对外经济贸易大学法学院
博士申请学位科研成果考核折算科研文献

文献形式（文献综述/读书报告）：文献综述

文献题目：企业数据出境监管研究之文献综述

博士论文题目：企业数据出境监管研究

导　　师：马其家

作者姓名：刘飞虎

专　　业：国际法学

学　　号：201900540098

企业数据出境监管研究之文献综述

摘　要：数据作为生产要素出境在国际贸易中愈发频繁和重要，而我国滞后的数据跨境传输立法，未能为我国企业数据出境提供足够的法律监管和保护。本文献综述聚焦企业数据出境监管中的三个核心问题。一是企业数据出境的限制。目前国际上存在以俄罗斯、美国、欧盟为代表的三种企业数据出境限制监管思路，分别代表严格限制出境、追求自由流动、平衡流动与安全的数据监管策略，这具体体现在各国企业数据出境受到数据本地化要求、出境前数据安全评估、出境前征求个人同意程序等的限制不同。二是企业数据出境的监管协调机制。其总体上可以归纳为欧盟的充分性认定及充分保护措施机制、美国的多边合作数据流动圈机制、日本的基于信任的自由数据流通机制，以统一区域内的监管标准并便利多个国家协同监管企业数据。三是数据出境企业的主体责任和追责问题。数据出境企业应负有内部管理、自查上报与泄露制止、配合审查等主体责任。至于责任的追究，部分国家的行政机构拥有对数据出境企业的处罚权和/或裁量权，美国等通过“长臂管辖”对数据出境企业有司法权，行业协会的自律监管权也在少数国家规则或实践中能体现。

关键词：企业数据；跨境传输；数据出境监管协调机制；企业责任

目录

一、企业数据跨境传输出境基本概念、理论的国内外文献 1
（一）企业数据的概念厘清 1
1．数据与信息的概念厘清 1
2．企业数据的概念厘清 2
3．个人数据与企业数据的概念厘清 3
（二）企业数据跨境传输出境的概念辨析 3
1．企业数据跨境传输与企业数据跨境流动的概念辨析 3
2．企业数据跨境传输与企业数据出境的概念辨析 4
3．数字贸易、电子商务与企业数据跨境传输的概念辨析 5
（三）企业数据出境监管的基础理论研究 7
1．数据权益的探讨 7
2．企业数据权益的探讨 8
二、企业数据本地化要求及出境限制的国内外文献 9
（一）保护数据隐私与促进数据流动为分歧的企业数据出境限制监管博弈 9
1．以俄罗斯为代表的侧重数据隐私保护的企业数据出境限制监管 9
2．以美国为代表的侧重数据自由流动的企业数据出境限制监管 10
3．以欧盟为代表的平衡数据隐私与流动的企业数据出境限制监管 12
（二）企业数据出境限制中的数据本地化监管争议 13
1．数据本地化的国家安全考量 13
2．数据本地化对跨境经济发展的抑制 14
3．数据本地化的企业数据出境限制监管平衡机制 14
（三）企业数据出境前的数据安全评估 16
1．对数据接收国数据保护立法状况的评估 16
2．对机器产生的非个人数据的分类安全评估 16
3．对涉及重点行业、领域企业数据的分类安全评估 17
（四）企业数据出境前的征求个人同意程序 19
1．征求个人同意程序的内涵及各国实施情况 19
2．俄罗斯征求个人同意程序的特殊规则 19
（五）小结 20
三、企业数据出境监管协调机制的国内外文献 20
（一）欧盟企业数据出境的“充分性认定”机制 20
1．充分性认定机制的内涵界定 20
2．充分性认定机制的国家/地区白名单规则 21
3．欧盟充分性认定机制与新加坡相似保护信任机制的异同 23
4．充分性认定机制的借鉴启示 23
（二）欧盟企业数据出境的“充分保护措施”机制 24

1．充分保护措施机制对充分性认定机制的补充作用 24
2．充分保护措施之签订标准合同条款合同 24
3．充分保护措施之建立有约束力的集团企业规则 25
4．充分保护措施之设定经批准的认证机制 25
（三）美国企业数据出境的多边合作“数据流动圈”机制 26
1．多边合作数据流动圈的内涵及实践 26
2．《安全港协议》、《隐私盾协议》及美国规则与欧盟规则的冲突 27
（四）日本企业数据出境的“基于信任的自由数据流通”机制 28
1．基于信任的自由数据流通机制的产生背景及内涵界定 28
2．基于信任的自由数据流通机制的妥协性及监管风险 28
（五）小结 28
四、数据出境企业主体责任及追责的国内外文献 29
（一）数据出境的企业主体责任 29
1．数据出境企业主体的内部管理责任 29
2．数据出境企业主体的自查上报与泄露制止责任 30
3．数据出境企业主体的配合审查责任 31
（二）对数据出境企业的追责形式 32
1．行政机构对数据出境企业的处罚权和裁量权 32
2．司法机关对数据出境企业的司法权 33
3．行业协会的企业数据出境自律监管权 34
（三）小结 36
五、完善我国企业数据出境监管制度的国内文献 36
（一）我国企业数据跨境传输保护现状及立法改革完善的研究 36
（二）我国在 WTO 电子商务谈判中关于数据跨境传输议题的策略 37
（三）国内博士论文对企业数据出境监管完善的研究状况 38
六、总结 38
七、参考文献 39
八、附录 47

企业数据出境监管是数据跨境传输监管的构成部分，对于数据跨境传输监管规则的研究，当前在国内外都是热点问题。国际立法及实践上，欧盟和美国走在了前列，分别主导了以“充分性认定”为核心的数据跨境传输规则和以构建“数据流动圈”的数据跨境传输规则这两种主流数据跨境传输监管协调机制。因此，国外文献主要聚焦于对欧盟、美国数据跨境传输国内立法、政策以及国际合作协议、条约的研究。国内方面，2017 年习近平总书记在中共中央政治局第二次集体学习时强调“要构建以数据为关键要素的数字经济”后，国内的相关研究爆发式增长，主要集中于对数据跨境传输基础概念理论、企业数据跨境传输域外国家规则、WTO 电子商务谈判中的数据跨境议题、我国数据跨境传输保护现状及立法情况以及数据出境限制规则等问题的研究。

一、企业数据跨境传输出境基本概念、理论的国内外文献

（一）企业数据的概念厘清

1．数据与信息的概念厘清

讨论企业数据问题，首先应当关注法律上的数据（data）与信息（information）的区别。数据与信息的内涵差异，会导致数据出境和信息出境的监管存在差异，为了更好的进行企业数据出境监管，在立法中应当坚持数据与信息的区分。采取国际标准化组织（ISO）的定义，信息是“在特定语境中具有特定意义的关于客体的知识，如事实、事件、事物、过程或思想包括理念”；数据是“信息的形式化表现，可展现其背后的意义，用于沟通、含义展示或处理，同时数据可以被自动化处理”。[1]简单而言，信息展现的是内容含义，而数据是这种内容的表现形式及载体。

对于数据与信息有无区分意义，学者们的观点不同。部分法学研究者认为，数据与数据的区分无意义（刘德良，2008），[2]或“仅仅在于不同的表述角度”（谢远扬，2016），[3]因此“约定俗成即可”（郭明龙，2012）。[4]而韩旭至持相反观点，他认为，区分数据与信息的重要意义在于，其对权利设定与裁判结果均有决定性影响。模糊性使用的后果即体现在这两个方面。于权利设定而言，模糊性使用将导致信息权利客体难以确定，信息权利设定出现偏差；于司法裁判而言，模糊性使用又导致了权利保护受限、法律论证矛盾的疑难问题（韩旭至，2020）。[5]梅夏英也认为，两者应当做出区分。他指出，信息和数据概念的区分仍然具有法律意义，即可对现实

[1] ISO/IEC 2382: 2015.
[2] 参见刘德良：《论个人信息的财产权保护》，人民法院出版社 2008 年版，第 20 页。
[3] 谢远扬：《个人信息的私法保护》，中国法制出版社 2016 年版，第 6 页。
[4] 郭明龙：《个人信息权利的侵权法保护》，中国法制出版社 2012 年版，第 19 页。
[5] 韩旭至：《信息权利范畴的模糊性使用及其后果——基于对信息、数据混用的分析》，载《华东政法大学学报》2020 年第 1 期，第 85-86 页。

中具体网络信息数据问题区分为两种基本问题类型：信息问题和数据问题，两种问题类型的区分标准在于当事人利益的侧重点、具体诉求的性质和救济的可能方式的不同上（梅夏英，2020）。[6]

结合上述文献，本人认为，在企业数据出境监管法律研究中，对于数据和信息概念区分的意义重大。数据作为内容的载体和信息作为内容含义的展示，一是，监管部门对两者的出境审批标准、监管方式会存在差异，如企业数据的“本地化存储”规定，而并无企业信息本地化存储这种规定；二是，在跨境时企业主体对两者的保护义务及责任存在差异，如企业数据违法出境不仅是商业秘密的问题，还涉及到企业未遵守数据安全保护义务的问题。

2．企业数据的概念厘清

对于企业数据（enterprise data）的概念定义，需要结合企业数据权益的性质来判断。对于企业数据权益的性质判断，当前理论上亦存在不同观点。李爱君从企业数据权益与传统民事权利的比较研究入手，她提出，数据权利是具有财产权属性、人格权属性、国家主权属性的新型的民事权利，由于数据财产权利集合被某一主体完全享有在大多数情况下无法实现，其中各类具体权利分属不同主体。因此，数据财产权和传统的所有权结构存在巨大差异，无法以所有权概念为基础解释和构建数据财产权（李爱君，2018）。[7]支振锋认为，讨论企业数据权益，应当先对企业数据分类。他指出，对企业数据的保护应当区分电子数据和非电子数据，以及按线上线下来分类比较分析（支振锋，2020）。[8]梅夏英则在提出的“数据控制论”基础上讨论企业数据权益。他认为，现在面临的问题是企业数据电子化后，线上线下的比较分析至少使我们确信，企业对数据的利益不在于对信息内容的独占，而体现在对数据的技术控制上，问题应交由数字技术中的数据操作秩序来解决（梅夏英，2020）。[9]

虽然目前对于企业数据权益的基本属性判断在理论上尚未完成，但是学者普遍认为，不能以我国民法中的所有权，即占有、使用、收益、处分四项权能，来定义“企业数据”的概念。对于企业数据出境中的“企业数据”，本文采用狭义的“企业数据”概念，即企业收集、控制、处理、传输的数据，不包括广义上的企业运营层面的数据，如企业财务数据、运营数据等（祝艳艳，2020）。[10]这些数据可能来自公共数据、个人数据、其他企业数据，只要企业对经手的数据有“技术上的控制”，即为本文讨论的“企业数据”。

---

[6] 梅夏英：《信息和数据概念区分的法律意义》，载《比较法研究》2020 年第 6 期，第 151 页。
[7] 李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期，第 64 页。
[8] 支振锋：《贡献数据安全立法的中国方案》，载《信息安全与通信保密》2020 年第 8 期，第 4 页。
[9] 梅夏英：《信息和数据概念区分的法律意义》，载《比较法研究》2020 年第 6 期，第 154-155 页。
[10] 参见祝艳艳：《大数据时代企业数据保护的困境及路径建构》，载《征信》2020 年第 12 期，第 29 页。

3．个人数据与企业数据的概念厘清

个人数据（personal data）和企业数据（enterprise data）的关系密不可分。个人数据是企业数据的重要来源和组成部分，企业对用户的个人数据予以收集归类处理，形成企业自有的数据库，并以此开展商业活动（汪晓华，2020）。[11]个人数据对于企业来说有重要的商业价值，如企业收集到的数据可以在贵阳大数据交易所（GBDEx）[12]等数据交易平台进行交易，获得正当经济利益；另一方面，在数据经济利益的诱惑下，通过企业渠道获取的个人数据也会在“黑市”被交易，损害个人权益，如支付宝、华住、Facebook 等知名企业就出现过用户数据泄露事件。此外，企业之间亦因个人数据产生争执，如华为和腾讯就分享微信用户数据产生了分歧；阿里巴巴与顺丰物流数据控制权之争等等。

欧盟《通用数据保护条例》（General Data Protection Regulation, GDPR）的定义为，“个人数据”即与一个身份已经被识别或者身份可识别的自然人（数据主体）有关的任何信息；“非个人数据”（non-personal data）的具体示例包括用于大数据分析的聚合和各种匿名化的数据集，不断扩大的物联网、人工智能和机器深度学习，这些代表了非个人数据的主要来源。[13]因此，个人数据和企业数据的界限在哪里？企业付出时间、人力、科技及金钱成本收集到的个人数据，是否转化为企业财产？

本人认为，企业获得的个人数据能否转化为企业财产，不能笼统对待。对于企业数据中的“机器产生的非个人数据”（non-personal data），企业可以拥有财产权利；对于其他来源于个人的数据，企业并不能拥有个人数据的所有权，只能作为个人数据的控制者，承担相应的保护责任。区分企业控制数据中的“个人数据”和“非个人数据”的意义在于，企业数据出境监管中对两者的出境审批安全性评估标准等会存在差异。

（二）企业数据跨境传输出境的概念辨析

1．企业数据跨境传输与企业数据跨境流动的概念辨析

跨境数据流动（Trans-border Data Flows），也被译为“数据跨界流动”、“数据跨境传输”、“数据转移”及“数据的国际流动”等（相丽玲、张佳彧，2021）。[14]根据 1980 年经济发展与合作组织（Organization for Economic Co-operation and Development，OECD）发布的《关于隐私保护和个人数据跨境流动的指南》，“跨境数据流动”是指“个人数据的传输跨越了国家边界”。在此之后这一定义不断

---

[11] 汪晓华：《企业数据财产权与用户个人信息权益之冲突与协调》，载《西南民族大学学报(人文社科版)》2020 年第 10 期，第 93 页。

[12] 贵阳大数据交易所（GBDEx）是经贵州省政府批准成立的全国第一家以大数据命名的交易所，2015 年 4 月 14 日正式挂牌运营并完成首批大数据交易，是一个面向全国提供数据交易服务的创新型交易场所。

[13] Free Flow of Non-personal Data，https://digital-strategy.ec.europa.eu/en/policies/non-personal-data（last visited May 11, 2021).

[14] 相丽玲、张佳彧：《中外跨境数据流动的法律监管制度研究》，载《情报理论与实践》2021 年第 4 期，第 74 页。

延伸，不再限于个人数据，如联合国跨国公司中心（United Nations Centre on Transnational Corporation，UNCTC）对跨境数据流动的界定为“跨越国界对存储在计算机中的机器可读的数据进行处理、存储和检索”（UNCTC，1984）。[15]但至今跨境数据流动仍未形成全球统一的定义（孙方江，2021），[16]不同国家/国际组织对该概念的表述和定义存在差异，不同的表述包括“向境外传输”“向第三国提供”等。

尽管在表述方面存在差异，但总体来看，跨境数据流动这一概念，包括两方面的核心要义。一是数据是指能被识别、可读取、包含特定信息的数据。依托于传感器、电子软件、网络通信等设备和基础设施，机器与机器、人与人、机器与人之间进行交互，实现人与产品、服务、资本等要素和资源的相互识别、实时联通，而这些交互得以实现的载体就是数据。二是数据流动的范围跨越了国家边界。在跨境商品贸易和服务贸易时，数据会在境内外机构之间进行传输。在发生商业贸易时，以跨境电商为例，消费者购物会涉及选择物流、收货地址、检索记录、支付偏好、税务信息等大量数据，这些数据会留存在境外。

依据上述定义，“数据跨境传输”和“数据跨境流动”貌似是定义相同、译法不同的同一概念。虽然内涵基本一致，在学术研究中也经常混用，但两者的侧重点不同。笔者认为，“数据跨境传输”强调“传输”这个具体操作，而“跨境数据流动”则相对概况笼统，前者的概念涵盖范围小于后者。本文采用“数据跨境传输”的表述方式，并不纠结于两者概念定义上的局部争议，目的是为了更好聚焦数据跨境“传输”环节的监管问题，因此使用“数据跨境传输”表述更为妥帖。

2．企业数据跨境传输与企业数据出境的概念辨析

“企业数据跨境传输”是指企业数据跨境的双向流动，即出境（exit）和入境（entry），而“企业数据出境”是指数据从企业所在国向数据接收国的单向流动，即出境，前者的概念包含后者。企业数据出境的监管，主要涉及企业数据允许出境的审批、企业数据出境的监管协调机制以及企业主体责任及追责等问题。而企业数据跨境传输除了包含这些问题外，还涉及数据入境的市场准入问题、贸易壁垒问题、监管机构对数据的调取等问题（许可，2021）。[17]

余振认为，在数字产品和服务贸易政策方面，多数国家均对数字产品和服务贸易自由化采取了积极的态度。在数字企业本地进入政策方面，各国的差异性较小，共性内容居多，取得协商共识的可能性也较大（余振，2020）。[18]因此，本文只关

[15] Transnational Corporations and Transborder Data Flows : Background and Overview, https://digitallibrary.un.org/record/250595?ln=zh_CN（last visited May 11, 2021).
[16] 孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 13 页。
[17] 参见许可：《自由与安全：数据跨境流动的中国方案》，载《环球法律评论》2021 年第 1 期，第 22-37 页。
[18] 余振：《全球数字贸易政策：国别特征、立场分野与发展趋势》，载《国外社会科学》2020 年第 4 期，第 34 页。

注更有研究意义的企业数据出境监管相关问题，不同讨论企业数据入境监管问题。

3．数字贸易、电子商务与企业数据跨境传输的概念辨析

数字贸易（digital trade）作为一种新型的贸易模式，目前还很少有国家将其从传统贸易中分离出来单独加以统计和研究。虽然诸多国家、组织和学者从不同角度对数字贸易进行了界定，但是其在国内外学术界还尚未形成一个公认的标准定义（刘洪愧，2020）。[19]有国外学者认为，总体来说，狭义的数字贸易被定义为“数字化产品贸易”，广义的数字贸易被定义为“利用数字技术开展业务”（Shamshad Akhtar、Hongjoo Hahm、Susan F.Stone，2016）。[20]

数字贸易最早起源于美国，2013 年 7 月，美国国际贸易委员会（United States International Trade Commission，USITC）在《美国和全球经济中的数字贸易Ⅰ》中总结认为，数字贸易是指通过网络传输而实现的产品和服务的交换活动，具体包括四方面内容：一是数字交付内容，如数字化的音乐、游戏、视频和书籍等；二是社交媒体，如社交网站、用户评价网站等；三是包括普通搜索引擎和专业搜索引擎在内的搜索引擎；四是其他数字化产品和服务，如应用软件、通过云计算提供的数据和计算服务以及通过互联网传递的通信服务等（USITC，2013）。[21]但该定义主要强调数字贸易产品和服务必须通过互联网实现交付，排除了大部分借助互联网实现交易的实物产品。美国贸易代表办公室（the Office of the U.S.Trade Representative，USTR）在 2017 年发布的《数字贸易的主要壁垒》中也指出，数字贸易是一个比较宽泛的概念，它既包括在互联网上的产品销售和线上服务的提供，又包括能够实现全球价值链（Global Value Chain，GVC）的数据流、实现智能制造的服务等（USTR，2017）。[22]国外学者 Mitchell 等在研究数字贸易中的比较优势问题时提出，国际数字贸易是一种涉及多国的贸易活动，其中所包含的某些贸易产品本身就是数字产品，或者贸易产品的订购、交付、支付或服务中的任何一个步骤或环节是通过互联网技术或数字技术来实现的（Andrew D.Mitchell、Jarrod Hepburn，2017）。[23]

国内方面，马述忠等对数字贸易的内涵进行了系统梳理，将其定义为：通过信息通信技术（ICT）的有效使用以实现传统有形货物、新型数字产品与服务、数字化知识与信息的高效交换，进而推动消费互联网向产业互联网转型并最终实现制造业智能化的新型贸易活动，是传统贸易在数字经济时代的拓展与延伸（马述忠、

---

[19] 刘洪愧：《数字贸易发展的经济效应与推进方略》，载《改革》2020 年第 3 期，第 40 页。

[20] See Shamshad Akhtar, Hongjoo Hahm, Susan F.Stone, *Asia-Pacific Trade and Investment Report 2016*, http//: www.unescap.org/sites/default/files/publications/aptir-2016-full.pdf（last visited May 11, 2021).

