

“数据控制者标准”取证模式及中国因应

陈 爱 飞^{*}

摘 要:“数据控制者标准”取证模式是以“数据的实际控制者”为属人连结点来确定跨境数据管辖权的模式,其指向的是跨境网络服务提供者控制的能够作为证据的各类境外数据。该模式正将跨境数据取证由以“数据本地化”为表现形式的属地原则转向以“数据控制者”为核心管辖要素的属人原则。基于“数据控制者标准”取证模式直接向数据控制者调取境外数据的特点,该模式极易引发其与包括我国在内的采用“数据本地化标准”国家之间的数据主权冲突。“数据控制者标准”取证模式与我国相关程序法和数据保护法相抵牾,而我国阻断法在应对境外数据强制调取时发挥的制约作用有限。我国可尝试采用“以数据本地化标准为主,以数据控制者标准为辅”的策略,在尊重主权差异与国际礼让的基础上,实行对等原则基础上有限度的数据出境。同时,充分发挥阻断法的作用,以消减“数据控制者标准”取证模式对我国的不利影响。

关键词:数据控制者标准 跨境取证 数据主权 证据开示 阻断法

2022年6月,美国联邦北加州地方法院在“益华公司诉新拓尼克(北京)公司案”^①(以下简称“益华案”)的裁决中认为,美国法院的证据开示命令与《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13条、第38条、第39条的规定并不冲突,驳回了被告请求重新审议的动议。在本案中,双方针对《个人信息保护法》相关规定能否豁免证据开示命令进行了辩论,在听取双方的辩论意见之后,法院作出要求被告方履行证据开示命令的裁定,从而产生一种《个人信息保护法》不限制美国法院域外证据开示制度的外在观感,但实际上这与《个人信息保护法》的立法意旨和跨境诉讼取证规范相违背。“益华案”是美国法院首次在司法实践中解释与应用《个人信息保护法》的案例。随着跨境数据取证的频繁化,未来同类型案例将不断增加。那么,为应对境外强制性的数据调取命令,我国应如何在跨境数据取证方面予以回应就成为我们不得不关

^{*} 中南财经政法大学法学院副教授、数字法治研究院研究人员
基金项目:国家社会科学基金资助项目(21CFX030)

^① See Cadence Design Systems, Inc., Plaintiff, v. Syntronic AB, et al., Defendants, United States District Court Northern District of California, Case No. 21-cv-03610-SI (JCS), Order Denying Motion for Reconsideration, Re: Dkt. No. 137.

注的问题。

跨境诉讼中的数据取证关涉一国的数据主权,如果数据被非法调取或非法出境,那么将可能对国家安全、数据安全、个人信息保护构成严重威胁。从主权国家角度看,跨境数据取证主要表现为两种形式:(1)本国需要调取的数据存储在国外;(2)外国需要调取的数据存储在本国。^① 本文的研究对象主要为后者,然而,面对美国与欧盟“数据控制者标准”取证模式的外在压力,我国仍未形成有效应对策略。有鉴于此,本文主要从以下方面展开:(1)在阐明“数据控制者标准”基本内涵之时,揭示“数据控制者标准”的理论基础和其在取证环节的适用特点,以及美国与欧盟的具体方案;(2)分析上述模式在取证环节适用时可能对我国产生的多重挑战;(3)探索“以数据本地化标准为主,以数据控制者标准为辅”的应对方案,着力化解境外“数据控制者标准”取证模式可能产生的数据主权冲突,消解证据开示等制度与我国相关制度之间的抵牾,并将阻断法作为境外执法或司法机关、我国当事人、案外人等主体在跨境数据取证领域的平衡点。

一、“数据控制者标准”取证模式的理论基础与域外方案

(一)“数据控制者标准”取证模式的理论基础

当前,全球各国关于数据管辖主要有“数据本地化标准”与“数据控制者标准”之分。前者又被称为“数据存储地标准”,主要是以数据实际存储的物理空间来确定何者享有管辖权。但在云计算技术的影响下,用户与数据之间的联系被不确定化,我们无法像以前确定电子数据的硬件存储设备一样准确识别数据存储地。^② 简言之,“数据本地化标准”难以适应云空间数据的取证需求,这就使“数据控制者标准”的适用呈现出扩大化趋势。^③

首先,需要厘清“数据控制者标准”取证模式的法律机理。该模式是以“数据的实际控制者”为属人连结点来确定跨境数据的管辖权,其指向的是跨境网络服务提供者控制的能够作为证据的各类境外电子数据。一方面,就法理基础而言,在本质上,“数据控制者标准”取证模式是将跨境数据取证由以“数据本地化”为表现形式的属地原则转向以“数据控制者”为核心管辖要素的属人原则。^④ 另一方面,就运行机理而言,“数据控制者标准”取证模式通过向数据控制者施加一定的证据提出义务,要求其按照执法或司法部门的命令提供其掌握的境外电子数据。在该模式中,数据控制者的协助义务替代了原来的司法协助,从而创设出一种可以不经司法协助或外交途径即可获取境外电子数据的新型取证模式。此外,该模式还尝试重新界定数据主权,意在突破数据主权的属地边界,将其延伸至技术边界,从而规避数据存储地的数据管辖权。以我国为例,在跨境数据取证领域可表现为,他国可以通过“数据控制者标准”向我国取证,而我国却不能通过“数据本地化标准”向他国取证。此时,我国作为采用“数据本地化标准”的一方明显居于弱势地位。

^① 参见洪延青:《“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》,《环球法律评论》2021年第1期。

^② 参见吴玄:《云计算下数据跨境执法:美国云法与中国方案》,《地方立法研究》2022年第3期。

^③ 参见孔庆江、于华溢:《数据立法域外适用现象及中国因应策略》,《法学杂志》2020年第8期。

^④ 参见刘品新:《跨境电子取证的欧盟方案及启示》,《国家检察官学院学报》2022年第5期。

其次,“数据控制者标准”在取证环节的适用具有多重特点。具体而言:其一,该标准将数据控制者作为跨境数据取证中的一项关键节点,甚至可称之为具体取证环节的直接行为人;其二,数据控制者有义务依法保存和披露其控制的境外数据;^①其三,执法或司法机关可通过向数据控制者发出提供证据的命令来获取对方控制的境外数据;^②其四,该标准对数据的司法管辖权进行了扩张,直接表现为诉讼所在国的执法或司法机关能够在无须经过他国同意的情况下获取其国内的数据。当然,在不同地区,“数据控制者标准”取证模式可能呈现出不同的样态。譬如,美国是以《澄清数据的合法境外使用法》(以下简称《美国云法》)为主,加上其既有的证据开示制度,从而形成独具美国特色的跨境数据取证模式,欧盟则体现为欧洲调查令、欧洲出示令与欧洲保全令^③。但无论何种样态,它们在取证环节适用时均具备以上基本特点。

