跨境数据流动安全治理

董京波

中国政法大学国际法学院,北京 100088

摘要　数据安全治理规则对于数据跨境流动至关重要。在评析典型国家和国际现行的双边和多边跨境数据流动安全治理规则的基础上,分析了中国跨境数据流动安全治理立法现状,并提出相关建议:中国应细化相关规定并完善数据分级分类监管制度,同时要完善数据领域的阻断法,积极应对他国的长臂管辖;要积极参与数据跨境国际规则的制定,将数据安全条款嵌入国际经贸规则中,并进一步促进达成全球数据安全流动规则。

关键词　数据安全;数据主权;跨境数据流动;安全治理

数字贸易是国际经济贸易的重要组成部分,跨境数据流动作为数字贸易的基石,在促进世界经济贸易的发展与合作方面发挥着至关重要的作用。但是,数据在跨境流动过程中也对数据主体的隐私及国家安全带来了一定的挑战,因此对跨境数据流动进行治理以保证数据安全具有必要性。在数据跨境传输中,一国的关键数据或特定行业数据流向境外后可能会对该国国家安全产生潜在的威胁,可通过未经授权的黑客或网络攻击破坏个人数据、网络攻击域名系统、攻击国家的关键基础设施等[1],同时还包括一些非法收集或监控他国数据的行为。尤其在2013年"棱镜门"事件后,各国对数据安全愈发的重视,纷纷通过立法加强对跨境数据流动的限制以维护本国的数据安全。

在数据跨境自由流动的过程中,对个人数据权利的侵权行为也值得关注。首先,受到侵犯的可能性更大,侵权行为也更难以发现和追溯;其次,救济更为困难,境内的相关法律不一定能对境外的侵权行为进行管辖,损害发生时要寻求救济更加困难;最后,影响范围更广,有时不仅是数据主体的个人数据权会被侵犯,甚至可能会对该国的公共利益、国家的网络安全等问题造成严重影响。近日滴滴出行受到安全审查就是明显的案例。2021年7月2日,国家互联网信息办公室网络安全审查办公室对刚刚在美国纽约证券交易所上市的滴滴出行进行安全审查,以防范国家数据安全风险,维护国家安全,保障公共利益。为配合网络安全审查工作,防范风险扩大,审查期间滴滴出行停止新用户注册。滴滴出行拥有大量的个人数据,也许单一的乘客信息、司机信息和轨迹信息并不具有特别重要的价

收稿日期:2021-06-20;修回日期:2021-09-10

基金项目:中国政法大学科研创新项目/中央高校基本科研业务费专项(ZFYZ82004);北京市社科基金重点项目(15FXA007);中国政法大学网络法学院课题(201912)

作者简介:董京波,副教授,研究方向为国际经济法、知识产权法、大数据与人工智能法等,电子信箱:boboanney@hotmail.com

引用格式:董京波. 跨境数据流动安全治理[J]. 科技导报, 2021, 39(21): 9-17; doi: 10.3981/j.issn.1000-7857.2021.21.001

值。但是通过对以上综合信息的大数据分析,就可以得出很多其他重要信息,这不仅危害消费者的个人数据安全,甚至可能危害国家安全。

跨境数据流动对国家数据安全带来了一定的挑战,但笼统地对其予以严格的本地化限制并非保障国家数据安全的最佳策略,通过制度设计和技术支持的完善进行跨境数据流动安全治理,促进数据在安全的前提下进行跨境流动才能顺应数字经济的发展。

对此,国内外学者展开了研究,但角度不太相同。国外学者重点关注为保证数据跨境安全所采取"数据本地化"措施带来的挑战。Anupam[2]认为数据本地化会侵蚀隐私和安全,同时也会增加国内监控的风险。国内学者张舵[3]则从"公共利益保护"的角度,对数据跨境流动中限制性规定的正当性进行分析。彭岳[4]针对具体的数据跨境限制措施,提出将数据隐私保护问题的讨论放置在国际贸易规则的视域下解决。本研究以跨境数据流动中的安全治理为视角,在讨论跨境数据安全治理典型国家的实践和国际双边、多边制度的基础上,比较分析中国现有立法的不足并提出改进建议。

