全球数据跨境流动政策与中国战略研究

阿里巴巴数据安全研究中心
上海赛博网络安全产业创新研究院
上海社会科学院互联网研究中心

2019 年 3 月

目录

数据跨境流动，又称信息跨境流动、信息跨境转移，是指通过各种技术和方法，实现数据跨越国境（地理疆域）的流动。在数字经济时代，数据跨境流动广泛存在。麦肯锡全球研究院（MGI）《数据全球化：新时代的全球性流动》报告指出，自 2008 年以来，数据流动对全球经济增长的贡献已经超过传统的跨国贸易和投资，不仅支撑了包括商品、服务、资本、人才等其他几乎所有类型的全球化活动，并发挥着越来越独立的作用，数据全球化成为推动全球经济发展的重要力量[1]。

从地缘政治层面来看，2013 年“斯诺登事件”推动了各国将数据跨境流动纳入政治议题，与国家安全、网络安全、隐私保护等政策紧密挂钩，加剧了各国政府在网络空间的战略博弈与数据资源争夺。**从经济贸易层面来看，**数字经济发展对传统国际贸易和分工机制产生重大冲击。随着中国科技企业在全球产业价值链中的地位不断上升，以美国为首的一些西方国家经济政策开始转向“保护主义”，并在科技领域对中国实施“战略围剿”，国际经济和贸易秩序面临重大的分化与重组。**从产业发展层面来看，**在大数据、云计算、AI、5G 等新兴技术产业领域，各国政府倾向于通过干预导向的产业政策加强本国的数字资源禀赋，与此相关的数据跨境流动的政策考量最终也成为国家间产业政策竞赛的内容之一。当前，各国数据跨境流动政策选择越来越受到地缘政治、国家安全、隐私保护、产业能力、市场准入等复杂因素的影响。同时，利益的复杂性、价值认同的差异性和国家间信任的缺乏，阻碍了各国在短期内形成规则共识。究竟是推动“数据自由流动”还是加强“数据本地化”，如何在安全性和成长性中实现平衡，考验各国政府的数据战略思维和治理能力。

作为数字经济发展最为迅速的国家之一，中国在数字经济总体规模和电子商务、金融科技等领域都位于世界前列，阿里巴巴、腾讯等互联网龙头企业位列全球上市公司中市值前十。中国在全球数字经济产业价值链中的地位迅速提升，全球新经济的地理重心从环大西洋地区转向了环太平洋地区。随着我国改革开放政策和“一带一路”倡议的持续深化推进，我国数字经济在跨境贸易和全球化方面

[1] Mckinsey Global Institute. Digital Globalization, http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/Digital-globalization- The-new-era-of-global-flows, 访问时间：2018 年 11 月 28 日。

有待进一步拓展和提升。因此，根据我国推动大数据发展的国家战略背景，基于我国当前数字经济发展现状和产业能力，分析各国跨境数据流动规则背后的产业竞争和政策选择，探讨如何完善国内法规定，保证数据在确保安全的情况下实现自由流动，提出制定和参与国际规则的策略方案，构建我国数据资源战略和数据治理能力，无疑具有重大的理论价值和迫切的现实意义。

一、全球数字经济发展格局与产业竞争态势

2016 年 9 月的 G20 峰会上，二十国集团对数字经济的定义是：“以使用数字化的知识和信息作为关键生产要素、以现代信息网络作为重要载体、以信息通信技术的有效使用作为效率提升和经济结构优化的重要推动力的一系列经济活动。”从上述定义可以发现，数字经济没有明确清晰的行业分类与边界。全球知名统计数据网站 Statista 尝试将数字经济细分为数字媒体（Digital Media）、电子商务（E-Commerce）、电子服务（E-Service）、智能家居（Smarthome）、金融科技（Fintech）、数字广告（Digital Advertising）、联网汽车（Connected Car）以及数字旅行（E-Travel）八个产业领域。

1. 中美两国在数字产业总体规模上优势凸显

为了清晰地观察全球数字产业规模分布情况，本报告在 Statista 对 2019 年各国数字经济发展的预测数据中，选取了 50 个国家的数据绘制于图 1 中。由图 1 和表 1 可见，全球数字产业规模分布呈现较强的不平衡状态。中美两国在数字产业领域的规模优势凸显无疑，数字产业总规模分别将达到 2.56699 万亿美元和 1.902037 万亿美元。西欧、北美地区的数字产业规模集聚程度也处于较高水平，非洲很多国家并不存在数字产业、中东欧地区国家的数字产业规模也同样较小。东南亚地区国家的数字产业主要分布于马来西亚、印度尼西亚、新加坡和泰国，其余国家的数字经济产业规模较小。

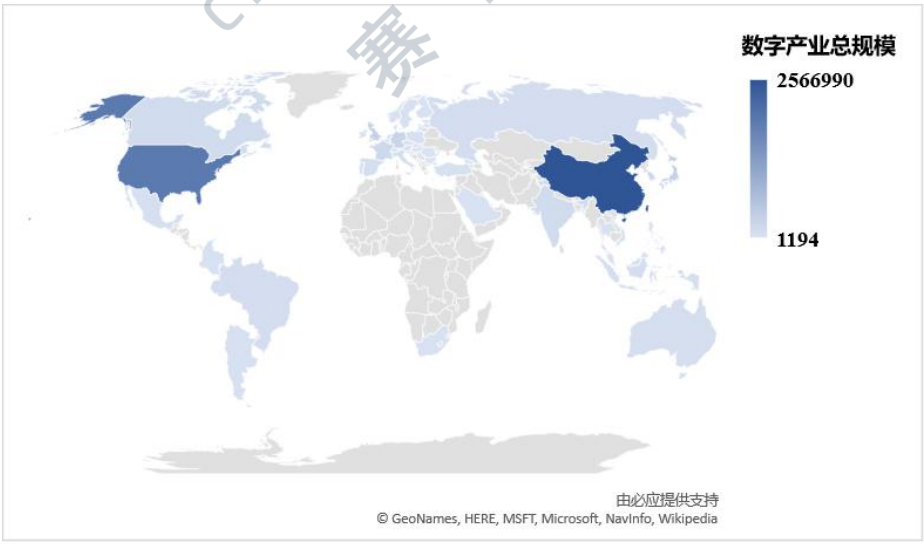

图 1 全球数字经济规模分布情况图（2019）

（本课题组根据 Statista 网站数据绘制）

表 1 全球数字产业规模排名前 50 国家（2019） 单位：百万美元

排名	国家	Digital Media	Digital Advertising	eCommerce	eServices	Smart Home	FinTech	Connected Car	eTravel	数字产业总规模
1	中国	28011	6915	718389	53895	11613	1563675	4050	180442	2566990
2	美国	46167	26457	547690	55734	27240	962027	6968	229754	1902037
3	英国	6691	1883	91750	8794	3882	162082	1364	45095	321541
4	日本	16372	4266	86125	5094	4193	163843	763	37743	318399
5	德国	4399	1854	75445	6191	4042	118404	1586	34121	246042
6	韩国	4547	1254	68554	3332	2379	113254	506	18022	211848
7	法国	3588	641	49929	4239	1903	88300	803	27932	177335
8	印度	2217	493	32348	10444	1691	64775	614	17797	130379
9	加拿大	2391	1228	31214	3891	1211	61616	245	18498	120294
10	巴西	1617	1545	15955	3168	734	47639	276	18943	89877
11	俄罗斯	2302	320	18613	3585	609	45137	263	18182	89011
12	意大利	2181	650	18991	2776	953	40576	740	14624	81491
13	澳大利亚	1200	829	21224	2632	1278	41728	376	11582	80849
14	西班牙	1473	431	19679	2055	723	41344	485	13816	80006
15	印度尼西亚	1477	760	11133	1891	303	32446	149	17052	65211
16	荷兰	961	331	16780	1885	917	29569	146	8809	59398
17	墨西哥	1721	811	9224	2127	367	30279	251	13492	58272
18	瑞典	726	394	11264	1005	728	23761	195	8047	46120
19	瑞士	547	319	8563	693	383	19191	184	6413	36293
20	波兰	708	277	9917	765	230	17205	75	4542	33719
21	阿根廷	592	2298	3432	977	59	16599	52	9287	33296
22	土耳其	669	565	6108	1161	303	16817	117	5559	31299
23	奥地利	439	140	8783	695	350	13895	120	4082	28504
24	比利时	483	132	6377	894	230	13572	246	5238	27172
25	泰国	420	199	4375	373	57	13213	57	7961	26655
26	沙特阿拉伯	625	515	7141	396	305	13465	92	3743	26282
27	丹麦	306	295	7176	560	411	14097	87	3109	26041
28	挪威	422	430	6361	569	402	12994	83	3933	25194
29	新加坡	224	105	4989	431	115	12309	46	5859	24078
30	哥伦比亚	952	208	3807	250	127	13179	17	5241	23781
31	爱尔兰	284	150	6775	450	49	10947	77	2594	21326
32	马来西亚	262	135	3751	252	105	10533	85	5234	20357
33	芬兰	393	203	3557	458	240	8940	40	3568	17399
34	越南	228	42	2709	301	83	8524	24	5035	16946
35	南非	263	328	3308	793	299	8054	63	3098	16206
36	以色列	287	161	3801	264	118	8529	83	2182	15425
37	葡萄牙	178	54	3290	279	88	7532	46	2508	13975
38	菲律宾	335	64	970	443	134	7353	17	4484	13800

39	捷克	194	286	2674	379	112	4519	25	2077	10266
40	罗马尼亚	175	15	2809	146	107	3380	16	1898	8546
41	匈牙利	102	54	2042	120	81	3180	14	1386	6979
42	斯洛伐克	81	30	930	122	52	1882	12	1033	4142
43	克罗地亚	41	10	492	71	60	1260	6	607	2547
44	保加利亚	33	37	627	59	40	991	3	669	2459
45	立陶宛	31	29	694	50	45	1189	3	409	2450
46	斯洛文尼亚	42	12	366	43	20	956	6	512	1957
47	拉脱维亚	20	18	356	33	32	875	2	426	1762
48	塞尔维亚	34	30	354	42	40	813	3	429	1745
49	爱沙尼亚	14	15	339	41	25	802	3	299	1538
50	格鲁吉亚	37	11	151	6	4	663	0	322	1194

（本课题组根据 Statista 网站数据制作）

为了更加清晰地分析全球数字产业发展格局，本报告选取了中国、美国、欧盟[2]、日本、韩国、印度、俄罗斯、澳大利亚、印度尼西亚和新加坡这 10 个积极制定数据跨境流动政策的国家/地区，对其 2019 年数字产业规模以及增长速度情况进行分析。图 2 可见，根据 Statista 的预测数据，2019 年，中国、美国和欧盟的数字产业规模位居前三位，日本和韩国紧随其后，但是其在规模上已经与中美欧存在非常显著的差距。印度尼西亚和新加坡在十个经济体当中的排名为第九和第十。中国在数字产业总规模上将超越美国，这得益于中国庞大的国内市场和数字化消费群体[3]，催生了基于平台的社会化大协作。[4][5]

从增长速度来看，位居前三甲的中国、美国和欧盟，中国的数字产业增长速度最高，美国其次，欧盟位于中美两国之后。印度、新加坡、澳大利亚和印度尼西亚的数字产业规模虽然较中美欧三国/地区存在很大差距，但是其在数字产业增长速度上表现出强劲的势头，照此速度，印度、新加坡、澳大利亚和印度尼西亚的数字产业在未来有望快速发展。除此之外，俄罗斯、日本和韩国的数字产业增长速度在这十个经济体当中处于较低水平。

[2] 由于数据限制，本文统计的欧盟国家仅包括英国、德国、法国、西班牙、意大利、荷兰、瑞典、波兰、奥地利、丹麦、比利时、芬兰、爱尔兰、捷克共和国、罗马尼亚、匈牙利、斯洛伐克共和国、立陶宛、保加利亚、克罗地亚、斯洛文尼亚、拉脱维亚、爱沙尼亚等 23 个国家，下同。

[3] 依据中国互联网信息中心的统计数据，截止 2018 年 6 月 30 日，中国网民数量达到 8.02 亿。

[4] 阿里研究院、KPMG：《2018 全球数字经济发展指数》。该报告也将美国、中国、英国、韩国、瑞典、挪威、日本、丹麦、新加坡、荷兰分列 2018 全球数字经济发展指数前十名。

[5] 中国互联网信息中心：第 42 次《中国互联网络发展状况统计报告》，https://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201808/P020180820630889299840.pdf, 访问时间：2018 年 12 月 7 日。

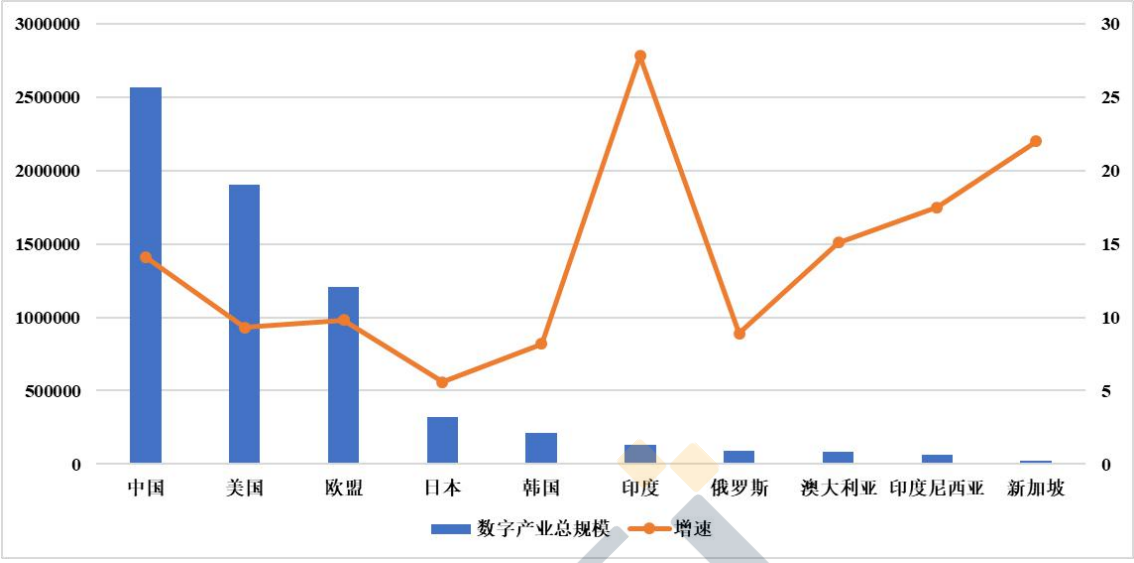

图 2 世界主要经济体数字经济总规模与增长率情况（2019）

（本课题组根据 Statista 网站数据制作）

2. 中美两国在数字产业细分行业领域各有千秋

为了更加深入地分析当前全球数字产业细分领域的发展格局，探究各国在数字产业细分领域的发展优势与不足，本报告对数字产业的八个细分行业数据采用功效得分公式进行百分制标准化[6]，对上述十个主要经济体的数字产业内部细分产业发展状况进行深入分析。从数字产业构成比例来看（见图 3），十个全球主要经济体的数字产业内部细分行业中，金融科技（Fintech）在上述十个经济体当中均占据较高比重，其次是电子商务（E-Commerce），这种比例结构特征得益于近年来全球电子商务和互联网金融的飞速发展。目前中美欧等全球主要经济体均把电子商务和互联网金融等新兴数字产业领域作为本国发展的重点。

[6]具体公式是某国在某一细分行业领域的得分 $\boldsymbol{X=(X_c-X_{min})/(X_{max}-X_{min})\times 100(c=1,2,3...)}$，$X_{min}$ 为某细分行业规模最小的国家的行业规模数值，X_{max}为某细分行业规模最大的国家的行业规模数值，X 为计算的目标国家在该细分行业的百分制得分。

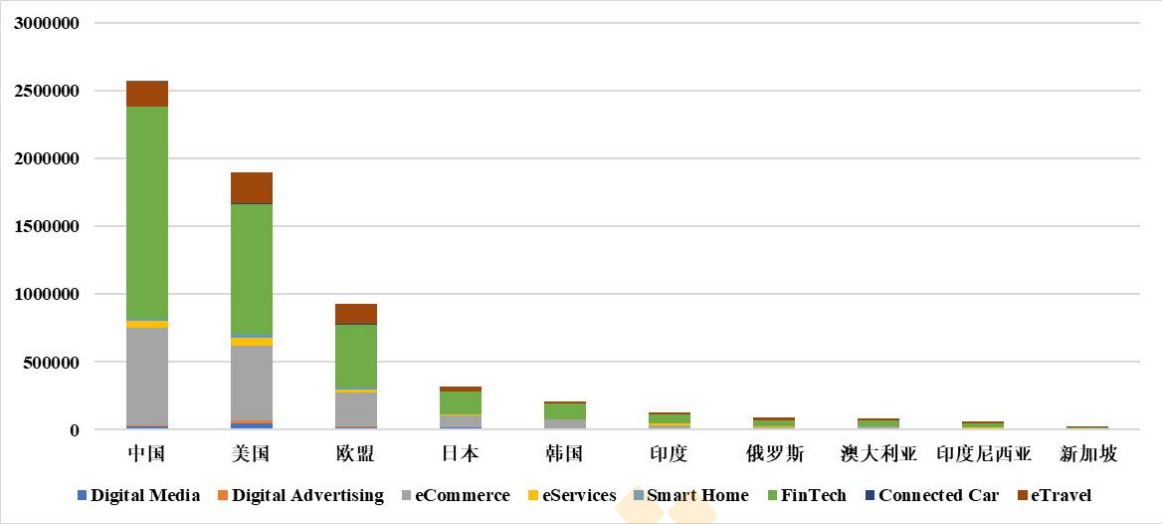

图 3 全球主要经济体数字产业构成

（本课题组根据 Statista 网站数据制作）

各国数字产业内部细分行业发展状况存在较强的异质性（参见图 4）。中国在电子商务（eCommerce）和金融科技（FinTech）这两个细分行业领域规模位居全球第一，电子服务（eServices）行业规模仅次于美国，且与美国保持极小差距，但是其余五个细分行业规模得分相对较低，其中数字媒体（Digital advertising）和智能家居（Smart Home）两个细分行业规模则处于中下游水平。美国在数字媒体(Digital Media)、智能家居(Smart Home)和联网汽车(Connected Car）、电子服务（E-Services）、数字广告（Digital Advertising）、数字旅游（E-travel）这六个细分行业规模局全球首位。且与中国相比，美国的数字产业各细分行业领域发展比较均衡，呈现出结构均衡的数字产业大国形象。日本数字产业细分领域中，数字媒体（Digital Media）规模相对较高，但是其他细分行业规模与中国和美国相比均处于较低水平。欧盟的数字产业各细分行业当中，数字旅游（etravel）和联网汽车（Connected Car）规模较大，其余细分行业规模仍有待提高。除此之外，其余 6 个国家的数字产业规模已经与前面 4 个国家（或地区）存在非常显著的差距。

