我国企业数据出境的安全监管问题研究*

焦小妹，沈本秋
（广州大学 公共管理学院，广东 广州 510006）

摘 要：数字经济时代，数据跨境流动成为常态。伴随企业数据跨境规模越来越大，所产生的隐私挑战与安全威胁也随之增加，研究企业数据出境的安全监管问题具有重要的理论与实践意义。立足于我国企业数据出境的安全风险，针对跨境数据采集、存储、传输与交换、销毁等环节出现的问题，多维度、系统化分析其深层原因。研究发现，我国企业数据出境存在监管制度供给不足、数据出境安全评估的分类分级标准有待完善、与国际社会对接不够、管理主体难以协同等问题。对此迫切需要实施出境数据全生命周期安全过程控制，对数据跨境流动监管机制进行扩容，健全出境数据分类分级制度，寻求国际规则制定中的衔接与共赢，建立多元主体联动协调的监管机制。

关键词：数据跨境流动；数据出境监管；数据全生命周期安全
中图分类号：G203　　文献标识码：A　　DOI：10.19358/j.issn.2097-1788.2022.05.004
引用格式：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(5)：22-29.

A study of the problems in security regulation of China's enterprise data cross-border transfer

Jiao Xiaomei, Shen Benqiu
(School of Public Administration, Guangzhou University, Guangzhou 510006, China)

Abstract: In the era of digital economy, the cross-border flow of data has become normal. Along with the increasing scale of enterprise data crossing borders, the privacy challenges and security threats generated have also increased. It is of great theoretical and practical significance to study the security supervision of enterprise data crossing borders. Based on the security risks of China's enterprise data cross-border transfer, this paper analyzes the deep causes of cross-border data collection, storage, transmission and exchange, destruction and other aspects in a multi-dimensional and systematic manner. The study finds that there are problems such as insufficient supply of regulatory system, imperfect standards of classification and grading for data cross-border security assessment, insufficient integration with the international community, and difficulties in collaboration of management subjects. In this regard, it is urgent to implement the whole life cycle security process control of outbound data, expand the regulatory mechanism for cross-border data flow, improve the classification and grading system for outbound data, seek convergence and win-win situation in international rule-making, and establish a joint and coordinated regulatory mechanism for multiple subjects.

Key words: cross-border data flow; outbound data regulation; full lifecycle security of data

0 引言

数据跨境流动，又称信息跨境流动、信息跨境转移，是指通过各种技术和方法，实现数据跨越国境（地理疆域）的流动[1]。数字贸易时代，数据流牵引和驱动着商品流、业务流、资金流及人才流等一系列全球贸易活动，数据跨境流动规模大幅增长，已成为促进全球经济增长的主要引擎。数据跨越国家地理边界时，地缘政治、产业竞争、数据主权博弈、数据泄露、非法传输等问题都可能出现，个人、企业和国家的数据权益亦会受到影响。出于数据安全性考虑，建立并完善数据安全监管机制已成为各国

* 基金项目：2018 年国家社科基金《大数据支持下的国际公共危机治理模式及中国方略研究》系列成果（18BGJ079）

的主要着力点。数据跨境包括数据出境和数据入境。相对于数据入境,数据出境风险更大,本文的讨论语境正是数据出境安全监管。我国“十四五”规划明确提出要建立跨境数据流动安全监管制度。近年来,我国陆续出台《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)、《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)等法律法规保障国家数据安全,但尚未出台完备的数据出境安全监管制度。我国目前的数据跨境流动监管机制与位居世界第二的数字经济规模仍不匹配。

国内学者主要从三大视角对数据跨境流动安全监管进行研究。一是从立法角度比较分析各国数据跨境流动的规制路径,发现当前国际上存在四种典型的立法取向:美国经济利益最大化原则下的宽松立法、欧盟人权保护原则下的严格立法、俄罗斯数据主权安全战略下的本地存取型立法、澳大利亚数据安全与发展利益均衡原则下的折中型立法[2]。其中,美国与欧盟在数据跨境流动领域已建立了相对完善的监管体系[3]。美国凭借信息通信技术和互联网企业实力优势采取了最为宽松的监管模式和最低限度的隐私权保护制度;欧盟基于尊重和保护人权的立法传统,采取了更高标准的个人信息保护和更严格的数据跨境流动监管规则[4]。第二种视角聚焦政策制定偏好,各国在数据跨境流动政策制定中会综合考虑跨境双方的数据处理技术能力、数字产业规模、数据安全保护立法、国际规则对接等因素,继而在宽松立法、严格立法、低保护立法、本地化存取型立法和折中型立法中选取最适合本国国情的数据跨境监管政策[5]。也有少数学者聚焦第三种视野,探讨数据跨境的安全风险与监管策略。有研究从金融数据跨境[6]、电商数据跨境[7]、粤港澳大湾区数据流动[8]等具体问题探讨机制与对策,也有研究从个人数据权益受侵害、国内数据资源流失以及国家社会安全受威胁的角度分析了数据跨境流动面临的风险[9],还有研究从国家安全、商业利益、个人信息保护三个方面分析了海量数据的跨境流动给我国带来的挑战[10]。