1 典型国家跨境数据流动安全治理实践及评析

1.1 俄罗斯和印度:公权力直接介入保护数据安全

俄罗斯将数据本地化作为基本原则,要求数据回流。俄罗斯通过不断地修法和颁布法令加强了对数据流动的管控,2015年9月1日生效的《俄罗斯联邦澄清部分关于信息和电信网络联邦法律中适用处理个人资料程序的修正案》确立了数据本地化存储的规则[5]。数据本地化法律的实施使俄罗斯快速发展起了大数据市场,并推动跨国企业兴建大量数据中心。在执法层面,俄罗斯也希望通过数据本地化存储加强政府执法权和对数据的控制力,这一点也在其反恐法修正案"Yarovaya's Law"中得以体现。该法要求在互联网上传播信息的组织者保留俄罗斯用户的互联网通信数据、用户本身的数据和某些用户活动的数据,在俄罗斯境内留存6个月时间,并应要求向俄罗斯当局披露。2006年《个人信息保护法》划定了数据自由流动范围,允许自由流向第108号《有关个人数据自由化处理之个人保护公约》(以下简称108号公约)缔约国和俄罗斯自行拟定的俄罗斯版"适当性认定"通过的白名单国家。如果数据接收方位于法律仅提供"不充分保护"的国家,则《个人信息保护法》要求满足某些条件。

印度政府极力主张数据主权,并以公权力直接介入的方式对跨境数据流动进行规制,提出了数据本地化存储的强制性要求。在《印度电子商务国家政策框架草案》中,印度政府就主张:"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。各种形式的国家数据均是国家资源,所有印度人都应公平地获取,但非印度人没有获取印度数据的平等权利。"基于数据主权,以保护数据安全为主旨目的,印度在跨境数据流动治理时采取了反对跨境数据自由流动的态度,主张实施数据本地化和跨境数据流动限制性措施。近年来,印度相继颁布了一系列法律法规构成了其跨境数据流动治理体系。2018年,《印度电子商务国家政策框架草案》出台,明确将逐步推进数据本地化存储、建立数据中心,同时也列出了一系列数据本地化的豁免情形,比如初创公司的数据传输,跨国企业内部数据传输,基于合同进行的数据传输等并不加以限制[6]。针对个人数据,采取分级分类进行管控的方式,实施不同的数据本地化要求。在《个人数据保护法草案2018》中,印度将个人数据分为3种类型,一般个人数据、敏感个人数据和关键个人数据,并针对3种数据类型实施不同的数据本地化和跨境流动限制。首先,对于一般个人数据和敏感个人数据,草案要求这两类数据应当在印度境内存储副本,可以跨境流动。同时,印度政府可以对一般个人数据进行清单化的豁免限制。其次,关键个人数据仅能存储在印度境内的服务器/数据中心,绝对禁止离境的。而对于金融数据,则强制本地化存储,促进印度银行金融业发展。印度中央银行要求2018年10月15日之前,所有在印度的支付企业都要将数据强制性存储在印度本地。对此,欧盟和美国政府及企业都提出了大量的反对意见,但是印度仍强势推进

了支付数据的本地化规定。

在实践中,印度则更是将数据本地化措施一以贯之。2020年6月29日以来,印度政府数次宣布禁用多达200款以上中国手机软件,包括TikTok、微信、支付宝、百度等。印度信息与科技部(MEIT)宣称这些软件长期收集、分享数据,侵害个人数据与用户信息,不利于印度主权和完整、印度国防、国家安全与公共秩序,故依据《信息技术法案》第69条A的"禁止公众访问"予以封禁。但实际上,禁止公众访问决定的做出需要履行一定的正当程序,而此次禁令并未满足正当程序的要求,且这些软件危及其国家安全的证据亦并不充分。

通过分析俄罗斯、印度跨境数据流动治理的立法实践可以发现,政府对数据跨境都施加了强有力的限制性措施以保障本国的数据安全。但网络空间实则是没有边界的,数据的跨境流动能够创造出巨大的经济价值,推动全球贸易的发展。仅通过将数据限制在本国境内的方式保证数据安全并非万全之策也不具有经济效益。从数据安全的角度看,并不取决于数据的存储地点,而是数据存储和流动的方式,互联网的跨地域性使得对数据的攻击无分边界。将数据留存在国内只能从防守方的角度加强国内法律对其保护与管辖,在此程度上降低数据安全风险,但通过国际合作等方式加强数据流动过程中的安全保护措施亦可达到同等效果。因此,适当程度的数据本地化措施可以在一定程度上降低跨境数据流动带来的数据安全风险,但通过国际合作完善数据跨境流动的安全保护措施才是符合数字贸易发展的长久之计。而印度在跨境数据流动治理方面的司法实践则说明数据安全或是国家安全存在着被滥用的可能,一国可能出于政治目的而滥用跨境数据流动限制性规则,打击他国投资者合法的对外投资。因此,在重视数据安全的同时也应当防止该理由被不合理地滥用构成贸易保护主义。