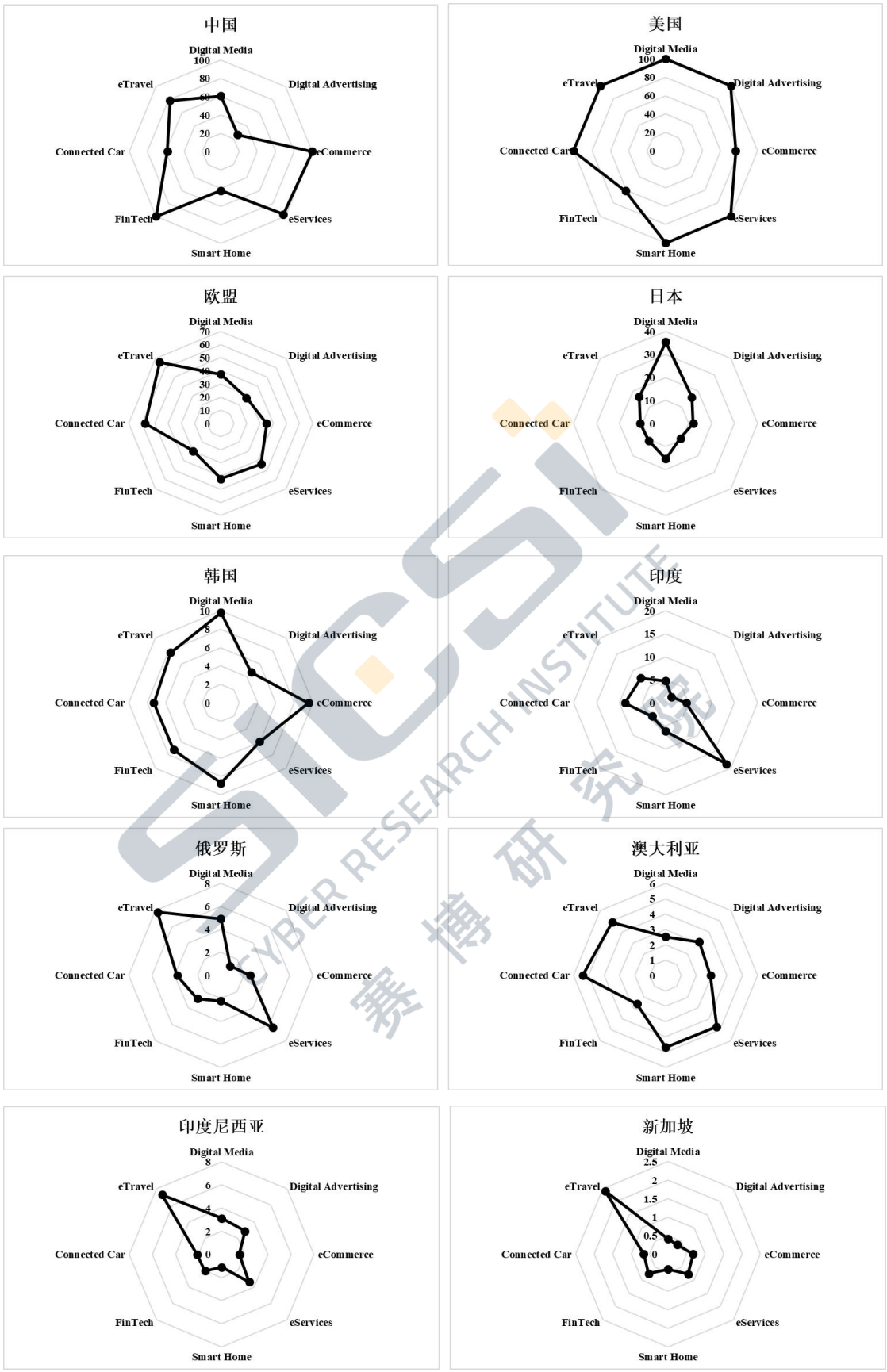

图 4　全球主要经济体数字产业内部结构情况图

（本课题组根据 Statista 统计数据绘制）

3. 中国 ICT 服务出口落后于美欧印等国家和地区

一国数字产业的竞争力水平除了规模竞争力之外，还包括市场竞争力等因素。本文选取 2017 年世界银行 ICT 出口额统计数据，通过 ICT 出口数据分析主要国家数字产品和服务在国际市场上的竞争力状况。

ICT 是世界经济增长的新领域，中国凭借着制造业的强大优势，在 ICT 商品出口方面占据了全球超过 1/4 的份额。但是从 ICT 出口的全球发展趋势来看，随着全球网络用户和移动用户渗透率趋向于饱和，设备、终端等与制造业相关的 ICT 需求量的增长速度趋于下降，而用户数量的增长驱动了长尾效应和用户价值的增长，ICT 服务将有长期的需求。而我国虽然 ICT 商品出口在全球处于领先位置，但是 ICT 服务还缺乏出口的竞争力。ICT 服务是数字经济发展的重要领域。我国国内网络用户渗透率高、用户总量大，形成了全球最大的数字经济国内市场，在数字产业总体规模上与美国相当，但是在 ICT 服务贸易上与美欧等发达国家和地区还有差距，甚至落后于印度，成为我国数字经济发展的一块短板（参见图 5）。因此，保障数据跨境自由流动，推动我国 ICT 服务出口的发展，才能在未来的数字经济竞争中取得进一步的发展。

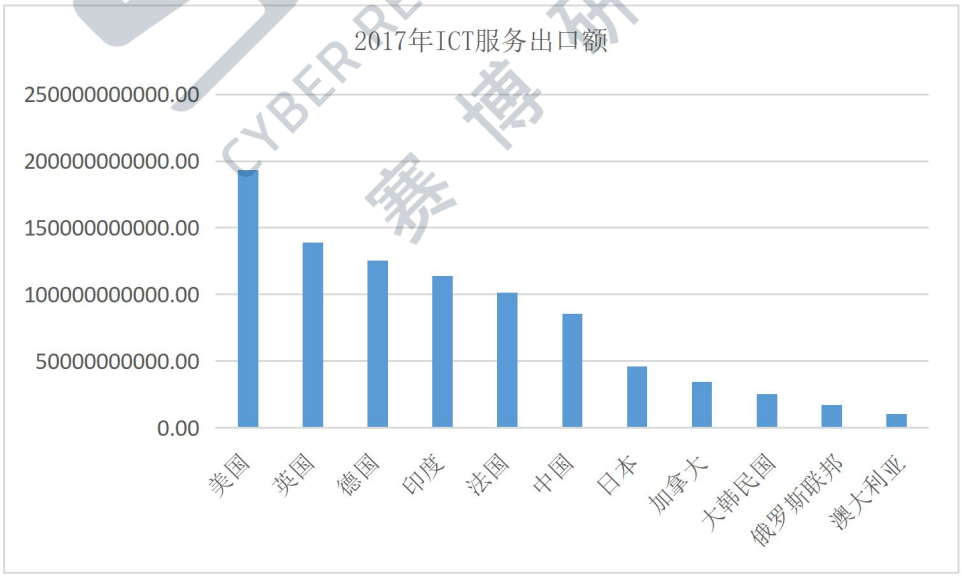

图 5 主要国家 2017 年 ICT 服务出口金额（亿美元）

（本课题组根据世界银行数据绘制）

二、跨境数据流动的价值与风险

1. 数据跨境流动的价值

总体来看，跨境数据流动在促进经济增长、加速创新、推动全球化等方面发挥了积极作用，推动数据跨境自由流动能够实现保障用户权利和提升全社会经济总体效用。

（1）促进经济增长。基于生产要素国际流动理论，数据的跨国界流动可以帮助企业更直接、更合理地利用全球要素资源，不仅支撑起包括商品、服务、资本、人才等其他几乎所有要素的全球化活动，也在发挥着越来越独立且重要的作用。世界经济论坛称“跨境数据流动的能力是高效行业的一个关键要素，也是关键的生产力增强剂，对维持全球复苏和为经济体奠定长期竞争力基础至关重要。”[7]思科公司的数据分析表明，数据跨境流动可以改善企业流程并产生巨大的经济价值。在 2015-2024 年期间，跨境流动潜在的最低价值（定义为包括增加的收入和降低成本的双重含义，这种价值由于互联网技术的采用而在公司和行业之间产生和转移）估计为 29.7 万亿美元[8]。由此可以看出，数据跨境流动将带来全社会经济总体效用的提升，对国家和企业经济增长具有重要的积极意义。

（2）提升创新能力。数据跨境流动意味着信息、知识的传播与共享，自由流动的数据是国家创新的重要催化剂，根据 Frost & Sullivan 的 2025 年大趋势预测，数据支撑着未来，90%的变革性转变严重依赖于数据[9]。目前，几乎所有行业都依赖于跨境数据的流动和实时分析数据的能力，以此作为其供应链、运营和商业模式创新的推动力。数据跨境流动使创新性的想法在全球扩散，使全球的互联网用户都可以接触、利用最新研究成果和技术，并激发更多创意，催生新业务、新模式和新企业，实现国家创新能力的整体提升。

---

[7] Kuner C. Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future, http://www.oecd-ilibrary.org/science-and-technology/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_5kg0s2fk315f-en, 访问时间：2018 年 12 月 8 日。

[8] Cross-Border Data Flows, Digital Innovation, and Economic Growth, http://reports.weforum.org/global-information-technology-report-2016/1-2-cross-border-data-flows-digital-innovation-and-economic-growth/，访问时间：2018 年 12 月 8 日。

[9] Frost & Sullivan, Mega Trends in LATAM, Forecast to 2025，http://www.frost.com/sublib/display-report.do?id=K015-01-00-00-00&bdata=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS9AfkBCYWNrQH5AMTU0NzI1ODIyMDQ2Nw%3D%3D, 访问时间 2019 年 1 月 10 日。

（3）推动全球化发展。互联网开放互联的特性满足企业天然的全球经营需要和便利。数据是企业经营的“血液”，跨境数据流动极大地推动了企业面向全球的商业拓展。WEF《2016 年全球信息技术报告》认为，正是跨越国界的数据传输能力优化了企业运营，使企业能够重新构想他们的方法。[10]以跨境电商为例，阿里巴巴、亚马逊等互联网平台企业通过互联网获取、处理和跨境传输数据，为各类跨境贸易商构建了全球用户社区，实现了电子商务模式的全球扩张，帮助企业融入全球供应链。同时，企业跨境数据流动降低了企业贸易和交易的成本，大量中小型公司几乎和大型企业有了同样的国际贸易能力[11]。

（4）保障用户数字权利。以云计算为例，根据思科预测，到 2021 年全球云数据中心流量将达到每年 19.5ZB，2021 年全球将有 628 个超大规模数据中心。[12]基于云计算的跨境数据流动模式弱化了 存储地理位置的约束，而由用户根据服务内容、质量、成本等在全球范围内灵活地选择云计算服务商，可以提升用户服务水平和体验，保障用户的数字权利。

2. 数据跨境流动的风险

大数据环境下，大规模和复杂的数据跨境流动成为常态。数据跨境活动带来的风险成为许多国家实施数据本地化策略的正当性理由。尤其是网络空间博弈愈来愈与地缘政治、产业竞争、经贸关系、网络主权、权利保护等各种议题相结合，数据跨境流动也成为当前国家地区间政策博弈最为复杂的领域之一。

（1）数据跨境流动引发数据安全风险担忧。数字经济的快速发展加速了个人数据的全球流通和融合，也使其作为重要的生产要素的价值得以凸显。个人数据的价值和重要性决定了其被觊觎的高概率，全球数据黑色产业链日益成熟，离境数据被恶意利用和买卖的现象频发，个人数据泄露事件不断发生，对个人隐私、财产甚至人身安全造成威胁。与此同时，各国个人数据保护标准不一致，造成数

[10] World Economic Forum: Global Information Technology Report 2016, https://www.weforum.org/agenda/2016/07/free-flow-of-data-between-countries/，访问时间：2018 年 12 月 23 日。

[11]美国国际贸易中心报告估计，跨境数据流动将全球贸易成本平均降低了 26%，利用互联网在全球各类商业平台上交易的中小型企业存活率为 54%，比线下企业高出 30%。参见 http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf，访问时间：2018 年 12 月 23 日。

[12] Cisco: Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html，访问时间：2018 年 11 月 28 日。

据在全球范围内不受限制地流动缺乏安全可信的在线环境。保护标准较高的国家质疑其公民个人数据流向保护标准较低的国家将导致数据隐私和安全风险。因此，许多国家的个人数据保护立法开始提出数据跨境流动的限制性规定，比如欧盟、新加坡、日本等国提出的“相同保护水平”要求，即个人数据接收国需要达到流出国相同的数据保护水平，以为本国/地区公民个人数据安全提供保障。

（2）数据不受限制地外流影响本国数字产业发展机会。据统计，2016 年全球新增数据量达到 16.1ZB，预计到 2025 年将再增长十倍达到 163ZB[13]。从长远发展看，数据本身是生产力的资源。越来越多的互联网企业通过对海量、实时、异构的数据资源进行开发利用并取得巨大商业成功。同时，数据也会变得像工业时代的石油一样，成为国家重要战略资源，如何积累数据、精炼数据以及加工和管控数据，将成为决定国家经济命脉的重要因素。对于许多数字产业能力不强的国家来说，放任数据不受限制地流向境外，可能损害本国企业开发利用数据资源的发展机会，影响本国数字产业和数字经济竞争力的提升。这也是许多网络用户众多，但是本国产业竞争力不足的国家出台数据本地化政策的理由，以此拉动本地数据产业的发展，保护本国产业利益。

（3）数据跨境流动阻碍政府实施执法权。大数据时代，犯罪技术更加具有隐蔽性，“跳板技术”等新兴犯罪手段可以更加容易地掩盖攻击源头。数据跨境使得大量数据流向境外，执法机关提取有价值的证据需要耗费更多的时间和人力资源，高效甄别数据价值的挑战更大。[14]在跨境数据取证的合作过程中，执法活动会受到预防能力或补救权利不足的实际阻碍，使得域外取证处于被动地位。也就是说，数据离境会增加执法成本。当然，在不同司法管辖区域内的执法活动可以通过司法互助双边协议予以实现，但目前实施效果并不理想。为弥补跨国犯罪管辖权不足、提升执法便利性，美国依托其遍布全球的互联网跨国企业实施长臂管辖，而以俄罗斯为代表的国家则提出数据本地化备份等要求，对数据跨境活动实施监管。

（4）数据跨境流动威胁国家主权与安全

[13] IDC. Data Age 2025: The Evolution of Data to Life-Critical[EB/OL].[2017-1-5]. https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.
[14] 黄道丽，何治乐：欧美数据跨境流动监管立法的“大数据现象”及中国策略，载《情报杂志》2017 年 4 月。

大数据时代，“国家拥有数据的规模、流动、利用等能力将成为综合国力的重要组成部分。”[15]包括个人、企业和国家数据等在内的数据早已不仅是国家“软实力”体现，更关涉情报、军事、国防等国家安全领域。各国在新生的网络空间确立边疆追求权力，信息的流动和分享越来越受到政治性因素的影响。数据跨境流动议题由此与国家主权与安全密切联系。数据对国家主权维护有重要意义，是支撑国家安全与发展的重要战略资源，具有极为重要的主权保护价值。因为数字产业竞争力差距的存在，今天世界的基本现实是，数据产业竞争力较弱的国家的用户是数据的主要提供者，数据产业竞争力较强的国家的公司则是设备和服务的主要提供者，在不设限制的情况下，数据将自然向少数国家地理疆域之内汇聚。对于产业能力较弱的国家而言，拒绝数据跨境流动将使国家被排除在世界网络体系之外，损害数据经济发展机遇和公民福利，但是放任数据自由流动则将会引发国家安全威胁，给国家主权的完整性带来严峻挑战。因此，对数据跨境流动加以合理限制，有助于技术能力暂时处于弱势地位的国家，不会因为能力的差异而导致合法利益受到损害，使数据的使用能够促进数据初始提供者的利益，而非成为少数掌握了技术和产业优势的行为体过度追求自身利益的工具。

[15]李海英：大数据发展及其立法挑战，载《信息安全与通信保密》2015 第 6 期。

三、全球数据跨境法律政策与发展趋势

1.重要国家和地区的法律政策特点

（1）美国：以维护产业竞争优势为主旨，构建数据跨境流动与限制政策

一是主张个人数据跨境自由流动，利用数字产业全球领导优势主导数据流向。美国在信息通信产业和数字经济上具有全球领先优势，这一点是其主导全球跨境数据流向的前提。美国在制定“跨太平洋伙伴关系协定”（Trans-Pacific Partnership Agreement，TPP）时就提出“在确保保护个人信息等合法公共政策目标得到保障的前提下，确保全球信息和数据自由流动，以驱动互联网和数字经济。不将设立数据中心作为允许 TPP 缔约方企业进入市场的前提条件，也不要求转让或获取软件源代码。”[16]这一主张是美国个人数据跨境流动政策的集中体现。美国在与各国的新一轮贸易谈判中都主张将“数据跨境自由流动”纳入协议条款，以破除许多国家利用数据跨境流动设置的市场准入壁垒。