总的来说,国内学者对数据跨境流动监管的研究重点聚焦于法学和政治学视野,从政府管理视野进行的研究相对薄弱;在研究对象的选择上,主要集中于国家、区域、行业、个体的数据跨境流动监管,对企业数据出境合规监管的研究较少。目前,跨国企业在国际数字贸易中扮演着重要角色,深入剖析政府对企业在数据出境过程中的监管问题及原因,有利于更有针对性地加强对数据跨境流动的合规指导与安全监管。本文以企业数据跨境管理问题为导向,明确出境数据全生命周期安全,针对跨境数据采集、存储、传输与交换、销毁等环节出现的问题,从制度依据、分类分级标准、国际合作、机构协同方面分析深层原因,并为我国建立完善的数据跨境流动监管体系提供参考性建议。

1 我国企业数据出境的安全风险

在国内企业“走出去”和“一带一路”倡议的大背景下,境内企业海外上市、设立海外分支机构、海外并购、与境外企业合作等商务活动日益频繁,数据跨境流动需求显著增强。跨境数据不可避免地涵盖个人隐私信息、商业秘密和国家信息安全等敏感数据。随着数据跨境流动和使用规模越来越大,所产生的安全威胁与隐私挑战也随之增加。一些企业违反我国“数据本地化存储”的基本原则及相关行业数据出境管理规定,向境外提供大量敏感数据,给我国个人信息和国家数据安全带来了冲击和威胁。

1.1 外资企业数据出境带来安全风险

首先,我国关于数据出境的安全管理规则还不完善,导致外资企业在数据出境管理中存在不确定性。目前在中国运行的外资企业有 42.9 万家,外资企业为中国社会经济做出贡献的同时,企业数据跨境流动也给我国带来了数据安全风险。《数据安全法》《个人信息保护法》要求关键信息基础设施的运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者,在中国境内收集和产生的个人信息及重要数据应当实现存储本地化和跨境传输的安全风险评估。这两部法律明确了相关外资企业的数据安全管理责任与法律义务,但是对于外资企业的具体类型、数据出境安全管理的相关规则仍不明确,具体行业所涉及重要数据的定义、范围及认定程序也未厘清,使得一些外资企业在数据存储、跨境传输、数据销毁中存在许多不确定的因素。例如,不少外资企业的信息技术团队设立在境外,通过互联网访问并处理境内服务器上存储的数据来提供远程技术服务,而这种远程访问情形理论上也属于“数据出境”,在一定程度上亦会对境内存储的数据构成一定风险威胁。

其次,以美国为首的数字强国,通过“长臂管辖权”等举措,延展国内数据安全法的域外适用范围,获取源自我国的数据。美国 2018 年颁布《澄清海外合法使用数据法》(CLOUD ACT),秉承“谁拥有数据谁就拥有数据控制权”的理念,澄清了美国执法机构请求通信服务提供商所保管数据的地理范围,为其监管部门请求访问、程序调取美国公司存储在境外的数据提供了一个有利的机制。此举措将获取美国境外数据的行为合法化,从而避开了数据实际存储国的法律制度,该法案打破了以往跨国数据调取过程中遵循的数据属地管辖模式,构建了以实际控制权限为依据的标准框架[11]。这种“长臂域外管辖”与我国“境内存储+跨境评估”的管理规则存在矛盾,容易引发数据安全纠纷。例如,(中国)特斯拉(Tesla)汽车通过安装摄像头、激光雷达等传感器采集车内外环境,获得了人脸图像、个人语音、车辆行驶信息、道路信息等个人信息和敏感数据,并将上述数据传输至境外总部,这一行为严重违反了我国数据保护原则。特斯拉车主维权事件发生后,特斯拉才公开表示“今后在中国采集的数据会严格遵守中国的数据安全监管规定”。

