我国商业数据跨境流动合规治理的问题与完善

来小鹏　马诗雅

[摘　要] 数据经济发展全球化背景下，跨境数据传输愈发频繁，商业数据跨境流动在促进经济增长的同时，也引发了各国对个人隐私、国家安全的担忧。商业数据丰富的内涵特征加之外部环境的不确定性决定了商业数据跨境流动合规治理的必要性。应对现阶段在商业数据跨境流动治理方面存在的立法分散和企业合规难问题，我国应当完善商业数据合规法律体系，为企业商业数据跨境流动合规提供明确指引；设立专门、独立的数据跨境监督机构；构建商业数据跨境流动综合治理体系，为商业数据的跨境流动的监管提供切实保障；积极与世界主要国家和地区达成双边或多边合作，推动形成全球数据治理统一标准，减轻企业双向合规的压力。

[关键词] 商业数据；数据跨境流动；企业合规；数据治理；制度完善

[中图分类号] D63　　[文献标识码] A　　[文章编号] 1674-7453（2024）04-0043-11

DOI:10.14150/j.cnki.1674-7453.2024.04.004

引言

近年来，数据作为新型生产要素展现出巨大的资源潜能和经济价值，数据跨境流动合规治理问题引发了越来越多的关注。2024年3月22日，国家互联网信息办公室公布《促进和规范数据跨境流动规定》（以下简称《规定》），针对新形势下保障数据安全、维护个人信息权益，促进数据依法有序自由流动的现实需求，对数据跨境活动作出了明确指引，优化完善了现有数据跨境标准和程序。《规定》的出台顺应了我国数字经济高质量发展的趋势，适应了我国保障数据主权、维护国家安全的需要，体现了我国对数据跨境活动合法有序开展的重视。

[基金项目] 北京市法学会2023年市级法学研究课题“算法安全综合治理体系建构研究”（BLS(2023)B010）。

[作者简介] 来小鹏，中国政法大学民商经济法学院教授，博士生导师；马诗雅，中国政法大学民商经济法学院博士研究生。

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

商业数据是日益数字化的全球经济的核心，商业数据跨境流动被描述为“21世纪全球化的标志”和“维系全球经济的结缔组织”。[1]商业数据跨境流动是全球主要经济体之间商业贸易和通信不可或缺的重要环节。在我国不断加大对外开放的背景下，商业数据跨境流动成为继续推动数字经济发展的必然选择。

然而，商业数据跨境流动在为各国带来丰厚的经济收益的同时，也引发了一系列问题，对各国的国家安全、公民隐私带来负面影响。对此，各国相继从战略层面采取应对措施，通过出台数据跨境流动的相关法律，积极促成双边或多边协议等举措，对商业数据跨境传输活动进行治理。2018年，欧盟通过《一般数据保护条例》（以下简称GDPR），明确了数据控制者和处理者在开展数据跨境活动时的责任和义务，为数据流动的安全监管确立了标准。美国通过制定或参与双边、多边协定的方式，如《跨大西洋数据隐私框架》《APEC跨境隐私规则》等，积极促成与第三国数据的跨境自由流动。我国通过《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》）等基础性法律以及各项行政法规，为企业商业数据跨境合规提供了指引。随着商业数据跨境流动的政策环境趋于复杂，各国政府纷纷主张数据主权、网络主权，如何平衡数据安全与数据跨境自由流动，成为该领域面临的关键问题。我国作为数据大国，构建系统完善的商业数据跨境流动合规治理体系，在保障数据安全、保护个人信息权益的基础上促进商业数据有序自由流动，为企业做好商业数据跨境合规工作提供指引和保障，是当前需要关注的重点问题。

一、商业数据跨境流动合规的必要性分析

商业数据的重要性日益凸显，各国间的数字贸易往来日趋频繁，商业数据跨境流动在促进经济增长的同时也存在一定的安全隐患。结合商业数据的内涵特征以及对外部环境的考量，强调商业数据跨境流动合规确有其必要性。

（一）商业数据的内涵与价值

商业数据是企业等商业主体在其生产经营活动中积累的以电子或者非电子形式存在的信息、资料，[2]主要包括三个方面的要素内容：运营成本、战略规划以及用户联系信息。一般来说，企业用于市场营销、运营、人力资源或者是销售计划的任何数据信息都可以被视为商业数据。需要注意的是，此类信息中很可能会包含用户隐私信息或专有信息，企业应当采取有效的数据保护措施，做好数据合规工作，以防用户信息泄露。

