doi:10.3969/j.issn.1003-5559.2022.02.004

美国数据跨境流动监管的实践经验及启示

■ 余 萍 广州工程技术职业学院

摘 要:数字经济时代下,数据跨境流动在助推国际贸易发展的同时,也为国家安全、商业机密、民众隐私保护带来极大威胁。如何在数据跨境流动的安全性和成长性中找到平衡点,是中国政府管理部门及隐私保护机构必须思考的问题。美国在数据跨境流动监管方面先后经历"初步规制"、"安全港"、"隐私护盾"三个阶段,已经形成较为完备的监管体系。由此,中国应积极借鉴美国经验,从细化法律要素、建立分类跨境数据管理体系、打造政企数据共享机制、引入第三方机构评估、坚持较高强度的本地化约束、建构"空间命运共同体"等方面持续深化推进跨境数据监管。

关键词:美国;数据跨境流通;监管;多边合作

"数据跨境流动"这一概念由经济合作与发展组织(OECD)提出,具体指数据跨国界传输以及可被第三国访问的情况。在经济全球化背景下,数据跨境流动逐渐成为数字经济发展的显著特征。数据资源逐渐成为一国发展的"核心资源",同国家安全、个人隐私保护、经济发展等社会价值紧密相连。这一背景下,数据跨境流动监管问题成为各国关注焦点和矛盾频发区。例如,2021 年 7 月,莫斯科法院对谷歌处以 300 万卢布罚款,原因在于谷歌拒绝将俄罗斯用户数据存储于俄罗斯本土服务器之上。中国近年来虽已开始制定有关数据跨境流动的监管规则,但由于缺乏相关的监管及立法经验,致使数据跨境规制整体进度相对缓慢。作为数据跨境流动监管的重要范式之一,美国在数据流动规则制定、执法程序设置方面已经较为成熟,对于中国完善数据跨境流动监管、强化国际协作具有极为重要的现实意义。

一、美国数据跨境流动监管的演变历程

(一)初步规制阶段(1970-2000 年)

美国数据跨境流动监管活动最早可追溯到上世纪 70 年代。1970 年美国和瑞士共同成立《公平信息实务准则》(下称《准则》),其中规范了关于数据警告、许可、精确性、安全性等概念,是针对数据隐私权最早的一部监管立法。1974 年,美国进一步出台《隐私权监管法案》。然而,由于该法案执行权被分散到联邦贸易委员会、联邦预算管理办公室和联邦储备委员会等不同政府机构,实施效果不佳。1980 年,OECD 以《准则》为基础,形成《隐私权和个人数据跨境流动保护的指导原则》,使多数国家在国内隐私权管理方面达成基本共识。此后,美国携手多个国家、地区与国际组织共同关注数据跨境问题。1997 年,克林顿政府出台《全球电子商务框架》,其中关于跨境数据流动治理的准则成为多国立法参考标准。基于此,美国数据跨境流动问题得到初步规制。

(二)"安全港"阶段(2001-2015 年)

进入 21 世纪,美国加大了同其他国家的数据跨境流动联合监管力度。为适应欧盟"充分保护"原则,美国转向与欧盟合作,在数据跨境问题上构建合作机制。《安全港协议》由此诞生。在具体内容上,《安全港协议》要求参与数据跨境交换的相关企业严格遵守欧盟规则,但对于企业所在国家的法律体系并未做出要求。在协议签署后的一段时间中,《安全港协议》成为 Microsoft、Google、Facebook 等超过 4500 家企业赖以运营的生命线。2011 年,美国同欧盟就电子商务问题共同提出一般性原则,并将此原则引入双边和多边协定谈判。2013 年美国在全球范围内大肆监听的"棱镜计划"曝光,引起欧洲剧烈反响。基于这一事件,欧盟法院在 2014 年 10 月否决《安全港协议》,认为该协定已不再适用欧美双方。此后,美国对跨境数据流动监管更加具有针对性。除欧盟外,美国与约旦、韩国等多国在数据跨境流动方面也达成多项协定,对跨

