基于身份认知的美国跨境数据流动战略

沈　逸　高　瑜*

【内容提要】　进入大数据时代，数据成了大国战略博弈的新焦点，跨境数据流动治理是核心议题，也成为美国对内治理和对外战略的重要抓手。尽管有一套既定的跨境数据流动标准和制度，但在具体实践过程中，美国更多遵循身份认知的逻辑进行跨境数据流动治理。对于中国这类被认定为“敌人”的国家，美国以安全化视角处理跨境数据流动问题，无视数据流动的客观规律，进行“你死我活”的数据争夺；对于日本这类被认定为“对手”的国家，美国允许在符合利益的基础上进行跨境数据流动合作，但会在既定框架内进行数据竞争以获取更多红利；对于欧盟这类被认定为“朋友”的共同体，美国积极深化数据合作，共享数据流动带来的利润，并主动限制国家行为以换取长久的合作机制。

【关键词】　美国　身份认知　跨境数据流动

* 沈逸，复旦大学国际关系与公共事务学院教授、复旦大学国家发展与智能治理综合实验室全球治理与发展研判研究室主任、复旦大学网络空间国际治理研究基地主任；高瑜，复旦大学国际关系与公共事务学院2020级博士研究生。

一、跨境数据流动战略与身份认知

数字时代，互联网已渗透到各国的经济、政治、社会、文化等方方面面，网络空间成为继陆地、海洋、天空、外太空之后人类活动的“第五空间”，同样被视作大国之间权力争夺的场域。[①]在 2009 年到 2018 年间，随着移动互联网的飞速发展，跨境数据流动为全球经济贡献了 10.1%的增长率。[②]由此，跨境数据流动成为国家发展战略中的重要内容。一方面，各国纷纷出台跨境数据流动的治理架构，不断完善本国的法律法规和制度设计。各国都希望在保护国家数据安全和公民个人隐私的基础上，在新的数字经济浪潮中获取数字红利，提升社会经济发展水平。另一方面，数据作为一种新的权力资源，逐步成为国家资产的重要组成部分。因此，国家在制定具体的数据战略时，必然引入政治博弈视角，根据数据流动对象国的身份认知采取不同的跨境数据流动策略。

（一）跨境数据流动战略

从广义上看，跨境数据流动的形式多样，借助光盘、移动硬盘和 U 盘等硬件设备将境外数据带回，或将本国数据带到别国，均属于跨境数据流动的范畴。但这些数据的总量较小，社会影响力有限，尚未构成国家治理和国际博弈的重点内容。从严格意义上看，跨境数据流动正式成为国际治理热点议题，是在移动互联网络出现之后。海量数据在网络空间中广泛流动，成为网络信息内容和服务的主要载体，渗透到社会生活的方方面面，并推动互联网行业创新发展。从本质上看，数据治理问题从属于网络空间治理问题的子分支，同时也离不开大国战略博弈的国际政治背景。在网络空间，数据是国家的基础性战略资源。其中，跨境数据流动治理是保障国家安全的时代急务[③]，也是国家数据战略的

① ［美］米尔顿·穆勒：《网络与国家：互联网治理的全球政治学》，周程、鲁锐等译，上海：上海交通大学出版社 2015 年版，第 3—4 页。

② 贾开：《数据跨境流动全球治理机制创新》，中国社会科学网，http://www.cssn.cn/zx/bwyc/201903/t20190327_4854253_1.shtml。

③ 支振锋：《贡献数据安全立法的中国方案》，载《信息安全与通信保密》2020 年第 8 期，第 2—8 页。

核心。

跨境数据流动战略作为国家战略的重要组成部分，与现实空间战略的逻辑和行为有相通之处，也有不同的新特点。相通之处是国家战略博弈的基本逻辑不变：无论网络空间还是现实世界，均遵循“无政府状态”的基本特征，不存在一个统一的超国家政府来承担权威角色。因此，无论是何种形式的大国博弈，都没有超脱现实主义的基本假设，国家行为的根本目标是维护本国的利益。因此，在大国数据战略博弈领域，一国数字利益的界定主导了该国数据治理的原则和目标。不同之处在于，非国家行为体在网络空间占据优势，要求国家必须平衡好各方行为体的数据利益诉求，否则容易引发治理矛盾。从技术属性角度看，互联网本质上是一种技术性产物，具有某些区别于物理空间的特征。最典型的表现就是技术专家在这一虚拟世界中占据天然的独特优势，互联网诞生之初的运作方式和使用规则都由研发技术专家制定的，成为第一代互联网规则的雏形。事实上，网络空间的许多资源被非国家行为体控制，各类行为体在标准制定、网络犯罪、往来战争、情报分析、个人隐私等不同的子议题领域发挥着不同的作用。新自由制度主义的代表约瑟夫·奈（Joseph S. Nye）将这种情况概括为网络空间的“复合机制理论”①。这就导致在数据治理的具体实践中，国家不仅要考虑对外的国际博弈战略部署，还要对内处理好不同治理主体的权力分配问题。

据此，国家对内跨境数据流动治理，由该国家的数据利益偏好和数据主体间的利益诉求决定，并最终通过国家跨境数据流动治理机构和相关法律法规表现出来。国家的数据利益偏好分为经济和安全两大类：一国若以经济利益为主要偏好，则倾向于主张数据以超越国界的形式尽可能自由流动，以此来挖掘数据的商业价值；一国若以安全为主要偏好，不论是个人隐私安全还是国家政治安全，都会倾向于对跨境数据流动设置相关规则，以保护本国公民和政府的数据安全。同时，跨境数据流动战略需要兼顾各类数据主体的利益诉求。对于社会而言，要求国家跨境数据流动治理规制保障个人隐私不受侵犯；对于私营部

① Joseph S. Nye，“The Regime Complex For Managing Global Cyber Activities，” USA Belfer Center for Science and International Affairs，John F. Kennedy School of Government，Harvard University，2014.

门而言，希望在保障商业机密的前提下尽可能促进数据自由流动，从中获取更多经济利润；对于政府而言，要在平衡上述诉求的基础上保护国家数据安全。概言之，一国在数据治理领域的利益偏好，结合国内不同治理主体扮演的角色，最终形成一国的跨境数据流动治理模式。

（二）角色认知与跨境数据流动战略

无论网络空间还是现实世界，均遵循“无政府状态”的基本特征，不存在一个统一的超国家的政府来承担权威角色。这也是各国在制定跨境数据流动战略时不可忽视的根本背景。换言之，跨境数据流动战略不仅需要考虑跨境数据流动的规律和要求，还要结合国际社会无政府状态对国家观念和行为的影响。

