

数据主权视阈下的数据跨境流动 及中国因应

姚 天¹, 王 宇²

(1. 山东建筑大学 法学院, 山东 济南 250101;

2. 青海民族大学 法学院, 青海 西宁 810007)

摘要: 基于数据新型生产要素之战略性, 主权因素成为数据跨境流动场景的关键限制, 表现为数据定位壁垒与数据出境壁垒。不同国家之间的数据主权立场存在差异, 其中的数据主权博弈影响着一国数据跨境流动法律制度的立法目的, 国家间有失协调的数据跨境流动规则以及该领域内国际规则的缺位极大地阻碍了数据跨境有序流动。中国对待数据跨境流动秉持安全与自由相平衡的基本理念, 在此基础上应当完善数据跨境流动的制度框架, 在立法上应适时细化专门性的数据保护法, 重视数据跨境流动纠纷应对机制的建构。

关键词: 数据跨境流动; 国家安全; 数据主权; 数据安全

[中图分类号]F752 [文献标识码]A [文章编号]1002-4034(2025)02-0141-16

引 言

当前, 数字治理已进入全球化新拐点, 机遇与风险共举, 秩序与自由并存。在全球贸易时代, 数据的跨境流动是一项重大的战略性资源, 关系到个人信息的保护、社会秩序的维持、国家安全的保障、国际执法权责分配等多个法律问题。数据跨境流动是中国数字经济发展的关键驱动因素。目前, 中国数据跨境流动的法律规制存在一定的主权壁垒问题, 表现为立法和执法上对企业境外存储数据的限制, 以及司法上对域外取证困难的承认。造成主权壁垒的主要原因是中国企业对境外数据存储和处理的能力不足, 以及域外取证困难等。因此目前待解决的核心问题就是数据跨境流动法律规制之主权障碍。从技术角度来看, 前述的数据跨国流通中所遭遇的主权障碍, 存在通过法律技术解决的可能。本文拟研究数据自由与数据安全的矛

[收稿日期]2023-07-26

[基金项目]国家社会科学基金青年项目“算法中的反歧视问题研究”(19CFX016), 青海民族大学校级规划项目“中国共产党推进中华民族共同体建设的法治路径研究”(2022GH04)

[作者简介]姚天(1985—), 男, 山东济南人, 山东建筑大学法学院讲师, 博士, 研究方向: 科技法、行政法; 王宇(1997—), 男, 湖北天门人, 青海民族大学法学院讲师, 博士, 研究方向: 行政法、民商法

盾与融合问题,在此基础上,立足于自身数据产业发展的现实情况,以国际合作为基本原则,以促进企业境外存储和处理能力为重点,提出一套以数据主权为基础的中国特色跨境数据治理战略,重塑新型国际数据跨境流动秩序,实现对数据跨境流动的规制。

一、数据跨境流动场景中的主权因素

数据主权壁垒是指国家对数据跨境流动的数据保护措施,旨在保护个人隐私和数据安全,保障公民权利和国家利益。考察当前国际社会上的数据跨境流动立法,反映数据主权壁垒的数据安全保护要求包括以下几个方面:第一,个人信息保护。某些国家(地区)制定严苛的个人信息保护法律法规,要求各社会组织在数据主体明确授权的前提下,才能获取和利用其信息,且对个人信息范围采取扩大化理解。第二,数据安全保护。国家要求企业采取大量的技术和组织措施,保障数据的安全性和完整性,避免数据被非法获取、篡改、破坏或泄露,确保数据的机密性、可靠性和可用性。第三,数据隐私协议。国家要求企业在数据跨境流动之前,与数据接收方签署严密的数据隐私协议,明确数据使用的范围、目的和方式,保障数据主体的隐私权利和数据安全。第四,国家安全维护。由于数据及其跨境流动事关国家政治、经济、军事、文化等总体层面的安全,是国家的核心利益之一。国家通过数据主权的确立和行使,以及数据的内容和形式安全的保护,从而确保国家总体安全利益得到维护。正是由于上述数据安全保护要求的存在,数据跨境流动法律规制的主权壁垒的形成具有必然性。为了化解数据跨境流动法律规制的主权壁垒,有必要从本体论的角度对数据主权壁垒的形成机理及表现形式进行分析。

(一) 国家主权对数据跨境流动的限制

主权壁垒是限制数据跨境流动的主要条件,在主权的背后又进一步涉及法学、政治学、国际政治等多领域的内容。在国际法治得到尊重并推崇的当下,对主权壁垒的研究与限定必然体现在法学领域,也必须能够得到法律技术的重视与回应。国家主权概念最早由法国政治思想家、法学家让·博丹提出,在《国家论六卷》中,让·博丹对国家主权的含义进行了界定,国家主权不受法律约束,以此来对公民进行统治,属于最高国家权利(乔治·萨拜因,2010),论述了国家主权不受外部政体和外部意志的任何干涉和约束。在让·博丹的基础上,荷兰思想家、国际法学家胡国·格劳秀斯从国际关系的角度出发,从对内和对外两个维度对国家主权的内涵进行论述。对内维度而言,国家主权是指国家对领土范围内的人、事、物所享有的最高的、绝对的、独立的管辖权;对外维度而言,国家主权意味着国家的对内管辖权是独立的、自主的和排他的,不受任何国家和政体的干涉(格劳秀斯,2015)。从格劳秀斯等人的原始主权理论可以看出,主权概念发端于近代民族国家兴起的背景之下,具有强烈的政治色彩,虽然主权自成立之初的主要目的并非国家法层面的合法性证成,但其希望通过引发主权这个法学概念,从而证成数字时代国家权力运作的合法性和独立性。正是由于主权这一关键要素的存在,作为特定国家合法代表的政府很难在国家对外事务上放弃主权管辖,即使是在国内宪法明确规定国际法优

