我国数据跨境流动法律规制的问题检视与完善路径

万广军,马小蕊

郑州轻工业大学 政法学院,河南 郑州 450001

摘要:数据跨境流动在助力数字经济发展的同时也衍生出各类新型安全风险,加强对数据跨境流动的法律规制势在必行。虽然我国数据跨境法律规制的框架基本形成,但仍存在数据发展与安全并重的价值导向不够清晰、法律适用规则粗糙、域外规制效果不佳等问题。在域外,典型的数据跨境流动法律规制模式有美国的“宽进严出”模式、欧盟的“外紧内松”模式、俄罗斯的“安全防御”模式,这对反思和完善我国数据跨境流动的法律规制具有启发意义。我国数据跨境流动法律规制的完善应确立以数据自由流动为原则、以安全为底线的价值导向,基于数据分类分级明晰数据跨境流动适用规则的界限,立足数据主权理论适当强化数据立法的域外规制力度。

关键词:数据跨境流动;数据主权;数据安全;数据分类分级

中图分类号:D922.16 **文献标识码:**A DOI:10.12186/2025.01.008

文章编号:2096-9864(2025)01-0059-10

近年来,世界经济发展呈现出全球化和数字化的双重特性,数据跨境流动成为助力全球经济发展的新引擎。2023年9月,国务院发展研究中心和中国信通研究院联合发布的《数字贸易发展与合作报告2023》显示,2022年全球数字服务贸易规模达3.82万亿美元,我国数字贸易的发展规模和增速位居世界前列。跨境数据服务贸易成为全球数字贸易发展的新态势,数据跨境流动成为各大经济体关注的热点。数据跨境流动对促进经济发展发挥了重要作用,但同时也衍生出数据攫取、跨国窃取、境外攻击等各种新型安全风险[1]。为此,以美国、欧盟、俄罗斯为代表的世界主要经济体均相继出台了规制数据跨境流动的法律法规和多边、双边经贸协议[2]254-256。我国作为世界第二大经济体,为应对数据跨境流动带来的安全挑战,对内制定了《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》《个人信息出境标准合同办法》等一系列法律法规和部门规章,对外参与了《区域全面经济伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》《数字经济伙伴关系协定》等多边经贸协议,为确保我国数据跨境流动安全提供了有力支持。然而,我国数据跨境流动安全治理尚处于起步阶段,

收稿日期:2024-07-03

基金项目:河南省高等学校哲学社会科学基础研究重大项目(2024-JCZD-16);河南省软科学研究重点项目(242400411007);河南省高校人文社会科学青年项目(2025-ZDJH-002)

作者简介:万广军(1971—),男,河南省西平县人,郑州轻工业大学副教授,博士,主要研究方向:数字法学;马小蕊(1990—),女,河南省方城县人,郑州轻工业大学硕士研究生,主要研究方向:数字法学。

仍面临一系列治理难题,需要进行系统检视并予以完善。鉴于此,本文拟在对我国数据跨境流动法律规制问题进行检视的基础上,借鉴域外典型数据跨境流动法律规制模式,提出我国数据跨境流动法律规制的完善路径,以推动全球数字经济持续健康发展。

一、我国数据跨境流动法律规制的问题检视

当前,虽然我国数据跨境流动的法律规制体系已经基本建立,但在价值导向、适用规则和域外规制效果方面仍存在不少问题。

1. 价值导向不够清晰

流动性作为数据的天然属性,是释放数据经济效能的助推器。换言之,数据只有通过流动才能彰显其经济价值,尤其是数据的跨境流动已经成为推动全球经济发展的重要力量。2022 年 12 月,中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》明确提出,要充分发挥我国海量数据规模和丰富应用场景的优势,激活数据要素潜能,推动数据跨境流动,鼓励探索数据跨境流动与合作的新途径新模式。由此可见,数据跨境流动是促进我国积极融入全球数字经济新一轮竞争的重要一环。然而,如果一味地鼓励数据跨境流动而不予以必要的法律规制,势必会诱发侵犯个人隐私、损害公司权益,甚至危及国家安全的风险。例如,“‘滴滴出行’海外上市案”,在该案中,“滴滴出行”作为一家大型网约车公司,掌握了海量的关系到国家安全的测绘数据和公民个人信息,为拓展海外业务,该公司在未经数据出境安全审查的情况下于 2021 年 6 月 30 日在美国低调上市。两天后,国家网信办对其开展安全审查,发现该公司存在违法违规收集公民个人信息和关键信息基础设施数据等严重危害国家安全的数据处理活动,最终对其判处 80.26 亿元罚款[3]。

