国际法研究

数据主权与长臂管辖的理论分野与实践冲突

刘天骄

内容提要:关于数据跨境流动的法律规制,全球虽未形成统一规则,但其核心争议始终围绕数据与主权的关系展开。依托现代国际公法秩序的“数据主权论”坚持数据治理依然从属于传统主权,其理论沿革从网络主权向技术主权不断延伸和发展,而建立在互联网世界主义理想下的“数据自由论”强调数据可以排除主权干预地自由流动,并集中表现为对数据及其控制者的长臂管辖。两种秩序主张在实践中呈现彼此竞争又相互交融的复杂样态。实践中,体现二者直接冲突的案例屡见不鲜,而且同一主体主张双重秩序的混合范式时有发生。在此背景下,中国数据跨境流动的立法进路需要平衡两种秩序之间的冲突。既要坚持以数据主权为基础的秩序构建,在参考欧盟最新数字战略的基础上适当扩大现有理论外延,也要正视数字经济时代效率价值的重要地位,避免僵化地固守数据主权,注意行使主权的必要谦抑。同时还需重视对长臂管辖的立法阻断,在兼顾安全与发展的基础上通过内外联动的法律体系推动互联网国际治理体系的完善。

关键词:跨境数据　数据主权　长臂管辖　全球治理

刘天骄,复旦大学法学院博士后研究人员。

随着数字经济的发展,数据跨境流动成为关系世界贸易和各国利益的核心议题。关于数据跨境的法律规制,全球虽未形成统一规则,但其核心争议始终围绕数据与主权的关系展开。依托现代国际公法秩序的“数据主权”论坚持数据治理依然从属于传统主权的范畴,而建立在所谓互联网世界主义理想下的“数据自由”论则强调数据可以排除主权干预地自由流动。

值得注意的是,一方面,体现二者直接冲突的案例屡见不鲜,例如催生 2018 年美国《澄清域外合法使用数据法案》(*Clarifying Lawful Overseas Use of Data Act*)通过的 United

States v. Microsoft Corp 案以及 2017 年 Google Inc. v. Equustek Solutions Inc 案;[1]另一方面,同一主体主张双重规则的混合范式也时有发生,例如欧盟在 2020 年发布的数字战略文件中明确提出"技术主权",但在欧盟《通用数据保护条例》中又制定长臂管辖条款。[2]而随着越来越多的新兴国家参与网络空间的治理,过去由欧美主导的传统立法范式正不断被打破和重塑,崭新的全球数据治理法律体系正在形成。[3] 深入梳理两种秩序背后的理论渊源,剖析技术化法条背后的隐秘主张,揭示更深层次的利益博弈与秩序张力,对于完善我国数据跨境流动立法和推动构建互联网国际治理体系,都具有重要意义。

一 理论渊源:数据主权与数据自由

跨境数据治理的前提性问题在于数据与主权的关系到底如何? 至少从詹姆斯一世时代(1566 – 1625 年)开始,人们就已经意识到信息技术对国家主权的侵蚀。尽管当时印刷机与出版物的推广削弱了王室与教会的权力,但由于传统信息媒介仍在一国物理空间的可控范围内,所以主权者依然在其领土内保持着基本的管辖与支配。[4] 然而随着现代科技的发展,互联网的出现掀起了对主权理论的全新冲击。超越现实疆域的网络空间不仅对强调地域性的传统主权产生日趋深远的影响,更对以主权国家为基础的国际公法秩序造成愈加侵略性的威胁。一方面,具备虚拟性、开放性与无界性等特征的互联网与注重现实性、封闭性和排他性的主权概念形成了一定的理论张力;另一方面,全球化背景下的网络空间治理由于各国软硬实力的悬殊以及通行法律规范和国际司法机构的欠缺,在诸多领域发生着国家间管辖权乃至主权利益的冲突和碰撞。正是在此背景下,依托于互联网平台的数据流动问题同样引发了对主权的挑战。而近年来形成的两种相互竞争彼此交融的跨境数据治理秩序也恰恰是在数据与主权的关系问题上有截然不同的主张。"数据主权"论坚持关于数据的治理依然从属于传统主权的范畴,而"数据自由"论则强调数据可以排除主权干预地自由流动。"棱镜门"事件以来,网络空间主权和治理模式的世界论战更为激化,其背后不仅包含错综复杂的利益博弈,还有着更深层次的地缘政治

〔1〕 在 United States v. Microsoft Corp 案中,主张数据主权的爱尔兰与实践长臂管辖的美国发生了跨境数据治理的冲突。在 2017 年的 Google Inc. v. Equustek Solutions Inc 案中,加拿大法院要求谷歌公司删除在全球范围内的引擎搜索结果,而谷歌公司认为加方的主张是在监督外国主权国家(美国)执法活动的长臂管辖。同年,法国最高行政法院向欧洲法院提交了一份关于谷歌公司在全球范围内适用"被遗忘权"制度的案件,上述类似的争议也发生在法国法院和谷歌之间。United States v. Microsoft Corp. , 138 S. Ct. 1186 (2018); Jennifer Daskal, Google Inc. v. Equustek Solutions Inc. , 112 *American Journal of International Law* 727, 727 – 733, 2018; Andrew Keane Woods, Litigating Data Sovereignty, 128 *Yale Law Journal* 328, 328 – 406, 2018; Martínez José Manuel, and Juan Manuel Mecinas, Old Wine in a New Bottle?: Right of Publicity and Right to Be Forgotten in the Internet Era, 8 *Journal of Information Policy* 362, 362 – 380, 2018.