1.2　欧盟:以内化于私权的方式间接保护数据安全

欧盟向来具有尊重个人数据权利的传统,长期致力于个人数据保护,在进行跨境数据流动治理时,采取了将主权内化于私权的方式间接保护个人数据安全。2016年欧洲议会和欧盟理事会通过的《通用数据保护条例》(General Data Protection Regulation, GDPR)详尽地对个人数据跨境流动问题进行了规定,力求在促进跨境数据流动和个人数据保护之间进行平衡。

GDPR的相关规定提供了个人数据跨境转移的法律基础,这种条件设置是具有层级的,上一级的条件不满足时适用下一级条件。首先,根据GDPR第45条规定,如果第三国或其他组织获得了欧盟委员会的充分性决议,能够确保充分的保护程度,则意味着已经对该国的整个法律体系进行了充分地评估,数据可以跨境转移至这些国家或组织。而欧盟委员会在评估保护程度是否充分时应考虑以下3个因素:第三国与数据保护相关的法律体系是否完备;第三国境内是否存在有效运作的独立监管机构;第三国是否做出与个人数据有关的国际承诺,承担相关义务。与此同时,GDPR还将充分性认定的对象范围从国家扩大到一国内的特定地区、行业领域以及国际组织[7]。其次,如果没有获得充分性决议,但可以通过标准合同文本或者约束性公司规则等建立一些保障"充分性"的小岛,即采取了适当的保护性措施,则数据也可以进行跨境传输。这些适当保护措施包括:制定约束性企业规则;采用标准数据保护条款;根据经批准的行为准则及数据控制者、处理者所做的承诺提供的适当保护;根据经批准的认证机制及数据控制者、处理者所做的承诺提供的适当保护。最后,GDPR规定了在没有"充分性决定"和"适当保护措施"时的法定例外,只要满足了这些法定特殊情形,则可以向第三国或国际组织进行数据跨境转移[8]。欧盟GDPR的跨境数据流动治理实践不仅规定了具有条件层级的个人数据跨境条件,在保障数据安全的情形下促进跨境数据流动,同时也创立了一些具有借鉴意义的安全保障规则。例如适当保护措施中的约束性企业规则、标准数据条款等。约束性企业规则(Binding Corporate Rules, BCR)是针对国际性企业进行个人数据跨境传输而制定的,最终目的是保证企业在出口和进口个人数据时能按照一定的保护标准来保障个人数据的安全[9]。企业集团如果能够遵循一套完整的、经过主管监管机构批准的数据保护政策,

则该集团可以整体被视为一个“安全港”,个人数据可以在集团内部进行跨境自由流动。而GDPR更是对约束性企业规则提出了极高的要求,企业集团必须确保个人信息安全在每时每刻每地每个环节都得到充分保障,否则将随时面临在欧盟境内被起诉或申诉的法律风险[10]。在执行监管方面,则利用其数据保护官制度来监督企业准则被遵守执行,数据保护官或相关负责人应向成员国监管机构汇报约束性企业规则的执行情况、变化情况以及第三国可能对规则有效执行产生负面影响的立法情况等。

通过上述实践可以发现,欧盟已通过GDPR构建了严格的个人数据保护法律框架,并在此框架下力图推进数据的跨境流动,达成二者之间的平衡。欧盟在试图统一欧洲的数据保护规则、推进数字单一市场的同时,在2020年2月,更是连续发布了《欧洲数据战略》《塑造欧洲的数字未来》和《人工智能白皮书》3份文件,集中提出了“技术主权”观念,在技术、规则和价值方面扩大了数据主权的外延,试图将欧盟对网络空间的控制力和主导权从规则制定领域进一步覆盖到网络关键技术和基础设施领域。完善的规则有利于提升国际影响力并在相关领域的国际协调与合作中争夺话语权,因此,中国更应该加快跨境数据流动安全治理的步伐,完善相应的法律法规,提高治理水平以应对国际挑战。

1.3 美国:系统的数据安全审查机制及扩张的域外数据管辖权(长臂管辖)