温特按照主体位置的不同，将无政府状态文化分为三类：第一类是以“敌人”为主体位置的霍布斯文化，行为体相互威胁，无限制地采取暴力行动。一旦把他者定义为“敌人”，就会以相互威胁的姿态面对对方，并对其采取摧毁或征服行动，由此进入“一切人反对一切人的战争”状态。[①]在“敌人”的角色认知下，国家先验性地判定对方怀有恶意企图。此时，若对方的实力加强，则会激化该国的安全焦虑，认为该国会对自己的生存造成威胁。在这种高度的零和博弈状态中，任何一点落后或被超越的风险都可能成为致命弱点，因此国家的战略重心在于寻求并维系相对优势地位。若技术水平相对较强，该国极大可能以先发制人的姿态发起第一次打击，以此寻求获得决定性的领先地位。[②]换言之，在这种殊死搏斗的状态中，实力的相对大小是决定生死存亡的关键，稍逊于人就可能招致灭顶之灾。因此，国家的首要任务是避免本国落到相对劣势的境地，为此会毫不犹豫地牺牲一些边际收益。

第二类是以“对手”为主体位置的洛克文化，行为体相互竞争，以暴力维护自身利益，但不会无限度地相互杀伐。与“敌人”的角色认知不同，对手之间认可彼此的主权和基本利益，并予以充分尊重。在追求自己的生存和发展过

① ［美］亚历山大·温特：《国际政治的社会理论》，秦亚青译，上海：上海人民出版社 2000 年版，第 334 页。

② James D. Fearon，“Rationalist Explanations for War，” *International Organization*，Vol.49，No.3，pp.379—414.

程中，也承认别国的生存与发展，基本逻辑是“生存并允许生存”。但与“朋友”也不同，“对手”之间存在竞争关系，在利益面临纠纷时会以各种方式争夺优势地位。但即便是发生暴力冲突，双方相互攻击的行为也会限定在既定的制度框架中，即“不会试图夺取对方的生命和自由”①。换言之，在洛克文化状态中，安全的“稀缺性”有所下降，国家面临的威胁减弱，不再像霍布斯文化一样为了确保当下的生存而时刻处于忧虑状态。因此，国家开始以发展的眼光看待世界，将资源更多投入自身发展的事业，同时不再执拗于短期内争夺相对收益，而是认识到绝对收益给长期带来的好处。但当陷入利益冲突时，国家仍会以竞争关系看待彼此，为自己争取更多好处，并着力提升国家实力。

第三类是以“朋友”为主体位置的康德文化，行为体相互帮助，不使用暴力并协力抗击安全威胁。在康德文化状态中，各国认定彼此的意图是和平友善的，因此不会采取暴力行动，并在面临第三方威胁时互相帮助。由此，国家间的行为逻辑由“自助原则”变为了“互助原则”，即“大家为一人，一人为大家”。②这种“朋友”关系的紧密和信任程度，远高于国际体系中存在的“盟友”关系。“朋友”的战略重心在于长久地维持友谊，国家力量会用来维护集体利益，因而一国的强大会被另一国视作共同财富；然而，结盟可以是对手或敌人在面临安全威胁下的权宜之计，这种合作关系随时可以终止，之后重新进入相互竞争甚至是相互敌对的关系。

在跨境数据流动领域，角色认知的逻辑影响到一些国家的战略制定，美国就是典型例子。第一，若将对方设定为“敌人”，则会以泛安全化的逻辑看待跨境数据流动治理问题，以维护国家安全为标准进行国内数据治理和对外数据博弈。然而，网络空间具有天然的全球属性，跨境数据流动更是网络技术和经济全球化发展到一定阶段的必然产物。若一国执意以霍布斯文化的逻辑处理这一问题，其行为必然违背跨境数据流动的发展规律，从而拖慢国内经济发展并挤压对外交往空间。对内，原本设计的数据治理框架将不发挥作用，国家间的商业数据和个人数据的法律法规让位于国家政府机构的行政指令。对外，国家一

① ［美］亚历山大·温特：《国际政治的社会理论》，秦亚青译，第 274 页。
② ［美］亚历山大·温特：《国际政治的社会理论》，秦亚青译，第 291 页。

味寻求相对优势地位以保障自身安全。不再重视数据合作带来的绝对的收益，取而代之的是“你死我活”的数据争夺之战。总之，基于“敌人”身份的认知导致对国家安全的过度焦虑，迫使国家脱离跨境数据流动的基本框架和规律，最终在国内和国际层面造成双重反噬。

第二，若将别国视为“对手”，则会在跨境数据流动治理的制度框架内进行数据竞争。在洛克文化状态中，网络空间治理议题不再具有“泛安全化”属性，各国遵循跨境数据流动本身的规律进行对内治理和对外竞争的活动。首先，尊重别国的数据主权成为共识，允许他国保护自己的数据安全。其次，随着数字经济的发展，各国开始追求数据红利，并允许别国同样获取商业利益。在此基础上，数据合作成为可能。最后，“对手”之间仍会进行数据博弈，在数据合作中尽可能为自己争取更多数据红利，占据优势地位。尽管数据竞争和博弈仍然存在，但其行为限定在各国既定的跨境数据流动制度中。

第三，若将别国视为“朋友”，则国家间开展并深化数据合作的可能性较大。按照康德文化的互助原则，彼此认定为“朋友”的国家，会帮助对方尽可能获取数据红利，自己也将从中获得更多发展机会。然而，跨境数据流动进入治理视野的时间较晚，目前各国的治理水平不一而足，全球合作治理机构更加匮乏。因此，在数据业务运营的具体实践中，难免出现定义不明、标准不一、规则不清等情况。面对类似的数据纠纷，“朋友”身份的国家会采取不同于“对手”竞争的处理方式：“朋友”会以积极方式解决争端，在不断的沟通交流中探索一种满足双方数据利益诉求的新机制，以此保障双方的跨境数据流动能够在安全、互利的基础上持续合作。

此外，值得注意的是，个体国家眼中对别国的“角色认定”具有较大程度的主观性，并不是某个国家本身的特征。首先，“角色是结构特征”，对他国角色的判定在很大程度上由行为体在结构中所处的位置所决定的。其次，对别国的角色判定完全基于主观臆断。在冷战时期，无论角色认知的真实性如何，美苏最后都不会影响到由此构建出的文化结构特征。即“无论是真实还是虚构，如果行为体认为敌人是真实的，那么，从结果方面来看，敌人就是真实的”①。

① ［美］亚历山大·温特：《国际政治的社会理论》，秦亚青译，第243页。

表 1　角色认知对跨境数据流动战略的影响

角色认知	敌人	对手	朋友
文化状态	霍布斯文化	洛克文化	康德文化
战略逻辑	一切人反对一切人	生存并允许生存	大家为一人，一人为大家
战略目标	追求相对收益，避免处于劣势	追求绝对收益，避免相对损失	长久维持友谊，保护共同利益
行动姿态	相互威胁	相互竞争	相互帮助
跨境数据流动战略逻辑	数据问题被泛安全化	尊重数据流动规律	深化数据合作，推动制度良性变革
跨境数据流动战略目标	维护本国绝对安全和数据相对优势	掌握更多数据红利	共同享受数据红利
跨境数据流动政策倾向	“你死我活”的数据争夺	在制度框架内进行数据竞争	积极解决纷争，主动自我限制

