doi. 10. 3724/1005-0566. 20261016

# 发展与安全并重:
# 人工智能新业态的数据跨境流动治理

王楚晴[1],张子玉[1],于华溢[2]
(1. 中国政法大学国际法学院/涉外法治学院,北京　100088;2. 北京工商大学法学院,北京　100048)

**摘　要**:随着人工智能国际产业持续深化,加工服务型、远程访问型、模型输出型等数据出境新形式不断涌现,呈现衍生化、隐蔽化、内嵌化等特征。面对新型出境形态,我国以原始数据物理传输为核心的数据出境治理体系在主体识别、客体界定、行为定性三个层面存在法律适用困境,既会形成国家安全风险的监管盲区,也会制约我国人工智能产业的国际竞争力与合作空间。对此,本文提出面向人工智能新业态推动治理体系转向。治理理念由数据安全逻辑主导向安全逻辑与经贸促进逻辑相协调转变;治理手段从事前静态申报审查向"负面清单+事后追责"的动态机制转变;治理格局从国内制度自我完善向国内治理与国际合作协同推进转变。以此在守住安全底线的前提下释放产业创新活力,为我国参与全球人工智能竞争、引领区域人工智能合作提供法治保障。

**关键词**:人工智能;国际服务贸易;数据跨境流动;经贸促进逻辑
**中图分类号**:D920. 1　　**文献标识码**:A　　**文章编号**:1005 - 0566(2026)10 - 0199 - 12

## Balancing development and security:
## Governance of cross-border data flows in the new AI landscape

WANG Chuqing[1], ZHANG Ziyu[1], YU Huayi[2]
(1. *School of International Law/School of Foreign-Related Rule of Law, China University of Political Science and Law, Beijing* 100088, *China*;
2. *School of Law, Beijing Technology and Business University, Beijing* 100048, *China*)

**Abstract**: With the deepening of international cooperation in the artificial intelligence industry, new forms of outbound data transfer—such as the processing-service type, remote-access type, and model-export type—keep emerging, exhibiting core features of derivation, concealment, and internalization. In the face of these new exit forms, China's outbound data transfer governance system, which is centered on the physical transmission of raw data, faces legal application dilemmas in three dimensions: subject identification, object definition, and behavior characterization. These dilemmas not only create regulatory gaps for national security risks, but also risk constraining the international competitiveness and cooperation space of China's artificial intelligence industry. To address this, this paper proposes a systematic shift of the governance system for new AI business formats: in terms of governance philosophy, shifting from the dominance of data security logic to the coordination between data security logic and economic and trade promotion logic; in terms of governance instruments, shifting from static ex-ante declaration and review to the dynamic mechanism

**基金项目**:中国政法大学青年教师学术创新团队支持计划(26CXTD01)。

**作者简介**:王楚晴(1989—),女,辽宁沈阳人,中国政法大学国际法学院/涉外法治学院助理教授、硕士生导师,研究方向为全球数字治理、人工智能法学。通信作者:于华溢。

of negative list + post-event accountability; in terms of governance structure, shifting from the self-improvement of domestic institutions to the coordinated advancement of domestic governance and international cooperation. This shift aims to unleash the vitality of industrial innovation while upholding the security bottom line, and provide legal guarantees for China to participate in global AI competition and lead regional AI cooperation.

**Key words**: artificial intelligence; international trade in services; cross-border data flows; trade-promotion logic

人类社会正加速迈入智能时代,人工智能成为大国战略博弈与全球治理议程的关键议题。2026 年 7 月 16 日,29 个创始成员国在上海签署《关于成立世界人工智能合作组织的协定》,全球首个人工智能政府间国际组织正式成立[1]。国家主席习近平在 2026 世界人工智能大会暨人工智能全球治理高级别会议开幕式主旨讲话中强调,“中国坚持发展和安全并重,不断完善相关法律法规、政策制度、应用规范、伦理准则,确保人工智能安全、可靠、可控”[2]。

近年来,人工智能领域跨境经贸活动日趋活跃,数据作为人工智能的核心燃料[3],其能否合法、高效、可预期地跨境流动已成为人工智能领域跨境经贸活动落地的首要前提。然而,人工智能新业态下数据出境形态正发生根本性嬗变,对现行以原始数据物理传输为核心的跨境流动治理框架带来深刻挑战,数据出境规则供给的确定性也因此而成为决定产业发展水平与国际合作深度的关键变量。

在此背景下,如何面向人工智能时代数据出境新形态构建适配数据跨境流动治理体系已成为当前亟待回应的关键命题。本文立足新型数据出境特点以及安全防控与产业发展的张力需求,系统探讨数据跨境流动治理的范式转向及其制度建构路径。

## 一、人工智能新业态中数据跨境流动的新型形态

人工智能产业深度融入传统国际服务贸易、货物贸易、技术贸易与投资合作,数据出境方式正从“数据资源的跨境传输”转向“数据价值的跨境获取”。人工智能新业态中的数据跨境流动场景不再局限于原始数据集的直接交付,而是更多内嵌在数据加工服务、场景采集服务、模型与应用产品出海等多元形态中实现跨境,在出境客体、加工深度、交付方式等方面呈现出新型样态与特征。

### (一)加工服务型出境

加工服务型出境以经深度加工的衍生数据成品为出境客体,以一次性或周期性的批量传输为交付方式。其是指境内主体接受境外委托,对原始数据开展清洗、标注、脱敏、特征提取等加工处理后,并将生成的衍生数据成品传输至境外的跨境服务模式。

第一类是“境外数据 + 境内加工”场景,指数据原始采集地与最终使用地均位于境外,中国企业仅作为受托方提供中立的数据加工服务。该场景是传统来料加工在数字服务领域的业态延伸。传统来料加工是指进口料件由境外企业提供,经营企业不需要付汇进口,按照境外企业的要求进行加工或者装配,只收取加工费,制成品由境外企业销售的经营活动(《中华人民共和国海关加工贸易货物监管办法》第四十条),性质上属于跨境服务贸易;数字经济语境下的来数加工泛指境外人工智能企业将采集自境外的原始图像、语音、文本等数据,委托中国数据处理者进行清洗、标注、分类、对齐等工序,待加工完成后将标注数据集、特征数据集等衍生产品回传至境外的商业模式。典型实践集中于数据标注领域,数据标注本质上属于劳动密集型产业,中国则凭借人力资源充裕、加工成本较低等比较优势,在全球人工智能数据标注市场中占据了重要地位[4]。