二是通过限制重要技术数据出口和特定数据领域的外国投资，遏制中国等战略竞争对手发展，确保美国在科技领域的全球领导地位。自特朗普政府大力推行“美国优先”的贸易保护主义政策以来，美国积极使用这类管制措施作为遏制中国等战略竞争对手的重要手段。美国《2019 财年约翰•麦凯恩国防授权法》（NDAA）更新和改革了美国对外国投资审查和新兴基础技术出口限制措施。[17]在出口管制方面，根据《出口管理条例》（EAR）[18]，美国的出口管制并不限于硬件的出口，还包括具体的技术数据[19]，即受管制的技术数据“传输”到位于美国境外的服务器保存或处理，需要取得商务部产业与安全局（BIS）出口许可。2018 年 11 月美国商务部工业安全署（BIS）发布 14 类前沿技术封锁清单，拟制定针对关键技术和相关产品的出口管理体系框架，包含生物技术、人工智能和机器学

[16]商务部国际司翻译《跨太平洋伙伴关系协定》内容摘要，http://mp.weixin.qq.com/s?__biz=MzA5MTg4MjA2Mw==&mid=400018789&idx=1&sn=fa84d5598bf5004d6220161755e6a316&scene=1&srcid=1017plcR2X3ZJQ3vpBxu5u2i#rd， 访问时间：2018 年 12 月 14 日。

[17] NDAA 的主要内容包括《外国投资风险审查现代化法》（FIRRMA）、《出口管制改革法》（ECRA）、《中国投资活动报告》，建立人工智能国家安全委员会。

[18] EAR 主要对既有军事用途也有商业用途的两用物品以及有关的数据信息提出管控要求。

[19] 15 C.F.R. § 730.5(c)

习等十四项核心前沿技术。[20]2018 年 10 月 29 日，美国商务部还以“对美国国家安全利益构成显著威胁”为由，将约 90 家中国企业列入违反美国国家安全和外交利益的企业名单，要求对这些企业出口、再出口及转让美国原产货物、软件及技术，必须遵守额外的许可证规定。美国的出口管制内容与“中国制造 2050”有较大重叠部分，其政策主旨在于强化对华技术出口封锁。

在外国投资审查方面，美国外国投资委员会（CFIUS）有权在必要时审查和限制广泛的投资交易和出口交易，建立多种机制来识别和保护关键的新兴技术，以保障美国的安全。[21]改革后的《外国投资风险审查现代化法》扩大了“涵盖交易”的范围，将涉及所谓“关键技术”、“关键基础设施”的公司以及外国人对保存或收集美国公民敏感个人数据的公司进行非控制性、非被动性投资都纳入其审查范围。同时 CFIUS 还要求投资者签署安全协议[22]，对内部安全管理制度、产品和服务的本地化、政府审查权等规定了详细的内容，以防止敏感信息、产品和服务出境。尽管该法案针对的是所有国家投资美国核心高科技行业的审查，但在 35 页的法案中，对中国提及 15 处，远超其他国家，并专门在条款中明确要求美国商务部部长每两年向国会提交有关“中国企业对美直接投资”以及“国企对美交通行业投资”的报告，还规定当 CFIUS 在进行国家安全评估时，CFIUS 可考虑“适用交易是否涉及特别关注国，而该国已表明或宣布收购某种关键技术为战略目标”，针对中国的指向明显。

三是制定受控非秘信息（controlled Unclassified Information）清单，界定“重要数据”范围。根据美国总统 2010 年签署的 13556 号行政令要求，为改善美国法律、条例、政府政策文件等规定的政府受管制非秘信息过于分散，无统一要求的现状，由美国档案局牵头，各相关政府部门协同参与梳理、统一美国法律、规定、政府政策规定的受管制非秘数据分类及依据，形成管控非秘数据列

[20] Bureau of Industry and Security, Commerce, Review of Controls for Certain Emerging Technologies, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies, 访问时间：2018 年 12 月 14 日。

[21] 2018 年 11 月 BIS 公布的拟制定的针对关键技术和相关产品的出口管理体系框架，包含生物技术、人工智能和机器学习技术、定位、导航和定时技术、未处理技术、先进计算技术、数据分析技术、量子信息和传感技术、物流技术、增材制造、机器人、脑机接口、高超音速空气动力学、先进材料、先进监控技术等十四项核心前沿技术。

[22] 安全协议的官方称谓是“风险减轻措施”（Mitigation Measures）。根据 15 年发布的报告，2011 年-2013 年间，CFIUS 在 27 起并购申请中采用安全协议，约占总审查案件的 8%，2013 年则在 11 起并购申请中采用，比例也上升到 11%。

表（CUI）（参见表 2）。CUI 详细列出了农业、受控技术信息、关键基础设施、应急管理、出口控制、金融、地理产品信息、信息系统漏洞信息、情报、国际协议、执法、核、隐私、采购与收购、专有商业信息、安全法案信息、统计、税收等 17 个门类。这类数据可以视为美国政府识别的“重要数据”，采取较为严格的管理措施。同时将 CUI 的传播范围分为七类：禁止向外国传播、联邦雇员专用、联邦雇员和承包商专用、不向承包商开放、受管制的开放列表、只允许开放给某些国民、仅显示。[23]

表 2 美国受管制非秘信息清单（CUI）分类情况

目录		类别描述
组织性的索引分组	CUI 类别	
关键基础设施	硝酸铵、化学品恐怖主义脆弱性信息、关键能源基础设施信息、应急管理、一般性关键基础设施信息、信息系统脆弱性信息、物理安全、受保护的关键基础设施信息、SAFETY Act 信息、有毒物质、水质评估	对安全、经济、公共健康或安全、环境等有重大影响的系统和资产。
国防	受管制的技术信息、国防部关键基础设施安全信息、海军核动力推进信息、非机密受控核信息-国防	国防安全信息。
出口管制	出口管制、出口管制研究	预计信息出口会影响美国的国家安全和核不扩散目标的不保密信息。
金融	银行秘密、财政预算、总审计长、消费者投诉信息、电子资金转账、联邦住房金融非公共信息、金融监管信息、一般金融信息、国	与金融机构的职责、交易和美国政府财政职能管辖相关的信息。

[23] National Archives: Controlled Unclassified Information, https://www.archives.gov/cui/registry/limited-dissemination, 访问时间：2018 年 12 月 22 日。

	际金融机构、合并、净资产、退休	
移民	难民、受虐待的配偶或子女、永久性的居民身份、身份调整、临时受保护身份、人口贩卖的受害者、签证	有关接纳非美国公民进入美国，申请临时和永久居留权的信息。
情报	农业、外国情报监控法、外国情报监控法商业记录、一般情报、土地测量产品信息、情报财务记录、内部数据	与情报活动、来源或方法有关的信息。
国际协定	国际协定信息	与外国政府或国际组织合作生产，根据现有条约需要保护的协定。
执法	事故调查、竞选基金、精神病人、通信、受管制物质、刑事历史档案信息、DNA、一般执法活动、线人、调查、青少年、执法财务记录、国家安全信函、笔式记录器/陷阱及追踪、奖励、性犯罪受害者、恐怖分子筛选、告密者身份	有关执法行动、调查、检控的技术和程序。
法律	行政程序、儿童色情、儿童受害人/证人、集体协商、联邦大陪审团、法律特权、法律资料、现况报告、前次逮捕、保护令、受害者、证人保护计划	司法或准司法程序中有关诉讼的信息。
自然及文化资源	考古资源、历史建筑物、国家公园系统资源	自然及文化资源保护信息。
北大西洋公约组织	北约受限制信息、北约非加密信息	北大西洋公约国际协定所产生的信息。
核能	一般核能、核建议资料、核安全相关信息、安全保障信息、非机密受控核信息-能源	有关核反应堆、材料或安全信息的保护。
专利	专利申请、发明、保密令	专利权是一种财产权。

隐私	合同使用、死亡记录、一般隐私、基因信息、健康信息、向检察长报告者的身份、军事人事档案、人事档案、学生记录	个人信息。
采购及购置	一般采购及购置、小型企业研究与技术、资源选择	与货物或服务的获取和采购有关的信息。
专有商业信息	一般专有商业信息、海运共同承运人及海运码头经营人协议、远洋共同承运人服务合同、专有制造商、专有邮政、承包商建立管理系统	与公司的产品、业务或活动相关的信息。
暂行	国土安全协议信息、国土安全执法信息、信息系统脆弱习惯信息-国土、国际协定信息-国土、运营安全信息、人员安全信息、物理安全-国土、隐私信息、敏感个人身份信息	
统计资料	投资调查、除害剂生产者调查、统计信息、美国人口普查	由联邦统计机构收集的统计信息。
税务	联邦纳税人信息、税务协定、纳税人律师资料、书面决定	有关政府收入的强制性贡献的信息。
交通	铁路安全分析记录、敏感安全信息	与任何旅游方式或运输方式有关的信息。

（本课题组根据美国国家档案馆资料整理）

四是通过“长臂管辖”扩大国内法域外适用的范围，以满足新形势下跨境调取数据的执法需要。2018 年，美国议会通过《澄清境外数据的合法使用法案》（Clarifying Lawful Overseas Use of Data Act，CLOUD 法案）结束了“微软 vs FBI”案中关于美国执法机关是否有权获得美国企业存储在境外服务器中的用户数据的争议。通过适用“控制者原则”，该法扩大了美国执法机关调取海外数据的权力，同时为美国政府与其他国家签订双边条约设定了具体路径，允许适格外国政府（qualifying foreign government）执法机构调取美国存储的数据。

CLOUD 法案对要求美国总检察长（连同国务卿）向国会提交书面报告，判定“适格外国政府”的认定条件，也就是“外国政府的国内立法，包括对其国内法的执行，是否提供了对隐私和公民权利足够的实质和程序上的保护”。认定基于可信的信息和专家的意见，考虑了六方面的因素：①外国政府在网络犯罪和电子证据方面，是否拥有足够的实质性和程序性法律，是否加入了《布达佩斯网络犯罪公约》，或其国内法与该公约的基本规则相吻合[24]；②展现出对法治和非歧视原则的尊重；③遵守国际人权义务或展现出对国际基本人权的尊重，包括保护隐私免于肆意和非法的干涉、公平审判权、言论、结社及和平集会的自由、免肆意逮捕和监禁、避免酷刑和残酷的非人道或贬低人格的待遇和惩罚；④对允许通过行政协定获取数据的外国政府机关，有清晰的法律要求和程序，包括这些机关收集、获取、使用和共享数据的程序，以及对上述数据活动的有效监管；⑤有足够的机制能对外国政府收集和使用电子数据课以责任和提供适当的透明度；⑥展现出对全球信息自由流动和维护互联网开放、分布式、互联本质的决心和承诺。除此之外，该外国政府应采取了适当的程序，最小化了对涉及“美国人”信息的获取、留存和散布。

CLOUD 法案抛开了传统的双边或多边司法协助条约，[25]加剧了当前国家间与数据有关的司法主权冲突，其有效落实有赖于美国的国际经济与政治的强势地位以及与相关国家的合作。其他国家要调取存储在美国的数据，则必须通过美国“适格外国政府”的审查，需满足美国所设定的人权、法治和数据自由流动标准。

（2）欧盟：统一规则实施欧盟数字化单一市场战略，以数据保护高标准引导全球重建数据保护规则体系

一是消除欧盟境内数据自由流动障碍，实施欧盟数字化单一市场战略。2015 年 6 月，欧盟提出实施《数字化单一市场战略》，主要目的就是消除成员国间的管制壁垒，将 28 个成员国的市场统一成一个单一化的市场，推动欧盟数字经济发

[24] 《布达佩斯网络犯罪公约》（Cyber-crime Convention）是于 2001 年 11 月由欧洲委员会的 26 个欧盟成员国以及美国、加拿大、日本和南非等欧洲委员会观察员国家共同签署的国际公约，是全世界第一部针对网络犯罪行为所制订的国际公约。截止 2019 年 3 月，已有 63 个国家批准了该公约，还有 4 个国家签署了该公约，但尚未批准。参见网络犯罪公约网站
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[25] 比如美国参加的《海牙取证公约》《布达佩斯网络犯罪公约》等司法协助条约。

展。为了实现数字化单一市场，欧盟通过了《一般数据保护条例》（GDPR）和《非个人数据在欧盟境内自由流动框架条例》。通过 GDPR 在成员国层面的直接适用，消除成员国数据保护规则的差异性，实现个人数据在欧盟范围内的自由流动。《非个人数据在欧盟境内自由流动框架条例》则致力于消除各成员国的数据本地化要求，确保成员国有权机关能够及时获取数据，保障专业用户能够自由迁移数据。

二是通过“充分性认定”确定数据跨境自由流动白名单国家，推广欧盟数据保护立法的全球影响力。列于白名单中的国家，不受欧盟个人数据跨境流动的限制。欧盟对“充分性认定”的考量因素包括了政治因素、法治因素、数据保护立法与执法情况，签订的国际协议等等。“充分性认定”规则在一定程度上对其他国家改革个人数据保护法产生了重大影响，提升了欧盟个人数据保护规则对全球的示范效应。目前欧洲委员会确认的白名单国家共有 13 个，包括安道尔，阿根廷，加拿大（商业组织），法罗群岛，根西岛，以色列，马恩岛，泽西岛，新西兰，瑞士，乌拉圭和美国（仅限于隐私盾框架[26]）、日本。韩国正在与欧盟谈判之中，印度也被考虑纳入谈判议程。GDPR 还允许欧盟委员会对第三国或国际组织内的特定地区、一个/多个部门进行充分性认定。这似乎为一个国家内的特定地区或经济部门提供了充分性认定的大门。

三是在遵守适当保障措施的条件下，提供多样化的个人数据跨境流动方式。在缺乏充分性认定的情况下，欧盟还为企业提供了遵守适当保障措施条件下的转移机制，包括公共当局或机构间的具有法律约束力和执行力的文件、约束性公司规则（BCRs）、标准数据保护条款（欧盟委员会批准/成员国监管机构批准欧盟委员会承认）、批准的行为准则、批准的认证机制等。这些机制为在欧盟收集处理个人数据的企业提供了可选择的数据跨境流动机制，但是以 BCRs 为例，欧盟成员国的批准要求非常严格，需要漫长的审批过程。此外，行为准则和认证机制是 GDPR 提出的新的跨境流动机制。欧盟委员会很有兴趣开发这些机制，但是欧洲法院是否会限制这类机制的适用范围还有待观察。

[26] 2016 年 7 月 12 日，“美欧隐私盾框架”获得了欧盟充分性认定，并于 2016 年 8 月 1 日开始运作。根据隐私盾框架，加入该框架的美国企业可以为商业目的将欧盟境内个人数据自由传输至美国。

四是积极推进行犯罪数据的境外调取。2018 年 4 月，欧盟委员会提出了《电子证据跨境调取提案》[27]。与美国的 CLOUD 法案类似，欧盟将不以数据存储位置作为确定管辖权的决定因素，只要同时满足以下条件，欧盟成员国的执法或司法当局可直接向为欧盟境内提供服务的服务提供商要求提交电子证据：（1）被要求提交的数据为刑事诉讼所需 ；（2）被要求提交的数据与服务提供商在欧盟境内提供的服务有关。

（3）新加坡：以建设亚太地区数据中心为导向，积极参与数据跨境流动合作机制

一是主张高水平的数据保护和数据自由流动相结合，吸引跨国企业设立数据中心。新加坡是亚太地区第四大互联网数据中心，仅次于日本、中国和印度。通过“智慧国家（Smart Nation）”战略，新加坡实现了信息基础设施现代化，推动了电信业与数据中心的投资。[28]在亚洲云计算协会（ACCA）发布的“2018 年云就绪指数（Cloud Readiness Index，CRI）”中，新加坡位列第一。其在宽带质量、网络安全、隐私保护、政府监管、知识产权保护等细分领域都排名第一，显示在基础设施和监管方面的优势地位。[29]同时，新加坡从地理上靠近成熟的澳大利亚、日本、韩国等亚太地区公共云服务市场，这也是推动新加坡以建设亚太地区数据中心为战略目标的重要因素。新加坡建立了与欧盟类似的数据跨境传输要求，禁止向数据保护水平低于新加坡的国家或地区转移数据，但在特殊情况下，企业可以申请获得个人数据保护委员会的豁免。[30]此外，立法还提供了“数据跨境传输合同条款”作为补充。[31]这些弹性化的机制使新加坡成为跨国企业设立亚太区域数据中心的优先考虑之地。

[27] Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters

[28] 2016 年，新加坡数据中心的收入为 7.3 亿美元，印度为 10 亿美元，中国为 29 亿美元，日本为 65 亿美元。根据 Broad Group 的《东南亚数据中心》报告的数据，新加坡目前有 22 家数据中心运营者，管理 46 个 facilities。Cushman & Wakefield’s 最近发布的《数据中心投资: 合适投资者的难得机会》报告，将新加坡列为亚洲 10 个国家中数据中心业务运营最强劲的市场。

[29] 参见亚洲云计算协会：Cloud Readiness Index2018，http://asiacloudcomputing.org/studies/cri2018/results/