当前，数字技术得到了普遍的应用，从数据源来看，商业数据类型丰富，既包括企业在经营过程中收集而来的与个人紧密相关的个人数据，也包括不涉及自然人权益的非个人数据。数据的“可识别性”是区分个人数据以及非个人数据的标准。[3]根据《个人信息保护法》的定义，个人数据是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种数据信息，不包括匿名化处理后的信息。非个人数据则是指无法识别出特定自然人的数据信息。从企业的角度来看，非个人数据可以被分为两大类别，一类是企业生产经营中产生的数据，比如企业财会数据、企业经营记录、日常管理记录等；另一类是企业对原始数据信息，通过深度分析过滤、提炼整合以及匿名化脱敏处理后获得衍生数据，如搜索引擎记录、用户偏好数据、潜在用户群等。[4]

随着商业数据市场价值的日益凸显，商业数

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

据成为企业的核心战略资源，企业通过云计算、区块链等前沿技术对数据进行深度开发和系统整合，形成具有经济价值的数据产品，通过市场交易由此获得可观的经济利益和商业价值。①我国于2022年11月发布的《中华人民共和国反不正当竞争法（修订草案征求意见稿）》中对商业数据作出定义，“本法所称商业数据，是指经营者依法收集、具有商业价值并采取相应技术管理措施的数据”。其中，“依法收集”要求经营者在收集数据，尤其是涉及个人隐私相关的数据信息时，必须依法、依规；而“具有商业价值”主要体现在经营者收集整合的数据可以为其带来商业利益，带来市场竞争优势，可见，商业数据之所以受到保护主要在于其市场意义与经济价值。

综上，商业数据逐渐成为社会经济发展中的关键要素。商业数据的内涵较为丰富，不仅包括商业信息还涉及与个人紧密相关的个人数据。因此，我国企业在进行商业数据跨境活动过程中要尤其注意依法依规，做好合规工作，防止关键核心数据泄露，避免侵犯用户个人隐私，保障数据安全。

（二）商业数据跨境流动的不确定性

数据跨境流动（Transborder Data Flows）这一概念最早在经济合作与发展组织（OECD）公布的《跨境数据流动宣言》中被作出解释，即“计算机化的数据或者信息在国际层面的流动”。[5]商业数据跨境流动意味着商业数据需要跨越地理边界，且处于可以被获取的状态。商业数据跨境传输具有体量大、速度快的特征，具备不确定性和不可控性。在商业数据跨境流动的过程中往往涉及不同国家或地区的数据处理者，而不同国家或地区的数据保护程度要求高低不一，数据处理者的数据保护能力参差不齐，一定程度上加剧了数据的不当使用和数据泄露的风险。[6]

结合前述分析可知，商业数据涉及商业信息、经营信息乃至用户个人信息，单个数据可能价值有限，但一旦形成数据集合，便会产生巨大的经济价值和社会价值，他人通过对商业数据集进行处理、分析便可以挖掘数据集合背后的经营信息，用户信息等。企业如果未能恰当履行商业数据跨境合规义务，数据分析结果将可能被不当利用，企业甚至社会公众的数据安全将由此受到威胁。商业数据的跨境流动在为企业带来巨大商业利益的同时也存在着极大的不确定性，存在泄露侵犯个人隐私、危害国家安全的风险。

（三）商业数据跨境流动合规的社会责任要求

合规义务在设立之初是为了企业通过约束内部员工行为促使其依法依规行事，实现自我监督，从而减缓公众对企业不信任的情况。[7]从企业的角度探究合规，其本质在于企业通过建立合理的合规计划，并保证计划得到有效执行，以实现自我管理，避免承担包括刑事诉讼、行政处罚在内的运营风险。与传统公司合规治理体系相同，企业商业数据跨境合规也是一套旨在预防、识别和应对合规风险的自我监管机制，企业应当依据数据领域的特定风险，对商业数据的跨境处理行为进行有效规制，围绕商业数据的合规管理构建数据保护、预防、监控等流程体系。[8]

企业社会责任理论是企业约束自身行为，履行合规义务的重要依据。企业社会责任理论是指企业政策、运营和行为要充分考虑投资者、消费者、员工等利益相关各方的利益，强调企业不但要对股东负责，而且要对其他利益相关方负责。[9]数字化背景下，生产组织活动呈现开放融合的特征，公共利益、社会诉求等因素被内化于企业的经营活动之中，成为企业的必要考量因素。同时，数字技术的发展为企业履行社会责任