最后,“数据控制者标准”取证模式与常态性跨境司法协助模式存在较大差异。(1)在规范依据层面:前者的依据通常是国内法(美国)或者区域内的统一法(欧盟),后者则主要依据国际性或区域性取证公约以及双边或多边司法协助协议。(2)在对国际礼让原则的遵守层面:前者选择绕过数据本地化与属地原则构筑的主权屏障,使礼让分析名存实亡;而后者则充分遵循了国际礼让原则的基本要求,即使无法通过公约或双边条约调查取证,也依然还有外交途径可供选择。(3)在取证方式层面:前者可强制性调取他国境内的数据,且采用该模式的国家往往也不认可常态性跨境司法协助模式具有强制性,其既非获取境外数据的强制方式,也非唯一方式,当事人仍然可以根据国内法获取跨境数据。后者是在充分尊重他国主权的基础上,通过司法合作的方式来调和不同司法辖区之间的法律冲突,协调各国法律体系在取证方面的差异。例如,根据《关于从国外调取民事或商业证据的公约》(以下简称《海牙取证公约》)关于跨境取证的程序要求,缔约国司法机关应当向另一缔约国的司法当局呈递请求书,只有这样才能在他国获取证据。^④ 此为依据《海牙取证公约》获取跨境数据的主要方法,在这种情况下,适用数据接收者所在国家或地区的法律。然而,若选择绕开常规的跨境司法协助模式,而以本国法规定的“数据控制者标准”取证模式代之,则存在损害他国数据主权的风险。

(二)“数据控制者标准”取证模式的美国方案

美国不仅在互联网数据流动方面主张“世界主义”,而且主张通过“数据控制者标准”来解决域外数据取证问题。^⑤ 譬如,在中国对跨境数据取证存在限制的情况下,美国法院依然可以对相关的我国当事人行使管辖权,最为典型的是与其证据开示制度相配合,强制要求提供相关数据。但除非国家间有司法互助协议且经过承认与执行程序,否则其他国家的司法机关、数据保护机构

① 参见刘品新:《跨境电子取证的欧盟方案及启示》,《国家检察官学院学报》2022 年第 5 期。

② 参见梁坤:《基于数据主权的国家刑事取证管辖模式》,《法学研究》2019 年第 2 期。

③ 欧洲出示令是由一个成员国的执法机关向在欧盟范围内提供服务的网络服务提供者签发的一项具有约束力的决定,命令其提交电子证据。欧洲保全令是由一个成员国的执法机关向在欧盟范围内提供服务的网络服务提供者签发的一项具有约束力的决定,命令其保全电子证据以便事后进行提交。See Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings, Art. 3(1), Art. 3(2).

④ See Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 231.

⑤ 参见杨永红:《美国域外数据管辖权研究》,《法商研究》2022 年第 2 期。

并不认为美国法院的裁决对其国内当事人产生约束力。事实上,《美国云法》是美国“数据控制者标准”取证模式之基石,其使美国的域外数据取证由“数据本地化标准”转向“数据控制者标准”,^①试图以“数据控制者标准”构建单边性跨境数据获取规则。^②但实际上,《美国云法》规定的是两种标准,即对境外数据采用“数据控制者标准”,对境内的数据则采取“数据本地化标准”。^③《美国云法》改革了美国当前的司法互助程序,其可以绕过数据所在国主管部门直接向数据控制者提出数据取证,这明显不符合对等原则的意旨。虽然美国有对于适格外国政府实施互惠对等原则的规定,但其往往通过对外国政府的适格性条件审查拒绝协助他国进行数据调取,实质上也不符合对等原则的内涵。^④

事实上,早在2011年12月,美国塞多纳会议第六工作组就已经发布《关于开示、披露与数据保护的塞多纳国际原则(2012)》(以下简称《塞多纳国际框架与原则》),其在最大限度地同时遵守外国数据保护法和美国数据披露义务的基础上,确立了6项与跨境数据取证相关的基本原则。^⑤不过,随着《美国云法》的施行,《塞多纳国际框架与原则》的适用空间被极大地压缩,从近几年美国法院对外国当事人或案外人发布的域外证据开示命令来看,《美国云法》已成为第一选择,几乎看不到《塞多纳国际框架与原则》的身影。

(三)“数据控制者标准”取证模式的欧盟方案

2023年7月以来,欧盟在跨境数据取证领域同样确立了“数据控制者标准”,最为典型的是欧盟成员国相关部门能够利用欧洲出示令与欧洲保全令来突破电子数据存储的物理空间,直接向跨境网络服务提供者(即数据控制者)获取数据。根据2023年《欧盟关于刑事诉讼中和刑事诉讼后执行监禁判决时电子证据的欧洲出示令和欧洲保全令第2023/1543号条例》(以下简称《欧盟电子证据条例》)“鉴于”部分第18项的规定,在根据本条例进行刑事诉讼后,可通过欧洲出示令或欧洲保全令强制欧盟范围内的服务提供商出示或保全电子证据。^⑥

在欧洲出示令与欧洲保全令出现之前,欧盟成员国一般是通过签发冻结令或证据授权状、司法协助委托书等方式获取境外数据的,^⑦但此种方式存在效率低下与难以契合司法实践等问题。迫于欧盟内部取证制度变革的需要与外在压力,欧盟一直在尝试对其跨境数据取证方式进行修

① 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。

② See Andrew Keane Woods, Litigating Data Sovereignty, 128 Yale Law Journal, 328-407(2018).

③ 参见梁坤:《美国〈澄清合法使用境外数据法〉背景阐释》,《国家检察官学院学报》2018年第5期。

④ 参见唐彬彬:《跨境电子数据取证规则的反思与重构》,《法学家》2020年第4期。

⑤ See Jayne Rothman, Alison Wisniewsk, M. James Daley & Laura Clark, Stormy Digital Weather Ahead: The Forecast for Cross-Border eDiscovery in the Context of Litigation and Regulatory Investigations, 7 International In-House Counsel Journal, 1-15(2013).

⑥ See Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2023_191_R_0002, 2024-02-03.

