

TikTok 事件下中美数据主权博弈：特征、动因与对策

周雁琳¹ 王赛赛²

(1. 华东政法大学 上海 201620; 2. 西南政法大学 重庆 401120)

摘要：TikTok 事件深刻揭示了数字主权博弈的复杂性，反映出数字经济背景下权力结构的变化及国际技术竞争格局的重塑。美国通过泛化国家安全概念，以维护全球数据霸权为核心目标，对外扩张数据控制权，对内严密防御数据主权边界；中国通过技术创新和法律建设积极回应外部压力，维护自身数据主权与平台企业的全球发展空间。这场博弈不仅呈现“进攻”与“防守”的态势，也暴露全球数据治理面临的碎片化风险与制度对抗倾向。基于此，中国应在坚守数据主权的基础上，通过核心数字技术的自主创新增强规则塑造能力；以“依法自由流动”取代模糊的“数据安全”叙事，减少意识形态冲突；通过双边、多边和区域性合作积极参与国际规则制定；同时，以 TikTok 事件为契机探索与美国及其他有关方的数据主权对话机制，管控潜在冲突，为构建公平稳定的全球数据治理秩序提供可能路径。

关键词：TikTok；国家安全；数据主权；中美博弈；全球数据治理

中图分类号：D996

文献标识码：A

文章编号：1006-1894 (2026) 05-0086-10

TikTok 作为风靡全球的短视频平台，凭借其独特的算法推送机制和高度本地化运营策略迅速积累了庞大的全球用户群体，其跨境数据流动及数据处理问题也随之成为国际社会关注的焦点。自 2020 年特朗普政府首次以国家安全为由对 TikTok 实施限制以来，美国持续通过行政、立法和司法等多种手段推动对 TikTok 的监管。2024 年，美国国会通过《保护美国人免受外国对手控制应用法案》（Protecting Americans from Foreign Adversary Controlled Applications Act），要求字节跳动限期剥离 TikTok 在美业务。2025 年 1 月 17 日，美国联邦最高法院裁定该法案合宪，特朗普政府随后又通过行政命令暂缓执行相关禁令，为业务重组预留谈判空间。截至目前，TikTok 在美国的命运仍存在较大不确定性，中美双方围绕数据安全、算法控制和数字平台治理的博弈仍在持续。中国政府则认为，美方以国家安全为由持续打压中国数字平台企业，本质上是借安全议题维护其数字霸权和全球技术优势。由此，TikTok 事件已不再是纯粹商业纠纷，而是演变为中美围绕数据主权、数字规则制定权和国际数字秩序展开战略竞争的典型案例。

随着数字经济快速发展，数据已成为影响国家经济竞争力、科技创新能力和国家安全的重要战略资源。数据主权作为国家对本国数据资源享有控制权、管辖权和制度塑造权的重要体现，正成为国家主权在数字空间的重要延伸。同时，跨境数据流动又是数字贸易、全球产业链协同和人工智能发展的重要基础。如何协调国家安全、数据主权与数据自由流动之间的关系，已经成为全球数字治理面临的核心议题。TikTok 事件不仅折射出中美数字竞争的现实图景，也为观察全球数据治理规则演变和国家权力结构调整提供了重要样本。

作者简介：周雁琳，华东政法大学国际法学院博士研究生，研究方向：国际法；王赛赛，西南政法大学国际法学院法学博士，研究方向：国际法、数字法学。

基金项目：教育部重大攻关课题“我国海外利益保护体系构建研究”（项目编号：22JZD015）；重庆市教委科技项目“大变局背景下中国应对美国金融制裁机制研究”（项目编号：KJZD-K202400306）。

一、TikTok 事件下中美数据主权博弈的新特征

由 TikTok 事件可以看出,中美在大数据领域的资本竞逐早已超越单纯的商业博弈,演变为国家战略能力的深层较量。作为新兴战略资源,数据治理涉及主权、安全与经济发展三重利益的交织,日益成为大国博弈的重要议题。特别是美国在 TikTok 事件中对国家安全概念的持续泛化体现出数字经济时代国家安全评估与治理话语的变化趋势,有待从理论层面展开分析与厘清。

(一) 美国在 TikTok 事件中泛化国家安全概念

近年来,随着中美战略竞争不断深化(马其家和刘飞虎,2022),国家安全日趋成为美国调整对华数字科技政策的重要政策工具(池志培,2020)。TikTok 事件表明,美国国家安全概念不断扩展至数字平台、算法技术、跨境数据流动以及国际数字规则等领域,并将其嵌入数字技术治理体系。其本质是通过国家安全话语重塑数字治理规则,维护美国在全球数字经济中的主导地位,具体体现在以下 3 个方面。