①参见淘宝（中国）软件有限公司诉安徽美景信息科技有限公司不正当竞争纠纷案，浙江省杭州市中级人民法院（2018）浙01民终7312号民事判决书。

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

提供了便利，数字技术具备较高的包容性和普惠性，即便企业处于创业初期，也可以借助数字技术，通过商业模式创新向社会释放正外部性。[10]企业是社会的重要组成部分，兼具经济属性及社会属性，其数据处理行为将会对社会产生深刻影响。作为商业数据收集、处理、跨境运营的主体，企业在利用商业数据创造经济价值的同时，理应积极承担社会责任，保障公共利益、满足社会诉求。因此，企业应当规范商业数据的收集和处理行为，遵守数据输出国和输入国的相关立法规定，保障商业数据安全合法合规地跨境流动。

二、商业数据跨境流动的主要规制模式

据联合国贸易和发展会议的相关统计，在194个成员国中已经有137个国家或地区制定了数据与隐私保护相关立法，其中大多数包含跨境数据流动法律、法规或者相关政策规定。[11]部分国家和地区已经具备较为成熟完善的立法体系，并对数据跨境流动的国际基本格局产生了影响。

（一）以数据保护为核心的欧盟规制模式

欧盟地区很早就注重对数据的保护，在数据跨境流动治理方面比较有代表性。欧盟早期较多关注个人数据的保护，数据跨境治理方面主要强调对个人数据的规制。随着数字经济的蓬勃发展，数据的经济价值逐渐显现，欧盟出台了《非个人数据自由流动框架条例》《数据治理法案》《数据法案》等规范文件，弥补了非个人数据跨境监管的空白，形成了较为完整的数据跨境治理法律规范体系。

就数据传输而言，欧盟对于境内和境外采取了两种不同的规制标准，即对内鼓励数据的自由流动，对外则严格保证数据安全。[12]在成员国内部，欧盟确立了禁止成员各国借数据保护的名义限制数据在欧盟境内自由流动的标准，但针对数据跨境却作出了不同的规定，即禁止将数据转移到欧盟以外的地理区域，除非该国家或地区能够提供“充分”的数据保护。

对于个人数据的跨境流动，欧盟早在1981年就在《有关个人数据自动化处理的个人保护公约》中作出了规定，允许缔约国之间自由传输数据，同时对缔约方向非缔约方传输数据作出限制，仅针对特殊类型的数据，且要求非缔约方需提供同等保护。1995年欧盟《个人数据保护指令》（以下简称“95指令”）明确了个人数据的跨境自由流动仅限于欧盟成员国之间，而对于向第三国传输数据则作出了“充分性认定”的要求，即只有在第三国个人数据隐私的保护方面达到了足够的保护水平，才允许将个人信息向该第三国传递。此后，GDPR对“充分性认定”标准作了进一步明确。相较于95指令，GDPR对于“充分性认定”的评估增加了除国家外的特定区域及国际组织，但95指令所确立的规则继续有效。在评估第三国或国际组织对个人数据的保护程度时，GDPR在第31条中提出了相关的考虑因素，包括对基本人权的保护程度，是否存在独立且有效运作的监管机构，以及承担有关个人数据保护的国家责任或国际承诺等。可见，欧盟以保障境内个人数据安全为基本出发点，对个人数据跨境传输采取较为保守的态度。

在非个人数据的跨境流动监管上，欧盟也采取了“内外有别”的监管模式。对于欧盟成员国内部，《非个人数据自由流动框架条例》要求非个人数据成员国之间自由流动，但数据向域外流动方面则主要通过《数据治理法案》和《数据法案》加以明确。《非个人数据自由流动条例》对欧盟成员国实施数据本地化措施作出了限制，旨在降低欧盟内部数据驱动型经济的壁垒，促进非个人数据在欧盟境内的自由流动，以增强数据的可访问性与再利用性。[13]2022年通过的《数据治理法案》以及《数据法案》弥

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

补了欧盟非个人数据跨境监管的空白，均强调了欧盟内部数据的共享，而对于非个人数据向境外的传输，则表现出审慎的态度，通过扩张监管区域范围、设定严苛的审查标准、设置多样化的数据审核评估机构等形式，为数据的跨境流动设置了较高的壁垒。[14]

（二）以自由贸易为主导的美国规制模式

与欧盟不同，美国采取以市场主导、行业自律的分散式立法，在数据跨境流动上更加看重数据自由流动和经济利益，通过促进数据跨境维护信息优势，在与各国的贸易谈判中积极主张加入数字跨境自由流动相关条款。2004 年，美国推动构建了《APEC 隐私保护框架》，该协议成为亚太地区首份有关跨境数据流动规制的法律指导文件。《APEC 隐私保护框架》强调数据的自由流动，如协议要求各个成员体应尽可能采取恰当、合理的方法和措施，最大程度地避免甚至消除数据流动阻碍。随后，美国在美韩自由贸易协定以及 TPP 谈判中也相继加入了数据跨境条款。2019 年，美国与墨西哥、加拿大签订了《美墨加协定》（USMCA），试图进一步促进国际间的数据自由流动。