[21] U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part I*, https://www.usitc.gov/publications/industry_econ_analysis_332/2013/digital_trade_us_and_global_economies_part_1.htm（last visited May 11, 2021).

[22] The Office of the U.S.Trade Representative, *Key Barriers to Digital Trade*, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade（last visited May 11, 2021).

[23] Andrew D.Mitchell, Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 Yale Journal of Law and Technology 196（2017）.

房超、梁银锋，2019）。[24]伊万·沙拉法诺夫等则从广义的角度认为，数字贸易包括信息通信技术产品和服务的交易、数字产品及服务、人员流动和数据传输四个核心因素（伊万·沙拉法诺夫、白树强，2018）。[25]余振认为，根据各国有关数字贸易的法律和政策性文件，可以将数字贸易规则分为四类。第一，数据监管类政策，主要是对数据使用的管理，包括数据隐私保护、跨境数据流动、计算机本地化等。第二，网络平台管理政策，主要为了规范网络运营商的中介服务，包括网络内容许可和访问、互联网平台(ISP)中介责任、知识产权保护等。第三，产品和服务贸易政策，指对线上交易的产品和服务，以及数字技术产品的管理，包括线上销售管理、税收和补贴、政府采购、技术标准等。第四，数字企业的本地进入政策，包括投资、市场竞争等（余振，2020）。[26]

总体来说，目前还不存在被普遍接受的关于数字贸易的标准定义，但学术界和研究机构基本一致认为其既包括借助互联网及网上平台进行交易的货物和服务，也包括通过网络直接提供的数字产品和服务。

对于电子商务（e-commerce）的概念，2018 年美墨加三国签订的《美加墨协定》（United States-Mexico-Canada Agreement，USMCA）直接将“电子商务”章节表述为“数字贸易”（digital trade）。[27]林福辰、杜玉琼认为，该表述进一步凸显了新交易范式不同于传统贸易形式的数字化特征，明确了数据对交易环节的关键性影响（林福辰、杜玉琼，2020）。[28]美国更加看重的是贸易的数字性质，核心在于跨境数据流动，并不特意区分货物或服务贸易，倾向于用“数字贸易”术语取代“电子商务”，并且其认为其他国际组织对“电子商务”的界定过于狭窄，可能会影响这一术语在 WTO 框架内的使用（WTO，2019）。[29]因此，由于“数字贸易”的定义未完全达成一致，“电子商务”的表述只是为了区分在货物贸易（trade in goods）和服务贸易（trade in services）中的企业数据传输，“电子商务”在实质上也可以归为“数字贸易”的概念之中，只是界定范围比数字贸易狭窄。

从以上梳理中不难看出，虽然数字贸易定义仍存在分歧，但与企业数据跨境传输关系密切。总体来说，企业数据跨境传输是数字贸易的构成部分，企业数据的跨境传输可以认定为“通过网络直接提供的数字产品和服务”，这也是国际合作中对于数据跨境传输相关跨境货物、服务贸易的处理方式。

---

[24] 马述忠、房超、梁银锋：《数字贸易及其时代价值与研究展望》，载《国际贸易问题》2019 年第 2 期，第 176 页。

[25] 伊万·沙拉法诺夫、白树强：《WTO 视角下数字产品贸易合作机制研究——基于数字贸易发展现状及壁垒研究》，载《国际贸易问题》2018 年第 2 期，第 149 页。

[26] 余振：《全球数字贸易政策：国别特征、立场分野与发展趋势》，载《国外社会科学》2020 年第 4 期，第 36 页。

[27] United States-Mexico-Canada Agreement, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement（last visited May 11, 2021).

[28] 林福辰、杜玉琼：《发展与蜕变：多边视域下数字贸易规则建构路径之审思》，载《江海学刊》2020 年第 5 期，第 160 页。

[29] WTO, INF/ECOM/5, March 25, 2019.

（三）企业数据出境监管的基础理论研究

1．数据权益的探讨

梅夏英、龙卫球、李爱君等国内学者较早对数据权益进行了系统探讨。龙卫球认为在当前数据经济的环境下，面向个人信息和数据利益关系的法律建构，应与数据经济的结构本质、特别是其双向动态特点紧密结合，采取一种更加复杂的权利配置方式。从体系上说，应该在区分个人信息和数据资产的基础上，进行两个阶段的权利建构：首先对于用户，应在个人信息或者说初始数据的层面，同时配置人格权益和财产权益；其次对于数据经营者(企业)，基于数据经营和利益驱动的机制需求，应分别配置数据经营权和数据资产权（龙卫球，2017）。[30]李爱君也认为，由于数据具有客体属性、确定性、独立性，存在于人体之外，因此数据权利属于民事权利。但由于数据权利客体“数据”的自然属性与现有的民事权利客体的自然属性不同，所以数据权利是具有财产权属性、人格权属性、国家主权属性的新型的民事权利（李爱君，2018）。[31]国外学者 Lawrence Lessig 在更早的时候也提出，可以通过赋予数据以财产权的方式来强化数据本身的经济驱动功能，以打破传统法律思维之下依据单纯隐私或信息绝对化过度保护用户而限制、阻碍数据收集、流通等活动的僵化格局（Lawrence Lessig，2000）。[32]

而梅夏英持相反观点，认为计算机数据是不是财产以及其与民法客体的关系问题在民法理论上缺乏基础性研究，既有的网络民事纠纷裁判及理论研究倾向于单独将数据进行客体化和财产化的处理。数据没有特定性、独立性，亦不属于无形物，不能归入表彰民事权利的客体；数据无独立经济价值，其交易性受制于信息的内容，且其价值实现依赖于数据安全和自我控制保护，因此也不宜将其独立视作财产。基于数据的非客体性，大数据交易的合同性质宜界定为数据服务合同；基于主体不确定、外部性问题和垄断性的缺乏，数据权利化也难以实现。数据具有工具中立性的本质特征，法律能够对其实现的规制功能有限。网络民事纠纷可以区分为工具性和虚拟性两类，分别适用一般侵权救济和违反保护他人法律的侵权救济（梅夏英，2016）。[33]

上述学者对数据权益的争议，目前为止在学界仍无定论，但梅夏英的观点已逐渐占据主流。本人倾向于梅夏英对于数据权益的观点。数据具有明显区别于传统民法中物权的特征，为了将数据纳入法律规则，勉强赋予其财产权，会导致很多相关法律问题无法处理，如企业数据中有来自于个人的数据，那么这些个人数据的财产权到底归个人所有，还是企业所有？在梅夏英的数据权益理论下，不设立数据财产权，而是通过“数据控制”理论来处理数据法律问题，在此基础上，企业数据的跨

---

[30] 龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期，第 65 页。
[31] 李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期，第 69 页。
[32] Lessig, L., *Cyberspace and Privacy: A New Legal Paradigm: Foreword*, STANFORD LAW REVIEW (2000).
[33] 梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016 年第 9 期，第 164-183 页。

境传输问题，涉及得为数据控制者及其行为的监管，本论文也是在此基础上展开的。

2．企业数据权益的探讨

丁晓东在否认数据财产权基础上，认为数据已经成为企业的重要资产，但对企业数据不宜进行绝对化与排他性的财产权保护，因为此种保护违背数据的基本特征——数据并不具有排他性与竞争性。保护企业数据权益应当以促进数据共享为目标，企业数据的合理保护应当有利于促进数据共享。对企业数据应当进行类型化与场景化保护。对于非公开的企业数据，应当提供商业秘密保护；对于半公开的数据库数据，应当提供类似欧盟的数据库特殊权利保护；对于公开的网络平台数据，应当采取竞争法保护，避免恶性搭便车行为（丁晓东，2020）。[34]

龙卫球在肯定数据财产权基础上，认为从私法保护角度来说，企业数据保护走出借用传统法律的策略转向数据新型财产权化新机制，时所必然、事所必然。他提出，应该注意企业数据保护形式上虽然采取私权形式，但与民法上典型的财产权不同，需要兼顾多种功能、多种利益协同的保障要求，因此无法采取简单意义的财产权构造，而是需要呈现为一种具有极强外部协同性的复杂财产权设计（龙卫球，2018）。[35]

时明涛则提出了折中的观点，认为既有立法例多以个人数据保护为中心，从中反向推导出企业的数据权利范围。这一立法模式因个人数据权利难以精确界定，导致企业数据权利边界模糊。赋权保护说虽已明确意识到数据权属界定的积极意义，却没有考虑到企业数据来源的多样性而陷入了一体保护主义。我国未来数据权利保护立法宜采取正面界定的方法，明确企业对数据产品及非个人数据享有占有、使用、收益、处分等所有者权益；对企业数据中涉及个人数据的部分，借鉴数据控制者的立法设计，构建企业对个人数据的权限范围与义务内容（时明涛，2020）。[36]

由于对于数据财产权是否存在的争议，导致企业数据权益也存在争议。上述学者分别从否认数据财产权、肯定数据财产权和折中的三个立场，对企业权益进行了探讨。企业数据的合理保护应当有利于促进数据共享。简单的为企业数据设定财产权，由于数据来源的多样性，实践中难以实现有效保护。另一方面，设计复杂的企业数据财产权，又可能导致了立法困难和司法冲突，不是企业数据立法最优选择。因此，对企业数据进行分类型化、分场景化进行监管，是本论文采取的立场。

[34] 丁晓东：《论企业数据权益的法律保护——基于数据法律性质的分析》，载《法律科学(西北政法大学学报)》2020 年第 2 期，第 90-99 页。
[35] 龙卫球：《再论企业数据保护的财产权化路径》，载《东方法学》2018 年第 3 期，第 53 页。
[36] 时明涛：《大数据时代企业数据权利保护的困境与突破》，载《电子知识产权》2020 年第 7 期，第 61 页。

二、企业数据本地化要求及出境限制的国内外文献

（一）保护数据隐私与促进数据流动为分歧的企业数据出境限制监管博弈

企业数据跨境传输的数据不仅有企业数据，还包括个人数据。前者关乎企业创新价值，后者被视为隐私范畴。数据可以创造巨大价值，被视为重要的战略资产，但各方围绕数据安全的核心关切并不相同。例如，俄罗斯的态度则较为保守，在数据流动方面出台了很多限制性规定。美国看来，贸易规则最重要的目标是消除贸易壁垒，过度强调个人数据安全会阻碍跨境数据流动，是贸易保护主义的表现。欧洲将保护隐私置于较跨境数据流动更优先的地位，希望能在跨境隐私保护和数据流动之间保持平衡，为此可限制个人信息流向保护标准不足的国家。

1．以俄罗斯为代表的侧重数据隐私保护的企业数据出境限制监管

欧洲国际政治经济中心（European Centre for International Political Economy，ECIPE）2018 年 4 月发表的《数字贸易限制性指数》（Digital Trade Restrictiveness Index，DTRI）报告中显示，俄罗斯在“数据限制”指标中的“数据政策”分指标中排名最高。对于俄罗斯的企业数据出境限制监管，2015 世界经济论坛（World Economic Forum）报告认为，美国是推动数字贸易自由化最积极的国家，但其他国家对参与数据或数据服务相关贸易态度谨慎，俄罗斯、中国、印度、印度尼西亚和越南被美国认为是数字贸易限制最严格的国家。[37]

周念利、李金东、米铁男等对俄罗斯跨境数据传输进行了研究，他们认为俄罗斯制定了世界上最为严密的数据流动限制性政策。俄罗斯的数据流动限制措施具有 3 个典型特征：一是数据输出规则针对“白名单”和“黑名单”对象做出鲜明区分；二是设置严密的互联网准入和监管措施；三是实施严格甚至激进的数据本地化政策（周念利、李金东，2020）。[38]同样，米铁男研究了俄罗斯数据出境的限制，他指出，俄罗斯根据数据内容的合法性标准将其划分为可以流通的数据和禁止流通的数据，同时根据流通范围、方式等因素对内容合法的数据流通进行了相对化限制。俄罗斯在数据流通监管方面采取双重标准，同时规定应符合本地化的要求。他提出在监管方面，时至今日，俄罗斯数据流通监管制度越发呈现出极端态势，已经从地域管控演变为特定条件下的强制中断（米铁男，2021）。[39]

2014 年俄罗斯出台的《就“进一步明确互联网个人数据处理规范”对俄罗斯联邦系列法律的修正案》（Federal Law No. 242-FZ）要求所有收集俄罗斯公民个人数据的企业在俄罗斯联邦的数据库中“记录、系统化、积累、存储、更新、更改和

---

[37] World Economic Forum, *The High and Low Politics of Trade：Can the World Trade Organization's Centrality Be Restored in a New Multi-Tiered Global Trading System?*,https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.4362&rep=rep1&type=pdf（last visited May 11, 2021).

[38] 周念利、李金东：《俄罗斯出台的与贸易相关的数据流动限制性措施研究——兼谈对中国的启示》，载《国际商务研究》2020 年第 3 期，第 85 页。

[39] 米铁男：《俄罗斯网络数据流通监管研究》，载《中国应用法学》2021 年第 1 期，第 207 页。

检索该信息”。[40]处理俄罗斯公民个人数据的运营商，必须通知俄罗斯联邦通信、信息技术和大众媒体监督局（The Federal Service for Supervision of Communications, Information Technology and Mass Media，Roskomnadzor）[41]存储此类个人数据的服务器所在地，而且该法律也适用于参与处理俄罗斯公民个人数据的外国公司。此外，俄罗斯通信部要求电信和互联网提供商安装设备，在其服务器上收集和保留数据至少 12 小时以便俄罗斯联邦安全局（Federal Security Service，FSB）在必要时访问数据。这些数据包括用户的电话号码、流行的国内和国外在线资源（如 Gmail、Yandex、Mail.ru 等）的帐户信息、IP 地址和位置数据。[42]

此后随着网络安全状况的日益严峻和国际网络力量的博弈，俄罗斯最终选择了实行所谓的“孤岛计划”，尤其是随着《主权互联网法》[43]的颁行更是主动采取了断网行动，使其此前的数据本地化制度得到了进一步强化。

2．以美国为代表的侧重数据自由流动的企业数据出境限制监管

美国以促进跨境数据自由流动思想为主导，自 2004 年起促成了多个跨境数据自由流动的国际协定。2004 年美国促成亚太经合组织（APEC）通过了《亚洲太平洋经济合作组织隐私框架》（APEC Privacy Framework），要求成员国“采取一切合理步骤避免任何不必要的数据流动障碍”。[44]这是亚太地区第一份有关跨境数据流动规则的指导性文件。随后几年，美国力争将跨境数据流动的有关内容纳入自由贸易协定（Free Trade Agreement，FTA）谈判并取得成效，如 2012 年与韩国达成《美韩自由贸易协定》（U.S.—South Korea Free Trade Agreement），推行跨境数据自由流动的主张。[45]2015 年，美国主导促成了《跨太平洋战略经济伙伴关系协定》（Trans-Pacific Partnership Agreement，TPP）通过，专门设置了“商业信息跨境自由传输条款”，美国“跨境数据自由流动”的规则被缔约成员国接受。[46]尽管美国于 2017 年 1 月宣布正式退出 TPP，但该协定的国际影响力依然存在。2018 年 3 月 23 日，美国总统特朗普签署通过《澄清域外合法使用数据法案》（Clarifying Lawful

[40] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks，https://pd.rkn.gov.ru/authority/p146/p191/（last visited May 11, 2021).

[41] 它既是被授权保护个人数据的联邦执行机构，也是负责俄罗斯互联网审查的机构。参见 Federal Service for Supervision of Communications, Information Technology and Mass Media，http://government.ru/en/department/58/（last visited May 11, 2021).

[42] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks，https://pd.rkn.gov.ru/authority/p146/p191/（last visited May 11, 2021).

[43] В РФ приняты ограничивающие законы о «суверенном интернете»，https://rusidea.org/250950141（last visited May 11, 2021).

[44] APEC Privacy Framework，https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx（last visited May 11, 2021).

[45] U. S.-South Korea Free Trade Agreement，https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta（last visited May 11, 2021).

