doi:10.14089/j.cnki.cn11-3664/f.2023.05.007
引用格式:李凡.商业数据跨境流动的规范重塑及合规治理[J].中国流通经济,2023(5):71-80.

商业数据跨境流动的规范重塑及合规治理

李　凡
(中南财经政法大学知识产权研究中心,湖北 武汉 430073)

摘　要:跨境数据流动监管规则的行业化特征日趋凸显,商业数据类型和权属的独立性预设了其特殊的跨境流动治理方案。基于开放、动态的数据安全主权理念和兼顾安全与发展的风险规制进路,商业数据跨境流动治理应在确保个人信息、重要数据等敏感数据安全可控性的同时,赋予一般商业数据自由流动空间,实现商业数据流动和规制的结构平衡。据此,可自由流动的一般商业数据在满足合同备案的形式化条件后,由政府部门加强事后监管;而包含重要数据和特定个人信息且难以完整析出的重要商业数据,需根据不同情况分别适用出境安全评估、标准合同和保护认证等规则,实现商业数据场景下我国数据出境安全规则之间的内在体系化。此外,除加强法治保障以解决企业数据跨境流动合规难题外,企业构建跨境数据流动合规体系的价值追求应从合规性驱动转为业务价值驱动,围绕数据跨境全流程开展安全防护和价值运营,立足现实需求制定契合的数据跨境流动合规体系建设方案。

关键词:商业数据;数据跨境流动;监管规则;合规治理
中图分类号:F114.4　　**文献标识码**:A　　**文章编号**:1007-8266(2023)05-0071-10

在以数据要素为核心驱动力的数字经济时代,数据跨境流动驱使国际经济活动高效、便捷、智能开展,并在国际贸易、全球经济增长、加速创新等方面发挥着越来越重要的作用。2022年1月,《国务院关于印发"十四五"数字经济发展规划的通知》明确指出,要探索建立健全数据跨境流动治理规则。近年来,我国逐步形成以《全球数据安全倡议》为基础,以《中华人民共和国网络安全法》《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》)三部上位法为主干,以《数据出境安全评估办法》《网络安全审查办法》《个人信息出境安全评估办法(征求意见稿)》等多层次跨境细则和指南为具体指引的数据跨境流动法律法规体系。现有数据跨境流动监管规制的实践运行和理论研究主要围绕数据跨境流动法律治理逻辑[1]及其发展趋势[2]、数据跨境流动规制模式的国际比较[3]、我国数据跨境流动治理困境及对策方案等[4]展开,落脚于如何在数据跨境流动语境中平衡数字经济的开放和安全[5]。现有研究往往以个人权益、国家安全等外部关切视角审视商事活动中的数据跨境流动,缺乏主体视角下围绕特定数据产权属性和流动需求的有益探讨。当前各国数据治理战略的差异源自利益倾向以及各自国内数字产业发展重点的不同,但在数据跨境管理方面也形成了一定的共识,即基于数据重要

收稿日期:2023-02-22
基金项目:国家社会科学基金重大项目"总体国家安全观下产业知识产权风险治理现代化研究"(21&ZD203),教育部人文社会科学重点研究基地重大项目"知识产权领域的国家安全治理研究"(22JJD820029)
作者简介:李凡(1997—),女,湖北省恩施市人,中南财经政法大学知识产权研究中心助理研究员,博士研究生,主要研究方向为知识产权法。

程度，分类分级开展数据跨境管理工作，不断探索数据跨境流动治理的国际合作与竞争。

据此，本文以商业数据为独立规范对象，依据数据集合中不同数据跨境流动规制需求，类型化分析其治理情形。一般商业数据属于经营自由权范围，应纳入自由流动范畴，无需针对其跨境流动设置专门数据安全监管机制，但仍需以合同备案作为数据出境的形式条件；而重要商业数据因牵涉国家安全、个人信息权益和公共利益，只可附条件流动或有限流动，需从严适用重要数据和个人信息的出境安全评估规则。此外，审视企业数据跨境传输活动中面临的内外部合规瓶颈，除多数研究探讨的制度构建和法治保障层面的问题[6-8]外，还应积极探讨企业如何通过主动合规优化自身业务结构，在数据安全防护和业务价值赋能之间寻求最佳平衡，制定契合发展需求的跨境数据流动合规体系建设方案。

一、逻辑前提

（一）商业数据的权属界定

首先，商业数据赋权保护的正当性。确权是资源交易和流转的前提，数据确权是构建数据制度的中枢和核心。经过高技术加工的数据集合是企业的重要资产，其中各类型数据相互交织，利益主体众多，要求数据处理者尽快明确数据集合的权益归属和利益分配。为将零散单一数据转化为蕴含丰富市场信息的商业数据集合，数据处理者通过匿名化脱敏和搭建算法模型实现对海量原始数据的挖掘分析，在此过程中会付出大量人力和资本，并添附包括体力和脑力在内的多元劳动[9]。对商业数据确权的正当性，可基于劳动财产权理论、功利主义理论等具体基础理论，亦可从激励投资、促进数字经济发展等公共效益目标出发。唯有将其确定为类型化的独立权利，才可正面界定商业数据权利属性、范围、归属及例外，并在此基础上安全开展数据开发、利用和交易流转等活动，为激活数据要素价值提供法律基础和保障[10]。