第一,以国家安全为名泛化审查标准。美国对 TikTok 的限制最初源于其对跨境数据流动的担忧,并指控 TikTok 可能向中国政府提供美国用户数据。为此,TikTok 先后推出 Project Texas 计划,引入甲骨文公司负责美国用户数据托管和合规监管,^①并持续完善数据访问权限管理和数据透明度机制。然而,美国政府并未因上述整改措施而调整监管立场,而是在缺乏充分证据证明 TikTok 已构成现实国家安全威胁的情况下,持续强化行政、立法及司法限制。此外,美国将字节跳动与中国政府之间有限的股权关系作为推导 TikTok 可能受到政府控制的重要依据,并进一步将这种未经证实的可能性升级为国家安全风险(于跃,2024)。截至目前,美方始终未能提供 TikTok 在政治操控或非法传输数据的直接证据,却持续通过立法和政策强化相关风险叙事,将尚未发生的潜在风险视作现实威胁。这种“风险优先于证据”的治理逻辑背离了国际法上的“证据充分原则”,也违反了世界贸易组织开放、透明和非歧视性原则。该做法反映其国家安全审查标准日益泛化与模糊化,使国家安全逐渐由客观风险判断演变为服务战略竞争的政策工具。

第二,以网络安全风险为借口推行“预防性审查”模式。美国将 TikTok 的软件来源直接与网络安全风险相联系,认为中国开发的软件天然存在安全隐患,并据此实施持续性的安全审查。^②然而,这类判断更多建立在国家间战略竞争所形成的制度性不信任之上,而非公开、充分的技术审查证据。网络安全由此逐渐从传统的信息安全议题演变为数字竞争的重要治理工具,其监管逻辑也由“事后处置”转向“事前防范”,进一步扩大了国家安全的适用边界。

第三,将企业技术竞争上升至国家地缘政治层面。随着 TikTok 迅速成长为全球最具影响力的数字平台之一,美国逐渐将其由普通商业主体重新定位为具有战略属性的数字基础设施,认为其发展可能削弱美国在数字平台、算法规则和全球数据治理中的主导优势(刘洁和刘战伟,2025)。由此,企业竞争被赋予了国家竞争的战略意义,^③数字平台不仅承担商业功能,也被视为影响国际规则制定、数据资源配置和意识形态传播的重要载体。美国对 TikTok 的持续打压,本质上反映的是其维护数

① Musoni, M., Karkare, P., Teevan, C., et al. Global Approaches to Digital Sovereignty: Competing Definitions and Contrasting Policy [EB/OL]. 2023, ECDPM Discussion Paper No. 344. <https://ecdpm.org/work/global-approaches-digital-sovereignty-competing-definitions-and-contrasting-policy>. [2023-11-28] (2025-07-14).

② Lewis, J. A. TikTok and National Security [EB/OL]. 2024, Center for Strategic and International Studies. <https://www.csis.org/analysis/tiktok-and-national-security>. [2024-03-22] (2025-07-14).

③ How TikTok Became a US-China National Security Issue [EB/OL]. 2024, The Straits Times. <https://www.straitstimes.com/world/united-states/how-tiktok-became-a-us-china-national-security-issue-0>. [2024-03-09] (2025-07-14).

字技术霸权和国际规则主导权的战略诉求，而非单纯的数据安全考量。

（二）TikTok 事件下中美数据主权博弈的策略与手段

TikTok 事件使数据主权竞争由传统的数据安全议题进一步演变为围绕技术控制、制度竞争与国际规则塑造的综合博弈（冯硕，2021）。双方围绕数据控制权、算法治理权和规则制定权展开持续互动，形成了以法律、技术和制度竞争为核心的多层次博弈格局（程柏华等，2022）。相较于传统贸易摩擦，数字平台已成为国家战略能力的重要载体，中美数据主权竞争也由企业竞争演化为国家治理能力和制度优势的竞争。

美国在 TikTok 事件中的策略具有明显的法律化、制度化和联盟化特征。首先，美国不断强化国内法律工具在数字治理中的运用。从 2020 年行政命令到《保护美国人免受外国对手控制应用法案》的出台，美国逐步构建起行政、立法和司法相互配合的数据治理体系，通过国内法实现对跨境数据流动的域外规制，将国家安全审查机制制度化和常态化（Clausius，2022）。其次，美国持续强化国家安全审查机制，以外国投资委员会为核心，对 TikTok 涉及的数据存储、算法控制和跨境数据流动进行持续审查（Sitaraman，2022）。^①这种治理模式将技术治理与国家安全深度融合，实现了由企业并购审查向数字平台治理的制度延伸。最后，美国积极推动国际规则联盟建设，借助盟友体系协调数据安全、隐私保护及数字贸易规则，^②通过构建价值观联盟强化其国际规则塑造能力，进一步压缩中国数字平台的国际发展空间。

面对美国的强势施压，中国逐步形成了以制度建设、技术自主和多边合作为核心的应对策略。首先，中国不断完善数据安全法律体系。《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》）等法律相继实施，逐步建立起覆盖数据分类分级、安全评估和跨境流动管理的数据治理体系，为维护国家数据主权提供制度保障。其次，中国持续推进关键数字技术自主创新，加快算法、云计算、数据存储等关键基础设施建设，^③降低对外部技术体系的依赖，不断增强数据治理能力和数字产业竞争力。最后，中国更加注重通过国际合作参与全球数据治理，积极推动“全球数据安全倡议”和“共同安全”等理念（张毅，2023），并依托联合国、G20、金砖国家等多边平台推进数据治理合作。结合 2024 年世界贸易组织部分成员达成的《电子商务联合倡议》关于跨境数据流动与个人信息保护的最新实践，中国也更重视通过双边、多边和区域合作参与国际数字规则协调，努力提升在全球数据治理中的制度影响力。

可以说，中美数据主权博弈“分圈而治”的格局在 TikTok 事件的推动下进一步深化（Mitchell and Mishra，2021）。美国倾向于依托国内法、安全审查和联盟体系构建具有排他性的数字治理秩序，而中国则更加注重法治建设、技术创新和多边合作，通过制度供给和国际公共产品参与全球数据治理。双方不同的数据治理理念和战略选择，不仅加剧了国际数据治理规则的竞争，也推动全球数字秩序由相对统一逐渐走向规则多元并存的发展格局。^④

① Roumeliotis, G., Yang, Y., Alper, A., et al. Exclusive: U.S. Opens National Security Investigation into TikTok—Sources [EB/OL]. 2019, Reuters. <https://www.reuters.com/article/technology/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IJ/>. [2019-11-01] (2026-02-14).

