法商研究 Studies in Law and Business
Vol. 39 No. 2(2022)

美国域外数据管辖权研究

杨 永 红*

摘 要:美国通过立法确立了以数据控制者为标准的域外数据管辖权,将美国公司在全球数据领域的优势转变为美国对域外数据的管辖权。尽管美国对域外管辖权设置了一定的限制,但是这些限制规则在很大程度上仅具有形式意义,并不能实际避免其域外管辖与数据所在地国的属地管辖发生冲突,进而严重威胁到包括中国在内的大部分国家的数据主权。中国应积极联合新兴国家与发展中国家,主动参与国际数据合作机制的创立,提升在数据管辖方面国际规则体系构建中的话语权。同时,中国应采取措施提高中国企业在全球数据领域的竞争力及规则意识,真正地应对美国的数据霸权。

关键词:数据主权 域外管辖 立法管辖权 执法管辖权 中间人 控制者

近年来,随着数据主权的概念被广泛接受,国家对域外数据的管辖问题成为争议的焦点。过去,计算机数据几乎都储存在美国境内的美国公司的服务器中,美国对这些数据具有毋庸置疑的管辖权,因此 1986 年《美国存储通信法》(以下简称《存储通信法》)规定的电子通讯隐私条款并未规定美国对境外数据拥有管辖权。而今天,尽管互联网公司巨头仍然以美国的为主,但是数据的储存地早已分布在全球各地。"微软搜查令案"①使美国意识到明确域外数据管辖权的紧迫性,美国通过修改《存储通信法》将美国对数据的管辖权延伸至域外数据。尽管美国对域外数据的管辖权并未扩张至与美国无关的域外数据,而是通过数据控制者的属人连接点建立域外管辖权,但是基于美国的公司是全球数据的主要控制者,美国对域外数据的管辖权将严重影响到数据存储国对数据的主权。数据跨境获取将对中国的国家安全、数据主权、国际话语权及中国企业的合规问题等带来巨大的冲击,直接影响到中国作为新兴数据大国的利益和中国企业及个人的权益,对美国的域外数据管辖权进行深入研究十分迫切和必要。

* 西南政法大学国际法学院教授、博士生导师
基金项目:司法部国家法治与法学理论研究项目(19SFB2057)

① See Microsoft v. United States, 829 F. 3d 197 2d Cir. (2016).

一、域外数据的判断标准

首先必须澄清的是,“数据”在本文中包括“个人数据”(含电子邮件服务器上持有的私人数据)、“公司数据”以及“(非公司)实体数据”。本文中的域外管辖的概念是公法意义上的,它是相对于域内管辖而言的一个概念,笼统而言,是指一个国家跨越边界主张管辖权。[①]《美国对外关系法重述(第四次)》[以下简称《重述(第四次)》]第402条将域外管辖视为属地管辖之外的基于非属地连接点的管辖,并强调基于英文“extraterritoriality”一词含有治外法权的含义,使用较中立的“地理范围”来指代“域外管辖”一词,表明域外管辖判断的标准是地理位置。故域外数据的管辖应是指非存储地国家对存储在其他国家或地区的数据的管辖。

1. 数据的属地性

数据与债权、股票或其他无形资产在流动性方面极为相似,但与对无形资产主张管辖权相比,对数据主张管辖权似更容易。因为与债权、股票不同,数据无论存储在何处都具有实际存在于领土上的特性。美国法院在许多不同情况下都承认数据的物理属性。美国联邦第四巡回法院指出:“计算机通过重新排列磁盘或磁带的原子或分子来存储信息,以形成特定顺序的磁脉冲,并形成有意义的序列电磁脉冲……擦除是一种直接的物理损失。”[②]美国路易斯安那州法院亦有同样的裁定。[③] 因此,数据所存储的计算机、磁盘等物品的位置反映了数据的属地性。基于数据的物理特征,数据的属地性被广泛接受。早在20世纪80年代,美国就意识到数据的价值与监管数据的必要性,《存储通信法》规定美国政府可以通过行政传票、法院命令或搜查令获取存储在本土的数据,包括用户姓名、地址、电话、网络地址、通话记录和支付信息等,但是没有对境外数据的访问作出授权。该法显然是将数据存储地视为美国管辖的法律基础,体现了数据的属地特点。

2. 数据的属人性

对于数据的物理性,美国的判例法并未形成共识。美国加利福尼亚州法院主张,硬盘驱动器被擦除不会导致明显的物质损失。[④] 美国联邦巡回第四法院曾称数据因无法触摸而是无形的。[⑤]虽然美国国际贸易委员会在“克林科瑞特案”[⑥]中确定数据构成进口物品,但是联邦巡回上诉法院推翻了美国国际贸易委员会的裁决,认为“物品”是“实质性的东西”而数据不是。这种解释上的分歧在于数据的双重性质——既有形又无形。当数据处于无形的时候,它可以存在于任何地方,难以与某个特定的地理位置建立一个特定的联系。因此,数据应依属人进行管辖的观点亦得到不少支持。

3. 数据属地性主导域外数据的判断标准

---

① See Anthony J. Colangelo, What Is Extraterritorial Jurisdiction, 99 Cornell Law Review, 1303 (2014); Danielle Ireland-Piper, Extraterritorial Criminal Jurisdiction: Does the Long Arm of the Law Undermine the Rule of Law, 13 Melbourne Journal of International Law, 122 (2012).