〔2〕 《欧洲数据战略》《塑造欧洲的数字未来》《人工智能白皮书》,https://ec. europa. eu/info/strategy/priorities – 2019 – 2024/europe – fit – digital – age/european – data – strategy_en, https://ec. europa. eu/commission/presscorner/detail/en/ip_20_273, https://ec. europa. eu/info/sites/info/files/commission – white – paper – artificial – intelligence – feb2020_en. pdf,最近访问时间[2020 – 03 – 07]。

〔3〕 参见许多奇:《个人数据跨境流动规制的国际格局及中国应对》,《法学论坛》2018 年第 3 期,第 130 页。

〔4〕 Perritt, Henry H. Jr. ,The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance, 5 *Indiana Journal of Global Legal Studies* 423, 425, 1998.

角力。因此,真正理解对数据与主权关系的不同诠释,就不能局限于命题表述本身,而需要追溯其中的理论渊源,梳理它们的发展线索,而这也是进一步分析技术化法条背后隐秘主张的关键基础。

(一)延续传统主权脉络的“数据主权”论

1. 网络主权视域下的数据主权

由于数据以网络为重要传播渠道,因此数据与主权的关系在很大程度上和网络与主权的关系密切相联。在既有的理论梳理中,网络主权的概念延续着传统主权的脉络,强调尽管网络具备一系列的新技术特征,但关于网络的治理仍然从属于国家主权,网络主权是传统主权在网络空间的自然延伸,也是现实主权在网络虚拟空间的逻辑映射。[5] 虽然全球化以来学界关于主权的解释有着愈发严重的分歧,但大多认可主权对内具有最高性、领土性和排他性三个特征,对外则不受另一主权的控制,强调应在国际法的指引下调整独立平等的主权国家间关系。[6] 据此,网络主权在实践中也呈现内外两个维度。前者表现为一国在其领土范围内对信息通信技术活动(针对网络虚拟角色)、信息通信技术系统(针对平台)及其承载数据(针对网络虚拟资产)具有最高的、排他的管辖权与支配力;[7] 后者反映为在以主权国家为单位构建的国际公法秩序下,各国遵守《联合国宪章》有关国际关系的基本原则,不受他国干涉地治理本国网络空间,以平等参与协同共治的理念解决争端、推动发展,坚持网络空间和现实空间在国际制度上的一致性。[8]

上述观念在跨境数据治理领域体现为“数据主权”的主张。在延续传统主权概念的基础上,强调关于数据的治理仍然从属于国家主权,各国有权独立自主地规制在其领土范围内收集和产生的数据,跨境数据的法律规制应维系以主权国家为基础的国际公法秩序,以尊重主权差异为原则,以联合国及其下设的国际仲裁机构和国家间司法互助协议为解决争议的主要渠道,通过各国平等参与实现跨境数据的共享共治。[9] 其中,数据主权的范畴不仅包含国家对其境内“数据控制者”(收集、使用或披露个人信息的组织、机构或个人)的管辖,而且更强调国家对网络空间中所承载“数据”本身的治理。[10]

2. 技术主权对数据主权的扩张

技术主权是欧盟于 2020 年 2 月密集发布的三份重要数字战略文件[《欧洲数据战

〔5〕 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 日第 004 版。

〔6〕 Andrew Keane Woods, Litigating Data Sovereignty, 128 *Yale Law Journal* 328, 351 – 371, 2018; Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignty, 5 *Global Legal Studies* 475, 475 – 476, 1998;参见[美]乔治·萨拜因著:《政治学说史》(下卷),邓正来译,上海人民出版社 2010 年版,第 98 页;俞可平:《论全球化与国家主权》,《马克思主义与现实》2004 年第 1 期,第 4 – 21 页。

〔7〕 参见方滨兴主编:《论网络空间主权》,科学出版社 2017 年版,第 82 页。

〔8〕 参见黄志雄主编:《网络主权论——法理、政策与实践》,社会科学文献出版社 2017 年版,第 70 页。

〔9〕 参见 Jack Goldsmith, Sovereign Difference and Sovereign Deference on the Internet, 3 *The Yale Law Journal Forum* 818, 818 – 826, 2019;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,第 188 – 208 页;齐爱民、盘佳:《数据权、数据主权的确立与大数据保护的基本原则》,《苏州大学学报(哲学社会科学版)》2015 年第 1 期,第 64 – 70 页;翟志勇:《数据主权的兴起及其双重属性》,《中国法律评论》2018 年第 6 期,第 196 – 202 页。

〔10〕 Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, pp. 15 – 17; Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, in C. Czosseck, R. Ottis, K. Ziolkowski (eds.), *2012 4th International Conference on Cyber Conflict*, NATO CCD COE, 2012, p. 7.

略》(*A European Strategy for Data*)《塑造欧洲的数字未来》(*Shaping Europe's Digital Future*)和《人工智能白皮书——追求卓越和信任的欧洲方案》(*White Paper: On Artificial Intelligence-A European Approach to Excellence and Trust*),下称"《人工智能白皮书》"]中首次提出并贯穿始终的重要概念。该概念与数据主权密切相关,但在技术、规则和价值三个方面大大拓宽了原有理论的外延。

其一,在技术层面,技术主权强调欧盟在数据经济的关键技术和基础设施领域要确保相关能力的自主性,减少对全球其它地区的依赖。例如《塑造欧洲的数字未来》强调"欧洲技术主权的出发点,是确保我们的数据基础设施、网络和通信的完整性和恢复力。这就需要创造正确的条件,让欧洲去发展部署自己的关键能力,从而减少欧洲对全球其它地区关键技术的依赖"。[11]