《数据安全法》第十一条规定,国家要促进数据跨境安全、自由流动;第十三条规定,国家要统筹发展和安全,坚持以数据发展促进数据安全,以数据安全保障数据发展。基于此,学界通常认为,我国数据跨境流动治理应坚持发展与安全并重的原则。一方面,在数字经济已成为全球经济新的竞争点的背景下,数据跨境流动治理不能因安全需要搞“一刀切”而增加企业数据跨境流动的合规成本,以致降低企业开展海外业务的积极性,损害数据跨境流动带来的巨大经济利益;另一方面,要坚持数据安全不动摇。当前,虽然我国数字经济产业的规模居于世界前列,但数字创新能力和数字治理水平不高,应对各类数据安全风险的能力不足,必须通过构建完备的数据跨境流动安全治理体系才能确保数字经济健康有序发展[4]。

诚然,发展与安全并重是处理数据跨境流动问题的理想状态,但二者毕竟价值导向不同,一旦发生冲突,如何进行平衡和抉择便成为无可回避的问题。作为价值导向原则,如果缺乏明确的指引性,势必会造成实践的困惑,导致过度监管和过度放纵两个极端。

一方面,长期以来,我国对数据跨境流动持谨慎态度,数据跨境流动的路径过于单一,即需要通过有关部门审查许可之后方能出境。这种过度追求安全价值的“一刀切”模式不仅在无形当中增加了审查机关的工作量,而且损害了数字经济的效率价值,导致数字经济活动无法及时有效开展[5]。欧洲国际政治经济研究中心的报告显示,过于严苛的数据跨境管控导致中国 0.55% 的 GDP 损失[6]。另一方面,随着我国对外开放的不断深化,大量外资企业进入国内,为我国经济发展作出了重要贡献,但其在经营过程中收集的海量数据通过跨境流动引发了一系列安全风险。与此同时,越来越多的国内企

业开始走出国门,积极拓展海外市场,开展涉外业务。在此过程中,一些涉及我国关键信息基础设施、地理测绘、人类遗传等的重要数据在未经有效甄别和审查的情况下流向境外,给我国的数据安全带来了极大隐患。除前文提及的“‘滴滴出行’海外上市案”外,还有“深圳华大基因科技公司案”,该公司在与英国牛津大学开展人类基因国际合作研究的过程中,将 14 万条中国人基因数据非法传输到境外[7]。显然,笼统地强调发展与安全并重难以为数据跨境流动安全治理提供行之有效的价值指引。

2. 适用规则粗糙模糊

我国数据跨境流动法律规制的适用规则经历了一个不断演变发展的过程。2016 年 11 月出台的《网络安全法》第三十七条首次规定,对于关键信息基础设施运营者在境内收集和产生的个人信息和重要数据应当实行本地存储,确需向境外提供的,应进行安全评估。2021 年 6 月出台的《数据安全法》第三十一条进一步区分了关键信息基础设施运营者和其他数据处理者,8 月出台的《个人信息保护法》第三十八条针对个人信息出境确立了安全评估、保护认证、标准合同的法律规制体系。随后,《数据出境安全评估办法》《个人信息保护认证实施细则》《个人信息出境标准合同办法》等一系列细化规则相继推出。据此,安全评估、保护认证、标准合同构成了我国数据跨境流动的基本法律规制体系[8]。然而,上述规则看似精细完备,实则粗糙模糊,导致在具体适用中出现了规制空白和界限不清等问题。

例如,按照数据跨境流动的现有法律规制体系,重要数据和大规模的个人信息跨境流动需要进行安全评估,中小规模的个人信息跨境流动需要进行个人信息保护认证或签订标准合同。但问题在于,数据和信息并不属于同一范畴。从存在形式上看,信息的载体广于数据,即信息除可以依附于数据外,还包含其他存在形式;从具体内容上看,数据的范围广于信息,即数据既可以是具有现实意义的信息,也可以是无现实意义的代码。概言之,两者是相互交叉的关系[9]。这就意味着,数据有一般数据和重要数据之分,个人信息有普通信息和敏感信息之别。由此导致,既非重要数据又非个人信息的一般数据的跨境流动无法得到有效规制,而对个人信息不以重要性而单纯以规模作为规制标准同样会导致敏感个人信息的跨境流动面临如何规制的尴尬境地。

