法学与社会治理学刊
2026 Vol. 1, No.1，ISSN 3154-746X

数据主权的“阵营化”困境：跨境数据流动的法律博弈与中国立场

刘华章

重庆工业职业技术大学

通讯作者*：刘华章　E-mail：liuhz@cqipu.edu.cn

论文信息

关键字
数据主权；跨境数据流动；阵营化；制度互操作性；中国立场

摘要

随着全球数字经济深入发展，跨境数据流动已成为国际贸易与数字治理的核心议题。然而，各国基于不同的价值取向与战略考量，围绕数据主权形成了欧盟、美国、中国三种相互竞争的治理模式，全球数据治理日益呈现“阵营化”格局。本文系统比较了欧盟以基本权利保护为核心的 GDPR 框架、美国以市场主导和长臂管辖为特征的 CLOUD Act 模式、以及中国以安全评估与本地化为支柱的数据出境管理制度，揭示了三大模式之间在价值理念、制度设计与权力结构上的根本分歧。在此基础上，本文分析了数据自由流动与主权控制之间的张力、美欧数据隐私框架的波折、以及国际经贸协定中的规则分化等阵营化冲突表现，进而阐明中国在安全与发展双重目标下的平衡策略与制度实践。文章最后提出，破解阵营化困境的关键在于推动制度互操作性、发展隐私增强技术等中立技术路径，并构建包容性的多边协调机制。中国应在维护数据主权的前提下，积极扮演“桥梁”角色，促进全球数据治理从对抗走向对话。

The "Camp" Dilemma of Data Sovereignty: Legal Games and China's Position in Cross-border Data Flows

ARTICLE INFO

Keywords
Data sovereignty
Cross-border data flow
Factionalization
Institutional interoperability
China's Position

Abstract

With the in-depth development of the global digital economy, cross-border data flow has become a core issue in international trade and digital governance. However, based on different value orientations and strategic considerations, countries have formed three competing governance models around data sovereignty: the European Union, the United States, and China. The global data governance is increasingly presenting a "camp" pattern. This article systematically compares the GDPR framework of the European Union with the protection of basic rights as the core, the CLOUD Act model of the United States

Citation：Liu, H. Z. (2026). 数据主权的“阵营化”困境：跨境数据流动的法律博弈与中国立场 [The “camp” dilemma of data sovereignty: Legal games and China’s position in cross-border data flows]. *法学与社会治理学刊, 1*(1), 34-42.

https://doi.org/10.64744/law.2026.197.

characterized by market dominance and long-arm jurisdiction, and the data export management system of China with security assessment and localization as the pillar, revealing the fundamental differences among the three models in terms of value concepts, institutional design and power structure. Based on this, this paper analyzes the tension between the free flow of data and sovereign control, the twists and turns in the data privacy framework of the United States and Europe, as well as the rule differentiation in international economic and trade agreements and other manifestations of bloc conflicts, and further clarifies China's balanced strategies and institutional practices under the dual goals of security and development. The article concludes by suggesting that the key to breaking the camp formation predicament lies in promoting institutional interoperability, developing privacy-enhancing technologies and other neutral technical paths, and establishing an inclusive multilateral coordination mechanism. China should, on the premise of safeguarding its data sovereignty, actively play the role of a "bridge" to promote the shift of global data governance from confrontation to dialogue.

