主题研讨

自由与安全:数据跨境流动的中国方案

许　可

内容提要:各国近年来就数据跨境是否以自由流动为原则、数据跨境管制是否具有正当性等议题存在重大分歧。我国《数据安全法(草案)》首次提出“数据安全自由流动原则”,将“数据自由流动”作为基础性原则,将“数据安全流动”作为限制性原则,以平衡对外开放和国家安全的双重目标,为全球数据治理提供了审慎包容、鼓励合作的中国方案。不过,数据自由流动与数据安全流动的冲突并不会自然消解,其有赖于不同数据跨境类型下的原则权衡。在数据出境的场景中,数据“静”的安全(数据完整性、可用性、保密性)是自由流动的前提,数据“动”的安全(重要数据可控和非重要数据可信)则构成自由流动的硬约束和软约束。在数据调取的场景中,我国可基于“重要数据可控”事由调取境外重要数据,同时亦应根据互惠原则,为他国调取我国数据提供制度化渠道。

关键词:数据跨境　数据安全　数据本地化　数据调取

许可,对外经济贸易大学法学院副教授。

这是一个数据全球化的时代。从个人隐私到数据利用,从国际贸易到国家监控,从数字经济到网络主权,在瞬息万变的全球网络治理中,还没有哪类议题能像数据跨境流动一样,激发出如此之多的价值分歧和制度冲突。〔1〕旧规则不敷适用,新秩序远未成型。就此而言,作为数据基本法之一的《数据安全法(草案)》恰逢其时。面对数据跨境流动的“风暴之眼”,《数据安全法(草案)》第10条旗帜鲜明地申明了“数据安全自由跨境流动”的基本原则,这是对《网络安全法》第12条“网络信息依法有序自由流动”的重大改变。那么,如何理解这一原则?它将如何构造我国未来的数据跨境流动制度?又将如何影响世界数据治理规则?本文试图在全球视野和中国实践的双重背景下,回答这些问题。为此,本文第一部分将勾勒数据跨境流动的基本架构和主要类型,通过对国际规则的梳理展现既有争议;第二部分将深入剖析作为基础原则的“数据自由流动”和作为限制原则的

〔1〕由于本文涉及跨国比较,考虑到各国语词的差异,本文对“信息”和“数据”不加区分,且限于电子化的“信息”和“数据”。

“数据安全流动”;最后将采用原则权衡方法,根据数据跨境流动的不同类型,尝试提出我国数据跨境流动的制度构想。

一 数据跨境流动:基本架构与全球实践

自1980年经济合作与发展组织《隐私保护和个人数据跨境流动指南》(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)将“数据跨境流动”纳入法律议题以来,随着跨境流动数据质与量的飙升,数据跨境流动的管与控亦急剧增多,截至2017年,在全球64个主要经济体中,对数据跨境流动加以限制的国家已近90%。[2] 为了把握数据跨境流动管制的全景,不妨先从讨论数据跨境流动的基本架构开始。

(一)数据跨境流动的基本架构

“数据跨境流动”意指“在一国内生成电子化的信息记录被他国境内的私主体或公权力机关读取、存储、使用或加工(合称‘处理’)”。[3] 就流动方向而言,其可分为“跨境流出”和“跨境流入”;就处理主体而言,其可分为“私主体跨境处理”和“公权力机关跨境处理”,由此形成如下架构:

表1 数据跨境流动架构

	私主体	公权力机关
跨境流入	数据入境	数据调取
跨境流出	数据出境	

在“数据入境”的场景中,国家管制体现为对一国之内个人、企业或其他私人组织对境外数据处理的限制上。回顾历史,如果我们将数据转换为信息内容的话,那么这种“入境管制”源远流长。事实上,从印刷品的海关检查到国际无线电通讯的干扰措施,从卫星技术的禁令到互联网的“防火墙”,从美国、加拿大到印度、韩国、马来西亚,[4] 基于国家“信息主权”的信息进入控制屡见不鲜。[5] 1972年,联合国教科文组织《为信息自由流通,扩大教育范围和发展文化交流而使用卫星无线电广播的指导原则宣言》(*Declaration of Guiding Principles on the Use of Satellite Broadcasting for the Free Flow of Information, the Spread of Education and Greater Cultural Exchange*)第6条确认了国家对流入信息内容的自主决定权。国际电联《组织法》第180、181段亦重申:各成员国有权对危害国家安全、违反法律、妨碍公共秩序或有伤风化的电报、电信停止传递或予以截断。一国对“数据入境”的管控,基本出于国家安全、文化安全以及民族认同、意识形态等原因。[6] 而在文化

---

〔2〕 See Martina F. Ferracane, Restrictions on Cross-Border Data Flows: A Taxonomy, *ECIPE Working Paper*, No.1, 2017, p.2.

〔3〕 UNCTC, Transnational Corporations and Transborder Data flows, 1984. 特别说明的是,这里的“数据”不包括“过境数据”,即仅在一国境内传输、存储,但不在此生成的数据。

〔4〕 参见[美]门罗·E.普莱斯著:《媒介与主权:全球信息革命及其对国家权力的挑战》,麻争旗译,中国传媒大学出版社2008年版,第6-13页。

〔5〕 参见刘连泰:《信息技术与主权概念》,《中外法学》2015年第2期,第505-522页。

〔6〕 See Gong Wenxiang, Information Sovereignty Reviewed, Vol.14 (1), *Intercultural Communication Studies*, 119-135 (2005).

多元的世界中,该管控不可避免地与他国发生冲突,2000 年雅虎纳粹物品拍卖案便显示出数字时代控制数据跨境流入的法律之争。[7]

在“数据出境”的场景中,国家管控体现为对一国境内的数据被他国个人、企业或其他私人组织处理的限制,人们往往将该等“出境数据管控”称为“数据本地化”(data localization),但这种说法可能忽略了两者微妙而重大的差异。“数据本地化”的关键在于本地化存储或处理数据或其副本,而不在于禁止数据被他国处理。[8] 类似地,实施“数据出境管控”也不意味着数据一定做本地化存储。有鉴于此,本文将“出境数据管控”和“数据本地化”视为不同的制度设计。[9]

数据出境下的管控类型纷繁芜杂。其中,欧盟《一般数据保护条例》(GDPR)是针对个人数据出境最普遍、最严格的管控制度之一。为避免欧盟个人数据保护水平的减损,《一般数据保护条例》第 44 条至第 50 条禁止将境内个人数据传输至保护充分性不足、无适当安全维护措施、亦不符合特定例外情况的第三国。欧盟的强硬立场体现在 Schrems II 案件中。在该案中,欧洲法院指出,美国《外国情报监控法案》(*Foreign Intelligence Surveillance Act*)的存在,使之可能超过必要限度访问所传输的数据,且无法给欧盟居民提供必要救济,因此宣告美欧《隐私盾协议》无效。[10] 就非个人数据而言,美国根据《出口管理条例》(*Export Administration Regulations*)、《国际武器贸易条例》(*International Traffic In Arms Regulations*),限制出口管制物品、商品、技术、软件或其他类型的非密受控信息(CUI)的出境,未经政府批准,不得向外国公民或实体披露。尽管尚无任何一个国家全面禁止数据出境,但各国或基于特定行业而施加限制,如健康、财务、税收、博彩、金融、地图和政务数据,或基于特定流程或服务而施加规制,如在线的出版、赌博、金融交易等。[11]