第二类是“境内采集 + 境内加工”场景,即原始数据采集自中国境内,由中国企业完成数据加工的服务并向境外交付。相较于来数加工服务,该场景下数据加工服务链条向上游延伸至数据收集环节。典型实践体现在具身智能数据采集、自动驾驶路测数据采集等领域,得益于中国境内可供依托的复杂多元应用场景,得以采集到动作轨迹、环境交互、传感器读数等高价值训练数据集。

加工服务型出境的核心特点在于出境客体完成了从原始数据到衍生数据的形态转换,即以进

行深度分析、过滤与提炼整合等处理活动后生成的高附加值数据形态[5]出境。从形式上看,原始数据经加工处理后,直接标识符被移除,信息内容杂糅,个人信息与敏感信息的可识别性降低,出境安全风险随之弱化。但实质上,衍生数据风险等级并非静态不变,其安全属性高度依赖原始数据的来源与敏感程度,以及加工处理的脱敏深度。上述两类场景出境条件存在差异。一是数据完全来源于境外的场景,因安全风险度低,已被纳入现行规则数据出境豁免范畴(《促进和规范数据跨境流动规定》第四条);二是数据源自境内场景下能否出境还需结合具体情况认定。从概念边界看,加工服务型出境虽也涉及境内数据,但其以"加工数据成品的一次性交付"为标志,既区别于远程访问型对原始数据的持续开放访问权限,也区别于模型输出型对技术产品的跨境部署与持续性服务调用。

**(二)远程访问型出境**

远程访问型出境的数据物理位置留存境内,出境实质为境外主体对境内数据的远程访问权限及经由访问获取的数据本身。随着中国人工智能企业全球化布局加速,越来越多的企业选择在境外部署算力中心、研发机构等产业设施。例如,字节跳动已于2024年6月宣布投资100亿林吉特(约21.3亿美元)在马来西亚建设人工智能中心,其子公司BytePlus正考虑在泰国建设数据中心[6];科大讯飞作为亚太地区知名的智能语音和人工智能企业,携手马来西亚企业在吉隆坡建设"人工智能多语言智能译制中心"基地[7]。这均是这一产业趋势的直观体现。

人工智能企业境外建厂的产业布局,带动境内总部与境外机构之间研发协同、业务联动与系统对接的常态化开展,催生出远程访问型这一更具隐蔽性的数据出境形态。在这一形态中,数据物理位置并不发生移动,境外主体通过远程系统登录、API数据对接、远程查询调取等技术路径,获得对境内数据的访问权限及经由访问所获取的数据本身。由于加工深度极低,境外主体触达的是原始或近原始状态的境内数据,因此该出境形式同样会构成实质性的数据利用与暴露。

远程访问型出境在流动逻辑与风险特征上与传统数据跨境传输存在本质差异。其一,流动形态从"数据物理传输"转向"访问权限获取"。远程访问的核心是数据的可接触性,最低层级权限为只读式的数据调取与获取,更高层级权限可延伸至对数据的编辑修改、状态调整,乃至对存储与处理系统的远程控制[8]。其二,风险呈现隐蔽化、持续性特征。传统数据跨境传输多为一次性或周期性的批量交付,行为边界清晰,易于识别与申报。远程访问型出境则具有持续性、实时性和隐蔽性的特征,境外主体可在任何时间点通过接口调用、数据查询等方式获取境内数据,单次访问的数据量可能极小且分散,但长周期的持续访问会形成数据聚合效应,其整体信息泄露风险与数据价值转移规模,并不亚于甚至可能超过单次批量数据出境,且累积效果难以通过单次审查加以评估。

远程访问型出境与后文模型输出型出境中的云服务部署路径,虽在技术实现上均借助API接口,但前者的访问对象是原始数据集或衍生数据集本身,是"对境内数据的直接访问",而后者获得的是模型输出的结果,而非原始数据集直接访问,是"对境外部署模型能力的间接调用"。

**(三)模型输出型出境**

模型输出型出境,指境内主体将训练完成的人工智能模型以技术产品的跨境部署与持续性服务调用等方式向境外提供,使模型及其内化的数据价值实现跨境转移的出境形态。大模型本质是海量训练数据经过学习、压缩、抽象后的价值凝结体;模型的跨境输出便是以这种凝结了数据价值的模型产品为载体实现价值跨境移交的过程,是数据出境从"显性资源交付"向"隐性技术内嵌"升级的典型形态。

当前中国人工智能模型产业已跻身全球第一梯队,模型出海正成为我国人工智能产业全球化布局的核心路径。截至2025年7月,中国已发布1 509个大模型,占全球总量超40%,位居全球第一[9]。全球排名前10的开源模型中,有8款来自中国[10]。中国高性能人工智能模型的数量和质量正不断提升,中外顶尖模型之间的性能已不相上下,约80%的美国初创企业使用中国基础模型进

行二次开发[11]。这标志着中国人工智能模型已获得全球市场的广泛认可。在海外市场对中国模型需求日益旺盛的背景下,模型输出型出境可以说是未来人工智能时代最具持续性与代表性的数据出境形态。

从产业实践来看,模型出海呈现出多元化的路径。一是硬件内嵌型输出。2025 年,中国首次成为工业机器人净出口国,工业机器人出口同比增长 48.7%[12],硬件产品的大规模出海为人工智能模型的出海提供了重要载体,工业机器人在境外部署时高度依赖人工智能模型提供感知、决策、控制与优化能力,构成模型算法等技术的同步输出。二是开源生态型输出,中国企业通过权重开放模式将模型参数向全球开发者释放,促进下游应用的二次开发与生态扩散。三是云服务部署型输出,中国人工智能企业将模型本体及推理环境部署在境外云服务商,直接面向海外用户提供服务。其中云服务部署型模式下,境外用户调用的是模型的服务能力,获取的是推理结果,而非直接访问训练数据集,这与远程访问型出境"持续访问境内数据"的特征形成明确区分。

基于产业实践,模型输出型出境的核心特征可归结为"技术产品形式下的隐性数据出境"。其一,模型权重内化了训练数据的敏感信息。大语言模型的权重文件是模型在训练过程中对海量数据学习、压缩、抽象后的产物,承载了经训练内化的信息。但隐性不等于安全。研究表明,通过模型逆向攻击、成员推理攻击等技术手段,并不排除从模型权重中恢复出原始训练数据中的敏感内容的可能性。其二,模型海外部署下数据出境活动具有持续性。境外部署大模型在向中国境内用户提供服务时,用户提问等个人信息将持续流入境外服务器,模型的运行日志、调用频率等技术数据可能被留存在境外云算力环境中。这意味着模型输出型出境并非一次性的技术转让,而是一个持续性的、多层次的跨境过程。