1.2 境内企业海外上市、海外并购中的数据安全风险

近年来越来越多的国内企业在美国证券交易所上市融资。据相关数据显示,2021 年上半年,在美国纳斯达克或纽交所主板上市的中国企业就达 38 家。2020 年底美国通过《外国公司问责法案》(Holding Foreign Companies Accountable Act),要求赴美上市的外国公司披露额外的信息数据,如证明自身不被外国政府所有或控制,披露董事会里共产党官员姓名、共产党党章是否写入公司章程,从企业原始交易数据到形成审计结论的过程中使用的数据和材料等。因此,美国证监会可能根据自身的监督职责,要求我国赴美上市的公司提交我国数据安全管理所规定的限制跨境传输的敏感数据。由于不提供的企业可能需要承担巨额罚款,以及连续三年内达不到美国证监会信息披露要求的企业还可能面临强制退市的威胁,造成一些企业往往冒着违规风险提供企业相关数据。我国互联网企业掌握海量数据资源,很多涉及我国关键信息基础设施、地理测绘信息、人口健康、人类遗传等重要数据资源,一旦泄露出去,将给我国个人信息和国家数据安全带来重大隐患。

2021 年 6 月,依托“大数据”运行的滴滴出行在美上市。根据我国相关规定,该企业属于关键信息基础设施运营商,掌握大量用户隐私信息、国家道路概况信息等敏感数据。为保护个人数据权益、维护国家数据安全,中国网络安全审查办公室在审查中发现该公司有违法违规收集和使用个人信息的严重问题。更严重的是,这种大型数字平台企业在境外上市易引发数据安全风险,因为根据美国的《外国公司问责法案》的规定,中国企业在美上市需提供可能侵犯个人隐私和威胁国家安全的数据材料。滴滴事件过后,国家网信办发布《网络安全审查办法(修订草案征求意见稿)》,专门明确了对境外上市企业进行更严格的安全审查,但是该办法未明确已在境外上市的企业如无法通过网络安全审查会导致何种后果,而《网络安全法》仅规定了需停止使用数据并且进行罚款处罚,仍需完善相关配套制度并强化监管实践。

1.3 境内机构通过合作等方式将数据传输至境外

近年来,互联网企业非法收集使用用户信息,滥用、售卖或者大规模泄露个人隐私数据等严重侵犯数据权利的事件层出不穷,有些企业甚至将我国重要数据资源传输至境外引发数据安全风险。2015 年深圳华大基因科技服务有限公司被发现同华山医院与英国牛津大学共同开展的人类基因国际合作研究中,在未经许可的情况下将 14 万中国人基因大数据从网上传递出境。根据《2020 年中国互联网网络安全报告》,2020 年我国共发现国内基因数据通过网络出境 717 万余次,流向境外 170 个国家和地区,其中流向美国 273 万余次,占出境总次数的 38.1%[12]。为此,科技部依据《人类遗传资源管理暂行办法》等有关规定,对华大基因科技服务有限公司实施了行政处罚,其中要求销毁该国际合作研究中所有未出境的中国人基因大数据。此外,科技部在其官方网站还公布了 8 份 2015-2020 年间未经授权将部分人类遗传资源信息通过互联网传输到境外的行政处罚决定书。从行政处罚书的内容上看,企业或科研机构私自将中国人基因大数据传递出境,处罚仅是停止国际合作及销毁未出境的数据,对已出境数据造成的国家经济和数据安全损失难以追回。基因数据是我国重要数据资源,企业违规跨境传输基因数据等国家重要数据资源会给我国带来数据安全风险。

2 我国企业数据出境安全风险的成因

2.1 出境数据全生命周期下的监管制度供给不足

就出境数据全生命周期来看，从数据采集、存储、传输与交换到销毁，我国对于数据出境的监管主要集中于数据存储本地化和跨境传输的安全风险评估方面，对出境数据的采集、销毁过程中涉及的监管还不到位。我国早期关于数据跨境流动的管理规定散见于有关行业规范或指导性文件中，均要求保护个人信息数据和数据本地化存储。2017 年 6 月开始实施的《网络安全法》第三十七条规定关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。如确需向境外提供数据，应当按照相关规定进行安全评估。由此我国正式确立了“数据存储本地化+数据出境安全评估”的管理框架。

