主题研讨

“法律战”旋涡中的执法跨境调取数据：以美国、欧盟和中国为例

洪延青

内容提要：在行政执法和刑事司法领域，信息技术的广泛应用使得证据材料普遍以电子数据的形式存在。同时，全球化、数字化使得执法跨境调取数据成为必要。执法跨境调取数据主要由两个场景组成：一是执法所需的数据存储于国外；二是外国执法部门需要调取存储于本国的数据。因此，一国政府往往有从境外“取”的需求，也要“防”境外获取。作为数字经济中主要板块的美国、欧盟，对执法跨境调取数据中的“取”和“防”分别从各自的现实需求、产业发展情况、法律传统和总体战略等因素出发，采取了不同的模式。近年来，随着《国际刑事司法协助法》《数据安全法（草案）》《个人信息保护法（草案）》以及相关部门规章的立法推进，我国逐渐形成自己的独特制度风格。通过对美欧中三种模式进行分析和归纳，可以预测三种模式互动可能产生的结果，并分析互动对我国主权、安全、发展利益的影响。

关键词：数据主权　跨境数据　数据调取　数据封阻

洪延青，北京理工大学法学院教授。

在全球化、网络化、数字化时代，出于执法目的跨境调取存储在他国的数据（本文简称为“执法跨境调取数据”）对于任何国家而言几乎都不可避免。[1] 从主权国家的角度来说，执法跨境调取数据主要由两个场景组成：一是执法所需的数据存储在国外，二是外国执法部门需要调取存储在本国的数据。前者要求从境外“取”（本文简称为“取”），后者要求“防”境外获取（本文简称为“防”）。总的看来，我国目前对执法跨境调取数据的态度主要沿袭了前网络时代的传统主权观念，将数据和地理意义上的国境相绑定。然而，

〔1〕 对执法跨境调取数据的一个一般性探讨，参见 Jennifer Daskal, Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues, Vol. 8 (3), *Articles In Law Reviews & Other Academic Journals*, 473 – 502 (2016)。

不论是作为全球互联网产业领头羊的美国还是全球数据立法标杆的欧盟,近期都不乏“绕过他国主权”直接从境外调取数据的立法和实践。必须承认,这样的做法不全然是对他国主权的忽视,也有网络时代下真实的执法需求为支撑。随着我国通过《国际刑事司法协助法》并推进《数据安全法(草案)》立法,相关制度设计意味着我国在执法跨境调取数据之上采取了与欧美截然不同的立场。因此,在理论上梳理和分析中、美、欧三大法域在执法跨境调取数据所采取路径的异同,具有重要而现实的意义。本文就是对此的一个尝试。在思路上,文章将首先从既有实践出发,详细描述执法跨境调取数据中的“取”“防”博弈,然后分别归纳总结美国和欧盟的执法跨境调取数据模式,进而提炼和分析中国所预设的制度安排,最后探讨中美欧三种执法跨境调取数据模式可能的互动,尝试提出维护我国在跨境数据调取制度设计中有关主权、安全、发展利益的相关观点。

一 执法跨境调取数据中的“取”“防”博弈

伴随着人类生活的网络化和数字化,在执法和司法活动中,越来越多的证据呈现为电子证据形式,“电子证据不仅仅是‘入法’获得了独立的证据地位,更是呈现出新一代‘证据之王’的气象”。[2] 但是,网络空间无国界导致电子证据事实上不可避免地包含跨境因素,使得各国在执法过程中面临电子证据存储于境外的难题。

(一)取之有道:跨境数据调取的既有形式

通常来说,不论是本国执法机关调取存储在国外的数据,还是外国执法机构调取存储在本国的数据,均需要通过数据存储地所在国家有权机关的同意和协助,而不能越俎代疱,如此方能体现对主权的尊重。[3] 在国际法框架内存在如下五种典型方式:一是国际公约中包含部分司法协助的条款;二是国家之间签署的司法协助程序;[4] 三是基于互惠原则,以一事一议方式展开具体的司法协助;四是司法协助函,即一国法院向另一国法院提出正式协助请求;五是双多边警务合作。

上述五种形式共同的特征是国家主权充分的参与:公约和司法协助条约的内容由主权国家共同协商,并需要主权国家签署批准;其他形式的协助请求和警务合作,也需要国家有权机关的共同参与和执行。但也正是因为不能“绕过”主权,使其实践存在较高的“门槛”,例如寻求协助的事项必须在被请求国家中也被认定为犯罪、是否提供协助由被请求国家自行决定等。其中既包含出于本国国家安全、重大公共利益等考量,也不免存在非司法方面的考量,例如美国经常抱怨俄罗斯政府鲜少协助美国对俄罗斯网络罪犯进行执法调查。[5]

---

〔2〕 刘品新:《电子证据的基础理论》,《国家检察官学院学报》2017 年第 1 期,第 151 页。

〔3〕 See Maruša T. Veber and Maša Kovič Dine, *Big Data and Economic Cyber Espionage: An International Law Perspective*, Routledge, 2014, p. 11.

〔4〕 See Valsamis Mitsilega, New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data, Vol. 8(4), *European Foreign Affairs Review*, 515 – 536 (2003).

〔5〕 See Roderic Broadhurst, Developments in the Global Law Enforcement of Cyber-crime, Vol. 29(3), *Policing: An International Journal of Police Strategies & Management*, 408 – 433 (2006).