[30] 参见新加坡《2012 年个人信息保护法》第 26 条“个人信息跨新加坡国境传输”条款。

[31] 参见《个人信息保护法关键概念咨询指南》（2015 年 5 月）19.5 “数据跨境传输合同条款”。

二是积极加入 CBPRs，寻求区域内数据自由流动。2018 年 2 月，新加坡加入了亚太经合组织(Asia-Pacific Economic Cooperation，APEC)主导的跨境隐私规则（Cross-Border Privacy Rules，CBPR）体系。根据 CBPR 的文件，加入 CBPR 体系要求评估成员国当前的隐私保护法、隐私保护执法机构、隐私信任认证机构、隐私法与 APEC 隐私框架的一致性。新加坡个人资料保护委员会目前正在发开一项与 CBPR 对接的认证机制。获得这一认证，在新加坡经营业务的企业即可以与 CBPRs 成员国的认证企业自由传输数据。

（4）日本：同时与欧盟、APEC 等机制对接，积极推动跨境数据自由流动规则构建

一是国内立法形式上参考欧盟，但通过更为弹性化的解释推动数据跨境自由流动。作为亚洲最为成熟的经济体，日本早在 2003 年就通过了《个人信息保护法》（APPI），并在 2015 年进行了修改。数字经济的全球化发展也推动日本在修订 APPI 之时引入对数据跨境转移的监管，规定了三种向境外转移个人数据的合法方法：（1）事先征得个人同意；（2）转移的目的国是个人信息保护委员会认可的具有和日本同样保护水平的国家（白名单国家）[32]；（3）接受数据的海外企业依照个人信息保护委员会的要求建立了保护数据的完善体系，能够为数据提供有效保护（与 APEC 跨境隐私规则体系相一致）。虽然数据跨境转移的规则形式上参考了欧盟，但日本对规则的解释更为弹性，为数据跨境自由流动提供了空间。比如根据日本个人信息保护委员会（PIPC）发布的指南，日本向外国进行数据传输中的接收方如果能够确保采用“适当与合理的方式”，这种数据传输即可被允许。PIPC 指南给出了一些实例，比如数据发送方和接收方之间通过签订合同、认证、签署谅解备忘录等方式，日本境内的经营者将个人数据的处理委托给外国的经营者；还有一种情况是，个人数据是在同一个集团内部根据管理规则、隐私政策等规定进行传输，这些规则和政策同时约束数据发送方和接收方。PIPC

[32] 同等保护水平需满足的条件包括：①对于处理个人信息的经营者或其下属机构规定了同等的法律或其他规则；②设立了与“个人信息保护委员会”同等的独立监管机构以及配套机制，以实施必要和适当的监管；③基于对于个人信息利用和个人权益保护的共同理念而与日本达成合作；④在保护个人信息的同时，互相保障数据的顺畅流动，对个人数据的国际传输施加的限制不得超越保护个人信息的必要范围；⑤按照第 24 条规定确定的外国列表，能够为日本的产业创新、经济社会蓬勃发展以及实现国民的富裕生活做出贡献。

指南要求采取的以上措施应当具有“国际一致性”。判断国际一致性时，需要考虑《经济合作与发展组织（OECD）隐私指南》、《APEC 隐私框架》等国际组织制定的规则。指南明确提到了根据《APEC 跨境隐私规则》（CBPR）制度获得认证的经营者可以被认为采用了“适当与合理的方式”。

二是积极参与多边和双边数据跨境协定谈判，推动数据跨境自由流动规则的构建。一方面，日本积极跟随美国数据跨境自由流动的政策主张，积极参与美国为主导的跨太平洋伙伴关系协定(TPP)和 APEC 的 CBPR 规则体系，并且在美国退出 TPP 后成为主导“全面且先进的跨太平洋伙伴关系协定”（CPTPP）的主要成员国。同时，日本作为 CBPR 的成员国，通过建立认证制度，为企业遵循 CBPR 规则实施跨境数据传输提供保障。日本的经济产业省（METI）也积极致力于推广 CBPR 体系，指定日本情报经济信息推进协会（JIPDEC）作为 CBPR 要求的独立的问责机构，负责审查和认证企业跨境数据转移活动。另一方面，日本又积极对接欧盟的数据保护规则，制定补充规则（Supplementary Rules）以弥合欧盟和日本在数据保护规则上的差异，对敏感数据、数据主体权利和继续转移源自欧盟的个人数据加强保护。2019 年 1 月 23 日，欧盟通过了对日本的数据保护充分性认定，实现了日欧之间双向互认。[33]此外，日本政府还积极推进“美国-欧盟-日本三方的数据跨境自由流动框架，并计划在 2019 年 6 月 G20 峰会期间进行磋商。日本在高标准的数据保护和数据跨境自由流动之间积极探索，致力于构建一个开放且安全的信息通信技术市场，但也有研究认为，日本致力于数据自由流动的开放政策，主要在于日本市场上各种形式的保护主义政策早已存在[34]，并不需采取其他国家将外国竞争者挡在国内市场之外的数据保护主义政策，比如数据本地化措施。

[33] European Commission: Questions & Answers on the Japan adequacy decision，http://europa.eu/rapid/press-release_MEMO-19-422_en.htm, 访问时间：2019 年 1 月 24 日。

[34]日本的经济政策严重依赖于大企业和企业联盟（Keiretsu），比如日本的出租车协会不希望优步进入日本，并且一直在阻止优步的扩张；日本汽车市场一直是受保护程度最高的汽车市场，日本汽车制造商控制着国内汽车零部件市场的 96%；另外，同时，日本的消费习惯通常更倾向于购买本地制造的产品。Helen Lui: Japan: Policy Commitment to Free Data Flow with Informal Restrictions, https://jsis.washington.edu/news/japan-policy-commitment-free-data-flow-informal-restrictions/#_ftnref16

（5）韩国：国家安全关切控制特定领域数据流动，对等原则控制跨境数据流向

一是国家安全关切下的特殊领域数据本地化要求。由于韩国在技术上仍与朝鲜处于战争状态，为了保护国家安全，韩国数据本地化法律有其独特性。韩国对空间地理数据的跨境传输予以限制，禁止将地图、照片、调查结果或任何土地检测数据传输至境外，禁止外国企业使用韩国国内资源，因为这将损害韩国的国家安全利益。[35]韩国在空间地理数据上的特殊保护措施是一种数据本地化措施的类型。韩国对个人地理位置信息也予以严格限制，[36]明确规定未经同意不得收集和使用。此外，韩国还规定通信服务提供商应采取必要手段，防止有关工业、经济、科学技术等重要信息通过互联网向国外流动。[37]

二是在公共服务领域内要求数据本地化存储，推动本国云计算产业发展。韩国利用数据本地化政策进行电子商务、在线支付、云计算等产业的保护主要集中在公共部门采购领域。比如在 2015 年颁布的《云计算促进和保护用户法》(Act on Promotion of Cloud Computing and Protection of Users）中，要求云计算服务商在为公共机构提供服务时需要将数据在本地存储，并且必须在物理上独立于为公众提供服务的网络。该法旨在为韩国云计算产业发展奠定基础。

三是对实施数据跨境流动限制的国家实施“对等原则”。2011 年韩国《个人信息保护法》对数据跨境流动的限制并不严厉，在“征得数据主体同意”的情况下即可转移。[38] 但是 2018 年 8 月，韩国通信委员会（KCC）修订《信息与通信网络法》，除了“数据主体同意”以外，还提出了“对等原则”，即韩国监管机构可以对限制个人数据流出的国家进行同样的个人数据跨境转移限制。韩国监管机构提出的“对等原则”为其动态控制数据流向提供了手段。

---

35 参见《1961 年韩国土地调查法》。

36 韩国《位置信息保护法》关注于未经位置所有人同意而收集位置信息的行为。该法第 15 条第 1 款规定，在未获得个人或移动物体所有人同意的情况下，任何人不得收集、使用或提供有关个人或移动物体的位置信息。

37 韩国《信息通信网络的促进利用与信息保护法》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”。

38 《个人信息保护法》第 17（3）条规定，个人信息管理者向任何境外地点第三人提供个人信息时，应当向数据主体通知本条第二款所列事项，并征得数据主体同意，并且不得签订任何违反本法规定的关于跨境转移个人数据的合同。

四是积极推动双边和多变跨境流动机制谈判。2012 年，韩美自由贸易协定（KORUS FTA）是双边贸易规则中首次提出数据自由流动问题的协定。KORUS FTA 第 15.8 条要求各缔约方“尽量避免对电子信息跨境流动强加或维持非必要的壁垒”。虽然该条并未禁止各缔约方设置贸易壁垒，也没有明确何为“必要”或“非必要”的壁垒，从实施上来说并不具有强制性。但是此后，“数据跨境自由流动条款“在“美-加-墨贸易协定”、TPP 和 WTO 有关“电子商务”议题谈判中都明确作为具有约束性和可诉性的条款。此外，2017 年 6 月，韩国加入了 APEC 的跨境隐私规则（CBPR），韩国网络和安全局（KISA）正准备申请成为 CBPR 所要求的问责机构。同时，韩国也正与欧盟开展谈判，欧盟正在评估韩国数据保护法律的充分性。

（6）印尼：数据跨境规则难以落实，尝试实施风险分类分级的数据本地化规则

一是现有的数据跨境流动规则形同虚设，政府倾向于签订国际双边协议。当前，印尼有关个人数据跨境流动的限制主要规定于 2016 年 10 月印尼通信与信息部长发布的《电子系统个人数据保护条例》（MOCI Regulation 20）。MOCI Regulation 20 要求将数据转移至海外必须与通信与信息部进行协调。协调意味着必须向 MOCI 报告转移个人数据的计划[39]，但是 MOCI 并没有明确规定该协调程序。因此，迄今为止，只有少数企业自愿遵守这项协调义务。MOCI 从未试图强制执行这一规则，该规则目前在实践中被广泛忽视。**目前，印尼《个人数据保护法》（草案）正在征求公众意见。**草案规定了个人数据跨境转移的数种合法性理由，包括以下几种：（1）数据主体同意；（2）数据接收国必须达到与该草案一样的个人数据保护水平；（3）在数据控制者和境外第三方之间签订了合同；（4）与数据接收国签订了国际双边协定。可以看出，印尼有关个人数据跨境流动的规定借鉴了欧盟 GDPR 中所使用的“充分性保护”的概念。但是在该法律草案的说明中，草案拟定者也承认，实践中监管机构很难实施或证实这一充分性标准，所以更倾向于签订国际双边协定。

[39] 报告的内容包括：目的地国家的名称；数据接收方的名称；转移日期；转移的原因或目的；要求 MOCI 协助转移（如果需要的话）；报告转移活动的结果。

二是对数据风险进行分类，实施分级本地化存储要求。根据 2012 年第 82 号政府条例，提供“公共服务”的电子系统运营者必须在 2017 年 10 月 15 日之前建立岸上数据中心和灾后恢复中心。但是“公共服务”的定义和范围一直未能得到澄清。云服务商和商业团体进行了广泛的游说之后，印尼政府表示将修订第 82 号政府条例，引入数据分类，并尽可能地减少数据本地化的要求。该条例将数据区分为战略性电子数据、高风险电子数据、低风险电子数据，根据不同的分类确定是否要设立本地数据中心和灾后恢复中心。①战略性电子数据(Strategic Electronic Data)：从战略上影响公共利益、公共服务、国家行政管理的连续性或国防及安全的数据。比如情报数据、人口数据或印尼公民的数据、国防和安全数据。战略性电子数据可以使用云计算进行管理、处理和存储，但云计算网络必须位于印尼境内，且不得将战略性电子数据传送、交换或复制到海外。②高风险电子数据（High-risk Electronic Data）：对电子数据所有者及其部门的利益影响有限的数据，比如与公司财务记录或业务数据有关的数据。高风险电子数据可以在海外进行处理和存储，但是必须能够在印尼进行以监督和执法为目的的访问和处理。③低风险电子数据（Low-risk Electronic Data）：战略性电子数据和高风险电子数据以外的电子数据，比如公司的人力资源数据或公共信息数据。低风险电子数据可以在海外处理和存储，但是必须能够在印尼进行以监督和执法为目的的访问和处理。印尼数据本地化政策尚处于制定过程中，其面临的质疑主要包括：一是对战略性电子数据的定义和范围并不清晰，无法明确哪些电子系统运营者需要设立本地数据中心；二是法案旨在加强数据相关执法，实施数据主权战略，但是反对者认为该法案不仅不能实现国家数据主权，还会打破平衡，更加有利益国际服务商，不利于印尼国内公司。

（7）印度：在融入全球化和促进本国数字经济发展之间寻求本地化中间路线

一是数据本地化政策以促进本国数字经济发展为前提。据印度科技企业界预测，印度数字经济规模到2025年将达到4万亿美元。[40] 印度政府对“数字印度”计划的拨款在2018-2019年度将达到480亿美元。印度正寻求将国家改造成一个连通的经济体，在机器人、人工智能、数字制造、大数据智能和量子通信等领域进行广泛的研究、培训和技能开发，确立印度在全球范围内知识和数字社会的地位。印度实施数据本地化的目的主要是为了促进本国的数据经济发展，通过落实数据本地化，进而实现数据价值的本地化。《印度电子商务国家政策框架草案》的前言部分明确提出，印度将会逐步推进数据本地化政策，要求建立数据中心。印度并不想实施严格的“数据保护主义”，但又不能放任数据的自由流动，因此其数据本地化策略一方面想要融入数据全球化的趋势，另一方面又想要刺激印度数字经济的发展。《电子商务框架草案》列出了一系列数据本地化的豁免情形，比如初创公司的数据传输，跨国企业内部数据传输，基于合同进行的数据传输等并不加以限制。

二是对个人数据实施分级分类，实施不同的数据本地化要求。在《个人数据保护法草案2018》中，印度将个人数据分为三种类型，一般个人数据、敏感个人数据和关键个人数据，针对三种数据类型，实施不同的数据本地化和跨境流动限制。首先对于一般个人数据和敏感个人数据，草案要求这两类数据应当在印度境内存储副本，可以跨境流动。同时，印度政府可以对一般个人数据进行清单化的豁免限制。其次，关键个人数据仅能存储在印度境内的服务器/数据中心，绝对禁止离境的。但是草案并没与具体说明“关键个人数据”的具体内涵和范围。

三是支付数据强制本地化存储，促进印度银行金融业发展。印度中央银行要求2018年10月15日之前，所有在印度的支付企业都要将数据强制性存储在印度本地。欧盟和美国政府和企业都提出了大量的反对意见，但是印度仍强势推进了支付数据的本地化规定。有研究认为，印度在此领域强制实施本地化与其银

[40]The Economic Times: Digital Economy Can Reach $4 Trillion in 4 Years: Tech Sector to Government, http://economictimes.indiatimes.com/news/economy/indicators/digital-economy-can-reach-4-trillion-in-4-years-tech-sector-to-government/articleshow/59188885.cms 访问时间：2018年12月26日。

行渗透率低下有密切关系。印度监管机构的目标不仅仅是出于执法便利要想访问这些数据，其目标是为了“控制”这些数据，以推动印度银行与金融业的发展。

（8）俄罗斯：通过数据本地化政策要求数据回流，以保护主义政策推动 IT 产业发展

一是数据本地化政策主要基于经济动机和执法动机。2006 年，俄罗斯通过了《联邦个人数据法》，但是该法并未得到严格实施。2014 年，俄罗斯通过了个人数据本地化规则，要求收集和处理俄罗斯公民个人数据的所有运营者使用位于俄罗斯境内的数据中心。法律并不限制个人数据出境，但是要求数据首次存储必须在俄罗斯境内的服务器上。俄罗斯数据本地化政策主要出于经济和执法两个目的。从经济方面来说，俄罗斯日益疲软的经济阻碍了其 IT 产业的发展。特别是近年来，美国和欧洲对其实施的经济制裁阻碍了俄罗斯数据产业的发展，导致俄罗斯的数据中心供过于求。[41]数据本地化法律的实施使俄罗斯快速发展起了大数据市场，并推动跨国企业兴建大量数据中心。[42]在执法层面，俄罗斯也希望通过数据本地化存储加强政府执法权和对数据的控制力，这一点也在其反恐法修正案“Yarovaya’s Law”上得以体现。该法要求在互联网上传播信息的组织者保留俄罗斯用户的互联网通信数据、用户本身的数据和某些用户活动的数据，在俄罗斯境内留存数据 6 个月，并应要求向俄罗斯当局披露。

二是划定数据自由流动范围，允许自由流向“108 号公约”缔约国和白名单国家。俄罗斯是“108 号公约”（《关于个人数据自动处理方面保护个人公约》）的缔约国，并于 2018 年 10 月签署了欧洲委员会对“108 号公约”修订后的议定书。108 号公约共有 53 个缔约国，俄罗斯《联邦数据保护法》承认加入“108 号公约”的国家为个人数据提供了充分的保护。此外，俄罗斯监管机构 Roskomnadzor 也确立了达到数据保护充分性水平的国家白名单，目前共有 23 个国家被列入白名单国家。[43]

[41] Alexey Danilyants, “State of the Russian Infrastructure Market,” Datacenter Dynamics, January 13, 2017.
[42] Alexey Danilyants, “State of the Russian Infrastructure Market,” Datacenter Dynamics, January 13, 2017.
[43] 截止 2017 年 6 月 15 日，共有 23 个国家被俄罗斯列入白名单国家，包括了安哥拉、阿根廷、澳大利亚、贝宁、加拿大、弗得角、智利、哥斯达黎加、加蓬、以色列、哈萨克斯坦、马来西亚、马里、墨西哥、蒙古、摩洛哥、新西兰、迷路、卡塔尔、新加坡、南非、韩国和突尼斯。

2. 数据跨境流动国际合作机制

（1）数据跨境流动的双边合作机制

当前，在联合国、WTO 等多边机制尚未提出各方可以接受的数据跨境流动规则的情形下，数据跨境流动的双边谈判成为确保电子商务和数字贸易正常开展的主要选择。双边谈判主要分为两种形式。