其次，商业数据弱权利保护理念的贯彻。现有制度的财产结构容易强化商业数据的绝对权保护，应积极构建符合商业数据特性、兼顾结构化利益平衡的弱权利保护格局。相比排他性专有权利，商业数据的内生价值属性决定了商业数据的保护制度应更注重数据财产的动态流转利用。合理路径是为耗费实质投入并达到实质规模的商业数据集合设置有限的数据制作者权，以数据适当控制和有效利用为赋权价值目标，通过有限产权激励促进数据的开发利用，包括制作者自行使用和第三人衍生使用。具体而言，在商业数据资源共享、数据挖掘分析、数据访问获取等法律政策指引下，可探索以公平、合理、无歧视原则为基础允许第三方付费访问和使用商业数据的多种方案。

最后，商业数据有限赋权模式下的权利归属。商业数据权属界定应根据数据信息的复合性、层次性等特征，综合参照投入原则、分层原则和责任原则确定归属主体。投入原则基于数据收集处理者的实质劳动投入，明确数据权利由收集数据并耗费实质投入进行加工处理的主体享有，实践中原始数据与衍生数据亦根据该原则确定权利归属。分层原则基于个人信息与整体数据的层次性，明确个人信息权仍由个人独自享有，而整体数据权利归属数据收集处理者。责任原则基于数据后续使用的不确定性，规定因违反法律规定或约定损害个体权利的，其责任由数据使用者承担。

（二）独立分析商业数据跨境流动规则的必要性

商业数据类型和规范权属的独立性预设了其特定的数据治理规则。数据迥异于现有类型化权利客体，涉及个人信息权益、国家数据主权等多重维度[11]，不同类型数据应分别适用相应的符合自身特性的规则体系。2022年12月颁布的《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》将公共数据、企业数据和个人数据相对称①，随后深圳②、上海③等地普遍采纳这种分类。本文采用“商业数据”而非“企业数据”称谓，是因市场数据持有人可能不限于通常意义上的企业，将市场主体为经营目的收集的数据称为商业数据，并使之与公共数据、个人数据相对称，不存在逻辑障碍，也不失准确性[11]。此外，单一数据跨境流动规则缺乏可操作性，无法满足诸多类型数据跨境流动的合规要求，难以有效衔接全球数据跨境传输制度[12]。当前数据安全立法的发展趋势和数据跨境流动的治理需求均反映我国数据跨境流动法律治理不可简单套用统一规制范式，而应建立多样性、针对性、层次性的数据跨境流动规则

体系，拓宽数据跨境传输的合规渠道，并结合数据类型、数据规模、安全需求等要素提供一般化和特殊性的制度方案。其中，商业数据场景下跨境流动规制的深入分析是核心环节，有必要结合商业数据产权属性和数字贸易中多方利益需求，独立探讨其跨境流动规则。由于商业实践中业务数据、个人信息、行业关键数据等各类型数据相互交叉，数据流动链牵涉利益主体众多，商业数据跨境流动规制体系不清，故厘清其中情形具有理论与实践意义，可以将是否包含重要数据和规模化个人信息且难以技术剥离作为分界点，使其适用不同的数据跨境流动规制方式。

二、商业数据跨境流动规则的适用情形

（一）可剥离的商业数据集合：自由流动与备案管理

实践中商业数据通常以集合形式存在[13]。尽管信息技术的创新使数据关联程度加深、数据分类困难，但仍有部分商业数据集合可在技术层面实现同个人数据和公共数据的剥离，从而避免数据权益主体诉求的冲突和纠缠。完成数据剥离后的一般商业数据可基于市场需求“自由、安全、有序地流动”。

1.商业数据、个人信息与公共数据的分野

一方面，个人信息去识别化是数据得以有序流动和再利用的前提。去识别化可在保留个体信息的基础上，通过哈希函数、加密等手段实现第三方无法独立识别或关联至特定自然人的技术效果[14]，有效降低数据流动中的隐私风险，是构建有序、健康数据流动秩序的必然要求，亦是个人信息商业利用的合理要求[15]。《个人信息保护法》第四条明确指出，个人信息不包括匿名化处理后的信息，可视为认可数据剥离具有特定规范效果，即匿名化的个人信息可自由地进行商业化使用。另一方面，公共数据脱敏化可在不降低数据开放流动性的前提下保障敏感数据安全。除涉及国家机密和国家安全的公共数据应绝对禁止开放、避免任何机构和个人接触使用该类数据外，涉及商业秘密和个人隐私的公共数据可根据数据敏感程度，运用脱敏技术加以针对性保护。技术脱敏是在保留原数据价值基础上对敏感数据进行技术处理，同时运用管理流程实现特定用户访问真实数据的一种处理方法[16]。按使用方法分类，脱敏可分为动态脱敏与静态脱敏[17]。前者在应用服务器和数据库之间搭建脱敏平台，向业务系统展示层实时传送脱敏处理后的信息，再结合系统后台数据库查询访问权限的控制，实现有效的实时脱敏，适用于数据库境外访问；后者根据需求设计特定的数据脱敏方案，基于算法破坏数据间的关联性，适用于整体性的数据出境储存。

2.规则适用：自由流动前提下的事后监管制度

脱敏技术或去识别技术可实现事前风险的有效控制，但技术层面的风险控制并非绝对，仍存在商业数据被溯源、重构或解密的风险，故应在保证商业数据自由流动的基础上对其出境活动予以持续性关注，事前遵循合同备案规则，事后实行监督机制，明确禁止对商业数据进行单独识别、交叉识别、算法反推。

