对薄弱[32]，容易导致监管盲区，进而影响数据安全与公平竞争。为缓解上述问题，我国可以基于互惠原则与主要国家和地区建立数据跨境监管互认机制，提升我国数据治理的话语权与国际影响力。

首先，应加强双边和多边数据治理合作，推动建立国家之间相互认可的跨境数据合规框架。我国提出的《全球人工智能治理倡议》主张在人工智能治理中加强信息交流和技术合作，共同防范潜在风险，推动构建广泛共识下的人工智能治理标准与框架，进而提高人工智能技术的安全性、可靠性、可控性与公平性[33]。在这一基础上，各国可通过协商明确数据分类标准、隐私保护规范以及安全评估机制，减少监管差异带来的合规障碍，促进生成式人工智能技术在全球范围内更加顺畅地规范应用和发展，更好地应对生成式人工智能时代数据跨境流动带来的挑战，为推动构建公平、合理、透明的国际规则体系奠定基础。

其次，应扩大数据跨境流动以及全球人工智能治理国际合作。生成式人工智能是数字经济的新质引擎，基于流动产生价值的数据在国际数字经济之重要性愈发凸显[27]。一是我国应在现有法律框架基础上，积极对接国际上已有的高水平规则与治理实践。在全球治理规则尚未统一的情况下，构建区域性标准联盟是推动数据治理优化的重要途径[34]。目前，RCEP 为区域合作提供初步框架，其条款强调开放与包容。我国可积极在 RCEP 框架内推动亚太区域互认协议的达成，通过制定统一的规则标准和技术规范，促进区域内数据的安全流动[35]。同时，要积极对接 CPTPP 和 DEPA 更高标准的协定，构建与国际接轨的多层次治理体系[30]。我国《全球数据跨境流动合作倡议》呼吁各国秉持开放、包容、安全、合作、非歧视的原则，平衡数字技术创新、数字经济发展、数字社会进步与保护国家安全、公共利益、个人隐私和知识产权的关系，在推动数据跨境流动的同时实现各国合法政策目标[36]。在此基础上，我国应进一步加强政策协调与规则对接，与主要贸易伙伴对接标准化认证体系，推动生成式人工智能数据跨境试点，推动数据流通的安全与便利协同发展。作为“一带一路”倡议的发起国家，我国亦应积极探索并与相关国家取得共识，推动区域性治理新模式，促进跨境数据的流动和监管[37]。二是促进生成式人工智能发展应加强全球治理合作。生成式人工智能训练数据具有全球依赖性，其影响跨越国界，尤其是在数据流动方面，仅凭一国之力无法有效实现人工智能的全球影响。因此，在生成式人工智能发展过程中，涉及基础层、技术层及应用层中使用、存储或利用跨境数据时，应充分尊重各国的数据主权及跨境数据流动规制[27]，要着力提升发展中国家在全球数据治理中的参与能力建设，推进数字基础设施共建共享[38]，通过全球治理合作加强技术发展，完善风险防控机制，促进全球人工智能治理体系的健康可持续发展。

4 结论

随着生成式人工智能技术的不断演进与蓬勃发展，数据跨境流动已成为不可忽视的重要议题之一。目前我国在数据治理方面已形成数据分级分类管理体系，并通过安全评估等制度手段强化对出境数据的监管控制，保障国家数据安全和个人信息隐私。然而，生成式人工智能数据在流动过程中存在复杂性以及隐私保护等挑战，再加上国际监管环境存在差异，所以仍需进一步优化治理体系。现阶段我国应在已有制度基础上，持续推进生成式人工智能数据跨境流动的精细化调整管理。具体而言，一方面应完善法律法规建设，进一步构建生成式人工智能数据跨境流动监管制度体系；另一方面应加强国际合作，推动数据跨境安全标准的互认，提升我国在全球数据治理体系中的话语权。

总之，在保障数据安全和国家利益的前提下，我国应合理引导和规范生成式人工智能数据跨境流动。这不仅有助于我国人工智能产业的健康发展，也将提升我国在全球数据治理格局中的影响力，为构建更加开放、安全、共赢的数据流动生态奠定制度基础。

参考文献

[1] 国家互联网信息办公室等七部门. 生成式人工智能服务管理暂行办法 [EB/OL]. (2023 - 07 - 10) [2025 - 02 - 10]. https://www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm.

[2] Sensor Tower: App-analysis Category-rankings [EB/OL]. (2024 - 02 - 26) [2025 - 02 - 26]. https://app.sensortower.com/app-analysis/category-rankings.

[3] 郭小东. 生成式人工智能的风险及其包容性法律治理 [J]. 北京理工大学学报 (社会科学版), 2023, 25 (6): 93 - 105, 117.

[4] 姚迁, 刘晋名, 盛小宝. 生成式人工智能数据跨境流动的安全风险及治理范式 [J]. 网络安全与数据治理, 2024, 43 (12): 80 - 87.

[5] 陈颖, 薛澜. 全球跨境数据流动治理的演进与趋势 [J]. 国际经济合作, 2024, 40 (2): 55 - 66, 93.

[6] 乔晗, 徐君如. 基于 LDA 模型与政策工具的中国数据主权政策研究 [J]. 中国科学院院刊, 2024, 39 (3): 498 - 508.

[7] 公安部第三研究所, 数据安全技术研发中心. 生成式人工智能数据跨境流动风险与治理白皮书 [R/OL]. (2025 - 01 - 10) [2025 - 02 - 12]. https://www.fxbaogao.com/detail/4667154.

[8] 曹晓明, 张永和, 潘萌, 等. 人工智能视域下的学习参与度识别方法研究——基于一项多模态数据融合的深度学习实验分析 [J]. 远程教育杂志. 2019, 37 (1): 32 - 44.