越地位的荷兰也不例外,这一主权优越性的存在直接导致了下文所述的数据定位壁垒与数据出境壁垒的问题。

(二)数据主权的具体表现之一:数据本地化

数据定位壁垒是数字主权在数据领域的直接体现,指某些国家(地区)对于其管辖范围内的数据,规定这些数据必须存储在本国(地区)的境内,并在境内进行处理或备份,不允许跨境流动。这种数据定位壁垒在国际上被称为数据的本地化,通常是基于维护国家安全的角度,对数据的跨境流动进行绝对限制。例如,俄罗斯在美国棱镜门事件后,为了维护国家数据安全,采取了孤岛式的数据保护策略,通过出台和修订《俄罗斯联邦个人数据法》等一系列法律,规定产生于俄罗斯境内的数据只能在俄罗斯境内存储与处理,禁止向境外传输数据以及从境外访问境内数据(孙祁和尤利娅·哈里托诺娃,2022)。考察现有国际立法,当前各国家(地区)都制定了不同程度的数据本地化措施,设定了不同程度的数据主权壁垒,即使是倡导数据跨境自由流动的美国也基于维护国家安全利益的需要制定了数据本地化的规则(蔡翠红和郭威,2022)。综合分析现有国际法律规范,这种主权壁垒的具体规范形式有三种:第一,数据存储要求。通常要求企业在本国(地区)境内建立数据中心或存储设施,以存储其在该国(地区)的业务所产生的数据。第二,数据处理要求。通常要求企业在本国(地区)境内对其在该国(地区)的业务所产生的数据进行处理,而不允许跨境处理。第三,数据备份要求。通常要求企业在本国(地区)境内备份其在该国(地区)的业务所产生的数据,以确保数据的可靠性和安全性。可以看出,上述三点数据本地化规则的实施可能会对企业的跨境业务产生不利影响,如增加企业的成本和管理难度、限制企业的业务拓展和发展空间、增加数据泄露风险和安全风险等。

(三)数据主权的具体表现之二:数据跨境管制

数据跨境流动是一种国际现象,与国家安全、经济发展、公民生活等密切相关。除了本国国内的数据定位受到主权壁垒的管辖之外,特定数据的出境也会被采取限制和管制的措施,即数据出境壁垒,这也体现了数字主权对内与对外的双重效力。数据出境壁垒是指某些国家(地区)对跨境数据流动采取的出口限制和管制的措施。在互联网、物联网、大数据、云计算等新一代信息技术的支持下,数据已经成为生产要素之一。“数据是互联网时代的石油”,是数字经济发展的核心要素,也是中国数字经济发展的新动能。安全保障是国家安全、公共利益、经济利益、科技创新等重大利益的综合性保障,但也会对数据的跨国流动造成一定的约束和冲击,从而形成一道以“数据-主权”为核心的主权壁垒。在国际层面,数据作为数字经济时代的生产要素和财富源泉,已经成为国家间竞争与合作的重要内容。而在国内层面,数据已经成为中国经济发展的重要驱动因素,也是“数字中国”建设的重要基础。

数据主权障碍主要体现为数据主权理论和数据自由理论两个法律原则(吴沈括,2016)。数据主权理论认为,全球数据治理仍然需要建立在对国家主权的尊重之上;数据自由理论则主张,国家不得以国家主权为借口,对数据的自由流通加以

限制,也不应对数据及使用者采取跨国强制措施,干扰数据的自由流通。美国是最为典型的数据主权理论派,提倡自由的数据跨境流通和产业自我约束。美国没有专门的、统一的数据和跨境流动的法律法规,也没有像欧洲的数据保护监管机构那样统一的强制执行机制;相反,它更多地将数据和跨境移动的隐私问题交给了行业自律。同时,为了保障美国在数据跨境流通中的安全利益,维持其在数字化竞争中的主导地位,美国颁布了《云法案》即《澄清域外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act,简称 CLOUD Act),将数据管辖权从国内扩展到国外,也就是在美国公司的控制下,不管是在国内还是在国外,美国政府均有权对其进行监控和提取。而欧盟则不同,欧盟是最为典型的数据自由理论派。欧盟1995年通过的《数据保护指令》(Data Protection Directive),明确将个人数据纳入隐私保护的范畴,规定了充分的法律保障原则,并在此基础上提出了完善的法律保障^①。为了进一步加强对于数据信息的保护,促进数据信息的跨境传输,2018年至2022年欧盟相继颁布数字市场、非个人数据自由流动、数字服务等一系列法律法规,如2018年欧盟《通用数据保护条例》(General Data Protection Regulation)正式生效实施,对个人数据涉及的相关权利做出详细说明,并对其跨境流动作出更为严格的限制。2023年11月欧盟通过了《数据法案》,该法案于2024年1月11日正式生效,也是数据自由理论的重要实践。因此,从现有的国际法律法规来看,对数据出境壁垒的管理措施主要有如下内容:第一,对于涉及国家安全和公共利益等重大问题的数据,实行出口许可证制度,也就是通过批准,企业才可以合法地进行数据的跨境流通。第二,数据出口登记制度,建设管理系统对出口数据进行备案管理。有些国家(地区)规定,企业在进行数据跨境移动时,必须向有关部门提出报告,以保证数据的安全性及合法性^②。第三,数据出口管制制度。有些国家(地区)对涉及国家安全、公众利益等重大问题的数据实行出口控制。也就是说,对数据的输出实行严格的限制与控制,只能向某些国家(地区)输出,或者只能向某一类企业提供数据。第四,数据出口禁令制度。一些国家(地区)可能会对涉及本国利益的信息采取限制措施,也就是不允许公司进行此类数据的跨境流通。以上所列的限制与监管措施,对企业的跨国数据流动带来巨大的影响,包括提高企业的经营成本与法律风险,制约企业的国际化经营与竞争力,影响企业的技术创新与发展。

从国内角度出发,数据安全是重要保障,如果无法保障数据安全,那么数据的跨境流动就会存在较大的风险,影响到个人、社会以及国家安全。为了强化中国个人信息的安全保护,中国颁布实施了一系列的法律,从立法层面上不断完善相关的法律条例,体现为对个人信息和重要数据的保护。此外,《网络安全法》第25条还规定,任何个人和组织将个人信息出境的,应当事先取得个人信息主体的同意。由于数据跨境流动具有无国界性,而《网络安全法》又明确规定了国家在数据安全领

^①为了保护个人数据中的隐私利益,《数据保护指令》规定,禁止向欧盟外的第三国传输个人数据,除非这些国家对这些个人数据提供充分的保护。

^②《中华人民共和国网络安全法》(文中简称《网络安全法》)第37条;《中华人民共和国数据安全法》(文中简称《数据安全法》)第17条;《中华人民共和国个人信息保护法》(文中简称《个人信息保护法》)第36条。