② Widener, J., Concurring, NMS Servs. Inc. v. The Hartford, 62 F. App'x 511, 514-15 4th Cir. (2003).

③ See Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc., WL 1094761M.D. La. (2012).

④ See Ward Gen. Ins. Servs. Inc. v. Emp'rs Fire Ins. Co., 7 Cal. Rptr. 3d 844, 851 Ct. App. (2003).

⑤ See Petition for a Writ of Certiorari at 13-14, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

⑥ See ClearCorrect Operating, LLC v. International Trade Commission, 819 F.3d 1286-1289 (2016).

数据的价值使其成为国家争夺的重要资产。越来越多的国家通过数据本地化或其他方式使互联网企业将数据中心设置在本地,美国亦不能如过去一样控制全球数据。然而,2018 年《美国澄清境外数据合法使用法》(以下简称《澄清法》)规定美国可通过控制者的属人管辖对位于域外的数据实现管辖权,似乎数据的属人性超越了属地性。正如美国司法部所称,该修改并未实质改变数据管辖问题,与传统的管辖规则亦没什么分别。① 与传统的管辖规则一样,对控制者的属人管辖仍然是对处于域外事物的域外管辖。

二、美国域外数据管辖权的构成

美国域外管辖权通常由立法管辖权、司法管辖权和执法管辖权构成。由于司法管辖权是以立法管辖权为基础且基本是一致的,因此本部分将从立法管辖权与执法管辖权两个方面来分析美国的域外数据管辖权。

(一)立法管辖权

如前所述,数据既是有形的又是无形的。只要有形的服务器存在于一国领土上(即具备被扣押的可能性),国家就有能力控制在其主权领土上的物理硬盘驱动器,进而控制数据。对于互联网公司而言,他们在经过深思熟虑后通过选择服务器的位置来选择适用的法律。对于数据大国而言,对控制者的属人管辖有着传统的属人管辖基础,较易被接受。目前,美国对域外数据的管辖权主要是通过立法扩展至属人管辖实现的。

1. 基于数据控制者的属人管辖

数据的管辖无疑是以其存储地管辖为主。这意味着,只要数据位于该国的领土内,该国就可以合法地主张对该数据的管辖权。《澄清法》通过明确美国对数据控制者的管辖权将域外数据纳入美国的属人管辖。根据该法的规定,无论数据位于何地,电子通信服务或远程计算服务提供商有义务保存、备份或披露有线或电子通信的内容以及该提供商拥有、保管或控制的与客户或用户有关的任何记录或其他信息,这些由在美国的通信服务提供商所拥有、监管或控制的数据,无论是否位于美国境内,美国都要对其进行监管或控制。数据控制者对海外数据的强制披露义务,仅在涉嫌危害美国国家安全的犯罪、严重的刑事犯罪等重大案件时才可适用。同时,该法还对域外数据的管辖情况规定了一些限制条件。值得注意的是,美国对属人管辖的连接点进行了扩大解释,只要被认定与美国有足够的联系,就足以触发美国对海外实体的属人管辖权。②

2. 基于数据主体的属人管辖

在传统的管辖原则中,消极属人管辖与保护性管辖均能够为国家对数据主体的管辖提供法律依据。因此,在立法管辖权方面规定数据主体的国籍国与惯常居住地国行使管辖权并无不妥。《美国金融服务现代化法》《美国健康保险隐私及责任法》《美国电话消费者保护法》均把美国消费者的数据视为保护对象。《澄清法》第 105(a)条将“美国人”定义为合法的美国公民与国民及作

① See Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019.

② See Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019.

为美国合法的永久居民的外国人，还包括非法人的商业协会，其中有主要成员是美国公民与国民或作为美国合法的永久居民的外国人和在美国注册成立的公司。该法还规定只有在数据主体为“美国人”的情况下才对个人数据的控制者行使域外管辖权。

基于美国企业在全球互联网产业中的优势地位，通过强制美国公司存储域外数据很可能将其在全球互联网行业的市场份额转变为美国的数据管辖权，美国的数据管辖权有可能发展成为类似美元霸权的数据霸权。

