

俄罗斯出台的与贸易相关的数据流动限制性措施研究——兼谈对中国的启示

周念利 李金东

(对外经济贸易大学中国 WTO 研究院, 北京 100020)

摘要: 在数据流动问题上, 出于维护本国网络空间安全的考虑, 俄罗斯制定了世界上最为严密的数据流动限制性政策。在对俄罗斯出台的与贸易相关的数据流动限制措施类别和相关立法进行梳理的基础上, 对其形成原因进行了分析。俄罗斯的数据流动限制措施具有 3 个典型特征: 一是数据输出规则针对“白名单”和“黑名单”对象做出鲜明区分; 二是设置严密的互联网准入和监管措施; 三是实施严格甚至激进的数据本地化政策。最后根据俄罗斯的相关实践给出了对中国实施数据流动管理的相关政策建议: 推进跨境数据流动限制分类管理, 减少不必要的数据流动限制; 保持网络空间自主可控, 非敏感领域适当放宽互联网准入和监管机制; 充分发挥中国互联网产业优势, 降低数据本地化带来的额外成本。

关键词: 数字贸易; 数据流动; 数据本地化

中图分类号: F742

文献标识码: A

文章编号: 1006-1894 (2020) 03-0085-12

一、引言

近年来, 云计算、物联网及大数据等新兴信息通讯技术的大范围普及与应用促使全球数字贸易规模加速增长。数字贸易发展需建立在数据跨境流动基础之上, 但世界主要经济体针对跨境数据流动的态度差异较大。美国是数据跨境自由流动的倡导者和相关数字贸易规则构建的积极引领者。在 WTO 框架下与贸易相关的电子商务诸边谈判中, 美国希望能将《美墨加协定》(USMCA) 中的数据跨境流动规则在全球扩展适用。欧盟对实现数据跨境自由流动态度犹疑, 希望能在跨境隐私保护和数据流动之间保持平衡。俄罗斯的态度则较为保守, 在数据流动方面出台了很多限制性规定。

作者简介: 周念利, 对外经济贸易大学中国 WTO 研究院研究员, 博士生导师, 研究方向: 数字贸易; 李金东, 对外经济贸易大学中国 WTO 研究院国民经济学硕士研究生, 研究方向: 数字贸易。

基金项目: 2019 年国家社科基金重点项目“数字贸易规则‘美式模板’的演化升级与扩展适用趋向及中国的应对”(项目编号: 19AGJ012); 国家自然科学基金委 2019 年第 1 期应急管理项目“基于维护世界线上市场统一的贸易相关电子商务谈判研究”(项目编号: 71941012); 对外经济贸易大学中央高校基本科研业务费专项资金资助“美式数字贸易规则的发展演进及中国的政策选择”(项目编号: ZD3-07); 对外经济贸易大学中央高校基本科研业务费专项资金“全球数字贸易治理体系发展趋向及其贸易影响研究”(项目编号: CXTD9-06)。

ECIPE^①最新发表的 DTRI^②报告中显示,俄罗斯在“数据限制”指标中的“数据政策”分指标中排名最高。中国是发展中国家,在网络安全、数据流动、互联网治理上一直将“安全可控”设定为重要目标,这使得中美双方在数字贸易治理的很多议题上分歧较多。本文对俄罗斯出台的与贸易相关的数据流动限制性措施展开梳理和分析,对于中国完善数据流动管理制度乃至理性参与全球数字贸易治理都具有重要的参考价值。

关于数据流动限制的既有研究多注重对相关限制措施的内容、特征及发展趋向进行描述和分析。考虑到各国经济基础不同或经济基础相似而发展阶段不同,各国发展数字贸易的意愿存在差别,所实施的数字贸易限制性措施也存在差别,所以这类研究偏好聚焦于对某一代表性国家所实施的代表性的数据流动限制措施展开分析。Holleyman (2015) 认为美国是推动数字贸易自由化最积极的国家,但其他国家对参与数据或数据服务相关贸易态度谨慎,中国、俄罗斯、印度、印度尼西亚和越南被美国认为是数字贸易限制最严格的国家。Ferracane (2018) 和 Castro (2015) 致力于对中国和俄罗斯在数据流动、公共采购、外国投资、内容访问和标准等方面实施的相关限制展开研究。何波 (2016) 从俄罗斯跨境数据流动立法规则和执法实践出发,分析了俄罗斯推行数据本地化的实施效果以及深层次原因。Fefer (2018) 认为俄罗斯限制数据流动的相关法规或政策为寻求使用云服务的公司和国家设置了障碍。