域的义务,因此数据跨境流动中的“安全评估”就成为中国对数据出境实施监管的重要依据。然而,安全评估并不能解决中国对数据出境实施监管过程中的所有问题,其中也包括数据壁垒问题。《个人信息保护法》在立法上明确了中国个人信息出境的基本原则是“合法、正当、必要”,并以安全评估为重要的补充。《网络安全法》虽然在立法上明确了网络产品和服务提供者的数据安全保护义务,但同时规定了“重要数据”的概念。而《数据安全法》在此基础上,又规定对重要数据进行出境安全评估的要求。除此之外,中国还不断完善法律法规,对个人信息保护高度重视,并对国家秘密、商业秘密和个人隐私进行保护。在这种情况下,中国企业如何应对境外数据存储和处理能力不足的问题成为法律规制的难题。这一问题不仅需要国内法和国际条约等法律手段加以解决,还需要通过双边或多边合作的方式来解决。而且,这一问题与主权有关,需要从法律层面予以明确。因此,在中国立法、执法、司法等方面都对数据跨境流动做出限制的情况下,中国应如何从国家层面来解决这一难题?这涉及对数据跨境流动法律规制中主权障碍成因的分析。

二、非协调性数据主权立场对数据跨境流动的阻碍

当前,全球范围内围绕数据跨境流动的法律规制争议背后是不同国家在数据主权、数据安全和网络安全等问题上的不同立场,是不同国家所代表的不同阵营。这些立场与阵营,主要体现为各国在数据主权、网络安全立法上的分歧。数据跨境流动法律规制主权障碍的产生有多种原因,最重要的原因是目前的国际政治和经济格局已经呈现出明显的阵营化倾向,导致各国对数据这种新的生产要素的态度发生变化,进一步对各国的数据跨境流动立法层产生了一定的影响,从而造成了数据跨境流动的法律规制在执行层上的矛盾。从政治原因到价值原因,从立法到执法,数据跨境流动法律规制壁垒的形成具有其内在逻辑性。

(一) 国家间数据主权博弈影响立法宗旨目的

数据跨境流动的规制,原则上应当以市场规律和与数据相关的国际法、国际条约、各国立法为依据,即对数据跨境流动的规制主要体现在法律和经济两个层面上,但是现实情况并非如此。近年来,美国频繁以数据安全的名义限制或排除中国企业参与全球市场竞争,该行为的底层逻辑仍然是以巩固自身在全球政治、经济等领域内的领导地位为目的。冷战结束后,WTO等国际组织不断出现,西方国家主导并积极推动的全球化趋势明显。吊诡的是,西方国家一方面在积极推动全球化,另一方面又提出与全球化相悖的、全方位针对中国的政治策略。西方国家政策导向的形成有其背后的现实原因。

首先,着眼美国的数据跨境流动规制措施,美国之所以坚持以其国内法为基础,维护其国家利益,主要原因是美国基于自身在数据治理方面的经验和优势。例如,在数字经济领域,美国是世界上最大的数字市场,掌握着全球80%以上的移动电话用户和70%以上的互联网用户。对此,美国不仅通过国内法实现对数据跨境流动的规制,而且通过双边或多边协定在国际层面进行合作。但是,仅仅通过法律手段来限制数据的跨国流动,无法达成其企图阻止中国互联网企业成长的政治目

标。目前美国对数据的跨国流动通常采用“长臂管辖”的方式进行管制。例如,在中美贸易谈判中,美国要求中国承诺不能限制数据跨境流动等。另外,美国的“长臂管辖权”也暗含着排斥条款,在美国设有子公司的外国公司,均不能获取美国用户的信息,比如中国的华为和大疆(黄海瑛等,2021)。

相比之下,以中国为代表的发展中国家则更倾向于国内立法与国际规则相衔接。作为对美国“长臂管辖”的回应,早在2021年,关于数据安全保障的法律《数据安全法》就已经出台,其中明确了“中国任何组织和个人在没有得到中华人民共和国有关部门许可的情况下,不得将存储在中国的数据提供给境外的司法部门或者执行部门”。进而,中美两国的法律条款产生了直接矛盾,例如,中美企业在跨国经营的过程中,美国《云法案》要求企业向美国政府提供所有经营信息,但根据《数据安全法》要求,此类信息出口须经中国有关部门审批。

其次,尽管互联网企业是数据跨境流动的主要载体,但并不能简单地用市场经济制度来解释其遇到的全部问题。当然,自由市场经济体制能够更好地巩固处于市场支配地位国家的优势,这也是美国推动这一过程的一个重要动因。同时,尽管美国坚持尊重自由的市场经济规则,提倡数据在国际上的自由流通,但却对自己国家的数据流通进行十分严厉的约束。例如禁止TikTok向其母公司字节跳动发送数据,以及强制剥离TikTok和字节跳动的联系。所以,美国在面临域外数据输入的问题上,提倡数据的自由流通;而在数据输出方面,则以国家安全为借口,加以阻挠。在欧盟成员国和美国等都制定了保护本国数据跨境流动优先权的法律制度的前提下,有关数据在跨国流动过程中产生的纠纷,是无法由一国的法律来解决的(黄海瑛等,2021)。以欧盟与美国的数据跨境流动为例,美国的《云法案》要求,美国网络公司如果在欧盟成员国经营,获得了当地居民的个人信息,就必须向美国境内转移,但按照欧盟《通用数据保护条例》规定,该信息不能在欧盟之外进行流动。例如,该条例不仅要求欧盟成员国向欧盟委员会提供必要的信息,而且还要求欧盟委员会应在与成员国签订双边投资协定时与成员国共同遵守。这一法案不仅体现了欧盟对成员国数据主权保护和数据自由流动之间平衡的追求,而且体现了欧盟坚持维护和保障自身在数据跨境流动方面规则制定权的立场。从根本上说,在许多国家(地区)都采取了本国优先或区域优先的原则,在对数据的跨国流动进行法律规制的前提下,只有通过政治手段才能解决因数据跨境流动而引起的争端和问题。

(二) 国家间数据治理分歧影响数据跨境政策

在数字经济时代,各国对数据的控制能力存在差异,这是主权壁垒产生的现实基础。主权是国家权力的体现,国家权力意味着一国政府或法院能够执行其法律、管理其事务、管辖其公民,而这些权利由国家立法赋予。但是,数据不同于传统意义上的物,它既包括物质属性,又包括非物质属性。在“数据是数字经济的核心资源”这一论断下,数据的非物质性使其与传统的物不同。数据主权概念的产生和发展,也是数据跨国流动遭遇主权障碍的重要因素。在数字化时代,数据主权是国家安全 and 国家利益的重要组成部分,也是数字时代网络主权的延伸。然而,当前各

