Open Journal of Legal Science 法学, 2025, 13(12), 2903-2912
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.1312395

Hans汉斯

生成式人工智能背景下的数据跨境流动安全规制问题

梁澜馨

澳门科技大学法学院，澳门

收稿日期：2025年11月5日；录用日期：2025年11月18日；发布日期：2025年12月16日

摘　要

本文围绕生成式人工智能背景下的数据跨境流动安全规制问题展开讨论，从技术与数据流动的共生关系出发，分析了生成式人工智能在基础层、技术层与应用层中给跨境数据流动带来的合规性挑战，并分析了现行法律规制在应对新型风险时的不足。在此基础上，笔者提出应当构建起“双轨并行”的治理路径：国内层面应完善数据分类分级制度，建立覆盖全产业链的跨境数据监管体系；国际层面则需积极参与并引导全球规则制定，以实现技术创新与数据安全的有效平衡。

关键词

生成式人工智能，数据跨境，数据安全，法律规制

Security Regulation Issues of Cross-Border Data Flow in the Context of Generative Artificial Intelligence

Lanxin Liang

Faculty of Law, Macau University of Science and Technology, Macau

Received: November 5, 2025; accepted: November 18, 2025; published: December 16, 2025

Abstract

This paper explores regulatory challenges for cross-border data flows in the context of generative artificial intelligence. Starting from the symbiotic relationship between technology and data mobility, it analyzes compliance challenges posed by generative AI at the foundational, technological, and application layers for cross-border data flows. It further examines the inadequacies of existing legal

文章引用: 梁澜馨. 生成式人工智能背景下的数据跨境流动安全规制问题[J]. 法学, 2025, 13(12): 2903-2912.
DOI: 10.12677/ojls.2025.1312395

frameworks in addressing emerging risks. Building upon this foundation, the author proposes establishing a "dual-track" governance approach: domestically, refining data classification and grading systems while establishing a cross-border data supervision framework covering the entire industrial chain; internationally, actively participating in and guiding global rule-making to achieve an effective balance between technological innovation and data security.

Keywords

Generative Artificial Intelligence, Data Cross-Border, Data Security, Legal Regulation

1. 引言

自 2022 年 11 月美国 OpenAI 公司推出 ChatGPT 以来，生成式人工智能迅速崛起，成为驱动数字经济发展的关键引擎，显著加速了人类社会迈向通用人工智能时代的进程。2024 年 12 月 26 日，中国深度求索公司发布自主研发的 DeepSeek-V3 开源模型，其多项核心性能指标已达到 GPT-4、Claude-3.5-Sonnet 等国际主流大语言模型的同等水平。2025 年 1 月 20 日，该公司进一步推出 DeepSeek-R1 开源模型，其性能与 OpenAI 的 o1 模型相当，但成本仅为后者的三十分之一，取得了突破性优势。

DeepSeek 系列模型的问世标志着中国在生成式人工智能领域进入全新阶段，要充分发挥生成式人工智能的潜力并确保其可持续发展，必须构建与之相匹配的高质量法律治理框架。从技术层面分析，海量的高质量数据始终是驱动生成式人工智能发展的核心因素。数据的规模与模型的性能呈现正相关的关系，丰富的数据资源能够有效提升生成内容的准确性、多样性和创新性，而数据要素的安全自由流动和合理配置也是推动生成式人工智能迭代升级的关键动力。

生成式人工智能技术的发展提高了数据跨境流动的自由度，也不可避免地提高了数据的泄露和滥用风险，这给现有的法律框架带来了全新挑战。在数据采集、存储和应用的全流程中，必须建立严格的法律合规和审查机制，做到促进数据高效流动的同时保障数据跨境的安全性。

此外，各国在监管制度和价值取向上的差异使得构建全球协同的治理机制变得尤为迫切。如何在确保数据安全的前提下推动形成开放、包容的国际合作格局，成为当前人工智能发展亟待解决的核心议题。

2. 数据要素的核心地位与跨境流动的安全挑战

生成式人工智能的发展建立在数据、算力和模型这三大要素之上。数据作为模型训练的基础原料，其质量与规模直接影响其性能的高低；算力为训练推理提供必要的计算资源，而模型架构则决定了系统的功能和效率。