[46] Summary of the Trans-Pacific Partnership Agreement，https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership（last visited May 11, 2021).

Overseas Use of Data Act， CLOUD 法案），标志美国新时期“数据主权战略”的实施。该法案采取的是“数据控制者标准”，进一步放开跨境数据流动，允许符合资格的外国政府调取存储于美国的数据。[47]这样，美国法律就可以覆盖至全球运营的美国企业数据，为其获取商业利益提供保障。

2019 年 1 月，WTO 成员签署《电子商务联合声明》（Joint Statement on Electronic Commerce）确认启动与贸易有关的、旨在确立电子商务/数字贸易领域国际规则议题的谈判上，美国提案指出，跨境数据传输在国际贸易中的重要性日益显现，推动各个产业增长和带来巨大的经济收益，主张成员国不应该禁止、限制、歧视性地管理个人和企业跨境数据传输，不应强制企业在司法管辖区内建设或使用特定的数字基础设施，同时没有提出明确的个人隐私保护主张。[48]综上美国制定或参与的规则，美国在企业数据跨境传输方面，单方面强调跨境数据自由流动，忽略他国数据监管治理诉求（岳云嵩、霍鹏，2021）。[49]

美国要求企业数据跨境自由传输的立场，有其对经济利益的追求和本国隐私权规定的缺失有关。张俊娥、董晓红认为，经济利益的追求方面，对于美国数字企业进入其他国家的情形，由于美国本土企业能够提供优质的云计算和储存服务，若别国强制美国使用其本土服务器来进行储存，将减少美国本土计算设施的使用及盈利机会。如果储存器设置在其他国家，美国获取数据时同样会面临别国监管政策限制。鉴于此，美国一再推崇“数据存储非强制本地化”，意图实现本国企业在其他国家或地区数据存储设施的产地、国别自由化（张俊娥、董晓红，2021）。[50]另一方面，美国隐私权规定缺失，隐私权从未明示于美国宪法和修正案之中，未能为保护个人信息提供直接的宪法依据。[51] Robert Wolfe 研究了美国一些州宪法中包含的隐私权条款，他认为，与《通用数据保护条例》（GDPR）为欧盟公民提供了全面的个人信息保护相比，美国的保护路径显得分散且缺乏统一的法律依据，就像是一件令人困惑的拼凑品（Robert Wolfe，2019）。[52]柯静也认为，接连发生的美国互联网巨头泄露用户信息事件，如 Facebook 大规模用户信息泄密事件、Amazon 涉嫌利用平台第三方商家收集个人信息牟利事件、Googel“夜莺计划”等，更是验证了欧盟对美国隐私保护的担忧（柯静，2020）。[53]

---

[47] H.R.4943-CLOUD Act，https://www.congress.gov/bill/115th-congress/house-bill/4943（last visited May 11, 2021).
[48] Joint Statement on Electronic Commerce ， https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf（last visited May 11, 2021).
[49] 岳云嵩、霍鹏：《WTO 电子商务谈判与数字贸易规则博弈》，载《国际商务研究》2021 年第 1 期，第 84 页。
[50] 张俊娥、董晓红：《从 USMCA 看中美数字贸易规则领域的分歧及中国应对策略》，载《对外经贸实务》2021 年第 2 期，第 42 页。
[51] 美国宪法第四修正案规定：“任何人的人身、住宅、文件和财产不受无理搜查和查封”，案例中通常被解释为个人隐私不受政府官员的无理搜查和查封，但它并不适用于私人企业收集和处理个人信息的情形。
[52] Robert Wolfe, *Leaning about Digital Trade: Privacy and Ecommerce in CETA and TPP*, WORLD TRADE REVIEW 69（2019）.
[53] 柯静：《WTO 电子商务谈判与全球数字贸易规则走向》，载《国际展望》2020 年第 3 期，第 48 页。

另一方面，美国并非没有数据出境限制。对于在数据存储地方面的跨境数据传输要求，可以说美国实行的是两套标准。对于别国数字企业进驻美国市场的情况，美国虽然声称奉行数据存储地自由化，但往往又会以国家安全为由，强制要求企业将数据存储地设置在美国（张俊娥、董晓红，2021）。[54]我国的 Tiktok、Wechat 均在担保将数据存储在美国后，才获准入驻。因担心企业专有信息泄露会削弱其技术领先优势，美国主张严格禁止本地化。为确保万无一失，《美日数字贸易协定》（Agreement between United States and Japan Concerning Digital Trade）在《美墨加协定》（USMCA）基础上增加了安全例外条款，以国际法中“自裁决”性质的表述和对“基本安全利益”不进行限定的方式，使美国拥有极大的自由裁量权。[55]

3．以欧盟为代表的平衡数据隐私与流动的企业数据出境限制监管

欧盟等发达经济体和部分高收入发展中经济体，同时强调跨境数据自由流动和个人隐私保护。早在 1981 年，欧洲第一部规制跨境数据流动的法律文件——《与个人数据自动化处理有关的个人保护公约》（European Treaty Series，No. 108）获得通过，规定成员国可以制定相关规定，对跨境数据流动进行限制。[56]随着时间的推移，欧盟逐渐意识到跨境数据流动的潜在风险，于是对数据跨境流动的规制愈加严格。1995 年，欧盟发布的《个人数据保护指令》（EU Directive 95/46/EC，第 95/46/EC 指令）提高了数据保护标准，规定只有当输出国达到欧盟认可的充分保护水平（Adequate protection）才能进行数据跨境传输。[57]为了适应新兴信息技术如云计算、大数据、智能终端等对个人数据保护造成的影响和冲击，构建统一的跨境数据流动法律框架，2016 年 4 月 14 日欧盟理事会通过了新的法律——《通用数据保护条例》（General Data Protection Regulation，GDPR），并于 2018 年 5 月 25 日正式生效、实施。GDPR 被称为欧盟“史上最严格”的数据保护法规，重申“不允许将公民的个人数据传输至境外不能提供充分保护的地区和国家”，在原有基础上增加了更多跨境数据流动的条件。[58]对此，金晶认为，GDPR 以保护前置的理念构建了数据主体权利，将类型化的数据保护前置到数据收集、处理阶段（金晶，2018）。[59]

2019 年 1 月 WTO 成员签署《电子商务联合声明》（Joint Statement on Electronic

---

[54] 张俊娥、董晓红：《从 USMCA 看中美数字贸易规则领域的分歧及中国应对策略》，载《对外经贸实务》2021 年第 2 期，第 42 页。

[55] Agreement between United States and Japan Concerning Digital Trade, Article 4. 该条款第一句规定禁止要求一方提供或允许接触该方判定的（it determines）与其基本安全利益相抵触的任何信息；第二句规定不得阻止一方采取它认为的（it considers）为履行其维持或恢复国际和平、安全或保护其基本安全利益所必需的措施。“该方判定的”“它认为的”是国际法中“自裁决”性质的表述方式，旨在将“基本安全利益”的裁量权交由本国而非第三方行使，以保留本国经济主权。与此同时，条款并未对“基本安全利益”定义或进行范围限定。

[56] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data，https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108（last visited May 11, 2021).

[57] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data，https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML（last visited May 11, 2021).

[58] General Data Protection Regulation(GDPR)，https://gdpr-info.eu/.

[59] 金晶：《欧盟<一般数据保护条例>：演进、要点与疑义》，载《欧洲研究》2018 年第 4 期，第 2 页。

Commerce）确认启动与贸易有关的电子商务议题谈判上，欧盟提案反映了其高自由和严治理的双重特点，主张成员国应确保跨境数据流动，不应对数据的存储、处理设备和所在地施加本地化限制，但是协定内容不能限制成员国采取适当措施保护本国公民的个人资料和隐私。日本、加拿大、新加坡、巴西等国对跨境数据自由流动和存储本地化限制方面的主张也基本一致，不过均加入了监管要求。[60]

欧盟的上述数据保护立法，其保护规范遵循两大目标，个人数据保护以及数据自由流动，前者是后者的前提。因此，数据保护法案的内容主要围绕如何对数据跨境流动中的个人数据予以保护展开。欧盟通过在法律层面统一成员国之间数据保护水平，消除了法律差异性导致的法律壁垒，实现了数据在成员国之间自由流动。对于数据向联盟外国家和地区流动的情形，欧盟法上贯彻充分保护原则（Adequate protection），对数据接收国或者接收者保护水平进行评估，以此裁定和批准个人数据的跨境传输。基于充分保护原则，欧盟发展出了以“充分性认定”（Adequacy Decision，亦译为“充分决定”）机制为核心，其他合理保障措施机制和例外情形为补充的数据跨境流动规制体系。[61]获得充分性认定的国家、地区或者国际组织，无需经过欧盟数据监管机构的事前授权，就可以实现与欧盟之间的数据自由跨境传输。

欧盟“充分性认定”机制是一种基于国家或者地区法律保护水平的立法设计，核心是对一国数据保护体系和实施机制的评估，最初目的是希望公民的个人数据在流出欧盟区域后仍然能够得到持续的保护，本质上是一国国内法律范畴内的评估。随着该机制的实施，该制度已发展成为欧盟数据保护法全球化的重要路径。

（二）企业数据出境限制中的数据本地化监管争议

1．数据本地化的国家安全考量

“数据本地化”法律通常要求在该国家内存储或处理从特定国家收集的某些类型的数据。换句话说，由国家本地化法管辖的那些类型的数据不能转移到另一个国家进行存储和处理，即数据必须在位于该国家的服务器上存储或处理。数据本地化法律有时被称为“数据主权法”，因为它们反映了某个国家对源自该国的数据的主权主张。

制定企业数据出境“数据本地化”限制，本质上是数据出境国对于保护国家安全的考量。俄罗斯、中国、印度、巴西均以限制重要数据出境、数据本地化储存维护国家利益与安全，其中最为直接具体的推动因素就是由斯诺登曝光的“棱镜门”事件，该事件把数据安全问题暴露无遗（米铁男，2021）。[62]发展中国家由于缺乏

---

[60] Joint Statement on Electronic Commerce，https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf（last visited May 11, 2021).

[61] General Data Protection Regulation(GDPR)，https://gdpr-info.eu/（last visited May 11, 2021).《通用数据保护条例》第 46 条规定了合理保障措施内容，包括数据保护标准条款、公司约束规则、行为准则等。

[62] 米铁男：《俄罗斯网络数据流通监管研究》，载《中国应用法学》2021 年第 1 期，第 202 页。

强有力的数据引流能力，如果放开管制，反而可能导致数据大规模向发达经济体输出，进一步削弱竞争力，国家安全也受到威胁。因此，大部分发展中国家采取严格限制数据流动的本地化政策。

2．数据本地化对跨境经济发展的抑制

“数据本地化”对跨境经济发展的抑制体现在两个方面。一方面，数据流动限制会提高跨境贸易成本。Ferracane 等研究者通过研究欧洲国际政治经济中心（ECIPE）对 64 个国家包括数据流动限制在内的数字贸易壁垒水平进行的评估打分，认为分数越高表明限制越多，由此带来的贸易成本也越高（Martina F. Ferracane，Hamburg University et al.，2018）。[63]ECIPE 的研究也表明，一些国家实施数据本地化政策会给该国的 GDP 带来损失，数据本地化措施会造成巴西 GDP 下降 0.2%、中国下降 1.1%、欧盟下降 0.4%、印度下降 0.1%、印度尼西亚下降 0.5%、韩国下降 0.4%和越南下降 1.7%（周念利、李金东，2020）。[64]

另一方面，过度的“数据本地化”措施会对降低本国企业的国际竞争力。刘洪愧认为，数据本地化要求限制了许多依赖数据流动的服务贸易的发展（如云计算、大数据、金融服务），也增加了企业数据存储的成本，造成规模不经济，特别是对中小企业非常不利（刘洪愧，2020）。[65]俄罗斯大力推动的“数据本地化”跨境数据传限制，可能会对那些依靠互联网进行交易、以服务海外客户并提高运营效率的公司构成障碍。

3．数据本地化的企业数据出境限制监管平衡机制

极端“数据本地化”的企业数据出境限制，并不可取。俄罗斯采用孤岛模式治理网络，显然是目前世界上规制数据流通的极端做法。从其目的来看具有正当性，是为了维护国家安全而不是为了侵害他国利益或者本国公民的利益。从手段来看，确实发挥了达到上述目的的作用。但米铁男认为，数据流通的孤岛模式未必适合其他国家，该模式是俄罗斯根据自身的网络安全状况进行评估后所采取的措施，立场特征显著（米铁男，2021）。[66]薛亚君通过对比认为，美国主张跨境数据自由流动，反对数据本地化措施，欧盟强调对区域安全和个人隐私有影响的数据应当采取本地化措施，而许多发展中国家则偏好数据本地化措施。他提出，我国应当在兼顾数据安全与经济发展的前提下，对相关数据进行分类监管，以确定我国数据本地化措施的范围（薛亚君，2019）。[67] Casalini 和 González 也从数据分类的角度进行阐述，他们认为，已有的数据跨境流动法律规制模式并未区分各个数据类型及细分领域，

---

[63] Martina F. Ferracane，Hamburg University et al., *Do Data Policy Restrictions Inhibit Trade in Services?,* https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf

[64] 周念利、李金东：《俄罗斯出台的与贸易相关的数据流动限制性措施研究——兼谈对中国的启示》，载《国际商务研究》2020 年第 3 期，第 85 页。

[65] 刘洪愧：《数字贸易发展的经济效应与推进方略》，载《改革》2020 年第 3 期，第 50 页。

[66] 米铁男：《俄罗斯网络数据流通监管研究》，载《中国应用法学》2021 年第 1 期，第 216 页。

[67] 薛亚君：《数字贸易规则中的数据本地化问题探究》，载《对外经贸实务》2019 年第 8 期，第 20 页。

而是采用了笼统的整体规制方式，缺乏针对性与灵活性，使得整个跨境数据流动的治理效果将大打折扣（Casalini, F., J. González，2019）。[68]

Daniel Castro 认为，正如美国信息科技与创新基金会（Information Technology & Innovation Foundation，ITIF）在一份报告中明确指出的那样，要求数据不得离开一个国家的强制性要求，绝对不会增加隐私性或安全性（Daniel Castro，2013）。[69] Stephen Ezell 等学者认为，这种对数据的保护采取的行动多种多样并且动机各不相同，但其中一种动机是被误导的自利性，即错误地认为，如果限制数据流动，数据相关工作可以转移到本国公司，从而获益（Stephen Ezell、Robert Atkinson、Michelle Wein，2013）。[70]但是，当涉及到数据安全性时，它并不取决于数据的存储位置，而是取决于存储数据的方式，老挝的安全服务器与巴西的安全服务器没有什么不同（范思博，2020）。[71]许可则反思“数据本地化”的立法意图，他认为国家对数据管控并不完全等同于“数据本地化”，在“数据出境”的场景中，国家管控体现为对一国境内的数据被他国个人、企业或其他私人组织处理的限制，人们往往将该等“出境数据管控”称为“数据本地化”（data localization），但这种说法可能忽略了两者微妙而重大的差异（许可，2021）。[72]

另一方面，实践中当前各国的“数据本地化”限制的推进也面临重重阻碍（孙方江，2021）。[73]比如，印度本土化政策受到美国阻拦，仅实现了支付系统数据本土化储存。2018 年印度《个人数据保护法案（草案）》（Draft Personal Data Protection Bill 2018）拟限制数据跨境流动，规定一般和敏感个人数据必须在境内留存副本，关键个人数据不得出境。但该法案遭到 Facebook、Mastercard、Visa、American Express、Paypal、Amazon、Microsoft 等美国支付和科技巨头强烈反对，称其为“新德里地方保护主义”。迫于压力，该草案在 2019 年已经进行了修改，规定敏感、关键个人数据在符合一定条件时可以向境外传输，但存储应继续留在境内，关键个人数据只能在印度处理。[74]又如，巴西出于国家安全考虑，也希望推行本土化政策，但其在云计算、大数据等技术方面发展相对滞后，技术条件不满足数据的境内储存。巴西《中央银行条例》（Brazilian Central Bank Regulation）规定，金融机构应尽量使用境内数据库，如果使用外部服务器，必须满足相应的数据保护条件，在巴西央行与外部服务器所在国监管机构签订协议后方可传输。[75]

---

[68] Casalini, F., J. González, *Trade and Cross-Border Data Flows*, 220 OECD TRADE POLICY PAPERS 17 (2019).
[69] Daniel Castro, *The False Promise of Data Nationalism*, 2 THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION 232 (2013).
[70] Stephen Ezell, Robert Atkinson, Michelle Wein, *Localization Barriers to Trade: Threat to the Global Innovation Economy*, 2 THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION 45 (2013).
[71] 范思博：《数据跨境流动中的个人数据保护》，载《电子知识产权》2020 年第 6 期，第 94 页。
[72] 许可：《自由与安全：数据跨境流动的中国方案》，载《环球法律评论》2021 年第 1 期，第 27 页。
[73] 孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 3 页。
[74] Draft Personal Data Protection Bill, 2018，https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018（last visited May 11, 2021).
[75] Lei Geral de Proteção de Dados Pessoais（LGPD），https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-ger

对于企业数据出境“数据本地化”监管要求的平衡，一是可以施行区分行业并结合数据出境安全评估的“数据本地化”措施，如澳大利亚、加拿大、新西兰、土耳其和委内瑞拉的数据本地化法律则仅适用于特定的行业，如医疗、电信、金融和国家安全等领域，针对特定行业进行数据本地化（戴艺晗，2021）。[76]二是，通过发展互联网产业，降低数据本地化带来的额外成本。如在政策上向国内新兴的数据提供商提供更多便利与支持，大力发展大数据等解决方案，在减少国内企业由于数据本地化而花费额外成本的前提条件下，促进重要数据及公民个人数据存储于国内，维护网络数据安全（周念利、李金东，2020）。[77]

（三）企业数据出境前的数据安全评估

企业数据出境前的安全评估，也是决定国内企业数据能否跨境传输出境的一种限制。以被评估的对象区分，企业数据出境前的安全评估可以分为对数据接收国数据保护立法状况的评估，以及对企业出境数据本身安全性的评估。对于企业出境数据本身安全性的评估，又可以分为以是否为“机器产生的非个人数据”的数据安全评估，和以行业领域区分的数据安全评估。

1．对数据接收国数据保护立法状况的评估

对企业数据出境数据接受国保护立法状况的评估，最有代表性的为欧盟的“充分性认定”（Adequacy Decision）机制。为避免欧盟数据传输至他国后保护水平下降，《通用数据保护条例》（GDPR）第 44 条至第 50 条禁止将境内个人数据传输至保护充分性不足、无适当安全维护措施、亦不符合特定例外情况的第三国。[78]欧盟严格执行对他国数据保护立法水平的评估，如在 Schrems II 中即能体现，欧盟指出，美国《外国情报监控法案》（Foreign Intelligence Surveillance Act）的存在，使之可能超过必要限度访问所传输的数据，且无法给欧盟居民提供必要救济，因此宣告美欧《隐私盾协议》无效。[79]

对数据接收国数据保护立法状况进行“充分保护”（adequate protection）水平评估的意义在于，获得“充分性认定”（Adequacy Decision）的国家、地区或者国际组织，无需经过欧盟数据监管机构的事前授权，就可以实现与欧盟之间的数据自由跨境传输。从另外一个角度说，这种对数据接收国数据保护立法状况的评估，也是对向未被列入“白名单国家/地区”的数据接收国传输企业数据的限制。

2．对机器产生的非个人数据的分类安全评估

企业在经营活动中获得的企业数据，既包括个人数据（personal data），也包

---

al-de-protecao-de-dados-pessoais-lgpd（last visited May 11, 2021).