正因为我国目前的数据安全管理主要集中于本地化数据，对跨境数据监管覆盖较少，尤其是在跨境数据类型和重要级别、数据跨境安全风险评估、跨境数据应用后的删除与销毁等方面尚未出台完整的标准规范，使得企业普遍缺乏标准的数据规范指引，监管部门无法顺利开展数据出境的科学监管。虽然我国金融、卫生健康、交通运输等部门很早就结合行业需求对特定数据出境提出了要求，如《征信管理条例》《人口健康信息管理办法(试行)》《网络预约出租汽车经营服务管理暂行办法》等，也形成了行业数据归口管理的惯例，对其出境进行了限制性管理，但从具体的行业规范和管理条例来看，在数据本地化存储以后，并未对数据出境的具体情形进行细化分类，缺乏相应的程序性规定，即数据本地化存储以后是否允许出境或者出境的条件是什么并不清楚，对相关具有数据出境需求的企业和监管主体很难形成规范性指引。

目前，我国对于企业数据出境的安全审查是程序性审查，由企业先进行数据出境风险自评估，网信部门再基于制度办法进行审查，其审查对象并非是出境数据本身，而是数据企业围绕数据形成的文字材料，很少涉及功能性检查等实质性措施。除了各方信用情况可以通过查阅相关材料进行判断之外，其余评估项很难单纯依靠企业的自评估材料进行审核，对于审核评价的具体标准、指标也未见明确规定说明。并且，当前具有监管效力的评估制度办法主要是针对跨境的个人数据，还未正式颁布有效的其他类型数据的评估制度。近些年我国也相继出台了一系列有关数据出境安全风险评估的管理办法，如《信息安全技术 数据出境安全评估指南(草案)》《数据出境安全评估办法(征求意见稿)》等，逐渐完善了数据出境安全风险评估的管理框架，但这些管理办法都处于征求意见阶段，尚未真正有效落地实施。

2.2 数据出境安全评估的分类分级标准有待完善

目前我国在数据出境评估审查中，对数据跨境进行“一刀切”式的审查监管机制无法满足跨国公司业务数据种类繁多的跨境合规需求。除了重要数据与个人信息数据绝对禁止出境外，国家网信办发布的《数据出境安全评估办法(征求意见稿)》对其他数据均规定了较为严格的出境安全审查程序，明确了数据出境安全评估的流程、要点、方法等内容，包括履行“通知—同意”程序，构建“企业数据出境自评估+主管部门评估”的两级评估体系。这种将数据出境安全评估作为单一合规监管机制，无法与全球化的数字经济发展趋势相适应，难以支撑国际贸易中大规模的数据跨境流动。从以上监管规定来看，将大量原本基于开展市场经营活动的数据出境需求纳入安全审查范围，容易增加数据跨境传输的时长，降低数据的时效性，特别是在金融等对数据时效性要求很强的领域，15 个工作日的审查评估时限难以满足瞬息万变的金融数据出境需求[13]。

究其原因，主要是我国还未完善数据分类分级方法和标准。早期关于数据出境的管理规定主要集中于个人数据的保护上，随着全球数字贸易的进一步发展，数据跨境流动已从个人数据扩展至个人和组织数据层面，建立完善的数据分类分级标准非常必要。首先，关于“重要数据”的规定有待清晰和完善。《重要数据识别指南》只是规定了 27 个特定行业的重要数据，主要关注具体领域或行业内部数据，无法适用于全部数据类型。其次，对“敏感数据”的界定标准不完善。跨国企业的数据流动包括个人数据、产品数据、业务数据、物流数据等不同敏感程度数据的跨境流动。尽管《数据安全法》强调建立数据分类分级保护制度，但尚未直接明确具体的跨境数据分类分级标准，未能妥善区分除个人数据和重要行业数据外的其他商业数据，未明确个人数据的范围以及安全评估的要求、程序及方式，使得数据安全监管主体无法开展统一的管理和监督工作。