一、引言

（一）全球数据跨境流动规则的“阵营化”趋势（2025—2026 年观察）

数字经济时代，数据已被视为“新的石油”，成为驱动全球经济增长的关键生产要素。然而，不同于传统货物贸易，数据的跨境流动天然与国家安全、个人隐私保护与数字贸易壁垒等多重复杂利益交织，各国政府出于对数据主权与国家安全的考量，纷纷建立以安全为名的数据壁垒。当前全球数据治理格局正发生根本性变化，主要经济体都在加速构筑以“数据主权”为核心的监管壁垒。

世界多极化格局下，各国在数据主权、本地化要求、跨境流动、隐私保护、安全审查等诸方面走上了迥异的数据法治道路，先发国家凭借其技术和经济优势试图主导国际数据规则的制定。跨境数据流动在实践中天然面临着一种难以调和的艰难困境，即难以在同一时空维度下完美兼顾数据自由流动、国家主权安全保障以及个人隐私权利保护。这种困境在 2025—2026 年进一步加剧：欧盟法院于 2025 年 9 月维持了欧盟—美国数据隐私框架（DPF）的充分性认定，但该框架的结构性脆弱性并未根本解决；美国方面，CLOUD Act 与 FISA 702 的持续争议、第 14117 号行政令对数据出口的限制，使美国的数据治理从自由流动向战略阻断转变；中国则持续完善数据出境安全管理制度体系，发布多轮政策问答，通过自贸区负面清单等机制探索便利化路径。全球数据治理的“阵营化”格局已经清晰形成。

（二）研究问题与意义

上述制度差异背后，究竟是价值分歧还是战略博弈？中国如何在“自由流动”与“主权控制”之间寻求平衡？这是本文试图回答的核心问题。文章通过制度比较与政策分析方法，系统梳理三种治理模式的内在逻辑与外在冲突，剖析阵营化格局的深层成因，并在此基础上评估中国现行制度的得失，探索破解困境的可能路径。这一研究对于理解全球数据治理的演变趋势、把握中国在国际规则博弈中的定位与策略，具有重要的理论价值与现实意义。

（三）研究方法与结构安排

本文采用比较法研究方法，对欧盟、美国、中国三大数据治理模式进行制度层面的系统比较，并结合政策文本分析与案例研究，考察阵营化格局下的张力表现。文章结构如下：第二部分比较三大模式的核心制度特征；第三部分分析阵营化的张力与冲突表现；第四部分阐明中国的立场与平衡策略；第五部分探索破解困境的路径；第六部分总结全文并提出展望。

二、全球数据主权的三大模式比较

（一）欧盟模式：以基本权利保护为核心的充分性认定与标准合同条款

欧盟将个人数据保护上升至基本人权的高度，《通用数据保护条例》（GDPR）构建了以“充分性认定”为核心、辅以标准合同条款（SCCs）等适当保障措施的跨境数据流动法律框架。根据 GDPR 第 45 条，若欧盟委员会认定某一第三国能确保“充分保护水平”，则数据可自由流向该国而无须额外保障措施。在缺乏充分性认定的情况下，数据控制者可依据 GDPR 第 46 条采用标准合同条款等适当保障工具进行数据转移。

SCCs 是欧盟委员会预先批准的标准化合同条款，也是 GDPR 下最广泛使用的国际数据转移法律机制。2020 年 Schrems II 案判决虽宣告 Privacy Shield 无效，但确认了 SCCs 在原理上的有效性，同时要求数据出口方逐案进行“转移影响评估”（TIA），审查接收国法律框架是否削弱 SCCs 提供的保护水平。2021 年 6 月，欧盟委员会通过了新版 SCCs，以模块化结构适配多种转移场景，并废止旧版。欧盟模式通过高标准的权利保护要求与具有域外效力的法律工具，将欧盟的数据保护标准向全球辐射，客观上构成了对其他治理模式的规制压力。

（二）美国模式：行业立法、市场主导与 CLOUD Act 的长臂管辖

美国的数据治理模式以市场主导、行业自律和事后问责为基本特征，强调低限制的数据自由流动。在立法层面，美国采取分散式的行业立法路径，如《加州消费者隐私法案》（CCPA）、《儿童在线隐私保护法》（COPPA）等，缺乏联邦层面的综合性隐私保护法律。