鉴于跨境数据流动属于治理领域的新兴议题，产生和发展的时间较短，因此，无论在哪种角色认知结构中，各国的“内化等级”都不高，没有形成“共同知识”，甚至连具体定义都没有国际统一的定论。因此，在跨境数据领域，对别国的角色认知在很大程度上仍处于该国的“自有知识”范畴。

二、美国跨境数据流动治理的制度设计框架

在跨境数据流动治理领域，美国采取商业利益优先的偏好，以互联网企业的数据红利作为政策出发点，保障业务遍布世界各地的美国互联网龙头企业能够持续不断地从自由流动的全球数据中获益。在治理主体方面，国家政府与大型互联网企业进行各种形式的合作，要求私营企业通过或明或暗的方式向美国政府提供其服务器上来自全球各国的用户数据。在此基础上，美国充分利用企业的数据抓取能力和政府的数据分析能力，对全球各国的数据进行直接或间接的监管，旨在形成一套以美国为中心的跨境数据流动体系。

（一）美国数据利益偏好

美国数据战略以商业利益为主要偏好，向来主张以“自由流动”为原则治理跨境数据流动。美国是互联网的诞生地，其经济科技实力也处于世界领先地位，谷歌、微软、脸书、推特、苹果、亚马逊等大型跨国公司已经基本覆盖到全球的数据流动。对于这些美国企业而言，在全球范围获取尽可能多的数据是现代跨国企业（特别是互联网企业）获利的重要手段。简言之，在数字时代，数据就意味着利润，数据广泛流动就意味着利润最大化。因此，消除数据跨境流动的壁垒会为美国带来显著的商业利益。早在 1997 年，美国总统克林顿（Bill Clinton）颁布《全球电子商务纲要》（A Framework for Global Electronic Commerce）政策文件，初步形成跨境数据自由流动的治理战略，主张在亚太经合组织、美洲首脑会议、《北美自由贸易协定》等多边平台展开对话，尽量减少各国为保护公民隐私而设置的非关税贸易壁垒。[①]尽管在遭受“9·11”恐怖袭击后，美国政府在一段时间内将网络空间治理的重点放在保护国家安全方面，但希拉里（Hillary Rodham Clinton）上任国务卿伊始，就把“互联网自由”重新设定为美国网络治理的主要战略，主张将网络空间看作“全球公域”，提倡数据在全球范围自由流动，并指责别国设置“数字屏障”的行为违反了《世界人权宣言》，以人道主义保护和现代化发展为由要求各国开放数据流动。美国政府致力于尽可能减少数据流动的国界壁垒，鼓励各国在跨境数据流动规制中采取宽松措施。[②]究其根本，这一政策主张的实际原因在于数据在全球范围自由流动会给美国带来丰厚的经济利润和政治利益，美国在网络空间占据先发性优势，其数据治理模式必然首先以大型企业的商业利益为先。

（二）美国数据治理主体

美国跨境数据流动的治理主体为政府和企业等私营部门。2018 年《美国国家网络安全战略》（National Cyber Strategy of the United States of America）以及

① The Framework for Global Electronic Commerce，https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

② Remarks on Internet Freedom，https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

拜登政府在2020年出台的《国家安全战略指导方针》（Interim National Security Strategy Guidance）均明确表示联邦政府与使用部门合作治理网络空间，以确保美国的互联网技术优势。[①]在数据攫取方面，美国拥有全球最大的互联网公司，在世界各地有广泛的用户，在数据挖掘、收集和分析方面的技术较为成熟。在此基础上，政府机构通过行政权力介入其中，与互联网巨头企业进行或明或暗的数据合作，形成千丝万缕的联系。在数据使用方面，美国依据其先进的互联网技术在全球网络空间推行数据霸权，企图要求各国产生的数据都能流入美国境内，并为美国政府所使用。《澄清境外合法使用数据法》（the Clarifying Lawful Overseas Use of Data Act）规定，只要服务提供者拥有或控制的信息，无论该信息是否存储在美国境内，服务供应商都有义务保存、备份或披露通信内容或相关记录等。[②]换言之，该法变相赋予美国政府通过网络运营商获取境外数据的能力，对本国政府和外国政府的规定体现出明显的“双重标准”。简言之，在对外宣传体系中，美国政府一向将“自由”奉为核心价值规范，在网络空间更是着力标榜数据在全球范围的自由流动。然而，所谓“全球化”不过是借助“自由”这一价值大旗占领道德高地，让全球的数据都流动到美国境内，在全球范围尽可能攫取利益，为美国政府所用，推动本国的数据产业发展，然后再凭借其强大的跨国企业进一步获取全球数据，如此反复循环。

（三）美国跨境数据流动治理机构

在大型企业和政府机构的共同推动下，美国在跨境数据流动治理领域形成以文件表述、官方言论为“虚”，以治理机构、法律法规为“实”的一套精密配合模式，实质是以“全球化”为包装，在数据空间继续推行美国霸权，监管世界各国的数据流动，具体体现在治理机构和法律法规两个层面。

在治理机构层面，美国的跨境数据流动规制主要由联邦通信委员会（Federal Communications Commission）和联邦贸易委员会（Federal Trade Commission）

① National Cyber Strategy of the United States of America Interim National Security Strategy，https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf；Interim National Security Strategic Guidance—The White House，https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/.

② Cloud Act Resources，https://www.justice.gov/criminal-oia/cloud-act-resources.

两大机构负责。一方面，联邦通信委员会旨在全方位监管国内外通信情况，确保美国的通信能力位于世界前列。联邦通信委员会于 1934 年建立，是受国会监督的独立美国政府机构，负责实施和执行美国通信法律法规，通过广播、电视、有线、卫星和电缆在美国领土内监管州际和国际通信，具体职责包括：促进宽带服务的设施的竞争、创新与投资；确保适当的竞争框架来推动通信技术革新以支持美国经济发展；鼓励国内外充分利用频谱；修订通信法规以保护新技术蓬勃发展；加强国家通信基础设施的防御能力。另一方面，联邦贸易委员会旨在通过商业数据管控，确保美国的商业市场处于高效、良性的竞争态势。联邦贸易委员会成立于 1914 年，最初的目的在于防止商业领域出现不公平竞争，从 1938 年起开始执行各种消费者保护法律，在 1975 年被国会授权负责制定和执行整个行业的贸易法规，具有保护消费者和促进良性竞争的双重使命。因此，在跨境数据流动规制中，贸易委员会主要负责在商业数据流动管理，确保公司履行用户隐私保护承诺，并对违反消费者隐私权的行为提起诉讼。这两大机构相结合，不仅确保美国政府能有效管控国内的数据和经济发展，还能帮助美国政府掌握其他国家的个人数据和商业数据，为美国“棱镜计划”“梯队系统”等全球监听系统的落实和运作奠定组织架构基础。

在法律法规层面，根据 2001 年颁布的《美国爱国者法》（USA Patriot Act），美国的远程电子服务和信息通信服务提供商可以直接获取国内外的通信记录，包括语言和文字，并将其披露给美国政府。而对于外国的信息搜集机构，则以“防范恐怖主义”为由设置了种种限制。2018 年美国推出《澄清境外合法使用数据法》（Clarifying Lawful Overseas Use of Data Act），对从国外调取美国数据的情况作出十分严苛的规定，要求外国政府在国内法的基础上，对调取数据的行为作出合理解释，同时要经过美国法院的审查，才能以最小化原则处理数据，之后还要定期审查。而对于美国政府调取境外数据的规定则宽松许多，允许美国在境外的通信服务供应商按照该法披露电子通信数据。同时还赋予美国法院巨大的裁量权，其中明确提出，若受到外国政府的起诉，法院也要保护本国的通信服务商，不能向国外政府提供相关的信息。但对于美国国防部对数据的处理和使用行为，则要求法院在“善意信任”的基础上行事。①

① Cloud Act Resources，https://www.justice.gov/criminal-oia/cloud-act-resources.