（二）执法管辖权

正如《重述（第四次）》第 432 条所言，国家主权原则要求在其他国家领土上行使执法管辖权需获得该国的同意，已经成为国际习惯。尽管立法管辖权奉行宽松原则，出现了若干域外管辖，而司法管辖权亦与立法管辖权保持一致，但是执法管辖权仍然以领土为界限，在实践中对域外立法管辖权构成重大限制。《重述（第四次）》第 402 条重申，美国在立法上行使属地管辖权、属人管辖权、效果管辖权、保护性管辖权，普遍性管辖权。但在执法方面，《重述（第四次）》第 402 条规定美国在其领土内行使执法管辖权，仅在其他国家同意的情况下，才能在其他国家的领土内行使执法管辖权。

在《澄清法》出台之前，美国采取查询信件和法律互助条约两种执行模式来获取域外数据。查询信件是一国法院发往另一国法院请求获取域外证据的信件。查询信件曾是国家间共享证据的主要机制。[①] 法律互助条约是 20 世纪 70 年代开始出现的获取域外数据的方式。法律互助条约建立了在刑事事务中跨越国界共享某些证据的标准化程序，[②]确立了以国际法为基础的条约义务。正如美国联邦第二巡回法院在“微软搜查令案”中重申的，美国只能通过查询信件和法律互助条约的方式获取外国同意获取的域外数据。但 2018 年美国国会以查询信件和法律互助条约两种执行模式效率低下为由通过了《澄清法》，从而将《存储通信法》的适用扩张到海外，改变了过去域外数据的执法管辖权需要数据所在国同意的原则。

尽管在传统法律领域，执法管辖权的地域性事实上成功地限制了域外立法管辖权的实现，但是在数据领域，美国可以凭借其在互联网领域的主导地位和国际金融体系的霸主地位，不经数据存储地国的同意即可对域外数据行使执法管辖权。这使传统意义上的领土疆界变得模糊，对执法管辖权限制在本国领土范围内这一习惯法构成严重的挑战。

三、美国域外数据管辖冲突

中间人通常指的是一个第三方环境的控制者，国家通过第三方环境的控制者对处于第三方环境下的个人进行管理。[③] 数据的流动性和互联网的整体性使得跨国互联网公司突破了传统中间人的定位，他们处于政府与数据之间，帮助政府管理数据，同时这些数据巨头也具备了限制政

① See Peter Swire and Justin D. Hemmings, Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program, 71 New York University Annual Survey of American Law, 695 (2017).

② See Treaty between the United States of America and the Swiss Confederation on Mutual Assistance in Criminal Matters, U.S.— Switz., May 25, 1973, 27 U.S.T. 2019, T.I.A.S. 8302.

③ See Alan Z. Rozenshtein, Surveillance Intermediaries, 70 Stanford Law Review, 99 (2018).

府的能力。[①] 根据经济合作与发展组织的定义,数据中间人是指"聚集或促进第三方在网络上进行交易的实体(主要以营利性公司为主)"。[②] 中间人可允许由第三方提供的内容访问、托管、传输和索引,或者在某些情况下,提供基于网络的服务,包括网络服务提供者、搜索引擎、社交平台、电子商务平台、电子支付系统等。[③] 中间人是数据的生产者、控制者或管理者。[④] 世界上最主要的数据中间人为美国公司的事实使美国能够通过控制人标准轻松实现域外数据的执法管辖权,并建立由其主导的全球数据分享机制。

1. 美国对域外数据的管辖侵犯了数据所在国的主权

如前所述,域外数据获取在相当长的时间是通过法律互助条约保证数据来源国的数据主权,但根据《澄清法》的规定,美国可以绕开数据主权国,依据控制者标准通过中间人行使域外执法管辖权。这必然损害其他国家的数据主权。美国通过国内法强制作为中间人的美国公司在美国存储域外数据,并通过扩大解释属人管辖,将全球数据视为其囊中之物,严重践踏了数据来源国的数据主权。这在全球金融数据方面表现得尤为突出。银行间的大部分跨境交易均通过环球银行金融电信协会系统进行,该系统以"每天超过一千一百万笔金融交易的天量成为财务数据的庞大存储库",[⑤]其既是全球金融业的神经中心,又是银行数据的宝库。由于在获取数据和存储数据方面的国际法缺位,[⑥]因此美国通过扩大其属人管辖对环球银行金融电信协会系统的全球数据适用美国国内法,并通过环球银行金融电信协会系统收集域外数据,对数据主体的人权和数据存储国的主权构成了严重的侵犯。[⑦] 美国对全球金融数据的染指使美国的金融制裁成为美国打击目标国威力强大的工具。

2. 美国凭借中间人挑战他国数据主权

即使在早期的互联网时代,国家也已经意识到,要实现数据主权和网络主权,通过监管雅虎、微软、谷歌等这样提供平台服务的中间人会更加有效。因为中间人通常是一个较大的公司,更容易进行管理,从而无须针对每个最终用户采取单独的强制措施。目前中间人已成为国家执法机构的执行代理人,中间人在数据管理过程中扮演了准立法者和准执法者的角色。例如,脸书发布并执行其服务条款协议,推特对仇恨言论行使执法权力,谷歌执行欧洲法院裁决。[⑧] 必须承认,基于网络的整体性和跨国性,网络中间人在网络治理中拥有全球影响力,在网络秩序塑造和维护上有着更重要的地位。在跨境执法的背景下,中间人在确定何时以及如何遵守执法对证据的要

① See Alan Z. Rozenshtein, Surveillance Intermediaries, 70 Stanford Law Review, 99 (2018).