至此,三类新型出境形态的界分可作如下归结:在出境客体上,加工服务型为衍生数据成品,远程访问型为境内数据(集)及访问权限,模型输出型为模型本体及其内化的数据价值;在加工深度上,自远程访问型、加工服务型至模型输出型逐级递增;在交付方式上,加工服务型表现为一次性或周期性的成果交付,远程访问型表现为持续性、实时性的权限访问,模型输出型则表现为产品化部署后的持续性服务调用。由此形成的类型化框架,为后文分析现行规制体系在各维度上的适用困境提供了清晰的问题坐标。

## 二、人工智能新业态下我国数据出境治理体系的适用困境

中国已初步建立起了以《网络安全法》《个人信息保护法》《数据安全法》为基础,以《数据出境安全评估办法》《个人信息出境认证办法》《网络数据安全管理条例》《促进和规范数据跨境流动规定》为配套规则,涵盖数据出境安全评估、个人信息出境标准合同备案、个人信息保护认证三项机制协同运作的数据出境规制体系。该体系以"数据处理者或关键基础设施运营者向境外提供个人信息和重要数据的行为"为核心规制对象,其制度设计建立在主体明确、客体清晰、行为可辨的基础预设之上。然而,人工智能新业态中数据跨境流动新形式,在出境主体、客体类型与行为方式三个维度上均突破了现行制度的基础性预设,除加工服务型中数据完全来源于境外的来数加工属于法定豁免情形以外,其余新型数据出境场景能否为现行体系所涵摄、涵摄后能否实现有效规制,均存在显著疑问。以下从主体、客体、行为三个维度逐一展开分析并系统探讨治理困境产生的根源。

### (一)新型数据出境形态的规则适用审视

1. 出境主体:新型跨境主体与法定概念的错位

现行数据出境治理体系将"关键信息基础设施运营者""数据处理者""个人信息处理者"作为数据出境合规的义务主体。然而,人工智能新业态中数据出境主体打破了这一法律规制的预设。

就处理者的认定而言,《数据安全法》第三条仅就"数据处理"活动界定为"包括数据的收集、存储、使用、加工、传输、提供、公开等在内的行为类型"。《个人信息保护法》第七十三条进一步将"个人信息"领域的处理者界定为"在个人信息处理活动中自主决定处理目的、处理方式的组织、个人"。

《网络数据安全管理条例》第六十二条进一步将“网络数据处理者”界定为“在网络数据处理活动中自主决定处理目的和处理方式的个人、组织”。由此“自主决定处理目的与处理方式”成为了界定数据处理者身份的识别标准与前提。

在加工服务型出境中,数据完全来源于境外场景属于豁免情形,而数据来源于境内,境内受托企业完全依据境外委托方指令开展数据标注、清洗的场景下,因其缺乏对处理目的与方式的自主决定而不会被认定为数据处理者或个人信息处理者。在远程访问型出境中,境外主体获取数据访问权限自主访问与调取数据,该情形下境内数据控制者并未主动实施数据处理活动,其法律地位更接近“数据访问通道的提供者”而非传统意义上主动实施出境行为的“数据处理者”。在模型输出型出境中,模型权重内化的训练数据信息向境外转移,出境行为的直接实施者是模型提供方,但其身份更接近“技术出口方”而非传统意义上的“数据处理者”。主体的法律身份与法定概念之间的错位,使得现有合规义务的分配逻辑难以直接套用于人工智能跨境合作场景,出境主体的识别与义务界定面临制度空白。

2. 出境客体:衍生形态或模型内化下数据分级分类的适用困境

现行数据出境规制体系并非针对所有数据,而仅以“重要数据”和“个人信息”为规制客体。当数据经加工转化为衍生数据或内化于模型权重时,出境客体的法律属性已无法依据外观直接判断。

就重要数据的认定而言,其以“一旦遭到篡改、破坏、泄露或者非法获取、非法利用,可能直接危害国家安全、经济运行、社会稳定、公共健康和安全”为判断基准。但无论在实务界还是学术界,重要数据的范围至今尚未形成明确、统一的界定[13]。《数据安全法》第二十一条确立了数据分类分级保护制度,确立了重要数据的识别以数据所承载的信息内容类型为判断基准的静态逻辑。然而,在远程访问型场景中,跨境流动的并非单次、确定的数据集,而是境外主体对境内数据的持续性访问权限。单次访问所涉及的数据内容、数量与敏感程度难以在事前静态清点,长周期访问的累积效应更无法通过以数据集为单位的分类分级判断予以评估。当重要数据的识别以数据的内容属性为锚点时,远程访问型出境所形成的数据暴露风险,恰因无法被还原为某一确定的数据集而逸出了这一判断框架。在模型输出型出境场景中,出境客体已从原始数据转化为模型权重。模型权重是训练过程中对海量数据学习、压缩、抽象后的参数化产物,已脱离传统“数据”范畴而进入技术产品形态,其承载的信息内容无法通过直接审阅加以判断。但技术形态的转换并不消解数据安全实质风险。权重参数中凝结的训练数据信息可通过模型逆向攻击、成员推理攻击等技术手段被恢复,其中可能包含个人信息、商业秘密乃至涉密内容。现行以数据内容属性为锚点的分类分级制度,不仅难以回应远程访问中数据暴露风险的动态累积性,也无力穿透模型权重这一技术产品形态识别其内化信息的安全风险,容易形成“实质出境而形式脱管”的规制盲区。

就个人信息界定而言,《个人信息保护法》第四条将匿名化处理后的信息排除于个人信息范畴,第七十三条将匿名化界定为“个人信息经处理无法识别特定自然人且不能复原的过程”。这意味着数据是否构成个人信息,取决于加工后的可识别性判断。然而,匿名化处理在法律层面上缺乏明确、可操作性的定义[14],且处理后数据仍可能具备再识别风险[15]。当前我国相关制度与技术标准模糊、法律效果争议,去标识化与匿名化的界限难以清晰划定[16]。在远程访问型出境中,境外主体通过 API 等接口对境内数据进行持续访问,单次访问所涉个人信息数量可能远低于法定出境监管门槛,但长期累积足以达到乃至超过触发安全评估或标准合同备案的数量标准,而现行以累计数量为触发条件的监管机制无法在事前对持续性访问的个人信息暴露量进行有效估算与拦截。在模型输出型出境中同样无法排除重识别或训练数据反推的技术可能性。一旦被识别或反推,以服务或产品为载体出境的数据实质上仍构成个人信息出境,只是此种风险具有潜在性与滞后性,难以在出境节点作事前判断。反之,若将上述场景中所有存在理论重识别风险的数据均归入监管范围,又将