在“数据调取”的场景中,国家管控呈现出一体两面的面貌,既表现为本国机关强制调取存储于外国的非公开数据(数据入境),也表现为外国机关强制调取存储于本国的非公开数据(数据出境)。[12] 美国 2018 年《澄清境外合法使用数据法》(下称“云法案”)是这一场景的典型立法。云法案源起于 2016 年美国政府诉微软案。在该案中,美国联邦法院第二巡回法院认为,由于用户通讯内容的数据储存地在爱尔兰,微软必须自爱尔兰数据中心取出数据并“进口”至美国境内,但美国《储存通讯法》(*Stored Communication Act*)并未允许法院以搜查令的方式要求微软提交存于境外服务器上的数据。为了改变法律束缚,云法案旗帜鲜明地采取了数据控制者标准,将数据主权从物理层边界延伸到技术上的

〔7〕 See Stephen J. Kobrin, Territoriality and the Governance of Cyberspace, Vol. 32(4), *Journal of International Business Studies*, 691 – 692 (2001).

〔8〕 参见世界银行著:《2016 年世界发展报告:数字红利》,胡光宇等译,清华大学出版社 2017 年版,第 310 页。

〔9〕 这一区分被《区域全面经济伙伴关系协定》(RCEP)所认可,在其第四节“促进跨境电子商务”中,第 14 条和 15 条分别规定了数据本地化和数据跨境流动两种情形。

〔10〕 See Data Protection Commissioner v. Facebook Ireland, Maximillian Scherms.

〔11〕 对不同国家的详细分析,参见 Nigel Cory, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?, https://itif.org/publications/2017/05/01/cross – border – data – flows – where – are – barriers – and – what – do – they – cost,最近访问时间[2021 – 01 – 01]。

〔12〕 如果是公开的数据,则无须诉诸强制力,并不构成这里的“数据调取”,参见《网络犯罪公约》(Cyber-crime Convention)第 32 条第(1)款。

“控制边界”,即授权美国法院向受管辖的科技公司发出法律命令,以取得该公司所拥有、保管或控制的数据,而不论数据存储于何处。[13] 放宽视野看,云法案是对刑事司法领域双边互助条约和协定不足的回应和调整。随着世界的数字化转型,刑事调查中的电子证据数量激增。在美国,2017 年国际事务办公室处理的来自外国的司法协助请求数增加了 85%,索取数据记录的请求数增加了 10 倍以上。[14] 显然,复杂冗长的司法协助机制已不敷适用,国家单方发起的数据调取由此成为可能的解决方案。

美国对境外数据的调取并不限于云法案,正如“棱镜计划”所揭示的,美国网络全球监控是长期和系统性的。[15] 9·11 事件之后,美国通过《爱国者法案》(*USA Patriot Act*)、《精确法案》(*Accuracy for Adoptees Act*)和《外国情报监控法案》,共同织就了一张巨大的网络情报监视网络。其中,《爱国者法案》第 215 条规定,为外国情报搜集和国际恐怖主义调查获取商业记录,可请求外国情报监视法庭传票,要求从运营商获取服务器日志,并对“善意披露”给予豁免。[16] 《外国情报监控法案》修订案第 702 条进一步指出,司法部长和国家情报总监可以授权情报机构对非美国居民的通信或会话进行监控,时间最长可达一年。

(二)全球数据跨境流动管控的重大分歧

尽管世界各国纷纷针对数据跨境流动采取法律措施,但就数据跨境是否以自由流动为原则、数据跨境管制的正当化事由何在等根本性问题却远未达成共识。

1. 关于数据自由流动原则的争议

所谓“数据自由流动”,意指数据控制者不受限制地将数据由一国流动到他国的状态、能力和权利。数据自由流动的要求因场景而变化。在数据入境和数据出境中,其体现为积极性的“主张”,以排除国家可能的干涉;在数据调取中,其体现为消极性的“豁免”,国家无权强制数据流动。[17] 还需要说明的是,“有原则恒有例外”,以数据自由流动为原则,并不意味着不存在“例外”的限制,事实上,世界上不存在对数据跨境流动不做任何限制的国家。因此,问题不在于是否“限制”,而是“限制”的范围与程度。

在“数据入境”和“数据出境”的场景下,美国是数据自由流动原则的坚定倡导者,并一直通过双边和多边的条约实践该原则。2004 年,美国在亚太经合组织(APEC)通过的《隐私框架》中就要求“成员国采取一切合理步骤避免任何不必要的数据流动障碍”。随着电子商务市场进一步扩张与发展,美国在其主导的《跨太平洋伙伴关系协定》(*Trans-Pacific Partnership Agreement*, *TPP*)中进一步提出“商业信息跨境自由传输条款”,即在保护个人信息等合法公共政策目标得到保障的前提下,确保全球信息和数据自由流动,以驱动互联网和数字经济。自由流动原则鲜明体现在美国《网络空间国际战略:互连世界的

〔13〕 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,第 40 – 42 页。

〔14〕 See U. S. Department of Justice Criminal Division, Performance Budget FY 2017 Presidents Budget.

〔15〕 参见[美]格伦·格林沃尔德著:《无处可藏:斯诺登、美国国安局与全球监控》,米拉等译,中信出版社 2014 年版,第 86 – 100 页。

〔16〕 See U. S. Public Law 107 – 56, Uniting and Strengthening America by Providing Appropriate Tools Required Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001).

〔17〕 关于“主张”和“豁免”的概念,参见王涌著:《私权的分析与建构:民法的分析法学基础》,北京大学出版社 2020 年版,第 76 页。

繁荣、安全与开放》的下述表述之中:“国家没有,也不必在信息的自由流通和其网络的安全性之间做出选择……网络空间……不是国家任意破坏信息自由流动以创造不公平优势的场所。”不过,在数据调取的场景下,美国一改初衷,不但通过长臂管辖权强化国家对境外数据的管制力,而且利用技术优势和网络霸权实现跨地域的全球监控。