[9] BALTRUŠAITIS T, AHUJA C, MORENCY L P. Multimodal machine learning: a survey and taxonomy [J]. Transactions on Pattern Analysis and Machine Intelligence, 2019, 41 (2): 423 - 443.

[10] 周坤, 傅德胜. 基于 Windows Socket 的网络数据传输及其安全 [J]. 计算机工程与设计, 2007 (22): 5381 - 5383, 5386.

[11] 鲁传颖, 章时雨. 东盟数字地缘政治的战略构想与实施路径 [J]. 南洋问题研究, 2024 (1): 45 - 60.

[12] 刘业. 美欧数据跨境流动博弈中的欧盟技术主权战略及其实现 [J]. 国际法研究, 2023 (6): 64 - 85.

[13] 赵昊. 三星员工被曝不当使用 ChatGPT 半导体机密数据直传美国 [EB/OL]. (2023 - 04 - 03) [2025 - 03 - 13]. https://mp.weixin.qq.com/s?__biz=Mzg4MTEyNzc4Mg==&mid=2247558592&idx=3&sn=4cc59652188ad8a68564ae3486d9dec7.

[14] United Nations Conference on Trade and Development. Digital economy report 2021: cross-border data flows and development-For whom the data flow [EB/OL]. [2025 - 03 - 13]. https://unctad.org/system/files/official-document/der2021_en.pdf.

[15] 王智珑. 中国如何因应欧盟《数字服务法》"布鲁塞尔效应"[J]. 西昌学院学报 (社会科学版), 2024, 36 (6): 75 - 85.

[16] 蔡开明. 美国对华法律政策工具以及我国反制措施研究 [J]. 行政管理改革, 2022 (4): 51 - 63.

[17] 孙永超. 论美国跨境刑事数据调取中的国际礼让: 以《云法案》为例的分析 [J]. 求是学刊, 2024, 51 (3): 126 - 139.

[18] 徐凤. 网络主权与数据主权的确立与维护 [J]. 北京社会科学, 2022 (7): 55 - 64.

[19] APEC. Enabling electronic commerce: the contribution of APEC's data privacy framework [EB/OL]. (2011 - 10 - xx) [2025 - 03 - 14]. https://www.apec.org/Publications/2011/10/Enabling-Electronic-Commerce-The-Contribution-of-APECs-Data-Privacy-Framework.

[20] 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.

[21] 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.

[22] 徐凌验. 全球跨境数据治理态势与启示 [J]. 中国经贸导刊, 2024 (7): 73 - 76.

[23] 白舒婕. "数字中国": 以开放之姿拥抱世界 [N]. 国际商报, 2024 - 11 - 28 (001).

[24] 中国人大网. 中华人民共和国网络安全法 [EB/OL]. (2016 - 11 - 07) [2025 - 03 - 10]. http://www.npc.gov.cn/zgrdw/npc/xinwen/2016 - 11/07/content_2001605.htm.

[25] 张新新，游恒飞. 从 ChatGPT 到 DeepSeek：多模态大模型与出版业未来——兼论走向“十五五”的出版智能化转型［J/OL］. 中国编辑，1－11［2025－08－01］. https：//link. cnki. net/urlid/11. 4795. g2. 20250409. 1500. 002.

[26] 马光，王丽雯. 国际软法视角下人工智能全球治理的现状与建议［J］. 海关与经贸研究，2024，45（3）：1－19.

[27] 冯洁菡，周濛. 跨境数据流动规制：核心议题、国际方案及中国因应［J］. 深圳大学学报（人文社会科学版），2021，38（4）：88－97.

[28] 张亮，陈希聪. 生成式人工智能背景下的跨境数据安全规制——基于 DeepSeek、ChatGPT 等主流 AI 的思考［J］. 湖北大学学报（哲学社会科学版），2025，52（2）：120－128，199.

[29] 刘权. 数字经济视域下包容审慎监管的法治逻辑［J］. 法学研究，2022，44（4）：37－51.

[30] 张涛. 生成式人工智能训练数据集的法律风险与包容审慎规制［J］. 比较法研究，2024（4）：86－103.

[31] 徐伟，赵洲. 隐私计算赋能政府数据开放：逻辑理路、现实风险与优化路径［J］. 情报杂志，2025，44（6）：193－200.

[32] 许皖秀，左晓栋. 全球竞争格局下的中国特色数据跨境流动治理方案研究［J］. 中国工程科学，2025，27（1）：111－121.

[33] 全球人工智能治理倡议［EB/OL］.（2023－10－20）［2025－03－24］. https：//www. fmprc. gov. cn/web/ziliao_674904/1179_674909/202310/t20231020_11164831. shtml.

[34] 魏巍. 完善金融数据跨境流动监管［J］. 中国金融，2024（14）：88－89.

[35] 张静，朱成凤. 金融数据跨境流动治理困境与完善进路［J］. 金融发展研究，2025（6）：82－90.

[36] 中国网信网. 全球数据跨境流动合作倡议［EB/OL］.（2024－11－20）［2025－03－24］. https：//www. cac. gov. cn/2024－11/20/c_1733706018163028. htm.

[37] 陈永怡，孟彦辰. 澳大利亚健康医疗数据跨境流动法律规制研究及其对中国的启示［J］. 中国全科医学，2024，27（25）：3091－3099.

[38] 姜海霞. 档案数据跨境流动的法律挑战与应对策略［J］. 山西档案，2025（9）：155－157.

（收稿日期：2025－08－03）

作者简介：

宋延敏（2002－），女，硕士研究生，主要研究方向：人工智能法、数据法。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部