其中，数据要素始终发挥着关键性作用，模型的性能提升与数据的获取和利用程度密切相关[1]。高质量的数据能够为模型提供更准确的学习样本，从而提升模型的泛化能力和生成质量。随着数据规模的不断扩大和数据类型的日益复杂，数据的存储、管理和安全保护成为亟待解决的问题。数据高度自由的跨境流动也带来了新的挑战，尽管 DeepSeek 系列模型通过优化算法设计显著降低了对高端算力的依赖，从而缓解了算力资源的瓶颈问题，但作为模型训练的核心资源，数据的关键作用依然不可替代。

跨境数据安全问题本质上源于生成式人工智能的技术特性与数据流动的客观属性。生成式人工智能

作为一种强大的内容生成工具，其运作必然依赖海量数据的处理与流动。数据的跨境流动是其技术应用的必然需求，但同时也带来了数据安全、隐私保护以及合规性等方面的挑战。生成式人工智能的底层技术逻辑决定了其对数据的依赖性，而数据的动态流动特性则进一步加剧了跨境数据安全问题，数据在跨境传输过程中面临着泄露、篡改、滥用等风险。

(一) 生成式人工智能的技术特性

生成式人工智能的核心特征是能够运用算法模型自主生成文本、图像、音频、视频及代码等多样化数字内容。我国《生成式人工智能服务管理暂行办法》将其明确定义为“具备文本、图像、音频、视频等内容生成能力的模型及相关技术”。

在生成式人工智能的底层技术逻辑中，数据是核心要素[2]。生成式人工智能从训练到内容生成均依赖数据，其运作机制是通过海量数据构建大规模数据池，再利用算法进行预训练、模拟演练、调整和优化，最终输出结果[3]。因此，数据是生成式人工智能底层技术的基础，大模型是技术层的核心，而像ChatGPT、DeepSeek、文心一言等聊天机器人及其生成的内容则是应用层的体现。

生成式人工智能模型具有涌现能力，例如聊天机器人依赖大语言模型的上下文学习、指令遵循和逐步推理能力，展现出“拟人化”的特性。然而，生成式人工智能的研发无法完全脱离人类参与，人类偏见可能通过数据和训练过程传递到模型中。此外，涌现能力可能导致数据风险在模型迭代和演化过程中不断传递到应用层面。主流应用如 ChatGPT、DeepSeek、文心一言、Sora 等能够实现人机实时交互，用户的使用过程涉及数据的交互和传输。这些应用具备收集、存储和使用交互内容数据的功能，而生成的内容也会被继续收集、存储和使用。在数据跨境活动的情况下，这进一步加剧了数据安全的挑战。

(二) 数据跨境流动与生成式人工智能发展的共生关系

生成式人工智能的发展离不开数据的跨境流动。总体而言，生成式人工智能的技术进步依赖于网络通用数据与垂直领域数据的协同应用。主流大语言模型普遍采用跨境数据作为训练基础，例如 Common Crawl 这类 PB 级别的多语态数据集，其构建过程本身就涉及全球范围的数据采集。在专业领域，金融大语言模型 BloombergGPT 的 FinPile 数据集同样融合了跨境金融数据与通用语料。随着技术的不断进步，数据跨境流动的效率也显著提升。以 DeepSeek-V3 采用的知识蒸馏技术为例[4]，该技术通过数据增强与合成方法，在提升模型训练效率的同时，进一步强化了数据要素的跨境流动特征。无论是基础训练数据还是模型优化技术，都不可避免地涉及数据跨境传输。

然而，数据跨境流动虽然能释放数据价值，但也带来了监管挑战。数据的高度流动性和穿透性特征，使其极易突破各个国家的监管边界[5]，对国家利益和社会公共利益构成潜在风险，使得主要国家和地区限制或禁止跨境数据流动[6]。从技术角度分析，生成式人工智能的数据需求呈指数级增长(如 GPT-4 所需数据量达 GPT-3 的十倍)，仅靠单一国家的数据储备难以满足。我国生成式人工智能同样面临着训练数据不足的困境[7]。

生成式人工智能发展对于跨境数据的需求与数据跨境流动安全问题之间的矛盾凸显了加强国际数据治理合作的必要性。在保障数据安全的前提下，推动数据要素的全球优化配置、建立跨境数据流动的协同治理机制，已成为人类通向人工智能时代的必然选择。