目前相关文献主要基于如下两个路径持续深化和细化。一是尝试对数据流动限制性措施的严格程度展开定量测度。数据流动限制措施种类繁多,适用范围广且零散,要用国际统一标准对其进行定量测度并非易事。ECIPE 对 64 个国家包括数据流动限制措施在内的数字贸易壁垒水平进行了评估并打分,分数越高表明限制越多,由此带来的贸易成本也越高 (Ferracane et al, 2018)。二是针对数据流动限制性措施的经济效应展开研究。以数据本地化措施为例,有研究发现一些国家实施数据本地化政策会给该国的 GDP 带来损失,数据本地化措施会造成巴西 GDP 下降 0.2%、中国下降 1.1%、欧盟下降 0.4%、印度下降 0.1%、印度尼西亚下降 0.5%、韩国下降 0.4% 和越南下降 1.7% (ECIPE, 2014)。同时,禁止数据跨境流动会增加贸易成本,不利于吸引外资,导致本国的中小企业成本上升,尤其对云计算等互联网技术依赖度更高的企业影响更大 (国际商会, 2018)。

以上分析表明既有研究对数据流动限制性措施的内容、特征及其经济效应进行了描述和分析。俄罗斯在数据流动问题上素以保守著称,对俄罗斯与贸易相关的数据流动限制性措施的类型、限制水平、法律来源以及典型特征进行全面梳理和分析的文献还不多见。有鉴于此,本文尝试从俄罗斯目前的数据立法状况出发,对俄罗

① 欧洲国际政治经济中心, European Centre for International Political Economy, 简称: ECIPE。

② 数字贸易限制性指数, Digital Trade Restrictiveness Index, 简称: DTRI。

斯与贸易相关的限制性措施具体内容进行分类,并侧重于对俄罗斯出台这些措施的原因及实施效果进行分析和评价,最后对中国的数据流动管理提出可行的政策建议。

二、俄罗斯出台的数据流动限制性措施主要内容及成因分析

(一) 俄罗斯实施的数据流动限制性措施的主要类型

根据 ECIPE 的定义,俄罗斯有关数据流动限制性措施可依据其实施范围分为两类(表 1):一是跨境限制性措施,二是境内限制性措施。

跨境限制性措施包含 3 类:第一类为“禁止跨境传输数据和数据当地处理要求”,是针对跨境数据流动所实施的最严格措施,在禁止传输数据或数据本地处理要求的情况下,如果这些国内服务提供商的效率低于外国提供商,公司需要在实施管辖区内建立数据中心或转向本地服务提供商,从而增加成本;第二类为“有条件的数据跨境流动政策”,除非满足某些条件,将数据转移到国外是被禁止的,如果条件严格,该措施很容易导致禁止转移数据;第三类为“数据存储本地化要求”,这些措施要求跨国公司在国内保留某些数据的副本,本地存储要求通常适用于特定数据,如会计或簿记数据,只要数据副本仍在国家领土内,公司就可以照常运作。

境内限制性措施主要包含 5 类:第一类为“与数据保留相关的措施”,主要是指规定公司应如何以及在多长时间内将某些数据保留在其处所内以便监管机构调查的措施;第二类为“数据隐私的主体权利”,主要指是否同意收集和使用数据以及删除数据的权利;第三类为“数据隐私的管理要求”,包括数据隐私影响评估、指定数据保护人员的要求、要求在数据泄露的情况下通知数据保护机构以及要求允许政府访问所收集的个人信息;第四类为“对违规行为的制裁”,包含因违反数据隐私规则而受到的罚款和刑事制裁两个方面;第五类为“与数据政策相关的其他限制性措施”。

表 1 俄罗斯所实施的数据流动限制性措施种类

措施类型	具体措施
跨境限制性措施	禁止传输数据或数据当地处理要求
	有条件的数据跨境流动政策
	数据存储本地化要求
境内限制性措施	与数据保留相关的措施
	数据隐私的主体权利
	数据隐私的管理要求
	对违规行为的制裁
	与数据政策相关的其他限制性措施

资料来源: Ferracane, M. F., Lee-Makiyama, H., Van Der Marel, E. Digital Trade Restrictiveness Index[J]. European Center for International Political Economy, Brussels: ECIPE, 2018.

