

# “双循环”格局下中国数据跨境制度创新研究

李晶,张靖辰

(厦门大学知识产权研究院,福建厦门 361011)

**摘要:**数据跨境制度是“双循环”格局下数字经济发展之需。通过对中国香港特别行政区、新加坡、爱尔兰及美国数据跨境制度与理念的考察,以期构建中国数据跨境制度框架。数据安全是中国数据跨境制度的根本遵循,根据立法者对数据分类的重要性标准,可将数据分为关键数据、非关键个人数据、非关键商业数据。对关键数据跨境应设置安全评估程序,严格限制流动;非关键个人数据可根据“白名单”规则与非“白名单”规则实现数据安全保障与有效跨境流动;非关键商业数据可基于备案制度提升行业自律,实现高效跨境流动。在未形成既定数据跨境国际规则时期,中国应积极参与国际规则制定,避免他国激进政策对中国的不利影响。

**关键词:**数字经济;数据跨境;数据安全;数据跨境效率;制度构建

**中图分类号:**F49 **文献标识码:**A **文章编号:**1671-2404(2021)102-0041-07

时代的更迭引发宏观趋势的涌动,经济高质量发展正处在新旧动能转换之时。科技产业变革下,数字经济正在重塑世界发展的基础动力。信息数据是数字经济的基础生产资料,不依赖于地理条件的数据则是基础生产要素,推动国际合作,扩大高水平开放是数字经济发展的应有之义。当代科技研发与经济贸易具有海量数据需求,充分释放数据经济潜能具有重要意义。在国内与国际双循环相互促进的新格局下,数据跨境逐步成为商业活动的必要需求。但数据跨境所引起的国家安全、个人隐私等问题亦不容忽视。数据跨境规则作为数据活动基础已受到各国重视,中国尚处于规则构建的积极探索阶段。本文在《网络安全法》与《个人信息保护法(草案)》的基础上,结合境外地区已有规则,进一步探讨中国契合双循环格局的数据跨境规则。质言之,如何实现数据经济效益与风险防控平衡是数据跨境问题治理之本。

## 1 中国数据跨境经济与制度概述

### 1.1 数据跨境是“双循环”格局下数字经济发展的必然要求

2020年5月14日,中共中央政治局常委会会议首次提出要“充分发挥中国市场规模优势和潜

力,构建国内国际双循环相互促进的新发展格局。”2020年8月24日,习近平总书记在经济社会领域专家座谈会上提到“要推动形成以国内大循环为主体、国内国际双循环相互促进的新发展格局。这个新发展格局是根据我国发展阶段、环境、条件变化提出来的,是重塑我国国际合作和竞争新优势的战略抉择。”可以说,这一新发展格局是科技革命、经济全球化退潮、中国地缘政治风险上升的必然趋势。

延循这一发展趋势,在传统经济陷入“存量博弈”泥淖的全球格局背景下,数字经济发展将承担着“双循环”格局中“新赛道”的核心功能。这具体体现在三个方面:数字经济产业化、传统产业数字化与经济治理数字化。<sup>[1]</sup>进言之,数字技术的创新实现了数字驱动的市场发展,其开发数字产品的同时,还数字化了传统产业。而且,国家基础设施的数字化升级,亦为产业治理的提供了数字化工具,提高了治理能效与社会环境。数字经济中,数据作为基础要素无时无刻不在产生,同时数据承载的信息作为数字经济的风向标,又时刻运用于数字经济发展之中。中国基于超大规模市场的潜力和优势,实现国内国际双循环需要有效联通国内市场与国际市场,因而数据跨境成为了数字经济双循环发展的必要活动。

以双循环为目标,推动中国数据跨境流动是数字经济发展的基本追求,亦是全球发展的总体趋势。数据跨境是指数据在国际层面的流动。<sup>[2]</sup>从经济学角度,数据流动是数据价值得以实现的方式,亦是推动数字经济发展的中坚路径。数据跨境有助于跨国