过度扩张规制边界,显著增加企业的合规成本。

上述分析表明,重要数据识别标准的内容属性锚定,使远程访问的累积性暴露与模型权重的内化信息无法被归类;个人信息匿名化标准的模糊,又使衍生数据的再识别风险与模型反推风险难以被排除,因此哪些情形确需纳入监管、哪些可以豁免将难以被有效界定。

3. 出境行为:隐蔽性跨境方式与行为定性的边界模糊

就行为要件而言,现行法上的“向境外提供”已有相对明确的规范界定。国家互联网信息办公室《数据出境安全评估申报指南》将数据出境行为界定为三类情形。一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外;二是数据存储于境内,但境外的机构、组织或者个人可以查询、调取、下载、导出;三是符合《个人信息保护法》第三条第二款情形,在境外处理境内自然人个人信息等其他数据处理活动。该界定已将“数据物理传输”扩展至“境外主体可访问、可调用”的行为类型,体现了从形式判断向实质判断的规范演进。

远程访问在行为定性层面与“向境外提供”并无实质差别,大体可为现行规范所涵摄。问题在于远程访问的持续性特征,其单次的访问行为可能并未触发安全评估条件且监管机关亦无法在事前对长周期访问的累积暴露规模作出估算。模型输出型出境则处于“向境外提供”的文义射程之外。训练数据信息内化于模型权重随技术产品出境,形式上虽不存在数据的传输或导出,但实质上构成数据外溢。当前立法虽在“物理出境”与“访问获取”之间虽已有所扩展,但对于“持续性低频访问的累积效应”“模型内化信息的隐性转移”等更深层的隐蔽出境方式仍缺乏有效的规制。

**(二)数据出境治理体系适用困境内含的治理错配**

前述主体、客体、行为三个维度的定性困境,看似是分立的适用难题,实则面临同一根源问题,即现行数据出境规制体系所依凭的规制范式,与人工智能时代数据价值的凝结方式之间发生了根本错配。

其一,治理理念层面的错配,安全逻辑单向主导难以适配多元利益平衡需要。现行治理体系的制度底色是安全治理逻辑,即以国家数据主权、关键领域安全、个人信息保护为价值基准。安全治理逻辑主导是必要的,面对无界的数字空间,必须筑牢安全治理底线。然而,随着数据要素市场化配置改革推进与国际经贸活动活跃,保障正常经贸往来不受不当阻碍的经贸促进逻辑与安全逻辑之间的张力日益凸显。

经贸促进逻辑植根于国际经贸法律体系,体现了贸易自由化、贸易便利化的价值取向与非歧视、必要限度等法律要求,即避免数据跨境流动限制措施对正常经贸活动过度限制。在多边层面,WTO《服务贸易总协定》(GATS)虽未专设数据跨境流动条款,但其跨境交付模式下有关的市场准入、国民待遇,以及最惠国待遇、一般例外等规定,共同构成审查相关数据限制措施的基础框架,其中在援引一般例外条款时限制措施须符合相关具体例外事项,其适用还不得构成任意或不合理的歧视,或者对服务贸易的变相限制;在区域层面,《全面与进步跨太平洋伙伴关系协定》(CPTPP)、《区域全面经济伙伴关系协定》(RCEP)、《数字经济伙伴关系协定》(DEPA)等协定基本形成了“原则 + 例外”的数据跨境流动规制规则,在确立数据跨境流动自由原则的同时,也承认缔约方可为实现“合法公共政策目标”采取或维持限制措施,但此类措施须符合各协定分别规定的例外条件,包括“不构成任意或不合理歧视或对贸易构成变相限制”“不超出实现目标所需限度的限制”等。我国作为 WTO 成员方与 RCEP 缔约国,且已正式申请加入 CPTPP 与 DEPA,促进数据跨境流动不仅是产业发展需要,也是履行我国已承担的相关国际条约义务、对接高标准国际经贸规则的要求。

2024 年出台的《促进和规范数据跨境流动规定》虽通过豁免机制与负面清单在一定程度上反映了对经贸促进逻辑与安全逻辑的“再平衡”,但安全逻辑的主导地位并未实质改变[17]。当规制对象是边界清晰的原始数据时,目标冲突尚可通过客体分类在技术层面予以调和;当规制对象变为形态动态、风险模糊的衍生数据与模型内化信息时,分类技术失效,理念层面的目标冲突便直接外

化为适用层面的定性困境。

其二,治理手段层面的错配,静态事前审查无法适配动态持续的出境形态。三项出境机制的运作模式均是以出境行为发生前作为审查时点,对客体风险作一次性判断,审查结论此后长期有效。这一结构以数据资源的静态跨境为基础,规制的度量衡是数据单元,即出境了什么数据、数量多少、敏感程度如何,均预设可在传输前静态清点、切分、定级。然而,新型出境形态的价值凝结于服务、权限与模型之中,无法在出境时点上被量化为明确且具体的数据单元;更根本的是,其价值跨境实现于过程而非时点。远程访问是实时、连续的行为流,风险依赖长周期的聚合效应;模型输出虽以产品交付为节点,但其承载的训练数据影子在模型全生命周期内持续暴露,且暴露程度随逆向攻击技术的演进而动态变化。以静态事前审查度量动态持续风险,度量衡既已失准,审查时点上的低风险结论便无法担保过程终点上的总体风险。规制手段与规制对象在客体形态与持续状态上的双重错位,导致事前静态审查对新型出境形态失灵。

