

我国域外数据执法管辖面临的困境与因应

陈俊秀, 王纬航, 李智

(福州大学法学院, 福建福州 350108)

[摘要] 基于争夺数据资源和维护本国数据资源安全之目的, 各国不断强化域外法权、扩张域外数据执法管辖, 形成“美国模式”与“欧盟模式”2种典型路径。现阶段我国域外数据执法管辖呈现出一定的局限性, 主要表现为域外数据执法依据不足、管辖范围有限、域外数据管辖执法难度大等。因应上述困境, 一方面有必要完善反长臂管辖法律体系, 加强阻断立法限制他国数据管辖范围的不当扩张, 规制数据控制者行为以强化我国数据管辖, 完善反制措施的法律依据; 另一方面需要健全域外数据执法管辖法律体系, 通过立法手段强化执法依据, 对我国域外数据管辖范围予以体系解释和扩大解释, 完善域外数据调取与取证等执法措施。

[关键词] 域外数据执法; 数据主权; 数据管辖权; 数据跨境取证

[中图分类号] D 99; D 912.1 [文献标识码] A [文章编号] 1008-889X (2024) 05-0027-09

域外执法管辖本质上是国内法的域外适用, 是本国对位于或发生在本国管辖领域之外的人、物或行为适用本国法律规范的过程^[1]。域外数据执法管辖指的是非数据存储地国对存储在该国领域外的数据行使执法管辖权的行政执法行为。当前, 数据已成为关乎国家核心利益的战略资源, 各国扩张域外数据执法管辖已成为一种趋势, 给我国带来影响和挑战。在国际层面, 域外执法管辖范围的扩大对我国数据管辖权和数据安全构成威胁; 在国内层面, 我国在域外数据执法时, 面临管辖依据不足、管辖范围狭窄等问题。为此, 需采取多重举措, 重构数据域外执法法律体系, 扩大我国域外数据执法权限, 有效维护国家数据安全和数据主权。

一、问题源起: 全球域外数据执法管辖扩张趋势

当下, 对数据资源的理解不再局限于“生产要素”层面, 而延伸至“个人安全”与“国家安全”领域, 其战略价值突显^[2]。国家间的竞争正逐渐从围绕土地、机器和工厂展开转向对数据控制权的争夺, 全球范围内各国域外数据执

法管辖的扩张即为例证。

(一) 全球域外数据执法管辖扩张的原因

近年来, 美国、欧盟、澳大利亚、巴西等国家和地区以各种方式扩张本国执法机关域外数据管辖的范围, 其动因主要包括以下4个方面:

1. 争夺数据资源以提升国家全球竞争力。数字经济时代, 数据要素已逐渐成为经济社会发展的根本性、战略性资源。当前, 各国对数据要素的重视程度逐渐提高, 围绕数据资源展开的国际竞争也愈发激烈。数据执法管辖权的域外扩张, 能够增强一国对域外数据的支配能力, 进而掌握更多的数据资源。随着数据战略价值不断凸显, 各国控制的数据资源会成为未来国际竞争的关键筹码。因此, 尽可能地向域外延展数据执法管辖范围, 把握对关键数据的控制权, 是一国获取数据资源、增强核心竞争力的战略抉择。

2. 应对数据全球流动带来的数据治理需求。网络科技尤其是云存储技术的发展, 令数据的收集、存储、处理、流通和共享等活动不再局限于一国境内。随着数据要素深度嵌入国际经济、政治交往中, 数据的跨境流动与跨境存储也逐渐成为一种常态。这一数据全球流动的新趋势, 削弱了数据位置的稳定性, 国家对于数据的管辖权受

到了数据“非领土性”挑战^[3]。并且,云存储技术使数据跨境流动得以避开一国法律和政府监管,坚持“数据存储地”管辖的传统做法,已难以适应当前的数据治理需求。

3. 弥补国际合作机制缺位以维护数据安全。愈发频繁的数据跨域流动与存储,令数据窃取、泄露等安全风险日益突出,当前的国际合作机制却无法满足不同国家在数据保护方面的立法存在显著差异,导致国际组织难以协调各国立场,无法构建强有力的国际合作机制。此外,传统司法协助模式在应对数据安全问题上近乎失灵。这种局限于缔约国之间的国际协作,不仅在效率和范围上完全滞后于数据的全球流动,日趋激烈的数据争夺也会放大条约缺乏强制力的先天劣势。

4. 强化执法管辖以提升域外数据执法效率。较之于频繁失灵的国际合作机制,域外数据执法手段在争夺数据资源、维护国家数据安全等方面的优势更为明显。域外数据执法由一国行政机关通过单方强制的行政手段完成。执法机关不仅可以直接对域外数据及相关主体行使执法权,也能够对域外主体威胁国家数据安全的违法行为进行及时、有效的打击。并且,域外数据管辖依据和执法权力可来源于国内法,这将有助于提升域外执法效率,更好地实现域外数据执法目的。

