引用格式：魏媛媛. 人工智能时代的数据安全与国际治理合作框架探究. 中国科学院院刊, 2025, 40(4): 663-671, doi: 10.16418/j.issn.1000-3045.20241208001.
Wei Y Y. Research on data security and international governance cooperation framework in era of artificial intelligence. Bulletin of Chinese Academy of Sciences, 2025, 40(4): 663-671, doi: 10.16418/j.issn.1000-3045.20241208001. (in Chinese)

人工智能时代的数据安全与国际治理合作框架探究

魏媛媛

香港中文大学（深圳）　前海国际事务研究院　深圳　518172

摘要　文章基于全球治理视角，探讨了数据安全治理的国际合作框架及其实施路径。首先，界定了数据安全与治理的概念，强调数据治理的核心目标是保障数据的安全流动与有效利用。其次，分析了全球数据治理体系的碎片化现状，揭示了其在地缘政治影响下的发展趋势与挑战，特别是在跨境数据流动等关键领域中的矛盾与协作。基于此，文章提出了“嵌入式数字命运共同体”理念，这一框架结合了“嵌入式自由主义”理论的国内政策自主性与“命运共同体”理念的全球协作愿景，旨在应对数字时代的全球治理挑战，推动全球数据治理合作。与此同时，进一步阐述了该理论框架的核心理念及其实践路径，并针对中国参与全球数据治理提出了具体政策建议。

关键词　人工智能，数据安全，数据治理，全球治理，国际合作，规则制定

DOI　10.16418/j.issn.1000-3045.20241208001
CSTR　32128.14.CASbulletin.20241208001

在人工智能（AI）和数字经济时代，数据成为关键生产要素，其安全与治理问题日益受到全球关注。数据安全不仅涉及个人隐私保护，更是国家信息安全和整体安全的关键组成部分。同时，数据治理已被提升至国家战略层面。中国、美国和欧洲提出的不同数据治理模式，受其战略利益、技术能力和监管框架的影响，这些差异导致了全球治理体系的碎片化。地缘政治竞争，尤其是中美竞争，进一步增加了建立统一的全球数据治理体系的复杂性和难度。数据治理的地缘政治属性，以及数据跨境流动的增加，迫切要求构建全球合作框架，以应对数据治理的全球性挑战。

1 数据安全与治理的理论内涵及核心要素

1.1 数据安全的概念界定

《中华人民共和国数据安全法》第三条将数据安

修改稿收到日期：2025年3月24日

全定义为“通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力”。学术界对数据安全的内涵进行了更详细的解读。方滨兴和殷丽华[1]将数据安全描述为在数据处理、存储、传输、显示等过程中的信息保护，确保信息的机密性、完整性、真实性和不可抵赖性等关键属性。张平文和邱泽奇[2]指出，数据安全是现代数字经济中信息、权属、价值、安全和交易5个关键要素的核心，它保障了数据交易和价值实现，从而决定了数据的价值和流通性。

在AI时代，数据已成为国家基础性战略资源，数据安全问题也提升至国家经济安全和战略安全的重要层面。例如，陈明奇等[3]指出，大数据在美国的多个关键战略领域中扮演着交汇点的角色，包括国家创新、安全、信息技术（ICT）产业和信息网络。他们提到美国已经制定了以大数据为核心的网络安全战略，旨在应对大数据技术挑战，并在未来增强其网络安全的战略优势。沈国麟[4]和杜雁芸[5]分别讨论了大数据作为国家战略资源，以及大数据的战略性。他们均强调中国应构建自己的国家数据战略，以确保数据安全与国家利益的紧密结合。

数据安全还关乎数据主权和国家主权。2018年发布的《大数据安全标准化白皮书》中强调，国家所掌握的数据规模及其运用能力正逐渐成为综合国力的关键组成部分，数据的占有权和控制权已上升为国家核心权力之一。

1.2 数据安全治理的内涵与外延

数据即权力[6]。数据已经成为全球贸易的核心，与权力紧密交织[6]。因此，数据治理的核心内容是权力的分配。对内，它是国家治理能力的重要指标；对外，它是国际话语权的衡量标准。2022年12月印发的《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》将数据基础制度的重要性提升至关乎国家发展和安全的战略高度，进一步强调了数据安全治理已成为国家治理体系和治理能力现代化的关键基础。