ECIPE 的 DTRI 报告(2018)对世界上 65 个主要经济体实施的数字贸易限制性

指数进行了发布。如表 2 所示，俄罗斯“数据限制”指数为 0.63，排名世界第 2。在“数据政策”这个二级指标上俄罗斯得分全球最高，也就是说俄罗斯采取了世界上最为严格的数据政策。此外，俄罗斯在“中介责任”^①和“内容访问”^②这两个二级指标上的得分分别排在全球第 18 名和第 4 名。与之对照，欧盟的主要国家——法国和德国的“数据限制”指数分别为 0.45 和 0.41，排名世界第 4 和第 7；在 3 个二级指标上，法国分别排在第 5 名、第 20 名和第 12 名，德国分别排在第 4 名、第 30 名和第 13 名，排名都相对靠前，可见欧盟对于数据流动问题也持较保守的态度。美国作为全球主要的数字产品和数字价值的输出者，推崇数据自由流动，“数据限制”指数为 0.15，排名世界第 53，在 3 个二级指标上的得分分别排在全球第 50 名、第 48 名和第 37 名。

表 2 数据流动限制性指标排名

指标级别	指标类型	俄罗斯	法国	德国	美国
一级指标	数据限制	2 (0.63)	4 (0.45)	7 (0.41)	53 (0.15)
二级指标	数据政策	1	5	4	50
	中介责任	18	20	30	48
	内容访问	4	12	13	37

注：排名越靠前则表示采取更为严格的措施，括号内数字为“数据限制”指数。
数据来源：同表 1。

（二）俄罗斯有关数据流动限制的相关立法

俄罗斯很早就建立起了较为完善的数据管理法律制度，从联邦层面的立法角度来看，立法主要涉及以下 3 个方面（表 3）。

1. 跨境数据保护

2006 年出台的《关于信息、信息技术和信息保护法》（第 149-FZ 号联邦法）规定了信息持有者或信息系统运营者需要承担信息保护义务。这种保护主要是从预防、发现和制止信息泄露 3 个角度进行切入：相关义务方需要确保信息不向无权限方泄露并能够在发现信息泄漏后及时采取弥补措施，例如尽快恢复被破坏的信息。同年出台的《俄罗斯联邦个人数据法》（第 152-FZ 号联邦法）专门针对个人数据实施跨境保护措施，旨在保护俄罗斯公民的信息自由及权利。除了需要满足前述同等要求外，相关责任方还需要确认个人数据传输的目标国家是否能够确保个人数据的安全，如果安全性无法得到保证，那么需要取消或中止数据传输。

2. 互联网访问、准入和监管

2017 年通过的《关于数据、信息技术和数据安全的联邦法修正案》（第 276-FZ 号联邦法）对俄罗斯境内除了公司网络以外的虚拟专用网络（VPN）以及类似服

① 包括互联网服务提供商（ISP）、搜索引擎和社交媒体平台等所承担的责任。
② 包括专门针对与内容阻止、过滤和通过网络带宽进行区分的相关问题。

务施以限制。该法案并未禁止使用 VPN 和类似技术本身,而是需要 VPN 和其他受影响平台的运营商阻止俄罗斯用户访问被俄罗斯当局阻止的网站和其他资源。根据 2016 年出台的《关于修改联邦反恐法和俄罗斯联邦立法法及关于制定旨在打击恐怖主义和保护公共安全的附加措施》(第 374-FZ 号联邦法),电信运营商及其他互联网服务提供商将有义务对用户的短信、语音及图像等通信信息进行长达 6 个月的存储,以备联邦政府查询。

3. 数据本地化

2014 年出台的《就“进一步明确互联网个人数据处理规范”对俄罗斯联邦系列法律的修正案》(第 242-FZ 号联邦法)要求所有收集俄罗斯公民个人数据的企业在俄罗斯联邦的数据库中“记录、系统化、积累、存储、更新、更改和检索该信息”。处理俄罗斯公民个人数据的运营商必须通知 Roskomnadzor^①存储此类个人数据的服务器所在地,而且该法律也适用于参与处理俄罗斯公民个人数据的外国公司。2014 年通过的《关于国家支付制度和某些立法法案的联邦法修正案(修订法)》(第 319-FZ 号联邦法)要求在国内处理国际支付卡,旨在巩固国家支付卡系统作为在俄罗斯提供支付清算和运营服务的单一运营商的作用。