(二) 域外数据执法管辖扩张的主要模式

当前,各国有关数据域外执法的法律框架、政策指引和基本立场均有所不同,不过总体上通行的管辖模式主要有2种:第一种是以美国为代表的、以属人管辖为基础的域外执法管辖,第二种是以欧盟为代表的行政机构在全球范围内的直接执法。

1. 基于属人管辖的域外执法管辖扩张。数字经济时代来临前,美国公司凭借技术优势掌握了世界主要数据,并大多存储在美国本土。因此,1986年美国《存储通信法》(the Stored Communications Act)并没有规定域外数据管辖权,而采取了数据存储地管辖模式。随着数据域外存储成为常态,美国公司也将大量数据存储于境外,美国政府却因受制于存储地规则而无法进行调取。2018年3月,美国通过《澄清域外合法使用数据法》(the Clarifying Lawful Overseas

Use of Data,以下简称《云法案》),确立了数据属人管辖的基本原则,其重要动因即是为了将美国公司所掌握的域外数据纳入管辖范围。有研究指出,属人管辖模式能够充分利用美国互联网企业的优势地位,将其在全球市场中的份额转化为美国的数据管辖权^[4]。

根据《云法案》的规定,美国通信服务提供商所拥有、监控或控制的数据,无论是否存储在美国境内,都应受美国的监管或控制。在适用主体方面,《云法案》未特别指明其所规范的提供商的范围。但是,该法案在“法律程序的礼让分析”中,要求法官在进行礼让分析时,必须考虑“提供商与美国产生联系的性质和程度”。这意味着,凡在业务或其他方面与美国存在联系的服务商都可能成为该法案的适用对象。这实际上是将数据管辖依据从传统的数据存储地转为数据控制者,即只要数据控制者与美国存在联系,其掌握的数据无论是否存储于美国境内,都受美国执法部门的管辖。对获取数据的范围,《云法案》也未予明确,只是在第102节笼统地表示,获取通信服务提供商持有的数据“是美国政府保护公共安全和打击包括恐怖主义在内的重大犯罪的关键”,即美国政府只要认为该数据对保护公共安全和打击重大犯罪有重要意义,便可以要求调取。由于《云法案》没有对可获取数据的范围作出具体规定,“公共安全”本身又是一个不易确定的概念,美国行政机关在形式上获得了极为宽泛的域外数据调取权限。

2. 直接域外执法模式。1995年欧盟《数据保护指令》(Data Protection Directive)确定的是属地管辖原则,即只有设立在欧盟的企业所掌握的或者通过欧盟境内的设备处理的数据,才会受到欧盟管辖。但是,2016年欧洲议会通过的《通用数据保护条例》(General Data Protection Regulation)则基于域外适用条款,赋予了行政执法机关全球范围内的域外管辖权。《通用数据保护条例》第1条开宗明义地表示,条例旨在“保护自然人的基本权利和自由”,具有比较鲜明的保护主义色彩;第3条将数据持有者、处理者和来源者作为确定管辖的依据,也是对当前数据全球流动现状所作的回应。《通用数据保护条例》也赋予了行政机关直接域外执法权,从根

本上说是为了扩大条例的全球影响力, 争取数据全球话语权^[5]。

《通用数据保护条例》扩张域外数据执法范围的主要依据是“商业存在”和“目标指向”标准。“商业存在”标准要求只要企业在欧盟境内有商业存在, 则在其经营活动范围内处理的数据, 便应当由欧盟管辖。“商业存在”标准划定的管辖范围极为宽泛, 一方面, 企业是否在欧盟境内进行注册登记不是判断商业存在的决定性因素, 只要企业稳定且真实地在欧盟境内开展经营活动, 便认为其在欧盟内有商业存在; 另一方面, 只要欧盟认定某一企业在欧盟内有商业存在, 该企业在欧盟外进行的数据处理行为也会被纳入欧盟的管辖范围。“目标指向”标准则针对在欧盟境内无商业存在的主体, 若其数据处理行为系为欧盟内主体提供服务, 或者以欧盟内的主体作为数据采集、处理对象, 则也应当遵守《通用数据保护条例》的规定。由“商业存在”与“目标指向”构成的宽泛的多重标准, 使得存储在欧盟之外的非欧盟数据也会受到欧盟管辖。

二、我国域外数据执法管辖的现状与困境

(一) 我国域外数据执法管辖立法现状

现阶段, 我国已对域外数据执法管辖作出了规定, 但总的来说, 既有法律仍存在一些不足。有关域外数据执法管辖的规定, 散见于《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》)和《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)等有关法律。