② 白宫的声明进一步强调了美国与盟友在对抗共同威胁方面的多层次合作，包括技术和数据保护方面的协作。Fact Sheet: Joined by Allies and Partners, the United States Imposes Devastating Costs on Russia [EB/OL]. 2022, U.S. Embassy and Consulate in Ecuador. <https://ec.usembassy.gov/fact-sheet-joined-by-allies-and-partners-the-united-states-imposes-devastating-costs-on-russia/>. [2022-02-25] (2026-07-14).

③ 2024 年《工业和信息化部等七部门关于推动未来产业创新发展的实施意见》[EB/OL]. 2024, 中国政府网. https://www.gov.cn/zhengce/zhengceku/202401/content_6929021.htm. [2024-01-18] (2026-07-14).

④ Chin-Rothmann, C. T. TikTok: A Casualty of US-China Geopolitical and Economic Tensions [EB/OL]. 2023, Georgetown Journal of International Affairs. <https://gjia.georgetown.edu/2023/05/19/tiktok-a-casualty-of-us-china-geopolitical-and-economic-tensions/>. [2023-05-19] (2025-12-14).

二、TikTok 事件下中美数据主权博弈的逻辑动因

TikTok 事件并非单纯的数据安全争议，而是数字经济时代国际权力结构调整和全球数据治理规则重构的集中体现。中美围绕数据主权展开的竞争，既源于数字技术发展推动国家权力边界不断延伸，也反映出双方在国家安全、国际规则和全球治理主导权上的战略博弈。基于此，有必要从权力重构与规则重塑两个维度，进一步分析中美数据主权博弈形成的内在逻辑。

（一）权力重构：争夺数字技术主导权，维护国家安全利益

TikTok 事件表面上聚焦于数据传输合法性与透明度两大关键问题，实则是中美两国在数字技术主导权与全球战略地位方面的深层次竞争。在数字经济时代，数据、算法、数字平台等构成了新的国家间权力资源，TikTok 作为全球用户规模庞大、数据资源富集且技术模式先进的短视频平台，已成为中美博弈的关键场域和象征。^①

传统地缘政治理论主要围绕地理空间、资源控制和军事力量展开（Lee，2018）。长期以来，美国依托其全球军事同盟和制度优势实施“离岸平衡”战略（Layne，1996），以维持国际主导地位。然而，数字经济的发展推动国际竞争由地理空间逐渐向数字空间延伸，国家间权力竞争的核心也开始由传统资源控制转向数字基础设施、数据资源和平台生态的控制能力。数字平台不仅承担经济功能，更成为数据汇聚、信息传播和规则输出的重要载体，其控制能力直接关系国家在全球数字治理中的制度影响力（Gray，2021）。

长期以来，美国依托 Google、Meta、Apple 等数字平台建立起覆盖全球的数据网络和平台生态，在国际数字规则制定、数据流动以及平台治理等方面保持主导优势（赵海乐，2021）。然而，TikTok 凭借推荐算法、本地化运营以及全球化传播能力迅速成长为全球最具影响力的数字平台之一，打破了美国数字平台长期占据主导地位的市场格局，推动全球平台竞争由单极主导逐步走向多元竞争（Cartwright，2020）。从国际关系现实主义视角来看，大国竞争的本质在于权力分配的变化。当新兴国家在关键战略领域快速崛起时，守成大国通常会采取遏制措施以维护既有优势。此外，从全球治理体系的视角来看，TikTok 是新型企业模式的一种代表，亦逐渐成为塑造国际社会规范和意识形态影响力的重要工具（Tusikov，2019），进而动摇了美国在国际数字治理中的制度优势，使美国逐渐将 TikTok 视为影响国际数字权力结构变化的重要因素（Keane and Su，2019）。

一般认为，国际秩序的稳定取决于主导国家的实力与新兴国家崛起之间的权力平衡（阎学通和何颖，2019）。权力转移理论认为，国家间竞争的本质不仅在于数字资源占有的此消彼长，更关乎对国际数据治理规则制定权的争夺（Capar，2022）。美国在 TikTok 事件中综合运用立法、行政命令和安全审查等手段对 TikTok 施加各种压力，正是近年来国家间权力结构调整引发的典型战略反应（Nye，2019）。此外，这一博弈过程也契合国际秩序演变的一般规律。一般认为，主导国家会对新兴国家的制度突破或战略跃升采取遏制性策略，以此延缓或阻断权力结构的调整（朱锋，2020；Ikenberry，2008）。

数据作为数字经济时代最重要的战略资源之一，直接关系到国家安全的维护和经济竞争优势的实现（许可，2018）。TikTok 掌握的全球性用户数据和先进算法属于典型的战略性数字资产。^②不

① Su, C. The Risks of a Digital Cold War[EB/OL]. 2024, University of Sydney. <https://www.sydney.edu.au/news-opinion/news/2024/03/14/the-risks-of-a-digital-cold-war.html>. [2024-03-14] (2026-01-14).