事实上,除了门槛高、需要大量协调合作外,上述五种形式在现实中最大的缺陷在于效率低下。据美国学者研究,外国向美国政府提交法律协助请求,平均的处理时间要耗时 10 个月。[6] 显然,这样的速度完全无法满足执法机关的需求,特别是在瞬息万变的网络时代。

外界的新变化也导致执法机关对司法协助程序愈发不满。随着通信加密技术广泛采用,执法部门在数据传输过程中通过拦截通信方式只能截获无法成功解密的加密数据包,无法获知通信内容,因此,"搜查"通信内容"落地"的服务器、终端、云端成为执法必需,但通信服务提供商出于成本等考虑往往将其部署在境外,客观上加强了执法跨境调取数据的必要。[7] 此外,还存在变换通信工具和渠道的问题。英国副国家安全顾问在美国参议院司法委员会作证时指出,以往,英国警方能够方便地监听英国境内实施恐怖主义的犯罪分子之间的通信内容,但越来越多恐怖分子使用美国通信产品和服务后,英国政府只能向美国通信公司提出获取通信内容的要求,但后者明确表示只能通过双边司法协助程序。[8] 易言之,本地行为人实施的本地犯罪,以往只需通过国内法律程序即可实施监听,但现在因为犯罪分子使用了外国通信产品或服务,却转而需要符合他国法律规定的监听或搜查的"门槛",征得他国司法机关的同意才能调取通信内容。在存在双多边司法协助的情况下,意味着复杂的人力成本和遥遥无期的等待,而如果犯罪分子故意选择那些所谓"犯罪天堂"出品的通信工具,执法几乎完全无法开展。

司法协助程序应对互联网时代的犯罪显得苍白无力,也倒逼执法部门在司法协助程序框架外探索其他方式。随着组织的跨国化和信息化程度越来越高,执法部门发现掌握境外数据的组织如在境内设有总部或分支,便意味着对该组织具有管辖权,由此可以通过境内法律流程和文书,直接要求或强迫组织在境内总部或分支将境外数据"带到"境内。例如巴西法院获取一起有组织犯罪和贩毒案件相关的 WhatsApp 中的通信内容被 WhatsApp 拒绝后,将 Facebook 巴西高管判决入狱。虽然 Facebook 抗辩 WhatsApp 在巴西没有工作人员,且与 Facebook 完全独立运营,不应对此事负责,[9] 但在巴西法院看来,Facebook 全资收购了 WhatsApp,又在巴西本地设立了办公室,如此便可以行使管辖权。

(二)防之有策:封阻跨境调取数据的典型操作

一些国家从境外"取"数据有创新,一些国家也开始在"防"的方面提出针对性措施。最具代表性的操作,当属大陆法系国家的"封阻法令"(blocking statutes),其意在阻断普通法系(主要是美国)的证据开示程序。

---

〔6〕 See Peter Swire and Justin Hemmings, Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program, Vol. 71 (4) *NYU Annual Survey of American Law*, 687 - 740 (2017).

〔7〕 See Peter Swire, From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, Vol. 2(4), *International Data Privacy Law*, 200 - 206 (2012).

〔8〕 See Written Testimony of Mr Paddy McGuinness United Kingdom Deputy National Security Adviser Before the Judiciary Sub-Committee on Crime and Terrorism United States Senate, https://www. judiciary. senate. gov/download/05 - 24 - 17 - mcguinness - testimony,最近访问时间[2021 - 01 - 07]。

〔9〕 See Jonathan Watts, Brazilian police arrest Facebook's Latin America vice-president, The Guardian, 1 Mar 2016, https://www. theguardian. com/technology/2016/mar/01/brazil - police - arrest - facebook - latin - america - vice - president - diego - dzodan,最近访问时间[2020 - 09 - 30]。

证据开示程序是美国民刑事案件中诉讼双方交换证据的司法过程,为了真相能从诉讼双方对抗中浮出水面,法官会支持和保障当事人充分的知情权。因此,美国法庭往往会以命令的形式(例如传票)支持一方当事人获取证据的要求,并且范围十分广泛。[10] 针对存放在境外的文件、数据等情形,早在 20 世纪 70 年代,联邦第二巡回上诉法院就清楚地指出:“如果某一联邦法院对某人具有管辖权,如果该人拥有某文件或对该文件具有控制能力,那法院就有权要求该人提供位于境外的该文件。联邦法院这样的权力毋庸置疑。”[11]刑事诉讼中,美国的判例法长久以来支持检察官通过传票的形式,要求在美国经营的公司交出处于境外的文件、记录等;[12]美国司法部也明确检察官可要求外国银行美国办公室提供位于境外的文件数据,只不过要经过额外的司法部内部程序。[13] 简单来说,在美国法中,能否从境外调取数据最为关键的因素并非数据的存储地,而是诉讼能否在美国进行。如果美国法院具有管辖权,那涉案方就需要提供其所拥有、控制或能够访问的与案件相关的境外文件和数据。[14]

在众多封阻法令的立法中,以法国最为著名,甚至封阻法令的名称即来自法国的立法。1980 年,为了阻止美国针对法国航运公司的反垄断调查,法国通过了专门的《封阻法令》。[15] 该法案第 1 条规定,在没有法国法院命令的情况下,禁止任何法国个人出于提交证据的目的,向境外司法或行政机关披露关于经济、商业、工业、金融、技术方面的信息。法国不是唯一向美国说“不”的国家。德国、英国等许多国家也有类似的封阻法令。例如,英国 1980 年通过《贸易利益保护法案》(*Protection of Trading Interests Act of 1980*),授权国务大臣基于英国主权或贸易利益,可以要求禁止配合外国法院或其他公权力机关的证据开示要求。[16] 此外,也有从客户信息保护的角度实现“封阻”的立法:由于执法跨境调取数据需求经常发生在银行业,各国银行业相关法律中有关客户信息严格保密的规定,也被认为在事实上构成一种封阻法令,例如瑞士、卢森堡、新加坡等国的规定;[17]另外是个人信息保护方面的法律,又以欧盟 2018 年生效的《通用数据保护条例》(*General Data Protection Regulations*,英文简称 GDPR)最为典型。

(三)旋涡中的跨国公司

从跨国公司的角度来说,由于其业务横跨多个国家,便面临着不同国家间的法律冲

---

〔10〕 参见宋冰编:《读本:美国与德国的司法制度与司法程序》,中国政法大学出版社 1999 年版,第 274 - 279 页。

〔11〕 See United States v. First Nat'l City Bank, 396 F. 2d 897, 900 - 01 (2d Cir. 1968).

