数据本地化的内涵分化及立法动因

刘蕙华

华南理工大学法学院，广东广州，510006；

摘要：全球化与数字化背景下，数据跨境流动引发管辖权割裂、治理规则碎片化等问题，数据本地化成为多国重要规制手段。本文梳理数据本地化的概念演进与类型，明确“法律上”与“事实上”的本地化分类及地缘政治影响下的新形态。从数据双重属性视角，剖析各国立法动因，指出其既源于个人隐私保护需求，更服务于国家安全与地缘政治博弈。研究为理解全球数据治理格局与各国政策选择提供理论支撑。

关键词：数据本地化；事实上的数据本地化；跨境数据流动

DOI：10.64216/3080-1486.26.03.053

在全球化与数字化交织的今天，数据的跨境流动已成为国际交往与经济发展的常态。然而，数据存储地与来源地的分离，不仅导致管辖权与数据所有权的割裂，更引发数据治理规则的碎片化与主体多元化。在此背景下，“数据本地化” 作为重要规制手段被多国采纳。本文系统梳理数据本地化的内涵分化，分析其类型与特征，并从立法动因视角，探讨各国在隐私保护、国家安全与地缘政治等多重考量下，如何通过数据本地化政策应对跨境数据流动的挑战与机遇。

1“数据本地化” 的概念及类型

常态性的数据跨境流动导致数据存储地与来源地割裂，直接造成数据所有权与传统管辖权分离，进而引发数据治理规则碎片化与治理主体多元化。当前数据治理的管辖权归属主要分为“数据本地化标准”和“数据控制者标准”：前者以属地连接点作为主权国家行使数据管辖的分界，贴近传统威斯特伐利亚体系的领土性；后者以属人性确定跨境数据管辖，在云技术影响下突破数据主权的属地边界，延伸至技术边界以规避存储地管辖权。目前，多数国家仍主要采用 “数据本地化标准” 行使数据管辖。

追溯发展进程，“棱镜门” 事件虽被视为数据本地化的关键催化剂，但早在 2005 年，哈萨克斯坦就曾立法要求所有数据存储于国内，虽因 Google 强烈反对被推翻，但印证了 21 世纪初国家对数据本地化的探索。进入 21 世纪 20 年代，互联网格局发生重大变革，新兴国家开始积极参与互联网治理规则建构，数据本地化的讨论达到空前高度。

2020 年，经济合作与发展组织（OECD）将数据本地化定义为：通过强行法或行政性规定直接或间接要求在特定管辖区内以独占或非独占方式存储或处理数据。其中 “独占式” 要求数据必须在本地存储或处理，严格限制数据及副本出境；“非独占式” 要求本地存储数据副本，满足条件后数据可跨境转移。该定义侧重实施效果，未明确措施的具体行为类型。

全球互联网治理委员会在研究其对金融服务的影响时，将数据本地化分为四类：（1）数据出境的地域限制，要求数据必须在特定管辖区内存储和处理，副本不得离开；（2）数据位置的地理限制，要求本地存储副本，不限制副本出境处理；（3）基于许可的数据传输，要求数据出境需有关机关许可；（4）基于标准体系的数据传输，要求数据出境满足标准化步骤以保障用户数据安全与隐私。前两类通过明确限制条件规制数据传输，是各国广泛采用的立法模式，称为 “法律上的数据本地化”；后两类则被称为 “事实上的数据本地化”。

“事实上的数据本地化” 指一国无明确本地化要求，但通过立法或授权规定，数据需满足特定条件方可传输至境外。此类规制依据监管机构对数据风险的研判决定是否允许出境，存在较大不确定性与复杂性。以欧盟跨境数据传输机制为例，其确立了针对特定国家“整体适用” 的充分性决定和针对特定商事主体 “个别适用” 的标准数据保护条款。后者地理范围不限于 “充分性认定” 国家，第三国数据进口方满足 “适当保障措施” 即可传输。根据《通用数据保护条例》（GDPR）第 46 条，“适当保障措施” 包括：（a）基于公共机构间有约束力和可执行力的协议转移；（b）企业制定经数据保护机关批准的拘束力公司规则（BCRs）；

（c）签署标准合同条款（SCCs）；（d）基于经批准的行为守则转移；（e）基于经批准的认证机制转移。

欧盟凭借市场优势输出跨境数据流动规则，形成“布鲁塞尔效应”。对第三国而言，若制定符合欧盟标准的国内法，其企业需遵守严格隐私标准，面临高昂数据传输及管理成本；若不修改国内法，企业需通过 BCRs 或 SCCs 确保隐私保护，而昂贵的时间成本、经营成本及潜在巨额赔款风险，促使企业选择将数据留在本地存储处理。因此，有学者指出 GDPR 是全球最大的事实上的本地化框架。笔者认为，此类通过设置跨境限制间接实现本地化目标的方式，虽具隐蔽性，但对国际贸易的影响与直接规定无异，且反映出数据本地化已成为强势国家与新兴经济体的共同选择，应纳入讨论范畴。