[作者简介]余萍(1982—),女,广州工程技术职业学院讲师;研究方向:金融经济、创新创业。

境电子数据传输等事项形成简单约定。

（三）“隐私护盾”阶段（2016年至今）

为削弱“棱镜计划”的负面影响，美国与欧盟经过谈判协商，于2016年2月2日达成“隐私护盾”协定。该协定主张在保护个人隐私的同时满足政府需求。此外，美国欲将获取海外数据方式合法化，通过增加多项立法为获取他国数据提供便利。2018年3月，美国通过《澄清境外数据合法使用法案》，击碎各国本土化数据保护屏障，在国际上形成了美国主导的数据主权规则体系。同年4月12日，美国向世贸组织总理事会提交了一份新议案（JOB/GC/178），提出包括信息自由流动在内的七项议题。总体来看，美国一定程度上支持数据跨境流动，但对于外国政府针对数据跨境流动设置的一系列措施则持反对态度。

二、美国数据跨境流动监管的措施及经验

（一）应用分类模式管理跨境数据

考虑到跨境数据来源渠道庞杂，为提高管理效率，美国依据数据价值形成重要数据、一般数据与个人数据三类管理模式。其一，重要数据。虽然在美国现有的法律体系中并未明确禁止数据跨境流动，但在认为国外网络运营商存在数据安全隐患时，会要求其在美国境内设置通信基础设施，并将通信数据、用户数据、交易数据等关键信息数据储存于美国境内。对于外资企业而言，这一强制措施意味着要在美国境内建立新的本地数据中心，导致运营成本进一步增加，损害投资利润。其二，一般数据。对于医疗、科技等行业数据，美国依据《出口管理条例》进行跨境管理。提供数据处理服务及数据所有权的相关主体必须取得出口许可证才能进行数据跨境流动。其三，个人数据。美国在个人数据的监管上相对宽松，允许个人数据自由流动。根据美国制定的个人数据隐私保护标准，监管部门很少在事前或事中对个人数据进行监管，仅在事后对于数据处理者的违法行为进行问责。整体而言，通过分级分类管理模式，美国不仅能够确保国家利益，还能使各类跨境流动数据得到适合自身特点的区别监督。

（二）采取政企信息共享强化数据跨境监管

在数据跨境流动监管方面，美国权力机关高度重视企业作用，常以国家安全为由，要求科技公司与执法机构进行数据信息共享。此前，美国纽约联邦地区法院曾要求微软公司协助调查一起毒品案，并要求其向调查局提交该用户的个人网络数据信息。但由于相关数据内容存储地并不在美国境内，因此微软拒绝向FBI提供用户数据，并提出废除搜查令的动议。这一事件引起社会对国家安全与个人隐私的广泛争论。为促进企业与执法机构数据共享，美国出台《网络安全信息共享法案》，以国土安全部为纽带，使企业与执法机构之间产生紧密联系，并以“阻止网络攻击”为名实现收集用户个人数据。2018年美国通过《CLOUD法案》，指导执法部门依法直接访问境外数据，为美国政府跨境调取本国公民数据提供极大便利。《CLOUD法案》的出台使得科技公司不仅可以减少因隐私案带来的漫长诉讼，而且也脱离了被舆论抨击的处境。同时，为尽可能多地收集跨境数据，美国一直以来在国际上倡导以大数据促进各国数据共享和交流。

（三）利用多边合作监管数据跨境

纵观美国数据跨境流动监管的历史进程可知，围绕跨境流动数据，美国一直尝试同其他国家进行联合监管。欧盟与美国2007年签署的《安全港协议》中，规定美国企业如果满足欧盟所规定的“充分保护水平”，则可获得跨境数据流动监管。2016年签订的“隐私护盾”协定又进一步规范了美欧之间企业及政府获取对方数据的权限。除了与欧盟之间的合作外，近年来美国还一直试图在其主导建立的TPP、USMCA中推行自身跨境流动数据的理念及制度。如此前TPP中就明确规定“允许缔约一方监管以电子方式传输的数据”，即TPP协定中包含的经济体之间可以联合监管。2018年美墨加三国签署的USMCA中在数据跨境流动方面同TPP也基本保持一致。此外，美国还与日本、韩国等国家联合推出CBPR体系。该体系以自愿认证为核心，通过认证的企业即可实现相互数据自由传输。借助联合监管，美国实现数据域名管辖权的大幅增加，跨境数据流动监管力度得到加强。

（四）借助第三方机构进行数据安全评估

在跨境数据评估方面，美国采