〔12〕 See In Re Grand Jury Proceedings (Bank of Nova Scotia), 740 F. 2d 817 (11th Cir.), cert. denied, 469 U. S. 1106 (1985); In Re Grand Jury Proceedings (Bank of Nova Scotia), 691 F. 2d 1384 (11th Cir. 1982), cert. denied, 462 U. S. 1119 (1983); In re Grand Jury Subpoena Directed to Marc Rich, 707 F. 2d 663 (2d Cir. 1983).

〔13〕 See Department of Justice, Criminal Resource Manual, https://www.justice.gov/usam/criminal - resource - manual - 279 - subpoenas,最近访问时间[2020 - 09 - 30]。

〔14〕 See Joel R. Paul, Comity in International Law, Vol. 32(1), *Harvard International Law Journal*, 1 - 79 (2001).

〔15〕 See The French Blocking Statute (Law No. 80 - 538 of 16 July 1980).

〔16〕 See Protection of Trading Interests Act 1980, http://www.legislation.gov.uk/ukpga/1980/11,最近访问时间[2020 - 09 - 30]。

〔17〕 See Christopher H. McGrath and Neil J. Schumacher, Beyond Blocking Statutes: Revisiting Foreign Discovery Under the Hague Convention, *Paul Hastings*, 3 February 2015, https://www.paulhastings.com/publications - items/details/? id =719ce369 - 2334 - 6428 - 811c - ff00004cbded,最近访问时间[2020 - 09 - 30]。

突,实践中是否配合执法跨境调取数据的要求,均可能引发法律和经营方面的风险。

一方面,跨国公司面临着法律不确定性,既包括他国执法部门所要调取的数据能否从数据存储地国家自由地向境外流动尚不明确,也包括即便数据能自由地向境外流动,但能否向外国政府披露或用于执法调查可能也并不明确。

另一方面,即便跨国公司满足了境外执法跨境调取数据要求,仍然面临着未来的经营风险。一是满足一国执法部门跨境调取数据的要求,可能引发其他国家执法部门仿效提出同样的要求,[18]由此可能引发法律冲突问题。为了避免法律冲突问题,跨国公司需要在每个国家设立数据中心,保存数据副本以供监管和司法的调取,[19]从成本上看无异于商业上的自杀。二是导致政府信任危机,为了防范跨国公司回应他国数据调取请求,数据存储地国家可能会制定数据本地化立法,并且在数据存储本地化要求之上,渗透至产品和服务的完全本地化。[20] 三是引发用户信任危机,如果用户知道自己的数据可以轻易地被外国政府部门调取,很可能会用脚投票弃用产品或服务。

二 跨境数据调取的美国模式

美国在执法跨境调取数据中"取"和"防"已经形成了相对丰富的实践,尤其是美国国会于 2018 年快速通过《澄清合法使用境外数据法》(*Clarifying Lawful Overseas Use of Data Act*,本文简称"云法案"),体现了美国模式的要旨——将自己的企业变成领土的延伸。这里结合促成该法案推出的 Microsoft Corp. v. United States 一案加以阐述。[21]

(一)《存储通信法案》中的"取""防"规定

《存储通信法案》(*Stored Communication Act*,SCA)是美国执法机构强制个人或企业披

〔18〕 See Andrew Pincus, Why is the U. S. government trying to help Vladimir Putin access information stored in the United States? 9 February 2018, http://www. scotusblog. com/2018/02/symposium - u - s - government - trying - help - vladimir - putin - access - information - stored - united - states/,最近访问时间[2020 - 09 - 30]。

〔19〕 See Matthew Kahn, Microsoft-Ireland Oral Argument Preview: Will the Supreme Court Stave Off Data Localization? Lawfare Blog, 26 February 2018, https://www. lawfareblog. com/microsoft - ireland - oral - argument - preview - will - supreme - court - stave - data - localization,最近访问时间[2020 - 09 - 30]。

〔20〕 "微软诉美国政府"案中,如果美国最高法院决定支持数据控制者标准的话,德国政府便会选择本地化的立场。See Craig A. Newman, Can the United States Search Data Overseas?, New York Times, 26 February 2018, https://www. nytimes. com/2018/02/26/opinion/united - states - searching - data - overseas. html,最近访问时间[2020 - 09 - 30]。

〔21〕 2013 年 12 月,美国纽约南区联邦地区法院签发搜查令,要求微软将一起毒品案件中所涉用户的电子邮件内容和账户信息提交给美国政府。但该用户的电子邮件内容数据存储在爱尔兰,微软拒绝向 FBI 提供,并提出废除搜查令的动议。2014 年 4 月,法院驳回了微软的动议,微软提出上诉。2014 年 7 月,美国纽约南区联邦地区法院作出裁定,支持原裁定。随后,微软向美国第二巡回上诉法院提出上诉。在上诉中,案件各方都认可基于《存储通信法案》的搜查令不适用于域外,但分歧在于:微软认为搜查令仅适用于存储在美国境内而不能覆盖到爱尔兰境内的数据,但政府一方认为搜查令只要求微软在美国境内作出一定的操作,并在美国境内向政府披露数据,搜查令因而没有适用于美国境外。2016 年 7 月,美国联邦第二巡回上诉法院认为,FBI 的搜查令不具域外效力,对于境外数据应当通过双边司法协助条约途径获取。FBI 提出重审申请,并在联邦第二巡回上诉法院拒绝重审后,将案件提交至美国最高法院。2018 年 2 月,美国最高法院就该案第一次开庭审理,但由于云法案的生效,使得案件争议问题已经不复存在,最高法院在 2018 年 4 月驳回该案件。