[76] 戴艺晗：《贸易数字化与监管碎片化：国际贸易制度框架下跨境数据流动治理的挑战与应对》，载《国际经济法学刊》2021 年第 1 期，第 6 页。

[77] 周念利、李金东：《俄罗斯出台的与贸易相关的数据流动限制性措施研究——兼谈对中国的启示》，载《国际商务研究》2020 年第 3 期，第 95 页。

[78] General Data Protection Regulation(GDPR)，Article 44-50.

[79] Facebook Ireland v. Schrems (Schrems II)（the European Union Court of Justice, 2020）.

括非个人数据（non-personal data）。个人数据是指与已识别或可识别自然人有关的各种信息，个人数据敏感度较高，一旦发生泄露可能会直接造成个人利益受损。以个人金融信息为例，其主要涵盖账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等。[80]非个人数据是指匿名化处理的数据，敏感度相对较低，不能指向已识别或可识别自然人，例如用于大数据、人工智能等分析结果、统计数据或不可还原的匿名数据集等。一般而言，跨境数据流动的限制主要集中在个人数据，而对非个人数据则以促进开放、共享、自由流动的监管思路为主（孙方江，2021）。[81]

欧盟已经有相关立法和实践，通过“非个人数据”的定义对企业数据进行分类，限制企业数据中的“个人数据”跨境传输，促进企业数据中的“非个人数据”跨境传输。依据欧盟颁布的自 2019 年 5 月 28 日起适用的《非个人数据自由流动条例》（Regulation on a Framework for the Free Flow of Non-personal Data in the European Union），该条例旨在消除非个人数据在欧洲成员国和 IT 系统之间自由流动的障碍，以达到对于非个人数据跨境自由流动和共享，鼓励公平竞争和后续创新（王中美，2020）。[82]通过会员国间的云服务器，欧盟监管部门和各会员国都将保留对数据的访问权限，每个组织都能够在欧盟任何地方存储和处理非个人数据。[83]

对企业数据是否为“非个人数据”的分类安全评估，使企业数据跨境传输的限制更加有针对性，更好的处理了企业数据中“个人数据”和“非个人数据”的关系，避免了笼统限制企业数据跨境传输的监管困境。

3．对涉及重点行业、领域企业数据的分类安全评估

随着企业数据出境愈加频繁，各国普遍认识到对涉及重点行业、领域企业数据的重要数据，进行本地化存储的重要意义，对于重要的数据禁止跨境流动。然而，各个国家对于重要数据的范围规定不同。

一是，以行业划分重要数据的范围。如在美国，并没有法律规定要求数据禁止跨境流动，但是在美国的外资安全审查机制中，如 CLOUD 法案中，对于国外网络运营商通常会要求其与电信小组签署安全协定，要求其国内通信基础设施应位于美国境内，将通信数据、交易数据、用户信息等仅存储在美国境内。[84]印度的电信许可协议中要求各类电信企业（包括互联网服务提供商），不允许将用户账户信息、用户个人信息（除了外国用户的漫游信息）转移至境外，否则可能面临吊销许可证的后果。此外，对于金融领域的关键数据，印度央行已于 2017 年禁止跨行、行内

[80] 《中国人民银行关于发布金融行业标准 做好个人信息保护技术管理的通知》，银发〔2020〕45 号。
[81] 孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 3 页。
[82] 王中美：《欧盟数据战略的目标冲突与中间道路》，载《国际关系研究》2020 年第 6 期，第 43 页。
[83] Free Flow of Non-personal Data，https://digital-strategy.ec.europa.eu/en/policies/non-personal-data（last visited May 11, 2021).
[84] H.R.4943-CLOUD Act，https://www.congress.gov/bill/115th-congress/house-bill/4943（last visited May 11, 2021).

支付系统产生的数据出境，且支付系统运营商和商业银行必须对技术服务提供商进行管理，确保所有数据本土化储存和处理。每个数据受托人应确保在印度境内服务器或数据中心存储至少一份个人数据的服务副本，关键个人数据必须在位于印度的服务器或数据中心中处理。[85]韩国《信息通信网络的促进利用与信息保护法》（The Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.）规定，政府可要求信息通信服务的提供商或用户采取必要手段防止任何有关工业、经济、科学、技术等的重要信息通过信息通信网络向国外流动。[86]

二是，以政府和公共部门数据为重要数据，针对政府和公共部门的数据跨境实施了限制条件及安全评估。如，加拿大财政委员会要求每一个政府机构对数据处理合同进行评估以识别任何与美国爱国者法案相关的潜在风险，评估风险层级，并且采取修正措施来解决安全风险问题。[87]澳大利亚《政府信息外包、离岸存储和处理ICT安排政策与风险管理指南》将政府信息分级，其中对于非保密的信息，要求政府机构要进安全风险评估之后才能实施外包，并且规定为政府部门开发的云服务，属于安全分类的数据不能储存在任何离岸公共云数据库中。[88]印尼在立法中要求，提供公共服务的电子系统运营商必须在印尼国内建立数据中心，交易数据必须存储在境内。

三是，只要涉及个人数据的都为重要数据。俄罗斯2014年出台了关于严格限制数据向境外流通的法案。对俄罗斯联邦公民个人信息进行搜集、记录、整理、保存、核对（更新、变动）、提取的数据库存放于俄罗斯境内。[89]

我国目前采用的也是以行业划分重要数据的范围。中国《网络安全法》第三十七条规定，对于某些关键信息基础设施运营者，其在境内收集或产生的个人信息及重要数据必须留存于境内，如中国人民银行《关于银行业金融机构做好个人金融信息保护工作的通知》中明确规定，境内收集的个人金融信息的存储、处理和分析工作应当在中国境内进行。

总体来看，当前的各国的企业数据出境前分类安全评估，主要与数据本地化措施相结合，考虑数据性质和数据用途对数据处理行为进行管理。一般认为金融数据、政府和公共部门数据、科技数据为重要数据。若企业出境数据中涉及这些类别的重

---

[85] Draft Personal Data Protection Bill, 2018，https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018（last visited May 11, 2021).

[86] The Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.，https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830762&fileSn=0（last visited May 11, 2021).

[87] 谭必勇、陈艳：《加拿大联邦政府数据治理框架分析及其对我国的启示》，载《电子政务》2019年第1期，第11页。

[88] The Privacy Act，https://www.oaic.gov.au/privacy/the-privacy-act/（last visited May 11, 2021).

[89] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks，https://pd.rkn.gov.ru/authority/p146/p191/（last visited May 11, 2021).

要信息，则禁止其出境。

（四）企业数据出境前的征求个人同意程序

1．征求个人同意程序的内涵及各国实施情况

企业数据出境的征求个人同意程序，是指未经数据主体同意，企业不得向境外传输其相关数据。征求个人同意程序保证数据主体对其个人数据持有一定程度的控制权，赋予个人知情权，是有利于数据保护的企业数据出境限制。目前各国普遍规定了企业数据中“个人数据”的出境需要取得数据主体同意，但征求个人同意的方式、程序要求等有差异。

依据相丽玲的梳理，日本境内的数据持有者向境外传输个人信息等数据时，必须事先获得信息主体的同意，对传输双方名称、传输日期等内容进行具体记录，且必须按照个人信息保护委员会的规定保存一定期限。欧盟规定，信息控制者对个人信息的处理和利用必须以信息主体的“同意”许可为前提。美国禁止所有个人、企业和未经授权的政府部门对通讯内容的窃听，禁止对存储于电脑系统中的通信信息未经授权的访问及对传输中的信息未经授权的拦截。德国要求收集、加工及使用个人数据必须遵守本法及其他法律的规定，或者经数据主体同意。印度明确，除非法规另有规定，个人数据传输始终需要征得个人的同意。韩国规定，数据跨境需要获得数据主体事先、明确、选择加入的同意。澳大利亚规定，受到“国家隐私原则”约束的机构不得将个人信息转移给其他外国人士（机构本身或该人除外），除该人同意这项转移。加拿大要求任何组织在收集个人信息时或在此之前都必须以有效的方式告知信息关系人收集、使用和披露个人信息的目的，并取得信息关系人的同意。此外，当所收集的个人信息用于新的用途时则必须再次取得同意。新加坡规定，数据控制者在收集个人数据之前需经数据主体的同意，但不指定特定的通知形式。在我国，将拨打国际电话、发送国际电子邮件、通过互联网跨境购物以及其他个人主动行为，视为已经个人信息主体同意（相丽玲、张佳彧，2021）。[90]

2．俄罗斯征求个人同意程序的特殊规则

俄罗斯关于企业数据出境前的征求个人同意程序较为特殊。一是，俄罗斯将签署“108 公约”[91]的国家（以欧洲国家为主）视为对数据主体的权利和利益提供“充分保护”（adequate protection）的管辖区，向其跨境转移数据无需取得数据主体额外同意。对于非“108 公约”签署国，Roskomnadzor 依然可以将其列入个人信息跨境流动的“白名单”中，被纳入“白名单”的官方国家名单包括秘鲁、南非等国，

[90] 相丽玲、张佳彧：《中外跨境数据流动的法律监管制度研究》，载《情报理论与实践》2021 年第 4 期，第 76 页。

[91] 《个人数据自动处理保护个人公约》（Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data，即“108 公约”），俄罗斯于 2001 年 11 月 7 日签署该条约，并于 2013 年 9 月 1 日正式生效。参见 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data，https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108（last visited May 11, 2021).

但不包括中国和美国。[92]二是，除了“108 公约”签署国以及 Roskomnadzor 确定的白名单外，其余国家均属于“未对数据提供足够保护”的国家。将个人数据跨境传输到这类无法提供足够保护的国家或地区必须获得数据主体出具的书面同意，或者需满足以下条件之一：（一）根据俄罗斯加入的国际条约，允许跨境数据转移的情形；（二）保护俄罗斯宪法体系、国家国防和国家安全、俄罗斯的运输系统等不受侵犯的情形；（三）为了履行数据主体所参与的合同；（四）保护数据主体的生命、健康或其他重要利益。[93]从以上数据输出规则的相关规定中，可以看出，俄罗斯的通过征求个人同意程序对数据流动的限制，基本是在“108 公约”的框架内进行的，针对欧洲国家的限制较小。但对于其他地区的国家，尤其是中国和美国这两个数字贸易大国，却没有放开这方面的限制。

（五）小结

综上国内外文献梳理，对于企业数据出境限制，各国首先的限制方式是通过设立数据本地化要求，结合数据分类管控，对于重要敏感数据禁止出境，对于非重要数据限制较少。其次，部分国家要求企业数据出境前，进行安全评估，主要是对数据接收国保护立法情况的评估以及数据本身重要性、安全性的分类评估。最后，多数国家目前对于企业数据出境，都要求企业明确告知与数据来源相关的个人，保障个人的知情权。

三、企业数据出境监管协调机制的国内外文献

（一）欧盟企业数据出境的“充分性认定”机制

1．充分性认定机制的内涵界定

欧盟、新加坡等数字经济发展已经较为成熟的国家和地区，希望维持较高的数据自由流动水平，充分利用数据资源。与美国极具侵略性的数据政策不同，欧盟、新加坡采取平衡的监管思路，在所在区域维持高标准隐私保护的前提下促进数据跨境流动，对未达标国家和地区或企业禁止数据自由流动。

欧盟建立以“充分性认定”（Adequacy Decision）为核心的数据跨境流动机制。欧盟《通用数据保护条例》（GDPR）于 2018 年正式生效，规定获得“充分性认定”（Adequacy Decision）的国家和地区可以在不经过数据主体授权的情况下接收欧盟个人数据。即个人数据可以从欧盟（以及挪威、列支敦士登和冰岛）流向第三国，而不需要任何进一步的数据保障措施，向有关国家的传输将同化为欧盟内部的数

[92] Federal Law of 27 July 2006 N 152-FZ on Personal Data，https://pd.rkn.gov.ru/authority/p146/p164/（last visited May 11, 2021).

[93] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks，https://pd.rkn.gov.ru/authority/p146/p191/（last visited May 11, 2021).

据传输。[94]欧盟委员会每四年通过数据保护立法、监管机构运作、国际承诺和公约签订等三个维度对“充分性认定”的国家和地区进行评估，目前仅加拿大、新西兰、瑞士等 11 个国家获得“充分性认定”（Adequacy Decision）。欧盟希望在实现内部的一致标准后，吸引更多发展中国家的接受和加入。[95]欧盟委员会迄今已承认安道尔、阿根廷、加拿大、法罗群岛、格恩西岛、以色列、马纳岛、日本、泽西、新西兰、瑞士和乌拉圭提供充分的数据保护。2021 年 3 月 30 日，欧洲联盟委员会与韩国就“充分性认定”进行了会谈。[96]

2015 年欧盟法院通过 Schrems 案对充分保护（adequate protection）的含义予以界定，即基于第三国国内法和所做的国际承诺，数据保护达到与欧盟“必要相等程度”水平。换言之，充分保护（adequate protection）不是相等程度保护，不要求第三国家个人数据的保护与欧盟一样（identical），允许第三国家采取不同于欧盟的保护方式，但应该证明这些保障措施在实践中能够达到与欧盟必要相等程度（essentially equivalent）的保护水平。首先，保护水平是基于对第三国国内法及所承担的国际义务评估后做出。第二，数据保护水平应从基本权利和自由层面评估。第三，必要相等是第三国保护水平需要基本上满足欧盟基于《欧盟基本权利宪章》和 1995 年指令（第 95/46/EC 指令）所给予的保护力度。[97]

袁慧对欧盟数据跨境转移中的充分性认定机制进行了研究，指出“充分性认定”（Adequacy Decision）机制是欧盟个人数据跨境转移的核心机制，实质是基于欧盟个人数据保护基本权利和次级欧盟数据保护规范，对第三国或者地区法律保护水平的评估，本质上是一种法律范畴的实施机制。欧盟有意将该机制发展成实现欧盟个人数据保护规范全球化的重要路径（袁慧，2020）。[98]孙方江也认为，该立法思路最主要的目的是维护其在数据领域的立法话语权，部分与其贸易或金融依存度较高的国家和地区，会在此影响下修订数据保护法律，达到同等的数据保护标准来获得信任（孙方江，2021）。[99]

2．充分性认定机制的国家/地区白名单规则

欧盟落实“充分性认定”（Adequacy Decision）机制，确定非欧盟国家是否拥有足够的数据保护水平，主要是通过设立“国家/地区白名单”来实现。“白名单”

---

[94] Adequacy Decisions：How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection，https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en（last visited May 11, 2021).

[95] EU Data Protection Reform: Ensuring Its Enforcement，https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-role-edpb_en.pdf（last visited May 11, 2021).

[96] Adequacy Decisions：How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection，https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en（last visited May 11, 2021).

[97] Maximillian Schrems v. Data Protection Commissioner, Case C-362/14, the Court of Justice of European Union, 6 October 2015.

[98] 袁慧：《欧盟数据跨境转移中的充分决定机制研究》，载《电子知识产权》2020 年第 11 期，第 57 页。

[99] 孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 6 页。

规则建立根据数据保护状况及对等措施，将部分地区纳入可自由流动的国家与地区范围。

依据欧盟规定，欧洲联盟委员会有权根据 GDPR 第 45 条，确定欧盟以外的国家是否提供足够水平的数据保护。[100]例如要获得欧盟委员会批准的“充分性认定”（Adequacy Decision）资格，一国数据保护立法、执法环境、是否存在有效的损害救济机制等是首要考量因素（贾开，2017）。[101]美国有类似规定，如美国 CLOUD 法案则规定，能与其进行境外数据执法合作的“适格外国政府”必须符合法治、人权、有充分的数据保护实体和程序立法等核心标准（魏书音，2018）。[102]

在斯诺登事件发生后，欧盟委员会在对《安全港协议》（US-EU Safe Harbor Framework）运行情况评估中指出，该框架缺乏有效限制美国执法机构的措施。[103]欧盟法院随后通过 Schrems 案件裁定《安全港协议》无效，理由是：欧盟委员会认可美国允许以国家安全、公共关利益、执法为由规避《安全港协议》的原则，但是却并未对这种规避行为进行严格限定，美国也未给个人提供法律上的救济途径，不符合基本权利保护的比例性原则，会严重危害《欧盟基本权利宪章》第 7 条、第 8 条个人数据保护权和隐私权的权利核心内容。[104]

欧盟数据保护委员（European Data Protection Board，EDPB）会依据 Schrems 裁判，提出四项欧洲核心保障措施（European Essential Guarantees），作为评估政府监控活动对个人数据保护和隐私侵扰的正当性的依据。[105]随后这四项核心保障措施被纳入新的“充分性认定”（Adequacy Decision）框架，对第三国家以执法和国家安全为由访问和使用数据的相关规范进行评估。核心保障措施是基本权利保护中的比例原则在个人数据保护领域的适用，包含四部分的内容：一是，政府处理数据应该具备法律基础，公权力机构对数据的处理应该依据清楚、明确、易懂的规则；二是，必要性和比例原则，处理行为应该与合法目的之间应存在必要性且不超过限度；三是，数据处理应该受到独立机构的监督；四是应为个人提供有效的救济途径。

随着信息时代的发展，欧盟对“充分性认定”（Adequacy Decision）赋予更多政治和经济方面的考量。欧盟委员会认为在“充分性认定”评估过程中，除了考虑数据保护规则相关监管和救济机制外，还应该考虑第三国家的其他情况：一是经济，

---

[100] General Data Protection Regulation(GDPR)，Article 45.