2.3 我国数据跨境流动管理与国际社会需要对接

我国签订的数据跨境流动国际合作协定较少,使得我国企业数据跨境流动面临双向合规难的困境。数据流动是全球性的,而立法与监管却是本地的,全球各地在数据安全监管方面出台的不同法规政策客观造成了数据跨境流动壁垒,增加了企业数据跨境业务的法律风险与合规成本。虽然我国数字经济发展已处于全球领先地位,但在数据跨境流动治理方面起步较晚,与数字贸易发展规模相比,在数据跨境流动领域的国际合作方面仍相对滞后。我国参与缔结的国际合作协议中有关数据跨境的条款较少,截至 2021 年 8 月,我国已与 26 个国家和地区签署了 19 个自由贸易协定。从协定内容上看,基本都包括了个人信息保护条款,但几乎都未涉及数据跨境领域的内容,仅在 2020 年签署的区域全面经济伙伴关系协定(Regional Comprehensive Economic Partnership,RCEP)中首次明确表示支持出于商业目的数据跨境自由流动,以及提出了数据本地化存储措施。RCEP 协定中关于电子商务的内容部分对计算机设施位置、采用电子方法跨境传送信息等作出了相应规定,但只是原则上的承诺。

美国、欧盟均是数据跨境自由流动的积极倡导者,主张将数据跨境自由流动引入双多边贸易谈判中。美国凭借已有的信息技术优势及相对健全的数据市场规则,在国际贸易谈判中把“数据跨境自由流动”列为协议条款,以降低主权国家利用数据安全保护立法设置的市场准入门槛,进一步实现对全球数据要素的跨境管辖。美国曾在“跨太平洋伙伴关系协定”(Trans-Pacific Partnership Agreement,TPP)中提出“在保护个人信息的前提下,实现全球数据自由流动。”欧盟制定《通用数据保护条例》(General Data Protection Regulation,GDPR)、《非个人数据在欧盟境内自由流动框架条例》(Regulation on the Free Flow of Non-personal Data)以减少欧盟内部数据自由流动阻碍,同时对欧盟外部实施高标准的数据保护要求,设置新的市场准入壁垒。我国数据管理体制难以与国际通行规则相对接。欧洲议会一项名为“中国个人数据保护管理体制”的调查结果表明,我国立法中缺少个人数据保护的国际通行原则,无法与欧盟数据保护规则进行紧密对接。

2.4 数据跨境流动监管主体之间缺乏协同

立法机关只能提供监管规则,但对于监管政策的选择和执行则要交由具体的监管部门加以落实。目前,我国数据跨境流动监管主体众多,国家网信办负责出台相关管理规章,审查企业申报的数据出境安全风险评估报告;工业和信息化部从工业和通信业行业管理视角出台数据出境的管理标准;各行业监管部门承担特定行业或领域的数据安全监管职责;公安机关、国家安全机关负责相应职责范围内的数据安全监管工作;网络运营者承担数据安全保护义务,实现数据存储本地化和跨境传输的安全风险自评估。

横向上看,数据跨境流动监管主体重复,易出现“多龙治水”现象,导致企业数据出境手续繁多、流程复杂、管理混乱等问题。例如,《数据安全管理办法(征求意见稿)》规定,网络运营者向境外提供重要数据前,要对安全风险完成自评估并经行业主管部门同意,行业主管部门不明确的,应经省级网信部门批准。而《数据出境安全评估办法(征求意见稿)》规定:“数据处理者向境外提供重要数据,应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。”从以上两个管理办法的条款中可以看出企业需要跨境传输重要数据时,网信部门和行业主管部门存在交叉监管的问题,而从现有规定上看,企业数据出境到底应该先报经行业主管部门同意还是应该先通过网信部门申报数据出境安全评估仍不够清晰。

纵向上看,目前我国尚未建立独立的数据出境监管协调机构。一直以来我国对跨境数据采取行业归口管理,这虽然强化了监管的针对性,但是一个企业产生的数据往往涉及不同的行业,各行业又分别适用于不同的监管办法和标准,行业监管机构仅在特定职能范围内发挥监管职责,因此容易产生沟通不畅、监管竞争的情况,存在协同不畅的问题。所以,在归口监管模式之下,多行业审核监管机制的实施必须建立协调机制,设立一个拥有最高监督协调权力的统一机构,以统筹各行业主管部门的审核职责,避免政出多门或监管漏洞等问题的出现。其次,已有法律规范仅明确了国家网信部门具有审查企业数据出境安全风险评估的职责,并未规定省市两级网信部门的审查许可责任。另外,中国目前缺乏专门机构对接国际数据跨境流动的有关事宜,代表国家参与数据流动的国际合作。