1. 我国关于数据域外执法管辖的规定。在数据管辖范围上, 《个人信息保护法》和《数据安全法》均以处理行为发生地作为管辖依据。根据《个人信息保护法》第3条第1款之规定, 只要数据处理行为发生在中国境内, 即应当由中国管辖。基于这一规定, 我国执法机关可以对在中国境内处理的外国数据进行管辖, 而不问该数据的存储地在何处。同时, 《个人信息保护法》

第3条第2款采用“目标指向”规则, 将发生在中国境外的“向境内自然人提供产品或服务”和“分析、评估境内自然人”的数据处理活动纳入管辖范围。《数据安全法》采取的则是保护主义规则, 要求对在境外开展的损害国家安全、公共利益或我国公民、组织合法权益的数据处理行为进行管辖。相比之下, 《网络安全法》的规定则更为笼统, 但总体上也是采用了与《数据安全法》相同的保护主义原则。

2. 应对外国域外数据执法管辖扩张的制度安排。我国立法对外国域外数据执法管辖的扩张也设置了一些防卫性的制度安排。比如, 《个人信息保护法》第41条规定, 主管机关必须依据国际条约、协定或按照平等互惠原则, 处理外国在中国境内调取数据的请求。非经主管机关批准, 任何人不得向域外提供存储于中国境内的个人数据。《数据安全法》第36条也有类似规定。《中华人民共和国国际刑事司法协助法》也明确了向境外提供数据或进行司法协助, 必须经国家主管机关同意, 任何机构、组织和个人不得擅自实施。此外, 商务部《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》)第11条规定, 中国公民、法人或者其他组织根据禁令, 未遵守有关外国法律与措施并因此受到重大损失的, 政府有关部门可以根据具体情况给予必要的支持。这在立法上对企业遵守中国法律、拒绝外国提出的跨域调取数据要求予以支持与激励。

(二) 我国域外数据执法管辖面临的困境

在域外数据执法管辖层面, 我国主要面临2个方面困境: (1) 如何应对外国域外数据执法管辖扩张对我国数据安全和数据主权带来的影响。(2) 如何在确保正当性的基础上, 扩张我国域外数据执法权限。

1. 域外数据执法管辖扩张对我国的影响。首先, 外国法律通常会划定较为宽泛的域外管辖范围, 外国执法机关可借此对存储在我国境内的数据进行管辖。比如, Apple、Microsoft、Amazon等美国企业拥有大量中国用户, 即使这些公司将用户数据存储在中国, 在“数据控制者”管辖模式下, 美国执法机构依然可以要求其提供这些数据。另外, 《云法案》将与美国存在关联

的数据控制者均纳入适用范围,凡在美国提供服务或与美国存在其他联系的中国企业,都可能成为法案所规制的对象,美国执法机关也可以要求调取其掌握的数据。欧盟《通用数据保护条例》通过“商业存在”与“目标指向”的多重标准,宽泛地确立了域外数据管辖的范围,无论数据持有者和控制者是否在欧盟注册,也不论数据处理活动是否发生在欧盟内,有关数据都可能受到欧盟执法机关的监管与控制。因此,外国域外数据管辖权的扩张,会将存储于中国境内的数据纳入其管辖范围,外国执法机构在一定条件下能够绕过中国政府对中国数据进行调查,会对我国的数据安全构成威胁。

其次,存储在中国的数据可能面临中国与外国的双重管辖。根据我国《数据安全法》和《个人信息保护法》的有关规定,凡在中国境内开展的数据处理活动,均应由中国管辖。这就确立起以“处理行为发生地”为管辖依据的域内数据管辖模式。在这种管辖模式下,数据存储地国出于维护数据安全等方面的考虑,往往会限制境内数据的跨境流动。外国在调取或访问由存储地国掌握的数据时,原则上必须通过司法协助的方式进行。然而,扩张化的域外数据执法往往不会寻求司法协助,而是试图单方、直接地进行数据调取。在此情形下,数据存储地国与调取国之间将引发单边跨境数据调取管辖权冲突^[6]。冲突的最终结果是,一国对特定数据行使了管辖权,同时排除了他国对该数据的管辖。国内法域外适用本质上是国家主权利力的延伸,数据管辖博弈也关乎一国对数据的管理权与管辖利益^[7]。当冲突发生时,数据控制者则必须在“本国”与“外国”之间作出选择,“违法成本”将是其考虑的重要因素。我国《阻断办法》虽然提出要对涉事数据控制者“给予必要的支持”,以促使其在面临管辖权冲突时遵守中国法律,但是由于缺少细化规定而很难落实。相反,欧盟《通用数据保护条例》赋予行政机构调查权、纠正权、行政处罚权等具体执法权,数据持有者为了避免承担过高的违法成本,往往不得不接受欧盟的域外数据管辖。