⑦ See Marcello Daniele, Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles, 6 New Journal of European Criminal Law, 180(2015).

改。^①除了 2014 年《欧盟关于刑事案件中欧洲调查令的指令》规定的在跨境电子取证中适用欧洲调查令之外,^②欧盟积极推动制定了跨境数据取证条例,至 2023 年终于达成初步框架。毕竟在欧盟看来,《美国云法》不仅有损害数据所在国主权之嫌,也与欧盟《通用数据保护条例》等规范的要求相悖。2023 年 1 月 25 日,基于欧盟成员国之间的相互信任,欧洲议会与欧盟理事会就与跨境数据取证相关的欧洲刑事案件电子证据出示令与保全令条例草案文本达成合意。^③2023 年 7 月 12 日,欧洲议会与欧盟理事会正式通过了《欧盟电子证据条例》。与欧洲调查令相比,欧洲出示令与欧洲保全令的最大优势是能够绕过数据所在国的相关主管部门,直接向网络服务提供者发出关于出示、保全证据的命令。换言之,《欧盟电子证据条例》旨在赋予成员国执法或司法机关利用欧洲出示令与欧洲保全令直接向其他成员国的数据控制者获取数据的权力,这也是欧盟向国际社会提供的一种新型跨境数据取证机制。

本质上,《欧盟电子证据条例》确立的境外数据获取模式与《美国云法》确立的“数据控制者标准”在原理上存在共通性。^④从表面上看,二者均规定执法或司法机关可以直接向网络服务提供者收集其控制的数据,但实际上这反映出欧盟与美国在跨境数据取证领域正在逐渐放弃“数据本地化标准”而转向“数据控制者标准”。可以预见的是,与《美国云法》一样,《欧盟电子证据条例》创设的“数据控制者标准”取证模式将对全球范围内的跨境数据取证机制产生重大影响。

二、“数据控制者标准”取证模式对我国的挑战

目前,我国尚未形成与跨境诉讼数据取证相关的全面性解决方案,全球各国的法规也呈现出迥异且分散之态势。若境外执法或司法部门欲通过“数据控制者标准”获取我国境内的数据,则可能在取证环节产生数据主权冲突。尤其是在与该模式极为契合的证据开示制度的共同作用下,矛盾显得更为突出。^⑤同时,我国现行阻断法在应对境外强制性的数据取证命令时所发挥的制约作用有限。

(一)“数据控制者标准”取证模式可能产生数据主权冲突

在跨境诉讼领域,若以“数据控制者标准”作为数据出境与调取的主要方式,则可能损害他国的数据主权。直言之,建立在“数据控制者标准”基础上的跨境数据取证模式极易导致与被取证国的数据主权冲突。

^① 参见刘品新:《跨境电子取证的欧盟方案及启示》,《国家检察官学院学报》2022 年第 5 期。

^② 根据《欧盟关于刑事案件中欧洲调查令的指令》第 32 条的规定,任一成员国的签发机关都可以通过特定的中央机构签发欧洲调查令的方式与另一成员国的执行机关进行直接合作。

^③ See Electronic Evidence: Council Confirms Agreement with the European Parliament on New Rules to Improve Cross-Border Access to E-evidence, <https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/>, 2024-02-03.

^④ 参见刘品新:《跨境电子取证的欧盟方案及启示》,《国家检察官学院学报》2022 年第 5 期。

^⑤ 根据《美国联邦民事诉讼规则》第 26—37 条关于证据开示制度的规定,当事人或案外第三人所掌握的事实材料,只要与案件有关,除享有秘密保护特权外,就都应向对方当事人披露,任一方当事人都享有要求对方当事人及诉讼外第三人披露上述事项的权利。

首先,数据主权是由网络空间主权衍生而来,与之相关的跨境诉讼数据取证案件易引发对是否损害国家数据主权的担忧。^①一方面,我国作为坚持“数据本地化标准”的国家,若他以“数据控制者标准”取证模式强行调取我国境内的数据,则显然不符合我国的主权利益。另一方面,根据《个人信息保护法》、《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)等相关规定,重要数据在被转移至国外之前需要进行审查,如果域外执法或司法机关或当事人需要获取与案件相关的重要数据,而此类数据保存在我国并受到前述规定的约束,那么数据出境依然会受阻。

其次,如果在寻求由跨国公司控制的数据时,所涉数据由另一辖区的提供者控制或者被存储在另一辖区,那么将使取证变得更加困难。在“微软公司诉美国政府案”^②中,微软公司与美国司法部就跨境电邮的数据主权争议与法律适用展开了辩论。微软公司提出数据的跨境取证易引发数据主权冲突,一国的单方执法或司法可能侵犯他国主权,将直接或间接性地产生影响外交政策的后果。回归到法律适用层面,该案呈现在美国联邦最高法院面前的核心问题是《美国存储通信法》与《美国电子通信隐私法》能否适用于域外。对此,持反对态度的美国第二巡回法院将该问题视为主权尊重与否的问题,选择正面解决数据管辖权的不确定性,在原上诉程序中其决定限制《美国存储通信法》与《美国电子通信隐私法》的领土范围,以符合国际礼让利益。^③然而,赞成者则选择绕过数据主权问题,而以“数据控制者标准”为论证基石,认为要求本国互联网公司提供境外数据并非《美国存储通信法》与《美国电子通信隐私法》的一种新型跨境应用,而是一种搜查令的国内应用,不损害他国数据主权。^④此后,建立在美国司法部早期提案主要框架基础上的《美国云法》改变了美国原有的跨境数据取证的法律互助程序,使“微软公司诉美国政府案”失去了实际意义。《美国云法》首次确认在向受监管的科技公司发出命令之时,无论数据存储在何处,美国政府都可以获得该公司拥有、保存或控制的数据。^⑤实质上,该法将主体与行为因素作为区分点,并通过采用“数据控制者标准”将数据主权从物理层边界延伸到技术控制边界。^⑥概言之,尽管《美国云法》在一定程度上考虑了数据主权冲突,美国依然可以单方面决定调取他国数据,有碍他国主权。

目前来看,我国已经通过较为严格的数据安全立法,确保对个人数据、企业数据、公共数据的

① 参见支振锋:《网络主权植根于现代法理》,《光明日报》2015年12月17日。

② See Robert Barnes, Supreme Court to Consider Major Digital Privacy Case on Microsoft Email Storage, The Washington Post (Oct. 16, 2017), https://www.washingtonpost.com/politics/courts_law/supreme-court-to-consider-major-digital-privacy-case-on-microsoft-email-storage/2017/10/16/b1e74936-b278-11e7-be94-fabb0f9fb_story.html?utm_term=.b8451f1a0e41, 2022-10-17.