值得一提的是，即便在数据跨境问题上与欧盟有着不同的基本立场，美国依然积极与欧盟进行谈判，实现数据的跨境互联互通。鉴于欧美之间数据跨境流动的现实需求，美国与欧盟于 2000 年签署了《安全港协议》，美国企业只需要向美国商务部证明满足了欧盟要求的包括告知用户数据使用目的等在内的七项原则即可进行数据跨境传输。2016 年，美国与欧盟签订了《隐私盾协议》，对美国的数据保护提出了更高的要求，美国需要设立数据监察专岗、建立欧美联合审查机制等。2022 年 3 月，美国与欧盟达成了《跨大西洋数据隐私框架》，对美欧之间的商业数据跨境传输进行了重构，为更好地促进跨大西洋的数据传输奠定了基础。

三、我国商业数据跨境流动合规治理的潜在问题

我国在数据跨境流动规制领域起步较晚，在商业数据跨境治理方面仍面临一些问题。一方面，我国现阶段相关法律体系尚不完善，存在一些立法空白和交叉，不利于商业数据跨境合规治理工作的开展；另一方面，各国数据合规标准不断提高，企业履行合规义务需要同时兼顾数据输出国与输入国的相关法律制度，当前我国企业的数据跨境合规意识与能力还有待加强，商业数据跨境合规治理仍存在不少难题。

（一）商业数据跨境流动的立法呈分散式

当前，我国出台了众多涉及商业数据跨境流动的规范性法律文件，主要包括数据跨境流动统筹立法和个人信息跨境流动专项立法两大方面。数据跨境流动统筹立法强调确保国内数据的规范跨境，维护国家安全，要求企业将其在生产经营过程中产生的重要数据存储在境内，确因业务需要跨境传输数据的，应当根据相关规定，进行风险预测与安全评估。2017 年 6 月，《网络安全法》的实施将我国数据治理纳入法治轨道时代，数据安全被纳入到国家安全的范畴进行保护，其中第 37 条规定了关键信息基础设施的运营者数据本地化要求，并明确因业务需求，需要向境外提供数据的，应当进行安全评估。2021 年 9 月，《数据安全法》作为数据安全领域内的专项立法在我国正式得以实施，对企业收集使用数据作出原则性要求，为我国企业域内数据合规提供指引。在数据跨境方面，该法采用了“参照”立法，即关键信息基础设施的运营者在我国境内运营中收集和产生的重要数据的出境适用《网络安全法》的规定。此后，我国陆续出台了《网络数据安全管理条例》《数据出境安全评估办法》等，作为《网络安全法》《数据安全法》以及《个人信息保护法》

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

的补充，规定了数据处理者对外提供数据需要申报数据出境安全评估以及重点评估的具体情形，为规范数据跨境流动活动提供依据。2024 年 3 月，国家互联网信息办公室公布了《促进和规范数据跨境流动规定》，对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度作出了优化调整，进一步完善了我国数据跨境治理机制。

个人信息跨境流动专项立法着眼于对本国公民个人隐私的保护。我国对个人信息跨境采取审慎的立法态度，作出立法限制，要求个人数据本地存储和处理，出境则需要经过网信部门的出境安全评估。2019 年 6 月，国家网信办发布了《个人信息出境安全评估办法征求意见稿》，明确网络运营者向境外提供其在中国境内运营中获取的个人信息，需要申报个人信息出境安全评估，并就评估的流程和要求作出了较为详尽的规定。2021 年 11 月，我国第一部个人信息专门性立法《个人信息保护法》正式实施，明确个人信息处理者向境外提供存储于我国的个人信息需要事前报请主管机关批准，确因业务需要向境外提供个人信息的，应通过安全评估、经专业机构进行个人信息保护认证或签订标准合同。2023 年 2 月，国家网信办公布《个人信息出境标准合同办法》，根据该办法，个人信息处理者向境外提供个人信息且未达到数据安全评估标准时，可以通过签订标准合同的方式实现个人信息出境。