国(地区)对数据主权的认识各不相同,叠加后造成了对数据跨国流动的壁垒高涨。尤其是一些国家,更是借着行使数据主权的名义,侵犯其他国家的数据主权,加剧了世界各国对数据主权概念的不同看法,导致无法建立起统一有效的数据跨境流动的法律调控机制。

数字化时代,数据主权是国家主权在互联网上的重要体现。目前,不同国家之间的数据主权竞争日益加剧,究其根源,就是对数据的管理与控制(许可,2021)。这一问题关系到一个国家的经济发展,也关系到一个国家的安全。但不同国家对数据的管理与控制有不同的价值观。目前存在两种主流看法:一种认为对数据的管理与控制应该由国家来进行,只要拥有了对数据的管理权,就可以有效地防止其他国家侵犯自己的数据主权,具体体现在数据的本地化存储、处理等方面,采取法律、技术手段来实现对数据的所有权和管理权;另一种认为对数据的储存和处理与管理没有多大关系,只要对随意访问数据库这类侵犯数据主权的行为加以管制,就可以把它视为对数据的管控。然而,这种看法的弊端最好的例子就是美国的“长臂管辖”。在大力推动数据的自由流通,对其他国家数据进行任意访问,以实现对其数据的控制权的同时,对本国数据进行严格管控,禁止本国数据流出,实质上是一种数据霸权行为(叶开儒,2020)。因此,对此类数据霸权行为应从世界范围内作出相应的限制。对数据进行规制就需要对其进行分类、分级和标记。然而,由于各国数字经济发展阶段存在差异,不同国家对数据的分类、分级和标记也不相同。这种不同的分类标准带来了不同国家间在数据领域价值对立问题上的分歧。这种价值对立对跨境数据流动产生制约。因此,各国对数据主权原则的认识上不同的价值取向,造成了目前数据跨国流动法律规制面临的主权障碍。

(三) 国家间数据法律的域外管辖缺乏协调性

1. 国际规则的缺位

当前全球发展态势紧张,各国的立场不同,在经济发展层面产生了利益冲突甚至对抗。为了本国经济利益最大化,各国数据跨境流动规则的差异化程度变高;加上各国政治经济文化观念的不同,进一步加剧数据流通规则的不一致性。这意味着在数据跨境流动方面尚未形成统一的执行标准,在数字经济快速发展的背景下,存在明显的政治化特征,划分为不同的阵营。纵观世界范围内的数字经济发展大国及地区,数据跨境流通规则影响力以美国、欧盟和中国为主,以三者的数字经济跨境流通的不同立场为主要代表,影响着其他经济国家。当前世界主要数字经济体对数据跨境流动都持有不同的态度,并在此基础上形成了各自的规范体系。正因为如此,关于数据跨境流动的国际规则难以形成,前述如美国和其盟友之间达成的双边或多边协议虽然也有“国际”的蕴含,但是要达成如知识产权保护那样由世界主要国家都参与的国际规则难度较大,这就进一步加剧了数据跨境流动法律规制的主权壁垒。最具有代表性的三个经济体的数字经济跨境流通规则与经济发展水平紧密相关。在全球数字经济一体化的格局中,法律规则的构建离不开政策导向与经济水平的影响,因此分析各个国家(地区)的数字经济跨境流通规则需要有全球视野。

美国作为世界经济强国,在建立数字经济跨境流通监管规则方面,始终以市场为导向,以发展国际经济贸易、维护本国经济利益为主要目标,有着最发达的市场经济和最先进的数据处理能力。美国数字经济跨境流通规则设计的宗旨是“法无禁止即可为”,在宽松监管之下能够最大程度地发展美国在全球范围的跨境贸易。对外而言,美国为了保障自身的数字经济霸主地位,与其他国家频繁签订区域贸易协定,如《跨太平洋伙伴关系协定》(Trans-Pacific Partnership Agreement, TPP)和《美墨加协定》(United States-Mexico-Canada Agreement, USMCA)等多边协定的签署。从立法体系上分析,美国隐私立法较为分散,缺乏统一的数据保护框架,主要通过行业立法和州立法来设置相关规定。行业立法主要覆盖金融、保险、电视电信、消费者信用、儿童隐私等领域(桂畅旒等,2023)。

欧盟采取外严内松的数据跨境流动规则。一方面,欧盟对个人数据的安全保护重视程度较高,上升到个人尊严的高度,要求数据主体应该掌握数据的控制权和使用权(叶开儒,2020)。为了关注人权、强调个人隐私保护,欧盟颁布并实施《通用数据保护条例》(General Data Protection Regulation, GDPR)来强化对个人数据的安全保护,减少阻碍因素,保障数据的跨境流动,并制定了一些规则,要求在数据跨境流动的时候,严格按照法律规则来执行。与1995年发布的《数据保护指令》相比,欧盟《通用数据保护条例》体现一种强化数据主体权利的进路(丁晓东,2018)。另一方面,欧盟对外采取严格的数据跨境流通监管规则,严格限制数据在欧洲以外的地区流动,加强数据共享,致力于打造欧洲共同数据空间。欧盟以充分性调查结果评估第三国个人数据保护水平,只有达到“充分”标准,才能实现个人数据的安全传输,严格控制个人信息传输的渠道,积极采取保障措施来保护数据安全(邹军,2019)。可以说,充分性决定制度可能基于维护数据主权的考量。欧盟是全球主要数字经济市场之一,是全球数字贸易的主要参与者,但是受制于美国发达的数字经济,目前采取保守的数据跨境流通的举措对保护本地区的互联网产业和跨国企业利益更加有利。

在数据成为重要资源的全球经济大背景下,中国同样注意数据主权和数据安全的保护。中国积极探索高效、安全的跨境数据流通的监管体系。2016年颁布的《网络安全法》聚焦网络安全领域,为跨境数据流通的监管体系建设打下基础。2021年出台的《数据安全法》和《个人信息保护法》共同构成中国数据跨境流通规则的监管体系。数据出境安全审查要求数据跨境传输前需要经过相关审查和批准,确保跨境传输的数据不会危害国家安全和公共利益。还要对内容进行评估,评估是否有跨境传输的价值,是否得到信息所有者的认可和支持,尤其是传输重要数据时,需要从多方面进行考虑,判断可能存在的各种风险,并采取有效措施来降低数据传输的风险(时业伟,2020)。这一措施可以有效防止敏感数据流失、被滥用或窃取,同时有利于促进数据的合法合规流通,保障数据主体的权益和隐私。总体来说,中国的数据跨境流通规制框架旨在平衡数据的自由流动与国家安全、公共利益的保护之间的关系,确保数据的合法、安全、有序流通,促进数字经济的健康发展(卢浩,2024)。