再次,单边主义的域外执法权扩张,会对我国国家安全构成威胁。公法域外适用以单边主义

方法为基础,立法者可通过明示立法或司法手段使某一公法具有域外效力^[8]。各国域外数据执法权扩张,通常也遵循了单边主义径路。譬如,《云法案》即表明在“保护公共安全和打击包括恐怖主义在内的重大犯罪”时,该法案具有域外适用效力。但是,该法案赋予美国在全球范围内宽泛的数据调取权力,却没有赋予他国对等的权力。《云法案》虽然在形式上允许“适格的外国政府”在同等条件下调取美国境内的数据,但外国政府“适格”与否完全是由美国依《云法案》设定的标准单方进行认定的。事实上,只有极少数国家在严格条件下能够调取美国控制的数据,这将使美国的全球数据霸权国内法化^[4]。同样,欧盟《通用数据保护条例》也具有很强的单边扩张特点。该条例一方面赋予执法部门全球性数据执法权,可以绕过一国政府对存储于该国境内的数据进行调取和监管;另一方面又对欧盟内数据出境作出严苛限制,即必须遵守条例的所有规定并经过欧盟委员会审查同意方可进行。从我国立场出发,倘若外国法律赋予其执法机关宽泛的域外数据管辖权,却严格限制我国对其域内数据的调取与访问,会侵害我国国家主权和管辖利益。对此,我国在立法上虽然已有一定的制度安排,但由于缺乏必要的反制措施,从总体上看仍处于“弱防御”状态。

2. 我国域外数据执法权限不足。我国在数据领域执法主要是针对境内主体实施的,境外执法则主要体现为技术防御,我国执法机关尚不能对境外主体采取行政处罚等强制措施。

首先,我国域外数据执法管辖依据不足。《个人信息保护法》虽然确立了“行为发生地”和“目标指向”标准作为管辖依据,但该法只能为个人数据的域外管辖提供依据,企业数据和公共数据等并不在其调整范围内。《网络安全法》和《数据安全法》则主要针对在刑事领域打击犯罪的情形,也不能为我国执法部门进行域外行政执法提供直接的法律依据。另外,《个人信息保护法》第43条及《数据安全法》第26条虽然确立了域外数据管辖中的“对等原则”,但其适用范围模糊,对有关部门在行政执法管辖领域可否采取“对等原则”并未予以明确。

其次,我国域外数据执法管辖范围有限。以

《个人信息保护法》为例, 中国欲对存储于美国的美国个人数据进行管辖, 需以该美国人在中国境内为连接因素。这就令我国的数据执法几乎囿于境内, 域外管辖范围相较于其他国家过于狭窄。并且, 数据跨境取证是域外数据执法管辖的重要内容, 但是根据《公安机关办理刑事案件电子数据取证规则》的规定, 执法机关只能调取境内远程计算机系统中存储的数据以及境外公开发布的数据, 管辖范围十分有限。

再次, 我国域外数据执法管辖的执行难度较大。当前, 我国域外数据执法管辖权责与程序界定并不清晰。在立法层面, 我国对有关部门的域外执法职权与责任的规定都比较模糊, 并主要是一种宣示性规定。譬如, 《数据安全法》和《关键信息基础设施安全保护条例》分别赋予国家安全机关数据安全监管和关键信息基础设施安全保护职责, 但对执法机关的职权内容、履职程序以及法律责任等都未作详细规定。过于笼统的规则很难为域外执法提供充分法律依据, 不仅会带来法律解释问题, 也大大限制了域外执法工作的展开。另外, 在各国竞相扩张域外数据执法管辖的背景下, 我国的域外执法也势必面临更多有关主权的诉争以及管辖权冲突。域外数据执法权责与程序性规定细则阙如, 会增加执法管辖难度, 令执法机构在工作中愈显捉襟见肘。

三、我国域外数据执法管辖的因应对策

(一) 完善反长臂管辖的法律体系

1. 加强阻断立法, 限制他国数据管辖范围的不当扩张。通过阻断法阻断外国法律在中国境内的不当适用, 可以有效对抗外国数据执法的长臂管辖^[9]。当前, 我国尚缺乏高位阶的阻断法律。商务部于2021年出台的《阻断办法》一定程度上弥补了我国阻断立法的空白, 但该办法将阻断范围限缩在经贸及相关活动领域, 且对外国法律与措施“不当域外适用”的认定标准过于笼统, 难以为执法部门提供明确指引。因应外国域外数据执法管辖范围的不当扩张, 首先, 需完善数据管辖领域阻断立法, 以提升阻断的针对性与明确性, 为有关部门实施阻断措施提供有效指