2024年5月发布的《数据安全治理白皮书6.0》明确指出，数据安全治理的目标是实现“数据的安全使用”。没有“使用”的安全将失去治理的意义。因此，数据安全治理的核心在于推动数据的安全有序流动，以实现发展与安全之间的动态平衡。这一目标在跨境数据治理领域尤为重要。

从内涵来看，数据安全治理涵盖数据主权、隐私保护、网络安全等多个维度，旨在通过规则制定和技术手段确保数据的安全流动和有效利用。从外延来看，数据安全治理不仅涉及国家安全和社会稳定，还与全球产业竞争和技术发展的深层联系。Goldsmith和Wu[7]指出，国家通过规则制定保护本国产业已成为普遍现象。规则和标准的制定本质上是产业竞争的延伸，而数据治理的重要性则源于数据已成为产业发展的核心资源。因此，不同国家的政策选择反映了其在全球数字经济中的战略意图和发展需求。例如，美国以“国家安全”和“数据安全”为由，对华为通信设备、TikTok、WeChat、DeepSeek等中国科技产品实施限制措施，其背后动机不仅限于安全考量，更包括遏制中国技术崛起和保护本国科技产业（如维护Google、Meta、OpenAI等科技企业的市场优势）的双重目标。

2 全球数据治理的现状、趋势与挑战

全球数据治理正面临着前所未有的挑战，这些挑战与AI的发展紧密相连。当前全球AI治理框架尚未建立，且呈现出阵营化、碎片化的趋势[8]。全球数据治理框架也深受其影响。

2.1 国际竞争加剧治理体系碎片化

蔡翠红[9]和任鹏飞[10]等学者指出，全球数据安全治理在规则制定上呈现出分散和碎片化特征，标准竞争日益激烈。世界主要国家和地区，如中国、美国和

欧洲，在数据治理方面展现出不同的主张和实践。

以数据跨境流动为例，美国推崇全球数据自由流动秩序，这反映了其互联网科技巨头（如Google、Meta）的利益诉求，以及其产业发展的需要。然而，随着中国科技企业（如华为、字节跳动、深度求索）在全球市场份额的不断扩大，美国对关键技术和敏感数据的出口实施了限制，以遏制中国AI产业的发展，保护本国产业。

欧盟通过严格的数据保护法规如《通用数据保护条例》（GDPR），以及《人工智能法案》（*Artificial Intelligence Act*）参与全球规则制定。一方面，体现了其通过规范性力量塑造全球治理的意图；另一方面，也是对其互联网及高科技企业相对滞后的一种补偿，旨在为本土企业提供发展机会。同时，欧盟在内部不断探索创新、发展与安全之间的平衡，其监管策略展现出灵活性。

中国通过推动数据本地化和跨境数据流动的规范化，探索兼顾数据安全和全球数据共享的平衡治理模式。这既保护了国家安全，又支持了数字经济的全球化发展，为数据治理贡献了中国方案。

各国和地区在数据主权和跨境流动上的立场差异，其背后的主要原因是国际竞争和各国的国家战略考量。这导致了全球数据治理规则缺乏统一性，进一步加剧了治理框架的碎片化。

2.2 技术标准和规则制定的地缘政治化

AI和数字时代，数字技术的标准与规则已经成为大国竞争的主要领域，数字标准地缘政治化的趋势越来越显著[11]。规则和标准是确保公平竞争和创新的关键，其不仅决定了技术的发展轨迹，还影响了国家之间的权力平衡。刘国柱[12]强调，“对任何国家而言，技术标准都属于具有战略意义的要素”。

以AI中的半导体芯片为例，美国利用其在半导体设计和制造领域的领先地位，制定了“外国直接产品规则”（FDPR）。这项规则允许美国政府对使用美国原产的工厂、设备、软件或技术生产的外国半导体产品施加管辖权。FDPR的实施体现了所谓的“相互依赖武器化”[13]，使美国能够控制全球半导体供应链，限制他国获取关键技术和知识，从而维持其在全球技术竞争中的领先地位，维护其霸权。这一规则的战略意图显而易见，它不仅限制了其他国家在高科技领域的发展，也凸显了技术标准在国际政治经济中的关键作用。