然而，美国模式最具争议性的是其“长臂管辖”特征。2018 年颁布的《澄清海外合法使用数据法》（CLOUD Act）是美国十多年来对《存储通信法》最重要的一次修订。该法明确，只要数据由受美国管辖的服务提供商控制，无论数据实际存储在何处，美国执法机关均可强制调取。CLOUD Act 还建立了双边行政协议框架，授权外国政府在与美国达成协议后直接向美国服务提供商调取数据——然而迄今为止仅与英国和澳大利亚达成协议，与欧盟和加拿大的谈判进展缓慢。此外，美国《外国情报监视法》第 702 条（FISA 702）允许政府对境外非美国人进行大规模信号情报收集，进一步强化了美国的数据获取能力。

美国模式在理念上主张数据自由流动，在实践中却通过长臂管辖构建了强大的数据获取网络。这种制度设计与其商业利益深度绑定，实质上是维护美国科技巨头在全球的数据霸权。

（三）中国模式：安全评估、本地化与数据出境安全管理制度

中国以《网络安全法》《数据安全法》《个人信息保护法》为顶层设计，构建了以数据分类分级为基础、以安全评估为核心的数据出境管理制度体系。国家互联网信息办公室先后出台实施《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》，并发布个人信息保护认证配套规则，明确了三种制度路径：安全评估、标准合同与保护认证。

《促进和规范数据跨境流动规定》于 2025 年 7 月正式施行，系统规范了数据出境的制度适用。其中值得注意的制度创新包括：其一，引入豁免机制，为跨境购物、跨境人力资源管理等场景提供免予评估的便利通道；其二，赋予自由贸易试验区负面清单制定权，负面清单外数据出境免予安全评估、标准合同和认证；其三，明确了重要数据的识别申报义务——未被公开认定为重要数据的，无需作为重要数据申报安全评估。在量化标准方面，自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息或 1 万人以上敏感个人信息的，须申报安全评估。评估结果有效期为 3 年，可申请延长 3 年。

中国模式以安全为优先价值取向，强调对数据主权与国家安全的保护，在制度设计上呈现出较强的政府主导特征和防范性思维。

三、阵营化的张力与冲突表现

（一）数据自由流动 vs. 数据主权控制：价值观的根本对立

三大模式之间的根本分歧首先体现在价值理念层面。数据跨境流动中“数据自由流动”与“数据主权控制”的对立，深刻影响了各国在国际规则制定中的立场选择。欧盟从基本权利保护出发，认为数据跨境流动不应以牺牲个人隐私为代价，主张通过高标准的法律约束实现有序流动；美国强调市场逻辑与商业自由，反对严格的本地化要求，主张数据跨境流动应当最小化政府干预；中国等新兴市场国家则更加重视数据主权，主张在优先保障国家安全的前提下进行有序流动。

这种价值分歧并非纯粹的意识形态差异，而是与各国的产业利益、技术能力与地缘战略深度嵌合。发达国家凭借技术和经济优势，试图通过输出自身的规则标准来主导全球数据治理格局，而发展中国家往往处于规则接受者的被动地位。美国对华“数据脱钩”现象日

益显著，美国通过立法、行政、司法三种层面的法律工具限制中美数据跨境流动，数据霸权呈现出泛安全化和美国优先的制度特征。

（二）长臂管辖与数据调取的对抗：美欧《数据隐私框架》的波折

美欧之间的数据转移安排集中体现了跨大西洋数据治理的张力。继 Safe Harbor（2015 年 Schrems Ⅰ案宣告无效）和 Privacy Shield（2020 年 Schrems Ⅱ案宣告无效）之后，欧盟委员会于 2023 年 7 月通过了针对 EU-US 数据隐私框架（DPF）的充分性认定，开启了第三次跨大西洋数据传输机制的尝试。