引; 其次, 可以结合数据分类分级体系, 在数据安全治理重点领域与重点行业实现阻断规则的专门化和精细化, 重点保障关乎国家安全与公共利益的数据免受外国法律管辖; 再次, 除高位阶的阻断立法外, 也需要多层次制定和落实行政法规、部门规章等不同位阶规范性文件阻断规则, 完善阻断性法律规范体系。

阻断法阻断外国法适用, 主要是通过公法机制与私法机制共同实现的, 前者主要是对遵守外国法律者进行处罚, 后者则是对违反外国法律者实施救济^[10]。考虑到数据对国家利益的重要性, 通过事后处罚方式进行阻断可能于事无补, 数据阻断立法更应考虑如何预防数据控制者选择遵守外国法律。一方面, 制定明确的数据领域阻断清单并匹配有力的处罚措施, 以高昂的违法成本震慑数据控制者。保护本国当事人合法权益是制定阻断法的逻辑起点^[11], 由于数据要素关乎国家、民族和社会利益, 在遵循价值位阶原则和比例原则的基础上, 可以考虑适当赋予数据控制者更高的禁止性义务。另一方面, 鼓励数据控制者遵守中国法律, 为其根据阻断禁令违反外国法律或措施的行为提供必要支持。《阻断办法》第11条已经为有关部门支持数据控制者提供了法律依据, 下一步应考虑在数据领域制定具体细则。这不仅有助于充分救济数据控制者损失, 也能够增强其拒绝执行外国法令的信心。

2. 规制数据控制者行为, 强化我国数据管辖。数据控制者在面临多重管辖时作出的选择, 关乎一国数据管辖利益的实现。为强化我国对本国数据的执法管辖, 有必要对数据控制者行为进行规制, 以促使其接受中国管辖。一方面, 可以为数据控制者设定通知义务, 要求其在收到他国指令时向中国报告。必要时, 执法部门可以根据《数据安全法》第34条的规定, 要求数据控制者在向外国提供关乎国家安全、社会公共利益的数据时, 应当获得行政机关的审核与许可。另一方面, 可以为重要数据与核心数据的控制者设定数据加密义务。《数据安全法》第21条将数据分为一般数据、重要数据与核心数据。以该分类分级体系为依托, 可以要求数据控制者对持有或处理的重要数据与核心数据进行加密处理, 并严格遵守限制数据访问与流通的法律规定。

此外,可以围绕数据本地化存储规则,为数据控制者设定相应的义务。数据本地化存储是应对域外单边长臂管辖所采取的防御性措施,如法国1968年“阻断法”即禁止将涉及法国经济、商业、工业、金融或技术的信息传递给外国^[12]。当前,我国《网络安全法》第37条对重要数据的本地存储作出了一般性规定,在金融、卫生、医疗及交通等重点领域,我国也相继出台有关政策与法律,对数据本地化存储提出了一些要求。例如,《征信业管理条例》即要求征信机构应当在中国境内处理在中国采集的数据。在此基础上,可以进一步明确数据控制者本地化存储数据的义务与责任,当其收到外国数据调取或访问指令时,必须首先遵守数据本地存储与禁止跨境流动的法律规定。

3. 完善反制措施的法律依据。反制裁与阻断立法能够起到消除外国制裁对国内经济的负面影响,更好维护国家安全和利益^[13]。我国实施反制措施的主要法律依据是2021年颁布的《中华人民共和国反外国制裁法》(以下简称《反外国制裁法》),该法反制的重点是外国对我国实施的制裁与歧视性限制措施。在数据治理领域,《数据安全法》第26条规定的“对等措施”也是针对歧视性的禁止、限制等措施采取的。因此,《反外国制裁法》《数据安全法》不能为针对外国数据执法长臂管辖所实施的反制措施提供直接法律依据。《阻断办法》第12条虽然规定中国政府可以针对外国法律与措施不当域外适用进行反制,但是对反制措施的适用范围、具体类型等缺少细化规定,本质上是一种宣示性规则。应当尽快完善数据领域反制类立法,为执法机关采取反制措施提供更有力的法律支撑。同时,应当制定反制措施的实施细则,以增强反制的针对性和有效性。

另外,也需要进一步细化执法程序,以保障反制的正当性与合理性。当前,《数据安全法》和《阻断办法》规定的概括性条款是在数据执法领域采取反制措施的主要依据。以《数据安全法》第26条为例,该条款规定的反制范围是“歧视性的禁止、限制或者其他类似措施”,有关反制措施的规定则使用“对等采取措施”的概括性表述,这就为法律解释预留较大空间。诚