表 3 俄罗斯数据流动限制性措施的主要法律依据

法律类型	法律名称
跨境数据保护	《关于信息、信息技术和信息保护法》(第 149-FZ 号联邦法)
	《俄罗斯联邦个人数据法》(第 152-FZ 号联邦法)
互联网访问、准入和监管	《关于数据、信息技术和数据安全的联邦法修正案》(第 276-FZ 号联邦法)
	《关于修改联邦反恐法和俄罗斯联邦立法法及关于制定旨在打击恐怖主义和保护公共安全的附加措施》(第 374-FZ 号联邦法)
数据本地化	《就“进一步明确互联网个人数据处理规范”对俄罗斯联邦系列法律的修正案》(第 242-FZ 号联邦法)
	《关于国家支付制度和某些立法法案的联邦法修正案(修订法)》(第 319-FZ 号联邦法)

资料来源:欧洲国际政治经济中心(ECIPE)数据库。

(三) 俄罗斯数据流动限制政策与美国、欧盟及中国之比较

与对数据自由流动持保守态度的俄罗斯不同,美国是数据流动自由化的主要推动者。例如,美韩双方于 2007 年正式签署的自由贸易协定(FTA)第 15.8 条就要求缔约国在充分保护个人信息安全的同时,促进数据在跨境贸易过程中的自由流动,防止对电子商务数据流动施以限制。跨境数据自由流动和数据存储非强制本地化策略是由美国在数字产业上相较于世界其他国家的比较优势决定的,并且这将有利于

① 俄罗斯联邦通信、信息技术和大众媒体监督局, The Federal Service for Supervision of Communications, Information Technology and Mass Media, 简称: Roskomnadzor; 它既是被授权保护个人数据的联邦执行机构,也是负责俄罗斯互联网审查的机构。

引导数据由海外向美国流动。

在欧洲,为了进一步消除欧盟内部各国间的数字贸易壁垒,欧盟委员会于2015年提出了“单一数字市场”的数字战略规划,其中包括了“欧洲数据自由流动计划”,以期实现欧盟内部数据资源的自由流动。与此同时,对于个人数据保护,欧盟于2018年起实施的《一般数据保护条例》(GDPR)加强并完善了数据主体对个人数据享有的控制权利,确立了数据处理者保护数据安全的义务。欧盟对数据自由流动的态度介于美国的激进和俄罗斯的保守之间,更希望能在跨境隐私保护和数据流动之间保持平衡。

同俄罗斯和欧盟一样,中国也侧重于维护网络安全,对本地数据的保护十分重视。2016年颁布的《网络安全法》第三十七条规定了中国的数据本地化政策,即在中国境内收集或产生的数据都应当存储于中国境内;第四十条规定了网络运营者对用户信息负有保密的义务。为进一步加强网络生态治理,中国于2016年提出了《国家信息化发展战略纲要》,致力于完善网络立法,维护网络主权和国家安全。

(四) 俄罗斯数据流动限制政策成因分析

1. 国内网络安全战略布局

互联网在俄罗斯迅猛发展,为其数字贸易的兴起注入了动力。但与此同时,俄罗斯的信息技术发展水平显著落后于欧美发达国家,信息化产品的国产率较低。在如此庞大的网络用户规模背后,俄罗斯网络安全面临着巨大的挑战。据俄罗斯著名IT安全公司卡巴斯基于2013年发布的年度电子信息安全公告显示,俄罗斯2011年及2012年连续两年在全球网络安全风险指数这一排行榜中位居第一,俄罗斯互联网用户面临的风险水平高达58.6%。^①2014年,《俄罗斯联邦网络安全战略构想》草案出台,明确了网络安全战略的基本原则以及实施方向,这意味着俄罗斯将网络安全提升到了国家战略的高度,对于国内网络安全形势的重视促使俄罗斯当局不断通过政策手段加强对数据流动的限制。

2. 应对境外压力的现实需求

作为新兴的互联网大国,俄罗斯数据流动政策的制定主要是为了应对来自西方网络大国尤其是美国的压力。早在2003年,美国就推出了《保护网络空间国家战略》。乌克兰危机后,欧美发达国家对俄罗斯信息产业的制裁不断深化,对俄罗斯信息安全造成了不小的威胁。2018年,美国特朗普政府发布了最新的《国家网络战略》报告,其中规定了美国可以使用数字武器来保护国家安全,允许包括军方在内的各类机构进行网络操作。^②这象征着美国网络安全战略由“以防为主”向“以攻代防”转变。

① 朱峰,王丽,谭立新.俄罗斯的自主可控网络空间安全体系[J].信息安全与通信保密,2014,(9).