2. 内国法之间冲突

在跨境数据流动规则的设置中,不同国家出于本国利益考量,规定往往最有利于本国的利益,导致数据管理者和数据传输方面面临不同国家法律的制约和限制。具体而言,造成全球数据跨境流动壁垒不断加剧的原因主要有:第一,法律适用范围不同。不同国家(地区)的数据保护法律规定不同,对于个人隐私、数据安全等方面的规定不同。因此,国家和企业等数据跨境流动行为主体在全球范围内进行数据跨境流动前,需要考虑数据的存储和传输是否符合各国的法律要求。第二,国家主权观念差异化。出于不同的主权观念,各国倾向于在保护本国数据利益方面保持高度的自治和管辖权。随着网络安全和数据泄露的风险日益增加,不同国家对于数据跨境流动会选择不同的限制措施,比如欧盟以保护个人权益为目标,美国以促进经济发展为宗旨。对于关注数据安全和国家安全的国家(地区)中,采取措施限制跨境数据流动,例如加强数据本地化要求、实施审查和监管机制。总体而言,诸多因素加剧了数据跨境流动的壁垒,阻碍了各国建立全球数据流动的统一标准和机制的进程。

跨境数据流动现象在当前非常普遍,与跨国贸易活动的开展有直接关系,有明显的全球性特征(张莱楠,2020)。而目前全球范围内存在不同法律体系和立法传统,例如大陆法系国家和普通法系国家在法律规定和争议解决方面存在很大差异,导致在处理数据跨境流动问题上的不同,依据的法律也不同。同时,数据跨境流通所涉及的管辖权问题也存在争议,如数据存储地、数据所有者、处理者的国籍和企业所在地等因素都可能影响不同国家对数据流动的管辖权主张。WTO 凭借与多国签订的贸易协定,作为解决跨国贸易争端的重要法律依据,以此来维护跨国贸易活动的稳定有序发展,对商品进行严格监督,对于服务贸易、知识产权贸易的发展的推动作用较大。尽管 WTO 与全球数字经济密不可分,但是无法完全适应当下国际经济新局势,尚且面临单边主义和逆全球化的挑战。所以,Burri(2017)认为,WTO 制定的贸易原则本质没有改变,依旧没有脱离互联网发展环境。美国的双边贸易协议均是为了巩固其商业地位和国际经济优势,影响着其他国家多(双)边的协定,进一步加强了美国的经济霸权。面对数据跨境流动存在的问题,国际社会尚且缺乏受到普遍承认的国际条约和协定,也没有提供关于数据跨境流动法律适用和管辖权争议的统一指南。这种情况给企业和个人在进行数据跨境流动时造成法律的不确定性和风险。因此,国际社会需要加强协作,发挥跨境数据流动“全球属性”,以便更好地应对数据跨境流动所带来的法律挑战。

三、数据跨境流动的中国因应:安全与自由相平衡的立场

为了促进数据的跨境流动,不同国家持有不同的态度,采取不同的措施来保障数据跨国流动的安全,核心问题是怎样达成统一的标准。数据流动和使用,有助于实现价值的增值,通过动态博弈,对流出的数据进行严格管控,不仅能够挖掘数据背后存在的经济价值,而且对于维护国家安全有着重要意义。对于中国而言,在跨国贸易活动中,势必会涉及跨国数据的流动,想要保障数据跨国流动的安全性,关

键在于需要明确平衡点,采取有效措施,强化数据管理,掌握数据的使用主权,确保核心利益不受侵害(文铭和李星熠,2024)。从宏观层面来理解数据的主权,实际上就要以保障国家安全为根本原则,在当前背景下,构建全新的安全保障格局,来提高数据使用的安全性。国家安全保障有着重要意义,建立在国家主权的基础上,数据主权可能会带来非传统安全风险,而维护国家安全的本质并没有发生改变,逐渐引起各国的重视。各国采取一系列的措施,来掌握数据主权,避免核心权益受损,保障国家安全。在当前背景下,数据是一种重要的禀赋资源,在国际竞争中起到越来越重要的作用,需要对数据安全引起高度重视,来增强国家核心竞争力。《网络安全法》的颁布实施有着重大意义,不仅能够维护网络数据安全,而且在维护国家安全上也起到不可替代的重要作用。中国对网络空间治理的相关研究处于初步探索阶段,尚未形成一套成熟的理论体系,还需要从不同维度进行深入研究,兼顾各方利益,掌握数据主权,积极参与到数据跨境流动中,逐渐形成统一的执行规范,确立统筹协调数据安全与数据自由原则。

(一)确立数据跨境流动的基本原则

数据跨境流动主权壁垒问题的破解,核心在于统筹协调数据安全与数据自由原则。一方面,从国际不平衡的角度出发,仅强调自由的网络领域将导致对发达国家的偏好,而不公平的竞争环境可能剥夺新兴国家的发展权利。另一方面,重视数据主权正是对潜在不公平格局扩大的抑制。因此统筹协调数据安全与数据自由原则的关系尤为重要,以从技术角度构建相关原则为支撑点,需要从以下三个方面加以设计。

首先,有限自由原则。数据流动自由是跨境贸易自由化和便利化的前提,为数据的自由流动创造有利条件,提高数据资源的利用效率,从而实现价值目标(薛亦飒,2020)。但在实际操作中,这一自由原则可能被技术占优国家所滥用,故此数据的自由流通,必须受到适当限制,不能仅以数据安全为由,直接否认“数据自由”,阻止各国间的信息流通,而是要依托大数据分析技术,促进各国民间网络数据的交换与交流,做到非敏感数据的共享。以构建人类命运共同体为指南,不仅在经济领域达成数据合作,对涉及环境、气候等方面议题的数据,也要保持各国间的及时分享,共同应对相关问题。基于上述有限自由原则,既能够保障国际数据的正常流动,又可以有效规避当中的错误信息。