在跨境数据流动治理领域,美国一向崇尚利用其互联网科技的优势地位推动跨境数据的自由流动。但实际上,美国仍然规定了一些限制性措施以保证公民敏感个人数据、重要数据及美国的国家安全。《2018年出口管制改革法案》规定,民用和军民两用科技数据出境应当符合一定条件,包括通过最小占比计算、获得授权许可或许可例外等。而对于国防数据、联邦税务数据,则通过立法要求这些重要数据仅在美国领土内存储。为了保护国家安全,美国2018年通过的《外国投资风险审查现代化法案》(FIRRMA)进一步解释关键基础设施、关键技术、敏感个人信息等术语,将美国外国投资委员会(CFIUS)的管辖范围扩大至涉及关键基础设施、关键技术或敏感个人数据的其他投资。美国通过一系列法规构建了其跨境数据流动安全治理的法律基础,在促进跨境数据自由流动的同时达到保障数据安全的目标。但在实践过程中,种种行为却与促进跨境数据自由流动的主张相悖,呈现出贸易保护主义的倾向。与印度相似,美国也存在出于政治目的而滥用国家安全、滥用跨境数据流动限制法规,打击他国投资者合法的对外投资的行为,特朗普以国家安全为名禁止华为参与本国5G网络建设、封禁TikTok以及后续以美国国务卿蓬佩奥为代表的美国政客发起的“清洁网络”计划都是典型的例子。而美国参议院法案《2019国家安全和个人数据保护法案》更是明确将中国和俄罗斯列入受关注国,规定受关注国家的相关企业不能将数据用于研发并且禁止向受关注国传输用户数据。该法案与CFIUS共同配合,全面地切断美国用户数据流入受关注国。

除了制定国家安全审查制度、重要数据本地化存储制度等,美国在治理中值得一提的实践还包括通过“长臂管辖”扩大了国内法域外适用的范围,以满足新形势下跨境调取数据的执法需要。2018年,美国议会通过《澄清境外数据的合法使用法案》(CLOUD法案),通过适用“控制者原则”,授权美国执法机关可以要求数据服务商保存、备份、披露其监管控制的数据,尽管这些数据存储于境外[11]。该法案扩大了美国执法机关调取海外数据的权力,将数据管辖权从美国领土延伸到了全球。同时CLOUD法案还抛开传统的双边或多边司法协助条约,仅允许适格外国政府执法机构调取美国存储的数据,而适格则需要符合美国所设定的人权、法治和数据自由流动标准。这种规定加剧了当前国家间与数据有关的司法主权冲突,美国单边主义及霸权主义的倾向昭然若揭。2019年,中国香港某公司涉嫌违反美国对朝鲜的制裁令遭到美国执法机构的刑事调查,美国法院向中国招商银行、浦发银行、交通银行发出传票要求配合调查,提供该公司银行账户和交易记录等数据。3家银行根据中国《国际刑事司法协助法》及国际礼让原则拒绝提供交易数据,因为如果向美方提供涉朝数据则违反中

国国内法,将受到国内处罚。传票之争在美国进行审理后,美方认为鉴于其中2家银行在美国注册了分行、1家银行使用了美国银行系统的服务故美国法院具有管辖权,同时根据最高法院的判例,本案不适用国际礼让原则。虽然这3家银行暂未因为拒绝执行传票而被美国政府采取制裁,但从本案中可以窥见美方依据其长臂管辖权侵害他国司法主权,枉顾国际合作,因此中国应当采取措施阻断美国的长臂管辖权,保护中国企业的合法权益。

1.4　日本:高标准数据安全保护与自由流动机制的结合探索

日本同时与欧盟、亚太经济合作组织(APEC)等机制对接,积极推动跨境数据自由流动规则构建。国内立法形式上参考欧盟,但通过更弹性化的解释推动数据跨境自由流动。作为亚洲最成熟的经济体,日本早在2003年就通过了《个人信息保护法》(APPI),并在2015年进行了修订。数字经济的全球化发展也推动日本在修订APPI时引入对数据跨境转移的监管,规定了3种向境外转移个人数据的合法方法:(1)事先征得个人同意;(2)转移的目的国是个人信息保护委员会认可的具有和日本同样保护水平的国家(白名单国家);(3)处于白名单范围内的国家和地区的数据接收企业依照个人信息保护委员会的要求建立了保护数据的完善体系,能够为数据提供有效保护(与APEC跨境隐私规则体系相一致)。立法形式上虽然参考欧盟,但日本在其基础上给予规则更大的解释空间,为数据跨境转移提供制度基础。