收稿日期:2020-11-01

作者简介:李晶,助理教授,法学博士,硕士生导师,主要从事知识产权法与数据法等方面的研究;张靖辰,硕士研究生,主要从事知识产权法与数据法等方面的研究。

企业提高资源利用能效,促进市场竞争,提升消费者权利保护。中国2019年数字经济增加值规模达到35.8万亿元,跃居世界前列。<sup>[3]</sup>在全球跨境贸易逐渐消沉的趋势下,国际数据跨境量却在激增,在全球资本流动价值创造中占比颇重,其不仅促进生产率增长,还提高了劳动力和资本使用量,但中国数据流动指数却排名较为靠后。<sup>[4]</sup>究其原因在于中国数据跨境制度有待完善。而且,时下数据跨境问题研究多集中于个人数据,<sup>[5]</sup>因此,应兼顾非个人数据,以保障数据安全为必要条件,以推动数据跨境为价值追求而构建中国数据跨境制度。

## 1.2 中国既有数据跨境制度采取严格管理型治理思路

中国数据跨境治理实践相较欧美国家起步较晚,且相关政策尚未实现体系化和细分化。但中国基础数据体量庞大,信息技术发展较快,时下面临“弯道超车”的历史机遇。<sup>[6]</sup>数据跨境作为全球视阈下的问题,与本国和外国科技发展、政策理念等密切相关。中国数据跨境治理理念、治理模式与欧盟、美国等有所不同。中美欧的数据跨境治理模式可分为三种类型,中国属于管理强化型,美国属于自由竞争型,而欧盟则属于管理与自由结合型。<sup>[7]</sup>管理强化型的特征是明确个人责任、严厉打击违法行为、重视网络空间秩序;自由竞争型的特征是共享数据、追求经济利益;管理与自由结合型的特征是重视保护隐私、同时注重经济自由竞争。<sup>[8]</sup>管理强化型在时下符合中国的本土环境和国家利益,但基于数据跨境的现实需求及发展趋势,或许中国在日后需重新审视相关制度安排并作出相应调整。

《网络安全法》第37条对关键信息基础设施收集的数据(简称“关键数据”)做出本地化要求,构建了中国数据出境的基本管理框架,体现了中国对数据跨境治理的管理型理念。《网络安全法》出台前,中国《保守国家秘密法》第25条规定了国家秘密禁止非法出境;以及各行业主管部门通过如《征信业管理条例》等对非国家秘密数据的跨境活动进行针对性规范。可以说,对于重要性较高的数据,中国一贯采取严格管理的治理方式。

《网络安全法》出台后,2020年10月21日中国《个人信息保护法(草案)》(简称“《草案》”)公布并公开征求社会公众意见。《草案》第三章制定了“个人信息跨境提供的规则”,中国版的个人信息跨境

规则已逐渐清晰。《草案》第三十八条规定了因业务而需要向境外提供个人信息的,需要具备以下条件之一:国家网信部门组织的安全评估;专业机构进行的个人信息保护认证;与境外接收方订立合同;法律、行政法规或国家网信部门规定的其他条件。上述各项条件皆在于保障个人信息安全。同时,第三十九条对个人信息跨境作出了“单独同意”的条件要求。总体来看,中国对于个人信息跨境规则采取了“同意加安全”的基础跨境规则。同时,第四十一条对于国际司法协助所需要的数据跨境作出了审批制安排。第四十二条与四十三条则是对于损害国家安全、他国歧视性做法的防御性制度。

《草案》延续了中国严格管理型的数据跨境治理倾向,表面上与域外其他国家的制度安排相比较为“保守”。其根本原因在于数据跨境利益牵扯与风险防范的复杂性。但如上文所述,数据跨境是数字经济发展的必要活动,推动数字跨境是发展的最终目标。因此构建便利数据跨境流动的制度是推动发展的应有之义。但目标亦是挑战,数据流动安全可控是制度调整的必要前提,便利数据跨境流动机制应同时兼具安全保障机制。在确保数据安全的基础上,可对制度安排做出适应性调整,以实现数据安全有序的跨境流动。