再如,安全评估和标准合同的适用界限模糊。从适用逻辑上讲,由于安全评估针对的是重要数据和大规模的个人信息跨境流动,标准合同针对的是中小规模的个人信息跨境流动,前者的规制标准应当高于后者。但从现有规定来看,两者的界限并不清晰。一方面,按照《数据出境安全评估办法》第五条的规定,数据处理者开展出境风险自评估应重点围绕数据处理的目的、范围、方式与数据本身的规模、范围、种类、敏感程度进行;《个人信息出境标准合同办法》第五条几乎全盘复制了《数据出境安全评估办法》第五条的规定,即要求个人信息跨境流动要重点评估个人信息处理的目的、范围、方式与个人信息本身的规模、范围、种类、敏感程度。另一方面,《数据出境安全评估办法》第四条、第六条规定,数据跨境流动应向省级网信部门提交申报书、自评估报告、法律文件、其他材料等;《个人信息出境标准合同办法》第七条规定,个人信息跨境流动应向省级网信部门提交标准合同、评估报告等以备案审查,尽管前者是申报,后者是备案,但两者在具体内容上并无实质差别[10]。显然,安全评估与标准合同的适用界限不清有悖其立法目的,导致实践中中小规模的数据出境门槛被不当提高,加大了中小企业开展数据出境业务的成本。

3. 域外规制效果不佳

数据跨境流动不可避免地会引发涉外案件,如何开展域外管辖和执法活动,成为各国数据跨境流动法律规制的焦点问题。目前,我国《数据安全法》第二条规定,发生在我国境内的数据处理活动和损害我国国家利益、公共利益或公民、组织合法权益的数据处理活动适用本法;第三十六条规定,国家有关主管部门针对国外司法或执法机关提出的关于提供数据的请求,依照我国参加或缔结的国际条约、协定,或者按照平等互惠的原则处理,未经批准,境内的组织或个人不得向国外司法或执法机关提供存储在境内的数据。这种属地为主的管辖原则和"公对公"的执法处置模式与欧美确立的域外管辖和执法模式明显不同。

在欧盟,《通用数据保护条例》第三条规定,本条例适用三种情况:处理个人数据的欧盟内组织,即使实际处理活动在欧盟外进行;欧盟外组织处理欧盟居民的个人数据(作为其向欧盟提供商品或服务的一部分)或对欧盟居民的行为进行监测;根据国际法,受欧盟法律管辖的欧盟外组织[11]9。不难看出,《通用数据保护条例》的管辖范围由属地向属人、保护管辖扩张,执法效力扩张到欧盟以外,使其事实上成为一部世界法[12]。在美国,《澄清境外数据的合法使用法案》第十条规定,只要数据处理者具有"美国人"身份,其数据处理活动都要受美国监管,而不论数据是否存储在美国境内。由于美国事实上在境外拥有海量和强大的数据企业,其执法机关可以依据长臂管辖权直接向数据服务提供者调取境外数据[13]。

显然,相比于欧美,我国数据跨境流动的域外规制力度较弱,导致针对涉外案件的管辖和执法效果不佳,如涉外信息网络犯罪。2022 年,最高人民法院、最高人民检察院、公安部联合发布的《关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》第 2 条规定,信息网络犯罪案件的犯罪地包括涉案服务器所在地、网络服务提供者所在地、被侵害的信息网络系统与管理者所在地、信息网络系统使用者所在地、被害人被侵害或财产所在地。该规定应对国内信息网络犯罪没有问题,但针对涉外信息网络犯罪案件则力有不逮。原因就在于,我国域外刑事执法管辖权缺失[14]。而现有"公对公"的跨境执法体系和机制不够灵活,且容易受到政治、外交等因素的影响,导致涉外信息网络案件侦破难度巨大、效果不佳[15]。

二、域外典型的数据跨境流动法律规制模式

在世界范围内,美国、欧盟、俄罗斯较早地开展了数据跨境流动的法律治理,并逐步形成了特色鲜明的治理模式,这对我国数据跨境流动法律规制的完善具有启发意义。

1. 美国的"宽进严出"模式

在全球范围内,无论是数字经济的规模还是竞争力,美国都处于无可争议的领先地位。因此,为了获取更大的经济利益,美国一直主张所谓的"数据自由流动"模式,这在其主导制定或参与的双边、多边经贸协议中得到了充分体现。例如,2019 年 10 月,美国和日本签订的《美日贸易协定》和《美日数字贸易协定》规定,所有供应商均可跨境传输数据,禁止限制数据本地化存储的措施。再如,2020 年 7 月,美国、墨西哥、加拿大签订的《美墨加协定》规定,要确保数据可以跨境流动,最小化地对数据存储和处理位置进行限制,交流与数字贸易有关的信息和经验,重视网络安全和政府数据公开[16]。还如,《亚太经合组织隐私框架》《跨太平洋伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》等多边经贸协定也都强调数据的自由流动,并通过《澄清境外数据的合法适用