露私人电子通信数据所依据的主要法律,但其主要在于获取境内数据,并未对境外数据获取给出明确标准。“微软诉美国政府”案中双方的分歧恰恰在于境外存储数据的管辖权问题,直指《存储通信法案》的立法缺失。微软旗帜鲜明地主张数据存储地所在国对数据具有管辖权,本文称之为数据存储地标准;FBI 则坚持无论数据存储地是否在美国,美国均可对微软能够控制的数据具有管辖权,也即基于国家对数据控制者的管辖权而获取由数据控制者所控制的数据,本文称之为数据控制者标准。事实上,两者各有利弊。如坚持数据存储地标准,尊重了数据存储地国家的主权,但会使得调取需求方国家面临执法低效冗余的困境。在此标准下,犯罪分子会选择变换使用外国的通信产品或服务而给侦查带来障碍,抑或跨国公司对数据中心的选址也能够在很大程度上影响侦查的难易程度,由此将会催生“数据天堂”,对国家执法造成阻碍。如坚持数据控制者标准,执法机关通过作用于国内数据控制者“撬动”存储于国外的数据,能够满足执法需求,但也会造成对数据存储地所在国家主权的侵犯,而且会使得跨国公司面临本国与数据存储地所在国之间的法律冲突,引发其海外运营的信任风险,更有可能倒逼各国进行数据本地化立法,最终增大跨国公司的经营成本。

对于防范他国执法机构调取美国境内的数据,《存储通信法案》作出了明确限定。第 2702节规定,电子通信服务和面向公众提供远程计算服务的个人或组织,不得在明知的情况下向任何个人或组织透露该服务所承载通信的内容。[22] 在第 2703 节中,《存储通信法案》将允许通过搜查令等法律流程强迫服务提供者披露内容数据的“政府部门”,[23] 限定为“美国政府的某一部门或机构,或者州政府或更低政治层级的政府”。[24] 因此,《存储通信法案》事实上限定了美国的数据控制者只能向美国政府部门披露信息,当外国政府通过其国内法律程序要求美国的数据控制者向其提交内容数据时,如果美国数据控制者予以响应即属于非法。

总结起来,在从境外“取”的方面,《存储通信法案》的标准尚不明确;在“防”境外拿的方面,《存储通信法案》又有严格的对象限定。

(二)以控制为主导标准的云法案

1986 年通过的《存储通信法案》在回应跨境数据调取需求时,存在“取”之标准不明,“防”之标准严苛的问题。如果不进行法律层面的改革,在“微软诉美国政府”案中,美国最高法院只能从两个不好的选项中做出选择,其结果是要么阻碍政府正当执法,要么极大损害美国企业的全球运营。2018 年 2 月,为针对性改革《存储通信法案》,部分参议员提交了云法案草案,不仅就微软与 FBI 之间的争议提出了解决方案,也为外国执法部门调取存储在美国的通信内容数据提供通道。2018 年 3 月,云法案迅速通过并立即生效,得到了包括微软、苹果、谷歌等在内的许多美国公司的支持。[25]

---

〔22〕 See 18 U. S. C. § 2702.

〔23〕 See 18 U. S. C. § 2703.

〔24〕 See 18 U. S. C. § 2711 (4).

〔25〕 See https://blogs. microsoft. com/datalaw/wp - content/uploads/sites/149/2018/02/Tech - Companies - Letter - of - Support - for - Senate - CLOUD - Act - 020618. pdf,最近访问时间[2021 - 01 - 07]。

1. 对数据控制者标准的确认

云法案明确采用数据控制者标准，规定只要是通信、记录或者其他信息为服务提供者所拥有、监管或控制，无论其是否存储在美国境内，服务提供者均负有依法保存、备份、披露相应内容的义务。从类型来看，服务提供者包括电子通信服务提供商和远程计算机服务提供商；从范围来看，不仅适用于美国企业，而且适用于在美国境内运营的外国企业。应当注意，此处受美国法管辖的企业并不限于在美国成立的企业。美国司法部在云法案白皮书中说明，只要境外的公司在经营活动中与美国存在足够的联系，便足以触发美国法律的管辖权。〔26〕 鉴于美国在全球互联网产业版图中举足轻重的地位，云法案事实上能够将适用触角延伸至全球大多数具有影响力的互联网公司，继而最大限度地扩张美国政府执法调取数据的广度。

与此同时，为缓解数据控制者标准之下服务提供者可能面临的法律冲突，云法案也明确了服务提供者提出抗辩的具体情形：如果服务提供者能够合理证明目标对象不是“美国人”且不在美国居住，并且披露义务将会使其面临违反“适格外国政府”立法的实质性风险，那么可以向法院提出“撤销或变更执法要求的动议”。

对于具体的数据调取执法请求及其抗辩，云法案认可法院的最终裁量权，由法院遵循礼让分析后作出决定。对于礼让分析，云法案明确了其主要的考量因素：一是美国政府的利益；二是适格外国政府禁止披露的利益；三是由于美国与适格外国政府之间的法律冲突而使得服务提供者或其雇员面临处罚的可能性、程度及性质，四是目标对象所处的位置和国籍，以及其与美国联系的性质和程度；五是服务提供者与美国的关联及在美国活动的性质和程度；六是所要求披露的信息对执法调查的重要程度；七是通过其他负面影响更小的方式及时有效地获取所需信息的可能性。整体上看，云法案试图通过利益平衡、比例原则解决跨国公司所面临的法律冲突问题。