## 2 境外国际数据中心数据跨境治理的比较分析

### 2.1 香港特别行政区:自由流动与合理限制相结合

中国香港特区将数据自由流动原则与合理限制原则相结合。香港《个人资料(隐私)条例》第3条确立了数据处理、使用等行为的根本要求,规定未经个人资料当事人的书面同意,不得将数据用以新的用途,仅可用于收集个人资料的初始用途或直接相关的用途。在此基础上,于第33条第2款规定了个人资料出境条件,满足条件之一即可进行数据跨境。香港数据跨境制度构建具有三项重要考虑因素,其一为目的地数据保护标准;其二为资料当事人利益;其三为数据安全。

第一,针对目的地数据保护标准,香港设立了“白名单”及其配套规则,通过香港专门评估而确定可以对数据提供充分保护的司法管辖区,并在“白名单”范围内予以数据跨境自由。在香港未评估地区,则可根据评估标准再确定数据是否可流向该目

的地,需确保有合理理由相信目的地具有相似资料保护制度。第二,针对资料当事人利益,个人同意是数据跨境的许可条件之一。以及,若有合理理由相信数据跨境可以避免对当事人的重大不利情形,亦可基于对当事人的权益保护而允许数据跨境。第三,针对数据安全,在已采取一切合理措施确保资料在跨境目的地不会被以任何方式收集、处理等,则可进行数据跨境。以及,若资料本身不在保护范围之内,则当然亦可进行数据跨境。

可以说,香港数据跨境制度以确保数据安全为条件,从而同时确保数据安全与数据跨境效率。这与中国对数据跨境治理理念基本一致,香港制度框架也因此可以起到借鉴意义。但是,香港未对关键数据作出特别限制,若借鉴香港数据跨境制度,则需设置较高确立标准的“白名单”从而确保关键数据的跨境安全。不过,考虑到中国的数据体量,在制度借鉴时有必要对此作出相应变通,而非直接进行制度移植。同时,有必要注意的是,香港对于本地数据保护亦非常重视,这也是能够与外国实现数据跨境往来的基础。只有在本国制定并执行了充分的数据保护标准,才可为外国所认可并作为数据自由入境地。

## 2.2 新加坡:高标准保护要求之上允许自由流动

新加坡基于高标准数据保护要求而适用数据自由流动原则。新加坡《个人数据保护法》第26条及《个人数据保护条例》第9条确立了新加坡数据跨境制度。由新加坡向境外转移数据,需确保数据接受方受到能够对数据提供与新加坡相对等保护的“强制性法律义务”。根据《个人数据保护条例》第10条,“强制性法律义务”是指数据接收方受到任何法律的约束、或根据数据跨境流动订立的任何合约、或具有约束力的公司制度以及其他任何具有法律约束力的文件。

作为补充,以下情形可被视为已存在“强制性法律义务”:数据当事人同意;为应对威胁到数据当事人或第三方的生命、安全、健康的紧急情况所必需;数据控制人为履行合同所必需;为国家利益或数据当事人利益所必需、正在传输中的数据、公开的数据。此外,新加坡隐私委员会可以根据任何组织的申请,以书面形式豁免对该组织数据跨境的限制。而且,新加坡并未要求数据跨境需取得行为许可,这意味着数据跨境活动符合上述规定时即可相对高效

地开展。

新加坡将“强制性法律义务”设定为数据跨境原则要求,但是过度抽象性的规则不具有实际可操作性。因此,在实践中得以更多应用的是新加坡《个人数据保护条例》第9条所列明的上述补充情形。可以说,新加坡对数据跨境设置了较低的要求,通过促进数据流动而提升数字经济效益,但也因此而提升了数据的不确定性。比较之下,中国对数据跨境相对“保守”的理念与新加坡并不相符。但这并非意味着新加坡数据跨境制度对于中国无可借鉴之处,对于不必进行安全评估的数据可借鉴新加坡而进行制度构建。

## 2.3 爱尔兰:“外严内松”的治理理念

爱尔兰《数据保护法》是首个欧盟境内贯彻欧盟《一般数据保护条例》的国内立法,推动了爱尔兰数据保护现代化与欧盟数据保护体制化。个人数据保护在欧盟属于基本人权,因此欧盟始终将个人数据保护置于重要地位,<sup>[9]</sup>严格限制数据跨境流动。在相关制度方面,爱尔兰《数据保护法》与欧盟《一般数据保护条例》的内涵相一致。