② Thubron, R. Putin Says Country That Becomes AI Leader Will Rule the World[EB/OL]. 2017, TechSpot. <https://www.techspot.com/news/70850-putin-country-becomes-ai-leader-rule-world-elon.html>. [2017-09-05] (2026-07-14).

同于美国的策略，中国政府则通过法律制度建设与技术自主创新等举措，构筑自身在数据主权领域的战略防御体系。尤其是施行《数据安全法》和《个人信息保护法》等法律，强调国家对关键数据流动的可控性与合法性边界。此种法律与政策相结合的策略意在回应外部数据管控压力，更体现出中国高度重视维护平台企业“出海”后数据资产安全与国家利益。

（二）规则重塑：强化数字技术控制，重构国际竞争格局

在 TikTok 事件发生之前，美国长期奉行以数据自由流动为核心的“数字自由主义”治理理念，主张减少跨境数据流动限制，以巩固美国数字企业在全美数字基础设施、平台生态和技术标准中的主导地位。然而，随着中国数字技术实力不断提升，特别是 TikTok 等平台快速进入全球市场，美国开始重新调整其数字治理战略，由强调数据自由流动逐步转向强化国家安全、技术控制和产业保护，其政策重心由“开放竞争”转向“安全优先”，反映出数字竞争优势变化所引发的战略调整。

TikTok 事件标志着美国首次明确将信息内容平台纳入国家安全风险框架。此前美国技术封锁更多聚焦于 5G 设备、半导体、高端制造等传统“硬技术”领域。^①针对美国的围追堵截，中国企业持续提升自身技术创新能力和全球化影响力，以削弱美国对全球数字治理和技术的控制权（Erie and Streinz, 2021）。这迫使美国采取“数据民族主义”式政策逻辑，试图稳固其在全球数字生态中的主导权。

相较于腾讯、百度等传统的中国互联网平台的区域性运营，TikTok 借助人工智能驱动的推荐算法与全球化运营策略，成功塑造了突破性的信息传播机制。其“为你推荐”系统通过深度学习与个体行为建模，实现了高效的信息精准投送，深刻影响了用户的思维方式、社交行为乃至商业消费习惯（沈伟和靳思远，2022）。正因为如此，美国政府更加担忧 TikTok 带来的不仅是经济竞争，还有文化影响力与舆论导向权的结构性转移，进而威胁美国在全球数字空间的文化霸权与意识形态主导地位。从表面上看，TikTok 事件似乎是国家与非国家行为体之间的数据安全与合规之争，背后实质却是中美之间在全球网络话语权方面的竞争（沈伟和靳思远，2022）。TikTok 迅速超越美国传统社交平台，成为全球信息流通的新枢纽，这一事实让美国感受到数字时代掌控力流失所带来的威胁。

更为重要的是，TikTok 事件揭示出中美技术竞争已成为重塑国际竞争格局的重要力量。^②以 TikTok 为代表的中国数字技术平台迅速崛起，预示着全球可能逐步形成“以技术标准为准”的平行数字空间体系，即中美主导下的双重平台秩序与治理规范体系。^③美国正力图通过对 TikTok 等企业的严格限制，遏制中国数字技术的外溢能力，巩固自身在国际技术竞争中的主导地位。TikTok 事件作为中美技术竞争“软化转型”的分水岭，既映射出美国技术治理的战略演化，更揭示了全球数字权力重构进程中平台主权、文化影响与治理理念的三重博弈格局，标志着数字空间将步入制度分化加剧、系统性对抗升级的新阶段。

三、TikTok 事件下中美数据主权博弈的因应之策

数据主权博弈正逐步超出中美双边范畴，具有向全球更广泛区域蔓延的潜在风险。面对这样的

① Clark, R. TikTok Ban Breaks New Ground for US Tech Controls[EB/OL]. 2024, Light Reading. <https://www.lightreading.com/security/tiktok-ban-breaks-new-ground-for-us-tech-controls>. [2024-04-24] (2025-07-18).

② Is the TikTok Saga Linked to the US-China Tech Competition?[EB/OL]. 2023, Tradaily News. <https://www.trtdaily.com/magazine/is-the-tiktok-saga-linked-to-the-us-china-tech-competition-66183>. [2023-03-16] (2026-07-14).

③ Zhao, B. China's Rising Data Power and the Global Impacts[R]. https://www.researchgate.net/publication/363863793_CHINA'S_RISING_DATA_POWER_AND_THE_GLOBAL_IMPACTS. [2022-09-27] (2026-09-01).