③ See Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 200, 201(2nd Cir. 2016).

④ See Andrew Keane Woods, Litigating Data Sovereignty, 128 Yale Law Journal, 328-407(2018).

⑤ See Chris Cook, Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook, 29 Stanford Law & Policy Review, 205-236(2018).

⑥ 参见许可:《数据主权视野中的CLOUD法案》,《中国信息安全》2018年第4期;梅夏英:《在分享和控制之间:数据保护的私法局限和公共秩序构建》,《中外法学》2019年第4期。

管理与控制,防止因数据非法出境而威胁国家数据安全与主权。^①“数据控制者标准”取证模式的强制调取程序极易引起与我国数据主权的冲突。反之,如果我国对网络服务提供者等数据控制者享有管辖权,那么是否可以突破“数据本地化标准”而以“数据控制者标准”直接向其获取境外数据?对此,同样缺乏规范依据,并且这样做也容易导致数据主权冲突。

(二)“数据控制者标准”取证模式与证据开示制度的叠加压力

“数据控制者标准”取证模式并不局限于对《美国云法》的关注,若将其向证据法领域延伸,则可以发现其与证据开示制度存在很多共同点。因此,在讨论“数据控制者标准”取证模式对我国的影响时,可将“数据控制者标准”与证据开示制度结合起来看待。事实上,早在《美国云法》确立“数据控制者标准”之前,美国的证据开示制度就已经具有“长臂管辖”的倾向,^②只不过该法案重在规制数据的跨境调取,而证据开示制度在针对境外当事人的数据调取方面具有与之类似的功能。

自 2006 年《美国联邦民事诉讼规则》将电子数据纳入证据开示的范围以来,要求国外当事人提供电子数据已成为美国法院域外证据开示命令的一种重要方式。^③但美国证据开示制度范围广且较为随性,即使开示的证据位于境外,其也依然可以发布证据开示命令,这一点与“数据控制者标准”取证模式的内涵基本一致。^④这一程序回避了《海牙取证公约》的规定,严重影响了他国的数据主权与司法主权。美国法院认为《海牙取证公约》等国际性公约与他国的数据保护法无法取代《美国联邦民事诉讼规则》,从而致使许多实质性冲突不可避免。在美国对抗制民事诉讼模式下,无论是否与外国法律冲突,美国法院都积极地推进证据开示,这种裁判思路可以追溯至 1987 年的“法国国家航空航天公司诉美国地区法院案”^⑤(以下简称“法国国家航空航天公司案”)。美国联邦最高法院在该案中提出,使用《海牙取证公约》获取域外证据并非强制性的,因此长期拒绝限制证据开示请求,尤其是当公约将不公平地抑制证据开示时,当事人可以根据《美国联邦民事诉讼规则》程序来获取境外证据。事实上,“法国国家航空航天公司案”关涉对法国飞机制造商的集体诉讼,制造商认为,由于案件所涉证据位于法国境内,因此如果违反法国的阻断法规,那么当事人不能将以诉讼为目的的证据材料转移至美国,也就无法遵守美国的证据开示制度。根据《美国联邦民事诉讼规则》关于证据开示的规定,法官可以强制当事人与案外人出示相关证据材料。同时,《美国联邦民事诉讼规则》第 16 条、第 34 条、第 45 条规定,如果美国法院对外国被告或案外人享有管辖权,相关证据在一方的“占有、保管或控制”范围内,那么持有证据的一方应当予以提供。另外,依据《美国联邦民事诉讼规则》第 34 条的规定,如果母公司对子公司有实质性的所有权和控制权,子公司及其雇员在正常业务过程中也能随时访问母公司数据,那么子公司对证据有控制权。当公司将相关的跨境数据存储在具有数据安全阻断法的国家之时,阻

① See Weiwei Zheng, Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China, 15 Frontiers of Law in China, 280—312(2020).

② 参见肖永平:《“长臂管辖权”的法理分析与对策研究》,《中国法学》2019 年第 6 期。

③ See Jack H. Friedenthal et al., Civil Procedure, West Academic Pressing, 5th edn., 2015, pp. 405—424.

④ 参见杜涛:《跨国取证司法合作中的不对称互惠问题研究》,《法律科学》(西北政法大学学报)2023 年第 1 期。

⑤ See Société Nationale Industrielle Aérospatiale v. U.S. District Court, 482 U.S. 522(1987).

断性规范必然与证据开示相冲突,此时情况也将更为复杂。^①

在跨境数据流动愈来愈频繁的背景下,我国与外国在跨境数据调取方面的矛盾愈加显著。即使有《数据安全法》《个人信息保护法》等法律法规的实施,也依然未在跨境诉讼数据取证领域确立完善的协调性规则,且这一问题在未来一段时期内还将持续。近年来就有相关案例凸显了上述矛盾。在“益华案”中,原告益华公司诉被告新拓尼克(北京)公司未经许可使用其软件,美国联邦北加州地方法院命令被告新拓尼克(北京)公司将24台计算机从中国运往美国接受审查,被告请求法院重新考虑这一命令,辩称计算机中包含员工个人信息,依据《个人信息保护法》第39条之规定,个人信息处理者向中华人民共和国境外提供个人信息的,应当取得个人的单独同意,因此只有经员工个人同意才能将他们的信息转移到境外。就被告新拓尼克(北京)公司针对法院此前支持原告益华公司提出的证据开示请求的重审动议,美国法院认为,上述命令与《个人信息保护法》第39条并不冲突,从而维持了原有的证据开示命令,驳回了被告请求重新审议的动议。^②上述裁决显然并未尊重中国的数据保护法规与跨境数据取证规则,该案例也直观地反映出中美两国在跨境数据取证方面存在现实冲突。

(三)阻断法对“数据控制者标准”取证模式的制约力度有限

一般而言,阻断法是指阻断一定行为或阻断外国法域外效力的一种法律,其与域外取证存在很大的关联性。^③早期美国学者将民事诉讼中他国禁止向美国法院提交证据材料的法律或规则统称为阻断法。^④本文所称的阻断法,则指的是跨境数据取证中的阻断法,其以境外数据强制调取程序的不合理性为基础,意在阻断其强制力。当前在跨境数据取证领域,《数据安全法》《国家安全法》《个人信息保护法》均有与阻断法相关的规定,但由于此类规范实质上依然是国内法,存在适用地域的限制,因此仅能约束本国当事人。实际上,阻断法仅为本国当事人提供了遵守或拒绝“数据控制者标准”取证模式中数据强制调取命令的两种选择,而无论作出何种选择,当事人都将承受不利后果。