爱尔兰《数据保护法》第96条至第100条规定了数据跨境规则。综合来看,对于非欧盟成员国,同时满足以下情形时可进行数据跨境:1、基于刑事活动需要,但公共利益相较于数据跨境更为重要时则不可适用;2、“白名单”数据跨境目的地的数据主管当局;3、“白名单”之外的第三国或国际组织数据主管当局能够对数据跨境提供适当保障措施,数据主体评估了数据跨境所有相关情况以确保数据受到足够保护;或,数据跨境是为了保护数据控制主体、数据当事人或其他主体的重大利益,如防止欧盟成员国或第三国的公共安全受到重大损害;或,数据跨境个案中基于刑事活动将数据转移至具有管辖权的主体是无效或不适当的,因而转移给其他主体的等,均需同时记载数据详细信息、跨境时间、数据接收方信息、跨境原因并报告欧盟委员会;

爱尔兰数据跨境制度似乎基于严格的限制而表现出数据本地化理念。但爱尔兰或者欧盟只是通过设置充分性数据保护要求,从而积极推动成员国数据共享,实现欧盟内部数据流通,这在欧盟早期区域性法律文件中体现的更为明显。<sup>[10]</sup>有所启迪的是,通过国际协议在区域性范围内实现数据共享不失为一种提升数据跨境效率的方式,这不仅保障了数据



安全,更是实现了数据双向流动,从而有效发掘数据经济效益;对非“白名单”国家或国际组织通过数据跨境报告要求的设置,可以提升相关部门对数据跨境活动的有效监管,同时还可以提升行业自律性,并降低监管成本。

#### 2.4 美国:推崇数据流动自由并强化本国数据主权

美国基于产业格局和世界地位考量,秉持商业优先及行业自律而采取宽松式立法。<sup>[11]</sup>因为严格限制数据跨境可能会给美国带来更大经济损失。<sup>[12]</sup>美国在联邦层面通过制度留白鼓励数据流动,但对关键数据跨境日渐苛刻,国家安全与遏制战略竞争对手发展是时下美国在数据跨境治理方面的重要考量。

美国在国际多双边协定中表现出数据跨境自由化理念。首先,《美韩自由贸易协定》、《美加墨协定》要求成员国避免限制个人信息的跨境流动。且《美加墨协定》未对数据跨境作出保留措施,即缔约国不论基于国家安全还是监管需要都不可妨碍数据跨境流动的自由。这契合了美国的数据跨境自由理念,但对别国数据安全与监管带来了挑战。<sup>[13]</sup>以及,美国曾参与的《跨太平洋伙伴关系协定》旨在最大限度地促进电子商务领域数据跨境流动。但如金融相关数据除外,且不适用于政府采购,以避免国家数据与商业数据交叉所引起的国家安全问题。还有,美国与欧盟达成的《安全港协议》与《隐私盾协议》相继失效,原因在于欧盟认为上述协议并不能对数据提供充分保护。但欧盟与美国仍通过标准合同而实现数据跨境。

随着美国单边主义的推行,美国开始从数据跨境多边治理转型为单边限制,以国家安全为由对关键数据作出严格跨境限制。美国通过发布《外国投资风险审查现代化法案》的实施细则,将关键技术、关键基础设施、敏感个人数据等相关投资均纳入国家安全审查范围,将受到管控的数据进行本地化储存。同时,美国通过《澄清域外合法使用数据法案》扩张本国数据主权,苛刻地限制别国对储存在美国数据的提取。因此,时下美国一方面基于经济发展角度推崇数据跨境自由,抨击别国数据本地化政策,而另一方面则基于国家安全限制本土数据出境,并通过域外执法政策而强化美国数据主权。