一是国家/地区的监管机构间达成数据保护充分性认定。这种形式以欧盟数据保护“充分性”认定（白名单国家）最为典型。以美欧隐私盾谈判为例，2016 年 2 月，欧盟委员会和美国商务部通过了美欧隐私盾协议，取代被欧洲法院（CJEU）判决无效的安全港协议(Safe Harbor Framework)，以支持跨大西洋商业目的的个人数据流动。欧盟希望通过“隐私盾协议”保护欧盟公民个人数据传输至美国后的基本权利，要求美国企业承担更多义务保护个人数据，并要求美国商务部和联邦贸易委员会承担更多的监督和执法责任。但是，美欧“隐私盾”协议的有效性一直受到欧洲法院的质疑，在双边贸易和政治互信发生危机时，欧洲法院很有可能会重新启动“隐私盾”协议的审查，可以说是欧盟与美国贸易谈判的重要砝码。

目前，欧洲委员会确认的白名单国家共有 13 个，包括安道尔，阿根廷，加拿大（商业组织），法罗群岛，根西岛，以色列，马恩岛，泽西岛，新西兰，瑞士，乌拉圭和美国（仅限于隐私盾框架）、日本。随着 GDPR 的实施，越来越多的国家通过制定或修订个人数据保护法，对接欧盟规则，试图与欧盟开展充分性认定谈判，以进入欧盟市场。目前，韩国正在与欧盟进行谈判，希望通过修订立法，赋予机构更多的独立性和执法权，以满足欧盟的要求。印度、智利、巴西等国家也正在制定或修改本国法律，以期加入与欧盟的数据保护“充分性”认定谈判。

二是在双边经贸协定的电子商务部分加入“数据自由流动”或“禁止数据本地化”等条款。据世界贸易研究所一项关于“双边贸易协定中的数据相关条款”的研究显示，自 2000 年起，全球共有 99 项双边协议中包含了至少一条电子商务和数据跨境流动的条款，其中有 72 项双边协议包含了电子商务和数据跨境流动

的章节。其研究分析了其中 62 项英文协议之后提出，美国、新加坡、澳大利亚、加拿大和欧盟是主要的规则制定者。[44]

美国、新加坡、日本等国家是数字跨境自由流动的积极倡导者，主张将数字跨境自由流动纳入双边贸易谈判。2012 年《韩美自由贸易协定》首次在电子商务章节中提出“数据跨境流动”规则，第 15.8 条规定，缔约方应尽最大努力履行义务，“避免对跨境电子信息流动设置或维持不必要的障碍”，同时承认“保护个人信息的重要性”。在 15.5 条在线消费者保护条款中，补充规定，缔约国认识到保护消费者免受欺诈的重要性，各国的消费者保护机构应当努力进行合作。该条款在当时虽然不具有强制执行力，但是在后续美国主导的 TPP 协定以及美国退出后的 CPTPP 中得以详细阐述。此外，新加坡与澳大利亚就《新加坡-澳大利亚自由贸易协定》达成修订协议，在该协定的电子商务一章中，几乎将 TPP 协定第 14 章“电子商务”内容完全纳入新修订协议之中。

欧盟通过 GDPR 设立了高标准的数据保护要求，可以说设置了相当程度的数字贸易技术壁垒。同时，欧盟将个人数据保护作为一项基本权利的立场与跨境服务贸易中的《服务贸易总协调定》（GATS）所规定的例外情形可能存在冲突，但是 2017 年，欧盟与日本达成的“日本-欧盟经济伙伴关系协定”可以看出双方在共同的经济利益背景下，仍可就数据跨境合作达成一致意见。

（2）数据跨境流动的多边合作机制

一是在多边贸易谈判中引入数据跨境自由流动条款。

WTO 是国际多边贸易规则的典型代表和集大成者。作为一个以自由贸易为价值追求的国际组织，WTO《服务贸易总协定》（即 GATS）的电信服务附件中规定“每一成员应保证任何其他成员的服务提供者可使用公共电信传输网络和服务在其境内或跨境传送信息，包括此类服务提供者的公司内部通信，以及使用在任何成员领土内的数据库所包含的或以机器可读形式存储的信息”。美国等国家认为，对跨境数据流动的限制行为其实是在设立国际贸易壁垒。反对意见则认为，

[44] World Trade Institute: Data flow-related provisions in preferential trade agreements, https://www.wti.org/media/filer_public/5f/92/5f920ca0-45b6-42e8-ad84-dae13c275c2a/wti_wp_03_2018_data_flow_related_provisions_in_ptas.pdf 访问时间：2018 年 12 月 26 日。

《服务贸易总协定》中规定了一般的例外条款，即隐私例外与安全例外。[45]近年来，随着信息通信技术的发展，数据跨境流动面临的形势发生了巨大的变化，但WTO 规则却没有随之更新。近年来，美国、日本、新加坡等国向WTO多次提交了推动电子商务谈判的提案，提出了禁止限制数据跨境流动的主张；以中国为代表的发展中国家以及欠发达国家，主张建立基于货物流动为主的跨境电子商务规则；而非洲、加勒比和太平洋岛国等相关国家，由于自身电信与互联网等基础设施较差，反对将数字贸易及跨境电子商务议题纳入多边贸易框架下讨论。[46]成员国，特别是主要大国之间的分歧难以弥合，目前来看，在WTO项下达成跨境数据流动规则的共识是比较困难的。

美国在2011年TPP第七轮谈判时，首次将次将强制性的跨境数据流动规制列入草案文本中。美国的主要目的是针对设置了数据本地化要求、对本地科技行业提供保护并阻止外国数据服务商进入本国市场的国家。TPP强制要求各方允许数据跨境流动，禁止数据本地化，允许为实现公共政策目标而采取或维持本地化措施，但不得以构成任意或不合理歧视的方式实施，或对国际贸易构成变相限制。此外，正在进行的《跨大西洋贸易与投资伙伴关系协定》（TTIP）和《服务贸易协定》（Trade in Service Agreement，TiSA）[47]谈判，也有谈判参与方提议，引入与TPP类似甚至相同的电子商务条款。当然，欧盟和美国在数据流动和个人隐私保护问题上持有不同观点，就此问题而言，双方可能提出不同诉求的谈判版本。取代北美自由贸易协定的美国-加拿大-墨西哥协议（USMCA）的数字贸易部分通过以下方式促进跨境数据流动：（1）禁止当地法律要求将数据存储在特定管辖区内（数据本地化），但有限的例外情况除外；（2）承认跨境隐私规则（CBPR）系统是美国、加拿大和墨西哥之间数据传输的有效数据隐私合规机制。再者，就中国参与的《区域综合经济伙伴关系协定》（Regional Comprehensive Economic

[45] 《服务贸易总协定》第十四条规定“本协定的规定不得解释为阻止任何成员采用或实施以下措施：1. 为保护公共道德或维护公共秩序而必需的；2. 为保护人类、动物或植物的生命或健康而必需的；3. 为确保服从与本协定规定不相抵触的包括与下述有关的法律和法规所必需的：（1）防止欺诈和欺骗做法的或处理服务合同违约情事的；（2）保护与个人资料的处理和散播有关的个人隐私以及保护个人记录和账户秘密的；（3）安全问题”。这两个例外也被业界称为个人信息保护例外和安全例外。

[46] 陈子媛：数字贸易战略比较与分析——以美国、欧盟、中国为例，https://mp.weixin.qq.com/s/h7WonTJAywQ0nyNtwBP8Uw，访问时间：2018年12月23日。

[47]服务贸易协定(TiSA)是包括欧盟和美国在内的23个WTO成员国提出的一项国际贸易条约。该协议旨在开放世界范围内的服务贸易，如银行业、医疗保健和运输业。

Partnership,RCEP）[48]而言，包括中国在内的谈判方也提出了在协定中纳入涉及跨境数据流动的条款。总的看来，跨境数据流动议题要在具有约束力的多边贸易条约中得到确认还需要漫长的谈判，以弥合各国利益诉求的差异。

二是弹性化的多边隐私与数据保护监管合作模式取得了一定的成效。

APEC 隐私框架是亚太地区第一个数据保护协同框架，并建立了一整套的落实措施，其跨境隐私规则体系（CBPR）是当前多边监管合作中较为成熟的机制。2004 年 9 月，亚太经合组织的 21 个部长签署了 APEC 隐私框架。该框架提出了 9 项指导性原则，帮助 APEC 成员国制定一致的个人信息保护规则。2015 年，APEC 发布了第二版的隐私框架。该框架构成了 APEC 跨境隐私规则（CBPR）这一区域性体系的基础。该体系旨在确保持续性的个人信息跨境自由流动，同时建立一个自愿性的问责机制，以切实保护个人信息和隐私。加入 CBPR 的评估标准包括：国内隐私法、隐私保护执法机构、信任标志（trust-mark）提供商、隐私法与 APEC 隐私框架的一致性等。据 2017 年 APEC 发布的一份《CBPRs 准备度报告》显示[49]，APEC 的 19 个成员国中大部分都已经加入或者有意愿/考虑加入 CBPRs，但是由于中国没有隐私保护法而被认为不具备加入 CBPRs 的条件（参见表 3）。[50]目前共有八个国家/地区参与了 CBPR，包括美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚和中国台湾。虽然 CBPR 规则体系具体实施效果还有待观察，但是据 Information Integrity Solutions 的研究显示，加入 CBPR 有助于企业向欧盟成员国数据保护监管机构申请“约束力企业规则”（Binding Corporate Rules）等数据跨境认证，同时日本也将企业获得 CBPR 的认证认为采用了“适当与合理的方式”处理数据。

[48]即由东盟十国发起，邀请中国、日本、韩国、澳大利亚、新西兰、印度共同参加（“10+6”），通过削减关税及非关税壁垒，建立 16 国统一市场的自由贸易协定。

[49] APEC Electronic Commerce Steering Group: Survey on the Readiness for Joining Cross Border Privacy Rules System – CBPRs, https://www.apec.org/Publications/2017/01/Survey-on-the-Readiness-for-Joining-Cross-Border-Privacy-Rules-System---CBPRs

[50] 从报告研究方法来看，该研究主要通过桌面调研实施，并向电子商务指导组（ECSG）的成员国发放了问卷，收到了 8 份回复。研究还调查了 5 家隐私认证服务商。针对中国只进行了桌面调研，且结论为不具备加入 CBPR 的条件。

表 3　APEC《CBPRs 准备度报告》（2017）

状态	经济体
加入	加拿大、日本、墨西哥、美国
计划加入	韩国、菲律宾
考虑中	中国香港、俄罗斯、新加坡、越南
不能加入	文莱、中国、印尼、巴布亚新几内亚、泰国
无计划加入	智利、马来西亚

APEC 的隐私框架还包括一项措施，即数据处理者隐私识别体系 Privacy Recognition for Processors System (PRP)，该体系采用与 CBPR 类似的问责制，但是与 CBPR 关注于数据控制者不同的是，PRP 关注于数据处理者。此外，APEC 还提出了一项跨境隐私执法安排（Cross-Border Privacy Enforcement Arrangement，CPEA）即鼓励数据保护监管机构合作的多边机制。[51]上述措施都是相辅相成的。例如，一个国家必须首先同意加入 CPEA 之后才能加入 CBPR。美国和新加坡已经加入了 APEC PRP 体系。

《关于个人数据自动处理方面保护个人公约》（108 号公约）（1981，2018）调和成员国在尊重隐私和数字自由流动方面的基本价值差异。在 OECD 隐私框架基础上，1981 年，欧洲委员会（Council of Europe）成员国签署了 108 号公约。该公约是首个寻求建立最低标准的区域间协议（例如承诺在其国内法中采取必要措施，不限制个人数据跨境流动），并开放非欧洲国家加入。[52]2018 年该公约出台更新协议，目前已有 28 个成员国签署该更新协议。虽然该公约需要签署国国内法进一步确认，但是俄罗斯在其国内数据保护法中确认该公约的效力，并将其签署国确认为满足充分性保护要求，这为该公约实际发挥效力提供了范例。

三是通过区域性的示范原则为成员国达成数据保护的共识提供指导。

[51] Cross-Border Privacy Rules System, “Glossary for the APEC CBPR system,” http://www.cbprs.org/GeneralPages/Glossary.aspx

[52]目前 108 号公约共有 52 个成员国，包括阿尔巴尼亚、安道尔、亚美尼亚、奥地利、阿塞拜疆、比利时、波斯尼亚和黑塞哥维那、保加利亚、克罗地亚、塞浦路斯、捷克、丹麦、爱沙尼亚、芬兰、法国、格鲁吉亚、德国、希腊、匈牙利、冰岛、爱尔兰、意大利、拉脱维亚、列支敦士登、立陶宛、卢森堡、马耳他、摩纳哥、黑山、荷兰、挪威、波兰、葡萄牙、摩尔多瓦共和国、罗马尼亚、俄罗斯、圣马力诺、塞尔维亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典、瑞士、马其顿、土耳其、乌克兰、英国、佛得角、墨西哥、塞内加尔、突尼斯、乌拉圭。

这类隐私和数据保护框架不具有强制约束力，但是在成员国制定国内数据保护法的过程中提供了原则指导，有助于在区域内形成数据保护原则共识，推动区域经贸合作和一体化发展。经合组织 OECD 隐私框架（1980，2013）是全球范围内首个隐私保护框架。OECD 隐私框架提出了如何在有效的隐私保护和个人数据自由流动之间达成最佳平衡，这是国际社会首次达成的共识。该框架致力于建立一套技术中立和灵活的官方指南，允许采用多种合规手段。包括东盟、APEC 框架和许多国家的监管和自我规制措施都以此为参考。东盟成员国经济社会发展水平不一，但是 2012 年，在数据保护方面达成了一项里程碑式的区域宣言。东盟部长会议通过了**《东盟数据保护框架》（ASEAN Framework on Personal Data Protection），**确立了一系列原则，指导成员国和区域层面的数据保护实践。[53]东盟数据保护框架旨在推动区域一体化与合作，推动东盟建设安全、可持续、转型升级的数字经济。要实现这一目标，加强个人数据保护，推动东盟成员国之间的数字贸易和信息流动是关键。东盟数据保护框架旨在灵活适应成员国在数据和隐私保护监管方面的不同的成熟度。在成员国层面适用该框架的经济体可以采取适用本国国情的例外措施，并且该框架不具有国内和国际的约束力。

3．全球数据跨境流动政策发展趋势

（1）中美科技冷战背景下，地缘政治因素对数据跨境流动政策的影响将进一步加大，以“国家安全”关切为核心的“重要敏感数据”将成为跨境流动限制重心。

斯诺登事件之后，网络领域的国家安全对国际贸易体系规则的破坏一直在全球蔓延，如数据本地化政策、网络安全审查，以及自主可控等理念在全球范围开始蔓延。随着中美在高科技领域的竞争有演化为科技冷战的趋势，以“国家安全”关切为核心的“重要敏感数据”也成为跨境流动限制重心。

特朗普上台后，美国先后出台了《国家安全战略》《301 报告》《外资投资风险审查现代化法案》《美国外国投资审查委员会改革》等一系列文件，对中国

[53] ASEAN, “Framework on Personal Data Protection” (16 November 2016), http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf.

高科技发展实施“战略围剿”。近期还针对中国 40 多家国有企业实施出口限制，加上原本对华设置的一系列高科技产品出口限制措施，美国已经从投资和出口双向对华设置了门槛。中美贸易战给美国出台上述法案和政策提供了团结的国内环境，两党和美国社会在这一问题上达成了高度共识。无论贸易战最终如何解决，美国在高科技领域对华的堤坝和防火墙已经建立起来。美国在前沿和基础技术领域对我国实施管控，限制大量技术数据和敏感个人数据的跨境转移，并通过长臂管辖和强大的情报和执法能力加以落实。与此同时，美国在此领域的强势主张势必影响其战略盟友对中国的技术转移和数据跨境流动策略，强化了以国家安全为主要考量的数据跨境流动政策的价值取向，这将进一步破坏既有的商业和贸易规则，阻碍数字贸易的全球化发展。

（2）各国数据跨境流动政策的选择极大地受制于本国数字经济产业竞争实力

除了国家安全和地缘政治因素的考量，各国对数据跨境流动政策路径的选择还极大地受制于本国产业能力和经济发展现状是否能够控制数据流向。基于不同的产业能力，目前各国政府在数据跨境流动策略选择上可以分为三种类型。

一种是以美国为代表的进取型策略。从上文全球数字经济发展格局和产业竞争态势分析来看，美国在数字经济产业竞争力方面处于全球领先地位，因此它的策略是积极主张数据自由流动，防止和消除数字贸易壁垒。它强调数字流动对经济增长的重要性，重视跨境自由流动数据的价值，数据本地化的成本，以及避免不必要的安全措施等。因此，美国在一系列贸易谈判中（TPP、TIPP、NAFTA）积极推进电子商务领域的数据自由流动。

第二种是以欧盟为代表的规制型策略。欧盟在数字经济领域的整体产业能力弱于美国和中国，虽然其认可许多自由主义的目标，但受制于产业竞争实力的现实，其更为依赖于规则制定能力，通过高水平的数据保护要求和强大的监管能力，加大外国企业数据跨境流动的成本，为本地区的数字产业发展构建保护壁垒。

第三种是以俄罗斯为代表的出境限制策略。由于本国数字经济产业竞争力不足，担忧数据流失损害本国产业发展和国家安全，俄罗斯、印尼、印度等国倾向

于采取对数据跨境流动实施限制和数据本地化存储等保护主义措施。虽然各国数据本地化的要求各有差别，但是这类措施很大程度上是作为一种市场准入壁垒加以运用，以保护本国产业特别是云计算等基础设施的发展。从结果来看，这也在一定程度上打破了美国云计算产业垄断的状况。

从产业能力的角度来说，我国数字经济发展仅次于美国，领先于欧洲和其他国家，但是我国在数据跨境流动政策上却趋于保守，更偏好数据本地化策略，与我国目前的位居第二的数字经济产业能力似乎并不相符。