2　数据跨境流动安全治理双边和多边制度

2.1　数据跨境流动安全治理双边协定——以欧盟与美国之间的双边协定为代表

在跨境数据流动安全治理方面,虽然没有专门的数据安全协议,但安全一直是跨境流动的重点关注,其中尤以美欧的双边协议引人注目,2000年,美国商务部与欧盟委员会达成了《美欧安全港协议》(U.S-EU Safe Harbor Framework)。《美欧安全港协议》由于不能充分保证欧盟个人隐私安全后,该协议被欧盟法院裁定无效。后来,双方经紧急磋商达成了《欧美隐私盾协议》(EU-U.S Privacy Shield Framework),成为规制双方数据跨境流动的新方案。《欧美隐私盾协议》实则是《欧美安全港协议》的升级版,两者都旨在在确保数据安全的情况下便利个人数据在两地间的自由流动[12]。然而同样因为个人数据安全问题无法在该协议下得到保障而无效。欧洲法院称,协议条款没有为个人信息从欧洲转移到美国的人提供充分的隐私和数据保护。首先,法院认为欧盟委员会在审核《欧美隐私盾协议》时,对美国的政府监控项目评估未能符合欧盟法律规定的严格必要及与目的成比例规定,因此并不符合《欧洲联盟基本权利宪章》第52条的规定。其次,法院认定对于美国的监控,欧盟数据主体缺乏可行的司法赔偿手段,违反《欧洲联盟基本权利宪章》第47条规定的救济。这意味着在《欧美隐私盾协议》框架下获得认证的5384家公司需重新考虑跨境数据传输机制,也意味着双方将回到谈判桌前,重新评估"加强版隐私盾"的可能性。

2.2　数据跨境流动安全治理多边合作机制

2.2.1　欧盟主导的数据跨境流动多边公约,着力保障数据跨境流动中的隐私安全

1981年1月28日,欧盟理事会各成员国签署108号公约,作为历史上首个在数据保护方面对跨境数据流动进行规定,具有法律约束力的国际条约;该公约向全球开放,乌拉圭已经作为第一个非欧盟国家加入该公约。2014年12月欧洲理事会通过了新版108号公约的提案。并将108号公约发展成为"向所有为个人数据提供所要求的保护的国家开放的全球数据隐私条约也正在进行当中。"

2.2.2　在多边贸易谈判中引入数据跨境自由流动条款,安全条款作为例外条款

世界贸易组织(WTO)是国际多边贸易规则的典型代表和集大成者。近年来,美国、日本、新加坡等国向WTO多次提交了推动电子商务谈判的提案,提出了禁止限制数据跨境流动的主张;以中国为代表的发展中国家以及欠发达国家,主张建立基于货物流动为主的跨境电子商务规则;而非洲、加

勒比和太平洋岛国等相关国家,由于自身电信与互联网等基础设施较差,反对将数字贸易及跨境电子商务议题纳入多边贸易框架下讨论。就目前的情况而言,在WTO框架下达成一个多边的数据流动协议是比较困难的。

美洲地区,新近达成的《美加墨协定》(United States-Mexico-Canada Agreement,USMCA)作为《北美自由贸易协定》的更新,表明特朗普政府在数据隐私保护和跨境流动方面的立场。总体上讲,USMCA要求当事方不得限制跨境数据流,例外情况下政府得以实施非任意的、非歧视性的、非变相贸易壁垒的措施或不得大于超出实现特定目的所必须以实现合法的公共政策目标(例如隐私安全、国家安全)。通过这种方式,各方寻求在保护隐私及安全与商务和通信数据自由流动之间的平衡。该协议提及成员国需认可美国主导的APEC的CBPR,意在促进CBPR和国家隐私制度的全球互操作性。三国政府还承诺鼓励私营部门自我监管模式,并促进合作以执行隐私保护法规。

在亚洲和太平洋地区,东盟十国以及中国、日本、韩国、澳大利亚、新西兰和印度等正在谈判的扩展性贸易协定,即《区域全面经济伙伴关系协定》(RCEP),有望建立一个统一的数据隐私规则。与此同时,该区域一些国家也在谈判《全面与进步跨太平洋伙伴关系协定》(CPTPP)。CPTPP跨境数据传输规则由从前的《跨太平洋伙伴关系协定》(TPP)电子商务章节(第14章)发展而来,依据CPTPP第14.11条,成员国应当允许跨境传输电子信息,对跨境数据传输的限制措施只能基于合法的公共政策理由,且该措施不对信息传输施加超出实现目标所需限度的限制,也不得通过对贸易造成不合理歧视或变相限制的方式实施。