3 加强我国数据出境安全监管的建议

基于保障数据安全和促进数据开发利用并重的发展原则，我国针对企业数据出境中的违规行为和数据跨境流动监管存在的问题，亟需在数据存储本地化原则下对数据跨境流动监管体系加以扩容。应理顺数据出境监管流程，对企业出境数据全生命周期的各个环节实施过程控制，督促企业数据依法合规出境；进一步细化管理制度和标准规范，健全出境数据分类分级制度，为企业数据出境提供清晰的制度依据；合理对接相应的国际规则，加强数据跨境流动监管的国际合作，协调解决数据管辖冲突，保障跨国企业在全球贸易活动中的合法权益和我国数据安全诉求；设立独立的数据跨境流动监管机构，强化专门机构的管理协调职能，同时构建多元主体联动的监管机制。

3.1 实施出境数据全生命周期安全过程控制

《信息安全技术 数据安全能力成熟度模型》中将数据生命周期分为采集、传输、存储、处理、交换和销毁六个阶段。从政府监管角度来看，对企业数据出境的监管主要集中于数据采集、存储、传输与交换、销毁这四个环节，数据处理环节是组织在内部对数据进行计算、分析、可视化等操作，很少涉及外部交流，因此无需过分监管。

数据采集应该与已经出台的数据安全管理有关的上位法要求接轨，明确数据采集渠道、范围及方法，规范数据采集流程，同时明确数据处理者的数据采集隐私保护责任与义务，在采集数据前应履行充分告知义务，遵循“告知—同意；撤回—同意；拒绝”的采集规则，并根据具体行业数据采集要求落实，实现数据分行业、分类、分级采集，为接下来的存储、传输与交换、销毁环节做准备。行业主管部门应重点立足知情同意、公开透明、分类分级、主体参与等原则进行监管审查。

数据存储建议采用最小化方法，以避免将本身并不敏感，但与重要、敏感数据并存的数据包括在内。在个人数据存储上，可以借鉴印度的做法，选择中间路线本地化存储的做法，对个人数据进行分类分级，对一般个人数据不做要求，对敏感数据、关键个人数据严格进行本地化存储。行业主管部门应重点立足数据类型、数据存储介质安全等进行监管审查。

数据出境安全评估应该继续予以完善，借鉴国外数据分类经验，合理确定重要数据、核心数据的内涵和范围，对其可能影响国家安全、商业利益和个人权益的数据跨境采取审慎态度。根据数据出境的业务需求和监管需求制定数据出境评估框架，尽可能对接 WTO 规则，为国际数字贸易创造有利条件。加快修订和出台具有可操作性和明确性的数据出境安全评估实施细则，进一步明确数据处理者对数据出境风险自评估的法律义务，明确网信部门对数据出境安全风险评估的审查职责。

出境数据删除与销毁通常是指数据接收方的处理行为，是跨境数据生命周期的最后一环。数据与传统货物不同，出境后被滥用可能会导致对国内组织与个人的数据权益造成损害，甚至会危害公共利益和国家安全。应依照数据分类分级建立针对出境数据删除与销毁的处置规范和管理制度，明确数据销毁的场景、对象、方式及要求，行业主管部门应明确有关数据销毁的监管机构与职责，并出台行业数据销毁的具体操作标准与程序，实现对数据销毁的有效监管。

3.2 完善数据跨境流动监管的制度依据

一是从法制途径入手确立监管依据。顺应全球数字经济发展趋势，针对数据跨境流动的现实需求，持续完善数据跨境流动监管的法制依据。通过出台专门监管制度和规则明确数据跨境的定义及类型、“重要数据”等关键概念及范围、数据权属、数据跨境流动的处理规则、数据主体的权利、数据处理者的法律义务、监管部门的管理职责、国内与国际数据跨境安全规制的对接机制等。

二是确立出境数据全生命周期的监管制度。当前数据跨境流动监管制度主要是基于数据本地化存储原则的静态规则设计，对跨境数据的采集、存储、传输与交换、销毁这一系列动态过程监管不足，需要出台出境数据全生命周期合规监管制度。针对出境数据全生命周期进行合规监管，形成配套的实施细则，明确数据出境各阶段相关监管部门的管理职责。

三是试点探索中国特色数据跨境流动监管制度。借鉴国际经验，结合特定地区数据跨境需求，建立数据自由贸易试验区，以“个人数据”先行试验，继而引入企业“业务数据”。积极探索数据出境风险评估、数据安全保护能力认证、标准合同条款、“白名单”等机制，尝试在数据自由贸易试验区建立数