（3）个人数据和重要敏感数据跨境流动规制基于不同的法益价值，采取不同的监管机制

从国际上主要国家数据跨境流动管理立法与实践来看，个人数据和重要敏感数据跨境流动威胁的法益有所不同，采取的监管机制也不一样。

个人数据跨境流动监管以企业自律为基础，政府监管为保障实施。个人数据跨境流动监管主旨以个人信息安全保护为出发点，以包括数据主体同意、数据主体权益保障、境内数据转出方与境外数据接收方的合同、数据接收方所在国家、地区数据保护充分性审查等多样化机制为抓手，保护个人信息出境流动安全。其监管措施主要包括以下两种：**一是由监管机构或监管机构认定的第三方机构为认证主体，采取实质性审查与形式审查相结合的方式进行评估认证，发挥行业协会等第三方监督与市场自律作用。**欧盟的“白名单制度”由欧盟第 31 工作组对申请国、地区数据主体权益保护情况、个人信息保护有效立法及执行情况、监管机构设立情况、国际公约加入情况等方面进行评估认证，对申请国、地区的个人信息保护水平进行认证。个人信息从欧盟境内向通过认证加入名单的国家、地区转移，免于审查。欧盟的《约束性公司规则》（BCR）规定由跨国集团公司向欧盟境内相关国家的数据保护机构提交申请，数据保护机构根据《约束性公司规则》要求，对其申请进行评估认证，认证通过后，该跨国集团组织可以在 BCR 要求范围内合法的进行数据出境，免于再次评估；而 GDPR 中提出的“行为准则”认证，则依靠行业协会提出，经由成员国监管机构或者欧盟数据保护委员认可后，可通过有约束力的承诺方式生效。此外，经认可的市场认证标志也可以作为数据

跨境转移的合法机制。APEC 数据隐私小组的 CBPR 体系也是由企业自愿申请，由参与国独立问责机构认证，认证通过后（需进行年度评估），可在 CBPR 规定范围内进行个人信息数据跨境转移；**二是合同干预制，欧盟、澳大利亚等政府部门制定并推行数据出境合同范本，合同中明确相关主体义务，从而约束数据接收方行为，对个人信息出境流动实现管理。**以欧盟为例，根据由欧盟委员会以《数据保护指令》为法律依据，参考各国数据保护机构意见制定，且经过欧盟第 31 工作组认定采纳，分别于 2001 年、2004 年、2010 年颁布的《标准合同》条款相关规定，企业之间签订出境数据流动处理合同如包含格式合同的条款，则可将欧盟内个人信息转移至欧盟境外不具备充足数据保护水平的国家。两种监管模式可并行采用，以企业自律为基础，政府审查为保障。

重要敏感数据采取一般性禁止，分级分类审查出境的监管模式。一是采取禁止出境和限制出境分级监管。根据数据属性、风险程度，并结合本国国情和政治文化差异，世界各国普遍对政府、银行、金融、征信、健康、税收等关键基础设施和重要行业/领域数据实施出境限制措施，包括完全禁止出境、选择性禁止、有条件出境等数据出境管理措施。如法国规定税收、管理和商业开发的数据需要本地存储；澳大利亚禁止将健康记录转移到澳大利亚以外的地方；印度规定支付数据禁止出境；美国规定属于安全分类的数据不能存储在任何连公共云数据库中，且要求存储该类数据的物理服务器分布在美国境内，只有美国公民可以访问，对于非保密的信息，政府要进行安全风险评估后外包。**二是采取一事一议的行政审查监管。**在特定类型的重要数据出境前，数据输出方向相关政府部门提交出境申报材料，政府部门对相应出境活动进行许可审查，通过后方可出境。如美国商务部对进行境外存储和处理的受管制技术是否取得出口许可进行审查；韩国对地图数据建立出境申请协商机制，由国土地理信息院、未来创造科学部、外交部等部门联合评估风险，判断是否允许出境。

（4）大国扩张性的数据主权战略加剧了管辖权冲突

随着数据成为国家重要战略资源，对数据的积累、加工和治理成为决定国家经济命脉的重要因素。对数据资源的渴求反映在主要国家扩张性的数据主权战略之中，在立法层面体现为管辖权的扩张。

美国、欧盟的数据主权战略以“攻”为主，通过“长臂管辖”扩张其跨境数据执法权。比如，美国《澄清域外合法使用数据法案》赋予美国执法机关对美国企业“控制”的数据，不论其在美国还是在境外都享有主权，同时对美国人的数据以及在美国境内的个人数据，外国政府必须经过美国国内司法程序。这种长臂管辖，使美国的数据主权扩展至美国企业所在的全球市场。欧盟的 GDPR 也同样适用于所有针对欧盟用户提供产品和服务的企业，不管该企业是否位于欧盟境内。美欧的长臂管辖无疑将加大与数据存储地国家的主权冲突。[54]

相对来说，**中国、俄罗斯等国的数据主权战略以“守”为主，通过数据本地化**解决法律适用和本地执法问题。此外，传统国家间的司法协助条约（MLAT）进展缓慢，也间接鼓励着各国政府更愿意选择数据本地化政策，数据存储在本地至少有执法便利，在法律适用上本身也是一个强有力的抗辩。

互联网是全球性的，然而立法与监管却是本地的。长期以来，互联网的管辖适用问题一直就未得到解决。当前，数据主权扩张，导致各国法律适用连接点增多，管辖冲突给跨境服务企业带来难以解决的义务冲突问题。

（5）大国战略互信成为跨境数据流动的双边/多边合作体系建立的基础，当前数据跨境流动的朋友圈主要围绕美欧日等西方国家来划定

大国是全球网络空间中至关重要的行为体，对基础设施的有效管辖，干涉数据全生命周期行为的强大能力，以及在建构数据跨境流动新模式方面的战略规划和政策执行能力，决定了其拥有无法替代的特殊优势。大国战略互信，是数据跨境流动有序实现的必要前提。缺乏信任的大国，会倾向于在网络空间采取限制性的行动，对数据流动形成事实上的壁垒，而且会出现竞争性的壁垒升级与政策复

[54] 许可：数据主权视野中的 CLOUD 法案，载《中国信息安全》2018 年 4 期。

制。不同于已经形成共识的统一国际贸易规则，由于各国在跨境数据流动问题上存在法律文化和价值认同的差异，很难在短期内形成共识从而达成全球协议。

从当前国家间数据跨境流动合作建立的多边和双边体系来看，全球贸易体系下的多边规则共识难度较大，大多数合作体系是从双边谈判开始，逐步扩大朋友圈。由于涉及国家安全、产业竞争力等复杂因素，数据跨境流动信任大多建立在长期的政治盟友、经贸伙伴以及具有相同价值目标的基础上（参见图 6）。最为典型的是以美国为主导的“五眼联盟”[55]情报共享体系，有着长期的、紧密的数据共享合作关系。

美国在个人数据跨境流动领域，一直推动数据不受限制地自由流动的理念和规则，以破除美国企业进入其他国家市场的壁垒。在韩美自由贸易协定首次提出之后，美国与贸易伙伴在 TPP、TIPP、美-加-墨自由贸易协定、CBPR 等协定和机制中都积极推动这一理念，主导数据跨境领域的话语权。以 APEC 的 CBPR 机制为例，其实质是要求以美国提出的较低水平的数据保护标准为基础，实现数据跨境自由流动。目前，美国正在努力争取其传统盟友加入 CBPR，包括加拿大、墨西哥、日本、韩国、新加坡、澳大利亚等，意图扩大 CBPR 参与国范围，形成网络效应，以真正实现该机制在数据跨境中的实际效果。

欧盟在长达半个世纪的时间里为建构全球跨境数据流动治理的框架提供了极具参考价值的蓝本与标准，并在后续以开放的姿态接纳了不同的规制体系。欧盟规则的溢出效应积极推动了世界范围内法律体系的趋同，通过充分性认定考虑的因素，输出欧盟的价值和目标（人权保护、独立监管机构等）。但是欧盟对维系基本权利价值的关注，在某种程度上也禁锢了欧盟在内政外交当中的选择，在数据跨境流动合作机制的谈判上相对来说进展缓慢。比如，虽然美国是欧盟最大的贸易伙伴，但是在“隐私盾”协议执行过程中，一直面临欧洲法院对其能否保护欧洲公民基本人权的质疑。在白名单国家的谈判中，欧盟对基本权利保护、反对政府滥用监控权、监管机构独立性等方面的追求也阻碍了其加快数据跨境流动合作的谈判进程。

[55] 五眼联盟国家包括美国、英国、澳大利亚、新西兰和加拿大。

日本一直是多边和双边数据跨境自由流动的倡导者。一方面，日本积极跟随美国数据跨境自由流动的政策主张，积极参与美国为主导的 TPP 和 APEC 的 CBPR 规则体系，并且在美国退出 TPP 后成为主导“全面且先进的跨太平洋伙伴关系协定”（CPTPP）的主要成员国[56]。日本作为 CBPR 的成员国，通过建立认证制度，为企业遵循 CBPR 规则实施跨境数据传输提供保障。另一方面，日本又积极对接欧盟的数据保护规则，并与欧盟就个人数据保护“充分性保护”达成互认。此外，据日本媒体透露，日本政府将在 2019 年 6 月的 G20 峰会之前公布“日本-美国-欧盟”三方数据跨境流通规则，建立三国“数据流通圈”，并严格限制向框架外缺乏数据保护“充分性”水平的国家转移数据。日本在高标准的数据保护和数据跨境自由流动之间积极探索，致力于构建一个开放且安全的数据自由流动市场。

俄罗斯目前主要通过“充分性认定”建立白名单国家，形成数据跨境流动合作机制。目前已与 23 个国家达成“充分性认定”协议。《108 号公约》成员国虽然数量众多，但是该公约作为一项人权性质公约，致力于在成员国内就相关基本人权达成共识，其效力有待成员国国内立法机构批准，难以成为有强制约束力的数据跨境合作安排。

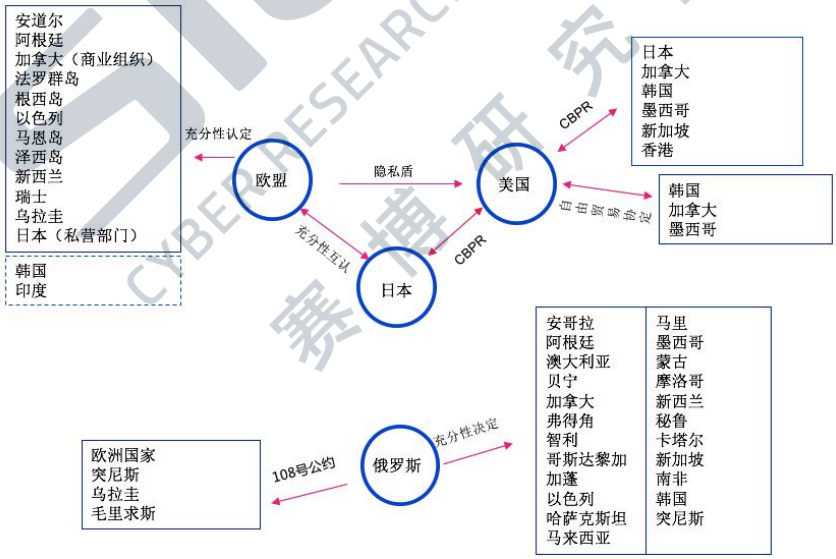

图 6 美国、欧盟、俄罗斯的数据跨境流动合作

（本课题组绘制）

[56] 其前身即为“跨太平洋伙伴关系”。

四、我国数据跨境流动管理的战略分析

（一）我国数据跨境流动管理政策现状

目前，我国数据跨境流动管理制度正在制定完善过程之中。《网络安全法》对关键信息基础设施数据提出了出境安全评估要求。在此之前，部分行业部门通过规章或规范性文件提出了数据本地化存储要求。

一是国家立法构建关键信息基础设施数据出境管理框架。《网络安全法》第 37 条就关键信息基础设施数据出境提出了安全评估要求，对安全评估的责任主体、管理对象、管理要求等内容进行了限定，从而确立了我国数据出境安全管理框架。为了落实《网络安全法》第 37 条规定，国家网信办 2018 年公布了《个人信息和重要数据出境安全评估办法》（征求意见稿），提出了建立“主管部门评估-网络运营者自评估”两级评估体系，扩大数据出境评估范围，加强数据出境安全风险管理。同时，参考美国受管控非密数据列表，以对国家安全、社会公共利益和公民个人权益危害程度为判定原则，按照国家行业和信息主题分类，拟定“重要数据”判定指南（具体行业分类见表 4 数据出境行业分类（征求意见稿）），通过《数据出境安全评估指南》（征求意见稿），细化安全评估启动条件、实施流程、审查内容、结果判定等配套规范要求。

表 4 数据出境行业分类（征求意见稿）

教育	水利	煤炭
通信（电信网、互联网）	医疗卫生	国防军工
钢铁	银行	地理测绘
有色	广播电视	铁路
化工	食品药品	民航
装备制造	证券	邮政
环境保护	保险	税收
民用核设施	电力	执法
公路	石油天然气	
农业	石化	

（来源《数据出境安全评估指南》（征求意见稿））

二是行业内重要数据率先开展数据出境管理实践。前期的行业管理实践主要集中于关键信息基础设施所处重要行业领域、信息通信服务领域。主要规定了对数据存储限定是否必须在境内、数据留存时间的最短时限以及对数据出境禁止性规定。如在关键信息基础设施领域中的金融行业方面，中国人民银行发布《关于银行业金融机构做好个人金融信息保护工作的通知》，明确规定“在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。”在信息通信服务领域中的网络约车行业方面，交通运输部、工信部等 7 部委共同颁布《网络预约出租汽车经营服务管理暂行办法》，规定“网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流。”《人口健康信息管理办法（试行）》禁止在境外存储人口健康信息；《保险公司开业验收指引》要求保险公司业务数据、财务数据等重要数据应存放在中国境内；《征信管理条例》规定征信机构对在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。此外，《地图管理条例》《网络出版服务管理规定》等都提出了不同程度的数据本地化要求。

当前数据本地化要求的管理实践问题在于，多数行业主管部门为了便于行业管理，针对行业内部分敏感数据，对其出境进行限制性管理，但并未根据出境具体情形做出细化要求，数据本地存储以后是否允许出境或者出境的条件为何往往并不清楚，对相关管理主体很难形成规范性指引。

（二）我国跨境数据流动环境和能力 SWOT 分析

制定跨境数据流动政策是一项需要综合考虑各种因素的复杂决策。本报告以 SWOT 方法分析探讨我国在跨境数据流动中面临的机遇、威胁、优势和劣势，以提出全面有效的数据跨境流动治理策略。

1. 机遇

（1）美国经济政策转向为中国参与构建数字经济贸易规则提供机遇窗口

特朗普上任后推出的“全球收缩”经贸保护政策和“美国优先”国内经济政策对全球经济秩序产生重大影响。在全球经济萎靡不振，贸易增长乏力和政治不稳定叠加的背景下，贸易保护成为特朗普对外经济政策的主要议题。美国政府退出了 TPP 等贸易谈判，放弃既有的多边贸易机制，试图逆转经济全球化。相比美国提出“回到美国”的政策，收缩在国际公共产品领域的责任和义务，中国则成为唯一一个仍在全力推动全球化的超级大国。美国退出 TPP 和全球战略收缩将可能为中国的“一带一路”倡议腾出空间，美国退出后在某些领域形成力量真空，成为中国参与构建数字经济贸易规则的机遇窗口。中国可以利用此基于，建立新的、中国主导的多边机制，重构全球贸易和数据治理体系。比如中国正在积极参与推进的“区域全面经济伙伴关系协定”（RCEP），通过推进区域投资贸易自由化、促进区域经济一体化，在其中发挥大国的影响力。

（2）新一轮技术变革改变数据流动逻辑为我国提升全球产业价值链中的地位提供机遇

5G、物联网、人工智能等新一轮技术变革命正将我们带入一个万物感知、万物互联、万物智能的世界。在迈向智能世界的过程中，泛在感知、高速联接、共享智能将带来前所未见的成长和价值，数据成为用之不竭的资源，智能主导数据价值的转换和输出，联接承载海量数据交互和智能价值创造过程。

智能世界的到来，一方面将改变数据流动的底层逻辑，另一方面将使全球产业图景发生革命性的变化[57]。首先，物联网、边缘计算等技术的出现，促使企业将重要 IT 资源转移到现场应用端以及数据源的网络边缘，冲击原有的后端数据中心汇集计算模式。这类新技术引发业务模式的变化，将深刻改变数据流动的底层逻辑，影响数据在全球的流动和分布。

[57] 华为：GIV 2025：打开智能世界产业版图，
https://e.huawei.com/cn/publications/cn/ict_insights/201805151128/view/201806121143

其次，数据的开放、流动和共享将颠覆传统工业时代的商业形态和产业边界，推动大规模跨产业协作和创新，衍生出包括平台经济、共享经济等经济模式，激活人类的创新力和生产力。[58]在数字经济发展推动下，国际分工和产业范式得以重构，竞争格局焕然一新。每个产业都依赖数据及其产生的全球数据流。通过遍布世界的数据基础设施(比如云计算),全球连通性使跨境经济活动成为了可能,从而让个人、初创公司和小型企业都能进入全球市场。其核心关键是,数据的自由流动降低了交易成本,突破了距离的限制,也提高了组织效率。互联互通加速了思想的传播,使世界各地的用户能够利用新的研究和技术打造新的企业。

我国在5G、物联网、大数据、云计算、人工智能等领域积累了良好的创新能力和技术优势，有机会通过创新实现跃升迭代，提升我国在全球产业价值链中的地位。因此，我国构建跨境数据流动规则应当在新技术变革带来产业升级的战略背景下予以考量。

（3）我国进一步扩大开放与“一带一路”倡议，推动合作共赢的“新型全球化战略”