如果我们将美国视为数据自由流动一极的话,那么在另一极就是印度。早在 1993 年,印度《公共记录法》第 4 条即规定,未经中央政府事先批准,任何人不得将任何公共记录带离印度。随着数字经济全球竞争的白热化,印度以“数据民族主义”为抓手,强调数据本地化政策的必要性,宣称印度需要同科技公司与敌对国家滥用数据“作斗争”。[18] 2019 年《国家电子商务政策》草案充分阐明了这一立场:“印度及其公民对其数据享有主权,这种权利不应扩展到非印度人(类似地,非印度人对印度煤矿也不享有任何原初权利或诉求)。”2020 年,印度的管控进一步升级,其电子和信息技术部以《信息技术法案》第 69A 条“禁止访问规则”为依据,以秘密传输用户数据至印度以外服务器为由,封禁 59 款中国背景的手机应用程序。但在另一方面,印度在“数据调取”的场景依然坚持《布达佩斯公约》的适用性,并不寻求通过境外的数据管辖权。

无疑,从数据自由流动到数据限制流动是一个渐变的光谱,在美国和印度之间存在无穷的可能性。总体而言,在数据入境和数据出境的场景中,非洲集团、俄罗斯、土耳其、印度尼西亚、越南、尼日利亚等偏向于“国家数据管控”,欧盟、加拿大、日本、韩国、新加坡、智利、哥伦比亚、科特迪瓦、墨西哥、巴拉圭等偏向于“数据自由流动”,[19] 在“数据调取”的场景中,澳大利亚、加拿大、新西兰、英国和欧盟等国偏向于“国家数据管控”,相反,其他国家多偏向于“数据自由流动”。

2. 关于数据管控正当性事由的争议

如果说数据自由流动和国家数据管控是抽象原则之争,那么数据管控的正当性事由就是具体规则之争。鉴于各国政策目标的多元性,本文试图从个人权利、国家安全、公共秩序、经济发展四个维度,作出类型化梳理。

其一,保护个人权利是数据管控中被普遍认可的事由。经合组织《关于保护隐私和个人数据跨境流动指南》明文规定,各成员国应取消限制个人数据流动的规定,但所转移的国家并无隐私权保护规定的不在此限。随着时代变迁,欧盟以《欧洲人权公约》为基,逐渐将“个人数据受保护权”上升为基本人权,成为制约数据流动的核心理由。2013 年,亚太经济合作组织《跨境隐私规则体系》同样将“个人信息的隐私与安全建立有意义的保护”作为数据跨境流通的前提。

其二,国家安全是数据管控的主要事由。不论是《服务贸易总协议》(GATS)和《技术性贸易壁垒协定》(TBT),还是《全面与进步跨太平洋伙伴关系协定》(CPTPP),均秉承“国家安全例外”(National Security Exceptions)原则,各国不得接受或要求他国提供违反其国家重要安全利益之信息。[20] 在数据出境的场景下,美国以金融安全、国防、核不扩散

〔18〕 参见毛维准、刘一燊:《数据民族主义:驱动逻辑与政策影响》,《国际展望》2020 年第 3 期,第 25 页。

〔19〕 See Nivedita Sen, Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path Vol. 21 (2), *Journal of International Economic Law*, 323 – 348 (2018).

〔20〕 参见张丽娟、郭若楠:《国际贸易规则中的“国家安全例外”条款探析》,《国际论坛》2020 年第 3 期,第 66 – 79 页。

目标等国家安全为由限制数据出境。在法国,“主权云”用于储存和处理公共部门的数据,此外,未经法院同意,诉讼相关数据不得传输境外。在“数据调取”的场景下,美欧“安全港协议”中明确将国家安全(如反恐、网络战和网络间谍等)作为例外。相应地,棱镜门计划曝光后,限制数据出境防范外国监控,转而成为俄罗斯、印度和印度尼西亚的重要关切。

其三,公共秩序是数据管控的重要事由。《跨太平洋伙伴关系协定》等一系列重要国际贸易协定均将“正当的公共政策目标”作为数据自由流动的例外。类似地,欧盟《非个人数据在欧盟境内自由流动框架条例》也将“公共安全原因”作为数据流动限制或禁止依据。但何为“公共政策”或“公共安全”?就“公共政策”而言,不妨借鉴 GATS 一般例外条款,将其进一步区分为“公共道德”和“公共秩序”,[21] 前者系一国支持的正确的行为标准,后者系对特定社会基本利益的维护。据此,“数据出境”的场景下,国家可以仇恨言论、极端主义、色情淫秽、民族歧视、反人道等事由,限制数据流动。就“公共安全”而言,根据《欧盟运作条约》第 52 条,其包含了刑事犯罪的侦查、起诉活动,以及维护国家机关、公共服务、人口生存等基本社会利益和外交关系、军事利益等国家利益。据此,刑事司法的跨境数据调取得以正当化。

其四,经济发展是数据管控的又一考量。“数据就是石油”的口号激发了各国争夺数据的热情,数据日益被视为展现政治、军事和商业影响力的杠杆。在此背景下,一种通过数据流动管控推动本国数字产业繁荣的“数据重商主义”开始出现。以印度为例,促进创新和经济增长是数据管控的首要目标。《保护隐私、赋能印度的自由公平数字经济》的官方报告指出,限制数据跨境流动有助于增加对数字基础设施的外国直接投资,利用数据中心本地市场的溢出效用,创造就业机会及专业人员,建立印度的人工智能生态系统。[22] 同样,在全球电子商务谈判中,南非 WTO 代表认为,跨境数据流动自由化是妨碍本地企业发展的“反发展”(Anti-Development)规则,进而主张拥有较为灵活的数据本地化措施,在采取数据保护措施上具有“一定自主权”,以抵御发达国家对本国数字产业的侵蚀。[23]

二 数据自由流动原则与数据安全流动原则

面对各国对数据跨境流动法律原则和管控事由的种种分歧,《数据安全法(草案)》首次提出“数据安全自由流动”原则,这既彰显出在逆全球化和民粹主义兴起的潮流下我国坚持对外开放与国际合作的基本立场(“自由流动”),又彰显出对国家安全的高度关切(“数据安全”)。然而,如何理解这一数据跨境流动的中国方案?本文试图将之拆解为数据自由流动原则和数据安全流动原则,以期剖析机理和辨明意蕴。

---

〔21〕《罗马条约》混用“公共政策”和“公共秩序”,可见两者的一致性,而公共道德和公共秩序有着内在重叠,参见翁乃方著:《WTO 下公共道德及公共秩序例外:共通标准之建立》,我台湾地区元照出版有限公司 2015 年版,第 8 - 9 页。

〔22〕See Srikrishna Committee, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, Report of the Committee of Experts under the Chairmanship of Justice BN Srikrishna, 2018, pp. 89 - 91.