[101] 贾开：《跨境数据流动的全球治理：权力冲突与政策合作——以欧美数据跨境流动监管制度的演进为例》，载《汕头大学学报（人文社会科学版）》2017 年第 5 期，第 59 页。

[102] 魏书音：《CLOUD 法案隐含美国数据霸权图谋》，载《中国信息安全》2018 年第 4 期，第 44 页。

[103] Facebook Ireland v. Schrems (Schrems II)（the European Union Court of Justice）.

[104] Maximillian Schrems v Data Protection Commissioner, Case C-362/14, the Court of Justice of European Union, 6 October 2015.

[105] Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection through Surveillance Measures when Transferring Personal Data (European Essential Guarantees)-wp237, https://ec.europa.eu/newsroom/article29/items/640363（last visited May 11, 2021).

第三国家与欧盟目前和未来的商贸关系；二是欧盟与第三国数据流动的频率和程度，例如地理或者文化上与欧盟的联系；三是法律体系影响力，侧重考察第三国家数据保护体系在区域法律协调中的影响力；四是与第三国家之间的政治关系，特别是双方在国际层面是否有共同价值和目标。[106]欧盟委员会积极寻求与贸易合作伙伴之间的充分性互认，促进外交关系向好发展。“充分性认定”（Adequacy Decision）已经不仅仅是对法律保护水平的评估，已逐渐成为欧盟发展对外关系、重塑国际地位的重要抓手（袁慧，2020）。[107]

3．欧盟充分性认定机制与新加坡相似保护信任机制的异同

新加坡建立以“相似保护”为基础的信任机制。新加坡的主张是建设成为亚太地区数据中心。2012 年出台的《个人数据保护法案》（Personal Data Protection Act）规定，新加坡企业传输个人数据至第三国时，应满足以下条件：境外接收者受法律义务约束，法律义务应为所传输的个人数据提供与《个人数据保护法案》相称的保护标准，法律义务可以通过签订合同、制定公司规程、接收国数据保护立法等途径实现（孙方江，2021）。[108]

新加坡的“相似保护”信任机制与欧盟的“充分性认定”（Adequacy Decision）机制相比，既有相似之处，也有细微差异。相似之处在于，都是通过国家/地区颁布示范法，作为地区/国内企业向境外传输数据的标准，吸引其他国家遵从自己的标准，从而实现企业数据跨境合法传输。不同之处在于，在企业数据跨境流动中，欧盟将评价数据接收国是否有达到数据保护水平，认定数据接收国是否可以合法接收本区域数据的权利，留给了欧盟监管机构，强调对出境数据的主动监管。正如学者 Lee-Makiyama 认为，没有任何先例可以预兆欧盟是否会与一国在电子商务议题上达成一致，无论欧盟是否认为其有（个人数据）充分保护的规定（Lee-Makiyama，2018）。[109]与欧盟的政策相比，新加坡则是通过公布示范法，只要数据接收国立法能与《个人数据保护法案》相称，企业数据即可以向其传输，相对来说监管强制力较弱。

4．充分性认定机制的借鉴启示

从本质上来讲，“充分性认定”（Adequacy Decision）机制及“白名单”机制是一国认为他国的数据保护水平达到本国的最低要求，进而认为本国数据流入他国会得到充分的保护（adequate protection），而不至于损害数据主体合法权益。但

---

[106] Exchanging and Protecting Personal Data in A Globalised World，https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN（last visited May 11, 2021).

[107] 袁慧：《欧盟数据跨境转移中的充分决定机制研究》，载《电子知识产权》2020 年第 11 期，第 58 页。

[108] 孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 3-13 页。

[109] Hosuk Lee-Makiyama, *E-Commerce and Digital Trade*, in Jane Drake-Brockman & Patrick Messerlin, POTENTIAL BENEFITS OF AN AUSTRALIA-EU FREE TRADE AGREEMENT: KEY ISSUES AND OPTIONS，UNIVERSITY OF ADELAIDE PRESS(2018).

需要注意的是，白名单本身应当是可以灵活调整的，应当建立起定期评估与临时评估等制度，以保证数据流入国始终保持较高的数据保护标准。

通过建立白名单机制，可以减轻企业合规负担，畅通数据跨境流动的渠道（马其家、李晓楠，2021）。[110]此外，在白名单之外还应配套相应的域外执法管辖和责任追究机制，白名单中的组织、个人开展数据活动，损害我国国家安全、公共利益或者公民、组织合法权益的，可以依法追究其法律责任。

（二）欧盟企业数据出境的“充分保护措施”机制

1．充分保护措施机制对充分性认定机制的补充作用

“充分保护措施”可以说是对“充分性认定”（Adequacy Decision）机制的补充，使欧盟向未获得“充分性认定”机制认证的白名单以外国家合法传输数据。若向白名单以外国家传输数据，只要数据控制者、数据处理者承诺提供充分的数据保护（Adequate protection）措施，数据就可以跨境流动。从实践看，“充分保护措施”主要包括标准合同条款（Standard Contractual Clauses，SCC）、具有约束力的集团企业规则（Binding Corporate Rules，BCR）、经批准的认证机制等。[111]

2．充分保护措施之签订标准合同条款合同

标准合同条款（Standard Contractual Clauses，SCC）由政府依据数据保护原则主导制定，通过合同来管控数据出境风险。在合同的具体内容上包含当事人双方应当遵守的数据保护规定，明确不得跨境的数据类型；要求境内企业对其数据进行分类管理，境外企业不得通过芯片后门等方式获得禁止跨境的数据；合作双方均应遵守数据出境国相关数据保护法律规定，合同适用该国法律，并由该国法院管辖等。如果数据控制者、数据处理者等主体间采用了标准合同条款，则合同仅需在主管部门备案而无需主管部门批准即可进行数据跨境流动。

欧盟制定了与未获得“充分性认定”（Adequacy Decision）机制认证的非欧盟国家之间数据传输的标准合同条款。欧盟委员会认为，通过签订标准合同条款，可以为数据跨境提供足够的保护，使数据能够在国际上传输。迄今为止，欧盟已发布了两套标准合同条款，规定从欧盟的数据控制区域向在欧盟或欧洲经济区（european economic area, EEA）以外进行数据传输，根据主体类型不同，数据出境企业可以选择不同的合同范本。[112]

除欧盟以外，一些国家对于企业数据出境也规定了类似的条款，但并未达到欧盟当前的标准化水平。如印度规定，传输是按照标准合同条款或者集团内计划进行

---

[110] 马其家、李晓楠：《论我国数据跨境流动监管规则的构建》，载《法治研究》2021 年第 1 期，第 91-101 页。

[111] 参见中国信息通信研究院安全所等：《欧盟 GDPR 合规指引》，https://www.cebnet.com.cn/upload/resources/file/2019/05/29/39038.pdf，2021 年 5 月 11 日访问。

[112] Standard Contractual Clauses (SCC)：Standard Contractual Clauses for Data Transfers between EU and Non-EU Countries，https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en（last visited May 11, 2021).

的，且上述合同和计划已获得数据保护局的批准。[113]加拿大要求，加拿大公司如果将其所持有的个人数据转移至第三方，必须在合同中明确数据保护条款，以确保第三方机构能够提供同等水平的保护。[114]巴西也明确了允许数据跨境传输的合同条款标准，要求数据控制者能向监管机构证明其符合国内的数据出境规定、数据主体权利和数据保护制度。[115]

3．充分保护措施之建立有约束力的集团企业规则

具有约束力的集团企业规则（Binding Corporate Rules，BCR）主要适用于跨国集团企业内部进行数据流动，是欧盟为在企业集团或企业内传输欧盟以外的个人数据而制定的数据保护政策。欧盟的 BCR 规则认为如果跨国集团遵循一套完整的，经个人数据监管机构认可的数据处理机制，则该集团内部整体成为一个“安全港”，个人数据可以从集团内的一个成员合法传输给另一个成员，而无需经主管部门批准。

关于跨国公司内部数据传输的公司规则，欧盟规定，这些集团内数据传输规则必须包括所有一般数据保护原则和可强制执行的权利，以确保为数据传输提供适当的保障。它们必须具有法律约束力，并由该团体的每个有关成员执行。具有约束力的公司规则批准方面，公司必须向欧盟数据保护机构提交具有约束力的公司规则以供其批准，监管部门会根据 GDPR 第六十三条所订的一致性机制，批准 BCR。同时，监管主管部门将集团公司的决定草案通知欧盟数据保护委员（European Data Protection Board，EDPB）会，该委员会将就具有约束力的公司规则发表意见。当 BCR 根据 EDPB 意见最终确定时，主管部门将批准 BCR。[116]

在 GDPR 之前，已有部分欧盟成员国的监管机构接受“有约束力的公司规则”，包括埃森哲、宝马汽车、惠普、摩托罗拉等 72 家跨国公司获得了“有约束力的公司规则”的认可。[117]

4．充分保护措施之设定经批准的认证机制

经批准的认证机制上，亚太经合组织（APEC）的《跨境隐私保护规则》（Cross Border Privacy Rules, CBPR）提供了极好的范例。CBPR 规则下，获得政府认可的评估机构对商业机构保护个人隐私与信息的水平进行认证，获得认证的企业之间

---

[113] Draft Personal Data Protection Bill, 2018，https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018（last visited May 11, 2021).

[114] 谭必勇、陈艳：《加拿大联邦政府数据治理框架分析及其对我国的启示》，载《电子政务》2019 年第 1 期，第 12 页。

[115] Lei Geral de Proteção de Dados Pessoais（LGPD），https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd（last visited May 11, 2021).

[116] Binding Corporate Rules (BCR)：Corporate Rules for Data Transfers within Multinational Companies，https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#bindingcorporaterules（last visited May 11, 2021).

[117] 王中美：《欧盟数据战略的目标冲突与中间道路》，载《国际关系研究》2020 年第 6 期，第 43 页。

可以进行数据的自由交换，当然也包括数据跨境流动（王中美，2020）。[118]

（三）美国企业数据出境的多边合作“数据流动圈”机制

1．多边合作数据流动圈的内涵及实践

与欧盟进行“充分性认定”（Adequacy Decision）结合“充分保护措施”构建企业数据出境规定的方式不同，美国对于企业数据出境监管协调机制的构建，则是以多边合作建设“数据流动圈”的形式展开，对于“数据流动圈”内的企业，企业数据可以自由流动。美国构建“数据流动圈”的国际行动包括：

一是，美国2000年与欧盟签订《安全港协议》（US-EU Safe Harbor Framework），包括 Googele、Facebook、Microsoft 等 5000 多家美国公司在欧洲运营受到该协议的保护，将欧洲用户数据传输至美国储存及处理。[119]《安全港协议》在 2015 年被判无效。

二是，2005 年美国促成亚太经合组织（APEC）通过《亚洲太平洋经济合作组织隐私框架》（APEC Privacy Framework），获得认证的企业可以自由进行跨境数据流动，但这一框架实施效果较差，仅 20 多家美国和日本企业获得认证。[120]

三是，2012 年签订《美韩自由贸易协定》（US-South Korea Free Trade Agreement）第一次将数据跨境流动引入自由贸易协定（FTA）。其中规定，成员国应“努力避免对跨境电子信息流动施加或保持不必要阻碍”。[121]

四是，2013 年 APEC 通过了《跨境隐私保护规则》（Cross Border Privacy Rules, CBPR），目前已有美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、我国台湾地区加入。CBPR 提出，若各成员国公司承诺遵守《亚洲太平洋经济合作组织隐私框架》（APEC Privacy Framework）九大原则，那么个人数据在这些公司之间流动应不受阻碍，进而成员国不得再以保护个人信息为由限制数据跨境流动。[122]

五是，2015 年由美国主导，日本、澳大利亚等 12 个国家达成《跨太平洋战略经济伙伴协定》（Trans-Pacific Partnership Agreement， TPP），在 14 章 11 条“以电子方式跨境传输信息”中约定，成员国应当允许个人信息自由跨境流动，除非出于正当公共政策目标。成员国可以采取以下方式履行协定，例如统一制定个人数据保护法、行业部门法或行业自律规则。[123]这样一来，不同数据保护水平、方式的成

---

[118] What is the Cross-Border Privacy Rules System?，https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system（last visited May 11, 2021).

[119] US-EU Safe Harbor Framework，https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework（last visited May 11, 2021).

[120] APEC Privacy Framework，https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx（last visited May 11, 2021).

[121] U. S.-South Korea Free Trade Agreement，https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta（last visited May 11, 2021).

[122] What is the Cross-Border Privacy Rules System?，https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system（last visited May 11, 2021).

[123] Summary of the Trans-Pacific Partnership Agreement，https://ustr.gov/about-us/policy-offices/press-office/press-

员国只要满足一定的最低线，就可以声称达到协定要求。

六是，2018 年 10 月美国、墨西哥、加拿大签署《美墨加协议》（U.S.-Mexico-Canada Agreement），规定“任何缔约方不得将金融机构或跨境金融服务提供者所采集的金融数据本地化储存，作为在境内开展业务的前提条件”，其 19 条约定遵守 APEC 跨境传输规则，并约定任何缔约国不得禁止或限制数据跨境传输。[124]

通过区域或双边协定的形式，美国倡议与其他国家共同建设无障碍数据流动圈，由于相对于其他国家，美国在数据技术上有领先优势，因此这种“数据流动圈”形式的企业数据出境监管协调机制，实际上成为了美国利用强权为其获取境外数据的通道。[125]

2．《安全港协议》、《隐私盾协议》及美国规则与欧盟规则的冲突

2000 年 11 月 1 日，《安全港协议》（US-EU Safe Harbor Framework）由美国商务部与欧盟委员会签署，规定只要美国遵守协议的七项原则，即：向外移转原则、安全原则、选择原则、获取原则、通知原则、资料完整原则和执行原则，[126]即被认为达到欧盟指令标准。《安全港协议》暂时缓解了美欧跨境数据流动受限的问题，但由于利益的根本冲突，加上棱镜门事件作为导火索，2015 年 10 月 6 日，欧盟法院宣布因无法达到保护标准，《安全港协议》失效。[127]然而时隔仅仅一年，2016 年 7 月 12 日，利益又将美欧重新拉回谈判桌，签订了数据流动新方案欧美《隐私盾协议》（EU-US Privacy Shield Framework），双方均做出妥协，仍保留《安全港协议》七项原则，并丰富了内涵：美国企业承担了更多数据保护义务；赋予欧盟公民多样化的救济途径；限制美国政府进行监控，获取个人信息；建立年度审查机制等。[128]2020 年 7 月 16 日，欧盟法院做出判决，认为由于美国《外国情报监控法案》（Foreign Intelligence Surveillance Act）的存在，使之可能超过必要限度访问所传输的数据，且无法给欧盟居民提供必要救济，因此宣告美欧《隐私盾协议》无效。[129]

对此，东方认为，欧盟、美国主导形成了国际上较为完善的跨境数据流动法律规制体系，两者的差异主要表现在规制模式、立法基础、价值取向三方面（东方，2019）。[130]范思博则提出，从根本上讲，美欧在个人数据保护的传统、立法、隐私意识上的巨大差异一直存在，基于商业利益的妥协仍存在很大的不稳定性（范思博，

releases/2015/october/summary-trans-pacific-partnership（last visited May 11, 2021).

[124] United States-Mexico-Canada Agreement，https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement（last visited May 11, 2021).

[125] 孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 4 页。

[126] US-EU Safe Harbor Framework, http://2016.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf（last visited May 11, 2021).

[127] Maximillian Schrems v Data Protection Commissioner（the European Union Court of Justice）.

[128] EU-US Privacy Shield Framework, https://www.privacyshield.gov/eu-us-framework（last visited May 11, 2021).

[129] Facebook Ireland v. Schrems (Schrems II)（the European Union Court of Justice）.

[130] 东方：《欧盟、美国跨境数据流动法律规制比较分析及应对挑战的“中国智慧”》，载《图书馆杂志》2019 年第 12 期，第 92 页。

2020）。[131]在存在差异的基础上，孔庆江等指出，包括欧盟在内的各国数据治理晚近以来呈现共同立法规则域外适用扩张趋势（孔庆江、于华溢，2020）。[132]这些因素共同作用下，欧美与美国跨境传输规则间产生冲突在所难免。

（四）日本企业数据出境的“基于信任的自由数据流通”机制

1．基于信任的自由数据流通机制的产生背景及内涵界定

日本希望构建“基于信任的自由数据流通”机制。日本于 2003 年通过《个人信息保护法》（Personal Information Pro‑tection Act，PIPA），并于 2015 年特别针对欧盟《通用数据保护条例》（GDPR）与亚太经合组织《跨境隐私保护规则》（Cross-border Privacy Rules，CBPR）对法案进行修改，即通过提升本国的数据保护水平与其他国家接轨，以此获取自由接收数据的权利。2019 年达沃斯会议，日本政府提出“基于信任的自由数据流通”（Data Free Flow With Trust，DFFT）机制，希望主导新的国际规则，在不牺牲个人隐私安全的基础上，允许医疗、工业、交通和其他非个人数据的自由流动。[133]2019 年 9 月，日本与美国签署《美日数字贸易协定》（Agreement between United States and Japan Concerning Digital Trade），确立了各领域数据无障碍跨境传输的总体思路，并要求禁止对金融业机构提出数据本地化要求，希望继续保持两国在数字领域国际规则制定的引领地位。[134]

2．基于信任的自由数据流通机制的妥协性及监管风险

可以看出，日本“基于信任的自由数据流通”（DFFT）机制对于本国企业数据出境的限制极少，几乎所有数据以任何形式出境，都是合法的。日本施行“基于信任的自由数据流通”机制，本质上是以牺牲本国数据安全为基础，对本国数据出境不设限制，以换取与美国、欧盟等国家/地区数据传输资格。这种主动放弃国家数据主权，忽视数据安全的企业数据出境监管协调机制，是日本对当前国际上已形成的以欧盟、美国跨境数据流动规则的妥协。当然，这种妥协下产生的“基于信任的自由数据流通”机制，也必然导致本国数据安全处于极大的风险之中，对本国企业数据出境的有效监管也基本无从谈起。

（五）小结

综上国内外文献的梳理，对于企业数据出境监管协调机制，当前国际上主要形成了欧盟、美国、日本为代表的企业数据出境监管协调机制。其中，欧盟以“充分性认定”（Adequacy Decision）、“充分保护措施”等方式维护数据立法话语权，构建企业数据出境监管协调机制。美国以促进跨境数据自由流动为原则建设“数据流

---

[131] 范思博：《数据跨境流动中的个人数据保护》，载《电子知识产权》2020 年第 6 期，第 86 页。
[132] 孔庆江、于华溢：《数据立法域外适用现象及中国因应策略》，载《法学杂志》2020 年第 8 期，第 79 页。
[133] Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows，https://www.weforum.org/white papers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows（last visited May 11, 2021).
[134] Agreement between United States and Japan Concerning Digital Trade, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf（last visited May 11, 2021).