其二,在规则层面,技术主权不仅关注欧盟要参与并制定下一代数据处理基础设施的技术标准(如5G),还极其看重欧盟在数据治理领域制定法律的权力,并进而提出要构建"单一的欧洲数据空间",以确保空间中通用的欧洲规则和高效的执法机制。《欧洲数据战略》指出,"欧盟委员会将利用其组织召集能力和欧盟的资助计划来强化欧洲对数据敏捷经济的技术主权。这将通过关于如何处理个人数据(尤其是匿名)以及构建用于数据处理的下一代基础设施的标准制定、工具开发、最佳实践收集来完成。"[12]而在三份数字战略文件中,欧盟多处提及《通用数据保护条例》在统一数据保护规则、推进数字单一市场方面的巨大作用。在该条例成功经验的基础上,《欧洲数据战略》和《人工智能白皮书》进一步提出了明确的立法计划,例如旨在激励各方数据共享的《数据法案》和针对科技巨头收集、使用、共享数据中限制创新和竞争问题的《数字服务法案》等。[13]

其三,在价值层面,技术主权强调欧洲要加强在数字时代定义并输出自身价值观的能力。《塑造欧洲的数字未来》写道,"欧洲的技术主权并不针对任何人,而是通过关注欧洲人民和欧洲社会模式的需求而确定的","数字欧洲应该反映出欧洲最好的属性:开放、公平、多样化、民主和自信",为此,欧洲要发展"服务于人的技术"、打造"公平竞争的经济"、建设"开放、民主和可持续的社会","欧洲数字化转型的方式,要能够增强欧洲的民主价值观,尊重欧洲人民的基本权利,并有利于实现可持续发展、气候中立和资源节约型经济"。[14]《欧洲数据战略》指出,欧洲愿意与"有同样数据治理标准和价值观的可信赖伙伴国开展合作,在符合其与欧洲相一致的价值观的条件下,为愿意赋予公民更强的数据控

〔11〕《塑造欧洲的数字未来》,https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273,最近访问时间[2020-03-07]。

〔12〕《欧洲数据战略》,https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en,最近访问时间[2020-03-07]。

〔13〕《欧洲数据战略》,https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.《人工智能白皮书》,https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf,最近访问时间[2020-03-07]。

〔14〕《塑造欧洲的数字未来》,https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273,最近访问时间[2020-03-07]。

制权的其他国家提供支持”。[15]

如果说数据主权还是在法律规制的层面对内强调数据治理从属国家主权，对外倡导数据跨境遵守国际公法秩序，那么技术主权则在延续传统主权脉络的基础上，从技术、规则和价值三个层面强有力地扩张了原有理论的内涵。正如欧盟委员会主席冯德莱恩（Ursula von der Leyen）所述，技术主权“描述了欧洲必须具有的能力，即基于自己的价值观、遵守自己的规则、做出自己的选择的能力”。[16]

（二）基于互联网世界主义的“数据自由”论

互联网世界主义是指在认可全世界人类同属一个共同体的意识形态下，基于互联网的虚拟性、开放性与无界性等技术特征，将网络空间诠释为一种独立于现实空间的，接近公海、太空的“全球公域”。[17] 在这种也被一些学者称为互联网乌托邦主义的理想下，人们认为网络空间可以排除传统主权的束缚，实行独立于国家的高度自治。而与此一致的“数据自由”论，则进一步强调数据的虚拟性、自由性和非排他性等技术特征能够超越传统的主权范畴，特别是主权理论中强调国家边界的领土原则，主张数据可以不受国家主权管治的自由跨境流动，数据治理应主要依靠弱主权化甚至去主权化的方式，也即以私营部门、民间团体和国家政府共同参与的“多利益攸关方模式”解决纠纷，实行自治。[18]

在理论渊源上，这股思潮原先带有 20 世纪 60 年代新左派和反文化运动的反体制与反国家主义冲动，其最重要的信条是网络空间要独立于政府和企业，摆脱权力与资本的宰制。正如约翰·巴洛在《网络独立宣言》中指出，“工业世界的政府们，你们这些令人生厌的铁血巨人们，我们来自网络空间——一个崭新的心灵家园。我代表未来，要求过去的你们别管我们。在我们这里，你们不受欢迎。在我们聚集的地方，你们没有主权……网络空间并不处于你们的领地之内……你们不了解我们的文化和我们的伦理，或我们不成文的‘法典’（编码），与你们的任何强制性法律相比，它们能够使我们的社会更加有序”，互联网世界主义者试图在虚拟空间中构建一个全新的、独立的共同体，彻底排除现实空间的干预。[19]

---

〔15〕《欧洲数据战略》，https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en，最近访问时间[2020-03-07]。

〔16〕Ursula von der Leyen, Op-ed by Commission President von der Leyen, https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260，最近访问时间[2020-03-07]。

〔17〕Department of Defense Washington, D.C. Strategy for Homeland Defense and Civil Support, https://fas.org/irp/agency/dod/homeland.pdf，最近访问时间[2020-03-07]；Hillary Rodham Clinton, Remarks on Internet Freedom, https://20092017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm，最近访问时间[2020-03-07]。

〔18〕参见姜涛著：《数据化：由内而外的智能》，中国传媒大学出版社有限责任公司 2018 年版，第 14-26 页；Albright Stonebridge Group, Data Localization: A Challenge to Global Commerce and the Free Flow of Information, https://www.albrightstonebridge.com/news/data-localization-challenge-global-commerce-and-free-flow-information，最近访问时间[2020-03-07]。