〔23〕参见方元欣:《数据本地化政策的全球博弈分析》,《中国信息化》2019 年第 12 期,第 102 页。

(一)“数据自由流动”作为基础原则

1. 数据自由流动的空间结构

数据作为网络“内容层”的组成部分,深深嵌入在“无国界”的网络空间的架构之中。在技术层面上,互联网“端对端”(End-End)架构最大程度地简化了人际复杂互动,“信息瞬时可达”大幅压缩了时空,虚拟空间、流动空间和无界空间相继产生。[24] 在网络空间中,划分区域的标准是 IP 地址和与之对应的域名,而非国家或地区之间的地域疆界,只要法律允许,用户就可以在全球各地登录任何国家的网站,进入全球性的信息交流和社会互动平台。不仅如此,随着云存储、云计算、物联网等信息技术的迭代,网络空间“无国界性”进一步加剧了。作为一种独立于位置的计算机资源无缝分配方案,云计算打破了服务器、数据中心、物理设备之间的划分,以实现动态使用和集中管理物理资源和虚拟资源、提高系统结构的弹性、降低成本和减少风险等目的。[25] 由于虚拟化技术,数据看似是单个计算的逻辑抽象,事实上却是在不同的硬件中以物理分布方式存储,这意味着一个数据集将被逻辑切分为大量碎片,再根据存储设备的空间限制和性能在不同位置存储,因此云存储不但是远程的,而且是不确定的。[26] 在欧洲,这一新的技术已经对欧洲主权和《一般数据保护条例》的实施提出了挑战:如何判断谁是数据控制者?如何认定数据流出欧盟?欧洲的管辖权是否随着云存储全球化而覆盖全球?[27] 这些问题还没有答案。

网络空间“无国界性”亦被法律所认可。在 American Library Ass'n v. Pataki 案中,法院认为:“互联网协议旨在忽略而不是记录地理位置。互联网对地理位置完全不敏感。互联网用户既不了解也不关心他们访问网络资源的物理位置。”[28] 而在网络法奠基性文献中,戴维·约翰逊(David Johnson)和戴维·波斯特(David Post)也指出,网络行为具有突破国界限制的天然属性,因此对跨越物理国界的电子数据流通进行控制时,如果仍以空间作为管制范围的标准之一,那么其努力很可能是徒劳的。[29]

2. 数据自由流动的“事物本质”

“事物本质”一直是法律的正当性基础之一,它要求法律必须与生活事实维持一致,彼此相互适应,立法者应根据事物属性作出调整,而不应“悖离事理”。[30] 据此,数据自由流动原则亦建立对“数据”性质的深刻认识之上。

2017 年,《经济学人》杂志以激动人心的口吻说道:“数据之于本世纪,就像石油之于上世纪:它是发展和改变的动力。”正如 20 世纪围绕石油爆发数次战争一样,《经济学人》预言:“未来,很多战争将围绕谁应该拥有数据和从数据中获利展开。”一语成谶,随着数据价值的飙升,通过贸易或非贸易壁垒,将这一资源尽可能保留在本国控制之下,成为各

---

〔24〕 参见[英]Martin Dodge, Rob Kitchin 著:《网际空间的图像》,江淑琳译,我国台湾地区韦伯文化“国际”出版有限公司 2015 年版,第 30 页。

〔25〕 参见周奇:《云计算技术专利保护初探》,《电子知识产权》2012 年第 12 期,第 22 - 24 页。

〔26〕 参见[英]克里斯托弗·米勒德著:《云计算法律》,陈媛媛译,法律出版社 2019 年版,第 11 - 13 页。

〔27〕 See Škrinjar Vidović, Marina, EU Data Protection Reform: Challenges for Cloud Computing, Vol. 12, *Croatian Yearbook of European Law & Policy*, 171 - 206 (2016).

〔28〕 969 F. Supp. 160, 170 - 171 (S. D. N. Y. 1997).

〔29〕 See David R. Johnson, David Post, Law and Borders—The Rise of Law in Cyberspace, Vol. 1 (1), *Stanford Law Review*, 1367 - 1402 (1996).

〔30〕 参见[德]卡尔·拉伦茨著:《法学方法论》,黄家镇译,商务印书馆 2020 年版,第 523 - 525 页。

国的优先选择。数据国际规则的缺失强化了“数据国家主义”。正如波斯纳所洞察的,在无法可依的社会中,“报复之威胁是维系初民社会公共秩序的基本机制”,[31] 如果一国或地区率先进行数据截留,那么他国不得不竞相效尤。然而,这种数据博弈完全误解了数据的性质,数据绝非真正的石油。

首先,数据并不稀缺。总量有限的石油牢牢把控在少数产油大国的手中。相反,数据无处不在且源源不绝。随着互联网、物联网和智能终端的发展,新的数据每分每秒都在产生。其次,数据是“非竞争的”。石油只能被特定的企业占有和消费,而数据被一家企业收集、使用并不以排斥他人为代价。“多重归属”的网络经济特性,将数据分散到各个网络平台上,以至于没有企业可以独占所有数据。再次,数据是高度差异化的。以一国国民生物数据训练出来的人脸识别算法,对于他国可能用处寥寥。最后,数据价值并不永久。作为典型的时效品,老数据不如新数据值钱,而且随着时间推移,前者越来越没有价值。大数据与其说是“大”的数据,毋宁是实时在线的“活”的数据。[32] 所以,因数据累积而形成的优势会迅速消逝,因为其寿命有限。

总之,将数据视为类似于土地的资产并严格管控的做法,悖离了数据作为“流动性财产”(fugitive property)的性质。[33] 正如对大数据的界定所表明的,只有在人、物、组织之间高速流动的数据,才能进化为指导当下、预测未来、引领发展的“数据智能”。经济学研究早已指出,在变动不居的数字经济中,几乎没有任何证据表明,仅仅拥有数据就能充分排斥更优的产品或服务的供给。要想建立可持续的竞争优势,数字战略的重点应当放在如何使用数字技术以前所未有的方式创造价值上。[34] 就此而言,“数据是石油”还有一层隐含的意义,那就是占有数据远没有开发数据有价值,正如石油大国往往不是经济强国,而这未尝不是“资源诅咒”的另类运用。

3. 数据自由流动的经济基础

首先,数据自由流动是经济全球化的不竭动力。如果说 20 世纪的全球化是货物和资金的全球化,那么 21 世纪就是数据的全球化。大型电商平台通过互联网获取、集合、处理和传输数据,将大公司主宰的国际贸易转变为无数消费者和中小企业聚集的无国界社区。其次,数据自由流动还是数字经济的创新引擎。研究表明,跨境数据在 2005 到 2015 年间使全球 GDP 增长了 10%,2015 年数据流附加值估计为 2.8 万亿美元,已超过了货物贸易的贡献。[35] 最后,数据流动和汇聚所形成的数据智能,不但能提升商业效率,而且有助于协助科学创造、监测自然系统、增进对社会的动态理解并解决重大全球问题。正因如此,国家的数据管控无疑造成了不利影响。欧洲国际政治经济研究中心的报告指出,数据跨境管控导致欧盟 0.48%、印度 0.25%、中国 0.55% 的 GDP 损失。[36] 2019 年,世界银行梳

〔31〕 参见[美]理查德·A. 波斯纳著:《正义/司法的经济学》,苏力译,中国政法大学出版社 2002 年版,第 215 页。

〔32〕 参见王坚著:《在线——数据改变商业本质,技术重塑经济未来》,中信出版社 2016 年版,第 62 - 72 页。

〔33〕 参见许可:《数据权属:经济学与法学的双重视角》,《电子知识产权》2018 年第 11 期,第 28 页。

〔34〕 See Manne, Geoffrey and Sperry, Raymond, The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework, *CPI Antitrust Chronicle*, No. 2, 2015, pp. 8 - 9.