然,保留开放性条款是必要的,它能够增强反制措施的灵活性,更好应对错综复杂的数据管辖问题。但是,通过法律解释扩大反制措施更需要评估其正当性。因此,需要通过设置告知程序和听取执法对象意见程序等,使执法部门采取的反制措施具有充分的正当性与合理性。

(二) 完善域外数据执法管辖的法律体系

1. 通过立法手段强化执法依据。面对当前数据跨境执法依据不足、职责不清、程序混乱等问题,亟待一部高位阶的法律予以规制。

在路径选择上,若坚持《数据安全法》保护主义域外管辖立场,或无法适应当前域外数据执法需求。而《个人信息保护法》构建的“以数据处理行为发生地”与“目标指向”标准为依据的数据管辖模式,则有效扩张了我国域外数据执法范围,在当前是更为明智的选择。此外,《个人信息保护法》《数据安全法》都确立了域外数据管辖的对等原则,未来有必要在坚持尊重他国主权原则的基础上,进一步细化对等措施的适用范围、主管机关和执法手段等相关规定。因应多重管辖局面,可以依托数据分类分级体系,将关乎国家利益和重大公共利益的核心数据以列举形式明确纳入管辖范围。具体规定特定数据的管辖权,不仅是为了指引数据控制者行为,也为阻断立法、设定数据控制者义务和采取反制措施等举措提供明确的法律依据。

在具体内容上,不仅需要明确具体的域外执法机关,也需要对其享有的具体执法权作详尽规定。可以参照欧盟《通用数据保护条例》的做法,赋予我国执法机关以调查权、纠正权、许可权、强制权等执法权力,使其能够依职权调取、访问或监管数据控制者数据。同时,为执法机关设定相应的处罚权是必要的。在境内对有关主体采取强制措施,是实现域外执法的有效手段^[14]。数据持有者在面临双重管辖时,违法成本往往会成为其作出选择的重要考量。执法机关具有足够的处罚威慑,才能驱使数据控制者接受我国数据执法管辖。另外,《通用数据保护条例》的数据保护官(DPO)制度也值得借鉴。数据保护官需参与数据控制者的数据管理,不仅在地位上保持独立,其职务行为也受到相应的保护。《通用数据保护条例》还为数据保护官设定协助执法

义务, 监管机构可以直接、秘密地与数据保护官联系^[15]。我国可以借鉴欧盟经验, 探索构建利益独立的数据监管制度。例如, 要求数据控制者必须在华设立数据专员, 并保证其与数据专员不存在利益关联。执法机关通过该专员, 或能更好开展执法工作。

在执法程序方面, 需要明确域外数据执法权行使的程序规定。我国在《全球数据安全倡议》中申明了尊重他国主权立场, “未经他国法律允许不得直接向企业或个人调取位于他国的数据”。因此, 我国域外执法必须尊重他国主权, 并以“取得相对国同意”作为合法性要件。但是, 当前我国并未对执法机关请求调取域外数据作出规定, “取得相对国同意”要件也没有在程序中得到落实。有学者认为, 绕过他国政府调取域外数据不全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^[16]。但是, 在域外执法中尊重他国主权依然是不可越过的红线, 在程序规则的制定上需要充分彰显我国秉持的基本立场。如何具体完善域外执法程序, 保障执法行为的正当性与合法性, 仍有待进一步研究。

2. 通过体系解释和扩大解释延展我国域外数据管辖范围。数据活动所涉领域极为广泛, 相应的管辖范围也很庞大。有鉴于此, 执法部门需要通过对有关领域的监管法规进行体系解释和扩大解释以延展数据执法管辖范围。以反垄断领域为例, 通过体系性研究不难发现, 《中华人民共和国反垄断法》能够为执法部门的域外数据执法行为提供法条支撑。比如, 该法第38条规定国安机关可以对外资并购境内企业等参与经营者集中的活动进行审查, 第9条同时明确经营者的数据和算法、技术等属于反垄断审查的内容之一。这就赋予了国安部门调取和审查外资企业数据资料的有关权限。另外, 通过扩大解释的方法, 将数据传输地、接受地、传输经过地等数据关联地纳入“数据处理行为发生地”范围, 能够最大程度延展管辖范围, 有效增强数据安全监督与执法管辖力度。

需要强调的是, 域外执法管辖范围的确定, 除了要以国内法为基础外, 还需符合国际法规则与习惯。在全球数据治理实践中, 要求本地化存储的数据范围与他国域外管辖的数据