在此背景下，国际标准和规则被用作地缘政治工具，旨在增强或限制特定国家的影响力。技术理性虽在制定过程中扮演关键角色，但标准的制定与实施始终伴随着地缘政治的权力博弈，即标准和规则的政治性。Mattli和Büthe[14]观察到，国际标准已经从技术规范演变为经济和政治竞争的焦点。标准的制定不仅涉及技术协调，更是分配利益的过程，反映了国家间和企业间的经济竞争与权力分配[14]。

标准和规则的地缘政治化无疑加剧了全球治理的地缘政治化趋势。标准和规则的地缘政治可以定义为标准和规则如何影响国家间的关系、权力结构，以及全球政治经济格局。这一过程涉及国家如何利用标准和规则来增强自身的经济、军事和政治实力，以及这些实力如何改变国家间的合作与竞争。

以TikTok为例，美国政府对中国背景科技公司的担忧超越了技术层面的数据安全问题，更多地从地缘政治竞争的角度进行考量。杨楠[15]指出，即便TikTok在数据保护方面采取了充分措施，其中国背景仍是美国政府关注的焦点，这反映了在美立法中政治因素对技术问题考量的影响。

同样地，美国和欧洲在数据治理领域的冲突与合作也是国际数据政策互动中的一个典型案例。尽管美欧基于共同的意识形态、价值观，以及长期建立的军事和经济合作关系形成了安全共同体，并以西方阵营的身份在全球治理中扮演着重要角色，但双方在利益上亦存在分歧。

2000 年的《安全港协议》（*Safe Harbor Framework*）和 2016 年的《隐私盾协议》（*EU-U.S. Privacy Shield Framework*）均旨在规范美欧间的数据流动，但因监控问题和数据保护要求未能持续，最终被欧洲法院宣布无效。2022 年，双方发布《跨大西洋数据隐私框架联合声明》（*EU-U.S. Data Privacy Framework*），寻求新的法律基础以促进数据流动。美欧在跨境数据流动的合作与冲突中不断寻求平衡与妥协，部分原因是为了应对来自中国的数字经济挑战。美国和欧洲都面临着中国等国家的竞争压力，这种竞争不仅体现在经济和技术领域，也体现在数据治理的标准和规则制定上。基于政治利益的考量，美国在数据治理上对欧盟做出了妥协，反映了美国数据自由流动规则向欧盟严格数据保护规则的调整[16]。

美欧在数据治理领域的互动展现了跨境数据流动全球治理的复杂性。这一过程不仅体现了冲突与合作的反复交替，也表明在不对其国内规章制度进行重大调整的前提下，政策共识与国际合作的可能性[17]。

3 国际合作框架探究

各国（及地区）在数据安全治理上的政策差异反映了其独特的国家利益、价值观和战略目标。构建有效的国际合作框架需要依据国际关系和全球治理的理论及原则，这对于解决各国在 AI 和数据安全领域的分歧、推动共识的形成至关重要。

3.1 构建国际合作的理论框架

3.1.1 从“相互依赖”到“嵌入式自由主义”

Keohane 和 Nye[18]将相互依赖定义为需要有关各方付出代价的相互影响（costly effect）。这也意味着相互依赖不仅有能够抑制冲突的互利性，还有可能出现互损性。近年来，随着国际局势的日益紧张，以中美博弈升级，中美贸易战、科技战等为典型，国家间的经济相互依赖成为制裁和对抗的工具，出现了相互依赖武器化现象。孙成昊等[19]将国家利用他国的敏感性和脆弱性，通过切断或减少相互依赖关系来损害他国利益或施压以改变他国政策，从而实现自身政治和安全目标的行为，定义为“相互依赖的武器化”。

因此，AI 和数字经济时代，我们正处于更加复杂的相互依赖状态中，Keohane 和 Nye 所提出的“复合相互依赖”理论仍然具有一定的解释力，特别是在多维度的相互依赖、非对称性依赖、多渠道互动和非层次问题结构方面。然而，面对技术垄断、数据主权、网络安全和发展中国家边缘化等新挑战，我们需要批判性反思该理论的适用性。

在经济相互依赖的背景下，为解释如何在国际经济合作与国内政策之间找到平衡，Ruggie[20]提出了“嵌入式自由主义”（Embedded Liberalism）理念。该理念将自由经济原则与国内政策干预相结合，允许各国在参与全球经济的同时，可以采取保护主义或监管措施来减轻全球化的负面影响。Ruggie 的嵌入式自由主义概念提倡对全球化采取一种和解态度，既倡导自由市场，又认识到国内干预的必要性。