〔35〕 See McKinsey Global Institute, Digital Globalization: The New Era of Global Flows, 2016.

〔36〕 See Matthias Bauer, Martina F. Ferracane, and Erik vander Marel, 2016, Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization, Global Commission on Internet Governance Paper Series, p. 10.

理了东亚 15 国的数字政策,使用定量研究的方法得出“数字限制指数”,直观展现出数据跨境管控与企业创新之间的负相关关系。〔37〕

我国是经济全球化和自由贸易的参与者、受益者和倡导者,从自由贸易区到“一带一路”倡议,中国始终坚定支持开放、包容、共赢的全球化,促进全球贸易和投资自由化和便利化。同时,我国还是数字经济的引领者。联合国《2017 世界投资报告》梳理了网络平台、电子商务、数字内容、IT、电信设施等主要数字经济领域,发现全球的领导者或跟随者基本被中美两国的企业占据。不过,中美两国相对优势地位未能掩盖我国数字经济规模只有美国三分之一的绝对差距。显然,不论是出于深化开放,还是发挥数字经济动能的考虑,数据自由流动都应成为我国基本立场和战略目标。〔38〕

事实上,我国已承认“数据自由流动原则”的基础性地位。在第七届世界互联网大会上,中国官方智库发布的《网络主权:理论与实践(2.0 版)》强调:“倡导与实践网络主权……并不否定网络空间的互联互通性、必要秩序基础上的信息自由流动性和创新性。”〔39〕在制度层面,我国于 2019 年签署《G20 大阪数字经济宣言》,积极回应了其中“基于信任的数据自由流动”(Data Free Flow with Trust)的倡议。2020 年,我国促成并签署的《区域全面经济伙伴关系协定》第 15 条申明:“不得阻止基于商业行为而进行的数据跨境传输。”在近期的地方性立法中,上海、深圳、北京、海南纷纷出台便利数据跨境流动的试行办法,《深圳经济特区数据暂行条例(草案)》甚至提出“数据跨境流通自由港”的政策目标。

(二)“数据安全流动”作为限制性原则

数据自由流动并不是无风险和无成本的。事实上,从个人信息滥用到数据泄露,从关键信息基础设施攻击到金融信息安全,从核心价值观削弱到网络犯罪和恐怖活动,数据流动的国家管控其来有自。职是之故,我国将“数据安全流动”作为限制性原则,以管理数据流动风险。可是,作为一个不确定概念,若“数据安全”失之宽泛,可能戕害了数据自由,而若过于狭窄,又可能引发不可控的风险。因此,对“数据安全”的准确把握成为了“数据安全自由流动”的重中之重。

1. 数据安全:技术与政治

技术安全是数据安全的基线。我国《网络安全法》76 条第 2 项将“数据安全”界定为“保障网络数据的完整性、保密性、可用性的能力”。这里的“保密性”指数据不为其他不应获得者获得;“完整性”指数据不被未授权的篡改或在篡改后能被迅速发现;“可用性”指数据满足一致性、精确性、时效性的要求。这一技术安全概念被各国普遍认可。早在 1994 年美国《重新定义安全》报告中,此三者就已成为信息安全的基本要求,〔40〕美国 2003

〔37〕 See Ferracane, Martina Francesca, Digital Innovation in East Asia: Restrictive Data Policies Matter, *World Bank Group Policy Research Working Paper*, No. 9124, 2020, p. 15.

〔38〕 我国对此已经有深入认识,《网络安全法》施行前夕,国家网信办负责人答记者问时说:“当今数据跨境流动已经成为经济全球化的前提,是推进‘一带一路’建设的必要条件。”http://www.cac.gov.cn/2017-05/31/c_1121062481.htm,最近访问时间[2021-01-01]。

〔39〕 《网络主权:理论与实践(2.0 版)》在第七届世界互联网大会上发布,http://www.cac.gov.cn/2020-11/25/c_1607869924931855.htm,最近访问时间[2021-01-17]。

〔40〕 See Joint Security Commission, Redefining Security-A Report to the Secretary of Defense and the Director of Central Intelligence, Washington DC, February 28, 1994, p. 2.

年《医疗电子交换法》和欧盟2019年《网络安全法》对此亦予以重申。

政治安全是数据安全的顶线。作为《国家安全法》的特别法,《数据安全法(草案)》不但在第6条规定"中央国家安全领导机构"作为数据安全决策、统筹、协调的负责机构,而且其第4条明确了"总体国家安全观"对数据安全的统领作用。综合2014年习近平总书记《在中央国家安全委员会第一次会议上的讲话》中的阐述和《国家安全法》第2条,总体国家安全观应具备如下内涵:

其一,总体国家安全观是包含多样化诉求的"综合安全观"。20世纪下半叶,随着冷战结束,建立在"战争与和平"之上的"传统安全"开始向以"发展与和谐"为导向的"非传统安全"转变,安全也从单一军事和政治安全向社会、环境、经济领域迈进。[41] 日本、欧盟、俄罗斯等相继出台综合安全保障战略、综合安全战略、综合安全构想等战略,融传统安全和非传统安全为一炉的"综合安全观"逐渐成为最主要的国际安全理念。[42] 在我国,数据(信息)安全亦与政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、生态安全、资源安全、核安全并列且相互交错,共同组成综合安全体系。

其二,总体国家安全观是考量发展的"相对安全观"。风险社会的来临使得"绝对安全"已沦为幻想,这不仅因为风险无所不在,而且因为风险具有"反身效应"——它既是社会发展的结果,又是社会发展的原因。既然风险无法根除,安全便只能是符合人们认知和期待的"主观安全"。[43]

其三,总体国家安全观是强调人民福祉的"人类安全观"。1994年,时任联合国秘书长加利在《联合国发展报告》中呼吁,安全的决定性因素,不再是单纯的"国家免于威胁",而是让所有人享有"平安",与传统的国土安全、政权安全相比,人类安全在于确保人民免于恐惧和免于匮乏。[44]

其四,总体国家安全观是兼顾他国的"合作安全观"。作为一种力求通过国家主体和非国家主体的合作来谋求国家安全、地区安全乃至全球安全的主张,"合作安全观"由美国布鲁金斯学会在1988年率先提出。2014年,习近平主席在第四次亚信峰会上发出合作安全、共同安全、综合安全、可持续安全倡议,号召走出一条共建、共享、共赢的亚洲安全之路。