三、美国身份认知下的跨境数据流动战略

温特在分析观念建构对国家认知的影响时，曾举过一个形象的例子：“500件英国核武器对美国的威胁还不如5件朝鲜核武器的威胁大。”[①]在跨境数据流动战略中，美国同样受到上述身份认知的影响。作为传统的网络霸权国，其他国家的网络技术水平和影响力发展过快，都会引起美国的焦虑。其中，被美国认定为“盟友”的国家所引发的担忧程度较低，美国可能会在跨境数据流动中采取部分限制性举措，通过提高门槛等方式适当减慢盟国的互联网企业发展速度。但这建立在“合作”的基础上，跨境数据流动业务依然处于正常进行中，只是对其中的规则进行不同程度的调整。对于不同等级的“盟友”，美国跨境数据流动规则的严苛程度也不同。然而，被美国认定为“对手”的国家则会引发美方的强烈焦虑，并采取全面打压的方式将其完全排挤出市场，甚至不惜牺牲本国的经济权益来遏制对手国企业。在这种情况下，美国政策的出发点事实上脱离了对跨境数据流动的客观规律，而是以“安全化”的视角对待对手国企业。

在这些观念的加持作用下，美国建构出不同的无政府状态结构，并以此为基础，发展出自身的独特“身份认知体系”。第一步，美国基于意识形态的基本判定，依据政权类型划分不同国家的“类属身份”，即相对友好的“民主国家”和具有威胁影响的所谓“威权国家”。第二步，面对不同类型的国家，美国进一步划分阵营，做出不同利益判定标准，进而影响对外决策。第三步，在对外政策实践中，不同的互动行为塑造出不同的交往方式，即与盟友合作，与对手竞争。

（一）基于“敌人”身份认知的美国跨境数据流动战略——以中国为例

自特朗普担任美国总统后，美国官方出台的各类文件均将中国的角色认定为“战略竞争者”。2017年12月，特朗普政府发布的《国家安全战略》称中国为“修正主义国家”，并与美国的“利益和价值观背道而驰”，成为美国的“头

① ［美］亚历山大·温特：《国际政治的社会理论》，秦亚青译，第323页。

号战略竞争者”。[①]2022 年 11 月，拜登政府《国家安全战略》对中国的角色定位是“最重要的地缘政治挑战”，是唯一有充足的意愿和能力对美国构成“威胁”的国家。[②]从美国对中国的战略描述中不难看出，美国对中国的身份认知越来越接近建构主义理论中的“敌人”角色。尽管美国在官方文件中依然保留了“竞争对手”这一表达，其对华数据政策彰显出典型的“霍布斯文化”特征，即完全脱离既定的数据治理框架，以“安全化”为由进行毫无节制的数据争夺。尽管中国一再重申对美国没有敌意。但美国当前的政策表明，对中国的“敌人”角色认定已经成为事实。那么无论这种“敌人形象”真实与否，“从结果方面来看，敌人就是真实的”。[③]

基于对中国“敌人”角色的认定，美国以“安全化”视角处理对华跨境数据流动问题。面对进入美国市场的中方企业，美国政府以高度警惕的态度全方位审视企业的数据运营，追求美方数据的“绝对安全”。同时，美国对华数据博弈中动用各种工具保护美方互联网企业的利益，全力保障美方在数据流动中处于优势地位。以短视频软件 TikTok 为例，该软件作为中国公司“字节跳动”针对海外市场发布的社交媒体应用程序，进入美国市场后迅速遭到极度严苛的数据审查。如表 2 所示，美国对 TikTok 发起审查和限制的根本原因在于对中国的“敌人”身份的认定，并将中国企业视为中国政府的“代理人”，予以严格打压。

综合美国对 TikTok 的上述打压行径，呈现如下三个特点。第一，美国对 TikTok 的审查存在明显的“泛安全化”倾向，对数据安全过度担忧，对中方企业过度警惕。这种担忧完全是基于对中国“敌人”身份的恐惧，而非基于 TikTok 企业的商业行为，甚至在焦虑心理作用下完全无视现实情况。纵观美国数次审查行为，始终以含混不清的“国家安全”作为理由，但并没能从实操层

① President Donald J. Trump Announces a National Security Strategy to Advance America's Interests，https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-announces-national-security-strategy-advance-americas-interests/.

② FACT SHEET：The Biden-Harris Administration's National Security Strategy，The White House，https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/.

③ ［美］亚历山大·温特：《国际政治的社会理论》，秦亚青译，第 243 页。

表 2　美国对 TikTok 的审查汇总

时间	部门/人员	具体措施	理　由
2019 年 10 月 9 日	参议员马尔科·卢比奥（Marco Rubio）	要求美国政府对 TikTok 展开调查，特别是该企业对国家安全的影响。	怀疑 TikTok 的内容审查制度服务于“中国领导人”，可能会“威胁”言论自由的传统西方价值观。
2019 年 10 月 23 日	参议员汤姆·科顿（R-Arkansas）和参议员查克·舒默（D-New York）	联名致函国家情报代理局长约瑟夫马奎尔，要求情报界对 TikTok 平台进行安全评估。	中国的情报、国家安全和网络安全法律迫使中国公司支持和配合中国共产党控制的情报工作。
2019 年 11 月	美国外国投资委员会（CFIUS）	开始审查 TikTok 在收购美国社交媒体应用程序 Musical.ly 的交易。	收购行为没有获得美国外国投资委员会许可，因为允许美国安全小组介入调查。
2019 年 12 月	美国海军、陆军	禁止士兵在政府发行的移动设备使用社交媒体应用程序 TikTok。	认为 TikTok 程序存在“安全风险”。
2020 年 2 月	美国运输安全管理局（TSA）	禁止员工使用 TikTok 在社交媒体上发帖。	国家安全专家不信任 TikTok 收集和处理用户数据和个人信息的方式，并担忧中国法律强制企业与政府合作并进行情报收集。
2020 年 3 月	共和党参议员乔希·霍利（Josh Hawley）	向国土安全和政府事务委员会提交立法建议，禁止任何联邦雇员在美国政府发布的设备上使用或下载 TikToK。	虽然 TikTok 已声明将美国用户数据存储在美国，但字节跳动仍需遵守中国法律，可能会被强迫与政府共享情报信息。
2020 年 7 月 6 日	美国国务卿迈克·蓬佩奥（Mike Pompeo）	宣称美国正在“考虑”禁止 TikTok 和其他中国社交媒体应用程序。	该平台会审查内容，而且其数据可能会被北京访问。
2020 年 8 月 6 日	美国总统唐纳德·特朗普（Donald Trump）	签署行政令，要求 TikTok 在 45 天后完全退出美国市场，禁止该企业在美国进行任何形式的交易。	中国公司开发和拥有的移动应用程序在美国广泛传播，会威胁美国的国家安全、外交政策和经济。