法案》确立了“长臂管辖权”[17]。

然而,从美国国内关于数据跨境流动的相关政策法规来看,其针对本国的一些重要数据采取了严格的监管举措。例如,《联邦、州和地方机构的税务信息安全指南》规定,联邦税务信息系统必须限制在美国本土、大使馆或军事设施内。再如,《国防部采购条例补充规定》规定,云计算服务条款规定的所有 CDI 必须保存在美国境内的云服务器中。还如,《出口管理条例》《出口管制法》《商业管制清单》规定,向外国人出售国家管制的技术数据之前,必须获得政府授权[17]。

不难看出,美国采取的是“宽进严出”的数据跨境流动法律规制模式,带有明显的双重标准特征。一方面,美国一直倡导所谓的数据自由流动模式,但实际上是境外数据自由流向本国境内的单向流动模式,并且赋予了本国执法部门对境外数据处理活动的“长臂管辖权”,其目的在于,利用自身强大的数字经济规模和竞争优势攫取他国的数据资源,获取巨大的经济利益,实现自身的数据霸权战略;另一方面,美国又因循属地原则,对本土数据尤其是涉及国家安全的数据,采取严格的管控措施,针对外国政府获取美国境内数据的行为,通过设立执行协议确立“适格外国政府”的认可制度,人为提高数据流出门槛,严控数据出境[18]。一言以蔽之,不论是“宽进”还是“严出”,其出发点和落脚点都是最大限度地维护美国自身的经济利益和政治利益。

2. 欧盟的“外紧内松”模式

欧盟作为世界上重要的经济体,在全球数字经济发展格局中居于举足轻重的地位。从价值导向来看,欧盟并没有将数据作为纯粹的经济资源,而是将其视为公民的基本权利。这是因为,二战期间,纳粹德国通过获取公民个人信息的方式对犹太人实施了惨绝人寰的种族灭绝行为。二战结束之后,强化对公民个人信息的保护成为欧洲社会的共识。因此,欧盟的《通用数据保护条例》第一条第二款明确规定,本条例旨在保护自然人的基本权利和自由,尤其是个人数据保护的权利。同时在具体条文中为数据主体详细设置了数据查阅权、更正权、被遗忘权、限制处理权、携带权、反对权、与自动决策有关的其他权利[11]31-37。

正因为欧盟对数据法律性质的高定位,其对欧盟内部数据跨境流向外部的行为采取了严苛的监管规则,主要表现为“充分性认定”制度。早在 1981 年,欧洲委员会制定的《关于个人数据自动化处理的个人保护公约》(即“108 号公约”)提出,缔约国之间的数据跨境流动应以数据接收国具备与欧盟“同等水平”的数据保护力度为前提。1995 年发布的《第 95/46/EC 号保护个人在数据处理和自动移动中权利的指令》以是否符合“充分性条件”将对外第三国的数据跨境流动分为符合型和不符合型两种。2018 年的《通用数据保护条例》则进一步将“充分性认定”细化为第三国是否加入了“108 号公约”、法治水平、人权保护度、是否设立独立的监管机构,并以此将符合上述标准的国家列入“白名单”[18]。

这从欧美关于数据跨境流动的激烈博弈便可窥见一斑。2000 年 11 月,欧美就数据跨境流动达成了《安全港协议》,后因“斯诺登事件”于 2015 年被欧洲法院判定无效。2016 年双方又签订了《隐私盾协议》,后因该协议提出的情报系统内控机制缺乏约束和国家安全条款引发权利保护的忧虑,于 2020 年被宣告无效,直到 2022 年欧美双方才最终达成了《欧美数据隐私框架协议》,历时 20 余年双方经过不断磨合才暂时达成了一致[19]。原因在于,与美国相比,欧盟的数字经济规模和竞争力都比较弱,因此,其对数据跨境向外流动采取的是收紧策略,背

后是数据权利的驱动;而美国因其优势地位强调数据的自由流动,背后是经济利益和政治利益的驱动。

相比于对数据跨境向外流动采取的高门槛不同,欧盟对内部的数据跨境流动采取了自动流动模式。1981 年通过的“108 号公约”要求成员国之间的个人数据应自由流通;2015 年公布的《数字化单一市场战略》旨在打破数字贸易壁垒,打造欧盟数字单一市场;2018 年通过的《通用数据保护条例》扫除了各成员国之间的数据流通障碍,为打造数字单一市场、促进数字经济发展提供了统一的立法依据[12]。由此可见,欧盟对于数据的跨境流动采取的是“外紧内松”模式,这与其重视权利保护的传统和数字经济发展的实力、地位等现实因素密切相关。