根据国家统计局发布的信息，2018年中国大陆对外货物贸易总额达到了4.62万亿美元，再次超过美国成为全球最大的贸易国。[59]习近平主席在“庆祝改革开放40周年大会上的讲话”中指出，“开放带来进步，封闭必然落后”。扩大开放意味着将有更多数据跨越国境进行流动，包括境内外资企业输出数据、境内中资企业输出数据、境外中资企业输入数据等各种情形。同时，我国“一带一路”倡议进入全面合作阶段，投资和贸易持续深化，双边及多边合作机制的完善推动我国“新型全球化”战略的实现。中国的“新型全球化战略”不是构筑排他性的贸易保护圈子，而是实现真正的互利共赢，实现全球的共同发展。这一理念得到了多数发展中国家的高度认同。目前，“一带一路”相关投资从传统的基础设施项目拓宽至贸易、互联网等数据密集型行业；2018年中国与“一带一路”沿线国家货物贸易进出口总额1.3万亿美元，同比增长16.3%，与格鲁吉亚、马

[58] 惠志斌、张衡：面向数据经济的跨境数据流动管理研究，载《社会科学》2016年第8期。
[59] 新华社：超30万亿元！我国2018年外贸进出口总值创历史新高，http://www.gov.cn/shuju/2019-01/14/content_5357701.htm

尔代夫签署自贸协定，与摩尔多瓦、毛里求斯正式启动自贸协定谈判。此外，中国还积极促进《区域全面经济伙伴关系》（RCEP）的谈判，促进中日韩自贸区的谈判。上海合作组织[60]也从原来六个成员变为八个。中国还与中东欧国家展开中国-中东欧“1+16“经济贸易合作，与非洲国家和拉美国家开展经济贸易合作。伴随大量双边和多边经贸合作协议的签订,以及与一带一路国家贸易关系的紧密发展，带动了双边和多边的数据交互流动的持续上升。

2. 威胁

（1）各国围绕数据主权的战略博弈呈现泛化趋势

全球化对各国经济社会发展起到了明显的促进作用,但同时也对民族国家主权管辖产生了现实的解构效应。德国著名社会学家乌尔里希·贝克曾提出：“全球化将导致民族国家、民族国家主权被跨国活动主体、被它们的权力机会、方针取向、认同与网络挖掉基础”。[61]当前，数据全球化趋势不可避免地引发了诸多国家对数据主权（Data Sovereignty）的担忧，尤其是在“2013 年棱镜门”和“2015 年美欧安全港废止”等重大事件的触发下，越来越多的国家对数据跨境流动采取规制措施。

相对领土、人口等其他类型的国家主权管辖对象，数据主权的实现又具有复杂性。**首先，数据天然的流动性导致各国的数据主权管辖必然需要与其他国家进行权利交换与权力妥协。**如果单方面强调对本国数据资源的绝对控制最终将导致数据流动停滞和与网络空间分裂，最终危害本国数据主权；**其次，当前数据主权博弈从个人权利和产业竞争泛化到国家安全和公共安全领域，**政治集团、行业巨头、人权组织等纷纷介入这一领域，从不同的角度给跨境数据流动施加非技术性的要求，使跨境数据流动问题变得异常复杂。**第三，国际法规则缺失和各国法律差异/博弈导致数据主权管辖边界面临重合与冲突。**例如美国通过“云法案”赋予执法机构获取在美经营业务的跨国公司分布在全球数据中心的数据的权力，同时又以“适格外国政府”（qualifying foreign governments）为条件，赋予

[60] 上海合作组织：http://chn.sectsco.org/

[61] [德]乌尔里希·贝克，《什么是全球化——全球主义的曲解:应对全球化》，常和芳译，上海：华东师范大学出版社，2008 年 11 月。

盟友向美国境内的组织直接发出调取数据命令的权限。我国《国际刑事司法协助法》仅仅阻断了直接来自外国政府对境内的机构、组织和个人控制的数据的刑事司法管辖权，且两国意识形态具有显著差异性的情况下，我国目前很难通过美国政府在“云法案”中提出的审查“适格外国政府”的人权、法治和数据自由流动的标准。在此情况下，在中美两国经营业务的企业可能面临两国执法管辖难以调和的冲突困境。**第四，各国数据主权管辖能力具有不对称性。**技术发展、商业创新导致数据性质和权属关系的模糊，海量、异构、实时数据的跨境流动削弱数据主权的管辖能力，美国在网络空间基础资源和技术产业的主导地位对各国数据主权保障能力形成现实压制，即便斯诺登事件之后各国高度重视数据安全技术和产业发展，但全球数据主权保障能力不平衡的现状依然明显。

（2）以美国为首的西方发达国家贸易保护主义抬头阻碍数据跨境流动

近年来，金砖国家等新兴大国群体性崛起势头明显，美国、西欧国家在全球“大蛋糕”中所占的份额相对缩小，且社会内部矛盾趋于复杂。同时，以中国为代表的新兴大国的科技水平也在急追猛赶，使西方发达国家担心无法安居于价值链高端获得超额利润。这种战略焦虑的结果是美国加强了新兴技术出口管制和外国投资审查。美国在对华出口上奉行“推定否定”政策，即原则上不允许出口，并将众多中国公司列入出口管制实体清单，这将阻碍中国以往通过正常经贸活动获得有价值的技术数据。

欧盟也于 2018 年 11 月通过了《外国直接投资审查框架协议》，德国、法国、意大利等国尤其主张对中国在欧洲基础设施和技术领域的掠夺性投资实施限制。[62]此外，欧盟正在为避免沦落至全球政治经济的边缘地位而寻求更高一体化水平，[63]通过制定（GDPR）、《非个人数据在欧盟境内自由流动框架条例》消除内部市场数据流动的障碍，同时通过高标准的数据保护要求，设置新的市场准入壁垒，以突破当前产业竞争力不足的困境。欧盟高标准的数据保护要求，也提高了中国企业获取欧盟公民数据的门槛。2015 年欧洲议会公民权利、正义和内政事务委

[62] 陆克：欧盟立法审查外国投资意在防范中国，载《金融时报》2018 年 11 月 29 日。
[63] 张宇燕：世界格局在 2018 年的多重变奏，载《全球政治与安全报告（2019）》，社会科学文献出版社 2018 年 12 月版。

员会（LIBE）一项名为“中国个人数据保护管理体制 ”的研究结论认为，中国立法中缺少数据保护的通行原则、没有数据保护监管机构、人权法治状况不佳。因此，中国当前的制度缺少对接欧盟数据保护规则所要求的立法、执法、人权、法治等关键要素，欧盟和中国之间缺少个人数据保护问题的共同立场。[64]由此可见，短期之内，我国很难通过谈判实现与欧盟的数据自由流动。

（3）数据安全威胁泛化造成数据跨境流动风险复杂化

数据跨境流动场景下，数据安全面临更为复杂的威胁。一方面是各国数据保护标准不统一，数据从高水平保护国家流入低水平保护国家，使流出国用户的权利在数据跨境转移后难以得到保障，执法和救济存在障碍；另一方面，各种国家关键信息基础设施和重要机构承载的庞大的数据信息具有重大的国家安全战略价值，如由信息网络系统所控制的石油和天然气管道、水、电力、交通、银行、金融、军事等领域的大数据安全已经上升为国家安全极为关键的组成部分。这些领域的大量敏感数据在跨境传输中存在不可控的风险，需要国家层面加强数据安全能力和监管能力。

3. 优势

（1）我国数字经济全球竞争力持续提升，大量企业的全球化拓展步伐在加速

纵观当前全球数字经济的发展态势，以美国和中国为核心的基本格局已经逐步形成，在互联网行业、人工智能产业等数字经济的重点领域，中美在产业体量、人才集聚、技术创新、影响力等方面均表现出较强的竞争优势。中国在多个领域的研发实力已处于世界领先水平，包括量子通信在内的一批成果获得国际认可。目前，我国高科技行业正处于向产业价值链中的高端攀升的关键期。华为、阿里巴巴、腾讯等一批高新技术企业走出国门成为真正意义上的跨国企业，通过创新的技术、产品和服务加速拓展全球市场；一大批中小型的科技企业也依托网络进

[64] LIBE Committee: The Data Protection Regime in China, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf

军海外。中国高科技企业一方面向世界输出技术、产品和商业模式，另一方面还通过在信息技术、计算机服务和软件业领域的海外投资并购拓展全球版图。中国数字经济全球竞争力的提升和高科技企业加速全球化布局，伴随而来的是中国企业对全球数据控制力的提升，吸引全球数据向中国汇聚。

（2）制度与监管体系的完善有助于改善我国数据保护不力的国家形象

我国数据保护制度不健全长期受到国际社会的批判。无论是欧盟还是 APEC 的研究报告，都认为我国个人数据保护程度无法达到充分的保护水平，因此无法开展数据跨境的国际合作。随着《网络安全法》《信息安全技术 信息系统安全等级保护基本要求》《信息安全技术 个人信息安全规范》等法律和标准的实施，《个人数据保护法》《数据安全法》纳入立法计划，我国个人信息保护法律制度有望在近期得以完善。在监管层面，国家网信办、公安部等监管部门也针对互联网服务实施了包括隐私政策评审、对不当数据处理行为进行约谈、对侵犯公民个人信息违法犯罪活动实施专项整治，落实信息安全等级保护制度等措施。制度与监管体系的完善，有助于我国塑造良好的数据保护的国家形象，为我国开展数据跨境流动的国际合作奠定基础。

（3）部分龙头企业积极提升数据安全管理能力，推动建立行业和国际标准

除了提升数据保护合规能力以外，我国互联网龙头企业在企业自律和数据安全管理能力建设方面进行了创新性的实践。比如阿里巴巴根据多年的数据安全实践经验，提出了《数据安全能力成熟度模型》(DSMM)，围绕数据生命周期开展 DSMM 评估认证工作，在行业内进行推广应用。该成熟度模型还报批成为国家标准，在此基础上，阿里巴巴还牵头制定了 ITU-T、ISO 的相关国际标准，将中国数据安全技术和管理经验推广至全球。阿里云还与 Oracle，IBM，SAP 和 Salesforce 等国际科技企业合作，参与制定欧洲云计算服务商行为准则(Code of Conduct for Cloud Service Providers (EU Cloud CoC))，并有望得到欧盟数据保护监管部门的认证。此外，蚂蚁金服、腾讯等都出台了各自的“隐私保护白皮书”，通过建立全生命周期的数据管理制度和多维度的隐私保护机制，确立

最佳实践，规范个人数据保护流程。互联网龙头企业的数据安全管理能力向世界先进水平看齐，并主导国内、国际标准的建立，不仅提升了自身在跨国经营活动中的合规能力和竞争力，也拓展了我国数据跨境流动合作的空间，增强了其他国家开放数据流入我国的信任和信心。

（4）我国数据经济产业增长空间大，优势明显

当前，我国数据经济产业展现出良好的发展态势，据中国信息通信研究院发布的《大数据白皮书（2018）》显示，2017 年，我国大数据产业规模达 4700 亿元，同比增长 30.6%，大数据与实体经济融合提速。[65]数据资源方面，我国在数据资源量和丰富程度上具有优势。中国拥有全球第一的人口基数、互联网用户数和移动互联网用户数，网络化、智能化、平台化的采购、生产、营销等开始受到越来越多的中国企业关注，中国已成为名副其实的“世界数据中心”。[66]在数据应用方面，我国企业也取得了显著成效。比如阿里巴巴的 DT（Data Technology）战略、腾讯的“大数据连接的未来”、百度的“中国大脑”战略都围绕数据驱动进行布局。在互联网产业 020 的趋势下，互联网企业逐渐将业务延伸到金融、保险、旅游、健康、教育、交通服务等多个行业领域，这极大地丰富了互联网企业的数据来源，促进了其数据分析技术的发展，进一步奠定了我国大型互联网企业在大数据领域的地位，同时也扩展了大数据分析在诸多行业的应用。此外，从中央到地方陆续出台一系列大数据产业支持政策，为大数据产业的发展提供各种财政、资金、资源等的保障，助推大数据产业发展，推动中国经济向全球竞争力的新阶段过渡。

[65]中国信息通信研究院：《大数据白皮书（2018）》，http://www.cac.gov.cn/wxb_pdf/baipishu/dashuju020180418587931723585.pdf, 访问时间：2019 年 1 月 14 日。
[66]茶洪旺，郑婷婷：中国大数据产业发展研究，载《中州学刊》2018 年第 4 期。

4. 劣势

（1）数据跨境流动管理的战略不清晰、制度不完善

当前，出于国家安全、执法便利甚至是“懒政”思路的考虑，我国政策制定倾向于以“本地化存储”为前提设计数据跨境流动顶层制度，未能正视我国数字经济全球竞争力已位居世界第二的客观现实，以及未能从推动实现我国企业全球化发展的战略目标进行考量，甚至未能为数字贸易活动正常开展提供多样化的机制选择。这种战略选择将带来我国数字贸易的“闭关锁国”政策。

立法者已经意识到事前“许可”的监管机制无法与全球化的数字经济发展相适应，因此引入了风险评估作为事中、事后监管的思路，但是立法者的数据本地化偏好仍将带来诸多问题。首先，将个人数据与重要数据都纳入出境安全评估的范围，将大量原本基于业务模式和市场经营活动需要开展的数据跨境活动都纳入监管范围，将极大地影响企业运营成本和经营效率，甚至影响企业跨境商业活动的正常开展，大大影响我国互联网企业的国际竞争力。其次，个人数据和重要数据涉及两种不同的法益，面临的安全风险也并不相同，在数据跨境监管手段的选择上也应有所区分，并非仅有本地化存储这一单一路径；第三，在监管者提出了数据本地化要求，但未禁止数据出境的场景中，我国还缺乏相应的程序性规定，明确数据出境的必要条件；第四，重要数据的定义不清晰，数据跨境流动评估办法还很不成熟，企业难以把握，效率和效果上也难以适应今天的实际情况。

（2）“数据本地化”偏好不利于提升我国参与全球规则的能力和实现长臂执法能力

《个人信息和重要数据出境安全评估办法（征求意见稿）》第十五条提出，“我国政府与其他国家、地区签署的关于数据出境的协议，按照协议的规定执行。”目前，我国数字经济发展已处于全球领先地位，但是与数字经济发展水平相比，我国在数据跨境流动的国际合作方面仍处于起步阶段。2016 年，我国向 WTO 总理事会提交了一份涉及电子商务相关议题的文件。虽然并没有签署 2017 年 12 月阿根廷召开的 WTO 成员部长级会议上 71 个 WTO 成员的声明，但参与了在日内

瓦进行的第四轮讨论。但是我国目前国内“数据本地化”的政策发展趋势，很难支持 WTO 声明所主张的“谋求禁止数据本地化”协定。

此外，“数据本地化”偏好也导致目前我国很难参与欧盟和美国主导的双边/多边机制。欧盟在数字经济发展中暂时落后，期待通过 GDPR 提出的高保护标准和数据向欧盟境外流动的限制措施构建面向非欧盟国家的贸易壁垒。欧盟和美国的“隐私盾协议”谈判就存在诸多波折，并且一直面临欧洲法院重新审查的威胁。中国的“数据本地化”政策也将会对我国与欧盟的谈判造成阻碍。而由美国主导的 APEC“CBPR”体系，强调的是国家间数据的自由流动，与我国当前的本地化政策相悖。同时，目前来看，APEC 也未显示出与中国积极协商的意向。2017 年 APEC 发布的《CBPR 准备度报告》更提出，由于中国尚未制定隐私保护法，因此没有资格加入 CBPRs。[67]

与此同时，自 2018 年年初以来，美国先后采取制裁中兴、宣布贸易战、纠集盟国禁用华为 5G 设备、要求盟友加拿大逮捕华为 CFO 孟晚舟等行动，凸显出地缘政治环境恶化将对我国数字经济发展产生消极影响。随着美国加强在先进科技领域遏制中国的力度，我国跨境数据流动的国际合作将面临更大的挑战。

（3）数据保护重点尚未形成共识，全社会数据治理能力还不均衡

我国数据保护监管尚处于起步阶段，除了重点打击数据黑灰产之外，明确数据保护的重点，防止影响企业正常经营活动中的数据使用，还有待于形成社会共识。此外，我国大部分政府机关和企事业单位的数据治理能力还存在很大的缺失。违规收集用户数据、缺乏必要的数据安全防护措施、滥用甚至贩卖用户数据、大规模数据泄露等等严重侵犯用户隐私和数据权利的事件屡见不鲜。有些组织缺乏基本的数据保护意识，也缺乏专业的数据管理人才；有些组织对数据安全有了初步的认识，但还缺乏良好的数据治理能力，无法将其转化为竞争优势；有些企业认识到了数据资源的财产价值，却滥用技术能力，为了获得商业利益而侵犯用户隐私。数据保护重点尚未形成共识，全社会数据治理能力不均衡，严重影响了我国整体数据保护能力的提升。

[67] APEC：Survey on the Readiness for Joining Cross Border Privacy Rules System – CBPRs，January 2017.