② See OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives, OECD Publishing, 2011, p.11.

③ See OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives, OECD Publishing, 2011, p.11.

④ See OECD, The Economic and Social Role of Internet Intermediaries, OECD Publishing, April 2010, p.9.

⑤ See Walker v. S.W.I.F.T. SCRL, 491 F. Supp. 2d 781, 785—86 (2007).

⑥ See Steven Bellman et al., International Differences in Information Privacy Concern: Implications for the Globalization of Electronic Commerce, 31 Advances in Consumer Research, 362 (2004).

⑦ See Craig T. Beling, Note, Transborder Data Flows: International Privacy Protection and the Free Flow of Information, 6 Boston College International and Comparative Law Review, 591 (1983).

⑧ See Paul Schiff Berman, Legal Jurisdiction and the Deterritorialization of Data, 71 Vanderbilt Law Review, 179(2018).

求方面拥有极大的自由度。[①] 作为数据的生产者、管理者、控制者，中间人可以塑造关键的政策环境。[②] 最具影响力的中间人多系美国企业，中间人权力的上升代表美国在数据监管方面影响力的上升，尽管他们仍必须服从所在地国数据管理规则及其他规则，但是美国可以通过中间人的监管权收集全球数据，并向全球输入其数据管理模式，削弱数据所在国家的管辖权。

无论是脸书还是谷歌、雅虎等互联网巨头都因拒绝向数据所在地国当地执法部门披露数据而发生过争端。[③] 在此类争端中，中间人直接处于冲突的交火地带，中间人的选择即是决定性的。“法国雅虎案”[④]的核心不在于法国对法国雅虎网站的管辖而在于美国雅虎网站。如果仅仅在法国雅虎网站执行法院判决，那么法国人只须转到美国雅虎网站并访问这些页面就可以访问到法国法院要求删除的网页。仅仅关闭法国雅虎网站访问根本无法达到执行法国法律的目的。因此，法国法院要求雅虎禁止访问法国服务器上存储的美国雅虎非法语网站。但雅虎只同意法国法院要求禁止访问法国雅虎网站上的相关信息，并以法国法院的裁决产生了域外效力为由，拒绝在美国雅虎网站履行裁决。雅虎甚至为此诉至美国法院，美国加利福尼亚州北区法院的裁决否决了雅虎执行法国法院的裁决。[⑤] 无独有偶，2017 年加拿大联邦最高法院要求谷歌不仅必须删除在加拿大谷歌网站上销售数据链公司侵犯知识产权的产品的页面，而且还须在所有谷歌的网站上删除这些网页。[⑥] 谷歌向美国加利福尼亚州地区法院提出诉讼，请求法院免除其遵守加拿大法院作出的要求谷歌从谷歌网站搜索结果中删除某些网站的裁决。谷歌表示，加拿大的裁决将加拿大法院置于监督其他主权国家（美国）的执法活动的位置。美国加利福尼亚州地区法院支持了谷歌的请求。[⑦] 美国法院的判决实际上是将美国法院置于了世界法院的地位。在“谷歌西班牙被遗忘权案”[⑧]中，欧洲法院将谷歌视为类行政机构，认为仅仅在谷歌西班牙的网页删除信息是不够充分的，谷歌作为搜索引擎的运营商有义务从根据某人的名字进行搜索后显示的所有结果列表中删除相关信息。但欧洲法院随后在“谷歌法国被遗忘权案”[⑨]的判决中称谷歌没有义务在全球适用欧盟法关于遗忘权的规则。显而易见，域外指控是双向的。如果法国或西班牙无法阻止其公民使用被禁网页，那么美国将有效地对整个世界实施美国法。由于中间人既在欧盟或加拿大范围内有准执法者的身份，在美国等其他国家也有准执法者的身份，因此域外执法管辖权可以通过对这些具有全球影响力的中间人来执行。以上案件表明，中间人的美国身份，使得

① See Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary, 115th Congress (2017).

② 参见解正山：《数据驱动时代的数据隐私保护——从个人控制到数据控制者信义义务》，《法商研究》2020 年第 2 期。

③ See Vinod Sreeharsha, Whats App Blocked in Brazil as Judge Seeks Data, New York Times, May 2 2016; Song Jung－a, South Korean Police Raid Google Offices, Financial Times, August 11 2010.