2. 外国政府调取美国境内数据

针对他国调取美国境内数据，云法案也通过认定适格外国政府的方式，激励外国政府与美国签订执行协议，并据此直接向美国境内的组织发出数据调取命令。

对于“适格外国政府”的判定，其核心准绳在于“外国立法及执行，是否就隐私和公民权利提供了充分的实质性和程序性保护”。对此，主要基于如下具体因素加以判断：其一，在网络犯罪和电子证据方面，外国政府是否具备充分实质性及程序性法律，如是否加入了《网络犯罪公约》或是否有与该公约第 1 章、第 2 章的定义及要求相一致的国内法；二是是否给予法治和平等原则的尊重；三是是否遵守国际人权保护义务及承诺，并充分尊重国际人权；四是针对数据的收集、获取、使用和共享及其监管，是否存在清晰的法律要求和程序；五是对外国政府收集、使用数据的行为的问责及透明度，存在充分的保障机制；六是展现出对全球信息自由流动和维护互联网开放、分布及互联本质的决心和承诺。

同时，对于“适格外国政府”直接向美国组织发出数据调取命令，也存在较为严苛的

〔26〕 See Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, April 2019, https://www.justice.gov/opa/press-release/file/1153446/download，最近访问时间[2021-01-07]。

限制要求,如应当为获取包括恐怖主义等严重罪行的预防、侦查、起诉相关的数据,调取命令应当限于特定的个人、账户、地址或个人设备,调取命令应当经过法院或其他独立机构的审查等。

(三)美国模式的基本要旨

从“取”的维度看,云法案对于数据管辖权的判定标准在于数据控制者而非存储地,事实上达成的客观效果是美国政府可以经由美国数据控制者直接调取全球数据,仅在数据涉及未在美国境内的非美国人时,才允许服务提供者据此提出抗辩,并由美国法院加以判断。立基于庞大的全球互联网产业背景,叠加云法案精细化的法律制度构建,美国政府的数据调取之手方便地延伸到国境之外,实现了“境内外一盘棋”。从“防”的维度看,云法案也实现了对《存储通信法案》的改革,仅在满足特定条件时,才认可适格外国政府直接向服务提供者调取数据。由此,美国既能够继续对受美国法管辖的企业所掌握的数据保持绝对控制,也可以借机要求意欲直接调取数据的外国政府必须遵守美国式人权和隐私保护基线,并给予美国政府对等待遇。

云法案在“取”和“防”两方面的设计,使得美国政府在事实上将受本国法管辖的企业扩展为自身在网络空间的国土,而上述企业在全球互联网产业版图中拓展到多少国家,美国的数据主权就扩展到哪里。同时,云法案允许适格外国政府“进入”自己的网络领土,以换取美国“进入”适格外国政府的网络领土。云法案在制度设计上充分考虑美国的产业优势和国际空间话语权,最大化保障美国利益。

三 跨境数据调取的欧盟模式

对于既非数据存储地所在国,又非数据控制者所在地的国家而言,会采取何种模式?典型的例子是欧盟。下文将结合欧盟的典型司法判例,提炼出欧盟模式的要旨——将规则的管辖范围扩展到域外,并以整个欧盟单一数字市场作为筹码,使得全球接受其规则扩张,进而在网络空间中变相地延伸了自己的领土。欧盟在执法跨境数据调取中的扩张思路之所以行得通,在于欧盟背靠整个单一数字市场,以约5亿全球相对富裕的人群的消费为筹码,使得跨国企业在进入欧盟市场的同时,“自愿”遵守其规定。

(一)司法判决对于“取”的规定

1. 对受管辖控制者的扩张

在欧盟也曾发生过类似数据调取争议,但采取了截然不同的裁判思路。2010年,比利时执法机关要求Yahoo提供能够识别特定用户的IP地址、电子邮件地址等身份类信息,Yahoo宣称其为美国公司且在比利时境内没有办公室,不受比利时法律管辖。比利时最高法院认为,任何实体“只要积极活跃地将比利时消费者作为其经济活动的主要目标”,即便在境内没有实体存在,也要遵守披露数据的命令;[27]并进一步指出,要求Yahoo

〔27〕 See Cass. 18 januari 2011, nr. P. 10. 1347. N Vol. 8, *Digital Evidence and Electronic Signature Law Review*, 216, 217 (2011).

披露数据的命令并不需要比利时政府向境外派遣执法人员或在境外采取实质性动作,而是由 Yahoo 将数据“带入”比利时境内后向比利时当局披露,因此披露数据的命令并非在境外执行,没有超过管辖权的地域限制。与“微软诉美国政府”案中的美国法院相比,比利时法院更加激进。

目前,与比利时法院判决类似的关于管辖权的理解已经被 GDPR 确立下来,成为欧盟正式的立场。GDPR 第 3 条第 2 款规定,对于在欧盟境内没有设立分支机构的数据控制者或数据处理者,只要其面向欧盟境内的数据主体提供商品或服务(无论是否发生支付行为),或监控欧盟境内数据主体的行为,均要接受 GDPR 的管辖。欧盟委员会新近公布的《数字服务法》草案也遵从了上述思路。[28] 该草案第 2 条规定即便在欧盟未设置机构的信息社会服务提供者,如果“将活动针对一个或多个成员国”,也应当被认为是“在联盟提供服务”并接受管辖。该草案第 31 条进而要求,受管辖的特大在线平台为配合欧盟委员会的调查和执法,需要向欧盟委员会提供与其运营等相关的数据。

2. 对控制者解释的扩张

欧洲法院在谷歌西班牙公司案中进一步扩张了“控制者”的含义。在该案中,谷歌提出谷歌搜索所依赖的索引建立是由谷歌美国总部完成的,因此其受美国法律管辖,而非欧盟法律管辖。但欧洲法院最终判定,谷歌在谷歌西班牙公司主要是“推广和售卖‘美国’谷歌搜索引擎提供的广告空间,而且面向西班牙开展其经济活动”,因此应该受欧盟法律管辖。[29]