首先,阻断法的完备与否将直接影响到跨境数据转移的合法性及对“数据控制者标准”取证模式的制约力度。为此,有必要考察数据出境是否与本国的阻断法、数据加密要求、海关要求等相冲突。即使本国当事人、案外人遵守境外执法或司法机关的数据调取命令向其提供数据,其也往往面临国内数据保护法、银行法、阻断法等引发的法律风险,情节严重的甚至可能构成犯罪。例如,法国的阻断法禁止为外国司法或执法之目的提供任何形式的任何数据,但美国法院并不认同法国的阻断法规可作为不提供跨境数据的合法依据。美国联邦最高法院认为,承认阻断法的合法性将使外国当事人、案外人在有阻断法的国家隐藏证据,即使出示证据的行为可能违反境外

^① See Marissa L. P. Caylor, Modernizing the Hague Evidence Convention: A Proposed Solution to Cross-Border Discovery Conflicts During Civil and Commercial Litigation, 28 Boston University International Law Journal, 341-388(2010).

^② See Cadence Design Systems, Inc., Plaintiff, v. Syntronic AB, et al., Defendants, United States District Court Northern District of California, Case No. 21-cv-03610-SI (JCS), Order Denying Motion for Reconsideration, Re: Dkt. No. 137.

^③ 参见徐伟功:《论次级经济制裁之阻断立法》,《法商研究》2021年第2期。

^④ See Vivian Grosswald Curran, United States Discovery and Foreign Blocking Statutes, 76 Louisiana Law Review, 1141(2016).

法规,阻断法依然无法剥夺美国法院命令受其管辖的一方出示证据的权力。^①与之相比,在我国跨境数据出境与取证领域,同样存在本国阻断法对美国证据开示命令强制力的制约力度受限之问题。尤其是美国以“数据控制者标准”不断扩张其管辖权,频繁针对中国当事人、案外人采取证据开示制度,扩张美国法域外效力,^②这种做法必然招致我国的抵触。

其次,即使我国已有相关的跨境数据出境阻断立法,他国也未必会予以尊重。从立法现状来看,在他国对我国境内数据的调取方面,我国是以“数据本地化标准”进行对抗,将网络空间主权与数据主权置于首位,严格限制或禁止他国调取我国境内的数据,并制定了应对境外数据强制调取制度的阻断法规。即便如此,在跨境诉讼中也依然存在罔顾我国个人信息跨境转移法规的案例,境外司法机关往往以对我国某一法律条文的扩大解释或曲解立法原意的形式,绕开我国阻断法并主张豁免。譬如,前文所述的“益华案”存在一个与阻断法相关的关键争点,即美国法院的证据开示命令是否属于《个人信息保护法》第13条第3项规定的法定义务。^③美国联邦北加州地方法院对“法定义务”做了扩张解释,认为美国法院的证据开示命令属于《个人信息保护法》第13条第3项规定的法定义务范畴,无须征得被告新拓尼克(北京)公司员工的同意。并且认为,《个人信息保护法》第13条存在例外情况,允许“为履行法定职责或者法定义务所必需”的情形下传输员工个人信息。在该案中,美国法院通过扩张解释将外国法律义务也纳入法定义务范畴。从立法论与解释论的角度看,一国法律的适用具有国别性、地域性,当前我国无论理论界还是实务界都是将“法定义务”限定在本国法,而未延伸至外国法。显然,美国法院的扩张解释与逻辑推理并未充分尊重中国法的立法原意,其不仅扩大了“法定义务”的范围,而且也是在为证据开示制度做背书,将对我国当事人产生不利影响。

三、“数据控制者标准”取证模式的现实应对

从作为数据控制者的网络服务提供者的角度看,鉴于美国和欧盟在网络服务领域具有显著优势,美国与欧盟在跨境数据取证领域确立“数据控制者标准”取证模式显然更符合其自身利益。甚至在美国与欧盟的协力作用下,该模式还可能成为“国际通行标准”。在这种情况下,我国的“数据本地化标准”在遇上境外强制性的“数据控制者标准”取证模式时该如何应对,就成为不得不重视的问题。

(一)确立“以数据本地化标准为主,以数据控制者标准为辅”的总体思路

随着云计算技术在数据存储领域的广泛应用,数据出境与传统的电子数据传输产生了一定的差异,它使原来束缚在物理空间内的电子数据转变为脱离物理空间地域限制的可访问数据。

^① See Marissa L. P. Caylor, Modernizing the Hague Evidence Convention: A Proposed Solution to Cross-Border Discovery Conflicts during Civil and Commercial Litigation, 28 Boston University International Law Journal, 341-388(2010).

^② 参见章晶:《美国事证开示程序对外国案外人管辖权的扩张——以涉中国金融机构案件为例》,《国际法研究》2020年第1期。

^③ See Cadence Design Systems, Inc., Plaintiff, v. Syntronic AB, et al., Defendants, United States District Court Northern District of California, Case No. 21-cv-03610-SI (JCS), Order Denying Motion for Reconsideration, Re: Dkt. No. 137.

我国可探索完善以“数据本地化标准”为主、“数据控制者标准”例外适用的新型跨境数据取证机制。

第一,以“数据本地化标准”为主的理据。首先,从立法论视角看,我国在跨境数据取证方面采用的标准与跨境数据流动的标准基本保持一致,即“数据本地化标准”,且该标准已通过基本法的形式确立下来。譬如,《网络安全法》第37条确立了以“数据本地化标准”作为明确数据位置的基本方法,并通过建立以数据主权为基础的安全评估体系来控制跨境数据传输。遗憾的是,《网络安全法》并未规定外国通过跨国公司等数据控制者或证据开示制度获取我国境内数据的具体情形。《数据安全法》第7条、第36条等从跨境数据取证等方面对数据出境进行了规定。《个人信息保护法》第38~43条更是以专章的形式规定了“个人信息跨境提供的规则”,第40条对“数据本地化标准”进行了明确规定。简言之,上述规定既从数据主权的角度明确了“数据本地化标准”下数据出境的基本要求,又在一定程度上回应了境外“数据控制者标准”取证模式可能侵犯我国数据主权的系列问题。其次,从解释论角度看,“数据本地化标准”是作为总体国家安全观制约境外数据调取的一道屏障,坚持总体国家安全观是贯穿我国数据法规与数据治理的一条主线,无论是宏观的跨境数据流动还是微观的电子证据出境,都应当符合网络安全、数据安全、个人信息保护以及国家安全的目标。值得注意的是,数据本地化是我国数据立法的基本理念,但数据本地化的目的并不是阻碍数据出境,而是在数据安全与数据取证中找寻平衡点。