其次,数据平等原则。实现数据自由流通与共享,就必须将任何阻碍数据自由流动、阻止市场主体平等获取数据的障碍全部破除(叶宣含,2020)。平等是自由的保障和前提,没有平等的自由,就只是拥有丰厚资源的少部分人的自由,因此确立数据平等原则是破解数据跨境流动法律规制主权壁垒的关键元素,它具有两层要义,这两层要义同时联结了数据自由和数据安全,成为调解两者冲突的中间桥梁。其一,在非敏感数据的获取和使用方面,各国均享有平等的权利,对一般性内容的数据,特别是关乎人类共同议题的数据,如环境数据等,所有国家都不得随意以主权问题的名义拒绝分享;其二,由于网络技术往往涉及尖端的科技,如人工智能和元宇宙等(皆以数据为基础),并非所有国家都能自如掌握和运用,这就造成了不同国家间的技术鸿沟。技术发达国家常常依靠着技术优势,搜集其他发展中国家和

落后国家的相关数据,乃至敏感信息,而处于技术劣势的国家则显得无能为力,因此必须强调数据平等的重要性,所有数据的开放必须是对等的,处于技术劣势的国家必须以此原则为基础,合理地建设有关数据出入境制度,防止技术发达国家的数据侵害。

最后,跨境审查原则。数据平等原则融合了数据自由与数据安全原则,后发国家必须构建相应的制度原则,以抵御他国的技术侵犯,跨境审查原则便是保障数据安全的根本原则。如果说有限自由原则关注的是外来数据本地化的问题,那么跨境审查原则主要针对的则是本地数据对外传播的审核。规范个人数据的使用行为,避免数据滥用行为的扩散,降低信息使用的风险,不断完善数据管理体系,完善基础设施,国家应该始终掌握数据流动的主动权(许可,2021)。

综上所述,数据自由原则推崇数字经济和数字贸易的开放与高效,而数据安全原则更关注主权国家的安全与发展。二者形成了原则层面的冲突,但这并不意味着不可以分别吸收两种原则的合理成分,将之重新改造成一种合理、开放、动态地结合数据安全与数据自由原则的调和论原则。据此,下文将提出一整套针对数据跨境流动法律规制的不同主权壁垒形式的法律技术的化解方案。

(二)完善数据跨境流动的制度框架

针对制度层面的数据跨境流动主权壁垒,数据安全与数据自由原则的协调和落实应当是动态调整而非固定不变的。作为当今的数据大国,中国应不断探索和调整更加合理、开放的数据风险防范方案,在设计静态的数据跨境流动法律规则体系时,避免“一刀切”,应积极、主动地增强与国际规则体系的适配性和兼容性,特别是在数据流动的关键法律概念方面与国际数据规则保持一定的契合性。

首先,探索统一的全球数据跨境流通体系。国家在国际层面的经济发展水平影响着数据跨境流通治理的方向。总体而言,美国等数字经济发展态势迅猛的国家倾向于采取开放的数据跨境流通规则,但是会以数字霸权制裁和打压其他经济发展国家;欧盟等地区的数字经济发展相较于美国缓慢,倾向于采取保守的数据跨境流通举措。因此不同的立场与利益角度,加剧了全球范围内数据跨境流通的壁垒。在数据的跨境流动和全球一体化的背景下,数字经济发展存在无限可能,因此更要加强不同国家(地区)之间的经济交流,共同构建统一的全球数据跨境流动体系,消除数字经济跨境流动壁垒。各国应当求同存异,积极推动国际规则的构建。可喜的是,相关国家政府与国际组织正在积极作为,如2019年二十国集团贸易部长会议在日本召开,与同期召开的数字经济部长会议举行了联席会议,重申可信数据自由流动框架的构建,强调跨境数据流动对促进生产率、创新和可持续发展的重要性,试图从消费者和企业对隐私保护与安全信任和不同法律框架之间的融合两方面进行规则构建(李墨丝,2021)。中国作为数据大国,更应当瞄准前瞻议题,推动数据跨境流动规则的标准化和科学化。当然,为了防止因各经济体数字治理水平的差异化而带来的数据跨境流动壁垒,需要有某些特殊或者例外情形的规定。例如,在设定相关合同义务、保护数据主体利益、维护公共利益等情形之中,应当有条件地允许不同保护水平条件下的数据跨境流动。

其次,统筹发展与安全,构建动态平衡的数据跨境流动规则体系。中国在加快数字化发展的过程中,需要注重“加强数据安全评估,推动数据跨境安全有序流动”(国家发展和改革委员会,2021)。立足世界百年未有之大变局和实现中华民族伟大复兴战略全局,统筹好发展与安全,是坚持总体国家安全观、构建良好数字生态的必然要求。一方面,需要保障数据流动过程中的完整性、有效性,确保能够挖掘其存在的价值,为信息跨境流动创造有利条件。国家互联网信息办公室于2022年发布实施的《数据出境安全评估申报指南(第一版)》指出,评估时重点考虑数据发送方和接收方的数据安全保障能力、技术实力和保护措施有效性。安全是发展的前提,发展是安全的保障(中国网络空间研究院,2017)。数据信息关乎国家安全、社会利益以及个人隐私保护等重要事项,需要谨慎对待。在推动数据跨境流动的过程中,不能损害国家、社会 and 个人的利益,否则便背离了技术发展的初衷。另一方面,对于安全流动和自由流动原则的发展,应保持均衡,两者兼顾。一是积极制定一系列法律法规和政策来规范数据跨境流动,进一步细化《网络安全法》《个人信息安全规范》等,强化个人数据和敏感数据的合法处理和传输责任,强调企业的责任和义务,确保数据在跨境流动过程中得到有效保护。二是着眼于构建开放共享的数据交流环境,促进经济的发展和 innovation。在全球经济一体化的过程中,中国积极推动“数字丝绸之路”倡议,致力于推进互联互通、数据共享等领域的国际合作。中国政府继续倡导建立开放的数据交换机制,通过与其他国家(地区)的合作,促进数据跨境流动,推动技术的进步和合作的发展。