④ See LICRA v. Yahoo!, Inc., TGI, Nov. 20, 2000.

⑤ See Yahoo!, Inc. v. LICRF, 169 F. Supp. 2d at 1194(2001).

⑥ See Google Inc. v. Equustek Sols. Inc., [2017]1 S.C.R. 824, 826 (Can.).

⑦ See Google Won a Default Judgment on the Grounds that the Canadian Order Violates Section 230 of the Communications Decency Act. Equustek, 2017 U.S. Dist. LEXIS 206818.

⑧ See Google Spain SL v. Agencia Espatiola de Protecci6n de Datos (AEPD), Case C－131/12, ECJ, 2014.

⑨ See Google LLC, Successor in Law to Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), Case C－507/17, ECJ, 2019.

加拿大、法国等国法院关于数据判决的域外效力受到了美国法的限制,而美国法院判决的域外效力却可依仗中间人的美国身份而得以执行。

综上所述,中间人在如何处理客户数据、如何组织业务以及遵守哪些法律规则方面拥有相当大的自由度,他们已经成为政府管理数据的主要实体,在确定互联网政策的主要方面发挥关键作用。国家对数据的主权不仅受到来自中间人的母国域外管辖的威胁,而且受到作为中间人的互联网公司的权力限制。美国借助中间人转变为全球数据的聚集地,直接威胁着其他国家行使主权保护公民隐私乃至国家安全的能力,但这也必然会迫使其他国家为保卫自己的数据主权与之进行抗衡,从而加剧网络与数据的碎片化。

四、美国域外数据管辖的限制

美国对域外管辖的限制通常体现为:在立法上明确域外管辖的条件,在司法上通过法院在审判实践中根据反域外适用推定等原则避免一些极不合理的域外管辖。

(一)传统的限制域外数据管辖的原则

传统的限制域外管辖的原则是由美国法院在多年的司法实践中建立起来的,目前毫无例外地适用于数据领域。

1. 反域外适用推定原则

推定美国法不适用于域外源自美国法的经典思想,即"如果有任何其他可能的解释仍然存在,那么国会的行为不应被解释为违反国际法"。[①]《美国对外关系法重述(第二次)》[以下简称《重述(第二次)》]第 38 条规定,反域外适用推定原则意味着美国的成文法(无论是联邦法还是州法)仅适用于在美国领土内发生的行为和效果发生在美国领土以内的行为,除非相关美国法明确规定了相反的情况。《美国对外关系法重述(第三次)》[以下简称《重述(第三次)》]则因缺乏案例法而未对反域外适用推定原则进行阐述。然而,美国联邦最高法院在 2010 年"莫里森案"[②]中再度启用反域外适用推定原则,强调其仍然是美国法域外适用的核心原则,除在美国国会清楚表明打算将美国联邦法的适用范围扩大到超过美国拥有主权或具有某种程度的法律控制权的地方以外,美国法不具有域外适用效力。[③] 随后,反域外适用推定原则便在涉及包括数据在内的域外管辖问题的案件中得到普遍适用,如"微软搜查令案"即是以适用该原则推定《存储通信法》不能在域外适用的典型案例。《重述(第四次)》重新对反域外适用推定原则进行了阐述。在域外数据管辖问题上,尽管《澄清法》明确规定可以通过控制人标准对域外数据进行管辖,但是同时规定了相应的条件,反域外适用推定原则或可防止美国政府任意扩大对域外数据的管辖权。但值得注意的是,反域外适用推定原则在现实中也推动着美国域外管辖权的扩张。在数据领域,正是美国法院在"微软搜查令案"中适用该原则,导致美国国会出台《澄清法》明确规定了美国对域外数据的管辖权。

---

① See Murray v. The Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804).

② See Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010).

③ See William S. Dodge, Presumption Against Extraterritoriality After Morrison, 105 American Society of International Law Proceedings, 396 (2011).

2. 国际礼让原则

国际礼让原则要求美国法院在解释美国联邦法律规定时考虑对联邦法律适用范围的限制，寻求避免不合理地干涉其他国家主权范围之内的事宜。这种解释本身有助于避免潜在的不同国家间的法律冲突。但如果美国联邦法律的域外适用符合美国的合法利益，那么干涉外国主权便是合理的。该原则通过平衡相互竞争的国家利益而不是仅仅依靠相关活动的地点来确定法律的选择。在关于域外数据的案例中，美国法院必须询问强制被告提交位于域外的数据是否符合数据所在地法律，还须考虑这一行为是否会影响另一国的利益。① 关于外国银行在美国的数据披露义务的案件不在少数，这些案件虽然均围绕国际礼让原则进行了解释，但是有着不同的裁决结果。美国联邦最高法院曾以“遵守（美国法关于）披露银行记录的情况本身即构成违反瑞士法律”为理由，责令地区法院减轻原裁决对不遵守“披露令”行为进行的处罚。② 而在中国三家银行拒绝披露域外银行记录的案件中，美国法院指出美国在朝鲜核武器问题上的重大安全利益以及从中国获取文件的困难程度，使得国际礼让原则难以支持撤销强制披露。③ 可见，衡量强制提供数据证据所损害的另一个司法管辖利益是否超过其所带来的美国利益系国际礼让的关键因素，在实践中这一因素是以分散、逐案的方式判断的，故法官的主观性举足轻重。从实践看，国际礼让原则的适用具有很大的随意性，对美国域外管辖的限制极为有限。