〔19〕参见刘晗：《域名系统、网络主权与互联网治理：历史反思及其当代启示》，《中外法学》2016 年第 2 期，第 518-535 页；[美]约翰·P.巴洛：《网络独立宣言》，李旭、李小武译，高鸿钧校，载《清华法治论衡》（第四辑），清华大学出版社 2004 年版，第 509-511 页；David Johnson and David Post, Law and Borders: The Rise of Law in Cyberspace, 48 *Stanford Law Review* 1367, 1367-1402, 1996; Timothy S. Wu, Cyberspace Sovereignty?, 10 *Harvard Journal of Law and Technology* 647, 647-665, 1997。

需要注意的是,网络自由或数据自由的概念往往被置于经济和政治的“单边主义”语境中使用。例如有学者指出,基于数字经济中的自由与效率价值,强硬的法律结构会“不可避免地阻碍商业活动”,任何阻碍数据跨境流动的法律政策均是设置贸易壁垒的表现,因此在互联网的“自由市场”中,应当彻底排除国家权力的干预。[20] 还有人认为网络主权是在阻挠互联网的自由和开放,并终将导致网络空间的“巴尔干化”。[21]

必须补充的是,在各国科技与经济实力存在巨大差异的前提下片面地追求数据自由或网络自由,其实是通过排除他国在领土之内的主权管辖而去固化一些国家业已建立的“数据优势”,在看似没有边界的虚拟空间担任立法者。[22] 因为只谈自由而忽视公平的规则无疑是有利于强者而有损弱者的,其实质是在维系既有的不平等竞争格局,剥夺新兴国家在相关领域的发展权,而强调“数据主权”恰恰是防守性地应对“数据自由”背后的扩张性。[23]

不难看出,“数据自由”论更看重数字经济背后的自由与效率,而“数据主权”论更关注其中的安全与发展,这也导致了二者在数据与主权的关系问题上有着彼此冲突的立场。事实上,理论的主张都必然与现实的诉求密切相关,各国关于数据治理的法律规制也正是基于不同的利益而选择了对其有利的理论支撑,呈现出彼此竞争、相互交融的复杂状态。

二、实践表达:数据主权的双重进路

对于“数据主权”论而言,问题的关键在于当这种主张试图转化为现实法律时,究竟如何具有可行性地治理虚拟空间中无形、无界、自由的数据。换句话说,国家如何通过具体规则实现对其领土内数据的主权能力。由于该理论延续传统主权的脉络,包含最高性、领土性和排他性等基本原则,因此其治理秩序的构建需要紧紧围绕政治体的疆域和边界展开。因为只有将虚拟空间的数据纳入现实空间的治理,国家才可能在领土之内实现最高且排他权力的构建。聚焦到数据跨境流动领域,究竟是以保护权利作为出发点,还是国家直接强制介入,构成了两条不同的实践表达进路,分别是以欧盟为代表的严格限制数据跨境流动模式和越来越多新兴国家采取的强制数据本地化存储模式。

(一)间接保护权利:严格限制数据跨境流动

欧盟从权利保护的历史传统出发,将数据权视作一种基本人权,通过主权者创建严格

---

〔20〕 参见[英]戴恩·罗兰德、伊丽莎白·麦克唐纳著:《信息技术法》,宋连斌等译,武汉大学出版社 2004 年版,第 308 页。

〔21〕 Andrew Keane Woods, Litigating Data Sovereignty, 128 *Yale Law Journal* 328, 351 – 371, 2018.

〔22〕 参见许多奇:《个人数据跨境流动规制的国际格局及中国应对》,《法学论坛》2018 年第 3 期,第 130 – 137 页;阚道远:《美国“网络自由”战略评析》,《现代国际关系》2011 年第 8 期,第 18 – 23 页;刘天骄:《大西洋立法者之争》,《开放时代》2016 年第 6 期,第 160 – 169 页。

〔23〕 Evgeny Morozov, Who's the True Enemy of Internet Freedom-China, Russia, or the US? https://www.theguardian.com/commentisfree/2015/jan/04/internet – freedom – china – russia – us – google – microsoft – digital – sovereignty,最近访问时间[2020 – 03 – 07]。

限制数据跨境流动的规则,以不直接介入具体跨境场景的方式间接保护数据主体的数据权利。[24] 2016 年 4 月,欧盟作为数据主权主体颁布了规制个人数据的《通用数据保护条例》,该条例于 2018 年 5 月正式生效。由于条例要求欧盟境外的数据接收方在达到与其相同的数据保护水平时数据才可跨境,该条例也被称为史上最严格、保护水平最高的数据保护规则。

条例第一章第 1 条指出,条例的主旨和目标在于"保护自然人的基本权利和自由,尤其是自然人的个人数据保护权"。条例第五章围绕"个人数据向第三国或国际组织的传输"作出规定。具体而言,数据跨境流动的方式包含两类,一是欧盟委员会认定第三国的立法、数据保护制度能够达到与条例相同的数据保护水平;二是当欧盟委员会尚未做出上述认定,但欧盟境外的数据接收方能够主动采取适当的保护措施,例如有约束力的公司内部规则,确保在境外提供与条例相同的数据保护水平。只有满足上述条件之一,欧盟数据才可跨境。[25]