第二,在建构以“数据本地化标准”为基石的数据出境制度且限制“数据控制者标准”的扩张性时,以有限度的数据访问权弱化“数据本地化标准”的封闭性。对于域外数据调取程序而言,即使我国当事人拒绝遵守其数据调取命令,对方也依然有很大可能通过线上访问的形式绕开该命令而以“数据控制者标准”调取。既然如此,那么我国可依据《中华人民共和国民事诉讼法》(以下简称《民事诉讼法》)第5条、第284条以及《数据安全法》第36条的规定,在对等原则与平等互惠原则的基础上,适当为“数据本地化标准”下的跨境数据出境或开示设立一定的“数据控制者标准”例外适用空间。《美国云法》虽然遭遇不少批评,但其规定的从“数据控制者”手中直接调取数据的模式确实能够提升司法、执法效率,即使在外国政府调取美国“数据控制者”数据方面存在诸多不合理限制,其关注数据访问权的路径也依然具有参考价值。^①

第三,适当开放数据访问权以适应跨境数据的取证需求。数据访问权在处理域外证据强制调取问题时有一定的优势,能够以低成本、高效率的方式实现跨境数据传输。但需要警惕的是,单方面的数据访问权开放并不符合我国的数据安全与国家安全政策,也与我国电子数据的出境规定相背离,必须为其施加必要的限制。尤其是在确有损害国家安全、数据安全、商业秘密、个人隐私的风险时,应禁止域外执法或司法机关利用数据访问权作为数据强制调取受阻的替代措施。^②

第四,面对境外出示令、保全令、证据开示命令等强制性数据调取程序带来的证据开示压力,以及维护国家信息安全与数据主权的需要,我国有必要在尊重主权管辖原则的基础上适当扩大数据执法与司法管辖权。^③目前,尊重主权原则作为国家间跨境数据取证的基本理念业已得到

① 参见刘金瑞:《迈向数据跨境流动的全球规制:基本关切与中国方案》,《行政法学研究》2022年第4期。

② 参见郑曦:《数字时代刑事证据开示制度之重塑》,《华东政法大学学报》2023年第4期。

③ 参见孔庆江、于华溢:《数据立法域外适用现象及中国因应策略》,《法学杂志》2020年第8期。

国际认可。《民事诉讼法》第 284 条、《数据安全法》第 36 条、《个人信息保护法》第 41 条规定的跨境取证模式均遵守了这一原则。譬如,在涉外民事诉讼领域,2023 年 9 月,我国在对《民事诉讼法》涉外民事诉讼程序的特别规定进行修改时,新增了关于跨境诉讼调查取证的条文,根据第 284 条第 2 款的规定,在所在国法律不禁止的情况下,经双方当事人同意,人民法院可以通过即时通信工具或者其他方式取证。事实上,该条规定既尊重了他国主权,又为跨境调查取证提供了简单、便捷的通道,且无论是采用即时通信工具还是其他方式,都在一定程度上突破了“数据本地化标准”的约束。

(二)确立共识性数据保护标准与主权差异的取证模式

我国数据出境面临的前提性问题在于如何回应境外“数据控制者标准”取证模式对我国数据主权的影响。为此,有必要在坚持主权差异、国际礼让等理念的基础上,通过确立共识性数据保护标准与主权差异的取证模式来缓和主权冲突。

第一,明确最低限度的共识性数据保护标准,减少我国与他国的外交摩擦,以及我国当事人被境外执法或司法机关制裁的风险。此种共识有利于提供一个长期稳定的法律程序渠道,从而减少后续可能产生的数据主权争议。跨境数据取证需要在一定程度上协调法律选择规则,采用共同的原则或标准,以提高其适用的确定性与可预测性。^①同时,我们也可以通过为明确最低限度的共识性数据保护标准提供基础,来提升执法或司法机关利用条约机制获取境外数据的能力。例如,2019 年 10 月,美国与英国就执法部门访问存储在国外的电子数据的联合框架达成《针对打击严重犯罪目的的电子数据访问协议》,允许美国网络服务提供者依据《美国云法》获取存储在英国的电子数据,^②该协议于 2022 年 10 月 3 日正式生效。2021 年 12 月 15 日,美国再次与澳大利亚达成敏感数据执法合作双边协议。^③2024 年 1 月 31 日,欧盟与日本也正式将关于跨境数据流动的条款纳入《欧盟—日本经济伙伴关系协议》,^④此举虽然不是专门针对数据取证,但跨境数据流动与跨境数据取证之间的关系极为紧密,与前者相关的双边协议同样可作为后者的依据。值得注意的是,双边协议无法为区域司法合作提供全面的框架,签订过多的双边公约也较为低效,潜在的条约冲突问题仍将继续存在。^⑤故而,有必要将加入现有的国际框架作为基础选择,同时可以依靠双边或多边协议来填补跨境数据取证国际框架的空白,促进与特定国家的司法

^① See Zheng Sophia Tang, The Belt and Road and Cross-Border Judicial Cooperation, 49 Hong Kong Law Journal, 121-152(2019).

^② See European Commission, Recommendation of 5 February 2019 for a Council Decision Authorising the Opening of Negotiations in View of an Agreement Between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matter, COM(2019)70 final, p. 1-2, https://eur-lex.europa.eu/resource.html?uri=cellarb1826bff-2939-11e9-8d04-01aa75ed71a1.0001.02/DOC_1&format=PDF, 2024-01-31.

^③ 美国与澳大利亚签署的双边敏感数据执法合作协议主要用于共享对恐怖主义、互联网上对关键基础设施的破坏、勒索软件攻击、儿童色情等严重犯罪活动进行防范、发现、调查和起诉的敏感数据。

^④ See EU-Japan Economic Partnership Agreement: EU and Japan Sign Protocol to Include Cross-Border Data Flows, <https://www.consilium.europa.eu/en/press/press-releases/2024/01/31/eu-japan-economic-partnership-agreement-eu-and-japan-sign-protocol-to-include-cross-border-data-flows/>, 2024-02-05.