② <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

如今,以美国为首的西方国家不断在这一领域对俄罗斯施压,来自境外的压力使得俄罗斯需要采取较为严格的数据管理措施。

三、俄罗斯出台数据流动限制性措施的典型特征分析

(一) 数据输出规则针对“白名单”和“黑名单”对象做出明确区分

近年来俄罗斯逐步建立起了严格的数据保护制度和信息管理体系,从网络立法的角度来看,目前与数据输出规则有关的国家层面的法律有两部:《关于信息、信息技术和信息保护法》(第149-FZ号联邦法)和《俄罗斯联邦个人数据法》(第152-FZ号联邦法)。除此以外,《俄罗斯联邦外国投资法》《俄罗斯联邦安全局法》《俄罗斯联邦大众传媒法》等法律作为重要补充,也对跨境数据流动管理做出了相关要求和规定。为保障公民权利,维护个人数据安全,第149-FZ号联邦法规定了数据所有者、数据运营者、数据处理者等相关方需要承担的数据保护义务,确定了利益相关方在传播、使用和保护信息时所产生的法律关系,并对个人数据的跨境转移提出了较为严格的保护要求。俄罗斯与美国在这方面的分歧较大,美国倡导数据跨境自由流动以充分发挥其数字产业优势,在数字贸易中取得领先地位。俄罗斯则更加注重个人隐私权利保护,以对个人数据提供保护的程度作为是否进行数据跨境流动的标准。

1. 向提供足够保护的国家转移数据无需取得数据主体额外同意

根据第152-FZ号联邦法律规定,在转移个人数据的司法管辖区确保对个人数据充分保护时,向境外的个人数据传输不需要数据主体的额外同意。所有签署“108公约”^①的国家(以欧洲国家为主)都被视为对数据主体的权利和利益提供“充分保护”的管辖区。同时,根据第152-FZ号联邦法案,对于非“108公约”签署国,Roskomnadzor依然可以将其列入个人信息跨境流动的“白名单”中,其主要评判标准是该国是否设立了高效的个人信息保护机构、是否拥有完善的个人信息保护法律体系,以及是否针对违反个人信息保护法律的行为建立了有效的惩罚措施等。在非“108公约”签署国中,Roskomnadzor纳入“白名单”的官方国家名单包括秘鲁、南非、墨西哥、马里、摩洛哥、澳大利亚、安哥拉、阿根廷、新加坡、贝宁、加拿大、卡塔尔、新西兰、加蓬、以色列、马来西亚、佛得角、智利、哥斯达黎加、哈萨克斯坦、蒙古、韩国和突尼斯等,这些国家被视为为跨境转移个人数据提供了足够的保护,向这类国家的数据传输不受任何限制。值得注意的是,中国和美国两个国家均未被纳入其中。

2. 向其他地区转移数据须获得数据主体同意

除了“108公约”签署国以及Roskomnadzor确定的白名单外,其余国家均属于

^① 《个人数据自动处理保护个人公约》(Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,即“108公约”),俄罗斯于2001年11月7日签署该条约,并于2013年9月1日正式生效。

“未对数据提供足够保护”的国家。将个人数据跨境传输到这类无法提供足够保护的国家或地区必须获得数据主体出具的书面同意，或者需满足以下条件之一：（一）根据俄罗斯加入的国际条约，允许跨境数据转移的情形；（二）保护俄罗斯宪法体系、国家国防和国家安全、俄罗斯的运输系统等不受侵犯的情形；（三）为了履行数据主体所参与的合同；（四）保护数据主体的生命、健康或其他重要利益。

从以上数据输出规则的相关规定中，我们可以看出，俄罗斯的数据流动限制基本是在“108 公约”的框架内进行的，针对欧洲国家的限制较小。但对于其他地区的国家，尤其是中国和美国这两个数字贸易大国，却没有放开这方面的限制。禁止企业将数据输出到国外，这些限制可能会对那些依靠互联网进行交易、以服务海外客户并提高运营效率的公司构成障碍。例如，限制跨境数据流动的规定可能迫使企业在一国内建立本地服务器基础设施，增加成本、减小规模。

（二）设置严密的互联网准入和监管措施

相较于美国宽松的互联网审查制度，俄罗斯实施的互联网准入和监管措施则显得十分严格，但在合理范围内的过滤网络信息、限制访问网络既符合服务贸易总协定（GATS）的相关规定，也能够对维护国家安全、社会稳定起正面作用。