可以看出,美国对关键数据的重视程度在本质上与中国存在一定相似之处,即严格限制关键数据

跨境,对非关键商业数据依然秉持自由化理念。但美国在国际层面表现更为强势,积极通过多双边协议以破除别国数据本地化市场壁垒。事实上,美国通过与他国缔结多双边协定,亦使得缔约国成为美国对数据跨境治理理念的推广者,以将美国的政策主张融入其他新达成的国际协定中。<sup>[14]</sup>因此,基于这一国际因素,中国不仅需严格限制关键数据出境,确保国家安全;更需积极参与或推动国际协定中数据跨境制度的达成,从而影响并主导数据跨境国际规则发展。

### 3 中国数据跨境治理的框架设计

全球化进程中,数据跨境规则发展分为3个阶段,1.单边规制阶段:各国根据本土环境制定政策;2.区域治理阶段:主要国家通过多双边协定形成数据跨境流动网络;3.全球阶段:形成全球化数据跨境体系,目前多国正处在单边规制完善阶段和区域治理萌芽时期。<sup>[15]</sup>可以说,全球阶段之前,数据充分保护、数据跨境自由与国家数据主权三者难以兼具,究其原因则是国内政策与国际协调的天然冲突。<sup>[16]</sup>全球化数据跨境体系必然在各国冲突与妥协中逐步发展。因此,结合各国数据跨境制度发展与国际体系发展趋势,对中国数据跨境制度构建作出如下建议:

#### 3.1 跨境数据分类管理

数据跨境问题上,进行数据分类管理不仅是政策方向,亦是现实需要。中国《网络安全法》第37条确立了关键数据本地化要求。从《关键信息基础设施安全保护条例(征求意见稿)》第18条可以看出政府数据、敏感个人数据、关键设施收集的数据均属于关键数据。事实上,在发生网络安全事故时可能影响重要行业正常运行,对国家政治、经济、科技、社会、文化、国防、环境及人民生命财产造成严重损失的系统都将被认定为关键信息基础设施。<sup>[17]</sup>而且,中国《网络安全法》立法者在数据分类问题上,并未严格按照国家数据、商业数据与个人数据的分类方法,而是根据数据不同的重要性着手,只要可能涉及国家或公共利益的数据,皆应被视为重要数据。<sup>[18]</sup>因此,遵循这一数据分类思路与制度方向,本文基于数据重要性、监管成本、制度可操作性等因素对数据进行以下分类:

一、关键数据,关键数据具有更高的数据重要性,其不仅包括公民敏感信息与重要行业数据,还包

括政府数据与国家数据。此类数据与公民权利、公共利益、国家安全紧密相连。二、非关键个人数据,关键个人数据包括如医疗健康等重要数据可以通过扩充解释而涵盖关键数据内,对此类数据的分离可有效提升个人数据的跨境效率,同时兼顾了公民权利保护。三、非关键商业数据,关键商业数据包括如金融数据等同样可受到关键数据的涵盖。非关键商业数据可包括如数字产品信息、经脱敏处理的衍生数据等。多国在数据跨境制度上主要聚焦于个人数据,亦是基于商业数据的特性而赋予其更大跨境自由。

以数据重要性为分类标准,以数据外在形式为分类框架,在数据跨境问题下将数据分为关键数据、非关键个人数据、非关键商业数据三类。这可避免如澳大利亚、日本等国过于细碎的数据分类范式,从而提高制度在实践中的可操作性。<sup>[19]</sup>

### 3.2 数据跨境规则框架构建

其一,针对关键数据。在无充分保护的前提下,数据跨境自由程度与国家安全性呈反比关系。美国虽推崇数据跨境自由,但对于关键数据却反其道而行,设置了严格的数据跨境限制条件。结合中国数据体量现实状况,以及政策理念倾向,中国对关键数据应继续严格适用本地化治理方案,对于确实有出境需求的,则依据相关规定进行安全评估。