具体而言，可剥离的一般商业数据属于经营自由权行使范围，不必设置专门的数据安全监管机制，但有必要以合同备案制度作为数据出境的事前形式条件。在尊重个人利益和公共利益的前提下，商业主体可自主决定一般商业数据的跨境流动事项，此时交易双方仅需通过履行合同的方式对数据跨境安全进行约束与保障，但仍要向所在地省级网信部门备案合同及补充协议。商业主体在跨境传输合同中需与境外接收方约定数据安全保护的责任义务，规范性内容可参考《个人信息出境标准合同规定（征求意见稿）》所附“个人信息出境标准合同”，以及《数据出境安全评估办法》对包含个人信息和重要数据的跨境数据传输协议的强制性规定。但根据“举重以明轻”的原则，此处商业主体无需强制采用上述标准合同，所约定的责任与义务强度可低于强制性规定，以实现最佳商业效果。

而基于技术剥离的局限性以及数据被溯源解密的风险，仍需实质性监督一般商业数据的出境活动，将事后风险控制在法律允许的安全范围内。《数据出境安全评估办法》虽提及境外接收方发生实质性变化的应对措施④，但未准确说明实践中何种程度变动属于此处所指的足以影响数据出境安全的变化情形，实践中的诸多复杂情况亦难以穷尽列举。基于此，有必要以风险评估结果为

判断基准，对商业数据跨境活动予以持续性监测，确保风险评估结果控制在法律允许的安全范围内。境内数据处理者应对可及的境外数据接收方的数据处理活动进行监督，交易双方须及时答复境内监管机构的询问，接受监督管理，配合有关调查，服从监管机构采取的措施或决定，并提供必要证明文件和审计结果。但事后监管措施不可管制性过强，否则可能会妨碍基于商业行为进行的一般数据跨境流动，不利于全球贸易投资的自由化、便利化。

（二）不可剥离的商业数据集合：从严安全评估

虽有技术剥离的可能性，但实践中不乏数据集合中各类数据无法完整析出的情形。例如，2021年7月，国家互联网信息办公室等七部门对“滴滴”实施网络安全审查[18]，原因之一在于“滴滴”境内运营和跨境传输的数据中包含大量反映国内各城市交通基建信息和司机乘客个人身份信息、出行信息的敏感数据，且难以同一般商业数据实现技术剥离，若依照美国《外国公司问责法案》（Holding Foreign Companies Accountable Act，HFCAA）履行信息披露义务，将严重危及我国数据安全、公共利益和个人信息权益保护。技术发展瞬息万变，无法同规范预设一般实现绝对的数据类型切分，相对化的类型转换在具体数据利用场景下毫无意义，此时须将商业数据集合视作整体，严格参照重要数据和个人信息的出境安全评估规则，梳理背后各项权益需求，在数据跨境流动规则实践中寻求价值衡平。

1.商业数据与重要数据、核心数据的交叉关系

商业数据与公共数据、个人数据是基于数据主体角度的分类，三者基本涵盖最基础和最重要的数据类型，且区分标准相对清晰，尽管在称谓和内涵上尚存争议，但对此分类方式已基本达成共识。而核心数据、重要数据、一般数据是基于数据性质和数据安全角度的数据分级，《数据安全法》基于危害程度将数据分为核心数据、重要数据、一般数据三个级别，其中核心数据和重要数据的识别需依照国家颁布的核心数据目录与重要数据目录执行，全国信息安全标准化技术委员会发布的《网络安全标准实践指南——网络数据分类分级指引》明确规定了重要数据和核心数据的具体内涵[5]。商业数据与重要数据、核心数据之间是不同分类视角下的数据类型，三者之间存在交叉关系，即商业数据可能包含牵涉国家安全的重要数据和核心数据，其在不同商业场景下的表现形式和范围也有所不同。目前一些特定行业如医疗领域的重要数据目录尚未明确，只能通过开展数据出境风险自评估和相关行业标准自行判断。《数据安全法》第二十一条要求相关行业主管部门加快制定重要数据目录，待目录公布并正式施行后，其将成为各行业重要数据识别的依据。而重要数据包含的数据主体类型多样，除商业数据外，亦有个人数据、公共数据、政务数据等，只要其泄露和非法使用行为严重危害国家安全、公共利益和社会经济稳定运行，均须纳入重要数据范畴。

2.规则适用：从严评估

进行数据跨境传输活动前，企业需及时进行业务梳理和评估工作，判断自身与合作伙伴是否为关键信息基础设施运营者（Critical Information Infrastructure Operator，CIIO），引入外部律师和专业人员梳理出境数据类型及所涉业务，统计数据规模和出境个人信息涉及的主体数量等。当商业数据集合包含海量个人信息或重要数据且无法实现技术剥离时，应从严适用重要数据和个人信息的出境规则。当前我国数据出境规则包括出境安全评估、标准合同和保护认证三大路径，在不同业务场景下存在不同的优先适用。

安全评估路径适用范围最广，采用综合性风险预防进路，对多种数据出境场景进行一体评估。据《数据出境安全评估办法》规定[6]，出现以下情况时，申报出境安全评估将成为商业数据主体的法定义务：一是商业数据集合中包含重要数据；二是商业主体为关键信息基础设施运营者；三是商业主体处理100万人以上个人信息或者自上年1月1日起累计提供10万人个人信息或者1万人敏感个人信息。申报出境安全评估前，商业主体还须进行风险自评估，二者在具体评估事项上基本相同，唯前者多了考量境外接收方数据保护水平和法规政策等国家安全与数据安全因素。