1. 对互联网访问设置禁区

2017 年 7 月通过的第 276-FZ 号联邦法《关于数据、信息技术和数据安全的联邦法修正案》要求虚拟专用网络（VPN）和类似技术的运营商阻止俄罗斯用户访问被俄罗斯当局禁止的网站和其他资源。该法律授权 Roskomnadzor 对提供如何规避政府封锁的指示网站进行阻止。它还授权俄罗斯的执法机构（包括内政部和联邦安全局）确定违规者和要求 Roskomnadzor 创建俄罗斯禁止的在线资源和服务的特殊登记。

2. 公共 Wi-Fi 用户实名制

根据 2014 年 7 月和 8 月陆续出台的第 758 条、第 801 条政府法令，为打击极端主义和恐怖主义，俄罗斯政府要求公共 Wi-Fi 进行用户识别。政府法令要求互联网服务提供商（ISP）应通过身份证件（如护照）识别互联网用户且应通过确定数据网络的唯一硬件标识符来识别终端设备。此外，俄罗斯的所有法律实体都必须每月向 ISP 提供使用其网络连接到互联网的个人列表。该法案旨在要求只有在实名制的情况下才能在公共场所免费使用互联网。

3. 电子监视规则

俄罗斯联邦总统于 2016 年 7 月签署了《关于修改联邦反恐法和俄罗斯联邦立法法及关于制定旨在打击恐怖主义和保护公共安全的附加措施》第 374-FZ 号联邦法）。该法律载有若干条款，扩大监测情报和私人服务以及私人电子通信，为执法机构获取“个人计算机信息”提供了法律依据。对于互联网服务提供商（ISP）及信息交换服务提供者，第 374-FZ 号联邦法规定了其必须将在线传输的有关内容所有连接、传

输和接收的元数据保留 1 年。

（三）实施严格甚至激进的数据本地化政策

数据本地化法律通常要求在该国家内存储或处理在特定国家收集的某些类型的数据。换句话说，由国家本地化法管辖的那些类型的数据不能转移到另一个国家进行存储和处理，即数据必须在位于该国家的服务器上存储或处理。数据本地化法律有时被称为“数据主权法”，因为它们反映了某个国家对源自该国的数据的主权主张。

俄罗斯通过第 242-FZ 号联邦法和第 319-FZ 号联邦法，基本建立起了数据本地化存储的规则。俄罗斯国内云数字产业相对并不发达，对美国的云服务提供商依赖过大，通过这种严格甚至激进的数据本地化政策对于其维护国家及个人利益有着积极的保护作用。

1. 个人数据存储和处理需在俄罗斯境内进行

俄罗斯新的数据本地化法（第 242-FZ 号联邦法）于 2015 年 9 月生效。法律要求在俄罗斯开展业务的网络运营商使用建立于俄罗斯境内的服务器或数据中心收集、存储和处理俄罗斯公民的个人数据。

此外，俄罗斯通信部要求电信和互联网提供商安装设备，在其服务器上收集和保留数据至少 12 小时以便俄罗斯联邦安全局（FSB）在必要时访问数据。这些数据包括用户的电话号码、流行的国内和国外在线资源（如 Gmail、Yandex、Mail.ru 等）的帐户信息、IP 地址和位置数据。

作为金砖国家之一，俄罗斯是一个庞大且日益重要的市场，许多海外企业已经拥有俄罗斯用户、客户或员工。这一事实意味着俄罗斯新的数据本地化法律推动了许多公司（不仅仅是那些位于俄罗斯的公司）为了遵守法律而在其运营中做出重大且可能代价高昂的变革。一些公司通过将某些数据业务迁移到俄罗斯来回应立法。与此同时，某些无法承受这种代价的外国企业可能会选择完全撤出俄罗斯市场。即使公司选择投资维护俄罗斯服务器以避免违反法律，还必须检查和隔离其收集的数据，以确保俄罗斯公民的数据留在俄罗斯。除针对个人数据的本地化要求外，金融部门和媒体部门还有部门数据本地化要求。

2. 线上支付业务本地化

2014 年，俄罗斯因为乌克兰危机遭受西方制裁，在 Visa 和万事达公司停止为某些俄罗斯银行服务之后，俄罗斯于当年 10 月通过了第 319-FZ 号联邦法《关于国家支付制度和某些立法法案的联邦法修正案（修订法）》，要求国际支付系统在 2015 年 3 月 31 日之前将其对俄罗斯国内业务的处理能力转移到当地国有运营商（国家支付卡系统^①），从 2015 年 4 月起，所有不在俄罗斯境内处理本地信用卡业务的外国