局势，中国的应对策略不能仅围绕美国，还应兼具全局性和前瞻性，与相关各方搭建对话平台协商解决潜在冲突，力求形成公平公正的全球数据治理体系。

（一）提升数字技术控制权与数字治理权

TikTok 事件表明，数字平台的核心竞争力已不仅体现在市场规模，更取决于算法技术、数据处理能力和数字治理能力。TikTok 凭借算法推荐和内容分发技术实现全球化突破，说明数字技术创新已成为提升国家竞争力和维护数据主权的重要基础（王沛楠，2023）。基于此，中国亟须持续推进数字核心技术自主创新，重点加强人工智能、大数据、云计算等关键领域的研发投入，完善政产学研协同创新体系，提升数字平台的核心竞争力，实现由技术追赶向技术引领的转变。提升数字技术竞争力的同时，更应增强数字治理能力。近年来，欧盟依据《通用数据保护条例》（GDPR）持续加强对大型数字平台的数字监管，TikTok 亦因个人信息保护问题受到处罚，这表明数据合规已成为数字平台国际化发展的重要前提。中国企业在“走出去”过程中，应更加重视跨境数据流动、个人信息保护和数据安全风险管理，加强国际规则研究，完善企业数据合规体系，提高应对不同国家和地区数字监管制度的能力，降低因制度差异引发的数据治理风险。

更为重要的是，应不断提升中国参与国际数字治理规则制定的能力。随着全球数字治理进入规则重构阶段，跨境数据流动、个人信息保护和国家安全例外等议题仍缺乏统一规则。2024 年世界贸易组织框架下的“电子商务联合倡议”，首次就跨境数据流动、电子交易和个人信息保护形成较为系统的制度安排，为全球数字治理提供了新的实践基础。中国可积极借鉴有关规则设计，结合自身发展需求和广大发展中国家的共同关切，深度参与数字贸易和数据治理规则制定，推动形成更加公平、开放、包容的国际数字治理体系。与此同时，中国可以充分发挥《全球安全倡议》的引领作用，将“共同安全”理念融入全球数据治理实践，坚持相互尊重数据主权、平等协商和共同治理（程聪瑞，2025），反对以国家安全名义实施技术封锁和单边限制，推动构建多边参与、利益共享的数据治理机制。依托“数字丝绸之路”、共建“一带一路”倡议以及上海合作组织、金砖国家等合作平台，加强数字基础设施互联互通和数据治理合作，不断扩大中国数字规则和治理理念的国际影响力，为完善全球数字治理体系贡献中国方案。

（二）完善国际数据治理话语体系

TikTok 事件表明，美国正不断扩大国家安全概念在数据治理中的适用范围，将数字平台、跨境数据流动等经济活动纳入国家安全审查框架，呈现明显的“泛安全化”趋势。所谓“泛安全化”，即将本应属于市场竞争、数据治理或数字贸易的问题，上升为国家安全问题，并借助“国家安全例外”实施限制措施。虽然《全面与进步跨太平洋伙伴关系协定》（CPTPP）和《区域全面经济伙伴关系协定》（RCEP）及《数字经济伙伴关系协定》（DEPA）均保留了国家安全例外条款，但国际法普遍认为，其适用须严格满足必要性、比例性原则，仅限于应对现实、明确且紧迫的国家安全威胁（安佰生，2013）。美国在缺乏充分证据的情况下，将 TikTok 认定为重大国家安全威胁（丁泰夫和高飞，2024），不仅突破了国家安全例外的合理边界，也削弱了国际社会对跨境数据流动和数字合作的制度信任。可以说，国家安全泛化不仅加剧了中美数据主权冲突，也可能对全球数字治理产生外溢效应。一方面，国家安全逐渐成为数字贸易限制和技术竞争的重要工具，削弱了全球数字市场的开放性，增加了跨境数据流动的不确定性；另一方面，泛安全化趋势容易诱发其他国家效仿，推动数字治理由规则竞争演变为安全竞争，加剧全球数字治理体系碎片化，尤其不利于广大发展中国家参与数字经济合作。

为此，中国有必要强化“反泛安全化”国际叙事，坚持数据安全和数字发展的协调统一，倡导国家安全例外的规范适用，反对以国家安全名义实施单边主义和技术封锁。具体而言，中国首先应明确并阐释“国家安全例外”的适用边界与法律适用标准，同时推动国际社会就数字经济领域“国家安全威胁”的界定达成共识。中国可积极联合国际法学界、智库及相关国际组织，共同开展深度研究和国际交流，定期发布具有全球影响力的研究报告与政策建议，揭示泛安全化滥用所造成的经济损失、贸易扭曲和技术隔离等负面后果，强化国际社会对“国家安全例外”滥用风险的认识，并推动建立明确且具有约束力的安全标准的界定与适用框架，从源头上压缩泛安全化措施的实施空间。

在规则实践层面，中国应积极参与国际数据治理标准建设，加强跨境数据流动、个人信息保护和数据安全认证等领域的国际合作，推动形成透明、可操作的数据治理规则，减少因制度差异引发的数据主权争议。对于明显超出国际法合理边界的泛安全化措施，应充分运用世贸组织争端解决机制及其他国际法律渠道维护合法权益，同时加强与欧盟、东盟等重要伙伴在数字治理领域的规则协调，共同维护开放、包容、非歧视的国际数字治理秩序，防止全球数据治理进一步走向阵营化和碎片化。