2. 数据安全:法律之具体化

尽管技术安全和政治安全共同塑造了数据安全概念,但在法治原则下,不论是国家安全还是数据安全,均非法律"黑洞"(法律无法规定)或"灰洞"(法律只能做形式上有限的规定),[45]相反,"数据安全"必须在法律层面具体化,才能回应各方的合理期待。为此,我们立足于"数据跨境流动"场景,使用"去价值化"和"价值补充的类型化"的法律技术,[46]尽可能明确其可能意蕴。还应承认,作为一种价值性不确定概念,"数据安全"无法完

〔41〕 参见[英]布赞等主编:《新安全论》,朱宁译,浙江人民出版社2003年版,第11页。

〔42〕 参见李效东、赵景芳、李瑞景著:《现代国际安全理论》,军事科学出版社2015年版,第130-146页。

〔43〕 参见沈逸著:《美国国家网络安全战略》,时事出版社2013年版,第91-93页。

〔44〕 参见[日]松下和夫:《论"人的安全"与"环境合作"》,李佳译,《浙江大学学报(人文社会科学版)》2008年第1期,第31页。

〔45〕 See Shirin Sinnar, Rule of Law Tropes in National Security, Vol. 129 (6), *Harvard Law Review*, 1566-1618 (2016).

〔46〕 参见王贵松:《行政法上不确定法律概念的具体化》,《政治与法律》2016年第1期,第145-150页。

全客观化,也不存在“唯一正解”,因此,其仍有必要保持开放性,以回应复杂多变的现实。

表 2 数据安全的具体化

面向	含义	理据	法律技术	法律依据
“静”的安全	数据的完整性、可用性、保密性	技术安全	去价值化	《数据安全法(草案)》第 3 条第 2 款:有效保护
“动”的安全	重要数据的可控	综合安全、人类安全	类型化	《国家安全法》第 25 条
	非重要数据的可信	相对安全、合作安全	类型化	《数据安全法(草案)》第 3 条第 2 款:合法利用

所谓“静”的安全,即对数据固有形态及其权益的保护,其体现在任何人不得非法访问、获取、使用他人数据,侵害数据的完整性、可用性、保密性,该类型的安全具有客观且清晰的判断标准。所谓“动”的安全,即对数据流动过程及其权益的保护。依数据类型,这一安全可以分为“重要数据”的自主可控以及“非重要数据”的合作可信:前者源于综合安全观和人类安全观,要求国家就“攸关国家总体安全的重要数据”享有实际支配力,避免被其他组织或国家非法操纵、监控、窃取和干扰,有损国家安全和人民福祉;后者源于相对安全观和合作安全观,将数据安全理解为各方彼此塑造的主观期待,在充分考量数据利用的基础上,促进各方切实履行承诺和约定,通过合作达成合理信赖。

3. 通过数据安全的跨境流动管控

与前述以“个人权利、国家安全、公共秩序、经济发展”为由管控数据流动的国际实践不同,《数据安全法(草案)》谨慎地将管控事由锚定在“安全”之上,从而避免宽泛限制阻碍了滚滚向前的数据洪流。必须说明的是,由于我国的“安全”既源自国家安全,又有所差异,因而得以在一定程度上吸纳“个人权利”和“公共秩序”。此外,根据《网络安全法》第 12 条,对“宣扬民族仇恨、民族歧视,传播暴力、淫秽色情信息,编造、传播虚假信息扰乱经济秩序和社会秩序的信息”等“危害公共秩序”行为的数据管控主要由《网络安全法》完成,并且,该等管控限于境内公民、法人和其他组织对境外数据的访问(数据入境),无关数据出境和数据调取。

三 数据安全、自由跨境流动的制度构造

如何调和自由流动原则和安全流动原则是数据安全自由跨境流动制度的关键。与美国将“自由流动”为原则、“国家管控”为例外的“原则—例外模式”迥然不同,[47] 我国采取的是自由和安全并列的“双原则模式”,如何有效平衡两者成为实践难题。由于法律原则的抽象性和价值多元性,其并非以“全有或全无的方式”予以适用,而是根据其“分量”,以权衡的方式化解原则间冲突。[48] 鉴于权衡必须在类型化场景中开展,为此,我们将“双原

〔47〕 参见石静霞:《数字经济背景下的 WTO 电子商务诸边谈判:最新发展及焦点问题》,《东方法学》2020 年第 2 期。

〔48〕 参见陈林林:《基于法律原则的裁判》,《法学研究》2016 年第 3 期,第 10 – 11 页。

则”置于数据出境和数据调取的背景下,尝试着建构制度上的平衡之道。

(一)安全、自由的数据出境制度

1. 数据“静”的安全:“自由流动”之前提

数据完整性、可用性、保密性的保障是数据出境的前提。数据“静”的安全在数据跨境流动中的优先地位被世界经济论坛报告所申明。[49] 我国《数据出境安全评估指南(草案)》亦将数据发送方和数据接收方的安全保护能力、采取措施作为评估的重点。数据“静”的安全之落实有赖于企业和政府的协力。就企业而言,其不但需要具有保障数据安全的信息系统、数据安全工作的自动化工具以及对数据安全风险的预防、检测及响应能力,其还应在组织、人员、制度三方面强化管理保障。合理和适当的数据安全保护水平至少应包含:(1)设立流程、程序和系统评估数据安全风险;(2)为员工提供数据安全培训;(3)限制和监控员工对数据的处理。[50] 就政府而言,各国将积极创建和支持稳固的数据安全基础设施,将数据“静”的安全作为开展数字贸易的基本条件,搭建数据安全信息共享和数据泄露通知机制。同时,恰如我国外交部《全球数据安全方案》所倡议的,各国应坚决禁止信息技术产品和服务供应企业设置后门非法控制或操纵用户系统和设备、获取用户数据,并应严厉追究任何组织和个人非法窃取数据的法律责任。

2. 数据“动”的安全:“自由流动”之权衡

与客观化的“静”的安全不同,数据“动”的安全和数据自由流动之间关涉到主观价值,其取舍可立基于德国法学家阿列克西的“权衡法则”之上:“对一个原则的未满足程度或损害程度越大,满足另外一个原则的重要性就必须越大。”[51] 根据该法则,安全流动原则和自由流动原则的权衡可分为三个步骤:一是确定自由流动原则未满足程度;二是确定安全流动原则的重要性;三是确定安全流动原则的重要性能否证立自由流动原则的未满足程度。事实上,通过权衡确定数据安全和数据自由何者原则优先的思路已体现在大量国际公约中。联合国《关于国家安全和信息权利的全球性原则》(Global Principles on National Security and the Right to Information)第3条针对“以国家安全为由限制信息访问”的情形,明确规定:“对限制必须遵守比例原则,必须是为防止危害可采用的限制最少的手段。”类似地,基于《关税及贸易总协定》第21条“安全例外”条款,可将数据安全视为一国“重要安全利益”,从而免于对外提供信息,但即使如此,这一条款亦受到“必要性”的限制。[52] 考虑到数据类型和价值纷繁芜杂,这里遵循数据分级分类原则,分别讨论“重要数据”和“非重要数据”的权衡结果。

3. 重要数据可控:“自由流动”之硬约束

作为高度敏感性的数据,重要数据一直是我国出境管控的重点。《网络安全法》第37条确立了关键信息基础设施运营者的重要数据境内存储和出境评估制度。《数据安全管理办法(征求意见稿)》第28条规定:“网络运营者向境外提供重要数据前,应当评估可能

---

〔49〕 See World Economic Forum, A Roadmap for Cross Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, 2020.