^① 俄罗斯国家支付卡系统，National Payment Card System Joint Stock Company，简称：NSPK JSC。

企业必须向中央银行缴纳一定数额的保证金,从而确保即使它们冻结服务,俄罗斯用户也不会遭受经济上的损失。俄罗斯此措施旨在巩固国家支付卡系统作为在俄罗斯提供支付清算和运营服务的单一运营商的作用。

3. 数据本地化与美国利益之间的冲突^①

美国认为数据本地化是阻碍数字贸易最常被引用的政策措施,美国国际贸易委员会2017年的一份报告显示,全球数据本地化措施的数量在过去6年中翻了一番。据估计,2015年全球70%的互联网流量通过云数据中心,2011年这一比例为30%。全球最大的云计算服务提供商大多是美国公司,约40%的云数据中心服务器位于北美。2014年,经合组织成员国22%的企业使用云计算服务,大型企业使用的比例更高,这一数字还在加速增长。因此俄罗斯数据本地化与美国云计算服务提供商的利益相冲突,将极大地影响到美国对俄罗斯数字贸易的开展。

俄罗斯大力推动数据本地化,主要是为了维护公民数据安全与国家主权安全,例如在面对西方制裁时,跨境支付业务本地化措施对维护其金融系统安全稳定以及保护俄罗斯公民个人数据有着积极正面的作用。但短期内,这些限制可能会对那些依靠互联网进行交易、以服务海外客户并提高运营效率的公司构成障碍。

四、对中国的启示

俄罗斯是实施数据流动严格管制的典型国家,通过借鉴以俄罗斯为代表的其他国家出台的数据政策经验,对于完善中国数据政策体系、促进数字贸易发展、保障数字贸易安全具有重要的战略意义。

(一) 推进跨境数据流动限制分类管理,减少不必要的数据流动限制

通过参考俄罗斯的相关经验,我们可以发现,俄罗斯对于数据的跨境流动采取分类管理的方式,针对“白名单”和“黑名单”对象做出鲜明区分,对于不同类型的数据流动实行不同程度的限制。但这种数据分类主要是建立在国别的基础之上,因此不可避免地会增大与某些国家间的数字贸易壁垒。有鉴于此,中国可以对数据进行分类管理,但应当建立在数据类型本身的基础上:对于个人用户的敏感数据、大型企业的商业机密信息以及涉及国家安全的数据严格限制跨境转移;对普通的个人、商业数据则可以放松跨境流动限制。目前中国基于新兴互联网技术的数字贸易相关产业呈现出飞速发展的态势,中国也有不少企业对于数据能够更加便捷地跨境流动有着巨大的需求。针对这部分需求,在维护数据安全的前提条件下,应当积极促进数据流动自由化,减少数字贸易壁垒。

^① Fefer, R. F., Akhtar, S. I., Morrison, W. M. Digital Trade and US Trade Policy[J]. Current Politics and Economics of the United States, Canada and Mexico, 2017, 19(1).

（二）保持网络空间自主可控，非敏感领域适当放宽互联网准入和监管

针对跨境网络数据传输以及提供相应服务的电信运营商，俄罗斯设置了十分严密的准入和监管措施，其主要目的是打击网络犯罪及恐怖主义活动。但与此同时，俄罗斯此类措施由于限制了信息的自由流动，可能对数字贸易存在负面影响。因此，在充分保障公民合法使用互联网资源的权利及网络资源合法有序自由流动的基础之上，互联网审查措施应当适度合理，在不涉及国家安全问题的非敏感领域适当放宽互联网准入和监管，从而将对数字贸易的不利影响降到最低。中国于2016年通过的《中华人民共和国网络安全法》对网络安全的监督管理做出了相关规定，对于推进网络空间治理活动起到了积极作用。应当继续制定和完善此类法规，并将监管标准和审核方式透明化、制度化，对互联网空间进行有效介入，维护国家安全、网络空间主权和社会公共利益，保持网络空间自主可控。