其三,治理格局层面的错配,属地管辖原则无法提供完整规制闭环。现行体系以属地管辖为原则,规制效力通常以数据物理存储位置为边界,制度运作依赖监管机关对境内处理者的直接管辖,但新型出境形态的风险链条是跨境联动的,出境后则难以有效应对。远程访问中,访问权限来源于境外、数据存于境内,管辖权行使效果被弱化,境内监管失去抓手;模型出海后,境外部署环境、境外用户交互、域外穿透式监管共同构成风险链条的域外环节,均非单一地域内规制所能覆盖。与此同时,各国数据治理规则的差异与治理理念的分歧,又使我国企业在跨境场景中同时承受境内合规与域外规制的双重不确定。治理格局的属地单边性与风险链条的跨境联动性之间的落差,带来数据出境治理新难题。现行规则预设了一个完整的属地管辖场景,通过观察行为、核实客体、约束主体,定性结论才有落实的对象;而当行为链条的关键环节不限于域内,属地单边规制既无法观察风险全貌,也无法有效规制域外环节,更无法为跨境风险提供完整的规制闭环。

这三重错配共同表明以“安全逻辑单向锚定、静态事前审查、属地单边规制”为特征的治理范式,无法直接套用于“数据价值动态持续跨境”的人工智能新业态。

## 三、人工智能新业态下数据跨境流动规制中安全与发展的张力

在现行规则预设与新型业态形态错配的背景下,数据跨境流动规制面临一个基础性的两难:若以安全逻辑为主导,即通过扩张解释将新型出境形态全面纳入事前监管,看似补足了定性缺口,却会忽视人工智能产业发展;若以发展维度的经贸促进逻辑为主导,即通过限缩解释将新型出境形态排除于数据出境规制之外,交由市场自律或事后救济调整,看似释放了产业空间,却同样产生难以承受的安全风险。安全与发展之间的这一张力,不再是简单地“管”与“放”之间取舍的问题,而应该是使安全管控与产业促进在制度设计中协同并进。

### (一)安全维度:监管盲区下的三重风险敞口

1. 高质量数据外流风险

高质量数据集是人工智能应用升级的核心要素[18],在人工智能领域跨境经贸活动中正面临外流风险。

其一,在加工服务型出境中,如被加工数据系境内采集的情况下,境内采集的具身智能数据、自动驾驶路测数据等经标注、脱敏加工后形成衍生数据向境外提供,但加工深度不足或境外接收方通过多源衍生数据的关联聚合,仍可拼凑出反映我国特定领域态势的高价值图谱[19]。其二,在远程访问型出境中,境外主体通过 API 接口对境内数据实施持续性访问,数据价值外流风险将长期持续。其三,在模型输出型出境中训练数据信息内化于模型权重,其梯度参数与模型权重往往隐含境内个人信息与重要数据的“数据影子”,原始数据的敏感信息也可能通过模型反演等技术手段被还原出来,产生“隐性出境”[20]。已有研究表明,模型可能记忆并泄露训练数据中的个人身份信息、敏感商业信息或医疗记录,当训练语料中包含电话号码、地址、病历记录等敏感信息时,这种记忆会进一步加大模型的隐私泄露风险。此外,若模型通过机器学习即服务方式部署,或以开源

形式共享结构和参数权重,攻击者也可能借此探测甚至完整提取训练数据中的隐私信息[21]。

高质量数据持续隐性外流将对国家数据安全与产业长远竞争力构成持久威胁。一方面,直接侵蚀我国的数据要素禀赋优势,削弱人工智能产业赖以发展的核心资源底座;另一方面,伴随数据外溢的是算法迭代能力与技术创新优势的同步流失,使我国在全球人工智能产业竞争中逐步丧失先发优势。

2. 数字主权被剥夺风险

数字主权是指国家对数据和与数据相关的技术、设备、服务商等的管辖权及控制权,体现为域内的最高管辖权和对外的独立自主权、参与国际事务的合作权[22]。其涵盖数据收集、存储、处理、传输与销毁的全生命周期。其一,加工服务型出境中,衍生数据经加工外衣遮蔽后出境,国家对数据内容的识别与管控能力因形态转换而被削弱。其二,远程访问型出境中,我国管辖权因访问行为的隐蔽性而事实性弱化。境外主体绕开传统数据出境审查程序,通过持续性 API 调用实现对境内数据的事实性控制与利用,在这种模式下,尽管国家在形式上仍保有对数据存储设施的属地控制,但实质上对“谁在访问、访问了什么、累积了多少”缺乏充分的感知与干预能力。加之,境内监管机关因缺乏实时监控与跨境执法工具,难以对每一次访问行为实施有效管控,域内最高管辖权因技术架构的转换而被悄然架空。其三,模型输出型出境中,训练数据内化于模型权重,国家对信息资产的追踪与追溯能力因技术黑箱化而受限。但就侵蚀的强度与持续性而言,对数字主权的威胁更为突出。

3. 意识形态风险

前述两类出境形态的安全风险,均以数据本身为风险载体,其危害路径可追溯至特定信息内容的跨境转移。模型输出型出境还叠加了大模型内容生成能力与话语交互能力所衍生的政治安全、文化安全与网络安全维度的风险。

模型出海固然承载着传播中国价值理念、塑造国际话语权的战略意图,但这一战略意图可能被境外交互过程中的价值渗透所反噬,形成“输出—污染—回流”的反向传导效应。我国大模型面向全球多语言用户提供服务时,为境外势力实施意识形态“数据投毒”[23]提供了可乘之机。恶意用户可通过对抗性提示词系统性地诱导模型,使其在主权立场、历史认知、制度评价等核心议题上出现表述偏差甚至事实性错误[24]。与此同时,即便境外用户的日常交互行为看似中性,其反馈数据中内嵌的西方价值标准与话语偏好,经模型迭代训练后同样会被逐步吸收,使模型在生成逻辑层面不自觉地嵌入域外价值导向。当更新后的模型同步部署至国内服务场景时,这一价值偏移将以“中性技术”的外衣,潜移默化地影响国内用户的认知与判断,形成“境外驯化、境内渗透”的隐性侵蚀路径,给模型带来不可逆转的影响。长此以往,也将挤压我国在全球意识形态领域的主动权与影响力,削弱构建自主话语体系的能力根基[25]。