3.一致解释原则

一致解释原则是美国处理国际法与国内法之关系的一项重要原则。④《重述（第二次）》《重述（第三次）》《重述（第四次）》将一致解释原则视为通过司法解释一般性地避免与国际法相冲突的规则，体现了国际习惯法对美国管辖权规则的限制。一般来说，美国法院试图以避免与有关立法管辖权的国际法发生冲突的方式解释联邦法规。同时，美国法院又承认，“如果国会在法案中表明了清楚明白的意图”，那么法院则“必须执行国会的意图，无论该法规是否符合习惯国际法”。⑤ 尽管基于后法优于前法的规则，后来的自动执行条约将优于先前的国会法案，但在实践中，美国尚未缔结过此类条约。⑥ 只要美国国会的意图是清楚明确的，一致解释原则就不会限制与国际法相冲突的国内法的适用。不过，因《澄清法》赋予了美国在其境内对域外数据的执法管辖权，故美国执法机构只要在该法规定的条件下行使，其行为就难以受到一致解释原则的限制。

（二）《澄清法》对域外数据管辖的限制

《澄清法》要求美国公司作为数据控制者在存储美国境内外数据的同时，应考虑基于美国公司在全球数据领域的主导地位。美国掌控来自各国的数据将引起各国对美国数据霸权的恐慌进

① See Linde v. Arab Bank, PLC (Second Circuit), 706 F.3d 98(2013).

② See Societe Internationale pour Participations Industrielles et Commerciales, S.A. v. Rogers, 357 U.S. 197 211－213 (1958).

③ See In re Grand Jury Investigation of Possible Violations of 18 U.S.C. § 1956 And 50 U.S.C. § 1705 (2019).

④ 参见杨永红：《调和中的强制——论欧共体法中的一致解释原则》，《河南师范大学学报》（哲学社会科学版）2007 年第 3 期。

⑤ See Cook v. United States, 288 U.S. 102, 120 (1933) ; Whitney v. Robertson, 124 U.S. 190, 194 (1888); Murray v. The Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804).

⑥ See Section 309(2)of Restatement (Fourth) of The Foreign Relations Law of the United States.

而采取对策限制美国公司的发展,也设定了限制美国适用域外管辖的条件。①

1.《澄清法》下美国获取域外数据的条件

《澄清法》在明确美国能够获取域外电子数据的同时,也为获取域外电子数据设定了门槛,即只有在涉及涉嫌危害美国国家安全的犯罪或严重的刑事犯罪的情形下,美国人和美国公司控制的域外数据才可能被美国执法机构获取。《澄清法》还包含旨在解决潜在冲突的规定,即只有同时满足以下条件,网络服务供应商才可以通过"抗辩"渠道免除披露域外数据的义务:(1)提供商合理地认为搜查令针对的目标不是美国人且不居住在美国;(2)提供商合理地相信披露义务将会导致其实质性地违反"符合资格的外国政府"的立法并因此产生法律冲突;(3)所违反的外国法的国家与美国之间存在数据共享的协议,且该协议获得《澄清法》授权;(4)法院需通过"礼让分析"来决定司法公正的利益是否足以驳回或更改搜查令。对于那些与美国没有数据分享协议的国家,《澄清法》第 103(C)条只保留了普通法礼让原则。如前所述,该原则在数据领域难以限制美国的域外管辖权。

2.《澄清法》下数据分享机制

《澄清法》第 104 条和第 105 条在将美国政府获取数据的权力扩大到全球的同时,还规定了外国政府获取存储在美国的数据的模式。《澄清法》创建了美国主导的国际数据共享安排范式,授权美国与适格外国政府签订行政协议。根据《澄清法》第 104 条的规定,与美国签有授权数据共享协议的外国政府可向美国提出分享数据的要求,服务提供者应外国政府要求披露电子通信的内容,既包括存储的交流信息也包括通过窃听截获的实时通信。对于何为适格外国政府,《澄清法》规定要满足以下两个条件:(1)外国政府必须为隐私权和公民自由提供强有力的实质性和程序性保护,并根据至少 7 个法定因素确定数据收集活动中的公民自由;(2)外国政府已采取"适当的"程序以最大限度地减少有关美国人的信息的获取、保留和传播。根据《澄清法》第 105 条的规定,美国与适格外国政府签订的行政协议还必须保留美国以"无法适当援引该协议"为由拒绝对这类命令适用行政协议的保留权。值得注意的是,美国与适格外国政府签订的行政协议不会解决端到端加密对执法造成的问题,因为只有最终用户才拥有解密能力。《澄清法》要求美国与适格外国政府签订的行政协议保持"加密中立",既不要求解密,也不要求政府在其法律授权的范围内下令解密。② 《澄清法》颁布后,目前仅有英国满足其关于适格政府的要求。2019 年英国在通过《犯罪(海外提交令)法》修改其数据披露规则后,与美国签署了《澄清法》下的行政协议,两国实现了数据共享。③ 澳大利亚在 2021 年 6 月修改相关本国法以达到《澄清法》所规定的条件,目