3 中国跨境数据流动安全治理立法现状及建议

3.1 跨境数据安全治理立法现状:立法分散

中国在跨境数据流动治理领域起步较晚,但近年来随着中国互联网产业的迅速发展和数据跨境传输需求的增加,政府已经开始关注数据跨境流动问题,加大了相关领域的立法工作。2017年颁布的《网络安全法》对数据跨境流动从法律层面上有所涉及,其中第37条明确规定了个人信息和重要数据应在境内存储。为了进一步完善《网络安全法》的规定,2019年国家互联网信息办公室发布了关于《网络安全审查办法(征求意见稿)》《个人信息出境安全评估办法(征求意见稿)》并公开征求意见,其中后者摈弃了之前将个人信息和重要数据一并处理的方式,对《网络安全法》进行突破。但与跨境数据流动相关的规定仍然是少之又少,专门统一的、可操作性强的法规也处于缺位状态,这一情况在《数据安全法》的颁布和实施后得到一定的改善。2021年6月,《数据安全法》出台,该法从多方面规定了数据安全前提下的跨境数据流动规则,构建了基础的法律框架。《数据安全法》第26条反制措施的规定则有利于塑造一个公平的国际竞争环境,双向的数据跨境流动才能促进国际协调与合作,当一国限制中国企业从数据跨境流动中汲取商业利益时,中国有权实施对等措施以保障企业的合法权益。再者,《数据安全法》第36条对诸如美国等国的长臂管辖规定了阻断措施,避免他国行使数据主权时对中国的数据主权造成侵犯。与此同时,该阻断措施对国际条约和协定予以了豁免,体现了中国遵守国际义务,支持国际协调与合作的态度。2021年8月出台的《个人信息保护法》对个人数据跨境流动的规则做出了较为具体的规定。《个人信息保护法》明确数据跨境传输的法定条件并规定了海量个人数据跨境传输需要经过安全评估。为了保护个人数据安全,该法还要求数据输入国家有同等的数据保护水平并需对个人告知并得到个人的同意。

3.2 当前立法体制存在的不足

基于不同的产业能力,目前各国政府在数据跨境流动策略选择上可以分为3种类型,包括以美国为代表的主张自由流动的进取型策略、以欧盟为代表的规制型策略和以印度、俄罗斯为代表的出境限制策略。从产业能力的角度来说,中国数字经济发展仅次于美国,领先于欧洲和其他国家,但是中国在此前的数据跨境流动政策上总体趋向保守,立法

滞后,与中国目前位居第二的数字经济产业能力并不完全相符。

第一,无论是《个人信息出境安全评估办法》,还是《网络安全法》和《数据安全法》,都存在原则性规定过多的问题,就个人数据安全的法律保护而言,不具有针对性。在具体的立法技术层面,规范相对不够充分。以《数据安全法》第2条域外效力为例,规定该法不仅具有域内适用效力,同时也适用于在境外开展数据活动损害到中国国家安全、公共利益或公民合法权益的组织和个人,该法的域外适用效力在一定程度上得以延伸。但与欧盟GDPR延伸域外适用效力不同,中国是基于国家安全、公共利益和公民合法权益保障的最低标准,只有当这些合法权益受到侵害时才得以使用以维护中国的数据主权,而GDPR却规定境外涉及对欧盟公民个人数据处理的任何机构均受其管辖。当然,《个人信息保护法》第3条进一步扩张了个人信息保护法的适用范围,但与GDRP相比而言,《个人信息保护法》在对域外适用范围的界定上较为模糊和保守。

第二,相关规定过于宽泛,操作上具有困难。尽管《数据安全法》及在试点方案中均提到数据分类的重要性,但仍未出台细化的规则。另外,第24条的数据安全审查制度,通过对数据活动如数据的收集、存储、使用、加工等行为进行安全评估,确保跨境数据流动中的数据安全。但这种审查制度不仅会增加时间成本、削弱数据流动产生的经济价值,同时如果规则规定不够详细,会带来实际操作上的困难,适用的随意性会彻底成为跨境数据流动的阻碍。

第三,数据安全配套法规并不完善。近来滴滴上市引发的数据安全问题就是个例证,由于滴滴注册地在海外,而中国未设置相关的境内前置审批程序,导致滴滴上市后才接受国内安全审查。

第四,应对长臂管辖的反制措施有待进一步细化。《数据安全法》第36条对长臂管辖规定了阻断措施,但对于当事人而言,可能面临两难的选择。不提供证据的,可能会在境外诉讼败诉。如若提供证据,则可能违反《数据安全法》。如何解决这种法律冲突,还需要将来法律和司法实践进一步明确。