此外，国际数据治理竞争不仅体现在规则制定和制度安排层面，也体现在治理话语和概念表达层面。近年来，中国已通过《数据安全法》《个人信息保护法》和《中华人民共和国网络安全法》（以下简称《网络安全法》）等一系列国内法律，初步建立了数据跨境流动的基本框架（王玫黎和陈雨，2022）。其中，《数据安全法》第11条强调“促进数据跨境安全、自由流动”，但目前中国对“数据安全”概念的理解与欧美国家存在一定差异：中国的政策更多强调国家安全导向，突出数据流动过程中的可控性与国家主权保护（刘金瑞，2021），而西方国家则多集中于数据安全的技术性指标，如完整性、保密性和可用性等技术标准层面。这种差异极易导致国际社会尤其是欧美国家对中国数据治理政策产生误读，也为个别国家将正常数据治理措施政治化提供了空间（刘金瑞，2022）。

围绕跨境数据流动，可强化“依法自由流动”的政策表达，在坚持维护国家安全和数据主权的基础之上，充分体现中国支持开放合作、依法治理和多边协调的基本立场，增强国际社会对中国数据治理理念的理解和认同。同时，应积极参与多边平台的数据治理规则讨论，加强与欧盟等主要数字经济体在个人信息保护、跨境数据流动等领域的规则对接，推动形成更加统一的数据治理共识。此外，中国还应强化跨文化沟通与国际法律人才培养，通过国际法专家和外交渠道，精准表达中国数据治理的真实意图与法律理念，避免因国际话语权弱势导致的不必要争议。可通过对国内外智库、大学与科研机构联合开展跨境数据流动法律和政策研究的大力扶持，培养相关人才，从而更有效地参与国际数据治理规则的制定，强化中国治理模式在国际社会上的接受度与认可度。

（三）深化国际数据治理合作机制

TikTok 事件暴露当前全球数据治理体系仍缺乏统一、稳定且具有普遍约束力的国际规则，各国围绕数据跨境流动、个人信息保护和国家安全之间的利益平衡仍存在明显分歧。美国一方面长期倡导数据自由流动，另一方面又以国家安全为由限制外国数字平台进入本国市场，在数据治理上体现出“双重标准”（杨永红，2022）。这种以单边主义和安全例外为基础的治理模式，不仅削弱了国际社会对全球数字治理规则的信任，也进一步加剧了国际数字治理体系的碎片化。

数据主权作为国家主权在数字空间的重要延伸，应建立在相互尊重各国发展道路、数据治理模式和合理安全关切的基础之上，通过平等协商协调数据跨境流动与国家安全之间的关系，反对滥用国家安全例外实施技术封锁和单边限制，推动形成兼顾发展和安全的国际数据治理共识。鉴于全球

统一规则难以在短期内形成，深化双边、多边和区域合作仍是推进国际数据治理制度建设的现实可行路径。具体而言，中国应从3个维度逐步推进国际数据治理协定的构建。其一，在双边层面，应优先选择与利益相近且治理理念兼容的国家，签署更为具体且具有约束力的数据治理协定，探索差异化对接路径（冉从敬和刘妍，2023）。例如，可基于中新（新加坡）数字经济伙伴关系、中阿（阿联酋）数字丝绸之路建设等双边机制，率先制定跨境数据流动与安全保护的示范性条款，形成可复制的制度模板，实现以点带面的规则影响力拓展（隗薪，2024）。其二，在多边层面，中国可借助“电子商务联合倡议”等国际平台，提出和推广符合自身利益又兼顾国际社会普遍关切的具体方案，尤其是在个人数据保护标准、数据跨境流动认证与数据本地化豁免标准等具体技术规则上，积极提出务实可行的解决方案，澄清国际社会对中国治理模式的误解。其三，从更宏观层面来说，TikTok事件及近期爱尔兰数据保护委员会对TikTok作出隐私保护罚款的事件，间接凸显出美国与欧盟在数据治理理念和规则制定上存在重大分歧，为中国推动多边和区域性治理合作提供战略性机遇。美国主张数据跨境自由流动，重视企业数据流动的商业便利性，而欧盟则更强调严格的个人数据保护与隐私监管，双方形成鲜明对比。基于此，中国可与其他国家在数据保护与治理领域展开深度的对话与合作，共同制定更为平衡且国际社会更易接受的数据治理标准。如此一来，便能在有效缓解数据治理风险的同时，获得多边治理的战略主动权和话语优势。

总体而言，国际数据治理合作不应建立在排他性和单边限制基础之上，而应坚持相互尊重数据主权、共同安全和开放合作原则，推动形成多边参与、利益共享、规则协调的国际数据治理体系。只有不断深化国际合作机制，才能有效降低类似TikTok事件引发的数据主权冲突，为全球数字经济健康发展提供更加稳定、公平和可预见的制度保障（鲁传颖，2023）。

（四）建立数据主权对话协调机制

对话与沟通是化解数据主权争议、避免战略误判的重要途径。TikTok事件凸显了中美在数据治理领域日益加剧的战略竞争态势。尽管该事件表面体现的是数据安全与企业合规层面的分歧，但实质上反映出两国在新兴技术主导和国际治理规则制定权方面的深层次博弈。然而，即便在当前竞争加剧的背景下，中美双方在保障全球数字经济稳定运行、促进跨境数据流动便利化、保护用户数据安全与隐私等领域仍存在共同利益和合作需求（冉从敬和黄文俊，2024）。据此，以TikTok事件为契机，探索建立稳定、透明、可预期的数据主权对话机制，不仅必要而且具有高度可行性。