上述法律法规的颁布实施，既表明我国的数据安全立法已进入快速发展阶段，也为当前我国境内企业进行数据跨境流动合规建设提供了基本遵循。然而，我国目前的立法仍然呈现分散式、碎片化的特点，表现为针对同一个问题作出重复性规定，甚至出现对于同一问题在不同的法律文件中有着不同解决方案的情况，这可能导致概念混淆、执法标准不统一、企业合规标准不明确等诸多问题。以数据出境安全评估为例，《个人信息和重要数据出境安全评估办法（征求意见稿）》规定，安全评估的主体为网络运营者，安全评估工作由国家网信部门统筹协调，行业主管或监管部门主要负责；而《数据出境安全评估办法》规定安全评估主体为数据处理者，安全评估工作由国家网信部门负责。商业数据和个人信息存有交叉重叠的部分，安全评估主体很难清晰判断应当依据哪部法律文件确定安全评估负责机构。此外，分散式立法特点使得相关法律制度并不明晰，企业寻求法律依据存在困难，这给企业开展商业数据跨境合规带来了阻碍。例如,《个人信息保护法》中要求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应当将在国内收集和产生的个人信息采取数据本地化措施，将数据存储于境内，但现有立法尚未对信息数量要求作出细化规定，导致企业难以判断其收集处理的数据是否可以跨境流动，不利于我国企业与境外接收方的数字贸易往来。

（二）各国规则未统一，企业双向合规难

由于各国的经济、技术发展水平不同，价值取向不一致等原因，各国在商业数据跨境流通相关立法上所反映的立法宗旨和保护目的存在较大差异。尽管目前不少国家都在积极签订双边或者多边协议，促成数据跨境的自由流通，但仍无法实现规则上的统一，这给企业商业数据跨境合规带来了较大的挑战。企业在“走出去”的过程中，需要同时关注本国以及进口国的相关立法要求。

从我国商业数据跨境规制的相关立法来看，我国更注重在保障数据安全以及个人信息权益的基础上，促进商业数据的依法有序自由流动。我国立法以确保数据主权为核心，强调国家对于商业数据跨境活动的合法规制。比如，我国要求特定类型的数据应当进行本地化存储，确因业务需要向境外提供数据的，应当报请国家主管部门进行安全评估。同时，我国在保障数据主权，确保数据安全的前提下，也积极鼓励商业数据的跨境

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

自由流动，通过参与国际协商的形式让渡一部分数据保护自主权，达成一致协议。[15] 截至目前，我国已与26个国家和地区签署了19个自贸协定，自贸伙伴覆盖亚洲、大洋洲、拉丁美洲、欧洲和非洲，积极推动实施《区域全面经济伙伴关系协定》（RCEP），持续推进加入《全面与进步跨太平洋伙伴关系协定》（CPTPP）和《数字经济伙伴关系协定》（DEPA）。由此，我国确立了以保障数据主权、数据安全为核心，鼓励数据依法有序自由跨境流动的规制模式。

企业在开展涉及商业数据跨境相关海外业务的过程中，不仅需要遵守“数据输出国”的数据跨境相关法律要求，还需要遵循“数据输入国”的数据跨境传输规则。目前，各国的数据跨境传输规则由于其基本立场的不同而存在差异甚至冲突，数据主权、国家安全问题上的争议以及由此引发的在出口管制方面的调查等诸多复杂局面给企业合规工作带来巨大压力，企业商业数据跨境合规难度也随之升级。

（三）跨境数据合规严，企业合规成本高

随着世界对GDPR等数据保护法、数据跨境规则的执行，相关企业将因未履行或未有效履行数据合规义务而被处以高额的罚款。以欧盟GDPR为例，该项数据法案对数据控制者和处理者提出了较高的合规要求：将个人数据从欧盟移转至其他国家或地区，需要满足欧盟委员会确定的满足“充分性保护水平”的要求；在缺乏GDPR规定条件的情况下，企业只有在提供适当的保障措施，且存在有效的数据主体法律保障的情况下，企业才可以向第三国提供数据。

此外，GDPR还规定，企业需要告知其客户数据的使用方式、使用范围以及使用对象，当发生个人数据泄露，并威胁客户隐私时，企业需要在得知泄露事件后的72小时内通知客户并报告。数据保护机构在综合考量侵权行为的性质、严重程度、持续时间以及数据控制者、数据处理者所采取的技术以及管理措施的充分程度等因素，将罚款分为两个层面，较低水平意味着最高可以处以1000万欧元的行政罚款；较高水平则指最高可以处以上一财政年度全球营业总额2%的行政罚款。[16]

为了规避高额数据的违规处罚，相关企业一般会主动开展数据合规工作，但此项工作对于企业来说也是一项高额的成本，且随着商业数据的体量不断扩大，企业必须定期重复审计过程以遵守公司政策和当地法律规定的合规要求，成本和工作量会随着时间的推移而不断增加。

（四）企业合规意识薄弱，数据跨境风险高

随着数字技术的飞速发展，商业数据的价值不断攀升，数据安全问题也逐渐暴露出来。从近年来发生的一系列数据泄露事件可以看出，企业面临的数据安全风险呈多元化趋势。现阶段，企业在数据方面的合规意识还有待提升，数据安全的技术措施和组织保障需要进一步强化。