据跨境流动便捷通道,实现数据跨境安全有序流动、循序渐进、以点带面。鼓励数据自贸试验区开展数据海关监管创新,建立“数据海关”试点,构建权责清晰的数据跨境流动管理规则、组织体系、技术平台及服务体系,建立针对数据出境的“自检”“报关”“通关”等制度,并建立对“通关”后数据的持续保护机制。

3.3 健全出境数据分类分级制度

个人信息、重要数据、其他商业数据涉及的风险和所需保护的法益各有不同,应健全分类分级监管制度,确立宽严不同的数据跨境流动监管政策。

首先,对于个人数据出境,应当坚持市场导向,建议根据个人数据对公民隐私保护、商业利益和国家数据安全影响的差异,分为一般个人数据、敏感个人数据、关键个人数据三个等级,根据不同重要级别采取差异化的监管要求,同时通过合同约束、备案许可等方式,重点保障出境后个人数据主体的权益。

其次,对于重要数据出境,根据数据出境具体应用场景,综合考察数据出境后产生的风险及影响,对其跨境传输实施差异化监管。根据数据跨境传输后对国家安全造成影响的程度,确定高、中、低风险下分别采取禁止跨境传输、评估后限制跨境传输或跨境传输后持续安全监测、跨境传输后备案等不同的监管方式[14],并从组织层面和技术层面做好数据出境后的安全保障。

最后,对于其他商业数据,原则上允许自由流动,企业应该承担主要风险责任。对低级别、非敏感的普通商业数据支持跨境自由流动,以促进企业合资、跨境经营、多厂商跨境合作等国际数字贸易的发展;而对高级别、敏感的核心商业数据需重点监管,综合考量数据权属、业务需求、应用场景、安全防护等关键因素,做好数据出境外部规则的排查、梳理及跟踪,在保障数据跨境安全流动前提下促进数据的开发利用,最大限度地释放数据价值。

3.4 寻求国际规则制定中的衔接与共赢

在“一带一路”倡议下尝试与沿线国家开展数据跨境合作。考虑到国际上暂时难以形成统一、全面的数据跨境流动规则体系,我国应当充分利用“一带一路”建设的主动优势,在完善国内数据跨境监管体系的基础上,秉持开放合作态度,积极探索与沿线国家在数据跨境流动领域的合作机制,努力争取数据跨境流动国际合作的主动权。我国与“一带一路”沿线国家已经具备了相当程度的互信合作基础,应该积极推动签订区域数据流动协议,将数据保护、数字贸易政策与标准、数据跨境流动规则等作为双多边贸易协定的谈判内容。采取共同或相近立法原则及规范措施,推动形成共同认可的数据保护认证、标准合同条款等机制,建立由中国引领的区域数据流动互信合作平台。

加强与欧美发达国家在数据跨境流动领域的对话与合作。欧美发达国家依靠信息技术优势,坚持数据自由出境不受干扰。在此背景下,更需加强与欧美等经济主体在数据跨境流动领域的对话与合作。例如,可考虑参与亚太经济合作组织(Asia-Pacific Economic Cooperation,APEC)下的《跨境隐私规则体系》(CBPR)等国际协定,CBPR 主要规范的对象仍是在亚太地区的贸易中牵涉到个人信息跨境传输的公司,既包括专门从事跨境电子商务的企业,还包括一些金融、交通、通信设备制造等关键信息基础设施运营者[15]。参与有关数据跨境的国际协定,可以通过享受协定签署各方所达成的平等待遇,减轻企业数据跨境流动的双向合规负担,支持出于商业目的数据跨境自由流动,提高数据跨境流动的便捷性和安全性。

此外,还应该以《全球数据安全倡议》为基础,在数据存储本地化、数据跨境流动、数据跨境执法协调等关键事项上加强与世界各国的对话与合作。在尊重他国数据保护原则情况下,应坚持立足于我国有关数据保护的法律法规、国际条约与协定,根据数据跨境具体应用场景和适用范围,设计符合我国国家利益、保障数据安全、利于跨境贸易发展的执法数据调取方案。

3.5 建立多元主体联动协调的监管机制

设立专门的监管协调机构,加强对跨境数据全生命周期管理的整体规划和协同管理。基于数据跨境流动的特殊性明确专门监管协调机构的职能,包括但不限于:(1)进行数据出境业务登记。(2)对于企业出境数据涉及多行业、行业主管部门不明确或标准不统一的情况,进行统筹协调。(3)对于非法跨境传输国内数据的行为主体,依法进行行政调查与处罚;对非法跨境传输国外数据的行为主体,可作为传入方代表或监管机构向具有管辖权的境外法院提出涉外诉讼。(4)与其他国家的主管部门签订跨