标准合同路径与安全评估路径互为补充，实践中通常适用于规模较小、跨境需求不多且满足法定条件的中小型企业，以及一次性的跨境投资并购交易。据《个人信息出境标准合同规定（征求意见稿）》规定[7]，处理个人信息数量规模未达到安全评估标准的个人信息处理者和非关键信息基础

设施运营者可将签订标准合同作为数据出境合规路径。作为数据跨境流动领域的有效监管工具之一，数据跨境传输合同的标准化路径始终是值得探讨的议题，通过限定跨境传输合同文本和条款框架来内嵌公法层面的数据安全保护义务，可建构商业数据处理者可信任的市场形象。而保护认证路径适用场景相对较少，实践中通常适用于企业员工管理的场景，以避免频繁重新签订合同以及备案。当前国家互联网信息办公室未就保护认证路径颁布具体实施细则，《个人信息跨境处理活动安全认证规范》作为标准技术文件对商业主体数据出境活动具有一定参考价值。

三、商业数据跨境流动法律规则的重构

（一）基本理念

在总体战略思路上，我国应秉持开放、动态的数据安全主权理念，明确风险可控安全观，强调安全与发展兼顾的规制进路。数据安全主权战略作为目前数据跨境法理的共识，不仅兼顾数据跨境流动的现有关切，且高度契合我国数据安全涉外立场[19]。尽管各国所持有或采取的数据保护目标、数据保护理念、安全保护措施等方面有一定差异，但均不否认风险规制进路。当然，不同国家对数据风险的识别和容忍度有所差别。我国应强调安全与发展兼顾的风险规制进路，并通过各类数据出境评估工具判断数据跨境流动风险是否处于安全、可控状态，以此决定是否准予相应的数据跨境处理活动，平衡数据安全与利用的关系，这应成为我国数据跨境流动制度建构的基本立场。

立足商业活动场景，市场导向是商业数据跨境流动规则的基本场景预设[20]。首先，应明确商业数据自由流动的基础性地位。现有研究表明，2014年数据跨境流动对经济增长的贡献已达2.8万亿美元，预计2025年可达11万亿美元，数据跨境流动已成为提升数字经济发展质量的重要途径[21]，其汇聚形成的数据智能亦可提高商业效率，促进电子商务和数字贸易领域的创新发展。作为经济全球化和自由贸易的参与者、受益者和倡导者，我国力求促进全球贸易和投资的自由化与便利化，强调必要秩序上的信息自由流动，实质上已承认数据自由流动原则的基础性地位[5]。我国促成并签署的《区域全面经济伙伴关系协定》（RCEP）第十二章第十五条明确申明，“不得阻止基于商业行为进行的数据跨境传输”。上海、深圳、北京等亦明确便利数据跨境流动的试行办法，例如《深圳经济特区数据条例（征求意见稿）》就曾提出“数据跨境流通自由港”的政策目标。其次，应将商业数据安全、可控流动作为限制性原则，以应对数据跨境流动风险，类型化实现动静结合的监管管控，充分发挥总体国家安全观对商业数据安全的统领作用。换言之，除保障商业数据自身的完整性、保密性、实用性外，应切实关注商业数据跨境流动全过程可能带来的动态安全风险，将风险控制在可接受范围内。从数据类型看，对商业数据的规制可分为包含敏感商业数据的自主可控规制和一般商业数据的合作可信规制。前者指的是包含海量个人信息和重要数据且无法完整析出的商业数据，须对其跨境流动实行从严评估规制，将数据风险控制在可控范围内；后者基于商业活动自由，在充分考量数据利用价值的基础上促进和保障各方切实履行数据安全保护的责任义务，合理制定违约责任条款，确保双方通过合作达成合理信赖。

（二）一般商业数据：事后监管制度的创新

可自由流动的一般商业数据只需满足合同备案的形式化条件即可跨境流动，但仍须进行实质性的事后监督。当前我国数据跨境规制多聚焦于出境前的风险评估与预防，缺乏对数据出境后的持续追踪与风险监管。基于一般商业数据被溯源、重构、解密的风险，有必要通过其他制度加强数据出境后续追踪监管，将事后风险控制在法律允许的安全范围内，但管制性不宜过强，否则不利于全球贸易投资的自由化、便利化。可行路径之一是设置灵活、适当的数据风险监管问责机制，在支持数据跨境自由流动前提下，鼓励商业主体将全部或部分数据审查义务委托于第三方专业代理机构。美国亦采取此类方式，其跨境隐私规则体系（Cross-Border Privacy Rules，CBPR）规定了数据跨境风险问责代理机制，由专业代理机构认定数据主体隐私保护规则是否符合要求，并明确约定审查范围和奖惩机制，二者共担数据风险，共享数据收益，充分发挥行业自律的协同效应[22]。此外，还可从试点入手探索事后监管机制创新，在有条件的国家和地区（如东盟）开展国际数据交互试点，例

如利用我国申请加入《数字经济伙伴关系协定》(Digital Economy Partnership Agreement, DEPA)的契机,推动建立更大区域范围的数据跨境流动监管试点。

(三)重要商业数据:安全评估机制的细化

包含一定数量个人信息或重要数据且无法完整析出的重要商业数据应根据具体情形从严适用相关出境规则,其中安全评估路径适用范围最广,当前多数用以跨境流动的商业数据均需完成数据出境安全评估申报才能顺利出境。《数据出境安全评估办法》围绕数据出境全流程和各主体进行综合性风险评估,是初期有效的制度尝试,但在制度执行层面存在执法难度大、规避成本低的问题,有必要针对重要数据等法定评估数据类型分别探索更精准的风险评估制度工具。