不难看出,在这两种情况中作为数据主权主体的欧盟均不直接介入具体场景中的数据跨境,而是通过判断数据接收方的数据保护水平是否达到标准来间接严格限制数据的流动。在这种模式中,公权力主体(国家)淡入数据跨境的背景之中而不直接介入,数据主权的意志通过明示数据流动基本原则、界定行为主体权利和义务等方式,使位于前台的数据主体(普通个人)、数据控制者(收集、使用或披露个人信息的组织、机构或个人)及其他相关方自主达成具体场景中的数据跨境流动安排。由于数据主权意志已有体现,公权力往往只需在事中或事后出场,根据既定的数据流动基本原则对私人主体自主达成的数据跨境流动安排给予核验即可,因此该进路也被一些学者称为"主权内化于私权"模式。[26]

(二)主权直接参与:强制数据本地化存储

与欧盟不直接介入具体场景保护数据权利不同,"主权直接参与"模式通常体现为数据主权主体以公权力直接介入的方式,与数据主体、数据控制者及其他相关方共同作为具体场景中的数据跨境流动安排的行为主体。作为数据主权主体的国家,往往在事前需要根据具体场景中的数据跨境流动给予审批或评估,做出个案裁量,深度参与最终达成的跨境流动安排。[27] 在这种模式中,又以国家对数据存储提出本地化的强制要求为数据主权最强烈的表现形式,其目的是将自由流动的虚拟数据限制在明确的领土范围之内,从而依属地管辖将其纳入现实疆域的国家治理。

我国《网络安全法》第 37 条明确指出,关键信息基础设施的运营者在中国境内运营收集和产生的个人信息和重要数据必须存储在境内。如因业务确需向境外提供的,应按

〔24〕 参见许多奇:《个人数据跨境流动规制的国际格局及中国应对》,《法学论坛》2018 年第 3 期,第 130 - 137 页。

〔25〕 参见《通用数据保护条例》第 1 条以及第 44 - 50 条,https://gdpr - info. eu/,最近访问时间[2020 - 03 - 07]。

〔26〕 参见洪延青:《在发展与安全的平衡中构建数据跨境流动安全评估框架》,《信息安全与通信保密》2017 年第 2 期,第 32 - 62 页。

〔27〕 参见洪延青:《在发展与安全的平衡中构建数据跨境流动安全评估框架》,《信息安全与通信保密》2017 年第 2 期,第 32 - 62 页。

相关办法报有关部门安全评估。第66条更是进一步规定了违反第37条所需承担的法律责任。[28] 俄罗斯2015年生效的第242－FZ号联邦法律要求对俄罗斯"公民个人数据的收集、记录、整理、积累、存储、更新、修改和检索均应使用俄联邦境内的服务器"。[29] 澳大利亚2012年生效的《个人控制电子健康记录法案》更是在第77条规定涉及个人信息的健康记录只能留存于澳大利亚境内，不得携带出境，否则将予以处罚。[30]

据统计，目前全球有超过60个国家提出了数据本地化存储的要求，既包括中国、俄罗斯、尼日利亚、印度等发展中国家，也涉及加拿大、澳大利亚等发达国家和地区。相较于发达国家，新兴发展中国家的规制更为严格，而各国通过立法要求数据本地化存储的趋势在2000年以后呈现显著上升的趋势。[31]

值得注意的是，在"主权直接参与"的进路中，除保护数据主体的数据私权维度之外，维护国家数据主权的公权维度居于相关立法主旨中的重要地位。比如我国《网络安全法》第1条指出，为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。俄罗斯第242－FZ号联邦法律作为对第149－FZ号《信息、信息技术与信息保护》法律的修订，在第三部分基本原则中也包含"保障俄罗斯联邦建立信息系统、运作信息系统及其所载信息安全"的内容。[32] 可以看出，数据权既有关权利义务的分配，更有关安全与保护。因此有学者主张，数据权应当包含私权、公权与主权三个维度。[33]

总体而言，不论是"间接保护权利"还是"主权直接参与"，虽然两种进路中国家介入的深度和维度不同，公权力拥有的裁量空间也不同，但数据主权的意志均通过具体法律得到了表达，并且二者都将虚拟空间的数据纳入了现实疆域的管辖之中，成功通过严格限制数据跨境或强制数据本地化存储的方式实现了基于领土范围内最高且排他权力的构建。

〔28〕《网络安全法》第66条规定，关键信息基础设施的运营者违反本法第27条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

〔29〕Federal Law No. 242－FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions), https://pd. rkn. gov. ru/authority/p146/p191/, 最近访问时间[2020－03－07]。

〔30〕Personally Controlled Electronic Health Records Act 2012, https://www. legislation. gov. au/Details/C2012A00063, 最近访问时间[2020－03－07]。

〔31〕Matthias Bauer, Martina F. Ferracane and Erik van der Marel, Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization, https://www. cigionline. org/sites/default/files/gcig_no30web_2. pdf, 最近访问时间[2020－03－07]；参见洪延青：《数据主权的必要谦抑：以〈网络安全法〉数据境内留存规定为例》，载黄志雄主编《网络主权论——法理、政策与实践》，社会科学文献出版社2017年版，第233－234页。

〔32〕Federal Law No. 149-FZ on Information, Informational Technologies and The Protection of Information (2006), https://www. wipo. int/edocs/lexdocs/laws/en/ru/ru126en. pdf, 最近访问时间[2020－03－07]；Federal Law No. 242-FZ on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions) (2014), https://pd. rkn. gov. ru/authority/p146/p191/, 最近访问时间[2020－03－07]。

〔33〕参见王锡锌：《数据治理中的私权、公权与主权》，http://law. zuel. edu. cn/2019/0930/c3733a224260/page. htm, 最近访问时间[2020－03－07]。