从当前全球数据治理趋势来看，未来类似TikTok事件的数据主权争议也许不限于中美之间，有可能扩展至中国与欧盟或其他区域之间。基于此，中国的应对策略既应深化双边互动，同时亦要在多边和区域积极布局。具体而言，针对中美博弈的情势，中国应利用现有中美高层对话机制，如中美战略经济对话、中美经贸磋商机制和网络安全对话平台，增设数据主权和跨境数据治理为固定议题或专项议题。双方可围绕数据跨境流动的安全标准、数据保护与隐私合规要求、国家安全例外适用边界等敏感话题进行初步磋商。通过定期、常态化的沟通机制，形成明确的预警与危机管控机制，以减少战略误判或信息不对称引发的风险升级。同时，可探索设立专门的技术层面沟通渠道，邀请企业和技术专家参与对话，加强务实合作，提高双边数据治理规则的透明度和可预测性。中国还可通过发起全球数据治理高峰论坛、成立国际数据治理咨询委员会等举措，强化全球范围内的数据治理共识，提升国际社会对中国数据治理政策的认可与信任。

此外，在实际推进上述多层次对话机制建设过程中，中国可特别关注并利用全球数据治理中的共同利益交汇点作为切入点。比如，打击跨国网络犯罪、反恐合作、儿童与用户隐私保护、数据安

全技术标准制定等领域均为美欧及其他区域广泛认可的议题，以这些议题为抓手能够有效降低对话的敏感性和政治化程度，逐步拓展数据治理合作领域，通过务实合作建立信任，逐步实现从合作到规则共识的有效转化。

四、结语

TikTok 事件作为近年来全球最具代表性的数据主权争议之一，其影响早已超越个别企业合规问题，更多是国家间围绕数据安全、技术主导权与制度话语权的深层次博弈。美国以国家安全为由对 TikTok 实施严厉制裁，并强化数据管辖边界与联合盟友行动，旨在重塑其在数字空间的主导地位，同时遏制中国数字平台企业全球化所带来的技术扩散与治理挑战。这一系列举动实则表明美国在应对数字权力结构变动时的战略焦虑与制度防御心态。

中国在此过程中面临的已不仅是外部制度壁垒的构建，而且是对数字时代国家竞争形态转变的系统性挑战。通过对 TikTok 事件中美博弈策略的深入分析，可以看出当前数据主权竞争呈现三大特征：一是全面嵌入地缘政治逻辑，数字平台成为国家间战略竞争的前沿阵地；二是在权力结构演化驱动下竞相争夺以规则制定权与平台标准控制权为核心的治理主导权；三是技术管控、平台遏制与数据脱钩等领域转向以国家安全为名进行治理。鉴于此，中国亟须系统构建涵盖技术、叙事、制度与对话的全方位应对体系：技术层面着力推进平台算法、数据安全与跨境合规的自主研发，筑牢数据主权治理根基；叙事层面打造“依法自由流动”的国际话语框架，明确国家安全例外边界以平衡数据流动与安全关切；制度层面积极参与多边机制，构建多层次协调的数据治理协定网络；对话层面以 TikTok 为契机尝试与美国及其他相关方建立常态化的数据对话机制，明确彼此利益关切，通过规则协商与标准统一，管控潜在冲突，维护全球数字经济稳定发展的整体利益。同时，还应秉持“共同安全”理念，推动构建包容、均衡和公平的国际数据治理体系，塑造以合作为导向的数字规则治理秩序。

总之，TikTok 事件为观察中美战略竞争趋势提供了新窗口，亦是深入研究全球数据治理变迁的典型案列。中国可以此为为契机，把握数字治理规则的重要战略机遇期，通过制度、技术与外交三位一体的综合战略布局，稳步提升自身在全球数据治理体系中的主动性、代表性与制度性影响力，为构建更加公平、有效、可持续的国际数字秩序贡献中国智慧和方案。

参考文献：

- [1] 安佰生. WTO 安全例外条款分析 [J]. 国际贸易问题, 2013(3).
- [2] 程柏华, 龙坤, 秦中南. 美国政府封禁 TikTok 的策略探究 [J]. 情报杂志, 2022(8).
- [3] 程聪瑞. 共同安全与全球治理：概念、挑战与路径 [J]. 华中科技大学学报 (社会科学版), 2025(1).
- [4] 池志培. 美国对华科技遏制战略的实施与制约 [J]. 太平洋学报, 2020(6).
- [5] 丁泰夫, 高飞. “相互依存武器化”背景下的泛安全化解析——以美国对华科技竞争为例 [J]. 国际安全研究, 2024(1).
- [6] 冯硕. TikTok 被禁中的数据博弈与法律回应 [J]. 东方法学, 2021(1).
- [7] 隽薪. 数据主权规则博弈的中国进路 [J]. 中国社会科学院大学学报, 2024(6).
- [8] 刘洁, 刘战伟. 平台基础设施、数字主权与新地缘政治——一项基于抖音和 TikTok 的研究 [J]. 新闻与传播评论, 2025(2).
- [9] 刘金瑞. 迈向数据跨境流动的全球规制：基本关切与中国方案 [J]. 行政法学研究, 2022(4).
- [10] 刘金瑞. 数据安全范式革新及其立法展开 [J]. 环球法律评论, 2021(1).
- [11] 鲁传颖. 全球数字地缘政治的战略态势及其影响 [J]. 当代世界, 2023(5).
- [12] 马其家, 刘飞虎. 数据出境中的国家安全治理探讨 [J]. 理论探索, 2022(2).
- [13] 冉从敬, 黄文俊. 中美数据主权战略博弈：理论框架、关键环节与因应之策 [J]. 图书情报工作, 2024(4).
- [14] 冉从敬, 刘妍. 数据主权的国际博弈与我国进路 [J]. 图书馆论坛, 2023(9).