尽管自由贸易和资本流动有利于经济增长，但它们也可能导致社会动荡和不平等。数据流动亦是如此。数据的自由贸易和流动可以促进创新和经济增长，但同样可能威胁国家安全和社会平等。因此，基于“嵌入式自由主义”理念建立一种国际数据治理框架有其合理性和可行性。这意味着允许各国在追求跨境数据流动和交易的同时，能够采取保护主义或监管措施来减轻关键和敏感数据流动带来的不利影响。

3.1.2 “嵌入式自由主义”与“命运共同体”的有机结合

“嵌入式自由主义”理论框架在数据安全全球治理中具有一定的局限性。① 国家主权的局限性。数据主权的崛起使得各国对数据本地化措施的重视程度远超传统经济领域，这可能阻碍数据跨境流动，削弱全球协作。同时，嵌入式自由主义强调国家主权的保留，但在数据安全全球治理中，一定程度的主权让渡

（如参与国际数据流动协议）是必要的，这与嵌入式自由主义的核心理念存在张力。② 规则约束的不足。嵌入式自由主义允许各国根据国内需求灵活调整政策，但这种灵活性可能导致规则的碎片化，增加数据跨境流动的成本和风险。此外，各国可能滥用嵌入式自由主义中的例外条款，以数据安全为由实施保护主义措施，阻碍全球数据流动。③ 技术垄断与不平等。嵌入式自由主义未充分考虑技术垄断对全球治理的影响。在数据安全领域，少数国家（如美国、中国）在技术和标准制定上占据主导地位，加剧了全球不平等。同时，发展中国家在嵌入式自由主义框架下缺乏话语权，难以有效参与规则制定，进一步边缘化了其在全球数据治理中的角色。

而中国“命运共同体”理念强调全球协作与共同发展，更具有包容性和公平性。基于此，本文将“嵌入式自由主义”的国内政策干预与“数字命运共同体”[21]的全球协作理想结合，提出“嵌入式数字命运共同体”理念。

“嵌入式数字命运共同体”是指在数字时代，各国在尊重国家主权和国内政策自主性的前提下，通过全球协作应对共同挑战，实现数据安全、技术共享和经济共同发展的新型全球治理框架。该理论框架有2个核心理念：① 全球协作与国内自主的平衡；② 分层主权与灵活性规则，即在核心利益领域（如国家安全、文化认同）保留主权，而在全球公共问题（如数据治理、网络安全）上适度让渡主权，参与全球协作。

3.2 “嵌入式数字命运共同体”合作框架实践路径

（1）多层次治理机制。尽管全球性的AI和数据安全治理机制尚未建立，但多层面的国际合作已在实践中进行。因此，在缺乏正式国际机制的情况下，应继续推动多层面国际合作，确保全球数据治理的灵活性和适应性。具体来说，① 制定全球数据治理协议，建立跨境数据分级流动规则，允许各国根据自身的数据安全需求和发展水平，灵活地决定在何种程度上让渡主权，以实现数据流动的有序性和安全性。② 推动技术标准互认机制，促进国际数据隐私标准的互认，减少数据跨境流动的障碍。③ 建立国家、区域和全球层面的多层次治理机制，将不同层面的规则有机结合，形成协调一致的治理框架。

（2）技术共享与援助。各国利益的平衡是构建有效国际合作框架的关键。考虑到不同国家在AI发展阶段的差异，以及现有的“数字鸿沟”，数据治理的国际合作框架应具备灵活性，以适应各国的发展现状，目标应是弥合而非加大这一鸿沟。具体来说，① 建立全球技术共享平台，通过国际合作促进发展中国家获取关键技术，提升其数字基础设施和技术能力。② 推广开源大模型（如DeepSeek），为发展中国家提供低成本、高效率的AI技术支持。③ 遵循“选择性参与”与“共同但有区别的责任”原则。例如，在数据跨境流动规则中，允许发展中国家根据自身数字经济发展水平和监管能力，在保护数据主权的前提下，分阶段、分领域逐步开放数据跨境流动。