三 实践异化:数据自由与长臂管辖

与“数据主权”论下实践表达不同的是,依托“数据自由”论的跨境数据法律规制呈现出与其理论初衷相悖的现象。如前所述,“数据自由”原本是基于互联网世界主义理想所构建,试图在所谓“全球公域”中塑造普遍主义的规则去规制数据的收集、使用和披露,其核心主张是网络空间要摆脱现实空间中权力与资本的宰制,实现“超越主权”的高度自治。然而,法律本身就是主权者意志的体现,立法权也是国家主权权力中最为重要的组成部分。因此除非“数据自由”的主张者能够彻底通过去主权化或去国家化的方式制定跨境数据规则,并使这些规则在全球范围内生效,否则只要有主权国家的出场,也即通过正式的立法权制定规则,均是对“数据自由”理论基础的背离。在现实中,“数据自由”恰恰是通过与主权国家立法的紧密结合,完成了从理论到实践的异化。以“数据自由”为名的主权国家正是通过行使立法权,实现了对他国主权的超越,也就是将一国的管辖权“自由跨境”地延伸到域外,构建出挑战他国主权的长臂管辖。

(一)长臂管辖的界定与制约

长臂管辖原先是美国民事诉讼中的概念,是指当非法院地居民与法院地之间存在某种最低限度的联系,同时原告提起的诉讼又产生于这种联系时,法院可以对被告主张管辖权,并对其作出有约束力的判决。换句话说,地方法院在满足特定条件时可以超越“属地管辖”将管辖权延伸至域外。[34] 而当长臂管辖置于国际语境中时,其理论基础则是管辖中的“效果原则”,即只要某个在国外发生的行为在本国境内产生了“效果”(最低限度联系),无论行为人是否具有本国国籍或者住所,也无论该行为是否符合当地法律,只要此种效果使一国法院行使管辖权并非完全不合理,该国法院便可对因为此种效果而产生的诉因行使管辖权。[35]

不难看出,一国在国际领域适用长臂管辖极易与行为人所在国的“属地管辖”或“属人管辖”发生冲突,因此国际法中通行的规则是对长臂管辖进行制约,即除非在某些公认的例外情况下,一国不应在另一国的领土之上行使国家管辖权,否则不仅是对他国主权的侵犯,也是对主权平等、互不侵犯等国际公法基本原则的破坏。[36]

(二)数据自由与长臂管辖

随着大数据时代的到来,以领土范围为标准的传统属地管辖界限逐渐模糊,而以属人管辖和效果原则为基础的长臂管辖凭借数据流动所载网络平台的虚拟性、开放性与无界性等技术特征,在近年来的数据跨境流动法律规制中正式出场,原先国际法中制约长臂管辖的传统共识开始松动。

---

〔34〕 Sher v. Johnson, 911 F. 2d 1357, 1361 (1990);参见郭玉军、向在胜:《网络案件中美国法院的长臂管辖权》,《中国法学》2002 年第 6 期,第 155 - 168 页。

〔35〕 参见李庆明:《论美国域外管辖:概念、实践及中国因应》,《国际法研究》2019 年第 3 期,第 3 - 23 页。

〔36〕 参见杜涛:《美国联邦法院司法管辖权的收缩及其启示》,《国际法研究》2014 年第 2 期,第 82 - 95 页。

1. 高效:美国《澄清域外合法使用数据法案》长臂管辖规则的价值基础

2018 年美国通过《澄清域外合法使用数据法案》。作为对 1986 年《存储通信法案》(*Stored Communication Act*)的修正,该法案抛弃了管辖权限于"数据存储地"的国际通行标准,转而主张"数据自由"规则,明确授权美国政府可以要求数据服务商保存、备份或披露受其拥有、监管或控制的数据,而不论这些数据存储于美国境内还是境外。[37] 该法案通过管辖数据控制者及其遍布世界的云服务网络,将本限于一国领土之内的管辖权延伸到了全球,正式授予美国执法机构单方调取域外数据的权力,建立了长臂管辖规则。

值得注意的是,美国司法部发布的白皮书明确指出"高效"是《澄清域外合法使用数据法案》制定的重要价值基础。通常而言,国家间的跨境数据取证一般都是通过双边司法互助协议机制完成,但随着近年来网络犯罪的日益增加,传统取证方式效率低下、适用困难的弊端愈发凸显。[38] 而该法案的颁布,正是为"加快获取总部设在美国的全球提供商所持有的电子信息速度……长期以来我们和伙伴国一直担心司法协助程序过于繁琐,难以及时处理对电子证据日益增长的需求",法案"刷新了 20 世纪的法律框架,以应对电子通信的革命和全球技术公司对其系统配置方式的创新",它"代表了一种新的范例:一种高效的保护隐私和公民自由的方法,以确保有效地获取电子数据"。[39]

但"高效"很显然难以构成对侵犯他国公民隐私、企业数据权和国家网络主权的合法性基础。因此《澄清域外合法使用数据法案》自颁布之日起就饱受谴责和争议。尤其法案还提出在"适格外国政府"之间构建跨境执法合作区的框架,强调经美国司法机构判断符合一定标准的外国政府才能对等调取存储于美国境内的数据。[40] 换言之,该法案不仅依托"数据自由"和"高效"价值扩大了美国执法机构单方调取域外数据的权力,还巧妙地凭借美国在相关领域的优势地位,初步构建出一个以美国为中心的全球数据治理体系。[41]