3. 俄罗斯的“安全防御”模式

与欧美相比,俄罗斯的数字技术发展水平较低,数字经济发展羸弱,为抵御外部风险,维护数据安全,其针对数据跨境流动采取了“安全防御”模式。这主要表现为两个方面:一是确立了数据的本地化存储规则;二是基于极端前置理念巩固属地管辖[18]。

早在 20 世纪 90 年代,俄罗斯就制定了《关于信息、信息化和信息保护法》,到了 2006 年,该法被《关于信息、信息技术和信息保护法》取代。同年,《个人数据保护法》出台,确立了以“同等保护”为标准的个人数据跨境流动规则。此时,俄罗斯针对数据跨境流动采取的“同等保护”标准类似于欧盟的“充分性认定”制度。然而,随着 2013 年“棱镜门事件”的发生,俄罗斯于 2014 年 5 月、7 月两次对《关于信息、信息技术和信息保护法》和《个人数据保护法》进行了修改,确立了数据本地化存储规则。其具体包括三点:一是公民个人信息和数据库必须在俄罗斯境内存储;二是对俄罗斯公民个人数据的处理活动必须使用俄罗斯境内的数据库;三是数据处理者必须向有关部门履行告知义务和协助义务。由此政府实现了对包括数据跨境流动在内的所有数据处理环节的全面掌控[20]。

此外,由于俄罗斯的数字经济发展竞争力较低,缺乏数据引流能力,贸然放开数据管制势必会导致该国数据大规模流向发达经济体,进而危及该国的数据安全。因此,俄罗斯基于极端前置理念,先是通过加强认证、实施“白名单”制度严控数据出境,主要依据是“108 号公约”和《个人数据保护法》,即只允许境内个人数据传输到该公约的签署国或者“白名单”所列的国家;然后从维护国家主权安全出发,通过颁布《网络安全战略构想》《关键信息基础设施安全法》等政策法规大力发展网络技术与关键基础设施,从根本上提高抵御外部数据风险的能力[18]。

纵观俄罗斯的数据跨境流动法律规制模式,其经历了从自由放任到安全防御的转变,除“棱镜门事件”这一直接诱因外,还与俄罗斯长期以来重视国家安全的历史传统和遭遇各类数据安全事件的现实需求密切相关[20]。

综上,我国在建立和完善数据跨境流动法律规制体系时可从上述典型的数据跨境流动法律规制模式中得到启示:首先,不能以数据安全为由“一刀切”地推行数据的本地化存储,从而不当限制数字经济的发展。在这一点上俄罗斯的安全防御模式即为典型。其次,数据跨境流动法律规制策略的选择应当与本国数字经济的发展规模和数字技术能力相适应。因此,像美国一样对外采取完全的数据自由流动模式也不适合我国,因为我国的数字经济发展规模和数字技术能力与美国还存在不小的距离。再次,欧盟的部分做法(如充分性认定制度)值得借鉴,这有助于我国数据跨境流动法律规制体系的完善。

三、我国数据跨境流动法律规制的完善路径

针对上述我国数据跨境流动法律规制存在

的现实问题,通过介绍美国、欧盟、俄罗斯的数据跨境流动法律规制模式,可从以下三个方面完善我国数据跨境流动的法律规制体系。

1. 确立以数据自由流动为原则、安全为底线的价值导向

在数字经济全球化的浪潮下,数据作为一种重要的战略资源已经成为世界各国竞相争夺和博弈的重点,因数据跨境流动产生的信息流已经逐步成为全球经济链不可或缺的部分,但与此同时,因数据跨境流动带来的各类经济社会安全风险也开始全方位显现[2]255-256。可见,数据本身是把"双刃剑",利益与风险并存。如前所述,世界各主要经济体基于自身的数字经济规模、数字技术水平、安全防范能力等多种因素考量,确立了不同的数据跨境流动法律规制模式。对于我国来说,既不能像美国一样因为拥有绝对的数字经济实力而对绝大多数的跨境数据流动采取自由宽松的态度,也不能像欧盟和俄罗斯一样出于保护个人数据权利和维护国家安全的需要严控数据出境,而应当在数据发展与数据安全之间寻求平衡,即数据发展与数据安全并重[4]。从更具指引性的角度讲,数据发展与数据安全并重不是数据发展与安全平行,而应以发展为原则、以安全为底线。换言之,对于一般数据原则上实行自由流动模式,对于涉及国家安全的数据实行严格的出境管制。