数据安全技术的不完善是企业数据泄露的一个重要因素，也是企业数据合规工作的重要突破点。根据《2022年数据泄露成本报告》，安全技术的短缺使得企业需要承担巨额的数据泄露成本。研究表明，目前只有38%的企业表示其安全技术团队有充足的人员配备，而这种技术差距将导致人员配备不足的企业的数据泄露成本比人员充足的安全技术团队高出55万美元。[17] 商业数据合规已成为企业开展合规工作至关重要的环节，构建完备的商业数据跨境合规管理体系、保障企业合法合规的开展商业数据跨境运营工作成为当务之急。

四、我国商业数据跨境流动合规治理的优化路径

构建良好的商业数据跨境流动生态是政府和企业的共同目标，构建科学合理的商业数据跨境

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

流动合规治理体系成为我国数据治理领域的重要议题。商业数据跨境合规不仅是企业履行保障信息安全这一社会责任的要求，更是企业走向世界，履行合规义务的职责所在。我国作为数据资源大国，应当积极参与全球数据治理，在商业数据跨境流动合规问题上贡献中国方案。

（一）完善商业数据合规法律体系

针对我国企业商业数据跨境流动立法的问题，相关部门应当对现有立法进行梳理、整合，衔接好相关行政法规之间、行政法规与各行业主管部门出台的部门规章之间的关系，统一基础概念，删除某些重复性规定，对不同类型的企业商业数据的处理情况进行清晰的划定，使《数据出境安全评估办法》《个人信息出境安全评估办法》等下位法更好地与《网络安全法》《数据安全法》《个人信息保护法》等上位法相互配合，为企业合规工作提供清晰明确的法律遵循。

具体而言，我国不同法律文件对数据出境安全评估的主体有“网络运营者”“数据处理者”等不同的称谓，且均未对其作出明确定义，不利于企业数据跨境合规工作的落实。对此，可以参考域外做法，将“网络运营者”细化为“数据处理者”以及“数据控制者”，进一步明确各自的权利与义务。例如，根据欧盟GDPR，“数据控制者”是指那些决定（不论是单独决定还是共同决定）个人数据处理目的与方式的自然人或法人、公共机构、规制机构或其他实体；“数据处理者”是指为了数据控制者而处理个人数据的自然人或法人、公共机构、规制机构或其他实体。由于我国目前已经引入“标准合同”，并出台了相应的办法，监管部门可以根据不同的数据主体，结合不同的数据类型，适用不同的标准合同条款，以更有针对性地确保不同场景下，企业商业数据的安全跨境传输。

《网络安全法》《个人信息保护法》等法律规范要求关键信息基础设施的运营者在我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，因业务需要，确需向境外提供的，应当进行安全评估。但相关立法并没有对关键信息基础设施的范围作出具体的界定，对于何种数据属于重要数据也欠缺明确的划分，这使得企业在处理商业数据跨境业务时，难以清晰定位从而采取适当的合规措施。再者，此种“一刀切”的模式会无形中增加评估审核的工作负担，不利于企业商业数据跨境自由流通。对此，可以采取数据分级分类管理的模式，依据不同行业典型数据类型以及应用场景不断完善立法，对于企业商业数据中与隐私紧密相关的个人数据严格禁止跨境流动，对于不涉及自然人权益的非个人数据则允许在满足安全管理要求的前提下有序跨境流动，管理形式除了安全评估外，还可以采用问责制、合同干预等。

（二）设立数据跨境监督机构

商业数据跨境流动引发的数据泄露、数据非法获取等数据安全问题频发，企业商业数据跨境合规工作的展开迫在眉睫。除了企业自身加强数据合规意识，主动展开合规工作外，监管机构的监督和管理也必不可少。通过对商业数据跨境涉及的网络安全、数据安全等展开监管、执法活动，有利于敦促企业进行合规整改，完善现有合规体系，从而实现商业数据的合法有序跨境。

我国数据跨境监管呈现多头监管的特点，数据监管职责分散在各个相关部门，尚未建立独立专职的数据监管机构。以商业数据跨境的安全评估工作为例，相关立法规定，由国家网信部门统筹协调，具体工作由各行业主管部门或者监管部门负责。事实上，国家网信部门和各行业主管部门或监管部门之间并不存在直接的领导与被领导的关系，不同类型数据的跨境会涉及不同的行业、领域、主体，如果缺乏统一的最高数据监管机构，可能会出现政策不协调、管理效率低、管理效果差等问题。