欧洲法院对谷歌西班牙的定位进一步扩大解释了“控制者”的含义。欧洲法院确实认同位于美国的谷歌公司为该案中的数据控制者,但是由于谷歌西班牙在西班牙境内活动的最终目的是服务于谷歌引擎和谷歌公司的赢利,因此借着谷歌西班牙在欧盟境内的存在,位于美国的谷歌公司也应被“连带”纳入欧盟法律管辖。

欧洲法院的观点也最终体现在 GDPR 之中。GDPR 第 3 条第 1 款规定,对在欧盟境内设有实体的数据控制者或数据处理者,只要个人数据处理活动发生在此实体活动的场景中,哪怕实际的数据处理活动不在欧盟境内发生,都应受 GDPR 管辖。而只要拥有管辖权,成员国的数据保护机构就自然具备跨境调取数据的权力。

(二)GDPR 对于“防”的规定

在美国最高法院审理“微软诉美国政府”案之前,欧盟向其提交“法庭之友”陈述,清晰地展现了欧盟对于他国调取欧盟境内数据的态度及要求。欧盟认为,在其境内的数据中心存储数据以及从欧盟向美国传输数据都属于 GDPR 规定的数据处理行为。对于“微软诉美国政府”案中的数据调取请求,必须符合 GDPR 第五章“向第三国或国际组织传输个人数据”的规定。

在分析 GDPR 第五章的规定如何适用时,欧盟首先提出,GDPR 第 48 条专门规定了第三国法院判决、仲裁裁决以及行政机构的决定要求数据控制者或处理者进行个人数据

〔28〕 See EU Commission, the Digital Services Act, https://eur - lex. europa. eu/legal - content/en/TXT/? qid = 1608117147218&uri = COM%3A2020%3A825%3AFIN,最近访问时间[2021 - 01 - 13]。

〔29〕 See Google Spain SL & Google Inc v Agencia Española de Protección de Datos (AEPD) & Costeja González.

转移或披露的情形和要求,实质是司法协助的方式。同时,第 48 条的规定也间接说明外国法院或执法机构调取数据并不适用 GDPR 第 45 条至第 47 条所规定的跨境传输的合法事由及情形。因此,在不寻求司法协助方式时,仅得通过符合第 49 条“特定情形下的例外”进行跨境传输。有两种情况可能适用:一是为公共利益而必须传输个人数据的;二是基于数据控制者的“重大的、高于数据主体利益的利益”,而且要求为非反复传输且仅涉及有限的数据主体。同时,数据控制者应基于对传输环境的评估而提供适当安全措施,向监管主体报告传输的发生及向数据主体履行告知义务。最后,欧盟提出,由于第 49 条规定的是例外情形,应结合个案的具体情形严格适用。

由此可见,欧盟对跨境调取欧盟数据的基本观点,仍在于坚持数据存储地原则之下的司法协助方式,“欧盟及其成员国签署了许多可以给美国提供司法协助的国际条约和协定。欧盟希望执法合作所依赖的法律框架能够避免法律冲突,基于持续的对话、自愿的合作、尊重对方对隐私和执法的根本利益”。[30]

(三)电子证据立法建议

2018 年 4 月,云法案生效后不足一个月,欧盟公布《欧洲议会和欧盟理事会关于刑事犯罪电子证据的调取令和保全令的规定的提案》(本文简称“电子证据立法建议”),[31]被国际社会视为欧盟版的云法案立法计划。在谈及立法缘由时,除了执法部门要比犯罪分子更快的客观需求外,欧盟最高司法官员也表示,希望借此增加欧盟筹码,“必须与美国当局达成互惠”。[32]

从内容看,“电子证据立法建议”沿用并确认欧盟既往法院判决和 GDPR 的理解。该建议规定,只要是涉及与欧盟相关的最低三年监禁刑罚的犯罪行为侦查,执法机构就可以调取任何国家公民的个人数据;而所有面向欧盟市场的服务提供者均应当配合执法机构的数据调取命令。具体到存储在境外的数据调取,只要发出调取证据命令的司法机关对刑事侦查具有管辖权限,并且服务提供者确实向欧盟居民提供服务(无论是否在欧盟境内设立了分支机构),便应当向发布命令的成员国提供相应数据。对于法律冲突问题,欧盟采取与云法案类似的态度,允许服务提供者提出撤销调取命令的动议,由成员国法院作出礼让分析。

(四)欧盟模式的要旨

总结起来,从“取”的方面来看,欧盟基本认同数据控制者标准,但针对数据控制者不在欧盟境内的情形采取了两类措施:一是境外数据控制者有意识地针对欧盟提供服务,即应接受欧盟管辖;二是对数据控制者及其分支机构做紧密联系,如欧盟境内分支机构相关活动场景能够囊括发生在境外的数据处理,则境外真正进行数据处理的控制者也应接受欧盟管辖。由此,欧盟在网络空间中变相地延伸了自己的领土。从“防”的方面来看,欧盟还是坚持地域的概念,并且坚持的是借助扩张解释加以延伸后的领土。结合“取”和

〔30〕 See United States v. Microsoft Corp., 584 U. S. (2018).

〔31〕 See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters, https://eur - lex. europa. eu/legal - content/EN/TXT/? qid = 1524129181403&uri = COM:2018:225:FIN,最近访问时间[2021 - 01 - 07]。

〔32〕 See Julia Fioretti, Europe Seeks Power to Seize Overseas Data in Challenge to Tech Giants, Reuters, 26 February 2018.