之所以强调对于一般数据原则上实行自由流动模式,这主要是基于我国数字经济发展的现实需要。一方面,发展数字经济是我国确立的重大战略,从2017年党的十九大报告首次提出"建设数字中国",到2020年党的二十大报告强调"要加快发展数字经济,促进数字经济和实体经济深度融合",再到2023年,中共中央、国务院专门印发《数字中国建设整体布局规划》。正是在此背景下,自2017年开始,我国数字经济规模连年增长,并于2022年首次突破50万亿元,占GDP的比重达到了41.5%,充分发挥了经济发展"稳定器""加速器"的作用①。由此可见,数字经济已经成为助推我国经济发展的重要力量。另一方面,从全球范围来看,虽然我国的数字经济规模仅次于美国,位居世界第二,但数字创新和治理能力仍显不足。《全球数字经济竞争力发展报告(2023)》显示,美国的数字创新指数为80.18,数字治理指数为86.54;而我国的数字创新指数为51.52,数字治理指数为49.65[21]。因此,要促进我国数字经济持续健康发展,必须提高数字创新和治理能力,而只有数据自由流动才能最大限度地释放数据效能,助力经济发展,不断提高数字创新和治理能力。《全球数字经贸规则年度观察报告(2022)》显示,数据跨境流动成为驱动全球数字经济增长、提高数字创新和治理能力的主要力量,数据流动量每增加10%,将带动GDP增长0.2%②。

与此同时,数据跨境流动并非毫无限制,需要恪守安全底线,即对于涉及国家安全的数据要实行严格的出境管制。这种底线安全观有助于明晰我国数据跨境流动的法律规制方向。具体来说,要重视关键、重点领域立法,聚焦敏感数据,细化相关领域数据跨境流动的法律规制细则。当前,我国只在《个人信息保护法》《数据安全法》等基础性法律中对数据跨境流动作了原则性规定,对涉及国家安全、健康医疗、金融信息等关键、重要领域的数据跨境流动缺乏充分观照,导致实践中对数据的跨境流动通常采用"一刀切"模式。而在国外,已有国家对关键、重点领域的数据跨境流动的法律规制开展

①参见中国信息通信研究院发布的《中国数字经济发展研究报告(2023)》。

②参见中国信息通信研究院发布的《全球数字经贸规则年度观察报告(2022)》。

了小切口、精细化立法,如韩国的《空间数据的建立和管理法案》、澳大利亚的《健康档案法案》等,这一点值得我国学习借鉴[22]。实际上,从我国近年来签署加入的多边经贸协议来看,已经将“自由流动 + 安全例外”确立为我国数据跨境自由流动法律规制的价值导向。2020 年签署的《区域全面经济伙伴关系协定》、2021 年加入的《全面与进步跨太平洋伙伴关系协定》、2024 年加入的《数字经济伙伴关系协定》均规定,除公共政策目标和保护基本安全利益外,缔约各方有义务实行数据跨境自由流动①。

2. 基于数据分类分级明晰数据跨境流动适用规则的界限

通过确立具有一定梯度和可操作性的法律规制标准,对拟跨境流动的数据类型及其安全风险进行评估,是明晰我国数据跨境流动法律适用规则的前提,而达成该目标的关键在于落实《数据安全法》第二十一条确立的数据分类分级制度[23]。问题在于,如何确立数据分类分级的具体规则。张勇[24]提出,应先进行数据分类再进行数据分级。对于前者,可依据数据所属主体将其分为国家数据、公共数据、个人数据,这是目前我国普遍采取的数据分类;对于后者,可依据对数据的侵害程度分为一级、二级、三级数据。高磊等[25]根据《数据安全法》的相关规定,将数据分为重要数据、个人信息、公共开放数据、其他数据,并综合考虑数据的应用场景、重要程度、影响对象、影响广度、影响深度等将各类数据分为一级、二级、三级、四级。

在我们看来,应当区分数据分类和分级,前者以权属类型为依据,后者以侵害程度为依据;前者是后者的基础,后者是前者的目的。因此,上文所说的重要数据应属于数据分级而非数据分类,而目前普遍采用的国家数据、公共数据、个人数据分类也存在疑问。因为看似全面的分类实则无法形成制度合力,呈现出零碎化设计,导致数据叠床架屋,难以实现数据要素的有效整合和高效运行。例如,《浙江省数字经济促进条例》将公共数据的主体限定在政务部门,忽视了政务部门以外的其他公共机构;《深圳经济特区数据条例》将数据划分为公共数据和个人数据,其在强调保护个人数据的同时,也传递了两者的对立关系,导致各类数据无法协调合作[26]。