（续表）

时间	部门/人员	具体措施	理　由
2020 年 8 月 14 日	美国总统唐纳德·特朗普（Donald Trump）	再次发布行政令，不允许 TikTok 收购 Musical.ly，并要求该企业出售全部在美业务。	TikTok 收购 Musical.ly 的商业行为可能损害美国国家安全。
2021 年 9 月	美国总统约瑟夫·拜登（Joseph Biden）	撤销特朗普总统对 TikTok 的禁令，由商务部长接手评估工作。	包括中国在内的对手国家拥有或控制的软件应用程序，继续威胁美国国家安全、外交政策和经济。但联邦政府应通过严格的、基于证据的分析来评估这些威胁。
2022 年 7 月 14 日	美国国会的共和党人	要求 TikTok 交出有关在中国访问用户数据的文件。	中国法律要求公司“支持、协助和配合国家情报工作”，意味着 TikTok 可能被迫向中国政府提供敏感的用户数据。
2022 年 11 月	佛罗里达州参议员马尔科·卢比奥（Marco Rubio）和威斯康星州众议员迈克·加拉格尔（Mike Gallagher）	称 TikTok 是中国的监视工具，希望出台立法以禁止该应用程序继续在美国运营，并批评拜登政府的相关决议。	担忧美国用户数据会被传输到中国，并为中国政府作用。
2022 年 11 月 15 日	美国联邦调查局局长克里斯托弗·雷（Christopher Wray）	向国会阐述 TikTok 是一个国家安全问题。	该应用程序由一家中国公司字节跳动所有，联邦调查局担心 TikTok 可能会与中国政府共享美国用户的数据。
2022 年 12 月 6 日	马里兰州	发布紧急网络安全指令，禁止州政府行政部门使用 TikTok。	给国家带来了不可接受的网络安全风险，并可能参与网络间谍活动、监视政府实体和不当收集敏感个人信息等活动。

面举证 TikTok 有任何违反美国法律的行为。[①]事实上，TikTok 作为一家合理合法的企业，中国政府并不能也不会强行获取该公司收集的商业数据。耶鲁大学法学院研究中国法律的高级研究员萨姆·萨克斯（Samm Sacks）明确表示："中国政府无法不受限制地实时访问所有公司的数据，中国企业也有自己的商业利益考量，并不是中国政府的代理人。"[②]与此同时，TikTok 也多次公开自己的数据处理方式，证明用户数据的安全性。字节跳动公司在开辟海外市场中采取了区域化方法，根据市场国当地的需求调整数据的采集、存储、处理和使用的具体方式，即将美国用户数据存储美国弗吉尼亚州的数据中心内，并在新加坡备份冗余。这些数据中心的服务器完全位于中国境外，并有专门的技术团队负责数据隐私政策的落实。此外，该公司还会定期进行内外部安全审查，确保用户数据不被窃取和滥用。此外，网络安全公司 Special Counsel 的顾问也曾分析过 TikTok 应用程序的源代码和数据存储方式，并没有任何迹象表明中国政府访问过用户数据。[③]尽管在法律层面和技术层面，TikTok 被多次证实商业运营合法合规，但美方仍冠以"国家安全"之名穷追猛打。究其根本，还是出于对"敌人"身份的主观臆断，认定"敌国"企业会服务于政府来威胁本国安全。因此在面对以 TikTok 为代表的中国企业时，先入为主地代入安全焦虑视角，从而采取严苛的限制措施。

第二，在中美数据竞争中，美国政府和业界对中国企业严防死守，确保美国数据处于绝对安全状态，追求在数据市场中的相对优势而非绝对收益。自 2016 年在国际市场上推出后，TikTok 在包括美国市场在内的各国广受欢迎，2022 年 10 月的下载量已经超过 Facebook、Snapchat、Instagram 和 YouTube 等美国传统龙头社交媒体应用程序。[④]在此之前，从未有任何一家中国社交媒体平台在美国市场

① White House Presses To Move Forward With TikTok Ban, https://www.mediapost.com/publications/article/356940/white-house-presses-to-move-forward-with-tiktok-ba.html.

② TikTok is a national security threat, US politicians say. Here's what experts think, *CNN Business*, https://www.cnn.com/2020/07/09/tech/tiktok-security-threat/index.html.

③ Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses, https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

④ TikTok is the latest social network sensation, *CNN Business*, https://www.cnn.com/2018/11/21/tech/tiktok-app/index.html.

上获得成功，导致业界人士担忧“TikTok 可能成为美国市场上第一家由亚洲公司所有并长期运营成功的社交应用程序”①。在此之后，字节跳动公司以 10 亿美元收购社交媒体应用程序 Musical.ly 的举动再度引发美方恐慌。在政界，美国外国投资委员会还对存储个人数据的方式提出质疑，总统特朗普直言这一收购行为“可能损害美国国家安全”，并签署行政令要求 TikTok 在 45 天后完全退出美国市场②，甚至要求该企业在内出售全部在美业务。③在商界，红杉资本和泛大西洋资本等投资者表态，希望将 TikTok 的多数股权转让给他们。④美国政府和互联网龙头企业相互联结，将国家安全与贸易谈判强行捆绑，以“赢者通吃”的逻辑打压 TikTok 的发展势头。归根结底，还是对华“敌人”认知的视角在作祟，致使美方放弃合作开发带来的商业利润，而一心将中方企业驱逐出市场。

第三，美方无视既有的制度约束，动用全部资源与 TikTok 进行“你死我活”的数据争夺，甚至以诽谤、抹黑等方式攻击该企业。对 TikTok 的数据审查中，不仅有联邦通信委员会和联邦贸易委员会等传统的数据主管机构，美国的交通部门、安全部门和军方机构等各类政府机关均参与其中。此外，Facebook 甚至策划了一场大型商业阴谋来诽谤 TikTok。其母公司 Meta 向共和党咨询公司支付大笔费用，杜撰 TikTok 滥用、泄露用户数据的虚假新闻。⑤例如，假借“一位年轻家长”之名在《丹佛邮报》上发布来信，称 TikTok 对美国青少年的心理健康造成伤害，并“怀疑中国政府故意收集我们孩子的数据”⑥。通过这种抹黑煽动公众对 TikTok 的厌恶情绪，帮助击败其最大的商业竞争对手，赢回 Facebook 流失的美

① TikTok Gains 30 + Million Users in 3 Months, https://blog.apptopia.com/tiktok-gains-30-million-users-in-3-months.