第五,未能有效地参与双边和多边数据跨境规则制定,增加了跨国企业的合规负担。中国在数据跨境流动方面态度整体相对保守,但是这并非长久之计,不仅导致国际规则制定方面缺乏中国声音,另外也影响了中国企业走出去。目前各辖区都有域外管辖的趋势,只要企业在当地有数据业务,就需遵守当地法规,而不管数据存储在何处。这使企业处于两难境地,企业业务需要数据跨境,而如果两国政府间没有协议,只能在数据获取地建立存储中心,相应数据的研发等都要本地化,将带来高额的企业合规成本。

3.3　完善中国跨境数据流动安全治理的建议

中国作为数字经济的积极参与者,需要借鉴别国经验,进行制度建设,以有效平衡数据流动与安全利益。中国可以仿效欧盟,在数据分类的基础上,提供多样化的有效合法数据跨境渠道;也可以参考美国灵活的、系统的数据安全审查机制,从技术出口法、外资安全审查等多方面全面规制,以总体的安全制度构建来保证数据跨境安全。在协调数据安全目标与跨境数据自由流动目标的基础上,结合各国跨境数据流动安全治理可取的实践为中国的跨境数据流动安全治理提供以下具体的建议。

3.3.1　出台细则、完善多元化的数据安全治理模式,保护个人数据跨境流动安全

从国外来看,数据跨境流动的安全管理可以根据不同情形建立多元化的管理手段。欧盟不断在数据流动与确保个人信息安全之间寻找平衡,GDPR确认了白名单、标准合同、风险评估、协议控制等多种方式。虽然中国新的《个人信息保护法》明确向境外提供个人信息的途径,包括通过国家网信部门组织的安全评估、经专业机构认证、订立标准合同、按照中国缔结或参加的国际条约和协定等,但是相关规定还需要细化,以便于执行。《数据安全法》对国家核心数据和重要数据之外一般数据的跨境流动,并未作明确限定,原则上可以自由流动,但是《数据安全法》同样"以原则为导向",缺少详尽的规则。中国应该提供更多细化的规则,为企业跨境传输数据提供安全有保障的可行路径。

3.3.2 制定跨境数据流动分级、分类的监管体系

中国应对重要数据和个人数据实施分级管理,分类监管。关于分类监管的问题,尽管在《数据安全法》及试点方案中均提到其重要性,但仍未出台细化的规则。因此,建议规定详细的数据分类管理制度,在提高数据保护水平的基础上对跨境流动数据进行分类,针对不同类型的数据采取不同的管理方法。对于涉及国家秘密等极其重要的数据,可以采取类似负面清单的模式,明确列出只能在境内的数据中心存储和处理,禁止跨境传输;对于有可能影响国家安全、社会公共利益的数据传输采取严格的控制,需要报请行业主管部门进行评估,评估后做出是否准许出境的决定;对于非敏感、非大量的数据跨境传输则采取自我评估为主的方式。与此同时,对不同类型的企业和不同出境事由进行差异化监管也是可取的方案。

3.3.3 在总体安全观下,完善跨境数据安全配套立法体系

数据安全作为国家总体安全观的重要组成部分,应在外商投资企业安全审查、出口管制法、网络安全法等方面予以体系化综合考量,可以借鉴美国的灵活立法模式,针对特定的新问题予以立法回应,以保护个人数据的跨境安全。

3.3.4 发展完善数据领域的阻断法,积极应对他国的长臂管辖

美国、欧盟地区域内法的规定使其数据主权向域外扩张,其域内法的适用不仅有可能使中国企业被波及,同时还侵犯了中国的国家主权。应当采取相应的措施应对GLOUD法案、GDPR等他国的长臂管辖规则。《数据安全法》第36条虽然对长臂管辖规定了阻断措施,但其规定过于笼统且有局限,不能有效对抗域外法的长臂管辖。因此,可以通过编撰相关国家涉及长臂管辖的法律附录,明确出于各种目的的长臂管辖并否认相关条款的域外效力。数据处理者应当向国家主管机关报告获得审批后才需遵守他国的相关要求。此外,他国行使长臂管辖权时不仅会导致国家间法律适用和管辖权的冲突,也会给相关主体带来损害。以跨境数据证据调取为例,企业遵守中国的法律则有可能会受到域外国家的强制性制裁,因此在阻断他国长臂管辖的同时亦应规定企业相应的救济途径,以免加重企业的责任负担。