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

在商业数据跨境监管上，可以适时在国家数据局下设立一个专门、独立、权责明确的数据跨境监管内设机构①，赋予其审核权、调查权、处罚权等权能，统筹负责国家层面的数据跨境监管工作。地方的数据跨境监管部门对国家数据局负责、并受其监督，统一履行数据监管职责，避免多头执法、权责不明的问题，为商业数据跨境流动的监管提供切实保障。

商业数据跨境监管需要企业主动配合，可以在企业内部设置数据合规官，主要负责企业商业数据的合规监管工作。具体而言，数据合规官不仅要维护企业日常商业数据的安全，保证企业数据跨境操作行为合规，包括承担数据处理中的审计职责，对企业内部员工进行合规培训等，还要积极与监管机构达成合作，配合其数据监管工作的开展，同时与数据主体进行对接，掌握企业商业数据跨境合规的监管动向。此外，企业应当重视数据信息安全技术的运用，聘用专门的安全技术团队，从技术层面对企业商业数据跨境活动进行全流程的跟踪监管，对企业商业数据安全隐患进行定期排查，将数据泄露的可能性降到最低。

（三）构建商业数据跨境流动综合治理体系

针对企业数据合规意识较为薄弱，商业数据跨境风险高的问题，国家数据局可以联合国家网信办、工信部、公安机关等行政机构强化执法权，加大对企业数据违规处理行为的处罚力度。虽然我国《数据安全法》针对未经安全评估违法向境外提供重要数据的行为，以及未经主管机关批准向外国司法或者执法机构提供数据的行为规定了分别向企业和直接责任人处以10万—100万，1万—10万不等的罚款，但相较于其他国家，②处罚力度明显偏低。相关主管部门应当依法、合理加大对企业商业数据跨境违规行为的处罚力度，提高企业商业数据违法跨境处理行为的罚金额度，增加企业违法成本，促进企业积极履行数据合规义务。

企业作为社会的重要成员之一，理应主动承担起数据跨境安全保护义务，保障自身管辖范围内的商业数据跨境安全，提高自身商业数据合规意识。对此，企业可以参考相应的法律法规的要求，构建企业内部制度规范，建立企业商业数据跨境合规体系。制度体系可采用分层的模式，内容上避免重复和矛盾。一般可以分为四级，一级文件包含方针、策略等总的管理要求；二级文件包含企业商业数据跨境流动的具体管理制度和办法；三级文件包含企业商业数据跨境各生命周期的操作流程、规范与具体操作指南，以便执行者理解；四级文件包含执行企业商业数据跨境管理制度产生的相应运行文件，包括表格、计划、报告、工作日志等。[18]

此外，第三方数据安全服务机构在企业商业数据跨境流动综合治理体系中也发挥着重要作用。企业可以通过外包托管的方式将企业的数据安全监管工作交给第三方服务机构，开展针对性的企业数据安全运营、管理与技术服务，协助企业构建数据安全防范机制。数据跨境安全监管是一项技术复杂、风险高的工作，涉及资产信息、机密数据等敏感问题，相较于企业自建的数据安全监管部门，第三方数据安全服务机构往往拥有更为专业的技术实力、丰富的数据监管经验，对数据安全问题和威胁有更为深入的了解，可以根据企业需求提供定制服务，节省企业自建数据监管体系的人力成本和技术投入。

①2023年10月25日，我国国家数据局正式揭牌，由国家发展和改革委员会管理，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等工作。

②根据欧盟GDPR的相关规定，针对企业数据处理违规行为，最高可以处以上一财政年度全球营业总额2%的行政罚款。

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（四）积极达成国际合作

为了打破不同国家及地区之间在数据跨境流动上的限制和壁垒，减轻企业商业数据跨境双向合规的压力，为企业合规工作提供标准化规范指南，实现全球数字贸易的自由化、便利化，各国应当积极达成合作，推动全球数据治理友好对话协商，促成统一数据治理国际规则，塑造共建共赢共享新格局。

一方面，我国应积极与其他国家和地区开展双边对话机制，在本国（地区）原有的数据治理制度基础之上，秉承着彼此尊重、充分协商的原则，最大程度地形成国家间的共识，构建互惠共赢的商业数据跨境传输制度体系。另一方面，随着国家间的数据跨境传输活动日趋频繁，国际间的合作必不可少，我国应当积极推动探索全球性的多边协商，为形成全球统一的数据跨境流动法律框架贡献中国智慧、提出中国方案。在“一带一路”背景下，我国可以与沿线国家积极展开谈判，践行相互尊重、合作共赢的国际关系理念，在商业数据跨境流动这一争议问题上与各方进一步达成共识，打破数字壁垒，深化数据互联，积极拓展平等开放共赢的数字伙伴关系。