② Executive Order on Addressing the Threat Posed by TikTok, The White House, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

③ Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., The White House, https://trumpwhitehouse.archives.gov/presidential-actions/order-regarding-acquisition-musical-ly-bytedance-ltd/.

④ U.S. Treasury to make recommendation on TikTok to Trump this week: Mnuchin, https://www.reuters.com/article/us-usa-china-tiktok-treasury-idUSKCN24U288.

⑤ Facebook paid GOP firm to malign TikTok, https://www.washingtonpost.com/technology/2022/03/30/facebook-tiktok-targeted-victory/.

⑥ Letters: Readers share their ideas on how to reform and save RTD, https://www.denverpost.com/2022/03/21/rtd-needs-help-funds-ridership/.

国年轻用户。值得注意的是，受到打压的不仅是字节跳动公司，华为、中兴、海能达、海康威视和大华科技均有类似经历。[①]但凡在美国市场崭露头角的中国企业，均会遭受美方“打地鼠”般毫无节制的打压。

（二）基于“对手”身份认知的美国跨境数据流动战略——以日本为例

日本尽管在20世纪中叶与美国结成军事同盟，但在美国的同盟体系中处于较为边缘的地位。尽管日本将美国视为“最可靠的盟友”[②]，但事实上，日本从未进入美国的核心盟友层，也从未被美国视为真正意义上的“朋友”。美国的盟友体系存在隐性的等级特征，处于最核心地位的是能够共享情报的“五眼联盟”，即英、加、澳、新四个亲缘国家；其次是军事联盟北约的成员国；第三梯队则是其他位于欧洲地区的盟友国家；最后才是位于其他地区的盟友，不同区域的重要程度取决于美国不同时期的战略重心。[③]其中，只有前两个等级的盟友处于温特所界定的“朋友”身份，对待其他等级的盟友，美国在存在共同利益的领域进行合作，并防范在利益不相干的领域本国利益的损失，更贴近于建构主义中对待“对手”的行为逻辑，日本就是典型代表。根据皮尤研究中心2021年的一项民意调查，美国民众对日本的好感度低于加拿大和英国等传统盟友，只有1%的人将日本视作“亲密盟友”[④]。近年来，日本以主要参与者的身份回归地缘政治博弈，在更多方面与美国形成竞争态势，强化美国对其“对手”身份的认知。最明显的是不断增加国防开支，甚至计划在五年内打破1970年设定的战后国内生产总值（GDP）1%的上限。这意味着日本政府已经放弃过去的防御性军事战略，引发美日安全同盟的角色转变：日本不再是同盟的被保护方，

① FCC List of Equipment and Services That Pose National Security Threat，https://www.fcc.gov/document/fcc-list-equipment-and-services-pose-national-security-threat.

② U.S. is seen as a top ally in many countries—but others view it as a threat，https://www.pewresearch.org/fact-tank/2019/12/05/u-s-is-seen-as-a-top-ally-in-many-countries-but-others-view-it-as-a-threat/.

③ 储召锋：《冷战后美国联盟战略研究》，国防科学技术大学博士论文，2017年；吴言：《“相对剥夺感”与弱盟友选择：冷战后美国东亚同盟体系研究》，外交学院2021年；刘柏骏：《美国亚太联盟体系网络化研究》，战略支援部队信息工程大学2017年。

④ China，Russia Images in U.S. Hit Historic Lows，https://news.gallup.com/poll/331082/china-russia-images-hit-historic-lows.aspx.

转而希望成为安全提供者。[①]这种角色的转变将引发同盟动荡，美国对日本军事行动的重视和警惕程度加深。

在跨境数据流动领域，美日之间的竞争关系更加显著。尽管日本的数据治理模式在很大程度上有美国的烙印，在外交场合曾多次表态追随美国的数据战略。但随着数字贸易成为国际贸易的重要部分，日本更加注重数字经济利益和数字主权保护。例如，2013 年提出以信息技术促进商业发展的“G space x ICT”模式[②]，2016 年发布“关于第五次科技基础计划”[③]，2017 年提出将网络空间与物理空间高度融合的“社会 5.0”愿景[④]，2019 年发布《制造业白皮书》[⑤]，2020 年成立供应链网络安全联盟等。[⑥]出于对经济利益的追求，美日数字贸易的摩擦日益凸显。但这种数据竞争不同于对“敌人”的数据争夺，不是毫无约束的针锋相对，而是承认并尊重对方安全利益基础上的有限竞争，遵循数据流动规律并在共同制定的制度框架内行事。

一方面，美国以符合数据基本规律的方式制定对日跨境数据流动战略，并承认日本的数据主权和安全。在数字经济时代，数据作为生产要素，在流动中才能创造出更大的价值。因此，美国牵头与日本制定了基本的数据流动制度，在数字贸易中为双方创造更多绝对收益。2019 年 10 月双方签订《美日贸易协定》（the US-Japan Trade Agreement），《美日数字贸易协定》（the U.S.-Japan Digital Trade Agreement）于 2020 年 1 月 1 日正式生效。在协定谈判过程中，美

① Japan’s Long-Awaited Return to Geopolitics，https://www.rand.org/blog/2023/02/japans-long-awaited-return-to-geopolitics.html.

② 総務省｜報道資料｜《「G 空間×ICT 推進会議」の開催》，https://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000081.html，访问日期：2022-12-06。

③ 内閣府：《総合科学技術・イノベーション会議（第 15 回）議事次第》，https://www8.cao.go.jp/cstp/siryo/haihui015/haihu-015.html，访问日期：2023-02-14。

④ 《科学技術イノベーション総合戦略 2016》，https://www8.cao.go.jp/cstp/sogosenryaku/2016/honbun2016.pdf，访问日期：2022-12-06。

⑤ 《2019 年版ものづくり白書（ものづくり基盤技術振興基本法第 8 条に基づく年次報告）（METI/経済産業省）》，https://www.meti.go.jp/report/whitepaper/mono/2019/index.html，访问日期：2022-12-06。

⑥ 経済産業省：《サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が設立されます》，https://www.meti.go.jp/press/2020/10/20201030011/20201030011.html，访问日期：2023-02-14。

国充分认可日本保护数据安全的诉求，规定严格保护企业的数据安全，确保企业能够自主设置密码，不会被其他企业或政府胁迫交出密钥或其他机密参数、算法等，也不能强迫企业解密用户资料。