^⑤ See Zheng Sophia Tang, The Belt and Road and Cross-Border Judicial Cooperation, 49 Hong Kong Law Journal, 121-152(2019).

协作。

第二,如果境外执法或司法机关欲通过其强制性数据调取命令获取我国的数据,那么应当尊重两国间的主权差异。譬如,由于美国证据开示制度中的跨境数据取证模式受到其互联网治理“世界主义”理念的影响,其希望跨境数据提供者可以忽略数据管辖地规则,而按照美国的证据开示制度提供证据。^①与之相比,我国在跨境数据的出境方面偏向于采用“主权差异”理念,其主要关注国家对电子证据的控制,且认为境外数据取证首先应重视“国家对领土的控制”这一主权的核心组成部分,而后根据各国的法律规范、习俗和规则,在不同地区适用不同的运作方式。事实上,各国可以在相互承认与尊重的基础上,以适应其他国家主权利益的方式获取跨境数据,这已然成为全球较为通行的取证理念。

第三,以国际礼让平衡我国法与境外“数据控制者标准”取证模式的冲突。跨境数据取证牵涉与国际礼让相关的外交事务法,而国际礼让是法院礼让分析中最重要的因素。^②国际礼让原则表明,各国应相互尊重彼此的立法、行政和司法行为,若境外司法机关欲以“数据控制者标准”强制获取中国境内的各类数据,则应充分考虑中国法的规定与相关当事人、案外人的利益,并在可能的情况下满足这些利益。^③具体来说:一方面,就外国而言,国际礼让原则要求外国法院充分尊重中国的数据主权,但可将该原则作为其自由裁量权行使的基石,以衡量是否向我国当事人发布跨境数据调取命令。另一方面,就我国而言,若认为境外数据调取程序与我国法不冲突,且不存在不可调和的价值矛盾,则应尊重其程序命令。依国际礼让之要义,若我国主管部门或司法机关对美国、欧盟等请求的数据享有管辖权,且根据《民事诉讼法》《数据安全法》等规定的程序进行司法协助对本国主权利益并无不当影响,则可以选择接受《海牙取证公约》等规定的协助程序。^④

(三)缓和“数据控制者标准”取证模式与证据开示制度的压力

我国在应对境外“数据控制者标准”取证模式与证据开示制度的叠加压力时,不能将视野限定在某一部门法,而应当从民事诉讼法、数据法、国际法的多维融合的视角出发,全方位构建数据出境与取证机制。

第一,完善立法与法律解释并行,将数据等级保护制度中的分层、分类、分级管理引入跨境数据取证领域。一方面,我国在缔结双边或多边跨境取证协议时,可在现行国内法与国际法的框架内通过谈判达成限制性更小、更有针对性的司法互助协议。当一项新型技术迅速发展时,短时间内司法机关缺乏相应的制度能力来掌握其对数据安全的影响,法官自由裁量权的行使也可能会导致个案的司法适用千差万别,影响法律适用的统一。对此,与其在数据安全、跨境数据取证等一系列问题上实施全面变革,倒不如尝试渐进式立法政策。另一方面,既然认识到境外“数据控

^① 参见刘天骄:《数据主权与长臂管辖的理论分野与实践冲突》,《环球法律评论》2020年第2期。

^② See Emily Burge, Patents vs. Privacy: Balancing Cross-Border Discovery with the General Data Protection Regulation in Patent Litigation, 48 American Intellectual Property Law Association Quarterly Journal, 719—758 (2020).

^③ See The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, 19 Sedona Conference Journal, 557—624 (2018).

^④ 参见郭玉军:《论美国与欧盟国家域外取证领域的冲突及其解决》,《河北法学》2011年第4期。

制者标准”取证模式与我国数据出境之间的冲突难以避免,那么可通过善意、合理的法律解释来减少风险。譬如,现有的《数据安全法》《网络安全法》《个人信息保护法》及相关规章条例已经确立以数据等级保护制度为基础的分层、分级、分类数据出境制度。在将其运用于对抗境外数据强制调取方面,可以在跨境数据执法、数据出境中确立以数据等级保护制度为基础,适当对等开放数据管辖的跨境数据取证机制,对涉及不同利益的电子证据进行分级、分类管理。未来可逐步形成一种尊重主权与保障程序参与者权利并重的数据出境与取证机制。^①同时,他国应将通过证据开示命令、出示令、保全令等程序获取的证据限制在与案件实质相关的范围内,且仅能作为诉讼中的证据使用,不能用作其他目的。这一点在《欧盟电子证据条例》中同样得到了强调,该条例“鉴于”部分第 15 项对根据本条例获取的个人数据的使用范围进行了限制,即只能在必要时以与预防、调查、侦查和起诉犯罪或执行刑罚以及行使辩护权相称的方式加以处理。^②

第二,借鉴美国在“法国国家航空航天公司案”中确立的五因素平衡测试法,重视考察诉讼中影响取证的多重元素。具体如下:(1)请求获取的数据对诉讼的重要性。法院尤其应当考虑被请求调取的证据与当事人提出的主张与辩护的相关性与重要性。(2)请求的特殊性与具体程度。法院应审查电子数据提供方的潜在压力,以评估请求方的取证请求是否会造成过于繁重的负担,当负担超过可能获取的利益时,应当限制取证。(3)跨境数据的来源地或者数据与当事人的物理空间。如果欲请求获取的所有数据或包含此类数据的数据库都位于境外,那么应考虑证据还可能受外国法律的约束。(4)是否存在获取跨境数据的有效替代方法。如果存在其他方式,且替代性取证方式与请求的取证方式在“实质上等效”,那么法院应充分利用替代方法的可用价值。就抗辩方而言,其更愿意选择实质上等效的替代方式,当唯一的数据来源由抗辩方控制时,替代性取证方法将更令人信服。(5)获取的数据对本国利益的重要性高于遵守公约对外国利益的重要性,以及不遵守规定对本国或外国重要利益的影响。^③除此之外,跨境数据取证不仅应当考虑到文件和保管人所在国的数据安全法规,还需要关注公共政策及其他组织可能妨碍诉讼的行为。在诉讼中,主要的公共政策目标是平等确定当事人权利与主权利益,不能为了追求取证的绝对化而损害当事人的合法权益与他国的主权利益。^④

(四)以阻断法限制“数据控制者标准”取证模式的强制力

虽然阻断法在应对域外数据强制调取命令时作用有限,但是我国相关主管部门依然可将阻断法作为限制境外执法或司法机关跨境数据取证命令或请求强制力的规范依据,只不过需要从多个方面进行补强。

^① 参见冯俊伟:《跨境电子取证制度的发展与反思》,《法学杂志》2019 年第 6 期。

^② See Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_2023_191_R_0002, 2024-02-03.