“防”两方面,欧盟在网络空间中变相地延伸了自己的领土,远远超过真实的欧盟地理领土;而欧盟在网络空间中领土有多大,对领土形式的主权就覆盖到哪里。

四 跨境数据调取的中国方案

与美、欧的“锐意进取”形成鲜明对比的是,我国坚守传统地域管辖的主权原则,强调对于发生在领土之外的事项应当采取主权合作的路径。

(一)我国执法跨境调取数据法律框架

对于境外调取我国境内数据,我国历来强调应当尊重国家主权,通过司法协助方式获取。这也是我国拒绝加入《网络犯罪公约》的原因所在。该公约第 32 条规定的通过互联网直接获取境外电子数据的取证方式,一直被我国视为侵犯他国主权的行为。出于维护国家主权和安全的考虑,我国一直拒绝加入该公约,并选择在联合国层面推动形成新的网络犯罪国际条约。〔33〕

对于我国涉外刑事案件中取证问题,在《国际刑事司法协助法》颁布前,主要由最高人民法院、最高人民检察院、公安部借助电子证据和网络犯罪相关司法解释加以推进。2005 年,公安部在《计算机犯罪现场勘验与电子证据检查规则》中对“远程勘验”作出规定;2014 年,前述三机关联合发布《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》,明确无法获取位于境外的原始存储介质的,可以提取电子数据;2016 年,前述三机关联合发布《关于办理刑事案件收集提取和审查判断电子证据若干问题的规定》,其中第 15 条明确规定对于无法扣押位于境外的原始存储介质的,授权公安机关通过网络在线提取电子证据,允许公安机关进行网络远程勘验。从其内容实质来看,与《网络犯罪公约》第 32条规定十分相似,也即我国相关规范及实务与外交部门的立场存在冲突。〔34〕

2018 年 10 月,《国际刑事司法协助法》通过,将我国涉外刑事司法协助上升至法律层面。就执法跨境调取数据而言,该法第 4 条规定:“非经中华人民共和国主管机关同意,中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和本法规定的协助。”全国人大对其说明时明确提及,该条的增加在于应对实践中有外国司法执法机关未经我国主管机关准许要求我国境内的机构、组织和个人提供相关协助的情况,应抵制外国的“长臂管辖”要求。〔35〕

在《国际刑事司法协助法》通过后不久,公安部发布《公安机关办理刑事案件电子数据取证规则》,相较于前述三机关的规范,最大的不同在于通篇不见“境外”字样,由此产生了该规则是未对“境外”电子数据取证作出规定,还是禁止通过单边方式进行电子数据

〔33〕 参见胡生健、黄志雄:《打击网络犯罪国际法机制的困境与前景——以欧洲委员会〈网络犯罪公约〉为视角》,《国际法研究》2016 年第 6 期。

〔34〕 参见梁坤:《跨境远程电子取证制度之重塑》,《环球法律评论》2019 年第 2 期。

〔35〕 参见《全国人民代表大会宪法和法律委员会关于〈中华人民共和国国际刑事司法协助法(草案)〉审议结果的报告》,http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-10/26/content_2064519.htm,最近访问时间[2020-09-30]。

取证的分歧。从对该规则的篇章结构和具体条文的体系解释来看,该规则事实上修正并废止了前述三机关文件对于境外数据进行远程勘验的规定。一方面,该规则是刑事案件电子数据取证规则的全面规定,从其章节来看完整覆盖了电子数据取证的全部流程和方方面面,难以认为是有意忽略境外电子证据取证的实践及规范;另一方面,该规则第 23 条的具体规定中明确提及了“境内”的限制规定,也反向说明其制定考虑了数据跨境调取的问题,而之所以未提及境外,原因在于借此将我国此前刑事案件电子数据取证问题修正到国际刑事司法协助的法律框架之下。同时,该规则第 61 条特别指出“公安部之前发布的文件与本规则不一致的,以本规则为准”,足见该规则代表了我国电子数据取证最新的立场和要求。

(二)我国的基本立场

不论立法还是实践,不论是“取”还是“防”,我国对执法跨境调取数据的基本立场均是强调主权不容侵犯,坚持应通过主权国家之间的平等互惠合作来开展。2020 年 7 月,《数据安全法(草案)》对外公开征求意见,其中第 33 条也与《国际刑事司法协助法》第 4 条一脉相承。虽然该法还未正式通过,但足见我国对前述基本立场的坚守。简言之,在面对执法跨境调取数据的利益考量时,我国在国家主权、安全和发展利益的平衡之上,更多地是遵循“防守”策略,考虑国家主权和安全利益。

五　中美欧三种模式互动的推演和分析

当下,美国和欧盟分别采取了“扩张式”的执法跨境调取数据模式,而我国强化“防守”模式,以此对抗美、欧的“长臂”。这样的模式互动在多大程度上符合我国的主权、安全和发展利益呢?

首先,在美欧坚持扩张、我国坚守传统地理边境的背景下,我国很可能需要坚持或采取更加彻底的“防御”措施:除了从立法上要求位于境内的组织或个人需经主管部门批准后方可回应境外执法跨境调取数据需求外,还可以进一步促使外资组织或个人无法成为美欧法律意义上的数据控制者。以云服务为例,目前外资云服务提供商如微软、亚马逊等均是以技术合作方式进入我国市场。云法案通过后,该模式被认为是抵挡美欧长臂调取数据的有效方式,因为微软和亚马逊均非数据控制者。从主管部门的角度来看,严控境内企业回应数据跨境调取申请的审核和批准,实际上是将压力传导并集中于主管部门,而通过立法或监管在数据控制者标准上做文章,看似更为有效和简便。按照这个思路,云业务管理的模式应当扩展到可能涉及美欧数据跨境调取的各个业务,但也会产生其他连带的影响,例如与我国加大改革开放力度、放宽境外主体市场准入限制的政策相违背,也会给外国政府和企业批评我国“保护主义”的额外口实等。

其次,采取“进攻”态势的各方反而更可能达成妥协,正如欧盟提出“电子证据立法建议”时表态意图与美国达成互惠一般。在云法案通过后,英国已经与美国达成云法案框架下的双边协议,澳大利亚也正在积极地和美国洽谈之中。随着与美谈判和妥协的增加,一旦达成更广泛的协议,不仅我国被排除在规则制定之外,诉求不会被吸纳,还会造成对我国更为巨大的政治压力。届时,我国原先采取的防御措施将难以为继,或只能再次加码。