〔50〕 See LabMD, Inc. v. Federal Trade Commission, (11th Cir. Sept. 29, 2016).

〔51〕 See Robert Alexy, On Balancing and Subsumption, Vol. 16 (4), *Ratio Juris*, 433, 436 (2003).

〔52〕 参见孙南翔著:《互联网规制的国家贸易法律问题研究》,法律出版社2017年版,第225-226页。

带来的安全风险,并报经行业主管监管部门同意;行业主管监管部门不明确的,应经省级网信部门批准。”

重要数据管控的确定性与重要数据外延的模糊性形成了鲜明对比。《数据出境安全评估指南(草案)》“附录 A 重要数据识别”将可能危害国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施安全的数据均囊括其中。《数据安全管理办法(征求意见稿)》将其缩限到“直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据”,但“社会稳定、公共安全”等表述依然过于宽泛。为此,本文将其限定为“一旦遭到篡改、破坏、泄露或者非法利用就严重危及国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益的数据”。这首先因为,这一源自《国家安全法》第 2 条的概念,与通过重要数据维护国家安全的立法目的若合符节。可资佐证的是,《数据安全法(草案)》第 23 条与我国《出口管制法(草案)》相衔接,确定了对两用物项、军品、核及其他与履行防扩散等国际义务和维护国家安全有关相关数据的出口管制。此外,在综合安全观之下,基于“国家安全”的重要数据一方面可以筛除普通的社会、经济和公共安全的诉求,另一方面也能将社会根本利益转为国家安全问题,避免失之过窄。[53]

以上述观之,《数据安全法(草案)》第 19 条“重要数据条款”有待完善。其一,该条将重要数据的考量要素分为“重要程度”和“危害程度”,看似全面,实则未能理解在安全/风险进路下,只有不利影响的严重性、持续性才是关键。其二,该条将“各地区、各部门”均列为重要数据认定主体,不仅可能不当扩大或缩小重要数据范围,还可能导致数据跨地区流动和处理,引发法律规避。为此,不妨汲取实施《保守国家秘密法》和《保守国家秘密法实施办法》的经验教训,限制重要数据认定权授予,设置严格认定程序,强化认定结果监督。为此,建议由中央国家机关划定重要数据的类型,各地区在上述划定范围内有权确定本地区重要数据目录,在不同地区出现冲突的情况下,可上报国家网信部门决定。

重要数据的认定只是第一步,重要数据如何出境依然悬而未决。鉴于重要数据攸关国家安全,且相关损害有着经验上的高度盖然性,重要数据的安全流动原则应优先于自由流动原则。换言之,只有在满足安全要求之后,重要数据才能出境。然则,何为“重要数据安全”?根据《国家安全法》第 25 条,重要数据安全与“重要数据可控”同义,即数据提供者对于出境后重要数据也应享有法律上支配权和事实上支配力,境外的数据处理设备和系统应具有充分的安全性、开放性、透明性、来源的多样性,难以被非法控制、遭受干扰或破坏。

4. 非重要数据可信:“自由流动”之软约束

较诸重要数据,企业数据、个人数据等非重要数据一方面相对芜杂,可能引致的损害也相对较小,另一方面,其自由流动的规模极大、价值极高。故此,在安全流动和自由流动的权衡中,应采取促进数据自由流动的立场。但是,这绝不意味着放任数据风险,恰恰相反,其要求将“动”的安全嵌入其中,赋予数据流动协议以强制执行力,向各利益攸关方科以全面、诚信履行承诺的义务,最终达成“可信的数据自由流动”。

这里的“可信”首先是个体与企业之间的“信赖”。面对用户对数据自由流动信心匮

〔53〕 公共秩序和国家安全的勾连,参见 ICSID, LG&E Energy Corp. v. Argentine Republic, ICSID Case No. APB/02/1, Decision on Liability, Oct. 3, 2006, paras. 226 – 161。

乏的现实,欧盟试图通过个人数据权利的赋予重塑信任。但遗憾的是,欧盟正确诊断了病灶,却开错了药方。须知,信任始终是共同的事业。《一般数据保护条例》试图通过"用户赋权—企业担责"的单向路径实现信任,忽略了在激烈市场竞争下用户和企业共赢的可能性。为此,不妨引入"信义规则"(fiduciary rule),同时承认用户和企业的利益,但企业必须将其利益的实现建立在用户利益实现的基础之上。作为受托人,企业对个人数据拥有开放性权力,由此从"动辄得咎"的境地中解脱出来,得以在不侵害用户利益的前提下,最大化数据价值。当然,这绝不意味着企业可以恣意妄为,国家可通过事后责任追究而非事前禁止的机制,监督其勤勉忠实地对待用户。同时,在数据出境后,数据原始控制者的信义义务持续有效,不论相关数据是否已经传输到境外,也不论境外的数据处理是其关联公司、代理人还是合作伙伴所为。[54] 以此观之,我国《个人信息保护法(草案)》第38、39条将个人单独同意作为个人信息出境的前提,未免重蹈了欧盟个人自主权利的覆辙,建议修改为"以企业满足客观保护要件为原则,以个人单独同意为例外"。

其次,"可信"是企业与企业之间的"信赖"。数据提供者和数据接受者可以采取如下方式化解猜忌的成本:(1)经由可信第三方达成交易,特别是当相关方已经取得行业协会或政府机构颁发的资格认证时;(2)遵循共同的行为标准,特别是当该标准系国际权威协会制定并经国家批准时;(3)使用国家发布的标准合同条款,以保障数据真实性、合规性,应约定数据提供者说明数据来源、承担数据瑕疵担保责任,数据接收者则承担数据完整性和保密性的义务;(4)改进技术手段,提升技术互操作性,令双方在不同系统之间能够共享和使用数据,同时,尝试区块链技术特有的不可篡改特性,以提升数据安全保障、增强数据供应链透明度。

最后,"可信"还是国家与国家之间的"信赖"。在国内层面,各国在制定数据法规时,应当充分开放和透明,为外国投资者、行业协会、国际组织提供广泛参与机会,相关规则应基于实证依据,并考虑技术和经济上的可行性,必要时,可以发布立法和执法评估,以确保监管措施的适当性和有效性。在国际层面,各国应遵循"数据保护随数据而行"的原则,避免他国的跨境数据遭致权利减损,亦不得歧视性对待他国数据。为此,各国数据监管机构可以建立定期合作机制以增强信任,推动"互不监控"(no spy)协议,最大程度限制政府对跨界传输数据的监控。可信自由的数据跨境流动是全球共同福祉,放眼未来,各国完全可以在WTO以及其他以联合国为基础的框架下共同磋商,形成兼顾本国诉求和他国主张的全球数据治理规则。