数据安全立法的核心在于确保重要数据安全可控[23],可通过限定重要数据的领域范畴以及提炼重要数据跨境风险点等方式进一步落实重要数据跨境的精准评估。重要数据概念为我国独有,但当前的定义过于泛化,难以实现精准评估,原本对国家层面的数据安全很难造成影响的一般商业数据可能会因宽泛解释而被纳入重要数据范畴,使得数据安全评估落入封闭、静态的安全认知陷阱。首先,应以"抽象概括+具体列举"的方式明确重要数据的识别范畴,进一步列举可能涉及的重要行业领域,例如医疗健康、金融、能源等,同时考虑到各领域数据的特殊性,将重要数据认定部门设定为各重要行业的主管部门。其次,应提炼重要数据风险点以实现更有效精准的事前预防,避免"撒大网"式泛化评估的弊病。例如实践中可对以下重要数据流动场景进行重点监测和审计,包括无认证访问、参数篡改访问、批量高频访问、低权访问高权业务、跨区域非法办理业务等异常行为。

(四)商业数据跨境流动合同的标准化边界

对自由流动的一般商业数据而言,数据跨境风险是否可控主要取决于境外数据接收方是否依合同约定采取安全技术措施和制定内部安全管理制度,以及违约责任的制定和承担是否具有实践性。对符合出境安全评估条件的重要商业数据而言,数据跨境流动合同作为评估事项之一,要求合同条款对数据安全保护责任义务进行充分约定。《数据出境安全评估办法》第九条细化了充分约定的判断标准;而对无须进行安全评估、选择标准化合同路径的其他商业数据而言,则需确保合同内容符合《个人信息出境标准合同规定(征求意见稿)》第六条规定,或直接采用所附"个人信息出境标准合同"作为拟签署法律文件。尽管相关规定已对标准合同内容作出限定,但整体上仍存在操作性弱的问题,应考虑如何在数据分级分类框架下细化数据跨境标准合同的权利义务[24],确保数据跨境流动链条上的主体在法律既定安全框架内从事数据交易活动。

市场机制的自由竞争属性决定了数据跨境流动合同的标准化应存在边界,合同仅能对涉及数据安全保护义务的事项予以细化和明确,其余内容则遵循私法自治的内在逻辑,由合同当事人自行协商满足实际商业效益要求的具体跨境数据类型、数量、传输方式和技术要求等。数据分级分类框架下细化商业数据跨境流动标准合同的指引功能在于,明确各类情形下合同内容在数据跨境安全保障和风险防控方面需特别关注的环节。其一,若商业数据涉及个人信息,则应根据敏感个人信息和一般个人信息的识别分类对合同义务履行予以细化。其二,若商业数据整体被视为重要数据,则风险防控重点应放在明确各业务环节数据安全保障义务的履行主体和违约责任方,细化自数据开始出境到数据出境目的完成间各业务环节应履行的义务内容。其三,若商业数据出境时不涉及个人信息权利和国家安全等事项,其合同标准化路径应关注跨境流动数据的数量层级和违约责任承担的实践性,例如针对海量规模的一般商业数据跨境活动,应设定更严格的数据安全保障义务,以预防数据积聚或技术解密后产生的性质变化。此外,在不涉及国家安全和社会公共利益的情形下,用户或者数据处理者难以通过民事诉讼要求境外数据接收方真正承担违约责任,故还应考虑通过合同标准化路径提高境外数据接收方违约责任承担的可操作性。

四、商业数据跨境流动中的合规对策与选择

数据全球化将成为推动全球经济发展的中坚力量[25],数据跨境流动直接影响企业成本收益、研

发创新能力乃至其商业模式全球扩张[26]。无论是2021年7月国家互联网信息办公室等七部门对“滴滴”实施网络安全审查[18],还是2022年1月美国联邦通信委员会(Federal Communications Commission,FCC)以危害国家安全为由宣布撤销中国联通美洲公司的214牌照[27],都反映出当前强监管环境下数据跨境流动风险已成为跨国企业和出海企业数据合规的重点,同时面临着识别难、规则异、风险高等严峻挑战。一方面,数据跨境传输过程中内外部风险的不断增多和公权力机关对企业监管审查义务的强化都对企业的数据跨境风险识别能力、追踪和安全监控能力提出极高要求,合规难度加大。不少企业员工通过移动客户端实现随时随地的工作信息交换和数据共享,但传输和存储数据载体的多样性和自由访问性加剧了商业数据不当泄漏的风险[28]。此外,我国数据安全监管的多主体协同执法机制虽能确保海量数据执法审查工作的细致进行,例如2019年中共中央网络安全和信息化委员会办公室、工业和信息化部、公安部和国家市场监督管理总局四部门联合开展了App违法违规收集使用个人数据专项治理行动,但也亦意味着企业合规成本不断升高[29]。另一方面,当前持续存在的全球数据治理博弈加剧、数据跨境流动规制的碎片化态势[30]即便因双边或多边积极对话机制有所缓解,也依然缺乏形成国际通行数据跨境流动规则的基础,企业面临双向合规压力,难以同时满足存在冲突或难以兼容的多种数据出境监管要求。无论是“滴滴”事件,还是2014年我国四大会计师事务所被美国证券交易委员会(Securities and Exchange Commission, SEC)要求提供在美上市公司审计底稿一案[31],均体现了数据跨境传输规则冲突下我国企业面临的严峻法律风险。数据跨境流动合规困境并非企业单方努力即可突破,需充分发挥政府、企业以及行业协会等多方主体优势,以企业积极主动合规为抓手,通过完善国内立法与加强国际合作来营造良好的内外部合规环境。