(三) 生成式人工智能法律研究的现状与跨境数据安全空白

随着生成式人工智能技术的快速发展，相关法律问题已成为学界研究的重要议题。当前研究主要集中在三个宏观层面：生成式人工智能的法律属性界定[8]、潜在法律风险分析[9]以及治理路径探索[10]。从研究范式来看，现有成果主要基于算法[11]、数据[12]和具体应用场景[8]三个维度展开，其中针对不同数据处理阶段的安全问题研究尤为突出。

在风险识别方面，刘艳红教授提出生成式人工智能在数据准备、模型运算和内容生成三个阶段存在

显著安全风险[13]。就规制路径而言，学界主要存在三种观点：一是主张以运行阶段为监管重点[14]，二是强调构建数据主体责任矩阵[15]，三是建议采用“敏捷治理”模式应对数据风险[16]。这些研究为生成式人工智能的数据治理奠定了重要理论基础，但跨境数据安全这一关键领域仍存在着研究空白。

DeepSeek 系列开源模型的发布使数据安全的问题更具现实紧迫性，在 DeepSeek-R1 和 V3 模型在海外市场面临的多国审查中，数据安全问题成为焦点争议，例如意大利数据保护局就对其数据收集范围、来源、用途及法律依据等提出质询[1]。这一现象凸显了在技术发展与数据安全之间寻求平衡的重要性，既要保障技术创新的自由空间，又要防范跨境数据流动带来的安全隐患。

3. 生成式人工智能的特有技术风险及其法律挑战

生成式人工智能不仅放大了传统的数据安全风险，其独特的运作机制还催生了新型技术风险。这些风险根植于其技术内核，对建立在传统数据处理模式之上的《数据安全法》《个人信息保护法》等现行法律框架构成了具体而严峻的挑战，凸显了法律的滞后性。

(一) 训练数据爬取的非针对性与原初合规困境

生成式人工智能模型训练依赖于对海量互联网数据的非针对性、自动化爬取。这一特性与建立在“目的明确、最小必要”原则之上的个人信息处理规则产生了直接冲突。

模型训练需要 PB 级别的数据集，其爬取过程是“地毯式”的，无法在数据收集阶段明确具体的处理目的，也无法事先征得所有数据主体的同意。这导致训练数据中可能混杂大量未脱敏的个人信息、商业秘密甚至敏感信息，且其处理行为在数据收集的“原初时刻”就脱离了《个人信息保护法》第 13 条、第 6 条所规定的“知情–同意”框架和目的限制原则。

根据《个人信息保护法》，处理个人信息需有明确、合理的目的。而生成式 AI 的训练目的具有高度的概括性和事后性，使得其在数据获取源头就面临合规不能的困境。这使得海量的训练数据池从形成之初就带有“原罪”，其后的匿名化处理等技术措施更像是事后补救，而非事先的合规设计。

(二) 模型“涌现”与“幻觉”带来的不可预测性风险

生成式人工智能具备“涌现能力”，可能产生训练数据中不存在的新内容，同时也存在编造虚假信息的“幻觉”现象。这两种特性共同导致了其输出内容的不可预测性。

首先是内容安全风险，模型可能“涌现”出生成有害、偏见或歧视性内容的能力，这些内容并非直接复制自训练数据，而是模型内化学习后的一种“创造”。其次，事实安全风险。“幻觉”可能导致模型生成看似真实实则完全错误的信息，若被应用于医疗、金融、司法等领域，将引发公共安全和社会信任危机。

这直接挑战了《数据安全法》第 27 条要求的“采取相应技术措施和其他必要措施，保障数据安全”的责任边界。对于模型自身“创造”出的非源于单一输入数据的新型风险，如何界定“必要措施”？同时，《生成式人工智能服务管理暂行办法》第 4 条要求服务提供者承担内容生成者责任，但对于模型自主“涌现”出的有害内容，其责任认定变得异常复杂，超出了传统内容审核的管控范围。

(三) 交互数据的实时跨境与全程留痕风险

生成式 AI 应用层的实时交互特性，使得用户与模型的每一次对话都可能涉及数据的即时跨境传输与永久留存。

用户在与模型交互时，输入的查询、指令乃至上传的文件，都可能包含个人隐私、商业秘密甚至国家秘密。这些数据一经发出，即可能瞬时传输至境外服务器进行处理，并可能被服务商留存用于模型迭

[1]《意大利监管机构向 DeepSeek 寻求数据保护方面信息》，2025 年 1 月 29 日，https://www.tmtpost.com/nictation/7439302.html，2025 年 2 月 15 日。