其二,针对非关键个人数据。非关键个人数据的跨境活动牵扯权益更为复杂,各国制定的相关规则也有所差异,但根本目标则是兼顾数据安全与跨境效率。通过对域外考察可以发现:1、“白名单”规则不失为一种兼顾二者的制度,中国可予以借鉴。但“白名单”规则要求中国本身制定较为充分的数据保护制度,否则难以实现数据双向流动。又由于数据制度在各国发展速度较快,基于全球化商业环境,有必要以固定周期动态化更新“白名单”以契合商业需求。以及为了确保“白名单”规则的实施,还需对行政监管、救济方式等方面作出配套制度。2、对于非“白名单”情形,应先确立可自由流动的情形:如数据当事人真实同意、为保障数据当事人切身利益、为保障公共利益、刑事程序需要等。目前中国《草案》将“个人同意”作为数据跨境“门槛”,相较略为苛刻。为保障数据安全,可借鉴爱尔兰的报告制度,要求数据转移主体书面记录数据详细信息、转移时间、数据接收方信息、数据转移原因等;同时为

提高数据跨境效率,在事前可要求相关部门仅进行形式审查,而在事中与事后进行实质审查。3、对于非“白名单”情形,且不属于上述许可情形的,基于数据安全考虑,则应要求数据转移主体作出事前报告,相关部门进行实质审查。

其三,针对非关键商业数据。由于其不涉及关键数据及个人数据,因此,基于其妨害国家安全、公共利益以及个人权益的可能性较小,可予以较高级别的跨境自由。但绝对化的自由势必对数据安全造成威胁,特别是在多类数据混合的情形下。因此,可借鉴新加坡的相关制度,要求非关键商业数据跨境需具备必要情形:商业合同需要、企业发展必要等。同时,对数据跨境活动在相关部门予以备案,相关部门可在必要时进行审查。备案制度不仅未影响非关键商业数据的跨境自由,还可通过行业自律而提升数据安全性。

### 3.3 积极影响或主导国际规则发展

通过国际协定完善中国数据跨境活动已受到研究者的普遍认同,但协定缔结目标还应进一步深化。欧盟的治理思路在于通过欧盟体系制度的一致性,逐步将欧盟标准发展为世界标准,看似欧盟秉持着严格的被动方案,但事实上起到了化被动为主动的效果,这不仅充分保护数据安全,更可有效对抗美国数据主权扩张。<sup>[20]</sup>美国亦有相似之处,即致力于破除他国数据跨境壁垒,推行美国数据跨境自由理念。因此,相关国际协定的缔结不仅是为了推动本国数据跨境活动发展,亦是各国推行本国数据跨境治理理念的重要方式,从而实现各国对国际规则发展的影响或主导。

在时下数据跨境国际规则尚未达成统一的时期,中国更应积极完善本国数据跨境制度,参与或推动国际数据跨境规则的发展。否则,不符合中国理念的既定国际规则必然对中国数据安全产生威胁。国际多双边协定多是各国基于已有的政治互信、经济合作和地缘政治需求所达成。<sup>[21]</sup>在欧盟与美国数据跨境制度日渐成熟的现状下,中国结合本土国情而制定出“第三套”数据跨境制度自然难以被他国所直接接受。因此,通过借鉴他国既有且适合中国本土的政策,就有制度共同性而开展国际谈判是与此类国家进行协议缔结的有效路径。但在具体缔结过程中,应注重中国企业的海外利益,弱化如美国等所提出的数据主权激进政策。<sup>[22]</sup>同时,考虑到发展

中国国家关键基础设施、数据保护制度与理念等因素的发展现状,中国可通过兼容性协议,填补国家间数字鸿沟,并基于一带一路等战略协助此类国家的数字发展,从而亦可提升中国的国际影响力。

## 结语

为实现中国数据跨境制度的价值追求,相关部门还可结合具体政策制定数据跨境指南,提高企业数据合规意识;亦可建议企业设置数据安全官等职位,以专门处理数据问题。而且,通过如海南自贸区等试点探索数据权设立,从而优化数据治理亦是提升治理力度的方式之一。从经济学原理来看,一般均衡状态即可达到最大经济化。数据保护与数据效益之间的平衡把控,是数字经济发展的根本追求。