(二)安全、自由的数据调取制度

国家对境外数据的调取构成对数据自由流动的干涉,其正当性同样应由"数据安全原则"证成。一方面,数据"静"的安全依然是数据调取的前提,任何国家不得滥用信息技术对他国进行数据监控,非法采集他国公民个人数据,破坏数据的完整性、可用性、保密性。另一方面,只有调取行为以数据"动"的安全为鹄的,且调取数据的收益足以弥补对自由流动价值的戕害之时,才有适用之余地。在"数据安全"的体系下,国家数据调取的

〔54〕 See Nigel Cory, Robert D. Atkinson, Daniel Castro, Principles and Policies for "Data Free Flow With Trust", https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust,[最近访问时间2021-01-01]。

实质是获得数据控制权,因此,基于“重要数据可控”的理由,国家可以调取关系国家安全的境外数据,同时,亦应允许他国在同等范围获取本国数据,以履行国际法上的对等义务。

1. 我国对境外数据的调取

一直以来,我国对境外数据调取的态度始终坚持自由流动原则,避免使用单边权力。不过,随着我国企业全球化布局的展开,我国数据领域立法也面临着“攻守易型”,适当扩展域外管辖权已经是当务之急。[55] 事实上,在犯罪国际化、虚拟化的背景下,我国单边主义的电子证据跨境收集已成常态。[56] 2016 年《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》明确了侦查机关对境外数据直接收集的权力。《数据安全法(草案)》第 2 条延续并革新了《网络安全法》第 75 条的域外保护性管辖权,在拓展保护权益的同时降低了触发门槛。为实现该等管辖权,与《一般数据保护条例》第 58 条类似,我国执法机关应享有获取境外电子证据的权力。另一方面,数据主权并不只有防御性权力。相反,作为更综合、更灵活的权力,数据主权包括了四种不同的面向:国家对境内数据的管控力(数据国内主权);国家参与数据国际条约缔结和参加数据国际组织的独立国家地位(数据法理主权);排斥他国干涉本国数据事务(数据威斯特利亚主权);国家对跨境数据的控制力(数据互赖主权)。[57] 根据国家利益,数据主权可以在不同面向上组合。在数据调取的场合,当他国威胁我国的国家安全时,我国可以通过强化数据互赖主权,令主权越过有形疆域。当然,为避免管辖权的过分扩张,境外的数据调取应以“重要数据”也即攸关国家安全的数据为限,这不但契合我国《网络空间国际合作战略》下“维护主权与安全”的首要战略目标,而且与“保护性管辖”的国际法准则相符。

2. 他国对境内数据的调取

基于防御性数据主权,我国一直限制或禁止他国数据调取。《数据安全法(草案)》第 33 条与《国际刑事司法协助法》第 4 条,被视为应对外国长臂管辖的“封阻法令”(blocking statutes)。与《数据安全倡议》将他国跨境调取数据必须依据“司法协助渠道或其他相关多双边协议”相比,上述规定预留了“主管机关批准”的窗口,值得赞同。但是,从提升规则执行性、降低企业合规成本的角度,尚有种种问题有待澄清。例如,上述条款中的“执法机构”是否包括司法机构?究竟有哪些“主管机关”?“存储”是否应改为“生成”,从而将经由中华人民共和国中转,未经任何变动或加工处理的境外数据排除在外?在未来,除了一事一议的审查制度外,还可以考虑根据互惠原则设立数据调取的白名单,并尝试与美国、欧盟等具有同样需求的国家和地区达成协定,同时依托“一带一路”倡议等合作平台,与沿线国家签署关于跨境数据取证的协定。[58]

四 结 语

《数据安全法(草案)》发布至今,从欧美之间“隐私盾”协议被欧洲法院(CJEU)判定

〔55〕 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,第 85 页。

〔56〕 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 201 页。

〔57〕 关于主权的不同维度,参见 Stephen D. Krasnera, Abiding Sovereignty, Vol. 22(3), *International Political Science Review*, 229 – 251 (2001)。

〔58〕 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,第 170 页。

无效,到 TikTok 以数据安全为由被强令出售,再到美国“清洁网络”计划,国际数据形势波诡云谲。正如世界互联网协会(ISOC)所警告的,美国的种种行为破坏了互联网的基础,威胁了互联网的开放性和可访问性原则。面对“政策走向保守、战略转向收缩”的“美国优先主义”和“分裂互联网”(Splinternet)的乱局,中国作为网络空间命运共同体的倡导者和数字经济大国,理应对自身的力量和责任充满自信,为全球数据立法提供审慎包容、促进交流、鼓励合作的中国方案。[59]

《数据安全法(草案)》所确立的“数据安全自由流动原则”正是中国智慧的重要贡献。在各国“数据自由”和“数据管控”的争议中,中国坚定选择了“数据自由”,涤除了中国是数据本地化最严苛国家的误解;在各国林林总总“管控事由”中,中国删繁就简选择了“安全”,锚定了数据主权的底线。无疑,这是一个给人以秩序感并具有价值感召力的数据跨境方案。可另一方面,亦应看到,“数据安全自由流动原则”尚待具体化,与既有制度的冲突也有待弥合,我们衷心期待这一原则在国内规则和国际规则中的早日践行,最终建立安全、自由的全球数据治理新秩序。

[本文为作者主持的2020年度中国信息安全测评中心“各国针对个人信息与个人跨境数据管控措施研究项目”(2019D11)的研究成果。]

[**Abstract**] Currently, countries around the world have sharp differences on issues such as “should free flow be a principle of cross-border data flow” and “what is the justification for regulating cross-border data flow”. China’s (Draft) Data Security Law puts forward for the first time the principle of safe and free flow of data, which takes the free flow of data as the basic principle and the safe flow of data as a restrictive principle, to balance the dual goals of opening up to the outside world and protecting national security and provide a prudent, inclusive, and cooperation-encouraging plan for global data governance. However, the conflict between free flow of data and safe flow of data will not disappear spontaneously by itself, because the solution of this conflict relies on the trade-off of different principles under different types of cross-border data flow. In the case of data flowing out of the country, the static security (integrity, availability and confidentiality of data) is the prerequisite for free flow of data, whereas the dynamic security (controllability of important data and credibility of non-important data) constitutes the hard and soft constraints on the free flow of data. In the case of data retrieval, China can retrieve important data from abroad on ground of controllability of important data. Meanwhile, based on the principle of reciprocity, China should also provide an institutionalized channel for other states to retrieve data from its territo ry.

(责任编辑:田 夫)

〔59〕 参见支振锋:《贡献数据安全立法的中国方案》,《信息安全与通信保密》2020年第8期,第7页。