动圈”，通过区域、双边合作来构建企业数据出境监管协调机制。而日本则基本放弃“数据主权”，建立“基于信任的自由数据流通”（Data Free Flow With Trust，DFFT）机制，以牺牲本国数据安全为代价，换取融入欧美等自由流动圈资格。总体来说，欧盟、美国的企业数据出境监管协调机制，对于我国企业数据出境监管立法有比较重要的参考意义。

四、数据出境企业主体责任及追责的国内外文献

（一）数据出境的企业主体责任

企业数据出境，是一个包含数据境内收集、存储、处理、出境审批、传输出境等多环节的过程。这些环节中，既涉及企业内部对数据的管理，也有对数据安全风险的关注和管控，还涉及企业数据出境前对监管部门要求的配合。对于这些方面，企业都应有相应的企业主体责任。

1．数据出境企业主体的内部管理责任

数据控制主体需要在企业内部层面建立起完善的数据保护体系，明确数据各生命周期环节的具体操作规范，加强内部监控，避免不当操作。凡出境业务，需经过合规部门预研、审核，确保涉及数据收集、传输、处理等操作的每一步都符合出境的监管要求（马其家、李晓楠，2021）。[135]

一是，内部管理人员设置方面。从国际经验看，澳大利亚采取了“数据创始人”（Originato，生成数据的人）的制度，利用数据保护性标识督促数据控制主体履行数据保护义务。当数据生成时，创始人需要评估未经许可访问或不当使用数据所带来的损害及后续影响，如果数据的跨境流动可能会损害国家和他人利益，则该数据应被施加保护标识，在披露或向机构外传输前，应采取适当保护措施。通过数据创始人（Originator）制度对数据跨境的要求进行处理，只有获得 Originator 授权并移除标记，相关数据才可跨境。[136]

另外，欧洲议会和欧盟理事会于 2000 年 12 月提出了“数据保护官”（Data Protection Officer，DPO）制度，并规定了其任命、任务、通知和登记。[137]GDPR 强化了必须设立 DPO 的法定情形，包括：公权力机构进行处理活动的；需要对数据主体定期进行大规模系统化监控的；处理大规模特殊类型的数据或与刑事犯罪相

[135] 马其家、李晓楠：《国际数字贸易背景下数据跨境流动监管规则研究》，载《国际贸易》2021 年第 3 期，第 80 页。

[136] The Privacy Act，https://www.oaic.gov.au/privacy/the-privacy-act/（last visited May 11, 2021).

[137] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data，https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045（last visited May 11, 2021).

关的。[138]GDPR 还规定了 DPO 的权利、地位和任务。[139]2019 年 12 月，美国白宫行政管理和预算办公室发布《联邦数据战略与 2020 年行动计划》，也确立了包括设立 GDPR 要求的首席数据官等 20 项行动计划。

二是，数据内部处理要求方面。《2019 美国国家安全与个人数据保护法案》（National Security and Personal Data Protection Act of 2019）第三节针对特别关注科技公司的数据安全要求，规定了“数据最小收集原则”，即收集的用户数据不得超过运营所需，以及“禁止二次使用原则”，即不得用于与运营无关的任何目的，包括提供定向广告、与第三方共享或者提供不必要的人脸识别技术。[140]另一方面，欧盟早在 1995 年通过的第 95/46/EC 号指令规定，个人信息不得被以与之最初被收集时特定的、明确的和合法的目的不一致的方式被进一步处理和收集。[141]这也基本上堵住了个人信息再利用的可能途径。

2．数据出境企业主体的自查上报与泄露制止责任

涉及数据出境业务的企业，在日常运营中，也需要定期自查，对公司运营中的数据保护措施是否落实，以及是否出现数据泄露的情形进行核查。对于发现企业存在数据泄露情形的，需要落实制止义务。

一方面，数据企业的应当负有对其数据保护措施运行实际情况定期自查的义务。《2019 美国国家安全与个人数据保护法案》（National Security and Personal Data Protection Act of 2019）规定，公司首席执行官或同级别高管人员应每年至少一次向联邦贸易委员会（Federal Trade Commission，FTC）、联邦和各州检察长提交报告。[142]该法案明确了数据企业的定期自查责任以及自查报告上报义务。

另一方面，对于自查中发现的数据泄露问题，数据企业应当负有阻止数据继续泄露和采取弥补措施的责任。俄罗斯 2006 年出台的《信息、信息技术和信息保护法》（Federal Law No. 149-FZ）规定了信息持有者或信息系统运营者需要承担信息保护义务，明确了相关义务方需要确保信息不向无权限方泄露，并能够在发现信息泄漏后及时采取弥补措施，例如尽快恢复被破坏的信息。[143]同年出台的《俄罗斯联邦个人数据法》（Federal Law of 27 July 2006 N 152-FZ on Personal Data）专门针对个人数据实施跨境保护措施，旨在保护俄罗斯公民的信息自由及权利。除了需要满足前述同等要求外，相关责任方还需要确认个人数据传输的目标国家是否能够确

---

[138] General Data Protection Regulation(GDPR)，Article 37.

[139] General Data Protection Regulation(GDPR)，Article 38-39.

[140] National Security and Personal Data Protection Act of 2019，https://www.govinfo.gov/app/details/BILLS-116s2889is（last visited May 11, 2021).

[141] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data，https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML（last visited May 11, 2021).

[142] National Security and Personal Data Protection Act of 2019, Sec. 3. (a).

[143] Federal Law No. 149-FZ of July 27, 2006 on Information, Informational Technologies and the Protection of Information，https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_369.pdf（last visited May 11, 2021).

保个人数据的安全，如果安全性无法得到保证，那么需要取消或中止数据传输。[144]GDPR 中也明确规定，组织必须在发现数据泄露后 72 小时内报告。[145]

3．数据出境企业主体的配合审查责任

绝大多数国家的企业数据出境规则虽然有差异，但在企业数据出境前基本都有相应的数据出境审查制度，如结合数据本地化要求的数据安全性评估、征求个人同意程序等要求。企业作为出境数据的控制者，应当负有配合国内监管部门对出境数据的审查。

征求个人同意程序，在许多国家法律框架下是数据合法跨境数据传输的前提，也是企业数据出境前必须的审核事项。一些国家对跨境数据流动的允许基于征求个人同意程序，要求数据跨境流动必须事先征得数据主体的同意。[146]如，欧盟规定，信息控制者对个人信息的处理和利用必须以信息主体的“同意”许可为前提。印度明确，除非法规另有规定，个人数据传输始终需要征得个人的同意。[147]韩国也规定，数据跨境需要获得数据主体事先、明确、选择加入的同意。[148]

是否符合本地化要求，往往也是企业数据出境前必须被审查的内容。2014 年 7 月 21 日普京签署了《关于“进一步明确互联网个人数据处理规范”之俄罗斯联邦系列法律修正案》（Federal Law No. 242-FZ），在《信息、信息技术和信息保护法》（Federal Law No. 149-FZ）第 16 条第 4 款中增加了以下内容：规定信息拥有者、信息系统运营方有义务将对俄罗斯联邦公民个人信息进行收集、记录、整理、保存、核对（更新、变动）、提取而形成的数据库存放在俄罗斯境内。[149]

总之，不管是基于风险控制还是利益补偿等角度考量，数据控制主体履行相应数据出境自查或者保护义务，符合责任分配的一般法理。具体来讲，每个数据控制主体需要根据不同业务要求和操作环境，确定其风险承受水平，人员、数据以及资产的具体风险，并采取相应的保护措施以减轻风险，包括采取风险识别、风险评估、制定风险排除方案等。

---

[144] Federal Law of 27 July 2006 N 152-FZ on Personal Data，https://pd.rkn.gov.ru/authority/p146/p164/（last visited May 11, 2021).

[145] What is the LGPD? Brazil’s Version of the GDPR，https://gdpr.eu/gdpr-vs-lgpd/（last visited May 11, 2021).

[146] 戴艺晗：《贸易数字化与监管碎片化：国际贸易制度框架下跨境数据流动治理的挑战与应对》，载《国际经济法学刊》2021 年第 1 期，第 7 页。

[147] Draft Personal Data Protection Bill, 2018，https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018（last visited May 11, 2021).

[148] The Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.，https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830762&fileSn=0（last visited May 11, 2021).

[149] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks，https://pd.rkn.gov.ru/authority/p146/p191/（last visited May 11, 2021).

（二）对数据出境企业的追责形式

1．行政机构对数据出境企业的处罚权和裁量权

数据企业的行政监管机构要定期审查企业行为、对数据泄露事件进行调查和对违法行为做出裁决并处罚，其对数据企业的行政监管权可归结为处罚权和裁量权。纵观各国立法，基本上各国行政机构对企业数据出境的监管机构设置和监管权利各异。

美国的联邦贸易委员会（Federal Trade Commission，FTC）拥有行政处罚权，曾开出对 Facebook 公司的 50 亿美元的罚单；加拿大专门设置隐私专员办公室（Office of the Privacy Commissioner of Canada），并且每年提供数据出境相关的年度报告；日本通过个人信息保护委员会（Personal Information Profection Commission，PPC），对其他司法管辖区法律中的保护标准进行评估；德国设置了联邦数据保护专员（Data Protection Officer），其处罚权限最高为数据企业全球营业额 4%；俄罗斯联邦通信、信息技术和大众媒体监督局（The Federal Service for Supervision of Communications, Information Technology and Mass Media，Roskomnadzor）统一负责对数据企业的行政监管，处罚权限最高罚款金额为 7 万 5000 卢布；韩国通过韩国通信委员会和韩国互联网与安全局行使行政监管权，最高可进行 2000 万韩元的行政罚款；新加坡设置独立的个人数据保护委员会（Personal Data Protection Commission，PDPC），拥有最高不超过 100 万美元的罚款权利；澳大利亚由信息专员办公室履行对数据企业的监管，审查政府信息公开法决定是否在企业中落实；印度由印度数据保护局对数据企业进行监管，行政处罚最高可达 5 亿卢比；中国则通过国家互联网信息办公室行使行政监管权，拥有警告、责令改正或通报批评或 50 万元以下的行政处罚权利。[150]

综上对各国企业数据出境监管机构行政权利的梳理，监管机构依据有无惩罚权和裁量权可分成三类。第一类，无处罚权、无裁量权，监管机构对跨境数据传输的监管主要依据法律法规执行，其主要职责为提供咨询服务、制定年度报告、审查备案企业。如加拿大、日本和澳大利亚。第二类，有处罚权、无裁量权，监管机构对违反个人数据保护法的行为进行行政处罚，处罚最高可达企业全球营业额 4%，如德国、俄罗斯等。第三类，有处罚权、有裁量权，监管机构除了依法惩处企业之外，还可自行裁定具体事件的模糊之处，如新加坡、中国和和印度。此外，欧盟作为国际组织，虽没有处罚权力，却要推动成员国的实施相应的法律和处罚。

另一方面，企业数据出境的行政监管往往涉及多个部门，如何协调各部门间对数据出境企业进行监管，是落实行政机构监管权利的重要问题。国际经验来看，新加坡提供了很好的示范。新加坡于 2013 年设立个人数据保护委员会（Personal Data

[150] 相丽玲、张佳彧：《中外跨境数据流动的法律监管制度研究》，载《情报理论与实践》2021 年第 4 期，第 76-77 页。

Protection Commission，PDPC）成为个人数据保护事务方面的主要权威机构，并代表新加坡政府处理与数据保护相关的国际事务。通过设立机构或由专门机构统筹协调不同行业主管部门的审核职能，可以阻塞监管漏洞，保证政策的完整性和连续性。这对我国企业数据出境监管立法中的机构设置有一定借鉴意义。

2．司法机关对数据出境企业的司法权

在数据出境前，司法机关对数据企业的司法权利依照国内法相关规定履行，如数据企业间的纠纷、数据企业与政府的行政诉讼等，司法机关均有管辖权。在数据出境后产生的数据争议，国内司法机关是否有司法管辖权，取决于各国采取的不同管辖权原则。冉从敬、陈贵容等对美国跨境数据流动监管规则进行了研究，在调研了美国跨境数据流动管辖的发展过程以及政策体系和管辖模式后，他们认为，美国的跨境数据流动管辖模式采取的是属人原则为主，属地原则为辅（冉从敬、陈贵容、王欢，2020）。[151]洪延青则从执法跨境调取数据的视角对进行了研究，他认为，作为数字经济中主要板块的美国、欧盟，对执法跨境调取数据中的“取”和“防”分别从各自的现实需求、产业发展情况、法律传统和总体战略等因素出发，采取了不同的模式（洪延青，2021）。[152]

美国对于本国数据企业在境外发生纠纷的司法管辖权，延续了其一贯的“长臂管辖”原则。美国在 2015 年颁布的《网络安全信息共享法案》中明确了美国对“国际网络罪犯”的管辖；[153]2018 年 3 月美国总统特朗普正式签署的《澄清域外合法使用数据法案》（Clarifying Lawful Overseas Use of Data Act， CLOUD 法案），既为执法机构的执法行为提供了合法性依据，也为网络服务提供商明确了不予执行的抗辩事由。[154]英国也通过上议院 2018 年 7 月二读审议的《犯罪（境外提交令）法案 2018》，明确了境外数据纠纷的司法管辖权，授予了英国执法机构依据英国法庭命令，在与英国签订相关国际协议的国家或地区直接获取境外数据的权力。拥有域外司法管辖权，意味着国家可以不受他国干涉独立处理对外事务，这些都是国家之间跨境数据获取和网络话语权争夺的体现，是对网络主权的承认和推广（韩冰，2018）。[155]对此，丁玮认为，数据时代的数据帝国主义/殖民主义和数据保护主义问题催生了各国跨境数据政策立法。数据关系形成了一种新的数据权力形式，美国跨境数据政策发展和变化是这一过程的反映（丁玮，2021）。[156]

---

[151] 冉从敬、陈贵容、王欢：《美国跨境数据流动的管辖模式研究及对中国的启示》，载《图书情报知识》2020 年第 6 期，第 136 页。

[152] 洪延青：《“法律战”旋涡中的执法跨境调取数据：以美国、欧盟和中国为例》，载《环球法律评论》2021 年第 1 期，第 39 页。

[153] S.754 - To Improve Cybersecurity in the United States through Enhanced Sharing of Information about Cybersecurity Threats, and for Other Purposes, https://www.congress.gov/bill/114th-congress/senate-bill/754（last visited May 11, 2021).

[154] H.R.4943 - CLOUD Act，https://www.congress.gov/bill/115th-congress/house-bill/4943（last visited May 11, 2021).

[155] 韩冰：《法制保障机制是落实网络主权的重要举措》，载《中国信息安全》2018 年第 11 期，第 76 页。

[156] 丁玮：《数据主义视角下美国跨境数据政策演进及我国的应对》，载《杭州师范大学学报(社会科学版)》2

另一方面，近年来由于互联网企业数据存储地与服务提供地的分离，主权国家出现相关司法管辖等问题。2013 年，美国政府因一起刑事案件向 Microsoft 公司调取相关电子邮件，Microsoft 公司表示该数据存储在爱尔兰的服务器，美国政府没有获取的法律依据。2016 年美国联邦第二巡回法院认为根据 1986 年的《储存通讯法案》（Stored Communications Act, SCA），搜查令不适用于美国服务商存储在境外的数据，做出了有利于 Microsoft 公司的二审判决。[157]显然，根据 SCA，美国无权管辖那些美国公司所拥有的，却存储在境外的数据。在这样的背景下，2018 年 3 月 23 日，特朗普正式签署《澄清域外合法使用数据法案》（CLOUD 法案），明确规定了美国政府有权在涉嫌危害国家安全、严重刑事犯罪等情形下调取美国互联网企业数据，无论数据存放在境内还是境外。CLOUD 法案通过“控制者原则”的“长臂法案”，扩大了美国执法机关调取境外数据的权力，而他国调取存储在美国的数据须通过“适格外国政府”审查，并满足美国设定的认定条件。

夏燕、沈天月通过对美国 CLOUD 法案进行了研究，认为 CLOUD 法案确立了“数据控制者”法律管辖原则，排除了美国获取跨境电子数据的障碍，也为其他国家快速便捷获得美国控制的电子数据提供了可能的法律途径。但囿于 CLOUD 法案的理论局限以及其产生“长臂管辖”的威慑力，CLOUD 法案实际上极大地加速了其他国家数据本地化的步伐（夏燕、沈天月，2019）。[158]

3．行业协会的企业数据出境自律监管权

相对于政府的行政监管，行业自律组织有更强的灵活性和及时性。鼓励行业协会及其他自律组织参与安全评估，建立可落地实施、具有活力的数据管理秩序，作为行政监管的补充（马其家、李晓楠，2021）。[159]

具体来说，行业协会可依据本行业的特点制定探索性政策的方式，对境内外法律规定的跨境数据流动的基本原则及主要制度作进一步细化，为企业和机构提供合规性操作指引。从欧盟的法律实践看，数据控制者可以成立协会并提出所遵守的详细行为准则（codes of conduct），该行为准则经由成员国监管机构或者欧盟数据保护委员（European Data Protection Board，EDPB）认可后，可通过有约束力的承诺方式生效。[160]

我国领先的数字企业也已在行业自律方面进行了实践。例如，阿里巴巴提出《信息安全技术数据安全能力成熟度模型》，评估数据的生命周期，并在行业内推

---

021 年第 1 期，第 121 页。

[157] United States v. Microsoft Corp., U.S. Supreme Court (2018).