代训练，形成“数据投喂”。这个过程具有即时性、单向性和不可逆性。

这给《数据安全法》第 31 条的数据出境安全评估、《个人信息保护法》第 38 条的个人信息出境合规路径带来了巨大挑战。对于亿万用户发起的、毫秒级的、内容不可预知的交互数据流，现行以事前评估、标准合同为主的出境监管模式几乎无法有效覆盖。用户无意中输入的重要数据，在现有技术框架下，其出境行为难以被实时阻断和审计，造成了监管的实质性盲区。

(四) 数据聚合与再识别的衍生风险

生成式人工智能具有强大的信息整合与推理能力，能够将看似无关的碎片化信息进行关联、整合，从而推导出新的敏感信息。

模型可能将来自公开渠道的多个非敏感数据片段进行聚合，从而精准推断出该主体的未公开敏感信息，实现数据的“再识别”与“增值”。这种衍生数据的敏感性可能远超其原始组成部分。

现行《个人信息保护法》第 4 条对个人信息的定义是“已识别”或“可识别”的，其保护重心在于原始数据的处理。对于通过 AI 聚合推理产生的、在收集时并“不存在”的衍生敏感信息，其法律属性和规制责任是模糊的。数据分类分级制度也难以预见和界定这种由技术动态生成的、高度聚合后的数据风险等级，使得《数据安全法》第 21 条的数据分类分级保护制度在应对此类动态风险时显得被动和滞后。

综上所述，生成式人工智能的非针对性爬取、不可预测的“涌现”与“幻觉”、实时交互跨境以及数据聚合衍生等特有技术风险，从数据处理的起点、过程、输出和衍生等多个维度，对现行数据法律体系的核心条款构成了精准而深刻的挑战。这不仅表现为监管范围的“空白”，更体现为法律基本原则与新技术逻辑之间的根本性张力。正是这种张力，确证了当前法律框架在应对技术范式变革时的结构性滞后，为下文分析现行规制模式的不足与构建新型治理路径提供了坚实的前提。

4. 立法现状

(一) 我国法治框架下的跨境数据安全

我国已构建起以《国家安全法》《网络安全法》《数据安全法》《个人信息保护法》为核心的数据安全法律体系，并配套出台《网络数据安全管理条例》《数据出境安全评估办法》《个人信息出境标准合同规定》等实施细则，形成了系统完备的数据治理制度框架。

这一法律体系具有以下特征：首先，确立了风险防控与安全保障的立法导向。四部基础性法律均将维护数据安全作为核心立法目标，其中《国家安全法》将数据安全纳入国家网络与信息安全保障体系；《数据安全法》创新性地界定了“数据安全”的法律内涵，强调通过必要措施确保数据的有效保护、合法利用及持续安全状态。其次，构建了覆盖境内外的全链条监管体系。《数据安全法》第二条第二款及《网络数据安全管理条例》第二条第三款均明确规定，境外数据处理活动如损害我国国家安全、公共利益或公民组织合法权益，将依法追究法律责任，充分体现了我国数据安全立法的域外效力。最后，形成了多层级协同的规范体系。从基础法律到配套法规，我国数据安全立法既确立了总体国家安全观的指导地位，又针对数据跨境流动等关键环节制定了可操作的实施细则。

我国数据保护法律体系以维护国家安全、公共利益及公民组织合法权益为核心要义，对跨境数据安全进行系统性规制。跨境数据安全作为数据安全的关键维度，其本质是国家安全的重要组成部分。本文主张，“跨境数据安全”概念应当有机整合“跨境数据流动”与“数据安全”的双重内涵，其界定标准应基于对数据本身的价值判断和事实判断，核心要义在于确保数据跨境流动不得损害我国国家安全、公共利益或公民组织合法权益。

随着生成式人工智能产业的快速发展，我国相继出台《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》《生成式人工智能服务安全基本要求》等专项法规。其中，《生成式人工

智能服务管理暂行办法》作为全球首部生成式人工智能专门立法，虽未直接规定数据出入境情形，但其第七条第五项明确要求服务提供者须依据《网络安全法》《数据安全法》《个人信息保护法》等法律法规开展训练数据活动。由此可见，生成式人工智能背景下的跨境数据安全保护，应当在把握技术特性的基础上，深入理解法益本位的安全要义，并以我国现行数据保护法治框架为根本遵循。