(三)细化中国数据保护专门性法律

从立法维度上分析,需要以国家安全观为指导,从保障信息使用安全和维护网络环境安全两个维度来执行,强化数据的管控,提高数据使用的全面性和完整性,避免数据的滥用问题,提高数据流动的安全性。从具体的产业发展维度上展开分析,中国在跨境数据流通上扮演着重要的角色,想要提高中国在国际社会上的话语权,就需要重视国家安全保障,坚持执行对外防御型治理方案,强化对跨境数据的管制。当前,西方国家采取了一系列的措施制裁中国,试图阻碍中国的发展,中国面临着较为严峻的外部环境,只有牢牢掌握跨境数据的主动权,才能在激烈的竞争中获取优势,充分发挥数据禀赋资源的优势,增强国家的综合竞争实力。除此之外,还需要对数据跨境流动的保护边界进行明确,支撑跨境贸易活动的持续稳定发展(文铭和李星熠,2017)。

首先,基于跨境数据的双重属性,整合现有法律法规,出台一部综合性的数据跨境流动保护法。近年来,随着大数据与人工智能的深入发展,中国在数字治理方面加强了立法力度。以2017年正式施行的《网络安全法》为基础,结合2021年施行的《个人信息保护法》和《数据安全法》,以及2022年施行的《数据出境安全评估办法》,共同形成了中国数据跨境流动的法律法规,建立了较为健全的跨境数据法规体系,为数字经济的发展提供了规则支撑。但是与此同时,在数字经济发展的浪潮之中,分散的、较低层级的管理办法,很难有效解决数据跨境流动的相关问题。因此有必要考虑在现有法律法规的基础之上,通过整合创新,以专门法律的形式,出

台数据跨境流动保护法,此举不仅可以提高数据跨境流动保护的层次,同时也可以增强针对性,提升应对数据风险的能力,有效解决数据跨境流动的基本问题(徐明等,2024)。

其次,在内容上,针对不同的数据采取不同的管理模式。在当前阶段,跨境流动的数据类型复杂,立法技术的实施需要建立在分类原则的基础上,根据数据的重要性程度,来设置相契合的权衡规制,进一步构建个人数据和国家数据的分类治理规则,并根据数据的不同特点和用途对个人数据与国家数据设置不同的治理模式。在现代国际社会,数据的分类分级保护已经成为各国共同的立法选择。以美国为例,一方面,对于非重要数据,依据数据自由流动原则,通过双边或者多边的国际协议,如美国与欧盟之间的《数据隐私盾协议》(后被欧盟法院认定无效)等,以此来带动数据跨境流动。另一方面,对于重要数据或者关键领域的数据跨境流动,则设置严格的管控要求。美国于2022年实施的《外国投资风险审查现代化法案》(FIRRMA),明示了国家安全审查在数据跨境流动层面的规则,将关涉敏感个人数据的交易行为纳入了国家安全审查的范围(国家发展和改革委员会,2022)。因此,在中国的立法过程中,遵循这一国际惯例,并努力推动国际社会共同打造均衡协调的数据分类分级保护规则,成为一种可行且必要的选择。中国《网络安全法》中明确提到,实施网络安全等级保护制度,划分数据的重要性等级,再按照对应等级的方式来强化风险管理,提高数据跨境流动的安全性。中国《数据安全法》第21条也对数据分类分级作出专门规定,且强调数据安全会直接影响到国家安全以及在国际社会上的话语权,中国要始终掌握数据跨境流动的主动权,强化对核心数据的保护,维护国家安全。这为中国数据分类分级管理提供了最为基本的法律支撑。

数据的跨境流动和分类分级保护规则,是统筹协调数据安全与数据自由原则的重要诉求。在当今国际社会中,数据安全和数据保护对于国家间竞争具有重要意义。面对欧美国家扩张式的数据权力,中国要获得数据跨境流动的话语权,就必须具有完备的法律规则体系,以应对外来的风险与挑战,而数据分类分级保护正是中国维护和发展数据主权的重要体现。此种数据分类分级,不仅是根据国家内部的具体情况而设置,在面向国际社会之时,更要根据不同的政治外交关系、国际法律协定等方面的具体情形,而设置出不同的重要数据目录(洪延青,2021),从而服务于中国的国家数据发展战略。

(四)建构数据跨境纠纷的应对机制

针对纠纷解决层面的数据跨境流动主权壁垒,当前的主流国际数据跨境流动规则体系未能提供有约束力的争议解决机制。对此,具体的应对措施可包括如下两个层面。

首先,应当通过国际协调和谈判尝试建立健全国际层面中立的、具有公信力与执行力的纠纷解决机制。在现代国际交往中,数据跨境流动越来越成为一种常态化现象,而随之产生的便是相关纠纷的解决问题。多年来,由于各国在数据保护立法层面的不同,在解决数据跨境纠纷问题上存在着诸多冲突与矛盾,为数据自由流动带来了巨大的困难,阻碍了数字经济的发展。因此,探索建立用于解决跨境数据流

动争议的国际机制,成为推动数据安全和数据自由均衡发展的迫切需要。随着数字化时代的到来,数据跨境流通带来了诸多复杂的法律问题,例如数据隐私保护、信息安全、知识产权等,而面对跨境数据存储、处理和传输过程所引发的纠纷,当前数据跨境流通的争议解决尚缺乏良好的纠纷解决机制。从传统贸易角度来看,可以借助WTO来解决贸易过程中的纠纷,通过制定相关的法律,来约束参与国际贸易活动各个主体的行为(易继明,2020)。但是,关于数据跨境流动的纠纷案件,尚未确定明确的上诉机制,各方就数据跨境流通的关键问题难以达成共识(郑淑凤,2022)。目前各国在跨境数据纠纷管辖权方面存在着不同的法律和规定,导致在纠纷解决过程中出现混乱和冲突。建立第三方机制可以推动各国在数据纠纷管辖权方面进行协商,能够为各国企业和个人提供一个公正、独立的纠纷解决机制,减少国与国之间的纠纷,促进跨境数据流通。