五、构建我国数据跨境流动管理体系

1.战略目标与原则

当前，在我国持续推动对外开放和“一带一路”倡议，积极推进贸易和投资自由化的大背景下，我国数字经济产业竞争力不断上升，大批科技企业开展了全球化布局；新一轮的技术变革为我国企业弯道超车，占领全球产业价值链的高端位置提供了战略机遇。与此同时，地缘政治环境呈现恶化趋势，作为战略竞争对手，我国未来将面临以美国为首的西方发达国家的科技围堵和数据封锁。

在这样的发展趋势下，构建数据跨境流动管理体系应当服务于我国建设“网络强国”的战略目标，服务于我国整体经济发展的战略需要。通过把握全球产业竞争和政策演进的趋势，认清我国当前产业能力和发展目标，明确我国国家安全和网络安全的“红线”，选择适当的数据跨境国际合作伙伴，建立确保我国数字经济全球竞争力的数据跨境流动互认区域，实现经济发展、国家安全、公民权益等多个价值目标的有机协同，真正推动我国数字经济的发展，保障数据主权。

我国构建数据跨境流动管理体系，应当遵循以下原则：

一是鼓励去政治化的有序流动原则。具体来说，数据是网络空间信息内容的基本载体和生产活动的基本材料，互联网的本质就是数据的流动。通过互联网消除信息不对称、市场壁垒，发现聚合数据的价值等均离不开数据的流动，可以说数据流动是全球数字经济持续发展的根本基础。在促进世界普惠发展的问题上，不应该强加政治诉求。目前西方主导的数据跨境流动规则依然带有这样的色彩，这是霸权思维的一种表现，而这恰恰也给我国建立受更多国家欢迎的去政治化的数据跨境流动规则提供了机会。另外，相对于西方甚至开始自己打脸的所谓“数据自由流动”，中国应该主张更实际的数据有序流动要求，一方面不能一刀切地阻断“数据自由流动”来实现安全目标，因噎废食地失去信息技术发展带来的巨大收益；另一方面还是要根据实际情况尊重一定的规则，例如根据不同类别的数据设定宽严不同的要求，充分发挥政府监管和企业、行业、社会的自律机制和市场能动性，使流动的数据带来效益的同时不至于被严重地恶意利用。

二是安全与发展并重原则。当前，数据跨境流动政策面临复杂甚至冲突的决策因素，但是服务于国家发展大局是最终目标。2016 年 4 月 25 日，习近平在全国网络安全和信息化工作会议上指出：网络安全是动态的而不是静态的，开放的而不是封闭的，相对的而不是绝对的。因此，在中央新一轮开放发展战略的总体指引下，我国开展跨境数据流动管理必须明确安全底线，廓清限制流动的数据范围，同时提升能力保持对跨境数据流的可知可控，保障国家安全和用户隐私。

三是合作共赢原则。网络安全领域的博弈，在当今的世界，本质上就是国家主权在网络空间的投影和互动博弈。习近平主席提出构建网络空间命运共同体的重要主张，体现了中国对网络空间全球治理的担当，成为指引中国推进网络空间国际合作和全球治理的核心理念。我国推动网络空间治理的目标不是阻断数据的自由流动，或者用主权壁垒分割全球网络空间，而是要保障所有国家，包括技术能力暂时处于弱势地位的国家，不会因为能力的差异而导致合法利益受到损害；不是一刀切地阻断与境外的数据交流，而是构建双边和多边的数据跨境流动信任体系。主权国家追求的目标，是数据的使用能够促进数据初始提供者的利益，而非成为少数掌握了技术优势的行为体过度追求自身利益的工具。对数据的使用和处置，必须遵循人类共同财产原则，也就是尽可能让大多数的行为体都能从中获益。掌握技术优势的先进行为体，无论国家、公司亦或某种形式的联合体，都不应该不加节制地滥用自身的优势，威胁、挤压乃至剥夺弱势行为体的合法权益。

2.实现路径

面对数字经济领域的新机遇、新挑战和新竞争，我国应当把握全球数字产业竞争和政策演进趋势，梳理各行业数据跨境流动的总体需求，充分利用自贸区创新发展试验田的作用，探索建立一个开放、透明且可操作的数据流动监管体系。

一是制度完善与先行先试阶段（1-2 年）。在 1-2 年内，以促进数字经济竞争力和保障安全和隐私为主旨目标制定《个人数据保护法》《数据安全法》，在顶层设计和法治基石上保障我国数字经济持续创新发展，更好参与全球数字经济竞争和治理。选择上海自由贸易区或者海南自由港作为先行先试地区，利用自贸区制度创新优势，试点制定完善自贸区数据跨境传输、利用、保护、流转等方面

规则体系，以自贸区数据自由港积极与欧盟对接商谈“充分性认定”。与战略合作伙伴和密切的贸易伙伴，包括俄罗斯、日本、韩国以及一带一路沿线重点国家开展数据跨境自由流动谈判。同时积极鼓励地方政府、行业主管部门、产业界和学术界在数据安全治理方面的创新和探索，发挥我国数字经济的特点优势，建立有国际影响力的标准体系和运行机制，为我国在全球开展有说服力的数据跨境流动规则奠定基础；

二是国内监管完善与国际合作推进阶段（3-4 年）。在 3-4 年内，实现政府高效监管、行业严格自律、社会服务健全的高水平的数据跨境流动安全评估和治理体系，建立以主要贸易伙伴和战略合作对象为核心的数据跨境流动朋友圈，建立重要的双边、多边数据跨境流动合作体系，初步形成一套充分体现我国主张的数据跨境流动规则和模式。

三是规则主导和引领阶段（5-8 年）。建立以中国为主导的多边贸易规则体系，重构数据跨境流动规则，推动一体化的数据保护标准和数据跨境流动监管机制。

3.实施策略

从实施策略上来讲，数据跨境流动政策的构建涉及隐私保护、产业竞争、国家安全等多维度命题的交织与互动。这一公共政策的复杂性体现在三重利益诉求上，一是从个人视角出发的权利保护诉求；二是产业视角的发展、创新和竞争诉求；三是从国家视角出发的数字经济国际竞争力和地缘政治影响下的数据主权安全需求。实施策略需要综合考虑多重利益诉求，实现目标与能力的平衡。

（1）加快出台数据跨境流动制度体系

由于个人数据与重要敏感数据涉及的风险和所需保护的法益各有不同，许多国家都在尝试分级分类监管的方法，通过精细化的法益衡量，确立宽严不同的数据跨境流动管理政策。

首先，对于个人数据出境，应当坚持以市场机制为主，企业自律和政府监管相结合，针对个人数据出境后可能遭遇的数据泄露、数据滥用等侵犯个人合

法权益的风险制定监管规则。我国目前初步建立的数据跨境流动政策，如将数据出境安全评估作为单一合规机制，在现实中恐难以适应海量数据跨境管理需求。建议参考欧盟及其他国家经验，丰富合法出境途径及配套管理办法，设立符合我国国情需要的多样化合法流动机制。

一是根据个人数据保护状况及对等原则，将部分国家和地区纳入可自由流动的范围。与国际通行做法接轨，以国家地域为主要认定准则，对个人数据保护状况实施评估，结合对等原则，同时兼顾我国管理实际需要，梳理总结我国典型的出境商贸企业和跨国公司个人数据出境现实场景和主要目的地，兼具确定性和灵活性，形成“以数据保护水平为原则加若干例外情况”的认定方法。数据跨境流动评估主要涉及对方的法律环境、数据安全能力、合同范本等几大部分领域。其中对于国家地域法律环境评估的工作绝大多数企业缺乏这样的能力，这部分应该由政府统一组织和公布，以确保科学和标准一致。

二是根据安全评估的主要标准，建立指引性的数据跨境流动协议范本，类似于欧盟、澳大利亚提出的标准合同范本，引导企业在个人数据出境活动中，通过合同法律机制来管控个人数据出境风险。

三是鼓励行业协会及其他自律组织参与安全评估认证。发挥社会力量，建立竞争机制，打造具有国际水平的行业协会和第三方组织，作为市场机制补充，在安全评估中发挥作用，从而建立可落地实施，具有活力的数据管理秩序。

其次，对于重要数据出境，需结合数据出境后的安全风险进行实地分析，根据数据出境实际场景，结合重要数据的定义及范围，综合考量数据出境后产生的风险及影响，对重要数据出境实施梯度性监管。

一是借鉴国外数据分类经验，按照重要行业和信息主题分类标准，合理确定我国“重要数据”内涵和范围，指导政府、信息通信、金融、交通等相关行业主管部门探索制定行业或领域内细化的重要数据列表或识别标准。

二是将数据泄露、篡改或滥用对国家安全和社会公共安全影响程度为标准划分“重要数据”出境的风险等级，在实施风险评估后确定高中低风险下完全限制出境、审批后限制出境和出境后备案等不同的监管方式。

三是依托大型成熟跨境企业，共同研究行业级的跨境数据流动安全管理规范，在电子商务、金融、航空、云服务等领域率先推动行业跨境数据流动标准的出台，以此来带动整个行业的数据保护和数据流动，并积极推动我国的行业标准成为国际或区域性的标准。

第三，在完善跨境数据国内监管的过程中，应当结合 WTO 规则和我国入世承诺，注重国内监管规则的合法性评估，使之与 WTO 规则相协调。一方面，在制订与数据流动相关的国内规则时，应当根据我国入世减让表中的具体承诺和关贸总协定（GATT）/服务贸易总协定(GATS)一般例外和国家安全例外的评估，即我国数据跨境流动规则是否能够满 GATT/GATS 的例外规定。另一方面，对数据的国内规制不应当构成任意或不合理的歧视或构成对国际贸易的变相限制。例如《个人数据和重要数据出境安全评估办法》将对数据本地化存储和数据出境安全评估的监管对象，从《网络安全法》规定的“关键基础设施运营者”扩展至所有“网络运营者”，扩大了该措施的适用范围。可考虑对该扩展进行必要性评估，使其适用尽可能不违背 WTO 规则而对国际贸易构成变相的限制。

（2）构建我国数据安全治理体系，打造全球数据安全高地，掌握数据跨境流动话语权

国家间数据跨境流动合作是建立在相互信任基础之上的，而一国数据安全治理水平则是建立信任、达成合作的重要考量因素。构建我国数据安全治理体系，需要发挥政府、行业、企业的各自优势，实现协同共治。发挥龙头企业的引领带动作用，提升行业、国家整体数据安全治理能力，打造全球数据安全高地，以掌握数据跨境流动合作的话语权和主动权。从政府层面来说，通过制定《数据安全法》《个人数据保护法》进一步完善规则，明确主体责任和监管内容，建设良好的监督协调机制。从行业层面来说，应当深度结合行业特点，研究建立各行业数据安全相关指南、标准，鼓励行业自律，推动和监督行业性数据安全测评、监测预警、教育培训，建立安全能力与发展机会正相关的行业内数据安全治理规则与体系，带动全行业提升数据安全能力的积极性。从企业主体层面来说，应当积极

提炼和推广实践经验，参与甚至引领标准，加强数据安全意识和能力教育，提升数据安全能力，让数据安全成为组织的核心竞争力。[68]

（3）构建国家保障数据跨境流动安全的能力体系

数据跨境流动带来的国家安全威胁主要源自于数据传输至境外以后的各种不可控风险。构建国家保障数据跨境流动安全能力体系，政府必须联合实施跨境业务的企业，通过公私合作，加强对数据跨境活动中安全防护及感知、检测、溯源能力。一是加强数据泄露威胁情报共享与溯源能力，打造龙头企业、安全机构与政府机构之间的快速生态协同系统，通过产品、服务、生态协同系统共享各种数据泄露的威胁情报，加强数据安全事件的快速和响应的能力，并追踪溯源恶意行为，快速定位威胁来源。 二是积极拥抱创新技术。数据跨境流动包含数据泄露、个人隐私风险、数据滥用等一系列安全风险，需要多方合作积极研发和应用创新技术如同态技术、多方计算等大量新技术来降低数据安全的威胁。三是加强政府反制和威慑能力。对国家安全构成重大威胁的数据泄露事件，综合利用外交、信息、军事、经济、情报以及执法等力量，对其进行威慑和打击，惩罚恶意网络行为者。

（4）积极推进双边、多边的数据跨境流动谈判

中国是国际体系的后来者，加之奉行不结盟政策，中国对其他国家的影响力投射无法与西方国家相比，主要是依靠援助来维护一定的影响力。但是 08 年金融危机和随后的欧洲主权债务危机使得西方国家在全球不断收缩，而经济实力的上升使中国成为国际舞台的重要力量。随着中国“一带一路”，上海合作组织、金砖国家、东盟地区论坛、中非合作论坛、中阿合作论坛、中拉合作论坛、中国-中东欧论坛等国际合作的开展，中国在全球的影响力在不断上升。这会总体上有效的提升中国应对地缘政治风险的能力。

我国应当充分利用“一带一路”建设等契机，在完善国内规则的基础上，由国家网信部门负责牵头，统筹外交部、商务部等相关部门以及主要龙头科技企业，

[68] 杜跃进：数据安全治理的几个基本问题，https://mp.weixin.qq.com/s/Pe2awsWdEMCVyn1A4lAjJw

启动跨境数据流动对外合作工作推进机制。在当前各种双边、多边贸易谈判中，增加数据跨境流动的谈判内容，在加强统筹的前提下，实现数据跨境流动规则的统一。

基于经贸伙伴关系、地缘政治、法律环境等因素，选择重要贸易伙伴国家、城市或行业，洽谈建立跨境数据流动的双边/多边规则，根据个人信息保护状况及对等措施，针对不同国家或地区在数据出境开放与限制程度上实施数据开放的不同承诺。优先选择开展谈判对话的国家可以包括俄罗斯、韩国、日本、上海合作组织成员国、东盟国家等。

比如当前，中日韩自贸区谈判正加速推进，这是中国正在推动的经济体量最大、占中国外贸比重最高的自贸区谈判之一，三国经济走向一体化将给中国外贸带来巨大红利，有效缓解外部环境不稳定、不确定因素造成的冲击。在中日韩自贸区谈判中可以将数据跨境流动议题纳入其中，推进区域内数据自由流动。

“区域全面经济伙伴关系协定”(RCEP)谈判有望在 2019 年完成。未来，我国可以借助 RCEP，推动与东盟国家的数据自由流动朋友圈建设。东盟国家具有巨大的市场空间和潜力，我国大量互联网企业已经进入这个市场。同时，东盟国家的数据保护制定正在制定完善过程之中，跨境数据流动规则也有待建立，我国可以尝试与东盟国家开展相关谈判，为我国互联网企业在东盟业务的发展提供支撑。

此外，我国也可考虑参与 APEC 下的 CBPR 机制，该机制虽然由美国主导，但是其遵循的 APEC 隐私框架要求不高，与我国数据保护要求较为契合，并且其制定的数据流动规则较为弹性，APEC 多数成员国大都有意向加入其中。参与 CBPR 有助于减轻我国企业在实施跨境业务时个人数据跨境流动的合规负担。

（5）建立国际执法协作条件和框架，解决数据管辖冲突

在各国纷纷主张数据主权的情况下，特别是欧盟和美国的长臂管辖对传统国际执法协作体系构成冲击。当前，我国应对管辖冲突的策略仍以防守为主，依据《网络安全法》第 37 条和《国际刑事司法协助法》，明确阻断直接来自外国政府对境内的机构、组织和个人控制的数据的刑事司法管辖权。“非经中华人民共

和国主管机关同意，中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和法律规定的协助。” 与此同时，依据《网络安全法》第 75 条，我国对来自境外的危害关键信息基础设施的活动将主张管辖权。为落实《网络安全法》第 75 条，我国执法和监管部门不可避免地要跨境调取大量数据。这种完全限制执法数据出境，又主张境外数据刑事司法管辖权可能难以实现。可能的解决方案是，未来在《数据安全法》中明确数据相关国际执法协作的框架与条件，应对美国、欧盟长臂管辖，设计符合国家利益和中国企业全球化战略的执法数据调取方案，并积极与各国建立双边-多边的数据执法调取协议。

（6）利用特定地区的政策创新优势，在确保可监管的前提下探索建设全球数据港

利用特定区域，如上海自由贸易试验区、海南自由港或者香港特别行政区等特定地区的制度创新优势，探索建立一个开放、透明且可操作的跨境数据流动监管体系，通过建成自贸区功能示范区，吸引涉及数据跨境业务的一批企业入驻，从技术和政策等方面完善跨境数据流动的解决方案，推动建设全球数据港。通过在自贸区功能区域的试点建设，探索监管经验，实现开放水平与监管能力的匹配，稳步实现我国其他地区城市的跨境数据流动水平的提升。

一是出台专项法规。发挥自贸区在跨境服务先行先试功能，探索试点放开电信业务外商投资的管理模式，研究出台《上海/海南（自贸区）跨境数据流动管理试行办法》，该办法包括数据流入和流出的负面清单，跨境数据流动的管理机构、电信增值业务开放以及离岸数据中心建设、数据流动财税优惠以及违法开展跨境数据流动的处罚细则等。

二是打造功能区域。在自贸区范围内，选择具备开发能力的地址空间，作为面向跨境业务功能的数据中心（IDC）承载区，并利用临港海光缆等登陆点，扩容跨境数据通讯专线，建设性能和安全达到国际最高标准的数据基础设施，设立外商投资企业数据出境的审查试验区，明确运营主体，分领域打造若干全球数据港功能示范区，以此为载体吸引跨国业务企业的入驻，实现跨境企业数据集聚和集中管理，进而带动相关产业的集聚。

三是组建数据海关。相关部门须联合组建数据海关，以跨部门、平台化的方式开展工作，通过制定数据分类分级监管体系，分行业明确敏感的个人数据和重要数据范畴，并充分运用大数据、人工智能等技术手段建立自动化监管流程，对企业跨境数据流动活动进行实时的风险评估和梯度管理，为企业跨境活动提供必要的技术解决方案指导。

四是创新技术模式。全球数据港必须有效识别和解决数据跨境流动过程中的安全风险。因此，需要充分调动国内外大数据安全技术公司，为全球数据港打造安全可控的跨境数据流动技术路径，全面支撑相关龙头企业和功能示范区企业的跨境业务。

（7）发挥产业界优势，鼓励龙头企业积极探索跨境数据流动的实践，更多地利用市场化机制提升跨境流动管理效率

政府应当鼓励建立行业性的数据保护的自律机制，鼓励企业加强与国内外监管机构的合作。比如借鉴欧盟 GDPR 条款，要求企业设置数据安全官，负责与监管部门的对接和对话。对企业申请国外监管机构或第三方认证提供帮助和指导。积极推广优秀企业的数据保护和跨境流动最佳实践，带动行业和社会整体保护水平的提升。通过行业协会、第三方机构实施数据跨境流动认证评估，推动优秀企业在市场竞争能够被广大用户清晰辨识，激发企业严格合规与高度自律的积极性。