(一)数据跨境流动应用场景及合规要求

数据全球流动在各类贸易活动下具有常态化趋势,合法合规的数据跨境流动将带来稳定的社会经济效益,企业数据跨境流动合规体系的搭建是其社会属性的理性选择。我国以行政主导机制推进企业合规管理建设[32],尽管已初步建立了包括多层次跨境细则和指南在内的数据跨境流动法律法规体系,但仍缺乏针对性的数据跨境合规规范。实践中不同领域和规模的企业开展跨境资本活动、公司管理活动和国际业务经营时的具体场景有所差异,在合规路径上难以作为有意义的分类依据。参考《数据出境安全评估申报指南》规定的六类数据出境行为,可根据数据落点不同将数据跨境场景分为境内主体收集境内数据后传输至境外和境外主体直接收集并处理境内数据,据此分析不同场景下各数据出境路径的选择标准和合规要求。

其一,境内主体收集境内数据后传输至境外,指的是境内商业主体收集、存储的数据由境内服务器传输或提供下载调取接口至境外数据处理者,之后在境外持续流转,常见于企业赴境外上市、开展业务合作或进行跨国企业管理活动时需向境外提供或披露有关数据的场景。结合当前法律法规搭建的数据出境合规框架,此类行为原则上应先判断后选择。先判断是指对境内商业主体性质、跨境数据类型、处理及出境所涉个人信息主体数量等要素进行判断,如符合数据出境安全评估条件,例如境内数据处理主体为关键信息基础设施运营者或跨境数据类型包含重要数据等,则依据《数据出境安全评估办法》开展安全评估;后选择是指不符合出境安全评估条件的可结合自身具体情况选择以个人信息保护认证或签订标准合同的方式进行数据跨境活动。

其二,境外主体直接收集并处理境内数据,指的是境外商业主体直接采集境内数据并存储至境外,常见于境外企业或租用境外服务器进行数据处理活动的境内企业,向境内自然人提供产品服务或采集境内用户数据分析评估其行为的场景。此时应判断商业主体个人信息处理活动是否符合《个人信息保护法》第三条第(二)项规定的域外管辖要件,符合的则遵循《个人信息跨境处理活动安全认证规范》开展个人信息保护认证工作;处理和传输的个人信息主体数量达到或超出出境安全评估门槛数量时则依法开展出境安全评估工作。

(二)商业数据跨境流动合规治理的应对

法治保障层面的对策包括我国明确自身数据跨境流动治理的价值选择,完善各实施细则以增强法律规范的操作性;创新数据跨境监管机构的统筹部署,将合规监管工作落至实处;同时积极参

与数据跨境流动方面的区域性谈判和国际规则研讨，推动国际规则的兼容发展，为本国企业争取最大利益等[6]。基于制度环境的不断调整优化，企业层面亦需要充分发挥自身主观能动性，转变合规体系建设理念，积极适用相关数据合规工具，对标国际规则进行内部合规体系建设，切实提升数据跨境合规管理能力。

其一，商业数据跨境流动合规体系建设的理念应由合规性驱动转为业务价值驱动，将主动适用跨境数据规则视为优化自身业务结构的契机。当前各国均加速数据立法以抢占制度先机，数据监管形势日趋严峻，跨国企业应直面国际数据治理难题，转变以往只满足监管要求的合规初衷，使企业数据跨境合规行动从成本投入转为价值投资⑧，在数据安全防护和业务价值赋能之间寻求最佳平衡。因合规管理体系的建设除规避法律风险、有效切割责任等消极受益外，亦具有增加企业商业价值、助力企业可持续发展的积极效能[33]，故企业应积极发挥自我驱动力，完善建设以市场竞争为导向的数据跨境合规体系[34]。具体而言，企业应围绕数据跨境全流程开展安全监管和价值运营，结合国家《信息安全技术—个人信息安全规范》(GB/T35273-2020)等相关规定细化并明确自身在数据采集、存储、传输、处理和交换共享阶段应采取的安全管理措施和数据保护义务。此外，企业应积极对标出口国的跨境数据规则，例如各国数据本地化的具体政策或者标准合同条款的审查要求等，根据当地司法执法特点研究最利于维护自身合法权益的纠纷解决方式[35]，遇阻时与当地政府和执法机关积极沟通并合理利用规则提出抗辩。

其二，为贯彻业务价值驱动理念，商业数据跨境流动合规体系建设的关注点应转至如何为企业产生实际效能，立足企业现实需求与国家数据跨境法律法规体系间的差异，制定相契合的跨境数据流动合规体系建设方案。除技术内核层面的创新发展外，在组织制度体系方面首先应强调对跨境数据基础信息的识别整理，包括跨境业务关系梳理、数据分级分类整理、重要数据和规模个人信息的识别以及具体业务场景下的数据权限，根据实践确定相应的数据跨境业务流程、数据分级分类实施指南、数据识别清单等工作文件。其次，应注重完善企业数据跨境活动的日常风险监测评估机制和安全响应机制，细化各类敏感数据跨境监测场景如数据脱敏化、无认证访问、高频次访问或者参数篡改访问行为等，规范数据跨境风险评估流程，提升数据跨境安全应急机制的实施效率。