2. 人权:欧盟《通用数据保护条例》长臂管辖的法理基础

欧盟《通用数据保护条例》第一章第 3 条规定,条例不仅"适用于设立在欧盟内的(数据)控制者或处理者对个人数据的处理,无论其处理行为是否发生在欧盟内","适用于对欧盟内数据主体的个人数据处理,即使控制者和处理者没有设立在欧盟内,但只要其处理

---

〔37〕 参见《美国〈澄清域外合法使用数据法〉译文》,张露予译,载周汉华主编《网络信息法学研究》,中国社会科学出版社 2018 年版,第 295 - 307 页。

〔38〕 比如一国地方侦查机关若要搜查谷歌公司存储于美国境内的邮件内容数据,按常规程序需首先将请求逐级上报该国中央主管机关,然后由后者将协助请求按美方要求的形式发送给美国司法部国际事务办公室。该办公室审查后将该协助请求交由检察官处理,然后再由后者向对数据有管辖权的法院申请搜查令状。之后警务人员方可持令状要求谷歌公司提供相应数据。统计数据表明,整个协助程序通常需耗费 10 个月甚至更长时间。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,第 188 - 208 页。

〔39〕 参见美国司法部白皮书:《推动全球公共安全、隐私和法治:云法案的目的和影响》,洪延青等译,https://www.justice.gov/dag/cloudact,最近访问时间[2020 - 03 - 07]。

〔40〕 参见《美国〈澄清域外合法使用数据法〉译文》,张露予译,载周汉华主编《网络信息法学研究》,中国社会科学出版社 2018 年版,第 295 - 307 页。

〔41〕 参见强世功:《帝国的司法长臂——美国经济霸权的法律支撑》,《文化纵横》2019 年 8 月刊,第 84 - 93 页。

行为”满足一定的条件,还“适用于设立在欧盟之外,但控制者所在地依据国际公法适用欧盟成员国法律的控制者进行的个人数据处理”。[42] 这意味着任何机构只要涉及对欧盟公民个人数据的处理,不论其是否位于欧盟境内,都可能受制于该条例。条例因而成为事实上的“世界性法律”,长臂管辖规则由此建立。

不同于美国的“高效”原则,在欧洲法律价值体系中,效率远低于“人权”。欧盟也正是在将数据权理解为一种基本人权的理论基础上制定了强有力的保护措施。尽管大数据时代有关个人数据权的外延不断在扩大,但其法律基础始终围绕《欧洲人权公约》第 8 条关于“私人和家庭生活、住所和通信”得到尊重的权利展开。欧洲人对数据的理解也至今延续传统时代的隐私权观念。在人们看来,技术进步并不能减少个人对隐私侵权的警惕,恰恰相反,各种新型技术可能对个人隐私带来更大的威胁。也正是在此观念的影响下,《通用数据保护条例》通过赋予数据主体更大权利、加重数据控制者或处理者责任义务以及强调条例域外效力(长臂管辖)的方式试图最大限度地保护欧盟公民的数据权利。[43]

尽管建立在欧洲人权的法理基础上,该条例的长臂管辖规定同样需要审视。由于涉及到他国公民隐私、企业数据权和国家网络主权的问题,因此并非只要欧盟单方面出台相关法律,欧盟之外的其他国家也应视其正当且必然遵守。事实上,该条例不仅本身并没有对管辖权的延伸,即对超越主权领土范围的管辖做出正当化、合理化的充分证明,同时在进入国际领域,即面对其他国家对该条例的承认程度、应对措施和可能发生的冲突情况都缺少明确的解决途径。

四 余 论

不可否认,数据跨境流动已经成为各国立法博弈的新领地。随着越来越多的新兴国家参与网络空间的治理,过去由欧美主导的传统立法范式正不断被打破和重塑,崭新的全球数据治理法律体系正在形成。在此背景下,中国数据跨境流动的法律规制格外重要。因为其不仅涉及中国公民和企业的数据权利,攸关中国的网络主权和国家安全,还关乎全球网络空间的规则构建。基于前文的理论分析与实践考察,或可从四个方面思考我国立法的路径选择。

首先,中国基于“数据主权”的秩序塑造,可参考欧盟最新数据战略中“技术主权”的主张,适当扩大现有“数据主权”对内强调数据治理从属国家主权,对外倡导数据跨境遵守国际公法秩序的理论外延。其一,在技术层面,积极推动立法扶持我国在数据经济关键技术和基础设施领域的建设和发展,确保相关能力的自主性,减少对全球其它地区的依

〔42〕 第 2 款适用的具体条件是(a)发生在向欧盟内的数据主体提供商品或服务的过程中,无论此项商品或服务是否需要数据主体支付对价;或(b)是对数据主体发生在欧盟内的行为进行监控。参见《通用数据保护条例》,https://gdpr-info.eu/,最近访问时间[2020-03-07]。

〔43〕 参见叶开儒:《数据跨境流动规制中的“长臂管辖”——对欧盟 GDPR 的原旨主义考察》,《法学评论》2020 年第 1 期,第 106-117 页。

赖。其二,在规则层面,既要继续参与制定最新数据处理基础设施的技术标准,还需进一步完善数据领域立法,兼顾个人数据保护、跨行业的数据共享以及数据主权和国家安全。例如,已纳入2020年正式立法计划的《个人信息保护法》和《数据安全法》可在结合本国国情的基础上参考欧盟《通用数据保护条例》《数据法案》和《数字服务法案》的相关规定。其三,在价值层面,不同于欧盟数字战略(输出欧洲民主价值观)和美国《澄清域外合法使用数据法案》(判断"适格外国政府")的规定,中国数据治理的价值目标是坚持在尊重各国网络主权的基础上,开放互信的携手共建网络空间命运共同体。[44]