[158] 夏燕、沈天月：《美国 CLOUD 法案的实践及其启示》，载《中国社会科学院研究生院学报》2019 年第 5 期，第 112 页。

[159] 马其家、李晓楠：《国际数字贸易背景下数据跨境流动监管规则研究》，载《国际贸易》2021 年第 3 期，第 79 页。

[160] General Data Protection Regulation(GDPR)，https://gdpr-info.eu/.

广；腾讯、蚂蚁金服等出台了各自的隐私保护白皮书[161]，在行业内部逐渐统一和规范数据保护体系和流程。

通过行业协会构建政府与企业之间的常设性沟通机制，对于落实数据企业自律监管也有重要的意义。企业因为政府的法律规制行为而遭受损失，在很多情况下是企业与政府之间的沟通不足而导致的。因此，构建企业与政府间的信息交流平台也是十分必要的。政府作为规制一方，应当承担起搭建这一平台的责任。政府通过平台主动向企业发布相关的规制信息，帮助企业更好地适应政府的规制行为。这同样可以增进企业与政府间的相互了解，形成良好的互动关系，营造良好的法律规制环境（刘晓春、赵世勋，2017）。[162]以美国为例，美国是善用政府与企业沟通机制的典范。20 世纪 70 年代，为辅助政府参与 GATT 东京回合谈判，美国根据《1974 年贸易法》建立了贸易咨询委员会机制，机制下设了 14 个产业贸易咨询委员会，由美国贸易代表办公室和美国商务部共同管理。[163]每个产业贸易咨询委员会由产业中的龙头企业和行业协会代表组成，每年召开 3~4 次有美国政府代表参加的会议。这些委员会不仅随时向政府反映本产业在外国遇到的贸易壁垒信息，还会通过研究报告的形式，向美国贸易代表办公室系统性地反映本产业对于制定国际经贸规则的立场。美国的产业贸易咨询委员会是常态化机制，能为美国政府提供稳定、高质量的信息，并有利于培养企业参与国际规则制定的意识（徐程锦，2020）。[164]

一般来说，数据企业向政府提供的反馈主要集中于企业的经营和技术细节，其诉求的颗粒度与国际规则制定提案的要求相比存在差距。而且对于政府来说，获取企业信息的渠道比较随机、零散。形成政府和企业的常态化沟通机制是落实完善企业数据出境监管应该努力的方向。

总而言之，通过上述文献梳理，在数据出境企业的主体责任及监管上，应当明确数据出境企业的主体责任和监管机构权限，从整体上形成政府、司法层面的宏观协调监管，行业协会自律监管和精细化指引，以及数据企业主体积极自我管理数据安全的监管架构。同时，除了上述主体外，也应当发挥其他市场主体功能，如鼓励第三方机构对提供云计算、大数据业务的服务商、境外智能制造企业进行安全资质信用评级，为境内企业选择合作方提供参考；鼓励互联网服务提供者自愿采取行动限制对数据的恶意访问或者对敏感信息和重要数据的访问等，引导多元化市场主体参与数据跨境流动规范建设。

---

[161] 阿里巴巴数据安全研究院：《全球数据跨境流动政策与中国战略研究报告》，http://www.chinabigdata.com/cn/contents/3/253.html，2021 年 5 月 11 日访问。

[162] 刘晓春、赵世勋：《亟需防范数据跨境流动中的法律风险》，载《中国对外贸易》2017 年第 10 期，第 39 页。

[163] Industry Trade Advisory Center, https://www.trade.gov/itac/（last visited May 11, 2021).

[164] 徐程锦：《WTO 电子商务规则谈判与中国的应对方案》，载《国际经济评论》2020 年第 3 期，第 52 页。

（三）小结

综上国内外文献梳理，对于数据出境的企业主体责任问题，数据出境企业应负有内部管理、自查上报与泄露制止、配合审查等企业主体责任。对于数据出境企业主体责任的追责问题，部分国家的行政机构对于数据出境企业拥有处罚权和/或裁量权，美国等通过“长臂管辖”对数据出境企业有司法管辖权，行业协会的自律监管权也在少数国家规则或实践中能体现。

五、完善我国企业数据出境监管制度的国内文献

（一）我国企业数据跨境传输保护现状及立法改革完善的研究

对于我国企业数据跨境传输保护现状及立法改革完善，陈红娜提出，跨境数据流动的规则谈判，我国不论是在参与水平还是制度准备上都尚显不足，被边缘化的风险不断加大，可能导致在未来的国际竞争中处于不利地位，亟需在自身制度建设和全球规则对接上采取积极行动。中国应以推动构建国内外共通的规则体系为目标，以打造有利于跨境数据流动的监管体系为核心，以营造有助于本土数字企业出海发展和吸引国际跨国公司来华经营的营商环境为手段，以数字基础设施建设为辅助，大力支持数字贸易发展（陈红娜，2021）。[165]

崔静则提出了我国跨境数据跨境传输保护的整体设计，其指出数字经济时代下，大规模数据跨境流动对公民隐私、企业商业机密及国家安全造成极大威胁。欧盟和美国在数据跨境监管方面起步较早，已形成较为成熟的监管体系。我国在实施跨境数据流动监管过程中，应结合自身特色，积极借鉴欧美经验做法，确立分级分类监管体系，打造数据联合监管同盟，增加统一机构评估情形及明确监管机构责任，以形成兼具中国特色与智慧的跨境数据监管体系（崔静，2021）。[166]马其家等提出，数据跨境流动是数字贸易下的基本构成要素，跨境数字服务的提供、数字产品的交付都离不开数据的跨境流动，但无序的数据跨境流动可能损害国家安全、企业利益和数据主体权益。为此，在数字贸易背景下，中国应当以风险为导向，加强数据跨境流动规则的研究，在促进数字贸易发展的同时，构建收放协调的数据跨境流动监管规则（马其家、李晓楠，2021）。[167]

周念利等以中国自由贸易试验区数据跨境流动的现状为入手点，指出我国目前数据跨境流动面临着国家层面相关法律法规尚未成体系、数据分类分级规则不健全、数据出境管制办法缺乏弹性、数据跨境传输安全评估和管理机制操作难及数据主权争议等难题。建议从设置灵活的数据出境路径、确定数据分类分级标准和扩

---

[165] 陈红娜：《国际数字贸易规则谈判前景与中国面临的挑战》，载《新经济导刊》2021 年第 1 期，第 15 页。
[166] 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》，载《经济体制改革》2021 年第 2 期，第 179 页。
[167] 马其家、李晓楠：《国际数字贸易背景下数据跨境流动监管规则研究》，载《国际贸易》2021 年第 3 期，第 81 页。

大国际影响力等方面应对当前的难点和问题（周念利、姚亭亭，2021）。[168]孙方江认为，我国选择了适应当前数字经济发展形势的本土化政策，但也面临对外和对内等多重挑战。建议在总体的监管路径选择上，合理兼顾审慎性和包容性；完善跨境数据流动制度体系，保障立法的全面性和灵活性；构建跨境数据流动治理的统一监管架构，提升治理体系的统筹性和协同性；完善跨境数据流动安全评估体系，平衡金融市场的开放性和安全性（孙方江，2021）。[169]

综上，对于我国目前的企业数据跨境传输保护现状，学者普遍认为，在企业数据跨境传输方面，我国的数据评估机构欠缺，分级分类监管体系不健全，制度建设方面滞后于国际主流国家。我国企业数据跨境传输监管急需完善，主要从国际规制的制定、企业数据合法出境的国内监管完善等方面改革立法。

（二）我国在 WTO 电子商务谈判中关于数据跨境传输议题的策略

石静霞、柯静、李墨丝等对 WTO 电子商务谈判中的数据跨境传输问题进行了探讨。石静霞从 WTO 电子商务诸边谈判的最新发展及焦点问题进行研究，关于跨境数据流动的问题，她指出各谈判成员数字经济发展水平不同，核心利益诉求有别，尤其是中美欧等主要成员的立场协调是决定该谈判是否能够成功的决定性因素。对此，有必要重点分析谈判中的跨境数据流动和禁止本地化要求、源代码及算法规制和电子传输的免关税及数字税征收等核心争议问题（石静霞，2020）。[170]柯静也对 WTO 电子商务诸边谈判和全球数字贸易规则走向进行了探讨，她认为在多边规则框架产生前，区域数字贸易规则仍会不断涌现，数字经济治理碎片化将会持续加剧，监管冲突现象也将更加频繁。提出，为了应对这些挑战，除了努力团结发展中成员在当前诸边谈判中搁置分歧、共同抵制发达成员不公平的谈判主张外，中国还需要平衡好保障国家安全和促进跨境数据自由流动之间的关系。为减少监管冲突带来的风险，加强全球层面监管合作是协调不同监管机制和凝聚共识的必然路径（柯静，2020）。[171]李墨丝也认为，参加方之间在谈判路径和诉求主张上存在明显分歧，对于电子传输免关税永久化、数字产品非歧视待遇、跨境数据自由流动这些核心议题的争议尤为尖锐。这些分歧不仅反映了贸易自由化与非贸易目标的冲突，也涉及数字技术给多边贸易体制带来的挑战，还交织着互联网治理的难题（李墨丝，2020）。[172]

综上，学者普遍认为，WTO 电子商务最新谈判，不仅是贸易自由化与碎片化

---

[168] 周念利、姚亭亭：《中国自由贸易试验区推进数据跨境流动的现状、难点及对策分析》，载《国际商务研究》2021 年第 3 期，第 11 页。
[169] 孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 3 页。
[170] 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》，载《东方法学》2020 年第 2 期，第 184 页。
[171] 柯静：《WTO 电子商务谈判与全球数字贸易规则走向》，载《国际展望》2020 年第 3 期，第 62 页。
[172] 李墨丝：《WTO 电子商务规则谈判：进展、分歧与进路》，载《武大国际法评论》2020 年第 6 期，第 74 页。

的问题，数据跨境传输规则也是在谈判中不可回避的重要问题。数据本地化要求是重要的争议，在处理该争议时，要考虑到各国数据经济发展水平的差异，处理好跨境数据流动和数据保护之间的关系。

（三）国内博士论文对企业数据出境监管完善的研究状况

2017 年以来，有数篇涉及数据跨境传输监管问题的博士论文。其中，刘新宇[173]、史宇航[174]、王磊[175]三人的研究成果，不涉及企业数据或数据跨境问题。他们关注于个人数据保护、数据权利构建及其交易规则研究，但其对数据与信息的概念区分、对数据的分类的论述，对相关的基本概念厘清有一定借鉴意义。

高楚南[176]的研究成果涉及到了数据流动问题，主要是境内流动的个人数据控制者相关问题。其以个人数据保护为研究内容，从数据控制者承担义务的角度，提出全新的数据安全保护义务，构建体系化的个人数据保护制度，研究涉及数据控制者的个人数据保护义务、数据控制者失范行为、数据控制者的法律规制等方面。

田旭[177]、张舵[178]的研究成果涉及到了数据跨境流动问题。田旭围绕围绕个人数据跨境传输规则展开，讨论了个人数据跨境传输的产生、国际多边规则、影响数据跨境传输形成的软法、区域性公约、境外数据调、数据二次传输、传输限制等问题。张舵将跨境数据流动政策目标分为国家安全、公共利益、个人数据保护和知识产权四个法律问题分别进行研究和探讨，并谈论了消除跨境数据流动壁垒的法律措施，最后提出了我国应加强跨境数据规则制定的话语权，在一带一路、RCEP 中推进发展中国家的数据开放机制，并平衡好同国家安全、公共利益、个人数据保护知识产生等法律利益的建议。

综上博士论文研究成果，主要是侧重境内个人数据权利、数据交易、数据控制者责任及监管，以及跨境数据流动国际规制的构建。暂无对企业数据跨境传输出境法律监管问题进行专项研究的文章。其中对于数据跨境传输的问题，对于数据跨境传输监管也主要聚焦个人数据，也并未注意区分为数据输入与输出两种类型的监管来分类讨论。

六、总结

综上对于国内外涉及企业数据跨境传输出境监管相关文献的梳理、评议，关于数据、企业数据权益等基本理论当前学界仍有争议，本文采用“数据控制”理论，即认为只要企业对经手的数据有“技术上的控制”，即为本文讨论的企业数据出境

[173] 刘新宇：《数据权利构建及其交易规则研究》，上海交通大学 2019 年博士论文。
[174] 史宇航：《数据交易法律问题研究》，上海交通大学 2017 年博士论文。
[175] 王磊：《个人数据商业化利用法律问题研究》，中央财经大学 2019 年博士论文。
[176] 高楚南：《数据控制者安全保护义务研究》，湘潭大学 2019 年博士论文。
[177] 田旭：《网络空间中个人数据跨境传输法律规则研究》，华东政法大学 2020 年博士论文。
[178] 张舵：《跨境数据流动的法律规制问题研究》，对外经济贸易大学 2018 年博士论文。

中的“企业数据”。企业数据有部分来源于个人数据，但企业控制数据应以“个人数据”和“非个人数据”进行基本分类，这影响到企业数据出境监管中对两者的出境审批安全性评估标准等不同。

对于企业数据出境的限制，目前国际上存在以俄罗斯、美国、欧盟为代表的三种企业数据出境限制监管思路，分别代表了严格限制出境、要求数据自由流动和平衡数据流动与安全的监管策略，这本质上体现了保护数据隐私与促进数据流动的价值在国家层面上的分歧。具体来说，企业数据出境受到数据本地化要求、出境前安全评估、出境前征求个人同意程序的限制。

对于企业数据的出境监管协调机制，国际上呈现了多种模式，总体上可以欧盟的“充分性认定”（Adequacy Decision）机制及“充分保护措施”企业数据出境监管协调机制、美国的多边合作“数据流动圈”企业数据出境监管协调机制、日本的“基于信任的自由数据流通”（DFFT）机制企业数据出境监管协调机制来归纳。这三种出境监管协调机制对于本国数据出境的监管标准依次递减，日本在企业数据出境监管协调机制制定上，基本放弃了国家数据主权。

对于数据出境的企业主体责任，数据出境企业应当负有内部管理责任、自查上报与泄露制止责任、配合审查责任等企业主体责任；对于数据企业主体责任的追责，部分国家的行政机构对于数据出境企业拥有行政处罚权和/或裁量权，美国等通过“长臂管辖”对数据出境企业有司法权，行业协会的自律监管权也在少数国家规则或实践中能体现。