（3）信任机制建设。全球治理中的信任赤字是合作难以达成的重要原因之一。国际机制的形成通常是主导大国利益协调的结果，从而在很大程度上体现了这些国家的利益诉求。Keohane[22]指出，许多重要的国际机制都面临着“民主赤字”（democratic deficit）问题。冷战结束后，因美国的单极霸权战略，这种不公平性与信任赤字进一步加剧[23]。因此，各国应通过正式与非正式合作框架建立信任机制。具体来说，① 重视非正式政府间合作，因其在解决跨国问题（尤其是在地缘政治化的全球治理背景下）时，能够有效弥补正式合作因信任赤字而面临的困境。② 充分发挥跨国公司、非政府组织和国际组织等非国家行为体的作用，将其纳入国际治理机制，以增强信任机制的包容性和有效性。

4 DeepSeek实践案例及我国参与全球数据治理合作的政策建议

4.1 DeepSeek实践案例

DeepSeek是中国企业发布的一个开源大模型，其发布和推广可以被视为“嵌入式数字命运共同体”理念的一个实践案例。首先，DeepSeek的研发和发布体现了中国在AI领域的自主创新成果，它既降低了对国外技术的依赖，又有效保障了数据主权和技术安全。其次，作为开源模型，DeepSeek致力于全球技术分享，促进国际协作，帮助发展中国家获取先进技术，推动全球数字经济的发展。

DeepSeek案例体现了在尊重国家主权和国内政策自主性的前提下，通过全球技术分享与协作，实现共同发展与技术公平，为“嵌入式数字命运共同体”理念提供了生动的实践范例。

然而，美国正在对DeepSeek实施限制措施。其目的是维护美国在AI领域的技术垄断地位，遏制中国在AI技术领域的快速崛起[24]，并防止中国通过开源共享模式挑战其技术霸权[25]。再者，随着DeepSeek在全球市场的快速扩展，可能涉及多国用户数据交互，基于此，美国试图调整其跨境数据流动规则，以确保其本土企业在全球数字经济中的主导地位。

4.2 政策建议

（1）积极参与全球数据治理体系建设至关重要。当前，美国正积极推动以数据为核心战略资源的全球数据治理体系构建。在这一进程中，中国若能深度参与相关规则制定，将有力提升在这一关键领域的话语权，为全球数字治理贡献中国智慧与中国方案。《全球数据安全倡议》为我国融入全球数据治理提供了战略选择。然而，参与全球数据治理的基础是国内完善的数据治理体系；缺乏这一基础，国家在全球层面的规则制定和话语权竞争中将会面临显著挑战。

（2）完善国内数据治理体系是参与全球治理的基础。我国国内数据治理的关键在于平衡安全与流通需求，确保数据在有效保护的同时，能够自由流通并被充分利用，以支持企业与产业的可持续发展。但过度的治理和监管可能限制数据流通和开放，导致资源匮乏，进而阻碍企业和产业发展。因此，平衡治理—即建立既能保障数据安全又能促进数据价值释放的治理体系—是实现数据驱动型经济发展和维护国家安全的基础。

（3）构建包容务实的全球数据治理合作策略。在参与全球数据治理时，我国应避免使数据治理模式陷入意识形态争议。尽管网络主权和数据主权的概念对我国至关重要，但互联网的跨国性使得传统意义上的“主权”边界相对模糊。过度强调与美国自由治理模式的对立，可能被误解为意识形态对抗，而这并不符合我国推动全球数字合作的初衷。相反，应坚持人类数字命运共同体理念，发展既保障数据安全又促进数据流动与创新的数据治理策略。这将确保数据治理既能反映国家利益，又能为全球数据治理贡献中国智慧。通过这样的方式，我们可以在尊重各国差异的基础上，共同推动构建更加公正、平衡和有效的国际数据治理框架。

5 总结

“嵌入式数字命运共同体”理论框架旨在为AI时代的数据安全治理提供一种新的国际合作思路。该框架主张在尊重各国主权的基础上，通过灵活的规则设计和多边合作机制，推动全球数据安全治理的协调与共识。本文对该框架的实践路径进行了探讨，包括构建多层次治理机制，通过技术共享与援助平衡各国利益，以及建立信任机制等，同时充分考虑了发展中国家在全球数据治理中的角色与需求。未来的研究可以通过深入的实证分析和具体政策工具，进一步验证该理论框架的可行性，特别是阐释国家主权与全球规则之间的动态互动关系。通过理论与实践的结合，这一