其次,正视数字经济时代"效率"价值的重要地位,避免过度僵化地固守传统主权,注意行使数据主权的必要谦抑。数据主权最强烈的表现形式是强制数据的本地化存储,但在网络时代,数据恰恰因快速流动而获得价值。因此在立法时需避免在数字市场中形成不必要的贸易壁垒,徒增数据交易成本,破坏互联网互联互通的基本特性。具体而言,要提升和优化我国数据跨境流动立法程序的可操作性,在保证数据安全和做好风险防范的基础上尽可能提高相关流程的效率。例如对数据进行科学分类,明晰可跨境数据的种类、处理方式以及相应责任。既为相关数据主体提供可预见性的判断标准,也为国家规制数据跨境提供更为明确的执法依据。[45]

再次,注意对"数据自由"下长臂管辖规则的立法阻断。欧盟曾通过启动"阻断法案"保护因美国国内法的域外制裁而受波及的欧洲企业。[46] 中国也可结合本国国情参考通过阻断立法阻止《澄清域外合法使用数据法案》《通用数据保护条例》等他国长臂管辖对中国数据主体的适用,有效保障我国的公民隐私、企业数据权和国家网络主权。其一,制定相关国家涉及长臂管辖的法律附录,从立法源头上否认相关条款的域外效力。其二,原则上禁止中国企业遵守附录所列法律以及外国法院据此做出可能损害中国合法利益的判决和行政决定。如若企业欲遵守相关制裁措施必须经过国家主管部门的通知或批准。其三,制定相关损害赔偿条款。自然人和法人可因附录所列法律制裁造成的损失向有关实体请求赔偿。其四,明晰阻断法案的执行和制裁机制。值得注意的是,阻断法案的制定需要科学考虑相关主体的可执行性,不能仅仅通过单方面增加企业责任的方式进行阻断,还需考虑为其提供综合有效的保障措施和援助渠道。

最后,构建内外联动的法律体系,推动开放且主动的治理方案。数据跨境治理从诞生伊始就关乎国内法与国际法的内外联动。一方面,对公民、企业和国家数据权的保护,需要国内法律和政策提供制度保障;另一方面,由于数据跨境涉及他国公民、企业或国家的数据权,因此相关规则的正当性、合理性与必要性理应接受国际主体的共同检验。在此背景下,中国数据治理的立法就不能仅仅是防守性地应对数据自由或长臂管辖可能带来的

〔44〕 参见世界互联网大会组委会:《携手构建网络空间命运共同体》,http://www.wicwuzhen.cn/web19/release/release/201910/t20191016_11198729.shtml,最近访问时间[2020-03-07]。

〔45〕 参见许多奇:《个人数据跨境流动规制的国际格局及中国应对》,《法学论坛》2018年第3期,第136-137页。

〔46〕 参见关依然、韩逸轩:《面对美国司法长臂管辖,欧盟"阻断法令"能走多远》,https://www.thepaper.cn/newsDetail_forward_2746181,最近访问时间[2020-03-07]。

安全风险,还需主动加强国际合作,通过创造开放的制度环境,吸引更多国际主体共同参与到全球数据经济的市场之中。

在实践中,不论是欧洲数据战略提出的“欧洲数据空间”,还是美国《澄清域外合法使用数据法案》中的“适格外国政府”,都是试图在可信赖的主体之间搭建跨境法律合作的框架,推动通用法律规则的适用和高效执法机制的建立。〔47〕 然而目前我国尚未与其他国家建立起数据跨境流动的互信机制,所提出的一些倡议也仍然停留在宽泛的理念层面,缺少技术上的可操作性,这势必会严重阻碍我国数据跨境流动的效率,影响企业跨境业务的开展,更可能丢失中国参与构建全球数据治理体系的主动性。因此,中国亟需建立科学的内外联动法律体系,以便通过多层次的国际规则谈判推广我们的治理方案,这样中国才能更有效地在兼顾安全与发展的基础上,推动互联网国际治理体系的构建。

[**Abstract**] Although there is no uniform global rule on the legal regulation of cross-border data flow, the core dispute in this field always centers on the relationship between data and sovereignty. The doctrine of data sovereignty, which relies on modern international law order, insists that data governance still belongs to traditional sovereignty and that its theoretical front line is continuously extending from network-sovereignty to technological-sovereignty, whereas the doctrine of data liberation, which is based on the idea of Internet cosmopolitanism, emphasizes that data should be able to flow freely without interference from sovereignty and is embodied in a concentrated way in the long-arm jurisdiction over data controllers. In practice, these two order propositions present a complex state of competition and integration. On the one hand, cases of direct conflict are common occurrences. On the other hand, mixed paradigm of double order advocated by the same subject sometimes happens. In this context, China's legislative approach to cross-border data flow needs to strike a balance between these two order propositions. It should adhere to the order construction based on data sovereignty and expand the extension of the existing theory in light of the latest digital strategy of EU while laying emphasis on efficiency value in digital economy era, avoiding rigid adherence to data sovereignty, and exercising necessary sovereignty-deference. Moreover, China should also attach importance to legislative blocking of the long-arm jurisdiction and promote the improvement of international Internet governance system through the coordination of internal and external legal systems on the basis of attaching equal importance to both security a nd development.

(责任编辑:郑 佳)

〔47〕 《欧洲数据战略》,https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en,最近访问时间[2020-03-07];参见《美国〈澄清域外合法使用数据法〉译文》,张露予译,载周汉华主编《网络信息法学研究》,中国社会科学出版社 2018 年版,第 295-307 页。