另一方面，美国在美日数字贸易中着力维持优势地位，确保美企从中获取更多商业价值，为美国数据霸权服务。美国前总统特朗普曾宣称该协定的签订意味着“以4万亿美元买断了日本数字市场”，是一种显而易见的“单赢”而非“双赢”。[①]事实上，美国的目标是按本国利益制定美日商业规则，以培育具有强大国家权力的本国公司。然而对于日本，国内互联网企业的业务上不成熟，个人信息保护和消费者保护方面还没有建立起可靠的机制，因此本国企业发展和个人信息保护可能会遭受损害。已有日本学者警惕，该协定可能会对日本数据造成一定威胁。[②]事实上，在美日数字合作中，日本只是充当美国实现其国内利益的“棋子”，美方尽力压榨其数据商业价值以提升本国实力，双方事实上处于不对等的数据竞争关系中。

（三）基于“朋友”身份认知的美国跨境数据流动战略——以欧盟为例

美欧伙伴关系由来已久，以1990年的《跨大西洋宣言》和1995年通过的《新跨大西洋议程》为基础，随着后续合作的发展逐步深化。拜登政府出台的《国家安全战略》将欧盟称为“应对各类全球挑战的主要伙伴”。其一，欧盟是美国最重要的贸易伙伴，拥有世界上最大的双边贸易和投资关系。双方的购买力占据世界国内生产总值的近三分之一，2021年双边服务贸易额创历史新高，超过5 000亿欧元。[③]其二，许多欧盟国家是北大西洋公约的成员，在美国军事安全联盟体系中占据核心地位，代表着美国盟友体系的“最高点”[④]。其三，欧

① 《「日米デジタル貿易協定」—前衆議院議員　高井たかし　公式サイト》，https://takaitakashi.com/archives/6177，访问日期：2022-12-06。

② しょうこ内田聖子うちだ：《日米貿易協定と日米デジタル貿易協定の何が問題なのか》，《月刊『住民と自治』》，2020年第4月号より期。

③ EU trade relations with United States，https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en.

④ US' new security strategy on Europe：Disconnection，differences | Opinion，https://www.daily-sabah.com/opinion/op-ed/us-new-security-strategy-on-europe-disconnection-differences.

盟有着与美国相似的文化背景，早在20世纪，美国领导人就认定与欧盟“在利益和价值观上有着极其广泛和深刻的共同点”①。时至今日，“共同民主价值观和世界上最强的经济联结”②也成为欧盟优先于与其他美国盟友的重要原因。在经贸关系、安全关系和共同价值观的三重支撑下，欧盟已成为美国最重要的盟友。一直以来，美国高度重视与欧盟的跨境数据流动合作，以积极态度面对治理纠纷，保障双方的数据流动渠道通畅。美欧峰会中，双方再次强调要深化贸易和投资关系，并共同推动数字化转型。③这意味着美欧的跨境数据流动合作将迈入新阶段。

第一，美国寻求与欧盟加强数据合作，在保证双方数据安全的前提下深化跨境数据流动，共同推动数据治理制度良性变革。美欧跨境数据流动的规则体系大体经历了三个阶段。第一阶段2000—2015年，美国与欧盟之间的跨境数据流动主要遵循《安全港隐私原则》（Safe Harbor Privacy Principles）。④然而，2013年“棱镜门”事件被披露后，奥地利公民马克斯·施雷姆斯（Max Schrems）向爱尔兰数据保护官投诉脸书（Facebook），指控该企业受美国《爱国者法》要求，将欧盟公民的数据传输到美国。最终欧盟法院判决《安全港隐私原则》无效。⑤第二阶段始于2016年，欧盟委员会认为《欧美隐私盾协定》（the EU-US Privacy Shield）足以保障数据传输符合欧盟法律。⑥据此，《欧美隐私盾协定》成为支撑美欧跨境数据流动的新框架。之后，施雷姆斯再次对脸书提起诉讼，指控该公司将其个人数据从爱尔兰分公司转移到美国总部。直到2020年，欧盟法

① Fact Sheet: U.S.-EU Relations, https://1997-2001.state.gov/regions/eur/eu/fs_980526_useu.html.

② U.S.-EU Summit Statement, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.

③ U.S.-EU Summit Statement, https://useu.usmission.gov/u-s-eu-summit-statement/.

④ EUR-Lex-32000D0520-EN, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

⑤ The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

⑥ COMMISSION IMPLEMENTING DECISION (EU) 2016/1250, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

院正式做出裁决，《欧美隐私盾协定》就此失效。[①]此后，双方开始积极推动新的跨境数据流动协定。经过了一年多的谈判，2022 年 3 月，美国和欧盟承诺制定新的跨大西洋数据隐私框架，以保持欧盟和美国之间的数据流动。[②]

第二，美国与欧盟的数据合作创造出大量商业价值，共享跨境数据流动红利。2019 年，美国对欧盟的数字化服务出口额超过 1 670 亿美元。作为回报，欧盟向美国出口了 1 300 亿美元。[③]2021 年美欧贸易和技术委员会（the EU-US Trade and Technology Council）成立，进一步深化数字经济和数据治理合作，共同保护关键技术供应链。[④]尽管 TTC 仍处于起步阶段，在推进过程中也遇到一些挑战，但仍表现了美国深化跨大西洋合作伙伴关系的决心。技术和贸易已成为美欧之间重要的两个议题，均与跨境数据流动密切相关。美欧在共享数据红利的同时，还在捍卫作为“朋友”所共享的价值观。例如，在美国的叙事体系中，将中国的数据治理制度描述为与欧美制度对立的“敌方”，前者的成熟与完善会威胁到后者的发展和利益获取。因此，美方认为，只有加强与欧盟的合作，共同破坏中国全球数据治理的愿景，才能确保美国和欧盟在跨境数据流动中持续获益，并在全球创造符合其利益和价值观的数据治理框架。[⑤]

第三，美国以积极态度处理对欧数据流动纷争，甚至自我限制安全活动以满足欧盟的数据安全标准。在《欧美隐私盾协定》被欧盟宣判失效后，美国方面一直寻求建立新的数据传输协定。出于美国对欧盟“盟友”身份的认定，在新协定谈判中以绝对收益的视角做出理性分析，愿意在国家安全方面做出让步，以换取欧盟数据合作带来的海量商业利益。从谈判结果来看，欧盟对数据传输

---

① EU T C O J. JUDGMENT OF THE COURT（Grand Chamber），https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227.

② The West's plan to keep global data flows alive，https://www.politico.eu/article/data-oecd-privacy-shield-national-security/.

③ EU/US：Cross-border data flows-a necessary part of global trade | DigiLinks | Insights | Linklaters. /en/insights/blogs/digilinks/2021/june/eu---cross-border-data-flows---a-necessary-part-of-global-trade.

④ EU-US launch Trade and Technology Council，https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2990.

⑤ EU-US tech cooperation：Strengthening transatlantic relations in data-driven economies，https://www.atlanticcouncil.org/blogs/geotech-cues/eu-us-tech-cooperation/.