(二) 在当前法律框架下生成式人工智能跨境数据安全规制的必要性

1) 多层级数据的安全风险分析

首先是基础层与技术层上的风险，生成式人工智能在基础层和技术层主要依赖公开数据进行模型训练。然而，跨境数据爬取行为往往涉及个人隐私、国家安全数据、商业秘密等非公开数据，这种行为既缺乏法律依据又存在重大安全隐患。而大模型在持续学习过程中很可能涉及敏感数据，对国家安全构成潜在威胁。以 DeepSeek-V3 等开源大模型为例，其 API 接口的开放性使得境内外主体均可调用训练数据资源，显著增加了数据跨境流动的安全风险[17]。

其次是应用层风险，在应用层面，生成式人工智能的即时交互特性带来了独特的数据安全挑战。以 ChatGPT 为例，用户查询的数据会实时传输至境外服务器进行处理，整个过程涉及敏感数据的即时跨境流动。尽管服务商制定了数据保护政策，但实际的监管效果非常有限。2023 年意大利数据保护局就因发现 ChatGPT 存在用户数据泄露风险而暂停其服务，这一案例凸显了应用层的安全隐患 [2]。

总体而言，生成式人工智能的跨境数据安全呈现出四大核心风险特征：首先，数据跨境流动具有即时性特征，用户交互数据可在毫秒级完成跨国传输；其次，监管机制存在明显盲区，现有体系难以有效监控用户自主输入内容；再次，风险传导效应显著，训练数据中的潜在偏差可能通过模型输出广泛扩散；最后，规模效应加剧风险，大模型参数量级(如 GPT-3 的 1750 亿参数)的指数级增长，使得安全风险呈几何级放大。这些特征共同构成了生成式人工智能跨境数据安全的系统性挑战。

而用户可能无意中输入涉及国家安全、经济运行等重要数据，这些数据的跨境流动将带来难以估量的安全挑战。当前亟需建立针对生成式人工智能特性的数据跨境流动监管框架，以平衡技术创新与安全保障。

2) 生成式人工智能对数据聚合的治理挑战

生成式人工智能技术与高聚合度数据的结合，可能自主生成危害国家安全、社会稳定和公共健康的内容并快速扩散。这一风险主要源于三个层面：

首先，数据类型的差异性风险。个人数据在用户知情同意前提下跨境使用风险可控，但政务数据等非个人数据的跨境流动可能直接威胁公共安全。以滴滴出行为例，其积累的地理坐标、街景建筑等数据一旦跨境流动，将严重危害我国国土安全、军事安全和经济安全。其次，垂直领域数据的特殊性风险。医疗健康、人类遗传资源等特定领域数据具有特殊敏感性。《人类遗传资源管理条例实施细则》明确规定，500 例以上的基因组测序数据向境外提供需通过安全审查[18]，这类数据的聚合流动可能危及国家生物安全。最后，技术特性的放大效应风险。生成式人工智能具有强大的即时交互能力，当高聚合度的垂直领域数据或个人数据被输入系统并跨境流动时，其危害性将被技术特性几何级放大，对国家利益和公民权益构成严重威胁。

治理困境的根源在于生成式人工智能的技术特性与数据聚合的规模效应相互强化，使得传统的数据分类分级保护机制面临新的挑战。需要建立与人工智能技术发展相适应的新型数据治理框架，在保障数据要素价值释放的同时，守住国家安全底线。

[2]《涉嫌侵犯隐私意大利数据保护机构对 ChatGPT 开发公司展开调查》，2023 年 4 月 1 日，http://world.people.com.cn/n1/2023/0401/c1002-32655784.html，2025 年 2 月 15 日。

3) 现行规制模式难以协调国际利益分歧

生成式人工智能技术的突破性发展标志着通用人工智能时代的来临。当前技术迭代已进入多模态阶段，应用场景持续拓展，正成为驱动全球数字经济发展的核心动力，这一技术革新正在重塑国际权力博弈格局[19]。

目前，主要国家和地区对生成式人工智能跨境数据安全的规制仍处于探索阶段，试图建立统一的数据跨境治理框架。现有规制模式主要形成于大数据时代，呈现出三大特征：一是区分个人数据与非个人数据的监管范式；二是采用数据分级分类的流动管控机制；三是通过规范协同扩大规制域外效力。然而，这些基于传统数据治理逻辑的规制体系已难以适应生成式人工智能的技术特性，呈现出明显的滞后性。