范围正在逐步重合^[17], 数据管辖权冲突会愈发频繁。但是, 当前国际法无法对管辖权进行排序, 属地管辖权并不当然优先于其他管辖权^[18]。笔者认为, 在面临冲突时进行国际礼让分析, 可以为域外执法行为提供合法性背书。但是, 实践中对数据利益进行礼让分析可能非常复杂, 因为数据经过汇总、分析和处理会衍生出新的信息, 这些信息的价值往往是潜在的和不易确定的。因此, 孤立地以发生管辖冲突时的特定数据进行利益权衡, 得出的结论可能未必准确。可以确定的是, 一国社会公共利益在国际礼让中是具有决定性的^[19], 而一国以本地化存储规则禁止流通的数据, 往往关乎该国的核心利益。因此, 从国际礼让原则出发, 当存在本地化存储规则时, 域外数据执法原则上应当有所克制。

3. 完善域外数据调取与取证等执法措施。当前, 我国域外数据执法难度较大, 需要探索司法协助与“公私合作”模式相结合的域外数据执法路径。出于尊重国家主权方面的考虑, 传统司法协助是我国域外执法的主要方式。我国只在有限情形下, 会直接通过数据控制者调取域外数据。比如, 《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》即有条件地授权公安机关直接通过网络在线提取电子证据和进行网络远程勘验。当前, 司法协助存在程序复杂、效率低下等问题, 尤其在调取电子数据时弊端明显^[20]。域外数据调取还会面临数据位置难以查明、数据多元储存、数据加密等技术性难题, 传统司法协助也很难克服这些障碍, 往往需要诉诸网络运营服务提供商协同解决。而通过数据控制者直接调取数据, 不仅能够提升执法效率, 也能够有效解决技术问题。当前, 美国 Google、X 等公司都允许国家安全机关直接向其调取部分非内容电子数据, 这就为探索“公私合作”的域外数据调取模式提供了可能。完善“公私合作”模式, 一方面, 公主体的执法行为需有相应法律依据, 所调取的数据应在我国管辖范围内, 确保数据调取行为具备充分的合法性; 另一方面, 在我国境内开展经营活动的域外运营商是“公私合作”的重要主体, 可以通过协议方式搭建数据

调取和访问渠道。必要时, 可以为其设定配合相关部门调取数据的义务, 并建立严密的追责体系, 追究其拒不履行义务的法律責任。

近年来, 我国对直接跨境调取数据所持的谨慎态度已有所缓和, 但是优化司法协助依然是优先选择^[21]。一方面, 执法部门应当以我国加入的国际公约、双边和多边协定为基本指引, 确保域外数据执法行为符合国际、区际司法协作的合法性要求; 另一方面, 面对数据治理国际规则缺位现状, 我国应当积极参与构建数据跨境执法国际合作机制, 提升制定国际公约、多边协定的话语权, 探索建立信息共享、合作案件优先处理和信息交换保密等国际合作机制。

四、结 语

数字经济时代下, 数据资源之于国家的战略意义凸显, 数据领域将成为国际竞争的“主战场”。在各国域外数据执法权不断扩张的现实之下, 我国数据控制权与数据安全面临挑战, 加强域外数据执法无疑将成为保障国家数据权益的重要手段。因此, 通过完善我国域外数据执法制度, 以摆脱域外数据执法管辖困境已刻不容缓。我国应当在尊重他国主权和数据管辖权的基础上, 借鉴国际经验并结合中国国情, 采取有利措施因应挑战。增强我国域外数据执法能力, 也有助于应对域外数据治理单边主义, 防止“数据霸权”蔓延, 更好地维护国际数字经济秩序。

[参考文献]