其三，推动数据合规团队建设及专家库建设，或引入第三方合规评估机构，提高数据跨境合规实效。数据跨境合规治理团队既需法律专业人才强化数据跨境风险评估导向、合理规避法律风险，又需技术专业人才运用各项关键技术助力企业境内外平台建设和数据跨境流动各周期的监管审计工作。有条件者可加强与高校科研机构的深入合作，借助专家智慧充分研判域外数据跨境政策，及时跟进规则变动，提高综合运用各类维权工具的能力。

其四，强调全流程、全周期数据合规理念，完善合规绩效考核、合规审计报告、违规调查应对机制等事后合规管理体系。数据合规管理应囊括事前识别预防、事中监测监管、事后问责应对等环节，分阶段建立相应的数据跨境管理措施[36]。其中合规绩效考核要求以客观明确的标准对数据跨境各环节或部门工作人员的工作合规情况进行评价，并纳入企业薪酬管理体系；合规审计报告要求企业对自身数据跨境处理活动的合规情况进行专项审计和定期审计，审计过程中发现的重要数据违法跨境、怠于管理等情况应及时处理，并形成完整记录以便后续调查。违规行为发生后，企业需接受各数据安全监管执法机构的调查，为避免因盲目应对而致使更严厉惩戒和处罚的情况，企业自身应建立有效应对机制，及时开展内部调查追责，完成相关合规漏洞的整改，并主动披露报告，积极接受有关机构的安全审查，制定包括内部调查细则、违规责任人处理办法、合规管理技术漏洞修复措施等在内的有效消除影响的补救应对方案。

五、结语

商业自由原则以及数据流动对经济社会的巨大价值驱使数据自由跨境流动，但数据安全风险客观上不可规避。鉴于商业实践中数据类型和形式较复杂，单一制度无法全面预防和纾解数据跨境流动风险，可对商业数据跨境流动法律规则进行类型化分析，将其分为敏感商业数据的自主可控规制和一般商业数据的合作可信规制。我国基

于数据安全流动理念构建了重要数据和个人信息出境规制的双轨并行制度框架，符合该制度要件的部分商业数据应从严评估规制，将数据风险控制在可控范围内。面对企业数据跨境流动合规治理困境，应增强国内数据跨境流动规则的操作性，积极参与国际规则制定，为企业提供良好的双向合规环境。更重要的是，企业自身需积极开展数据跨境合规行动，结合自身经营需求建立并细化、完善更具操作性与指引性的跨境数据流动合规体系。

注释：

①《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》中规定“要建立数据产权制度，推进公共数据、企业数据、个人数据分类分级确权授权使用。”

②《深圳经济特区数据条例》第二条（二）项规定：“个人数据，是指载有可识别特定自然人信息的数据，不包括匿名化处理后的数据”；第二条（五）项规定：“公共数据，是指公共管理和服务机构在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据”；第五十八条规定：“市场主体对合法处理数据形成的数据产品和服务，可以依法自主使用，取得收益，进行处分”。

③《上海市数据条例》第二条（四）项规定：“公共数据，是指本市国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织……，在履行公共管理和服务职责过程中收集和产生的数据。”

④《数据出境安全评估办法》第十二条规定：“……在有效期内出现以下情形之一的，数据处理者应当重新申报评估：（一）向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；（二）境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；（三）出现影响出境数据安全的其他情形。”

⑤《网络安全标准实践指南——网络数据分类分级指引》明确规定，重要数据是指“一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据”，核心数据是指“关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据”。

⑥《数据出境安全评估办法》第四条规定：“数据处理者向境外提供数据，有下列情形之一的，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：（一）数据处理者向境外提供重要数据；（二）关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息；（三）自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息；（四）国家网信部门规定的其他需要申报数据出境安全评估的情形。”

⑦《个人信息出境标准合同规定（征求意见稿）》第四条规定：“个人信息处理者同时符合下列情形的，可以通过签订标准合同的方式向境外提供个人信息：（一）非关键信息基础设施运营者；（二）处理个人信息不满100万人的；（三）自上年1月1日起累计向境外提供未达到10万人个人信息的；（四）自上年1月1日起累计向境外提供未达到1万人敏感个人信息的。”

⑧中国移动《企业跨境数据流动安全合规白皮书（2023）》。

参考文献：

[1]王佳宜，王子岩.个人数据跨境流动规则的欧美博弈及中国因应——基于双重外部性视角[J].电子政务，2022（5）：99-111.

[2]唐巧盈，杨嵘均.跨境数据流动治理的双重悖论、运演逻辑及其趋势[J].东南学术，2022（2）：72-83.

[3]洪延青.数据跨境流动的规则碎片化及中国应对[J].行政法学研究，2022（4）：61-72.

[4]刘金瑞.迈向数据跨境流动的全球规制：基本关切与中国方案[J].行政法学研究，2022（4）：73-88.

[5]许可.自由与安全：数据跨境流动的中国方案[J].环球法律评论，2021（1）：22-37.

[6]许多奇.论跨境数据流动规制企业双向合规的法治保障[J].东方法学，2020（2）：185-197.

[7]张翔，杨东.我国跨境企业数据合规治理之变革路径——基于TikTok事件[J].中国信息安全，2020（8）：43-45.

[8]黄志雄，韦欣好.美欧跨境数据流动规则博弈及中国因应——以《隐私盾协议》无效判决为视角[J].同济大学学报（社会科学版），2021（2）：31-43.