各国在跨境数据安全方面的利益诉求存在显著差异，美国奉行国家安全优先原则[20]，欧盟坚持个人数据保护至上。这种根本性的理念分歧导致国际规则制定陷入博弈困境，可能引发零和甚至负和博弈。在通用人工智能加速发展的背景下，亟需构建与之匹配的新型跨境数据安全治理体系，以有效协调国际利益分歧，促进技术健康发展。当前规制框架的不足，正日益成为制约全球生成式人工智能协同发展的重要瓶颈。

5. 我国生成式人工智能跨境数据安全治理路径

随着 DeepSeek-R1 和 V3 大模型在深圳、广州、无锡等城市政务系统的深度应用，生成式人工智能技术正加速与经济社会各领域逐步融合。在此背景下，构建完善的数据安全治理体系，确保国家、组织及个人数据在技术发展过程中得到有效保护和合法利用，已成为当前亟待解决的关键问题。

但鉴于人工智能技术的高度复杂性，要想在短期内建立统一的全球治理框架存在一定的困难。我国可以立足国情，采取“双轨并行”的治理策略，国内层面依托数据分类分级保护制度，建立覆盖数据全生命周期的监管体系；国际层面积极推动形成跨境数据安全治理共识，引导全球规则制定。这一治理路径既能保障技术安全可控发展，又能为全球人工智能治理贡献中国智慧，最终实现生成式人工智能技术的向善发展。

(一) 数据分类分级保护制度的构建与完善

数据分类分级保护制度是跨境数据安全规制的核心基础。《数据安全法》第二十一条明确规定，应根据数据在经济社会发展中的重要程度及其潜在安全风险，对数据实施分类分级保护。具体而言，数据安全风险主要体现为数据遭到篡改、破坏、泄露或非法获取、利用时，对国家安全、公共利益以及个人、组织合法权益可能造成的危害程度。基于此，我国确立了以一般数据、重要数据和核心数据为框架的分级保护体系，其中核心数据(涉及国家安全、国民经济命脉、重要民生及重大公共利益等)需适用更为严格的管理制度。

在现有制度框架下，跨境数据安全规制的构建应覆盖国家安全数据、公共数据、企业数据和个人数据等全类型数据，并依据其敏感程度实施差异化保护措施。对高风险数据实施重点管控是国际通行做法[21]，例如美国通过《国家安全信息分类》和《受控非密信息》行政令，建立了一套层次分明、覆盖全面的数据安全监管体系。该体系采用双轨制管理模式：一方面对国家安全信息实施严格的三级分类管理，将涉密信息划分为“最高机密”(Top Secret)、“机密”(Secret)和“秘密”(Confidential)三个等级，根据信息泄露可能造成的国家利益损害程度实施差异化管控，并建立动态调整机制，使分类标准能够随国际形势和技术发展而灵活更新；另一方面对受控非密信息进行精细化分类，将隐私数据、关键基础设施信息等重要但不涉密的数据细分为 20 个大类和 126 个子类，覆盖金融、医疗、能源等关键领域，通过这种多层次分类体系实现精准监管，既避免了“一刀切”监管可能导致的资源浪费，又确保了不同行业、不同敏感程度的信息都能得到恰当保护。

欧盟颁布的《人工智能法》作为全球首部综合性人工智能监管框架，通过系统性制度设计构建了人工智能时代数据保护的“黄金标准”。该法案在数据收集环节确立了严格的“最小化原则”，明确规定人工智能开发者只能收集与特定目的直接相关的必要数据，并通过“场景化限制”和“技术性要求”的双重约束，有效遏制了数据滥用现象。并且，法案创新性地将数据保护要求贯穿人工智能全生命周期，在开发阶段要求数据来源标注和偏见风险评估，在运行阶段强制实施数据完整性监控(如自动驾驶系统的异常数据识别)，并建立用户数据删除权和溯源机制，形成闭环管理。此外，法案将传统信息安全领域的三性原则(机密性、完整性、可用性)转化为具体技术标准，要求高风险人工智能系统采用同态加密技术、训练数据通过 ISO 认证、关键系统配备灾备方案。《人工智能法》进一步强化了数据保护要求，明确数据收集应遵循最小化原则，仅限实现特定目的之必需，并严格规范数据处理流程，确保数据的机密性、完整性与可用性。