- [1] 廖诗评. 国内法域外适用及其应对: 以美国法域外适用措施为例 [J]. 环球法律评论, 2019 (3): 166-178.
- [2] 杨楠. 大国“数据战”与全球数据治理的前景 [J]. 社会科学, 2021 (7): 40-58.
- [3] 袁康, 赵宛如. 跨境数据流动中的管辖权冲突及其协调 [J]. 重庆邮电大学学报 (社会科学版), 2024 (2): 66-76.
- [4] 杨永红. 美国域外数据管辖权研究 [J]. 法商研究, 2022 (2): 146-157.
- [5] 邵怿. 论域外数据执法管辖权的单方扩张 [J]. 社会科学, 2020 (10): 119-129.
- [6] 陈东阳. 论单边跨境数据调取中的管辖权冲突 [J]. 南大法学, 2023 (2): 103-117.
- [7] 曹亚伟. 国内法域外适用的冲突及应对: 基于国际造法的国家本位解释 [J]. 河北法学, 2020 (12): 81-101.
- [8] 宋晓. 域外管辖的体系构造: 立法管辖与司法管辖之界分 [J]. 法学研究, 2021 (3): 171-191.
- [9] 郭烁. 云存储的数据主权维护: 以阻断法案规制“长臂管辖”为例 [J]. 中国法律评论, 2022 (6): 72-85.
- [10] 丁汉韬. 论阻断法的实施机制及其中国实践 [J]. 环球法律评论, 2022 (2): 176-192.
- [11] 刘桂强. 阻断法的当代发展与价值选择 [J]. 中国应用法学, 2022 (2): 183-196.
- [12] 杨成玉. 反制美国“长臂管辖”之道: 基于法国重塑经济主权的视角 [J]. 欧洲研究, 2020 (3): 1-31.
- [13] 杜玉琼, 黄子琳. 论我国反制裁法的功能及其实现路径 [J]. 河北法学, 2023 (6): 90-112.
- [14] DAN JERKER B SVANTESSON. The extraterritoriality of EU Data Privacy Law: Its theoretical justification and its practical effect on U. S. business [J]. Stanford Journal of International Law, 2014 (1): 53-102.
- [15] IT Governance 隐私小组. 欧盟通用数据保护: GDPR 合规实践 [M]. 刘合翔, 译. 北京: 清华大学出版社, 2021: 86.
- [16] 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 [J]. 环球法律评论, 2021 (1): 38-51.
- [17] 万方, 赵琳琳. 数据域外管辖趋势及我国的立法应对 [J]. 图书情报知识, 2021 (41): 136-145.
- [18] 王雪, 石巍. 数据立法域外管辖的全球化及中国应对 [J]. 知识产权, 2022 (4): 54-75.
- [19] 安子健. 数据法律冲突中使用国际礼让原则的理论基础、实践应用与中国镜鉴 [J]. 河北法学, 2024 (5): 164-182.
- [20] 王立梅. 论跨境电子证据司法协助简易程序的构建 [J]. 法学杂志, 2020 (3): 82-92.
- [21] 梁坤. 网络犯罪国际公约中的跨境调取数据条款 [J]. 当代法学, 2024 (2): 123-135.

(下转第92页)

- [21] 张伯伟. 全唐五代诗格汇考 [M]. 南京: 凤凰出版社, 2006: 172 - 173.
- [22] 王国维, 著, 佛雏, 校辑. 新订《人间词话》广《人间词话》 [M]. 上海: 华东师范大学出版社, 1990.
- [23] 袁行霈. 唐诗风神及其他 [M]. 香港: 香港城市大学出版社, 2005: 19.

A Study of the Acceptance of Chinese Imagery in Charles Wright's Poems

GAN Ting, LI Ruoxin

(School of Foreign Languages, Jimei University, Xiamen 361021, China)

Abstract: Charles Wright is unique in modern American poetry with his rich and vivid poetic images. His self-consciousness of image construction, understanding of the principle of image acquisition and grasp of the emotional structure of poetic images are closely related to his comprehension and acceptance of the image construction method of Chinese classical poetry under the influence of his symbolic mentor Ezra Pound. By tracing Wright's encounter with the poetic art of Chinese Imagery, analyzing the confluence of "connotation" and "image", explaining the emotional structure of his poetic imagery and comprehending the overall artistic conception of his poetic text, we can clearly outline his acceptance of Chinese classical poetry art Chinese Imagery.

Key words: Chinese Imagery; Charles Wright; poetry art

(责任编辑 张永汀)

(上接第 34 页)

The Challenges Facing China's Extraterritorial Data Enforcement Jurisdiction and Their Solutions

CHEN Junxiu, WANG Weihang, LI Zhi

(Law School, Fuzhou University, Fuzhou 350108, China)

Abstract: In the pursuit of securing data resources and safeguarding national data security, countries worldwide are increasingly expanding their extraterritorial jurisdiction and enhancing their enforcement mechanisms. This has given rise to two typical approaches: the US Model and the EU Model. At present, China's extraterritorial data enforcement jurisdiction faces certain limitations, primarily reflected in an insufficient legal foundation for extraterritorial data enforcement, a restricted scope of jurisdiction, and significant difficulties in the enforcement of extraterritorial data jurisdiction. To overcome these challenges, it is necessary, on one hand, to improve the legal framework against long-arm jurisdiction, strengthen blocking legislation to curb the undue expansion of foreign data jurisdiction, regulate the conduct of data controllers to reinforce China's data jurisdiction, and establish a solid legal basis for countermeasures. On the other hand, it is essential to develop a robust legal system for extraterritorial data enforcement jurisdiction, enhance the legal foundation for enforcement through legislative measures, provide systematic and expansive interpretations of China's extraterritorial data jurisdiction, and enhance enforcement mechanisms including cross-border data retrieval and evidence collection.

Key words: extraterritorial data enforcement; data sovereignty; data jurisdiction; cross-border data evidences collection

(责任编辑 冯庆福)