在数字经济发展全球化的影响下，数据的收集、存储、使用、传输等行为已经遍及全球，早已跨越了国家及地区的界限，这意味着，商业数据的跨境流动问题的解决需要依托于各国之间的合作与协商。各国应当积极沟通，争取在商业数据跨境问题上达成共识，建立商业数据跨境流动的普适性规则，在保障商业数据安全的基础上，促进数据的自由跨境流动，促进全球数字贸易的蓬勃发展。

结语

数字经济时代下，大规模的数据跨境流动成为常态，商业数据跨境流动对我国对外贸易以及经济发展具有重大意义。然而，由于网络环境的复杂性与不可控性，各国对数据跨境流动问题持有不同的态度和立场，数据保护水平参差不齐。我国应当重视企业商业数据跨境合规工作，优化现有商业数据跨境流动合规治理路径。在国际层面，我国应积极与世界主要国家和地区就商业数据跨境问题开展双边或者多边谈判，在确保数据安全的基础上尽可能促进数据跨境的自由流动，共同推动全球数字经济蓬勃发展。在国内层面，我国应当完善现有数据跨境相关立法，为企业商业数据跨境合规提供更加系统、科学的法律指引。在数据跨境监管方面，应当构建企业自查自纠、第三方服务机构协助指导、国家数据主管部门统筹协调监管三位一体的组织格局。

[参考文献]

[1]Voss,W.Gregory.Cross-Border Data Flows,the GDPR,and Data Governance[J].Washington International Law Journal,2020(29).

[2]冯晓青.数据财产化及其法律规制的理论阐释与构建[J].政法论丛,2021(4).

[3]任龙龙.大数据时代的个人信息民法保护[D].对外经济贸易大学,2017.

[4]程啸.论大数据时代的个人数据权利[J].中国社会科学,2018(3).

[5]OECD.Declaration on Transborder Data Flows[EB/OL].http://dx.doi.org/10.1787/23024062440,2023-06-17.

[6]冯镇波.多重风险下数据跨境流动的法律规制[J].法治论坛,2021(3).

[7]陈瑞华.企业合规基本理论（第二版）[M].法律出版社,2021:13.

[8]毛逸潇.数据保护合规体系研究[J].国家检察官学院学报,2022(2).

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[9]闫丽萍.企业环境会计信息披露研究[M].知识产权出版社,2016:38.
[10]戚聿东,徐凯歌.数字经济时代企业社会责任的理论认知与履践范式变革[J].中山大学学报(社会科学版),2023(1).
[11]UNCTAD,Data Protection and Privacy Legislation Worldwide.[EB/OL].https://unctad.org/page/data-protection-and-privacy-legislation-worldwide,2023-7-17.
[12]王金照.跨境数据流动:战略与政策[M].中国发展出版社,2021:63.
[13]胡苗苗,胡代芳等.欧盟非个人数据自由流动框架条例指南[J].北外法学,2020(1).
[14]黄钰.欧盟非个人数据跨境流动监管模式研究[J].情报杂志,2022(12).
[15]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(5).
[16]Vandezande,Niels.An Update on GDPR Fines in Belgium[J].International Journal for the Data Protection Officer,Privacy Officer and Privacy Counsel,2019(3).
[17]IBM Security.2022年数据泄露成本报告[EB/OL].https://www.ibm.com/security,2023-07-20.
[18]中国移动通信有限公司研究院.企业跨境数据流动安全合规白皮书(2023)[EB/OL]https://www.doc88.com/p-88461502652134.html,2023-07-27.

责任编辑:林珊珊

Reform Path of Compliance Governance of Cross-border Flow of Commercial Data in China

Lai Xiaopeng & Ma Shiya

[**Abstract**] In the context of the globalization of data economy, cross- border data transmission is becoming increasingly frequent. While the cross-border flow of business data promotes economic growth, it also raises concerns about personal data security and national security in different countries. The rich connotation of business data, coupled with the uncertainty of external environment, determines the necessity of compliance governance of cross-border business data flow. In response to the current legislative decentralization and difficulties in corporate compliance in the governance of cross-border commercial data flow, below measures should be taken: perfect the legal system of commercial data compliance to provide clear guidance for cross-border commercial data flow compliance; establish a specialized and independent data cross-border supervision agency, and build a comprehensive governance system for cross-border flow of commercial data, to provide practical guarantees for the supervision of cross-border commercial data flow; actively reach bilateral or multilateral cooperation with major countries and regions around the world, promote the formation of unified global data governance standards, to reduce the pressure of two-way compliance for enterprises.

[**Key Words**] Business Data; Cross-Border Data Flow; Enterprise Compliance; Data Governance; System Improvement

(C)1994-2024 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net