框架有望为应对数字时代的全球治理挑战提供新的解决方案。

参考文献

1 方滨兴, 殷丽华. 关于信息安全定义的研究. 信息网络安全, 2008, 8(1): 8-10.
Fang B X, Yin L H. Research on the definition of information security. Information Network Security, 2008, 8 (1): 8-10. (in Chinese)

2 张平文, 邱泽奇. 数据要素五论: 信息、权属、价值、安全、交易. 北京: 北京大学出版社, 2022.
Zhang P W, Qiu Z Q. Five Theories of Data Elements: Information, Ownership, Value, Security, and Transaction. Beijing: Peking University Press, 2022. (in Chinese)

3 陈明奇, 姜禾, 张娟, 等. 大数据时代的美国信息网络安全新战略分析. 信息网络安全, 2012, 12(8): 32-35.
Chen M Q, Jiang H, Zhang J, et al. Analysis of the U. S. information network security strategy in the era of big data. Netinfo Security, 2012, 12(8): 32-35. (in Chinese)

4 沈国麟. 大数据时代的数据主权和国家数据战略. 南京社会科学, 2014, 28(6): 113-119.
Shen G L. Data sovereignty and national data strategy in the big data era. Nanjing Social Sciences, 2014, 28(6): 113-119. (in Chinese)

5 杜雁芸. 大数据时代国家数据主权问题研究. 国际观察, 2016, 30(3): 1-14.
Du Y Y. National data sovereignty in the big data era. International Review, 2016, 30(3): 1-14. (in Chinese)

6 Slaughter M J, McCormick D H. Data is power: Washington needs to craft new rules for the digital age. Foreign Affairs, 2021, 100(3): 54-62.

7 Goldsmith J, Wu T. Who Controls the Internet? Illusions of a Borderless World. New York: Oxford University Press, 2006.

8 魏媛媛. 生成式人工智能与全球网络安全——战略竞争视角下的风险与治理. 信息安全与通信保密, 2024, 22(8): 2-10.
Wei Y Y. Generative artificial intelligence and global cyber security—Risk and governance from the perspective of strategic competition. Information Security and Communications Privacy, 2024, 22(8): 2-10. (in Chinese)

9 蔡翠红. 全球数字治理的价值体系构建. 国家治理, 2025, 12(2): 33-40.
Cai C H. The construction of value systems in global digital governance. National Governance, 2025, 12(2): 33-40. (in Chinese)

10 任鹏飞. 全球数据安全治理面临的挑战与中国的治理方案. 社会主义研究, 2024, 46(5): 148-155.
Ren P F. Challenges of global data security governance and China's governance solutions. Socialist Studies, 2024, 46(5): 148-155. (in Chinese)

11 刘国柱. 数字标准的地缘政治论析——基于大国竞争的视角. 人民论坛·学术前沿, 2023, 12(4): 34-47.
Liu G Z. Geopolitical analysis of digital standards—From the perspective of great power competition. Frontier, 2023, 12 (4): 34-47. (in Chinese)

12 刘国柱. "数字威权主义"论与数字时代的大国竞争. 美国研究, 2022, 36(2): 35-57.
Liu G Z. "Digital authoritarianism" theory and great power competition in the digital age. American Studies, 2022, 36 (2): 35-57. (in Chinese)

13 米军, 陶欢, 兰迪. 相互依赖武器化、网络结构演化和网络性权力——以半导体和国际金融网络的案例分析. 当代亚太, 2023, 32(6): 30-60.
Mi J, Tao H, Lan D. Weaponized of interdependence, the evolution of network structure and network power: A case study of semiconductors and international financial networks. Journal of Contemporary Asia-Pacific Studies, 2023, 32(6): 30-60. (in Chinese)

14 Mattli W, Büthe T. Setting international standards: Technological rationality or primacy of power? World Politics, 2003, 56(1): 1-42.