- [15] 沈伟, 靳思远. 网络空间博弈时代跨国科技企业面临的公私矛盾及应对——以抖音 (TikTok) 为例 [J]. 国外社会科学, 2022(5).
- [16] 王玫黎, 陈雨. 中国数据跨境流动规则与 CPTPP 的对接研究 [J]. 国际贸易, 2022(4).
- [17] 王沛楠. TikTok 听证会: 国际传播中的跨境数据与网缘政治 [J]. 青年记者, 2023(9).
- [18] 许可. 数据主权视野中的 CLOUD 法案 [J]. 中国信息安全, 2018(4).
- [19] 阎学通, 何颖. 国际关系分析 (第三版) [M]. 北京: 北京大学出版社, 2019.
- [20] 杨永红. 美国域外数据管辖权研究 [J]. 法商研究, 2022(2).
- [21] 于跃. TikTok 禁令行为的定性及应对措施的研究 [J]. 特区经济, 2024(3).
- [22] 张毅. 网络空间国际合作治理: 现实挑战与机制重构 [J]. 国家治理, 2023(23).
- [23] 赵海乐. TikTok 争议中的美欧数据治理路径差异研究 [J]. 情报杂志, 2021(5).
- [24] 朱锋. 国际秩序与中美战略竞争 [J]. 亚太安全与海洋研究, 2020(2).
- [25] Capar, G. Global Regulatory Competition on Digital Rights and Data Protection: A Novel and Contractive form of Eurocentrism [J]. Global Constitutionalism, 2022(11).
- [26] Cartwright, M. Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle [J]. Internet Policy Review, 2020(9).
- [27] Clausius, M. The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes [J]. Washington University Global Studies Review, 2022(21).
- [28] Erie, M. S., Streinz, T. Understanding China's Growing Influence in Global Data Governance [J]. USALI Perspectives, 2021(1).
- [29] Gray, J. E. The Geopolitics of "Platforms": The TikTok Challenge [J]. Internet Policy Review, 2021(10).
- [30] Ikenberry, G. J. The Rise of China and the Future of the West: Can the Liberal System Survive? [J]. Foreign Affairs, 2008(87).
- [31] Keane, M., Su, G. When Push Comes to Nudge: A Chinese Digital Civilisation in-the-making [J]. Media International Australia, 2019(173).
- [32] Layne, C. From Preponderance to Offshore Balancing: America's Future Grand Strategy [J]. International Security, 1996(22).
- [33] Lee, K.-F. AI Superpowers: China, Silicon Valley, and the New World Order [M]. Boston: Houghton Mifflin Harcourt, 2018.
- [34] Mitchell, A. D., Mishra, N. WTO Law and Cross-border Data Flows [M]. Burri, M., ed. Big Data and Global Trade Law. Cambridge: Cambridge University Press, 2021.
- [35] Nye, J. S. The Rise and Fall of American Hegemony from Wilson to Trump [J]. International Affairs, 2019(95).
- [36] Sitaraman, G. The Regulation of Foreign Platforms [J]. Stanford Law Review, 2022(74).
- [37] Tusikov, N. How US-made Rules Shape Internet Governance in China [J]. Internet Policy Review, 2019(8).

China-U.S. Data Sovereignty Struggle in the TikTok Incident: Characteristics, Motivations, and Countermeasures

ZHOU Yanlin WANG Saisai

Abstract: The TikTok incident has profoundly revealed the complexity of the digital sovereignty game, reflecting changes in the power structure and reshaping the pattern of international technological competition in the context of the digital economy. By generalizing the concept of national security and maintaining global data hegemony as its core goal, the United States expands its data control rights externally and closely defends its data sovereignty boundary internally, while China responds positively to external pressures through technological innovations and legal constructions to safeguard its own data sovereignty and the global development space of platform enterprises. This game not only shows the situation of "attack" and "defence", but also exposes the risk of fragmentation and the tendency of institutional confrontation faced by global data governance. Based on this, China should, on the basis of data sovereignty, enhance its rule-shaping capacity through independent innovation of core digital technologies; replace the vague narrative of "data security" with "free flow of data in accordance with the law," so as to reduce ideological conflicts; actively participate in international rule-making through bilateral, multilateral, and regional cooperation. At the same time, China needs to use the TikTok incident as an opportunity to explore a data sovereignty dialogue mechanism with the United States and other relevant parties to manage potential conflicts and provide a possible path for building a fair and stable global data governance order.

Keywords: TikTok; national security; data sovereignty; China-US game; global data governance

(责任编辑: 金孝柏)