① See Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019.

② See Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, White Paper, April 2019.

③ See UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019,2021-07-07.

前澳大利亚与美国关于共享数据的合作仍处于谈判中。[①]《澄清法》规定的行政协议是由美国主导的法律合作协议，对合作国家相互之间法律制度的趋同性有极高的要求。无论怎么与美国法趋同，都需要修改本国关于域外数据管辖权的法律。目前，只有英国与美国达成数据分享行政协议的事实表明，《澄清法》下的行政协议模式仅能使极少数国家在严格的条件下获准得到美国控制的相关数据，这样非但无法起到抑制美国数据霸权的作用，反而会使美国将全球数据霸权国内法化。域外管辖权的传统限制规则不仅在过去未能限制美国域外管辖权的扩张，而且也在未来无法对美国的全球数据霸权予以限制。《澄清法》将数据披露控制在刑事犯罪与国家安全的条件下，虽然从表面上看似乎限制了美国政府获取数据的能力，但是美国近年来对“国家安全”概念的泛化模式使美国执法机构能够很轻易地获取域外数据。总之，基于对适格政府的苛刻条件要求，《澄清法》规定的行政协议非但无法在美国数据霸权与他国数据主权之间起到平衡作用，反而使数据国际共享机制美国法化。[②]

五、美国域外数据管辖权的中国应对

美国作为互联网的诞生地在全球网络与数据的权力博弈中处于绝对的优势地位。中国在数据的管辖问题上一直主张数据的属地管辖，坚持数据本地化原则。《中华人民共和国国际刑事司法协助法》第4条第3款明确禁止外国执法机构在中国境内收集数据证据，中国的个人和企业亦不能向外国执法机构提供数据证据。《中华人民共和国数据安全法》（以下简称《数据安全法》）第2条和《中华人民共和国网络安全法》第37条规定了境内重要数据出境的许可制度，并对损害中国国家安全、公共利益或者公民、组织合法权益的数据处理建立了保护性管辖制度。《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》）第3条第2款采取有条件的数据主体属人管辖来保护中国境内个人数据的安全。与美国通过对数据控制者的属人管辖以及对美国人进行扩大解释建立数据霸权不同，中国在强调数据本地化的同时，亦尊重其他国家对本地数据的主权。作为一个新兴的数据大国，中国对域外数据的获取是通过法律合作条约或其他获得数据主权国同意的方式为基础的，凸显了中国对他国平等主权的尊重。由于中国与美国在域外数据管辖权问题上的冲突难以调和且会长期存在，因此中国应积极采取措施以减少美国域外数据管辖权对中国的冲击，保护中国的数据安全和数据产业以及中国企业和个人的权利。

1. 鼓励中国互联网企业扩大全球影响力，提高中国在全球数据市场的份额

美国的数据霸权是基于其互联网企业在全球数据领域的主导地位，因此要削弱美国的数据霸权就应推动中国互联网企业走向全球。目前，中国互联网公司的影响力在很大程度上是基于中国大市场产生的，海外影响力仍有限。因此，中国不能仿效美国通过数据控制者对数据行使管辖权而加入全球数据的争夺战，一旦仿效就将极大地阻碍中国互联网企业在海外的发展。中国

① See Head in the Clouds: Australia Passes US CLOUD Act－style Law, https://www.simmons－simmons.com/en/publications/ckqtoc4gf1n910986tkl6pvio/head－in－the－clouds－australia－passes－us－cloud－act－style－law, 2021－07－07.