15 杨楠. 美国遏制中国应用程序的策略及其影响. 当代美国评论, 2024, 8(3): 21-42.
Yang N. US strategies to contain Chinese applications and their impact. Contemporary American Review, 2024, 8(3): 21-42. (in Chinese)

16 张倩雯, 张文艺. 欧美跨境数据流动合作的演进历程、分歧溯源与未来展望. 情报杂志, 2023, 42(1): 88-94.
Zhang Q W, Zhang W Y. Evolution, divergence origins and future outlook of EU-U. S. cross-border data flows

cooperation. Journal of Intelligence, 2023, 42(1): 88-94. (in Chinese)

17 贾开. 跨境数据流动的全球治理:权力冲突与政策合作——以欧美数据跨境流动监管制度的演进为例. 汕头大学学报(人文社会科学版), 2017, 33(5): 57-64.
Jia K. Conflict and cooperation: Evolvement of trans-border data flows between US and EU. Journal of Shantou University (Humanities & Social Sciences Edition), 2017, 33 (5): 57-64. (in Chinese)

18 Keohane R O, Nye J S. Power and Interdependence: World Politics in Transition. Boston: Little, Brown and Company, 1977.

19 孙成昊, 王叶潸, 董一凡. 相互依赖武器化的机制探析——权力来源与政策实践. 欧洲研究, 2024, 42(2): 63-86.
Sun C H, Wang Y Q, Dong Y F. An exploration of the mechanism of weaponized interdependence: Sources of power and policy practices. Chinese Journal of European Studies, 2024, 42(2): 63-86. (in Chinese)

20 Ruggie J G. International regimes, transactions, and change: Embedded liberalism in the postwar economic order. International organization, 1982, 36(2): 379-415.

21 马丙合, 马方. 中国式现代化进程中的数据风险与安全治理. 重庆社会科学, 2024, 33(10): 103-114.
Ma B H, Ma F. Data risks and security governance in the process of China's modernization. Chongqing Social Sciences, 2024, 33(10): 103-114. (in Chinese)

22 Keohane R O. International institutions: Can interdependence work?. Foreign Policy, 1998, (110): 82-96.

23 门洪华. 国际机制与中国的战略选择. 中国社会科学, 2001, 3(2): 178-187.
Men H H. International mechanism and strategic choice for China. Social Sciences in China, 2001, 3(2): 178-187. (in Chinese)

24 鲁传颖. 从DeepSeek禁令看美国技术焦虑. 当代世界, 2025, (2): 76-77.
Lu C Y. Examining US technological anxiety through the DeepSeek ban. Contemporary World, 2025, (2): 76-77. (in Chinese)

25 王文, 申宇婧, 金臻. 大跳跃:美国智库论DeepSeek中国人工智能. 智库理论与实践, 2025, doi: 10.1413.n.20250306.1115.002.
Wang W, Shen Y J, Jin Z. A major breakthrough: U.S. think tanks on DeepSeek and China's artificial intelligence. Think Tank: Theory & Practice, 2025, doi: 10.1413.n.20250306.1115.002. (in Chinese)

Research on data security and international governance cooperation framework in era of artificial intelligence

WEI Yuanyuan

（The Institute for International Affairs, Qianhai, The Chinese University of Hong Kong, Shenzhen, Shenzhen 518172, China）

Abstract This study explores the international cooperation framework for data security governance and its implementation pathways from a global governance perspective. First, the study defines the concepts of data security and governance, emphasizing that the core objective of data governance is to ensure the secure flow and effective utilization of data. Second, it analyzes the current fragmentation of the global data governance system, revealing its development trends and challenges under the influence of geopolitics, particularly the tensions and collaborations in key areas such as cross-border data flows. Based on this analysis, the study proposes the concept of the "Embedded Digital Community of Shared Future", a framework that integrates the domestic policy autonomy emphasized by the theory of "Embedded Liberalism" with the global collaborative vision advocated by the "Community of Shared Future for Mankind". This framework aims to address the challenges of global governance in the digital age and promote international cooperation in data security governance. Furthermore, the study elaborates on the core principles and practical pathways of this theoretical framework and provides specific policy recommendations for China's participation in global data governance.

Keywords artificial intelligence, data security, data governance, global governance, international cooperation, rule-making

魏媛媛 香港中文大学(深圳)前海国际事务研究院助理研究员。主要研究领域:网络安全与治理、人工智能与国家安全,以及大国关系等。E-mail: weiyuanyuan.sdu@gmail.com

WEI Yuanyuan Ph.D., Assistant Researcher of The Institute for International Affairs, Qianhai, The Chinese University of Hong Kong, Shenzhen. Her research focuses on cybersecurity and governance, artificial intelligence and national security, relations between major powers, etc. E-mail: weiyuanyuan.sdu@gmail.com

■责任编辑：武一男