**(二)发展维度:安全治理导向下的三重产业困境**

1. 抑制我国国际数据服务贸易发展

服务贸易已成为全球经济和贸易增长的新引擎,国际数据服务贸易是中国参与全球人工智能产业竞争的重要战略抓手。《中国数字贸易发展报告 2025》显示,过去 10 年,中国数字交付服务出口规模从 2014 年的 790.0 亿美元增长至 2024 年的 2 205.7 亿美元,增长了 3 倍[26]。然而,若对数据出境监管过于严苛,上述优势将难以兑现为实际的贸易利益。在加工服务型出境场景下,境内采集、标注、加工后的衍生数据可能因触发数据出境安全评估等程序而难以及时跨境交付,使数据处理者不仅面临对境外客户的违约风险,还可能因交付能力受损而丧失市场信誉。境外客户也可能因顾虑我国严格的数据出境监管规则转而将数据加工订单转移至新加坡、印度等数据出境监管环境更为宽松的国家。那么中国凭借应用场景与加工能力构筑的国际数据服务竞争优势,会因制度障碍而被逐步消解,进而失去前景广阔的全球数据服务贸易市场。

2. 迫使技术与产业外流

部分企业为规避合规风险与消除境外客户的顾虑而选择将数据中心、训练集群、研发中心整体

部署至境外。虽会为区域人工智能产业协作提供了算力支撑与物理载体,但这种以规避监管为重要动因的产业外迁,最终将造成产业发展与安全可控的双重损失。

一则,核心资源外流削弱国内人工智能产业的集聚效应与创新动能。海外建厂意味着核心算力资产、研发试验资源与高端技术人才同步向境外转移,原本集中于国内的人工智能研发、数据处理产业链出现核心环节外迁,不仅会稀释国内人工智能产业的集群优势与规模效应,还会导致本土创新生态的技术迭代速度放缓,长期将弱化我国人工智能产业的内生增长动力与国际竞争优势。

二则,境外数字基础设施存在控制权旁落与产业链安全风险。部分东道国存在泛化国家安全概念的监管倾向[27],可能以国家安全、数据安全为由对我国企业的海外算力中心、数据设施实施查封、数据管控甚至变相征收,直接导致我国企业丧失对数据资产与基础设施的主导权,既造成海外生产运营停滞,也冲击我国人工智能产业链的整体稳定性,反而放大了数据安全与产业安全风险。

3. 压缩人工智能产业国际合作空间

数据是人工智能大模型训练、微调与场景落地的核心生产要素,其价值释放高度依赖跨域流动与多元聚合。人工智能国际合作的纵深推进,本质上是数据要素双向流动、技术能力优势互补的协同过程。若以泛化的安全理由对数据出境设置过高合规门槛、实施刚性限制,将直接切断中国与合作对象国之间联合研发、模型适配及场景落地的数据核心链路。一方面,跨国联合训练、协同技术攻关会因数据无法有序流通难以形成技术合力,制约双方在多语种大模型、行业人工智能解决方案等领域的协作深度,使既定的联合研发举措流于形式;另一方面,适配东盟本地场景的人工智能产品与服务会因缺乏区域数据支撑难以完成本地化迭代,迟滞我国人工智能技术标准、开发框架与产业生态的区域输出进程,导致我国人工智能技术与行业解决方案的海外落地进程受阻。

**(三)安全与发展并重逻辑的必然性**

数据跨境流动治理并非要在安全与发展之间做单选题,当规制只能在“从严”与“放宽”之间做线性选择时,无论选择哪一端,都会同时损害另一端。安全逻辑解决不了发展代价的担忧,发展逻辑解决不了安全风险的敞口,这一双向诘难指向一个更深层的结论,即安全与发展的张力并非源于目标本身的冲突,而源于实现目标的逻辑单一。由此,发展与安全并重的逻辑转向,不仅是困境纾解的可选方案,更是规制范式适配业态形态的必然要求。

并重逻辑的必然性,根植于人工智能新业态下安全与发展关系的质变。在传统数据出境场景中,数据作为静态资源被传输,安全与发展的关系表现为此消彼长的线性权衡——出境越多,风险越大,管控越严,流动越少。但在人工智能新业态下,高质量数据、先进模型、跨境协作能力,既是发展的核心资源,也是安全的核心屏障;数据主权、监管能力、国际规则话语权,既是安全的核心保障,也是发展的核心条件。安全不再是发展的成本,而是发展的前提;发展也不再是安全的威胁,而是安全的根基。并重逻辑不是“既要安全又要发展”的并列取舍,而是“以发展固安全、以安全护发展”的有机统一。

并重逻辑的必然性,还深植于国际经贸规则约束之中。“经贸促进逻辑”并非空洞的政策偏好,而是有具体规范基础与法理支撑的治理逻辑。一方面,安全例外在国际经贸法理中从来不是自足的单向逻辑,而是被必要性、非歧视、最小限制等要求约束的例外,安全与发展的并重并非我国立法者的权宜选择,而是国际经贸规则体系的内在要求;另一方面,我国已缔结 RCEP 并持续推进加入 CPTPP 与 DEPA 的谈判,这意味着安全与发展并重是我国扩大制度型开放、对接国际高标准经贸规则所必须内化的规范约束,若以安全逻辑单向扩张监管,将新型出境形态全面纳入事前审查,即可能构成对服务贸易开放承诺的变相限制,与国际经贸要求发生抵牾;反之,若一概放宽、放任新型出境形态逸出规制,又将瓦解数据主权与国家安全屏障。这意味着,将经贸促进逻辑纳入治理体系,实现安全与发展并重,是我国作为开放大国履行国际义务、对接国际规则的必然要求,而非可选项。

无论是全面从严还是一概放宽，都只是在错误的框架内做加减法。真正的出路只能是治理体系的范式转向，即理念上确立安全逻辑与经贸促进逻辑的协调并重，手段上以动态化、差异化的机制替代静态事前审查，格局上以国内治理与国际合作的协同突破属地规制局限。

## 四、发展与安全并重的数据跨境流动治理转向

实现发展与安全并重的数据跨境流动治理转向，并非安全与发展的简单折中或静态平衡，而是从“安全单向主导、静态事前审查、属地单边规制”向“安全与发展协同、动态分类规制、国内国际联动”新范式的演进。

### （一）治理理念：“数据安全逻辑”与“经贸促进逻辑”的协调

实现发展与安全并重的数据出境治理转向，其逻辑起点在于破解单一治理的桎梏，推动数据安全逻辑与经贸促进逻辑走向协同，为人工智能新型出境场景构建兼具风险防控能力与产业包容性的制度基础。这一转向并非在两种逻辑之间做简单的此消彼长，亦非以经贸促进逻辑替代安全逻辑，而是将二者的规范要求同时嵌入规则设计之中。