妥当的做法是,根据数据所属的行业和领域,参考《国民经济行业分类》的规定,立足农林牧渔业、采矿业、制造业、建筑业、住宿和餐饮业、科学研究和技术服务业等 20 大类行业对所涉数据进行分类。此种分类符合《数据安全法》第二十一条关于数据目录的制定以行业、领域为准的规定,更为稳定和周全[27]。在分类确定之后,根据《数据安全法》《网络数据安全管理条例(征求意见稿)》的相关规定将数据等级划分为核心数据、重要数据、一般数据,然后再根据该数据的影响对象(主要是国家安全、公共利益、个体权利)和影响程度(如特别严重、严重、中等、轻微、无)进一步分为 5 个等级。

在对数据进行分类分级后,可按不同种类和等级的数据分别适用不同的数据跨境流动法律适用规则。首先,需要判定该数据是否属于关系到国家安全、国民经济命脉、重大公共利益和重要民生等的数据,即是否属于核心数据,如果是,则按照严重程度将其定为 5 级或 4 级数据,并适用安全评估规则。其次,如果该数据不属于核心数据,则需要判断其是否属于一旦遭到篡改、破坏、泄露或者非法获取、非法利用,可能危害国家安全、公共利益的数据,即是否属于重要数据,如果是,则根据其严重程度将其定为 4 级或 3 级数据,并适用安全评估或保护认证

①参见中国信息通信研究院发布的《全球数字经贸规则年度观察报告(2022)》。

规则。再次,如果该数据不属于重要数据,则将其认定为一般数据,并进一步将其细化为2级或1级数据,并适用标准合同或自由流动规则。

3. 立足数据主权理论适当强化数据立法的域外规制力度

通常来讲,数据主权是国家主权在网络空间延伸的产物,包括对内的数据管辖权和对外的数据合作治理权。与传统主权不同,数据主权具有空间的虚拟性、结构的层级性、边界的双重性等特点,由此导致数据主权的边界既有形(数据在境内)又无形(数据在境外),其边界大小取决于本国数据主权与他国数据主权抵牾博弈后形成的结果[23]。因此,为了维护本国的数据主权,应当采用有力举措积极应对域外的数据规制行为。如前所述,面对欧美不断扩张其数据域外管辖权,我国采取的是防守策略,这不仅使我国的数据产业发展陷入被动,而且不利于参与全球数据治理[28],未来我国应立足数据主权理论从以下两个方面适当强化我国数据立法的域外规制力度。

一方面,通过立法确立数据域外执法权。我国《数据安全法》第二条确立了以属地管辖为主、保护管辖为辅的数据管辖原则,即发生在我国境内的数据处理活动和损害我国国家利益、公共利益或公民、组织合法权益的数据处理活动适用本法。对于属地管辖争议不大,问题在于如何落实保护管辖。对此,有学者提出,考虑到当前我国的数字技术水平还不高,不宜采用美国式的"长臂管辖权",但可借鉴欧盟数据立法中的"市场破坏措施",即赋予数据监管机构执法权,针对域外的数据处理者不遵守我国数据法律法规的行为,禁止其在我国进行数字贸易或使其债权无法执行[15]。此建议具有较强的可操作性,因为我国拥有巨大的数字市场规模,能够以此倒逼境外数据处理者配合我国的域外数据执法行为,而且目前我国的数据监管机构是网信部门,本身拥有一定的执法权,具有开展域外执法的优势。

另一个方面,完善数据阻断立法。我国《数据安全法》第三十六条规定了"公对公"的数据执法处置模式,对域外的"长臂管辖权"进行了阻断,即针对国外司法或执法机关提出的关于提供数据的请求,依照相关条约、协定或者平等互惠的原则处理,未经批准,境内的组织或个人不得向境外提供存储在境内的数据。但以上规定过于原则、笼统。未来国家数据监管机构可以事前列明实施"长臂管辖"的国家目录,明确否认这些国家的数据调取请求,未经允许我国境内的数据处理者不得向其提供数据。如此攻防结合,才能牢牢把握数据跨境流动的主动权,切实维护我国的数据主权。

四、结语

当前,数据跨境流动已经成为全球数字经济发展的新常态,其在助力经济发展的同时也诱发了各种安全风险,这对各国的数字安全治理提出了新的挑战。近年来,我国积极融入全球数字经济圈,初步构建了数据跨境流动的法律规制框架,但仍面临一系列现实难题。为此,可从域外典型的数据跨境流动法律规制模式中得到启示,并从明确价值导向、明晰适用规则、强化域外规制力度等方面予以完善,从而为推动全球数字经济发展贡献中国方案和中国智慧。

参考文献:

[1] 董克,吴佳纯,马廷灿.我国数据出境安全风险要素体系研究[J].情报理论与实践,2024,47(6):49-59.