七、参考文献

（一）中文著作

【1】王金照等：《跨境数据流动：战略与政策》，中国发展出版社 2021 年版。

【2】孙登科：《个人数据跨境保护的法律适用问题研究》，辽宁大学出版社 2020 年版。

【3】何渊：《数据法学》，北京大学出版社 2020 年版。

【4】吴伟光：《网络、电子商务与数据法》，清华大学出版社 2020 年版。

【5】姚旭：《欧盟跨境数据流动治理：平衡自由流动与规制保护》，上海人民出版社 2019 年版。

【6】世界银行：《2016 年世界发展报告：数字红利》，胡光宇等译，清华大学出版社 2017 年版。

【7】谢远扬：《个人信息的私法保护》，中国法制出版社 2016 年版。

【8】郭明龙：《个人信息权利的侵权法保护》，中国法制出版社 2012 年版。

【9】熊励，刘慧，刘华玲：《数字与商务：2010 年全球数字贸易与移动商务研讨会论文集》，上海社会科学院出版社 2010 年版。

（二）中文论文

【10】刘俊敏、郭杨：《我国数据跨境流动规制的相关问题研究——以中国（上海）自由贸易试验区临港新片区为例》，载《河北法学》2021 年第 7 期。

【11】赵海乐：《Tik Tok 争议中的美欧数据治理路径差异研究》，载《情报杂志》2021 年第 5 期。

【12】何叶华：《论数据保护法的域外效力》，载《北京理工大学学报（社会科学版）》2021 年第 5 期。

【13】相丽玲、张佳彧：《中外跨境数据流动的法律监管制度研究》，载《情报理论与实践》2021 年第 4 期。

【14】赵磊：《数据产权类型化的法律意义》，载《中国政法大学学报》2021 年第 3 期。

【15】马其家、李晓楠：《国际数字贸易背景下数据跨境流动监管规则研究》，载《国际贸易》2021 年第 3 期。

【16】包晓丽：《数据产权保护的法律路径》，载《中国政法大学学报》2021 年第 3 期。

【17】周念利、姚亭亭：《中国自由贸易试验区推进数据跨境流动的现状、难点及对策分析》，载《国际商务研究》2021 年第 3 期。

【18】张哲、齐爱民：《论我国个人信息保护法域外效力制度的构建》，载《重庆大学学报（社会科学版）》2021 年第 3 期。

【19】蒋林君：《欧盟数据生产者权及其对我国的启示》，载《湖南科技大学学报（社会科学版）》2021 年第 2 期。

【20】李晓宇：《智能数字化下机器生成数据权益的法律属性》，载《北方法学》2021 年第 2 期。

【21】张俊娥、董晓红：《从 USMCA 看中美数字贸易规则领域的分歧及中国应对策略》，载《对外经贸实务》2021 年第 2 期。

【22】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》，载《经济体制改革》2021 年第 2 期。

【23】匡梅：《跨境数据法律规制的主权壁垒与对策》，载《华中科技大学学报（社会科学版）》2021 年第 2 期。

【24】赵盈盈：《欧盟 GDPR 对中欧数字经济合作的影响及应对》，载《对外经贸实务》2021 年第 2 期。

【25】孙浩、陈美：《荷兰政府开放数据的政策法规保障及启示》，载《情报杂志》2021 年第 2 期。

【26】许可：《自由与安全：数据跨境流动的中国方案》，载《环球法律评论》2021 年第 1 期。

【27】翟志勇：《数据安全法的体系定位》，载《苏州大学学报（哲学社会科学版）》2021 年第 1 期。

【28】叶嘉敏：《算法风险防控视域下企业数据权利的三维构建研究》，载《江西财经大学学报》2021 年第 1 期。

【29】孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期。

【30】岳云嵩、霍鹏：《WTO 电子商务谈判与数字贸易规则博弈》，载《国际商务研究》2021 年第 1 期。

【31】戴艺晗：《贸易数字化与监管碎片化：国际贸易制度框架下跨境数据流动治理的挑战与应对》，载《国际经济法学刊》2021 年第 1 期。

【32】马其家、李晓楠：《论我国数据跨境流动监管规则的构建》，载《法治研究》2021 年第 1 期。

【33】陈红娜：《国际数字贸易规则谈判前景与中国面临的挑战》，载《新经济导刊》2021 年第 1 期。

【34】米铁男：《俄罗斯网络数据流通监管研究》，载《中国应用法学》2021 年第 1 期。

【35】洪延青：《“法律战”旋涡中的执法跨境调取数据：以美国、欧盟和中国为例》，载《环球法律评论》2021 年第 1 期。

【36】丁玮：《数据主义视角下美国跨境数据政策演进及我国的应对》，载《杭州师范大学学报（社会科学版）》2021 年第 1 期。

【37】祝艳艳：《大数据时代企业数据保护的困境及路径建构》，载《征信》2020 年第 12 期。

【38】刘颖、谷佳琪：《个人信息去身份化及其制度构建》，载《学术研究》2020 年第 12 期。

【39】袁慧：《欧盟数据跨境转移中的充分决定机制研究》，载《电子知识产权》2020 年第 11 期。

【40】汪晓华：《企业数据财产权与用户个人信息权益之冲突与协调》，载《西南民族大学学报（人文社科版）》2020 年第 10 期。

【41】马海群、张涛：《从<数据安全法（草案）>解读我国数据安全保护体系建设》，载《数字图书馆论坛》2020 年第 10 期。

【42】徐文：《论个人数据的非财产性及其守护屏障》，载《兰州学刊》2020 年第 9 期。

【43】黄雨婷、傅文奇：《日本政府数据开放的政策保障及其启示》，载《数字图书馆论坛》2020 年第 9 期。

【44】孔庆江、于华溢：《数据立法域外适用现象及中国因应策略》，载《法

学杂志》2020 年第 8 期。

【45】支振锋：《贡献数据安全立法的中国方案》，载《信息安全与通信保密》2020 年第 8 期。

【46】时明涛：《大数据时代企业数据权利保护的困境与突破》，载《电子知识产权》2020 年第 7 期。

【47】范思博：《数据跨境流动中的个人数据保护》，载《电子知识产权》2020 年第 6 期。

【48】梅夏英：《信息和数据概念区分的法律意义》，载《比较法研究》2020 年第 6 期。

【49】李墨丝：《WTO 电子商务规则谈判：进展、分歧与进路》，载《武大国际法评论》2020 年第 6 期。

【50】王中美：《欧盟数据战略的目标冲突与中间道路》，载《国际关系研究》2020 年第 6 期。

【51】冉从敬、陈贵容、王欢：《美国跨境数据流动的管辖模式研究及对中国的启示》，载《图书情报知识》2020 年第 6 期。

【52】卢扬逊：《数据财产权益的私法保护》，载《甘肃社会科学》2020 年第 6 期。

【53】于浩：《我国个人数据的法律规制——域外经验及其借鉴》，载《法商研究》2020 年第 6 期。

【54】俞胜杰、林燕萍：《<通用数据保护条例>域外效力的规制逻辑、实践反思与立法启示》，载《重庆社会科学》2020 年第 6 期。

【55】任颖：《数据立法转向：从数据权利入法到数据法益保护》，载《政治与法律》2020 年第 6 期。

【56】林福辰、杜玉琼：《发展与蜕变：多边视域下数字贸易规则建构路径之审思》，载《江海学刊》2020 年第 5 期。

【57】马海群：《从<俄罗斯联邦信息安全学说>解读俄罗斯信息安全体系》，载《现代情报》2020 年第 5 期。

【58】王春晖：《完善<数据安全法（草案）>的十大建议》，载《南京邮电大学学报（自然科学版）》2020 年第 5 期。

【59】冯德淦：《数据的二元划分与体系保护》，载《中南大学学报（社会科学版）》2020 年第 5 期。

【60】崔聪聪、许智鑫：《数据保护影响评估制度：欧盟立法与中国方案》，载《图书情报工作》2020 年第 5 期。

【61】田旭：《欧盟个人数据保护法的全球影响成因与启示》，载《江西财经大学学报》2020 年第 4 期。

【62】李牧翰：《数字经济下民事新权利的构建：数据资源权》，载《云南社会科学》2020 年第 4 期。

【63】徐汉明、孙逸啸、吴云民：《数据财产权的法律保护研究》，载《经济社会体制比较》2020 年第 4 期。

【64】余振：《全球数字贸易政策：国别特征、立场分野与发展趋势》，载《国外社会科学》2020 年第 4 期。

【65】刘洪愧：《数字贸易发展的经济效应与推进方略》，载《改革》2020 年第 3 期。

【66】徐程锦：《WTO 电子商务规则谈判与中国的应对方案》，载《国际经济评论》2020 年第 3 期。

【67】柯静：《WTO 电子商务谈判与全球数字贸易规则走向》，载《国际展望》2020 年第 3 期。

【68】周念利、李金东：《俄罗斯出台的与贸易相关的数据流动限制性措施研究——兼谈对中国的启示》，载《国际商务研究》2020 年第 3 期。

【69】丁晓东：《论企业数据权益的法律保护——基于数据法律性质的分析》，载《法律科学（西北政法大学学报）》2020 年第 2 期。

【70】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》，载《东方法学》2020 年第 2 期。

【71】翁国民、宋丽：《数据跨境传输的法律规制》，载《浙江大学学报（人文社会科学版）》2020 年第 2 期。

【72】刘天骄：《数据主权与长臂管辖的理论分野与实践冲突》，载《环球法律评论》2020 年第 2 期。

【73】周斯佳：《个人数据权与个人信息权关系的厘清》，载《华东政法大学学报》2020 年第 2 期。

【74】丁曼：《数字经济与日本网络空间治理战略》，载《现代日本经济》2020 年第 1 期。

【75】韩旭至：《信息权利范畴的模糊性使用及其后果——基于对信息、数据混用的分析》，载《华东政法大学学报》2020 年第 1 期。

【76】许娟：《利用爬虫技术侵犯企业数据知识产权法益的司法解释》，载《苏州大学学报（哲学社会科学版）》2020 年第 1 期。

【77】王远志：《我国银行金融数据跨境流动的法律规制》，载《金融监管研究》2020 年第 1 期。

【78】郑令晗、肖冬梅：《欧盟非个人数据自由流动制度及其中国本土化》，载《图书情报工作》2019 年第 13 期。

【79】张涛：《欧盟个人数据匿名化治理：法律、技术与风险》，载《图书馆

论坛》2019 年第 12 期。

【80】刘江山：《欧盟通用数据保护条例中的数据保护官制度》，载《中国科技论坛》2019 年第 12 期。

【81】东方：《欧盟、美国跨境数据流动法律规制比较分析及应对挑战的“中国智慧”》，载《图书馆杂志》2019 年第 12 期。

【82】管洪博：《大数据时代企业数据权的构建》，载《社会科学战线》2019 年第 12 期。

【83】胡文华、孔华锋：《印度数据本地化与跨境流动立法实践研究》，载《计算机应用与软件》2019 年第 8 期。

【84】薛亚君：《数字贸易规则中的数据本地化问题探究》，载《对外经贸实务》2019 年第 8 期。

【85】齐湘泉、文媛怡：《构建“一带一路”个人数据跨境传输法律制度：分歧、共识与合作路径》，载《河南师范大学学报（哲学社会科学版）》2019 年第 6 期。

【86】石丹：《企业数据财产权利的法律保护与制度构建》，载《电子知识产权》2019 年第 6 期。

【87】韩伟：《安全与自由的平衡——数据安全立法宗旨探析》，载《科技与法律》2019 年第 6 期。

【88】夏燕、沈天月：《美国 CLOUD 法案的实践及其启示》，载《中国社会科学院研究生院学报》2019 年第 5 期。

【89】丁晓东：《用户画像、个性化推荐与个人信息保护》，载《环球法律评论》2019 年第 5 期。

【90】陆青：《个人信息保护中“同意”规则的规范构造》，载《武汉大学学报（哲学社会科学版）》2019 年第 5 期。

【91】梅夏英：《在分享和控制之间：数据保护的私法局限和公共秩序构建》，载《中外法学》2019 年第 4 期。

【92】李扬、李晓宇：《大数据时代企业数据权益的性质界定及其保护模式建构》，载《学海》2019 年第 4 期。

【93】程昊：《从“云幕”法案看我国数据主权的保护》，载《情报理论与实践》2019 年第 4 期。

【94】马述忠、房超、梁银锋：《数字贸易及其时代价值与研究展望》，载《国际贸易问题》2019 年第 2 期。

【95】谭必勇、陈艳：《加拿大联邦政府数据治理框架分析及其对我国的启示》，载《电子政务》2019 年第 1 期。

【96】韩冰：《法制保障机制是落实网络主权的重要举措》，载《中国信息安

全》2018 年第 11 期。

【97】曹博：《跨境数据传输的立法模式与完善路径——从<网络安全法>第 37 条切入》，载《西南民族大学学报（人文社科版）》2018 年第 9 期。

【98】石静霞、张舵：《跨境数据流动规制的国家安全问题》，载《广西社会科学》2018 年第 8 期。

【99】张继红：《个人数据跨境传输限制及其解决方案》，载《东方法学》2018 年第 6 期。

【100】金晶：《欧盟<一般数据保护条例>：演进、要点与疑义》，载《欧洲研究》2018 年第 4 期。

【101】胡炜：《跨境数据流动立法的价值取向与我国选择》，载《社会科学》2018 年第 4 期。

【102】魏书音：《CLOUD 法案隐含美国数据霸权图谋》，载《中国信息安全》2018 年第 4 期。

【103】龙卫球：《再论企业数据保护的财产权化路径》，载《东方法学》2018 年第 3 期。

【104】张舵：《略论个人数据跨境流动的法律标准》，载《中国政法大学学报》2018 年第 3 期。

【105】许多奇：《个人数据跨境流动规制的国际格局及中国应对》，载《法学论坛》2018 年第 3 期。

【106】李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期。

【107】伊万·沙拉法诺夫、白树强：《WTO 视角下数字产品贸易合作机制研究——基于数字贸易发展现状及壁垒研究》，载《国际贸易问题》2018 年第 2 期。

【108】刘晓春、赵世勋：《亟需防范数据跨境流动中的法律风险》，载《中国对外贸易》2017 年第 10 期。

【109】龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期。

【110】梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016 年第 9 期。

（三）学位论文

【111】田旭：《网络空间中个人数据跨境传输法律规则研究》，华东政法大学 2020 年博士论文。

【112】王磊：《个人数据商业化利用法律问题研究》，中央财经大学 2019 年博士论文。

【113】刘新宇：《数据权利构建及其交易规则研究》，上海交通大学 2019 年

博士论文。

【114】高楚南：《数据控制者安全保护义务研究》，湘潭大学 2019 年博士论文。

【115】张舵：《跨境数据流动的法律规制问题研究》，对外经济贸易大学 2018 年博士论文。

【116】史宇航：《数据交易法律问题研究》，上海交通大学 2017 年博士论文。

（四）英文著作

【117】KERBER,W.& ZOLNA,K.K., THE GERMAN FACEBOOK CASE: THE LAW AND ECONOMICS OF THE RELATIONSHIP BETWEEN COMPETITION AND DATA PROTECTION LAW (2020).

【118】LIU, H. W., DATA LOCALIZATION AND DIGITAL TRADE BARRIE RS: ASEAN IN MEGAREGIONALISM (2018).

（五）英文论文

【119】Mira Burri, *Towards a New Treaty on Digital Trade*, 55 JOURNAL OF WORLD TRADE 77(2021).

【120】Mira Burri, *Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions*, 22 JOURNAL OF WORLD INVESTMENT AND TRADE 34(2021).

【121】Ahmed Arafa Abdelrehim, Asif Khan, Nishan-E-Hyder Soomro, *Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response*, 8 INTERNATIONAL JOURNAL OF SOCIAL SCIENCES PERSPECTIVES 41 (2021).

【122】Taro Komukai， *A Comparative Study of the Extraterritorial Enforcement of Data Protection Rules in the EU, US and Japan*，1 GLOBAL PRIVACY LAW REVIEW 3（2020）.

【123】Khan, A. et al., *Plurilateral Negotiation of WTO E-commerce in the Context of Digital Economy: Recent Issues and Developments*, 26 JOURNAL OF LAW AND POLITICAL SCIENCES 28 (2020).

【124】Kahn, A., Wu, X.，*Impact of Digital Economy on Intellectual Property Law*，13 JOURNAL OF POLITICS AND LAW 117(2020).

【125】Dai, l.， *Data Protection Laws—one of the Most Important Sources of Competitive Advantage in the Context of International Trade*, 4 JOURNAL OF DATA PROTECTION & PRIVACY 72(2020).

【126】Casarosa, Federica, *Transnational Collective Actions for Crossborder Data Protection Violations*, 9 INTERNET POLICY REVIEW 1 (2020).

【127】Andrew D Mitchell, Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 JOURNAL OF

INTERNATIONAL ECONOMIC LAW 389 (2019).

【128】Clare Sullivan, *EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the Eu and Apec to Cross Border Data Transfers and Protection of Personal Data in the Iot Era*, 35 COMPUTER LAW & SECURITY REVIEW 380(2019).

【129】R.S.Neeraj， *Trade Rules for the Digital Economy: Charting New Waters at the WTO*， 18 WORLD TRADE REVIEW 128 (2019).

【130】Bennett C., *Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?*, 10 ASSOCIATION FOR COMPUTING MACHINERY 880(2018).

【131】Gao, H.， *Digital or Trade? The Contrasting Approaches of China and Us to Digital Trade*, 21 JOURNAL OF INTERNATIONAL ECONOMIC LAW 297(2018).

【132】Mira Burri， *Symposium-Future-Proofing Law: From RDNA to Robots the Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*，51 U.C. DAVIS LAW REVIEW 119（2017）.

【133】Andrew D.Mitchell，Jarrod Hepburn，*Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*， 19 YALE JOURNAL OF LAW AND TECHNOLOGY 196（2017）.

【134】Mitchell, A.D., Mishra, N.， *Data at the Docks: Modernizing International Trade Law for the Digital Economy*， 20 VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW 1073 (2017).

【135】Burri, M., *The Regulation of Data Flows Through Trade Agreements*, 48 GEORGETOWN JOURNAL OF INTERNATIONAL LAW 418（2017）.

【136】Stephanie Carroll Rainie et al.， *Data as a Strategic Resource: Self-determination， Governance， and the Data Challenge for Indigenous Nations in the United States*, 8 THE INTERNATIONAL INDIGENOUS POLICY JOURNAL 13(2017).

八、附录

【1】European Commission， *A European Strategy for Data*, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf (last visited May.11, 2021).

【2】UNCTAD， *Digital Economy report: Value Creation and Capture Implications for Developing Countries*， https://unctad.org/webflyer/digital-economy-report-2019 (last visited May.11, 2021).

【3】Eiichi Tomiura et al., *Effects of Regulations on Cross-border Data Flows Evi*

dence from a Survey of Japanese Firms , https://www.rieti.go.jp/jp/publications/dp/19e088.pdf (last visited May.11, 2021).

【4】Rachel F.Fefer, *Data Flows, Online Privacy, and Trade Policy*, https://www.everycrsreport.com/files/20190311_R45584_caa16f89385a9b89430cfaac5d6633c392313c45.pdf (last visited May.11, 2021).

【5】GS1，*New EU Regulation on the Free Flow of Nonpersonal Data*, https://www.gs1.org/sites/default/files/infopackage-free-flow-non-personal-data.pdf. (last visited May.11, 2021).

【6】European Commission , *EU Data Protection Reform: Ensuring its Enforcement*, https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-role-edpb_en.pdf (last visited May.11, 2021).

【7】European Commission , *Competition Policy for the Digital Era* , https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf (last visited May.11, 2021).

【8】AlphaBeta, *The Data Revolution: How China can Capture the Digital Trade Opportunity at Home and Abroad*, http://en.ccg.org.cn/archives/68004 (last visited May. 11, 2021).

【9】United States Congress, *Data Protection Law: An Overview - United States Congress*, https://fas.org/sgp/crs/misc/R45631.pdf (last visited May.11, 2021).

【10】European Commission, *EU Provisions on Cross-border Data Flows and Protection of Personal Data and Privacy in the Digital Trade Title of EU Trade Agreements*, https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf (last visited May. 11, 2021).

【11】*Comparing Privacy Laws: GDPR v. LGPD*， https://www.dataguidance.com/sites/default/files/gdpr_v_lgpd_revised_edition.pdf (last visited May.11, 2021).

【12】Martina F. Ferracane et al., *Do Data Policy Restrictions Inhibit Trade in Services?*, https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf (last visited May.11, 2021).

【13】USITC, *Digital Trade in the U. S. and Global Economies 2017*, https://epic.org/crs/R44565.pdf (last visited May.11, 2021).

【14】European Commission，*Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence*， https://ec.europa.eu/eip/ageing/sites/eipaha/files/news/shaping_europe_s_digital_future_commission_presents_strategies_for_data_and_artificial_intelligence.pdf (last visited May.11, 2021).

【15】ECIPE，*Restrictions on Cross-Border Data Flows A Taxonomy*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089956 (last visited May.11, 2021).