两种逻辑的协调可转化为“底线刚性 + 比例衡量”的两阶制度结构以化解二者张力。第一阶为安全底线的刚性划定。凡涉及重要数据、关键信息基础设施运营者数据以及达到规模门槛的敏感个人信息等触及国家安全与重大公共利益的事项，安全逻辑绝对优先，维持严格的事前审查与本地存储要求，在此领域内不与经贸利益进行权衡。这可与国际经贸规则中基本安全利益例外的安排相衔接，为我国保留必要的安全裁量空间。第二阶为底线以下的比例衡量。对未触及安全底线的场景，可将经贸促进逻辑的不超出必要限制等要求嵌入现有安全规制。一是在安全评估中增设“必要性测试”环节，审查监管措施是否为实现安全目标所必需、是否存在对产业影响更小的替代方案，避免施加超出规制目标所需的过度限制；二是在分类分级中体现产业差异，对贸易属性强、安全风险低的数据服务场景适用更宽松的规则，对安全敏感度高的领域维持严格管控。

这一协调逻辑的制度落点，在于依据前述新型出境形态的风险特征，对现行规则中的主体识别、客体分类与行为定性作出适配性调整，而非全盘重构。一是在出境主体识别上，应将受托加工方与自主决定处理目的的个人信息处理者加以区分，避免将不具备自主决定权的受托加工服务提供者与一般数据处理者等同视之，减轻服务贸易参与者的合规负担；二是在出境客体分类上，应根据加工深度与重识别风险区分衍生数据的风险等级，仅对存在实质性重识别可能性的衍生数据施加安全审查要求，避免对深度加工数据与原始数据适用同等监管强度；三是在出境行为定性上，应区分持续性高风险访问与偶发性低风险访问，对后者设置便利化通道，避免为防范持续性访问风险而对一切 API 调用行为实施无差别严控。通过上述调适，在坚守数据安全底线的同时，为正常的国际数据服务贸易与人工智能产业合作留出制度空间，实现安全逻辑与发展逻辑的协同并进。

### （二）治理手段：搭建“负面清单 + 事后追责”的动态规制机制

当前普遍实施的事前申报方式已难以适配人工智能业态发展，易对正常经贸活动形成制度性阻滞。对此，可考虑参照我国自贸试验区负面清单管理的实践经验，探索建立国内数据出境负面清单动态监管机制。该机制既对接《促进和规范数据跨境流动规定》第六条确立的自贸区负面清单试点方向，以负面清单划定安全管控的边界，清单之外以事后追责承接风险防控功能，又精准适配人工智能新型出境形态多元化、迭代快的特征。

需要强调的是，“负面清单 + 事后追责”并非对现行事前审查模式的替代，而是与既有三项出境机制嵌套衔接的双层结构。清单之内，继续适用数据出境安全评估、个人信息出境标准合同备案与个人信息保护认证等既有程序，审查标准、申报路径与执法措施依然适用，不发生制度断裂；清单之外，虽免予事前审查，但应转入“安全保护义务 + 持续监测 + 事后追责”。

其一，以清晰的规则边界替代个案裁量，提升出境便利化水平。该机制立足数据分类分级保护

制度,按行业、领域与数据敏感程度制定清单,明确禁止出境与限制出境的场景与客体范围,而清单之外的低风险领域免予事前审批,由市场主体自主开展跨境业务。以北京自贸区数据出境负面清单先行实践为例,该负面清单按汽车、医药、民航、零售与现代服务、人工智能训练数据、医疗器械、自动驾驶、贸易物流、银行业等行业进行分类,并针对各行业明确了“需要通过数据出境安全评估的数据清单”与“需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单”两类,为市场主体提供了清晰可预期的合规指引,大幅降低了合规成本与不确定性。

其二,明确负面清单动态调整的主导主体与程序安排,保障监管的持续有效性。在主导结构上,实行“国家统筹 + 行业参与 + 地方先行”的多层机制,先行提出清单条目增减的试点方案,经实践检验后再上升为一般规则。在程序安排上,建立定期评估与即时调整相结合的机制。以年度为周期,结合数据加工深度提升、重识别技术突破、模型逆向攻击门槛变化等技术因素以及清单运行的合规数据,对条目范围与管控强度作系统评估,及时将新出现的高风险出境形态纳入管控,将经实践验证风险可控的业态移出清单或降级管理;遇有重大技术突破或突发数据安全事件,启动即时调整程序。调整过程应经专家论证并公开征求意见,调整结果向社会公布并设置合理过渡期,保障市场主体的可预期性。

其三,以严格的事后追责体系为负面清单的放宽提供兜底支撑。事前便利化的正当性建立在事后追责有效性的基础之上。清单外数据出境免予事前审查,并不意味着安全义务的豁免,而是将风险管控的重心从事前审批转移至持续性监督与事后惩戒。首先,应明确清单外数据出境行为的数据处理者安全保护义务,即便免于事前审查,数据处理者仍须对出境数据的安全性承担主体责任,确保不存在以化整为零、加工遮蔽、模型内化等方式实质性规避清单管控的行为。其次,建立数据出境的持续性风险监测与事后审计机制,对远程持续性访问、衍生数据聚合等隐蔽性风险实施动态监控,一旦发现实质性安全危害,立即启动追溯性审查与执法程序。再次,完善行政处罚与刑事追责的衔接机制,对故意规避负面清单管控、造成重要数据泄露或危害国家安全的行为,课以严厉的行政处罚乃至刑事责任,形成有效威慑。

由此,“负面清单 + 事后追责”机制通过“清单之内严审、清单之外宽出但严责”的双层结构,实现了事前审查与事后追责的功能互补。其核心要义在于以规则确定性替代合规不确定性,以事后严厉追责替代事前普遍审查,在守住安全底线的前提下为低风险场景释放最大程度的产业空间。

**(三)治理格局:加强国际治理合作**

数据跨境流动治理困境在一定程度上源于各国数据治理规则的差异、治理理念的分歧、数据安全保护程度不一,单靠国内制度调适难以根本纾解。国际治理合作的核心目标在于,通过“区域先行、多边拓展、规则互认”的推进路径,由易到难逐步构建多层次国际治理合作网络,最终推动形成全球数字治理的规则共识。