[2] 方东兴,钟祥铭.中国数字治理发展报告:2023[M].北京:社会科学文献出版社,2023.

[3] 童磊."滴滴出行"事件的启示:企业数据安全合规需坚守红线[J].中国信息安全,2021(7):84-85.

[4] 郭德香. 我国数据出境安全治理的多重困境与路径革新[J]. 法学评论,2024,42(3):170 - 181.

[5] 李晓楠,宋阳. 国家安全视域下数据出境审查规则研究[J]. 情报杂志,2021,40(10):74 - 82.

[6] 许可. 自由与安全:数据跨境流动的中国方案[J]. 环球法律评论,2021,43(1):22 - 37.

[7] 焦小妹,沈本秋. 我国企业数据出境的安全监管问题研究[J]. 网络安全与数据治理,2022,41(11):22 - 29.

[8] 叶传星,闫文光. 论中国数据跨境制度的现状、问题与纾困路径[J]. 北京航空航天大学学报(社会科学版),2024,37(1):57 - 71.

[9] 刘宪权. 数据犯罪刑法规制完善研究[J]. 中国刑事法杂志,2022(5):20 - 35.

[10] 赵精武. 论数据出境评估、合同与认证规则的体系化[J]. 行政法学研究,2023(1):78 - 94.

[11] ITGovernance 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.

[12] 司伟攀. 欧盟个人数据跨境传输治理演进、范式及其镜鉴[J]. 科技管理研究,2023,43(20):205 - 213.

[13] 孙永超. 论美国跨境刑事数据调取中的国际礼让:以《云法案》为例的分析[J]. 求是学刊,2024,51(3):126 - 139.

[14] 甄航. 数据跨境流动刑事保护的困境与破解[J]. 安徽大学学报(哲社版),2024,48(1):119 - 127.

[15] 付裕媛. 我国数据跨境流动监管缺位问题及应对[J]. 法律研究,2024(1):91 - 101.

[16] 王晓瑾. 美国跨境数据自由流动与国家安全的平衡范式[J]. 北京政法职业学院学报,2021(4):49 - 54.

[17] 华佳凡. 美国跨境数据流动国际倡议与国内政策的差异及其成因[J]. 情报杂志,2024,43(1):98 - 105.

[18] 冉从敬,何梦婷,刘先瑞. 数据主权视野下我国跨境数据流动治理与对策研究[J]. 图书与情报,2021(4):1 - 14.

[19] 桂畅旎,任政,熊菲. 美欧跨境数据流动规则演变及启示[J]. 信息安全与通信保密,2023(11): 15 - 24.

[20] 何波. 俄罗斯跨境数据流动立法规则与执法实践[J]. 大数据,2016,2(6):129 - 134.

[21] 王振,惠志斌. 全球数字经济竞争力发展报告[M]. 北京:社会科学文献出版社,2023:3 - 4.

[22] 徐拥军,王广兴. 总体国家安全观下的跨境数据流动安全治理研究[J]. 图书情报知识,2023,40(6):20 - 30.

[23] 陈斌彬,王斌楠. 数据主权视阈下我国数据出境的法律规制及完善[J]. 华侨大学学报(哲学社会科学版),2024(2):49 - 63.

[24] 张勇. 数据安全分类分级的刑法保护[J]. 法治研究,2021(3):17 - 27.

[25] 高磊,赵章界,林野丽,等. 基于《数据安全法》的数据分类分级方法研究[J]. 信息安全研究,2021,7(10):933 - 940.

[26] 秦鹏,董雯静. 数据分类的结构样态、逻辑困境与规范进路:基于功能主义视角下央地制度文本的考察[J]. 中国行政管理,2023,39(9):114 - 123.

[27] 李怀胜. 数据安全合规实务[M]. 北京:中国法制出版社,2023:57.

[28] 王雪,石巍. 个人数据域外管辖权的扩张及中国进取型路径的构建[J]. 河南社会科学,2022,30(5):56 - 67.

[责任编辑:毛丽娜　吴永辉]

引用格式:万广军,马小蕊. 我国数据跨境流动法律规制的问题检视与完善路径[J]. 郑州轻工业大学学报(社会科学版),2025,26(1):59 - 68.