[9]冯晓青.知识产权视野下商业数据保护研究[J].比较法研究，2022（5）：31-45.

[10]孔祥俊.商业数据权：数字时代的新型工业产权——工业产权的归入与权属界定三原则[J].比较法研究，2022（1）：83-100.

[11]赵磊.数据产权类型化的法律意义[J].中国政法大学学报，2021（3）：72-82.

[12]陈少威，贾开.跨境数据流动的全球治理：历史变迁、制度困境与变革路径[J].经济社会体制比较，2020（2）：120-128.

[13]徐实.企业数据保护的知识产权路径及其突破[J].东方法学，2018（5）：55-62.

[14]蒋洁，兰舟，祁怡然.个人信息去识别化的类型解构与治理方案[J].图书与情报，2021（3）：79-86.

[15]金耀.个人信息去身份的法理基础与规范重塑[J].法学评论，2017（3）：120-130.

[16]王毛路，华跃.数据脱敏在政府数据治理及开放服务中

的应用[J].电子政务,2019(5):94-103.
[17]袁强.网络数据脱敏系统的设计与实现[J].通信与信息技术,2021(4):58-61.
[18]国家网信办、国家安全部等七部门进驻滴滴出行 开展网络安全审查[EB/OL].(2021-07-16)[2023-04-19].https://baijiahao.baidu.com/s?id=1705418575658713319&wfr=spider&for=pc.
[19]丁晓东.数据跨境流动的法理反思与制度重构——兼评《数据出境安全评估办法》[J].行政法学研究,2023(1):62-77.
[20]张学文."商业数据出境"的规则之治:权属分析、关系构成、实践面向[J].情报杂志,2022(2):176-181,189.
[21]McKinsey Global Institute. Digital globalization:the new era of global flows [EB/OL].(2016-02-24)[2023-04-27].https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.
[22]徐瑛晗,纪孟汝."三同时"制度:个人数据跨境流动风险监管之创新[J].情报杂志,2022(7):84-90.
[23]刘金瑞.数据安全范式革新及其立法展开[J].环球法律评论,2021(1):5-21.
[24]赵精武.数据跨境传输中标准化合同的构建基础与监管转型[J].法律科学(西北政法大学学报),2022(2):148-161.
[25]GREENLEAF G. Asia's data privacy dilemmas 2014—2019: national divergences, cross-border gridlock[J].Social science electronic publishing,2019(8):52-55.
[26]惠志斌.数据经济时代互联网企业跨境数据流动风险管理研究[D].南京:南京大学,2018.
[27]工业和信息化部针对美撤销中国联通214牌照事项的声明[EB/OL].(2022-02-03)[2023-04-19].https://www.miit.gov.cn/jgsj/txs/gzdt/art/2022/art_77c9d5181e574e1c809c0a9ff2ad56c2.html.
[28]王倩,顾雪莹.GDPR下涉欧企业的员工个人数据合规管理[J].德国研究,2021(2):117-131,136.
[29]中央网信办、工信部、公安部、市场监管总局联合开展"App违法违规收集使用个人信息专项治理"[EB/OL].(2019-01-25)[2023-04-19].http://www.cac.gov.cn/2019-01/25/c_1124042585.htm?from=timeline&isappinstalled=1.
[30]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(5):114-126.
[31]暂停审计资格半年,"四大"中概股审计底稿还交不交[EB/OL].(2014-02-08)[2023-04-19].http://finance.sina.com.cn/world/gjjj/20140218/115918250091.shtml.
[32]陈瑞华.论企业合规的中国化问题[J].法律科学(西北政法大学学报),2020(3):34-48.
[33]陈瑞华.论企业合规的基本价值[J].法学论坛,2021(6):5-20.
[34]尹云霞,李晓霞.中国企业合规的动力及实现路径[J].中国法律评论,2020(3):159-166.
[35]梅傲,侯之帅.总体国家安全观视域下企业跨境数据的合规治理[J].江苏社会科学,2022(6):169-176.
[36]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):84-100.

责任编辑:方程

Reshaping the Regulation and Compliance Governance of Cross-border Flow of Business Data

LI Fan

(*Intellectual Property Research Center, Zhongnan University of Economics and Law, Wuhan* 430073, *Hubei, China*)

Abstract: The industrialization characteristics of cross-border data flow regulatory rules are becoming increasingly prominent, and the discussion of the independence of commercial data types and ownership presupposes its specialized cross-border flow governance scheme. Based on the concept of open and dynamic data security sovereignty and the risk regulation approach that takes into account both security and development, the governance of cross-border flow of commercial data should ensure the "security and controllability" of sensitive data such as personal information and important data and give general commercial data "free flow" space, so as to achieve a structural balance between commercial data circulation and regulation. Accordingly, the afterwards supervision on the free flow of general commercial data is strengthened by the government department after the formal conditions for contract filing are met; while the important commercial data that contains important data and a certain amount of personal information needs to be subject to rules such as outbound security assessment, standard contracts, and protection certification according to its own circumstances, so as to realize the intrinsic systematization of China's data export security rules in commercial data scenarios. Besides, in addition to strengthening legal guarantees to solve the compliance problems of cross-border data flow of enterprises, the value pursuit of enterprises in building a cross-border data flow compliance system should shift from "compliance-driven" to "business value-driven", carry out security protection and value operation around the whole process of cross-border data, and formulate a cross-border data flow compliance system construction plan based on actual needs.

Key words: business data; cross-border flow of data; supervision rules; compliance governance