境数据共享协议等合作机制，以降低数据跨境的法律风险并营造良好的营商环境。

实施多元主体联动监管。延续目前行业归口管理和网信部门负责安全评估的同时，在数据自由贸易试验区增加海关作为监管部门，实现多元主体联动、双保险监管，塑造具有中国特色的数据跨境监管模式。行业主管部门在专门监管机构的统筹协调下承担本行业、本领域出境数据全生命周期的安全监管职责。网信部门根据企业体量、数据内容、内部数据合规制度、数据重要程度、接收方保障能力等维度，探索适用于企业的安全评估路径，包括但不限于定期认证、逐次评估、标准合同等，建立自评估、联合评估、申报等准则规范。“数据海关”在辖区范围内执行对数据跨境传输的审核、评估、监管等职责，对数据发送、接收等相关组织的数据保护能力制定相应的安全评估路径，并对境内相关责任方开展定期审计等工作。根据相关组织能力与数据分类分级情况，对数据跨境的风险程度进行综合评定。通过数据托管中心的方式，探索在数据自由贸易试验区针对风险综合评定级别较高的数据采取“托管存储、规范使用、技术监管”的强监管模式。

4 结论

数字经济时代，面对企业数据出境的安全风险，迫切需要实施出境数据全生命周期安全过程控制，对数据跨境流动监管机制进行扩容，健全出境数据分类分级制度，寻求国际规则制定中的衔接与共赢，建立多元主体联动协调的监管机制。鉴于国际上短期内难以形成统一的数据跨境流动规则，我国应在完善国内数据跨境监管体系的基础上，积极探索与“一带一路”沿线等国家建立数据跨境流动合作机制，争取数据跨境流动国际合作的主动权。同时，加强与欧美发达国家在数据跨境流动领域的对话与合作。

参考文献

[1] 阿里巴巴数据安全研究中心，上海赛博网络安全产业创新研究院，上海社会科学院互联网研究中心.全球数据跨境流动政策与中国战略研究[R].2019：2.

[2] 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)：95.

[3] 崔静.欧美数据跨境流动监管的经验做法及我国的策略选择[J].经济体制改革，2021(2)：173.

[4] 胡炜.跨境数据流动的国际法挑战及中国应对[J].社会科学家，2017(11)：107.

[5] 魏远山.博弈论视角下跨境数据流动的问题与对策研究[J].西安交通大学学报(社会科学版)，2021，41(5)：114-126.

[6] 范思博.个人金融数据跨境流动的治理研究[J/OL].重庆大学学报(社会科学版)：1-17[2021-11-30].

[7] 吕淑敏.跨境电商数据监管政策研究[J].现代商业，2021(24)：41-43.

[8] 申明浩，滕明明，杨永聪，等.数据要素跨境流动与治理机制设计——基于粤港澳大湾区建设的视角[J].国际经贸探索，2021，37(10)：86-98.

[9] 王志杰.论我国跨境数据流动的监管完善——基于数据安全性与数据开放性的利益平衡视角[J].福建金融，2021(7)：11.

[10] 黄观清.数字贸易背景下我国数据跨境流动监管规则的构建路径[J].西南金融，2021(8)：77-78.

[11] 郑琳.美国《澄清海外合法使用数据法》及其影响与启示[J].现代情报，2021(1)：130.

[12] 国家计算机网络应急技术处理协调中心.2020年中国互联网网络安全报告[R].北京：人民邮电出版社，2020：55-56.

[13] 田翔宇.金融数据跨境流动的特殊规制[J].海南金融，2021(4)：56.

[14] 阿里巴巴数据安全研究中心、上海赛博网络安全产业创新研究院，上海社会科学院互联网研究中心.全球数据跨境流动政策与中国战略研究[R].2019：56.

[15] 中国信通院：《亚太地区(APEC)跨境数据流动规则的未来趋势》[EB/OL].(2022-02-22).http://www.caict.ac.cn/kxyj/caictgd/201804/t20180428_159191.htm.

(收稿日期：2022-11-12)

作者简介：

焦小妹(1998-)，通信作者，女，硕士，主要研究方向：数字政府、数据治理。E-mail：1250909588@qq.com。

沈本秋(1976-)，男，博士，教授，主要研究方向：大数据治理。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部