最后,是对我国网信企业出海造成的影响。在“取”与“防”的矛盾越来越激烈的局势下,我国网信企业出海所遭遇的跨境执法调取数据冲突会呈上升趋势,而企业在中美欧不同模式的对冲之中,最佳策略只能是将数据本地化存储,甚至将同一个产品切割为国内版和国外版,分开存储中外用户的数据并限制国内外用户交叉注册,以避免法律冲突,例如我国腾讯的微信和 WeChat,字节跳动的抖音和 TikTok 等。但如此客观上造成了我国网信企业无法“全球统一部署”,更无法利用全球数据更新或升级服务,限制了规模效应的发挥。未来一旦美国和欧盟达成协议,至少美欧企业能够避免因法律冲突问题而采取数据本地化及切割运营的方式,可能将我国出海网信企业置于不利的局面。

有鉴于此,仅仅采取防御策略并非最佳出路,我国应当将单边式应对的压力,疏导到多边的框架下解决问题。习近平主席在联合国成立 75 周年纪念峰会上发表讲话时强调:“单边主义没有出路,要坚持共商共建共享,由各国共同维护普遍安全,共同分享发展成果,共同掌握世界命运。”〔36〕执法跨境调取数据的制度设计也应如此:每个国家都有自身不同的核心价值观和选择,任何解决方案都应当以彼此尊重主权为前提;同时,在数字服务市场全球化的今天,这一问题不仅关涉执法行动与违法犯罪行为之间的效率比较,也关涉到本国和他国跨国公司的全球运营,面对国内国外两个大局,没有任何一个国家能够单独解决这一问题,最终解决还应当回归到国际合作的模式。目前,我国提出的《全球数据安全倡议》便是在这方面的一个努力。

同时,我们也应当认识到,当前的全球政治形势使得包括网络安全、数据跨境流动等在内的互联网全球治理议题,难以在短时间内形成合理秩序和健全规则。此时,我国可以优先考虑探索一定范围的多边(如“一带一路”倡议)或双边方案(如明确双方相互认可的侦查措施等),在此前提下推进我国所缔结的司法协助条约进行升级改造,提升彼此的协作效率,尽可能回应司法实践诉求,同时也缓解我国企业出海压力,做到对我国网信企业出海的利益兼顾。

此外,面对美欧的扩张式立法,我国可通过强调数据安全的方式,应对执法跨境调取数据。《数据安全法(草案)》《个人信息保护法(草案)》已经明确有关组织、个人应当经主管机关批准后方可向境外执法机构提供存储于境内的数据,在后续立法过程中,还应进一步明确具体在申请、审核、批准等方面的法律程序和时限,与数据出境安全评估之间的关系和协调,以及违反该义务的法律责任等。同时,主管机关应在后续实施过程中采取坚持原则但灵活处理的态度,在维护我国数据主权的同时,避免对我国网信企业在海外的利益造成不利影响。

六 代结语:从发展的角度看待数据主权

在跨境执法调取数据方面,我国目前所坚持的传统主权观,实际上是基于整体国际形

〔36〕 习近平:《在联合国成立 75 周年纪念峰会上的讲话》,http://www.xinhuanet.com/world/2020-09/22/c_1126522721.htm,最近访问时间[2020-09-30]。

势和维护我国整体的主权、安全和发展利益的需要,在一个具体领域作出的基本选择和判断。对于干涉内政的侵犯主权行为,自然要针锋相对地“防御”。但在坚持局部服从于整体的同时,是否可考虑数字经济领域的特点,将原则性和灵活性相结合以动态地维护我国的数据主权?

相对于领土,数据不可避免地发生跨境流动。哪个国家能吸引更多的数据流入,就能控制更多的数据。因此,数据主权不仅仅是指保障一国政府对其管辖区域内数据的控制性权力,还应包括增强一个国家(包括其管辖的组织和个人)对(境内外)数据的掌握程度和处理利用能力。维护我国的数据主权,应同时考虑如何让我国企业能够在全球范围内掌握、利用更多的数据;毕竟,美国之所以能够将“手”伸到全球,依赖的正是其遍布世界的企业。

在丰富了数据主权内涵的基础上,笔者建议,在数字时代坚持传统的主权观念和多边主义的同时,如何为我国互联网企业出海以及“全球一体化运作”创建良好的数据流动秩序,也应当成为我国选择执法跨境调取数据模式的重要考量之一。

[本文为作者参加的2018年度司法部重点课题“大数据与网络安全立法研究”(18SFB1005)的研究成果。]

[**Abstract**] In the field of administrative and criminal law enforcement, the widespread use of information technology has made it common for evidentiary materials to exist in the form of electronic data. At the same time, globalization and digitization make it necessary for the cross-border access to data for law enforcement purposes, which exists in two main scenarios: first, when the data needed for domestic law enforcement in that country happens to be stored abroad; and second, when foreign law enforcement agencies need to access data stored in that country. Therefore, a government often has the need to “take” data from abroad and “prevent” data from being taken by foreign governments. As major players in the digital economy, the U. S. and EU have adopted different models of “taking” and “preventing” regarding the cross-border data access for law enforcement purposes on the basis of their respective practical needs, industrial development, legal traditions and overall strategies. In recent years, with the advancement in the making of the International Criminal Justice Assistance Law, the Data Security Law, the Personal Information Protection Law and related departmental rules, China is gradually developing a legal system of cross-border data access for law enforcement purposes with its unique style. This paper analyzes and summarizes the three different models of cross-border data access for law enforcement purposes, namely the US model, the EU model and Chinese model, predicts the possible results of the interactions between the three models, and analyzes their impact on China’s sovereignty, security, and development interests.

(责任编辑:田　夫)