3.3.5 积极参与国际治理规则的制定,为推进全球数字治理贡献中国智慧

国际层面的双边和多边数据跨境协定的谈判与合作亦是进行跨境数据流动安全治理的重要组成部分。建议中国可以在与欧盟等国家或地区的国际磋商或政治谈判中更多地涉及数据流动的相关问题,在寻求双方对数据安全问题共识的基础上,探索两地间数据跨境流动的方案,为彼此提供多样化、合法有效的数据跨境流动渠道。同时也建议中国可以借助区域全面经济伙伴协定(RCEP)、亚太自由贸易区(FTAAP)等区域谈判寻求建立符合中国利益的跨境数据流动规则。随着中国在国际事务中地位的提高,中国更可以运用博鳌亚洲论坛、“一带一路”战略等开启有关区域性的数据跨境流动规则的合作协议或规则的磋商与谈判,通过区域性的数据流动协议解决数据流动的问题。在多边层面,当前WTO缺乏明确地规制跨境数据流动的相关规则,因此通过国际协调借助WTO平台构建跨境数据流动国际规则,促进数据在全球范围内安全而自由流动也是数字贸易高速发展背景下的要求。中国应积极主张在国际贸易协定中嵌入安全条款,从而维护数据安全。

4 结论

安全与发展的平衡应当是跨境数据流动治理需追寻的目标,只有兼顾安全与发展的治理才能在保障本国国家安全的同时适应数字贸易时代的要求。纵观各国的跨境数据流动安全治理,印度采取的强有力的数据本地化措施过于重视安全忽视了发展,且有借安全为名侵害他国企业合法投资利益的倾向;欧盟的治理表现出完善的域内规则是争取国际话语权的基础;而美国的数据治理则扩大了国内法域外适用的范围,未做到尊重他国的数据主权。因此,中国在借鉴他国可取经验完善域内的跨境数据流动安全治理时,也应避免他国与中国国情

不符的实践,同时还需采取相应措施防止他国治理侵犯中国国家主权。除了国内层面对跨境数据流动安全治理的完善,在国际层面应充分利用自身在跨境电子商务领域的优势进行双多边的国际合作,在大国互信的基础上构建公正的数据安全流动全球规则。

参考文献(References)

[1] Mitchell A D, Mishra N. Regulating cross-border data flows in a data-driven world: How WTO law can contribute[J]. Journal of International Economic Law, 2019, 22(3): 394-395.

[2] Anupam C. Data nationalism[J]. Emory Law Journal, 2015(3): 678-739.

[3] 张舵. 跨境数据流动的法律规制问题研究[J]. 社会科学, 2018(1): 116-119.

[4] 彭岳. 贸易规制视域下数据隐私保护的冲突与解决[J]. 比较法研究, 2018(4): 176-187.

[5] 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): 130.

[6] 胡文华, 孔华锋. 印度数据本地化与跨境流动立法实践研究[J]. 计算机应用与软件, 2019, 36(8): 307.

[7] 王瑞. 欧盟《通用数据保护条例》主要内容与影响分析[J]. 金融会计, 2018(8): 17-26.

[8] Christopher Kuner. 欧洲数据保护法: 公司遵守与管制[M]. 旷野, 杨会水, 李晓娴, 等 译. 北京: 法律出版社, 2008.

[9] 弓永钦, 王健. APEC与欧盟个人数据跨境流动规则的研究[J]. 亚太经济, 2015(5): 9-13.

[10] 王融. 大数据时代——数据保护与流动规则[M]. 北京: 人民邮电出版社, 2017: 270.

[11] 刘天骄. 数据主权与长臂管辖的理论分野与实践冲突[J]. 环球法律评论, 2020, 42(2): 189.

[12] Schrems M. The privacy shield is a soft update of the safe harbor[J]. European Data Protection Law Review, 2016, 2(2): 148-150.

Research on the security governance of cross-border data

DONG Jingbo

Faculty of International Law, China University of Political Science and Law, Beijing 100088, China

Abstract Data security governance rules are essential for cross-border data flow. Based on the analysis of cross-border data flow security governance rules of typical countries and bilateral and multinational treaties, China's cross-border data flow security governance rules are studied and relevant suggestions are provided. Firstly, we should refine relevant regulations and improve the data classification supervision system; at the same time, we should improve the blocking law in the data field to avoid the long arm jurisdiction of other countries. Secondly, it is necessary to actively participate in the formulation of international cross-border rules for data, embed data security clauses into international economic and trade rules, and further promote the achievement of global data security flow rules.

Keywords data security; data sovereignty; cross-border data; security governance

(责任编辑　傅雪)