^③ See Marissa L. P. Caylor, Modernizing the Hague Evidence Convention: A Proposed Solution to Cross-Border Discovery Conflicts during Civil and Commercial Litigation, 29 Boston University International Law Journal, 341-388(2010).

^④ See The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, 19 Sedona Conference Journal, 557-624 (2018).

第一,衡量其他国家在执行跨境数据取证阻断法规方面的主权利益是否超过我国获取同类型证据用于诉讼的利益。在此基础上,面对境外强制性的数据调取命令,我国可通过阻断法予以对抗或主张豁免。此时,如何对上述两种利益进行衡量就成为阻断法能否发挥作用的重要判断标准。判断某一国家是否为跨境数据取证提供了对等或充分的保护,既是对该国数据监管体系的评价,也是对其跨境诉讼支持体系的考验。^①从域外经验来看,《欧盟通用数据保护条例》第45条和第48条关于阻断法的规定采用的是“充分保护”模式。即当事人只有在采取了隐私和数据保护措施,并且是在提出或支持其法律主张所必需的条件之下才可以将数据转移至他国,且只能向保护水平与其等同或更高的国家流动。根据“充分保护”理念的要求,数据存储国应当审查接受转移之辖区的数据保护法律是否充分。如果相关的数据出境法规不充分,那么需要根据数据传输协议或其他合同条款、标准示范合同、有约束力的公司章程以及适当的技术和组织措施,对电子数据出境的风险进行评估。譬如,可通过数据审查、程序控制、数据加密等方式,确保数据的保密性、可用性和完整性,并决定是否允许出境。^②“充分保护”模式对于我国如何适时运用阻断法、衡量国际民商事诉讼中牵涉的数据主权利益具有重要的参考价值。

第二,回归我国现有立法,充分利用已有的阻断法主张豁免。当事人或案外人可通过利用我国现有的法律法规、规章等规定的阻断性规范来对抗境外数据强制调取命令,以维护自身合法权益。《数据安全法》第36条、《个人信息保护法》第41条均属于阻断性规范,跨境诉讼中的当事人或案外人可在坚持未取得单独同意的抗辩之基础上,通过援引《数据安全法》第36条和《个人信息保护法》第41条等规定向境外司法机关主张证据开示命令的豁免,类似的还有主张属于国家秘密或商业秘密豁免等。除基本法律的规定外,近年来,我国还制定了相关的阻断性规章。譬如,2021年1月商务部公布的一项专门性的阻断办法——《阻断外国法律与措施不当域外适用办法》(以下简称《阻断办法》)——规定相关部门可以禁止跨境诉讼当事人“承认、执行、遵守”外国法律与措施,其中就包括美国法院对我国企业或个人作出的证据开示命令。《阻断办法》的出台:一方面在于反对外国法律与措施的不当域外适用,另一方面也为企业保障自身合法权益提供了救济渠道,^③可作为阻断“数据控制者标准”强制取证的武器。2022年7月国家互联网信息办公室公布的《数据出境安全评估办法》第8条规定,数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险,其中第2项就包括关于充分性与适格性的内容,即“境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响;境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求”。不过,面对境外“数据控制者标准”取证模式强大的“穿透性”,《数据出境安全评估办法》能否真正发挥阻断法的作用、为本国当事人在境外司法程序中构建一个有效的数据规范防护体系,还有待观察。

^① See Julian Rotenberg, Privacy Before Trade: Assessing the WTO—Consistency of Privacy—Based Cross—Border Data Flow Restrictions, 28 University of Miami International and Comparative Law Review, 91—120(2020).

^② See Jayne Rothman, Alison Wisniewski, M. James Daley & Laura Clark, Stormy Digital Weather Ahead: The Forecast for Cross—Border eDiscovery in the Context of Litigation and Regulatory Investigations, 7 International In—House Counsel Journal, 1—15(2013).

^③ 参见徐伟功:《论次级经济制裁之阻断立法》,《法商研究》2021年第2期。

四、结 语

跨境诉讼中的数据取证需要国内法、国际法、域外法的多重协调,双边、多边协议与国际规则的出台,也取决于各国、各地区和国际组织之间对跨境数据取证理念的共识,而国际法共识的达成也需要有国内法的回应。在大国司法与国家安全语境下,我国应当在《海牙取证公约》等民刑司法协助公约的框架下,协调好国内法与国际法的关系,推动建立更为完善的跨境诉讼数据出境与取证机制。同时,数据主权优先是主权国家之共识,每个国家在其数据领域的主权与利益均应得到保护。面对境外“数据控制者标准”取证模式的压力,我国应排除外界干扰,尊重主权差异,在数据主权优先的基础上完善数据共享与取证协助机制,确保跨境数据取证的双向透明。同时,采取礼让与合作的方式消除适用外国法的不必要障碍,促进我国更新国内法并使之现代化,以加强跨境司法合作。在缺乏国际层面协议的情况下,即使缺乏其他国家的合作,单边改进国内法也能有效地改善本地区的跨境司法合作,因此还应提升本国跨境数据取证规范的质量。

Abstract: The “data controller standard” forensic model uses the “actual controller of the data” as the personal link to determine the jurisdiction over cross-border data, which points to various types of offshore data controlled by cross-border network service providers that can be used as evidence. This model is shifting cross-border data forensics from the principle of territoriality, which is expressed in the form of “data localization”, to personalism, which takes “data controller” as the core jurisdictional element. Based on the characteristics of the “data controller standard” forensic model, which is based on the mandatory access to data outside the country directly from the data controller, this model is very likely to trigger a conflict of data sovereignty between it and the “data localization standard” countries, including China. In addition, the “data controller standard” forensic model contradicts China’s relevant procedural law and data protection law, while China’s blocking law is not enough to deal with compulsory access to foreign data. Therefore, China can try to adopt the strategy of “mainly based on data localization standard, supplemented by data controller standard”, and based on respecting sovereignty difference and international comity, implement the principle of reciprocity based on a limited number of data out of the country. At the same time, the blocking law should be brought into full play to neutralize the adverse impact of the “data controller standard” forensics model on China.

Key Words: data controller standard, cross-border forensics, data sovereignty, evidence of discovery, blocking legislation

责任编辑 王虹霞