DPF 在制度设计上吸收了 Schrems Ⅱ的教训。美国于 2022 年 10 月颁布第 14086 号行政令，对美国信号情报活动施加了“必要性”和“比例性”要求，建立了数据保护审查法院（DPRC）提供独立救济机制。2025 年 9 月 3 日，欧盟普通法院在 Latombe v. Commission 案（T-553/23）中驳回挑战，确认 DPF 符合 GDPR 所要求的“基本同等”保护水平。然而，这一判决并未消除制度的根本脆弱性。欧盟法院将审查限于充分性决定通过时的事实与法律状况，拒绝处理 2023 年后的发展变化；Latombe 已向欧盟法院提起上诉（C-703/25 P），DPF 的前景仍存在不确定性。此外，欧洲议会 LIBE 委员会曾拒绝支持 DPF，认为其未能提供与欧盟同等的保护水平。2025 年初，美国隐私与公民自由监督委员会（PCLOB）因成员被解职陷入瘫痪——而该机构在 DPF 充分性认定中被引用了 31 次，进一步动摇了 DPF 的制度基础。

（三）国际数字贸易协定中的规则分歧：CPTPP、DEPA 与 RCEP 的不同取向

在国际经贸协定层面，数据跨境流动规则的分化同样显著。当前以 RCEP、CPTPP 和 DEPA 为代表的国际经贸协定虽已普遍确立“以数据自由流动为原则，兼顾合法公共政策和基本安全利益例外”的规范模式，但由于例外条款核心概念模糊，引发了缔约方国内规则的不确定性以及国际协定的适配压力。

研究表明，相较 RCEP，CPTPP 与 DEPA 针对数据跨境自由流动、跨境服务贸易、数字贸易便利化等条款的规定更为严苛。CPTPP 第 14.11 条明确要求各缔约方允许以商业业务为目的的数据跨境传输，同时承认各方的监管自主权。DEPA 在数字治理规则方面具有较高的创新性，水平领先大部分自由贸易协定。而 RCEP 在数据跨境流动治理方面自由化水平相对较低，为发展中经济体保留了更大的政策空间。CPTPP、DEPA、RCEP 以 WTO 为范本纳入安全例外条款，但未作出明确界定，导致适用上的模糊性。

中国目前已正式申请加入 DEPA 和 CPTPP，但协定中的跨境数据传输规定与中国现行模

式存在较大差异——数据出境安全评估制度的要求最为严厉，在加入谈判中面临重大挑战。如何协调国内安全需求与国际规则承诺，是中国在参与数字时代全球经济治理时亟需解决的关键问题。

四、中国的立场与平衡策略

（一）核心制度：《数据出境安全评估办法》与《促进和规范数据跨境流动规定》

中国已基本建立起以《数据出境安全评估办法》《个人信息出境标准合同办法》和《促进和规范数据跨境流动规定》为核心的数据出境法律体系。《促进和规范数据跨境流动规定》明确了三种出境机制之间的适用关系：重要数据和达到量化门槛的个人信息需通过安全评估；未达门槛的个人信息可选用标准合同或认证；符合豁免条件的数据出境活动免予三项程序。

2025 年国家网信办发布多轮政策问答，细化了制度执行中的具体问题。例如，关于第五条豁免场景中“等”字的解释，明确豁免情形不限于所列举项目，但须满足“为订立、履行个人作为一方当事人的合同”且“确需提供”的双重要件。对于跨境人力资源管理场景，明确身份证、护照、银行账户等是否属于“确需”范围，须根据必要性、目的明确和最小化原则进行具体判断。这些政策回应表明，中国在坚守安全底线的前提下，正通过渐进式制度细化为企业提供更可操作的合规指引。

（二）国家安全与经济发展的双重目标：安全底线下的便利化探索

中国数据出境管理制度设计的核心特征是安全与发展并重的双重目标导向。《促进和规范数据跨境流动规定》第一条明确指出，立法目的包括“保障数据安全，保护个人信息权益”与“促进数据依法有序自由流动”。这一表述反映了中国在阵营化格局中寻求平衡的努力方向。