条件提出了更高标准的要求，需要美国做出更多承诺，如：保证个人隐私和公民自由；建立具有独立约束力的新申诉机制；加强对信号情报活动的严格管理和分层监督。值得注意的是，除了原有的个人隐私保护部分外，新框架还加入了对情报活动的管控内容。2022 年 4 月 13 日，相关各方在全球隐私峰会（IAPP Global Privacy Summit）上的言论表明，新的协定已初步成型，有望在 2023 年底达成最终协议。①2022 年 10 月 7 日，美国总统拜登签署行政命令，对 3 月签署的数据隐私框架做出具体指示，承诺在情报活动中进一步加强隐私和公民自由保障。②

四、结论及启示

温特的建构主义在较大程度上可以解释当前美国的跨境数据流动战略。被美国认定为“敌人”的中国互联网企业发展势头迅猛，引发美方强烈的安全焦虑，并不择手段予以打压；被美国认定为“对手”的日本在有限合作的同时，也面临来自美国的数据竞争；被美国认定为“朋友”的欧盟方可与美国共享数据红利，实现良性制度变革和数据合作共赢。总之，在无政府状态的加成作用下，美国在跨境数据流动战略中，事实上遵循了以身份认知的战略逻辑，而非跨境数据流动本身的客观发展规律。美国对于其他国家的“身份建构”，将美国代入到不同的无政府文化状态中，最终表现为美国的对外决策行动。

就美国的种种表现来看，对中国的敌视愈演愈烈，不断强化“敌人”的身份认知，并在具体政策中加大对中国互联网企业的制裁力度。因此，我国需要针对现实处境做好战略应对，探索跨境数据流动的新秩序、新安全和新模式。以 TikTok 为例，在应对美国政府的若干轮审查中，字节跳动公司不断改进数据管制规则，将全部的美国用户数据存储在位于美国弗吉尼亚州的数据中心内，

① Officials“thrilled”with EU-US data flows agreement，“work continues”on finalization，https://iapp.org/news/a/officials-thrilled-with-eu-us-data-flows-agreement-work-continues-on-finalization/.

② FACT SHEET：President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework，The White House，https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

并在新加坡备份冗余。这样一来，用户敏感数据并不会跨境流动，而是存储在当地，只有用户授权上传的数据才会进行跨境分享与处理。此外，有专门的技术团队负责数据隐私保护，定期进行内外部安全审查，确保用户数据不被窃取和滥用。①由此，通过数据的本地化采集、存储、处理和全球化运营，TikTok 解决了在美日常运营问题，同时为后续的大国数据战略博弈提供了全新的实践模式。与此同时，我国从未停止建设中美友好关系的步伐，官方媒体从中美友好合作的历史②、中美数字经贸的重要性③、美国从双边经贸中获益情况④等多个角度不断释放善意信号。在理想的状态下，希望可以通过重塑自我和他者的角色，来扭转美国对中国的敌对认知。例如，强调中美关于数据治理的利益共通点，包括合作打击网络犯罪、共同防范网络恐怖主义、维系全球网络空间的和平与稳定，等等。

总之，美国对别国的身份认知体系具有很强的主观色彩，根据意识形态先验性地赋予别国不同的“角色”。相较对日本和欧洲的身份认知，美国对中国“敌人”角色的认定时间较晚，在特朗普执政时期才开始逐步成型，因此在很大程度上只存在于美国的“自有知识”范畴中。换言之，中美之间的这一结构处于较为浅薄的层次，还没有形成“社会共有知识”。从长远来看，文化结构若要得以延续，则需要国家进行相应的实践活动，最终达成“自我实现的预言”⑤。这也给我国的应对政策留下一定空间。在未来的中美数据博弈中，我们要做好充足的战略准备，同时在心理层面加强对美国的认知引导。

---

① Pappas V. Explaining TikTok's approach in the US，https://newsroom.tiktok.com/en-us/explaining-tiktoks-approach-in-the-us.

② 《中美关系合作共赢的大势不可逆转》，中国共产党新闻网，http://theory.people.com.cn/n1/2022/0301/c40531-32362160.html。

③ 《青山遮不住——从经贸科技动向看中美合作发展大势》，新华网，http://www.xinhuanet.com/2021-09/21/c_1127885876.htm。

④ 《关于美国在中美经贸合作中获益情况的研究报告》，http://penang.china-consulate.gov.cn/chn/zt/zgwj/201911/t20191127_4883331.htm。

⑤ ［美］亚历山大·温特：《国际政治的社会理论》，秦亚青译，第 299 页。

challenges to traditional intellectual property governance. Against this backdrop, various functional bodies, with the United States Senate Judiciary Committee playing a leading role, have convened multiple hearings in the preliminary drafting of legislative policies. The purpose is to clarify specific disagreements in intellectual property governance and seek corresponding strategies. The disagreements in intellectual property governance addressed in the hearings mainly focus on the regulation of artificial intelligence, as well as patent and copyright domains, revealing the fundamental issue that the institutional development lags behind technological innovation. Discussions and potential measures taken by the United States on the above controversies can offer insights into the construction of intellectual property governance in the era of generative artificial intelligence: the path to resolving existing intellectual property governance disputes lies in defining the legal boundaries of artificial intelligence innovation on the basis of unified technological development and regulation. Specific measures should be taken in the domains of patents and copyrights to balance technological development with the interests of public innovation.

[**Key Words**] Generative AI Intellectual Property Rights AI Regulation AI Invention Fair Use

U.S. cross-border data flow strategy based on identity recognition

…… *Shen Yi Gao Yu*

[**Abstract**] After entering the era of big data, data has become the new focus of the strategic game among major powers. Cross-border data flow governance is the core issue, and it has also become an important point for the U.S. internal governance and external strategy. Even though there are lots of established practical standards for cross-border data flow, the United States actually follows the logic of identity recognition to govern cross-border data flow. For countries identified as "enemy", such as China, the U.S. handles the

issue of cross-border data flow from a security perspective, ignoring the objective laws, and engages in data competition. For countries identified as "adversary", such as Japan, the U.S. allows some cross-border data flow cooperation in its favor, but will conduct data competition within their framework to obtain more dividends. For entities like the EU that are recognized as "friend", the U.S. actively deepens data cooperation, share the profits brought by data flow, and promote long-term data cooperation mechanism.

[**Key Words**] United States Identity Recognition Cross-Border Data Flow

Development and countermeasures of the security review system of foreign investment in the United States—And the enlightenment of data security review to our country

…… *Liu Xiao*

[**Abstract**] As a key measure of end to end supervision, foreign investment security review is an important tool to effectively prevent foreign investment risks. In recent years, the U.S. foreign investment security review system has been continuously updated and enriched, which has a direct and significant impact on Chinese enterprises' investment in the United States. The U.S. foreign investment security review system details "sensitive personal data", attaches importance to cybersecurity risks, emphasizes "key technologies", maintains supply chain resilience, and strengthens review and enforcement procedures, resulting in data security reviews to curb the development of Chinese enterprises, significantly increase the risk of Chinese investment in the U.S., and delay the upgrading and development of new technologies in China. China realizes the importance of sensitive personal data, strengthen the review of foreign enterprises' processing of Chinese data, and improve China's foreign investment security review system, strengthen bilateral exchanges and enhance independent innovation capacity, and support enterprises to promote multi-