### 参考文献

- [1] 程实. 中国经济“双循环”的六大支柱[N]. 第一财经日报,2020-09-29(A11).
- [2] OECD. Declaration on Transborder Data Flows[EB/OL]. [2020-10-1]. <https://www.oecd.org/internet/ieconomy/declarationontransborderdataflows.htm>.
- [3] 中国信息通信研究院. 中国数字经济发展白皮书(2020年)[EB/OL]. (2020-07) [2020-10-01]. [http://www.caict.ac.cn/kxyj/qwfb/bps/202007/t20200702\\_285535.htm](http://www.caict.ac.cn/kxyj/qwfb/bps/202007/t20200702_285535.htm).
- [4] McKinsey Global Institute. Digital globalization: The new era of global flows[EB/OL]. (2016-02-24) [2020-10-01]. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows#>.
- [5] 黄宁,李杨.“三难选择”下跨境数据流动规制的演进与成因[J]. 清华大学学报(哲学社会科学版),2017,32(5):172.
- [6] 胡炜. 跨境数据流动立法的价值取向与我国选择[J]. 社会科学,2018(4):97.
- [7] 持永大,村野正泰,土屋大洋. サイバー空間を支配す

る者 21 世紀の国家、組織、個人の戦略[M]. 日本経済新聞出版社,2018:331.

- [8] 张晓磊. 日本跨境数据流动治理问题研究[J]. 日本学刊,2020(4):104.
- [9] 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):180.
- [10] 许多奇. 个人数据跨境流动规制的国际格局及中国应对[J]. 法学论坛,2018,33(3):130.
- [11] 黄宁,李杨.“三难选择”下跨境数据流动规制的演进与成因[J]. 清华大学学报(哲学社会科学版),2017,32(5):179.
- [12] 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]. 法学评论,2020,38(1):116.
- [13] 陈寰琦,周念利. 从 USMCA 看美国数字贸易规则核心诉求及与中国的分歧[J]. 国际经贸探索,2019,35(6):109.
- [14] 马光. 数据跨境流动国际规则的发展与我国的应对[J]. 国际法学刊,2020(2):98.
- [15] 张晓磊. 日本跨境数据流动治理问题研究[J]. 日本学刊,2020(4):91.
- [16] 黄宁,李杨.“三难选择”下跨境数据流动规制的演进与成因[J]. 清华大学学报(哲学社会科学版),2017,32(5):179.
- [17] 石静霞. 数字经济背景下的 WTO 电子商务诸边谈判:最新发展及焦点问题[J]. 东方法学,2020(2):74.
- [18] 洪延青. 在发展与安全的平衡中构建数据跨境流动安全评估框架[J]. 信息安全与通信保密,2017(2):59.
- [19] 胡炜. 跨境数据流动立法的价值取向与我国选择[J]. 社会科学,2018(4):99.
- [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]. 法学评论,2020,38(1):116.
- [21] 张衡. 跨境数据流动的国际形势和中国路径[J]. 信息安全与通信保密,2018(12):22.
- [22] 韩静雅. 跨境数据流动国际规制的焦点问题分析[J]. 河北法学,2016,34(10):178.

## Research on China's Cross-border Data Institutional Innovation under the "Dual Circulation" Pattern

LI Jing, ZHANG Jingchen

(Intellectual Property Research Institute of Xiamen University, Xiamen Fujian Province 361011, China)

**Abstract:** Cross-border data system is a necessity for the digital economy under the backdrop of the "Dual

Circulation" pattern. This paper, based on some research on system and concepts of cross-border data in Hongkong, Singapore, Ireland and the US, intends to build a system framework for Chinese cross-border data. Data security is the fundamental requirement for Chinese cross-border data system. According to the data classification regulated by legislators, data can be categorized into critical data, non-critical personal data, non-critical business data. For critical data, there should be security assessment procedures to limit its circulation; for non-critical personal data, its circulation should follow the "white-list" rule and non "white-list" rule to ensure its safety and efficient circulation; for non-critical business data, it can closely follow the register system and work according to the self-regulation rules to ensure the efficient cross-border circulation. When there lack established international rules for cross-border data, China should play an active role in rule making to avoid the possible negative impact of radical policies.

**Key Words:** digital economy; cross-border data; data security; cross-border data efficiency; system building