② 参见邵怿：《网络数据长臂管辖权——从“最低限度联系”标准到“全球共管”模式》，《法商研究》2021年第6期。

应继续坚持数据属地管辖权,推出符合数据所在地法规和民众需求的数据平台,还可鼓励中国企业收购一些具有发展前景的海外数据平台。同时也要注意与海外实体保持相互独立的关系,避免外国的长臂管辖,保护中国境内的国家数据安全和个人信息安全。

2. 联合新兴国家及发展中国家建立国际数据合作机制

尽管美国的域外数据管辖权侵犯了他国的主权,但是由于缺乏相应的国际法机制,目前难以通过国际规则限制美国的数据霸权。中国可以率先通过与新兴国家及发展中国家达成共识、缔结多边数据管辖方面的条约,反对域外数据管辖及数据霸权,提升在数据管辖方面的国际规则体系构建中的话语权。① 这在限制美国数据霸权方面能起到一定的道义作用,并有助于中国联合新兴国家及发展中国家共同应对美国的数据霸权。

3. 重视美国数据规则中的加密中立

重视美国数据规则中的加密中立,要求美国通信服务提供商在必要的情况下对在中国的数据提供加密服务。由于《澄清法》采取的是“加密中立”的立场,其没有赋予执法部门强制服务提供商解密数据的权力,因此可通过法律强制数据加密来避免美国的数据域外管辖,要求美国法下的“美国人”对中国数据使用加密钥匙且不得留有后门。

4. 评估风险

中国企业和实体以及个人在海外发展时须评估其对中国境内数据安全带来的风险。要注意美国法定义的美国人的范畴远大于拥有美国国籍的人及在美国登记注册成立的公司,还包括“其中有相当数量的成员是美国公民或拥有合法承认的永久居留权的外国人的法人团体,或在美国注册成立的公司”,要注意不慎成为“美国人”后,其在华母公司的数据可能会面临被要求在美国存储并强制披露的风险,从而威胁中国境内数据的安全。

5. 利用美国域外数据长臂管辖的限制规则

中国企业和实体面对美国域外数据管辖时,要充分利用美国域外数据长臂管辖的限制规则。尽管美国域外数据管辖的自我限制在很大程度上出于粉饰其数据霸权的目的,但是当已经面对美国的域外管辖权时,就只有利用《澄清法》对域外数据管辖的限制(包括反域外适用推定原则、国际礼让原则及一致解释原则)规则,争取排除强制披露数据的义务。

6. 完善中国相关的法律以反制美国数据霸权

《数据安全法》第 46 条和《个人信息保护法》第 42 条规定了违法向境外提供数据的法律责任,《数据安全法》第 26 条、《个人信息保护法》第 43 条以及《中华人民共和国反外国制裁法》(以下简称《反外国制裁法》)第 3、4、13 条规定应对针对中国歧视性的禁止、限制或者其他类似措施采取反制措施。《数据安全法》《个人信息保护法》《反外国制裁法》均需要行政法规的落实和施行。既要建立相应的应对及反制机制以防止美国强制中国海外企业和实体非法披露境内数据,也要防止美国通过美国企业侵犯中国的数据主权,要求外国数据的控制者严格执行数据的本地存储并禁止非法披露境内数据。对于美国单方通过域外数据管辖侵犯中国数据主权的行为,中国应依法采取针锋相对、适当可行的反制措施。

① 参见张倩雯:《本地化措施之国际投资协定合规性与中国因应》,《法商研究》2020 年第 2 期。

六、结　语

美国政府通过域外数据管辖权将美国企业铸造成“网络空间的国土”。美国企业在全球互联网行业的市场份额正转变为美国数据主权的域外扩张。[①] 美国中间人在全球数据行业的主导地位使得美国可以在其领土上对域外数据行使执法管辖权。这使得以属地管辖为基础的数据主权面临来自美国域外数据管辖权的严峻挑战。域外数据管辖问题呼唤在数据规制上的国际合作，承认并尊重其他国家对数据的合法利益，接受各国数据监管制度的差异，并在此基础上建立国际数据合作机制，如此才能合作维护网络的整体性及各国的数据主权。中国应继续坚持数据主权原则，积极联合新兴国家和发展中国家，主动参与国际数据合作机制的创立，提升在数据管辖方面的国际规则体系构建中的话语权。同时，采取措施提高中国企业在全球数据领域的竞争力及规则意识，当中国的数据主权遭到美国侵害时，亦应依法进行适当反制，抗击破解美国的数据霸权。

Abstract: The United States has published laws to establish United States jurisdiction over extraterritorial data in terms of data controllers, which turns the domination of American companies in the global data field into extraterritorial jurisdiction of the United States. Although the United States has set certain restrictions on extraterritorial jurisdiction, it cannot avoid conflicts between its extraterritorial jurisdiction and the territorial jurisdiction of the state where the data is located since those restrictions are largely a formality. It seriously threatens the data sovereignty of most countries including China. China shall also actively work with emerging countries and developing states, in order to establish an international data cooperation mechanisms which can countermeasure the United States data hegemony and promote international data governance. Meanwhile, China shall take measures to increase competitive of Chinese companies in the global data market and their spirit of rule of law in order to truly reverse domination of United States data power.

Key Words: data sovereignty, extraterritorial jurisdiction, prescriptive jurisdiction, enforcement jurisdiction, intermediaries, controllers

责任编辑　　何　艳

① 参见洪延青：《美国快速通过 CLOUD 法案明确数据主权战略》，《中国信息安全》2018 年第 4 期。