其次,提前阻断“数据自由”名义下的“长臂管辖”,尤其是部分国家在数据跨境流动纠纷中的“长臂”执法。随着数字时代的来临,数据的跨境流动突破了传统的国家疆界。依托于云计算、区块链、大数据与人工智能等新兴科技,跨境的网络或者数据供应商获取海量数据,部分国家尤其是发达国家,为了避开复杂的法律协助程序,利用其境内的各类数据总部,以“长臂”执法的方式调取存储于境外的关键数据(梁坤,2022),在一定程度上侵犯了他国的数据安全和法律主权。作为数据大国,中国在数据跨境流动问题上一直坚持国家主权至上原则,主张地理存储模式,在物理空间中承载虚拟空间,根据地域原则明确管辖范围。例如,中国法律体系中要求,数据跨境流动必须严格按照法律规定的流程来执行,如果没有得到批准,擅自向国外个人或者组织提供境内数据,属于违法行为。这些规定在国家法律层面否定了外国司法或者执法机构的“长臂管辖”,维护了国家主权和数据安全。当然,否认“长臂管辖”并不是否认合法的数据跨境流动,依据中国缔结或者参加的国际条约、协定,以及《数据安全法》第36条规定的数据跨境流动中的平等互惠原则,主管部门对于提交的数据跨境申请,根据法律规定要求,来落实审核工作。同时,中国《数据安全法》也设置了部分反制或者惩罚措施,没有经过相关负责部门的审核同意,擅自向境外个人或者组织提供境内数据,属于违法行为,要承担相应的法律责任,比如,罚款、警告、停业整顿等。相关法律后果的设置,在一定程度上体现出中国法律对他国“长臂管辖”效力的否定,有效保障了中国境内相关法律主体的合法权益。

四、结论与启示

在数字经济快速发展的背景下,数据资源已经成为各国参与国际竞争的重要禀赋资源。与其他生产要素一样,数据的跨境流动已成常态,但随之而来的以国家安全为代表的风险事件不容忽视。国家主权因素在数据跨境流动场景中扮演着边界控制的角色,国家利益直接影响着一国对待数据流动的基本价值立场和政策选择。由此,数据主权理念应运而生,成为管控数据跨境流动的基本原则。而在全球视野之下,不同国家之间的数据主权博弈导致了数据治理之分殊,进而形成了国家间数据

法律域外管辖效力的矛盾与冲突。中国在对待数据跨境流动时应当遵循安全与自由相平衡的基本理念,在法律技术上完善数据跨境流动的基本规则,有必要细化中国专门性的数据保护法,以此容纳相应的规范内容;在此基础上,还需要重视数据跨境纠纷应对机制的构建。

[参考文献]

- [1] 蔡翠红,郭威.中美跨境数据流动政策比较分析[J].太平洋学报,2022(3):28-40.
- [2] 丁晓东.什么是数据权利——从欧洲《一般数据保护条例》看数据隐私的保护[J].华东政法大学学报,2018(4):39-53.
- [3] 格劳秀斯.战争与和平法(第1卷)[M].马呈元,译.北京:中国政法大学出版社,2015:36-44.
- [4] 桂畅旻,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.
- [5] 国家发展和改革委员会.中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要[S].北京:人民出版社,2021:52.
- [6] 国家发展和改革委员会.《“十四五”数字经济发展规划》学习问答[M].北京:人民出版社,2022:5.
- [7] 洪延青.国家安全视野中的数据分类分级保护[J].中国法律评论,2021(5):71-78.
- [8] 黄海璜,何梦婷,冉从敬.数据主权安全风险的国际治理体系与中国路径研究[J].图书与情报,2021(4):15-28.
- [9] 李墨丝.欧美日跨境数据流动规则的博弈与合作[J].国际贸易,2021(2):82-88.
- [10] 卢浩.数字产品知识产权存续规则的理论基础、技术挑战与优化路线[J].法理-法哲学方法论与人工智能,2024,10(1):167-194.
- [11] 梁坤.长臂执法背景下的数据出境管制[J].国家检察官学院学报,2022(5):41-57.
- [12] 乔治·萨拜因.政治学说史(下卷)[M].邓正来,译.上海:上海人民出版社,2010:82.
- [13] 时业伟.跨境数据流动中的国际贸易规则:规制、兼容与发展[J].比较法研究,2020(4):173-184.
- [14] 孙祁,尤利娅·哈里托诺娃.数据主权背景下俄罗斯数据跨境流动的立法特点及趋势[J].俄罗斯研究,2022(2):89-107.
- [15] 文铭,李星熠.“自由-规制”框架下跨境数据流动治理及中国方案[J].中国科技论坛,2024(4):106-11.
- [16] 吴沈括.数据跨境流动与数据主权研究[J].新疆师范大学学报(哲学社会科学版),2016,37(5):112-119.
- [17] 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.
- [18] 徐明月,安小米.数智治理概念、体系构建、要素、特征及关系[J].中国科技词语,2024,26(3):47-56.
- [19] 薛亦飒.多层次数据出境体系构建与数据流动自由的实现——以实质性审查制变革为起点[J].西北民族大学学报(哲学社会科学版),2020(6):64-74.
- [20] 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[J].法学评,2020,38(1):106-117.
- [21] 叶宣含.数据自由和算法保护[J].理论月刊,2020(7):110-124.
- [22] 易继明.后疫情时代“再全球化”进程中的知识产权博弈[J].环球法律评论,2020(5):163-177.
- [23] 张茉楠.跨境数据流动:全球态势与中国对策[J].开放导报,2020(2):44-50.
- [24] 郑淑凤.数字经济视角下数据跨境规则的困境与回应[J].国际贸易,2022(5):63-71.

- [25] 中国网络空间研究院. 中国互联网20年发展报告[R]. 北京: 人民出版社, 2017: 122.
- [26] 邹军. 基于欧盟《通用数据保护条例》的个人数据跨境流动规制机制研究[J]. 新闻大学, 2019(12): 16-27+119.
- [27] BURRI M. The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation[J]. UC Davis Law Review, 2017(51): 65.

Cross-border Data Flows from the Perspective of Data Sovereignty and China's Response

YAO Tian¹, WANG Yu²

(1. School of Law, Shandong Jianzhu University, Jinan, Shandong, 250101

2. School of Law, Qinghai Nationalities University, Xining, Qinghai, 810007)

Abstract: Based on the strategy of data as a new production factor, the sovereignty factor has become a key limitation in the cross-border data flow scenario, which is manifested in the barriers of data location and data exit. Different countries have different positions on data sovereignty, in which the game of data sovereignty affects the legislative purpose of a country's legal system for cross-border data flow, and the uncoordinated rules on cross-border data flow between countries and the lack of international rules in this field greatly impede the orderly flow of data across borders. China's treatment of cross-border data flow upholds the basic concept of balancing security and freedom, on the basis of which the institutional framework of cross-border data flow should be improved, the special data protection law should be refined at the right time in the legislation, and emphasis should be placed on the construction of the response mechanism for cross-border data flow disputes.

Keywords: Cross-border Data Flows; National Security; Data Sovereignty; Data Security

(责任编辑 祝子白 武 齐)