（三）充分发挥中国互联网产业优势，降低数据本地化带来的额外成本

2013年斯诺登事件发生之后，世界主要国家都意识到了信息安全的重要性，并制定了一系列关于数据本地化的法律法规。俄罗斯制定的数据本地化法相当细致，且执行较为彻底，严格要求企业将数据进行本地化存储并深入推进了线上支付业务本地化。由于全球最大的云计算服务提供商大多是美国公司，数据本地化措施也给包括俄罗斯本国企业在内的跨境业务开展带来了不小的成本负担。尽管数据本地化会给类似俄罗斯这样的信息通信产业竞争力较低的国家带来不小的负面影响，但对于中国这样的互联网产业较为发达的国家而言，放弃数据本地化政策并不符合国家利益。对于中国而言，数据本地化政策主要有3个作用：第一，保障个人隐私以及国家安全；第二，便于本国有关部门执法，打击依托互联网进行的犯罪；第三，促进本国网络数据产业的发展。因此，既要实现以上3个目标，又要对数字贸易业务开展的成本加以控制，中国就需要充分发挥互联网产业优势，进一步完善数据本地化制度。中国是互联网大国，用户规模世界第一，在互联网创新上也走在世界前列。在政策上，应当参考俄罗斯及欧盟的相关立法经验促进数据本地化制度的完善。在实践中，应当向国内新兴的云服务提供商提供更多便利与支持，大力发展云计算、大数据等解决方案；鼓励中小企业使用国内的云存储设备；在减少国内企业由于数据本地化而花费额外成本的前提条件下，促进重要数据及公民个人数据存储于国内，维护网络数据安全。

参考文献：

- [1] 高际香. 俄罗斯数字经济战略选择与政策方向 [J]. 欧亚经济, 2018, (4).
- [2] 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).
- [3] 李杨, 陈寰琦, 周念利. 数字贸易规则“美式模板”对中国的挑战及应对 [J]. 国际贸易, 2016, (10).
- [4] 李忠民, 周维颖, 田仲. 数字贸易: 发展态势、影响及对策 [J]. 国际经济评论, 2014, (6).

- [5] 逢健, 朱欣民. 国外数字经济发展趋势与数字经济国家发展战略 [J]. 科技进步与对策, 2013, 30(8).
- [6] 伊万·沙拉法诺夫, 白树强. WTO 视角下数字产品贸易合作机制研究——基于数字贸易发展现状及壁垒研究 [J]. 国际贸易问题, 2018, (2).
- [7] 王晶. 发达国家数字贸易治理经验及启示 [J]. 开放导报, 2016, (2).
- [8] 张冬杨. 俄罗斯数字经济发展现状浅析 [J]. 俄罗斯研究, 2018, 210(2).
- [9] 周念利, 陈寰琦, 黄建伟. 全球数字贸易规制体系构建的中美博弈分析 [J]. 亚太经济, 2017, (4).
- [10] 周念利, 李玉昊. 全球数字贸易治理体系构建过程中的美欧分歧 [J]. 理论视野, 2017(9).
- [11] Burri, M. Should There Be New Multilateral Rules for Digital Trade?[J]. Think Piece for the E15 Expert Group on Trade and Innovation. Geneva: International Centre for Trade and Sustainable Development, 2013.
- [12] Ferracane, M. F., Kren, J., van der Marel, E. Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?[R]. Working paper, Brussels: European Centre for International Political Economy, 2018, <https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Impact-the-Productivity-Performance-of-Firms-and-Industries-final.pdf>.
- [13] Lund, S., Manyika, J. How Digital Trade Is Transforming Globalisation[C]. International Centre for Trade and Sustainable Development (ICTSD), 2016.
- [14] Wunsch-Vincent, S. The Digital Trade Agenda of the US: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization[J]. Aussenwirtschaft, 2003, 58.

The Research on Russia's Trade-related Data Flow Restrictive Measures: Its Enlightenment to China

ZHOU Nianli LI Jindong

Abstract: On the issue of data flow, for the sake of maintaining the security of its own cyberspace, Russia has formulated the world's most rigorous restrictive policy on data flow. Based on the analysis of the trade-related data flow restriction measures categories and related legislations introduced by Russia, the reasons for their formation are analyzed. This paper analyzes the typical characteristics of Russian data flow restriction measures. First, the data output rules make a clear distinction between whitelist and blacklist objects. The second is to set strict internet access and regulatory measures. The third is to implement strict and even radical data localization policies. Finally, this paper gives relevant inspirations for the implementation of data flow management in China according to relevant Russian practices. China needs to promote classified management of restrictions on cross-border data flow and reduce unnecessary restrictions on data flow. It needs to keep cyberspace autonomous and controllable, and relax internet access and regulation mechanisms in non-sensitive areas. Also China needs to give full play to the advantages of its internet industry and reduce the additional cost of data localization.

Keywords: digital trade; data flow; data localization

(责任编辑: 梁丽华)