其一,以中国—东盟人工智能合作为支点,推进区域数据跨境规则协调。中国与东盟在人工智能领域的合作已具备扎实的产业基础与制度储备,为数据跨境治理合作提供了理想的先行先试场景。应依托中国—东盟信息港、可信数据专区等既有平台,探索以下合作机制。一是建立负面清单互认安排,在清单外数据类别上实现跨境流动规则的对接与互认操作,降低合作项目的合规不确定性;二是推进跨境数据流动标准互认,在个人信息保护、数据安全评估等领域,就等效性认定达成双边或区域共识;三是探索联合监管沙盒机制,在可控范围内对远程协作研发、模型安全审计、加工服务监管等效性等问题展开测试性合作,积累共同治理经验。

其二,以数据安全风险管控为核心议题,构建多层次国际对话与协调机制。对于模型输出型出境中技术出口管制与数据出境监管的衔接问题、远程访问型出境中域外穿透式监管的应对问题,均非单一国家可独立解决。我国应在数字丝绸之路等多双边合作框架下,推动建立人工智能数据跨境治理的专项对话机制,就重要数据识别标准的协调与互认、政府访问企业数据的正当程序要

求、数据跨境流动限制措施的适用条件与程序等议题凝聚共识。通过规则层面的对话协调,降低我国人工智能企业面临的域外合规风险。

国际治理合作的要义,不在于追求全球统一的数据跨境规则,而在于通过区域试点的制度衔接、多边对话的规则协调、开放合作的战略定力,在安全与发展之间构建制度性缓冲带,为人工智能新业态的长期健康发展奠定规则基础。国内治理是国际合作的底气,国际合作是国内治理的延伸:通过国内负面清单制度的成熟实践形成可输出的治理经验;通过国际规则协调拓展国内制度的适用空间。二者相互支撑,共同推动治理格局从单边走向协同。

**参考文献:**


[1]新华社. 成立世界人工智能合作组织协定签署仪式在上海举行[EB/OL]. (2026-07-16)[2026-09-06]. https://www.news.cn/politics/leaders/20260716/8a9a63da84fb42779e9bd3357a7a38bd/c.html.

[2]新华社. 习近平出席 2026 世界人工智能大会暨人工智能全球治理高级别会议开幕式并发表主旨讲话[EB/OL]. (2026-07-17)[2026-09-06]. https://www.news.cn/politics/leaders/20260717/a40efe09846f418ca42ba096d7d6efd7/c.html.

[3]刘烈宏. 深化市场化配置改革释放数据要素价值[EB/OL]. (2026-06-23)[2026-06-24]. https://www.nda.gov.cn/sjj/jgsz/jld/llh/llhldhd/0623/20260623090203766355349_pc.html.

[4]胡泳,张文杰. 数据标注治理:可信人工智能的后台风险与治理转向[J]. 云南社会科学,2024(6):32.

[5]申卫星. 衍生数据的识别标准与产权配置[J]. 法学研究,2026,48(1):42.

[6]界面新闻. 字节跳动计划在马来西亚投资 21 亿美元建区域人工智能中心[EB/OL]. (2024-06-07)[2026-06-24]. https://www.jiemian.com/article/11267568.html.

[7]新华丝路. 科大讯飞携手马来西亚好享电视台共建东盟 AI 多语言译制中心[EB/OL]. (2025-11-09)[2026-06-24]. https://www.imsilkroad.com/news/p/800013.html.

[8]洪延青. 从传输到访问:跨境数据治理转向与中国应对[J]. 中国法律评论,2026(2):201.

[9]新华社. 我国大模型数量超 1500 个[EB/OL]. (2025-07-28)[2026-06-24]. https://www.gov.cn/yaowen/liebiao/202507/content_7034073.htm.

[10]求是杂志社经济编辑部、赛迪研究院联合课题组. 抢占智能时代制高点:我国人工智能产业发展调查[J]. 求是,2026(9):52.

[11]LUONG N. Two Loops: How China's Open AI Strategy Reinforces Its Industrial Dominance[R/OL]. (2026-03-23)[2026-06-24]. https://www.uscc.gov/research/two-loops-how-chinas-open-ai-strategy-reinforces-its-industrial-dominance.

[12]国家数据局. 数字中国发展报告(2025 年)[R]. 北京:国家数据局,2026.

[13]刘金瑞. 数据跨境双轨制下个人信息出境监管豁免制度的适用与完善[J]. 财经法学,2024(5):35.

[14]林北征. 个人信息匿名化概括式立法的困境与完善[J]. 行政法学研究,2024(6):34-35.

[15]夏庆锋. 个人信息匿名化制度的反思与改进[J]. 财经法学,2024(5):42.

[16]郭春镇,林泉君. 用户画像数据去识别化制度之反思与优化[J]. 浙江社会科学,2025(7):80-83.

[17]洪延青. 中国数据出境安全管理制度的"再平衡":基于国家间数据竞争战略的视角[J]. 中国法律评论,2024(3):204-209.

[18]中国信息通信研究院人工智能研究所. 人工智能高质量数据集建设指南[R/OL]. (2025-08-28)[2026-09-20]. https://www.caict.ac.cn/kxyj/qwfb/ztbg/202508/t20250828_691092.htm.

[19]李智,陈盈盈. 具身智能体数据隐私风险的合作治理[J]. 上海财经大学学报,2025,27(5):140.

[20]李贤森,李坤锦. 全生命周期视野下人工智能数据出境安全监管的具体场景、重点风险及体系构建[J]. 河北法学,2026,44(2):112-113.

[21]姜毅,杨勇,印佳丽,等. 大语言模型安全与隐私风险综述[J]. 计算机研究与发展,2025, 62(8):2000-2006.

[22]孙南翔,张晓君. 论数据主权:基于虚拟空间博弈与合作的考察[J]. 太平洋学报,2015,23(2):65.

[23]周瑞珏,赵精武. 立法还是释法:AI 数据投毒的治理纠偏[J]. 探索与争鸣,2026(5):78-87.

[24]亢升,兰曾妮. AI 时代美国对华认知战的手段及政治安全风险[J]. 统一战线学研究,2025,9(5):190.

[25]赵云泽,张琪赟. 中国智能传播自主知识体系构建研究[J]. 新媒体与社会,2026:1-17.

[26]中华人民共和国商务部. 中国数字贸易发展报告 2025[R/OL]. (2025-09-26)[2026-08-05]. https://fms.mofcom.gov.cn/xxfb/art/2025/art_3aeb2e47113845bdb16dcb053e5f6e9d.html.

[27]刘禹,莫漫漫,颜苏. 中国企业海外投资面临的国家安全审查风险与应对[J]. 中国软科学,2024(1):37.