由此可见，完善数据分类分级制度不仅是我国数据安全治理的内在需求，也与国际实践高度契合，为跨境数据流动提供了系统性保障。基于生成式人工智能的技术特性，其发展过程中应当建立“分层管控、量化评估”的跨境数据安全治理体系。具体而言，应当构建数据分层管理机制，也就是根据数据的重要程度、敏感程度、商业价值和应用场景，建立四级分类管控体系。首先，应当严格禁止任何形式的国家安全数据跨境流动，不得将其作为生成式人工智能的训练语料或输入数据；其次，对于公共数据应当基于数据的体量、内容属性和法益影响等维度进行风险评估，禁止将涉及重要民生、重大公共利益的核心数据用于基础层训练；此外，对于企业数据应当建立合规审查机制，防范通过境外人工智能服务导致的数据弥散性风险；最后，对于个人数据实行差异化管控，一般数据允许个人自主处理，敏感个人数据(如生物识别、医疗健康等)在达到特定体量时实施跨境流动限制。

还应当建立完善的数据量化评估体系，通过设置数据体量阈值、使用场景分类、处理主体资质等多维评估指标，构建动态化的安全评估模型。这一体系包含三个关键机制：首先，建立敏感数据聚合预警机制，防范碎片化数据经 AI 整合后产生的衍生风险；其次，针对基础层、技术层、应用层等不同层级，制定差异化的存储规范、访问权限和安全防护标准；最后，构建数据跨境流动的实时监测系统，实现全生命周期的可追溯性与可审计性。该治理框架既有效保障了数据要素的跨境有序流动，又通过精准管控关键数据风险，为生成式人工智能的创新发展提供了制度保障，能够实现技术应用与安全治理的动态平衡，为数字经济时代的跨境数据治理探索出了一条具有可操作性的实践路径。

(二) 构建全产业链跨境数据监管体系

在生成式人工智能快速发展的背景下，跨境数据安全监管应当立足“技术本位”的观念，秉持包容审慎原则，通过产业链各环节的协同治理，实现数据跨境自由流动与安全保障的动态平衡，促进技术向善发展。

首先，应在基础层和技术层建立多元主体共担的跨境数据安全责任体系。生成式人工智能产业链涉及数据提供者、模型开发者、服务提供者等多个主体，需要构建穿透式的责任分配机制。当前我国《生成式人工智能服务管理暂行办法》等法规主要规范服务提供者的数据保护义务，但产业链上游的数据采集、处理等环节同样关键。应当将监管范围扩展至网络爬虫公司、数据中介商等基础层主体，确保训练数据来源合法、处理规范，切实保护数据主体的合法权益。其次，在应用层要建立多方协同的风险防控机制。建议采取“政府引导 + 行业自律 + 企业自治”的协同治理模式：一是由监管部门制定分场景的数据跨境指引；二是推动行业组织建立自愿性标准；三是鼓励企业完善用户行为规范。通过多元主体共同参与，既防范重要数据泄露风险，又为技术创新留出空间，实现安全与发展的有机统一。

这种全产业链的监管思路覆盖了从数据采集到应用服务的完整链条，通过差异化责任分配实现了精准治理，为生成式人工智能的健康发展提供了制度保障。

(三) 构建跨境数据安全治理的国际共识体系

随着 DeepSeekV3 及 R1 模型的成功发布，我国的生成式人工智能技术实现了跨越式发展，其开源特性对全球生成式人工智能的技术进步产生深远影响，我国应积极推动形成适应生成式人工智能发展的跨境数据国际规则体系。

首先，依托现有国际合作框架深化各国间的共识。我国参与的《区域全面经济伙伴关系协定》(RCPC)正在推进的《全面与进步跨太平洋伙伴关系协定》(CPTPP)、《数字经济伙伴关系协定》(DEPA)等协定已为数据跨境流动规则奠定了重要基础。这些协定在促进数据自由流动的同时，均设置了差异化的安全例外条款：RCEP 通过国家安全例外保留监管空间，DEPA 强调安全框架下的开放共享，CPTPP 虽倡导高度自由化但仍保留安全例外。基于此，我国可结合生成式人工智能的技术特性，以 RCEP 的区域共识为基点，逐步对接 DEPA 和 CPTPP 的高标准，重点完善三方面工作：优化数据分类分级制度与国际标准的衔接，细化全类型数据出境评估机制，建立规范化的安全例外援引程序，从而实现数据流动与安全的动态平衡。