值得注意的是，中国的便利化探索主要体现在三个层面：第一，豁免机制的引入大幅降低了低风险场景的合规成本。除跨境购物、汇款、机票酒店预订等常见场景外，累计向境外提供不满 10 万人个人信息（不含敏感信息）的数据处理者也可免予三项程序。第二，自贸试验区负面清单制度赋予地方试点空间，负面清单外数据出境免予安全评估、标准合同和认证。第三，政策问答机制为企业提供了及时的制度释明，有助于降低制度不确定性。

然而，中国模式面临的挑战也不容忽视：安全评估的门槛相对较高，制度执行中的行政裁量空间较大，可能影响企业出境的效率和可预期性。如何在维护数据主权的前提下进一步优化制度供给，仍是中国立法者与监管者持续面对的课题。

（三）初步实践：自贸区负面清单、个人信息出境标准合同

在制度落地层面，自贸区负面清单机制是一项重要的制度创新。自贸试验区可在国家数据分类分级保护制度框架下自行制定数据出境负面清单，经省级网信委批准、报国家网信部门备案后实施。这一机制赋予地方以政策试验空间，为探索更加灵活的数据出境规则提供了“压力测试”场域。

个人信息出境标准合同办法则为未达安全评估门槛的数据处理者提供了具有操作性的合规路径。数据处理者可根据标准合同模板与境外接收方签订具有法律约束力的合同，确保出境后的个人信息获得同等保护。标准合同机制在一定程度上借鉴了欧盟 SCCs 的制度设计思路，但在适用范围和法律效力上与后者存在差异。

五、破解阵营化困境的路径探索

（一）制度互操作性：推动标准对接、等效性认定与数据空间合作

破解阵营化困境的核心路径在于提升不同治理模式之间的制度互操作性。制度互操作性是不同法律体系在保持各自规范特征的同时，通过相互承认、标准对接和等效性认定，实现跨境数据有序流动的能力。欧盟 GDPR 中的充分性认定机制即是一种典型的等效性认定工具；中国可借鉴这一思路，在双边层面探索与主要贸易伙伴的等效性谈判。

数据空间合作是欧盟力推的另一重要制度工具。欧盟《数据法》于 2025 年 12 月发布了非约束性示范合同条款的草案，旨在促进数据共享和云服务切换，与 GDPR SCCs 形成互补。中国可在“一带一路”数字合作框架下，推动建立区域性数据跨境协调机制，在参与各方之间探索共同的合规标准与相互认可机制。

（二）技术路径：隐私增强技术（PETs）——联邦学习、差分隐私、多方安全计算

制度互操作性的推进需要技术手段的有力支撑。隐私增强技术（PETs）作为重要的技术治理工具，在破解阵营化困境中具有独特价值。PETs 使实体能够在不必暴露个人或专有信息的情况下，访问、共享和分析敏感数据。其主要应用方向包括联邦学习、差分隐私、多方安全计算和同态加密。

在跨境数据流动场景中，PETs 可有效降低制度层面的信任成本。基于联邦学习构建的混合保护模型在金融医疗领域实践中将隐私泄露风险降低 78%，同时保持数据可用性达 95%；差分隐私机制可使个体识别概率降至 0.01%，数据分析准确率维持 92%以上。然而，PETs 并非万能药——存在效用、效率与可用性的平衡挑战，需要政策层面的配套支持。OECD 建议从需求侧（监管沙盒、创新竞赛）和供给侧（研发支持）推动 PETs 应用，值得各国借鉴。

（三）机制构建：双边或多边数据跨境协调框架

机制构建是破解阵营化困境的第三重路径。当前全球数据治理碎片化严重，发达经济体与发展中经济体之间缺乏公平数据合作。中国的策略应当是内外兼修：内部构建科学完备的法律监管闭环，外部积极推动构建多元共治、包容普惠的国际规则体系。