其次，推动全球人工智能治理的深度协作。DeepSeek 系列模型的开源实践重塑了行业生态，彰显了技术共享的价值。在生成式人工智能的发展进程中，应当坚决反对单边数据流动限制和技术出口管制等保护主义行为，引导企业恪守公平非歧视原则。具体而言，在基础层、技术层和应用层的跨境数据使用中，构建包含三重要求的治理体系：技术研发需遵循伦理规范，数据应用应坚持向善导向，国际合作要促进共同发展。通过这种多层次的协同治理，推动全球人工智能产业健康有序发展。

这一治理框架立足现有国际合作成果实现规则的渐进式演进，并且通过开源生态建设推动治理模式创新，为平衡技术创新与安全治理提供了中国方案，通过国际合作完全能够实现数据安全与流动性的有机统一，为数字经济发展创造更有利的国际环境。

参考文献

[1] 赵鑫. 大语言模型[M]. 北京: 高等教育出版社, 2023: 16.

[2] 时诚. 通用人工智能训练数据的权利配置——以 ChatGPT 类大模型为例[J]. 湖北大学学报, 2024, 51(4): 132-142.

[3] 邓建鹏, 赵治松. DeepSeek 的破局与变局: 论生成式人工智能的监管方向[J]. 新疆师范大学学报, 2025, 46(4): 99-108.

[4] 郑智航. 数据安全与数据利用平衡的法治保障[J]. 人民论坛·学术前沿, 2023(6): 79-87.

[5] 卫承霏, 蒋洁. 全球跨境数据安全治理的多维逻辑与中国应对[J]. 图书与情报, 2022(6): 26-33.

[6] 王飞跃. 我国生成式人工智能的发展现状与趋势[J]. 人民论坛, 2025(2): 21-26.

[7] 张凌寒. 生成式人工智能的法律定位与分层治理[J]. 现代法学, 2023, 45(4): 126-141.

[8] 刘艳红. 生成式人工智能的三大安全风险及法律规制——以 ChatGPT 为例[J]. 东方法学, 2023(4): 29-43.

[9] 罗亚海. 生成式人工智能法律治理现代化研究[J]. 湖北大学学报(哲学社会科学版), 2024, 51(1): 144-153.

[10] 丁道勤. 产业链视角下生成式人工智能的竞争法规制研究[J]. 西北工业大学学报(社会科学版), 2024(1): 99-107.

[11] 丁国峰, 寿晓明. 生成式人工智能算法的法律风险及其规范化防控[J]. 云南大学学报(社会科学版), 2024, 23(3): 107-119.

[12] 许雪晨. ChatGPT 等大语言模型赋能数字时代金融业: 基于隐私保护算法歧视与系统风险[J]. 暨南学报(哲学社会科学版), 2024, 46(8): 108-122.

[13] 马治国, 张楠. 通用人工智能的数据风险及法治应对路径[J]. 北京工业大学学报, 2024, 24(5): 131-142.

[14] 张欣. 生成式人工智能的数据风险与治理路径[J]. 法律科学(西北政法大学学报), 2023, 41(5): 42-54.

[15] 郑煌杰. 生成式人工智能数据风险治理的模式转型——从“传统治理”到“敏捷治理” [J]. 上海政法学院学报, 2024(6): 84-100.

[16] 孔祥承. 国家安全视阈下生成式人工智能的法治应对——以 ChatGPT 为视角[J]. 法治研究, 2023(5): 61-70.

[17] 李雅琴. 数字治理视域下健康数据利用权益制度构建[J]. 湖北大学学报(哲学社会科学版), 2024, 51(2): 163-173.
[18] 姚璐. 生成式人工智能形塑国际博弈新逻辑[J]. 中国社会科学报, 2024(7): 7.
[19] 程海烨, 王健. 美国升级跨境数据安全规制新动向[J]. 现代国际关系, 2024(12): 73-95, 145-146.
[20] 刘金瑞. 我国重要数据认定制度的探索与完善[J]. 中国应用法学, 2024(1): 189-200.
[21] 王剑. 数据分类分级: 实践进展与经验启示[J]. 数据与计算发展前沿(中英文), 2024, 6(6): 10-18.