在具体机制层面，可考虑以下方向：第一，在 RCEP 等区域框架内推动数据跨境流动规则的具体化，减少例外条款的模糊空间；第二，通过双边数据保护协议建立相互信任机制，降低合规成本；第三，在“一带一路”倡议框架下探索具有包容性的数字合作模式，为发展中经济体争取更大的规则话语权。中国倡导“数据命运共同体”理念，主张从东亚到“泛亚”发挥影响力，推动形成有序、合规、多元一体的全球数据治理体系。

六、结论

全球数据治理的“阵营化”困境根植于不同治理模式之间的价值分歧、制度差异与权力博弈。欧盟以基本权利保护为核心构建了高标准的数据保护壁垒，美国通过长臂管辖维持了强大的数据获取优势，中国则以安全为优先形成了政府主导型的治理格局。三大模式之间既存在价值理念的根本对立，又在跨境数据调取、贸易协定谈判等具体领域展开激烈的规则博弈。

然而，阵营化格局并非不可破解。本文研究表明，破解困境的可行路径包括：推动制度互操作性建设，通过等效性认定、标准对接和数据空间合作实现不同模式之间的协调；发展隐私增强技术等中立技术路径，以技术手段降低制度层面的信任成本；构建双边或多边数据跨境协调框架，推动包容性的规则制定进程。这些路径相互关联、互为支撑，共同构成从阵营化对抗走向协同治理的可能方案。

中国在这场全球博弈中面临着特殊的挑战与机遇。作为世界第二大经济体和最大的数字经济体之一，中国应当扮演“桥梁”角色：在坚持数据主权与安全底线的前提下，通过制度优化和技术创新提升制度的互操作性；积极参与国际规则制定，推动构建公平、包容的全球数据治理体系；通过自身实践为发展中经济体提供可借鉴的治理经验。唯有如此，中国才能在维护自身数据权益的同时，为破解全球数据治理的阵营化困境贡献积极力量。

参考文献

[1] 李智，刘思雨. 国际经贸协定数据跨境流动规则的传导性困境及因应[J]. 大连海事大学学报（社会科学版），2026(1)：60-71.
[2] 张福坤. 立足需求推动数据跨境流动法治化[N]. 检察日报（理论版），2026-01-25.
[3] 赵宏瑞. 世界多极化的数据治理与 WTO 合规审视[EB/OL]. 爱思想，2026-02-09.

[4] 霍俊先. 数据跨境流动安全例外条款的适用困境与中国对策[J]. 国际贸易, 2025(8).
[5] 彭圣, 罗福, 陈青梅. 跨境数据流动中的隐私保护技术与应用研究[J]. 中国科技投资, 2025(2): 49-51.
[6] 孔文豪, 陈玲. 重新理解跨境数据流动治理模式的驱动因素——基于跨国比较的组态分析[J/OL]. 电子政务.
[7] 申明浩, 姚凯辛, 沈晓娟. 数据自主权、数据保护与数据流动的不可能三角问题——以粤港澳大湾区跨境数据治理为例[J]. 南方经济, 2024(9): 45-56.
[8] 国家互联网信息办公室. 促进和规范数据跨境流动规定[EB/OL]. 司法部网站, 2025-07-02.
[9] 国家互联网信息办公室. 数据出境安全管理政策问答（2025 年 4 月；2025 年 10 月）[EB/OL]. 中国网信网, 2025.
[10] European Commission. Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Commission Implementing Decision (EU) 2021/914, 4 June 2021.
[11] Court of Justice of the European Union. Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (“Schrems II”), Judgment of 16 July 2020.
[12] General Court of the European Union. Case T-553/23, Philippe Latombe v. European Commission, Judgment of 3 September 2025.
[13] Daskal, J. Unpacking and Updating the CLOUD Act[EB/OL]. Lawfare Media, 2026-03-06.
[14] OECD. Sharing Trustworthy AI Models With Privacy-Enhancing Technologies[R]. OECD Publishing, 2025.