上述分类多从国内或区域立法维度展开，忽略了地缘政治这一重要因素。OECD 将可信赖的跨境流动规则划分为单边政策法规、政府间安排及技术和组织措施。政府间谈判合作有助于构建安全可信的跨境数据流动框架，但多边数据监管体系往往带有明显的意识形态和地缘政治色彩。美国长期高举“数据自由流动”旗帜，与盟国构建数据跨境自由流动格局，牵头推动亚太经济合作组织（APEC）制定《跨境隐私规则》（CBPR），参与国多为其盟友。同时，美国意图对中国、伊朗、俄罗斯等“受关注国家”实施数据封锁，2024 年 2 月，时任美国总统拜登签署第 14117 号行政命令，禁止或限制美国主体进行导致这些国家及相关主体访问敏感个人数据和美国政府相关数据的交易。可见，在地缘政治影响下，数据本地化演变为“政治利益共同体”内部自由流动，对共同体之外国家严格限制数据传输的模式。

综上，数据本地化可从三个维度分类：从数据存储及处理要求看，分为独占式和非独占式；从跨境数据流动规制方式看，分为法律上的和事实上的；此外，部分国家基于地缘政治竞争形成“政治利益共同体”的数据本地化。

2 各国采取数据本地化的立法动因

西方学者曾研究数据本地化对经济的不利影响，认为技术产业依赖全球经济规模，强制数据中心本地化会阻碍其发展。另有研究显示，若欧盟服务贸易与跨境数据流动严重中断（假设企业约束性规则、示范合同条款及欧美安全港框架不再被认可），其国内生产总值（GDP）可能遭受 - 0.8% 至 - 1.3% 的负面影响。尽管数据本地化存在经济负面效应，各国仍坚持采取不同力度的相关措施，需从立法动因角度进行解释。

OECD 于 2020 年将主权国家采取数据本地化的九大动因归为个人隐私与国家安全两类。上世纪 70 年代起，欧美数据博弈主导跨境数据流动机制变革，背后是欧盟“权利本位”与美国“市场本位”的话语权争夺。欧洲重视人权保护传统，在数据流动中强调个人隐私保护，数据主体享有知情权、可携带权、被遗忘权等主动权利；美国“市场本位”观念下，个人数据保护更多置于市场环境，用户仅在“免于商业欺诈或不公平交易”层面获得隐私保障。在欧盟数据博弈推动跨境数据发展的前四十年，数据本地化的核心宗旨是通过提升数据主体对数据的控制力，实现个人隐私保障目标。

近十年，全球化深入与新兴国家“入局”使跨境数据流动呈现新样态：新兴国家未被充分挖掘的数据市场成为强势国家的目标，而新兴国家也在寻求构建数据主权。此时，数据本地化的意旨不再局限于维护个人隐私权和市场经济环境，更成为主权国家在数据领域主张主权的规范表达。

在从国家战略角度解构数据本地化运作机理时，有学者提出“数据保护主义”，认为国家通过限制性数字贸易措施，促使数据相关高科技投资与生产留在国内，增强本国企业或产业的市场竞争力；也有学者提出“数字民族主义”，指国家通过权威方式控制数据存储、处理等问题以实现政治经济利益。但既有理论缺乏从国家互动和博弈视角解析因果逻辑。事实上，跨境数据流动已不仅是技术和经济问题，更涉及国际政治考量，国家政策选择深受国内外多重因素影响。本文拟从数据的双重属性视角解释各国立法动因。

数据作为数字技术的生产要素本无价值倾向，但在数字经济发展中，已成为国家重要新兴资产和权力象征，兼具自然与社会双重属性。

在自然属性层面，数据具有可复制性、高度流动性和无边界性，唯有流动才能产生价值。纯粹从技术和经济价值创造角度，更少的跨境流动壁垒能促进数据全球自由交换，实现资源优化配置，最大化数字经济价值。但这一理想模式建立在各国跨境数据流动地位绝对平等的假设之上，否则依据数据市场“丛林法则”，技术优势国家可能为追求利润最大化蚕食弱小国家数据

市场，导致 “公地悲剧”。此外，在无政府状态的国际体系中，力量悬殊引发的国家博弈恒定存在，跨境数据流动作为国家互动的表现形式，无法突破国际体系运行基本规律。因此，单纯从自然属性批判本地化措施的合理性，忽视了其在国家竞争与互动框架下的社会属性。

在社会属性层面，数据成为地缘政治竞争中国家博弈的战略工具。国际政治语境中，古典现实主义学派代表摩索根认为人性本恶，国家为维护安全需尽可能追求权力；新现实主义学派代表沃尔兹基于 “安全困境” 提出，国家只需保持权力优势即可避免引发他国不安。两种理论均表明，占有权力优势是国家维护安全的重要保障，这一逻辑在数据竞争中同样适用。数据作为数字时代的 “石油”，数据大国依托强大信息基础设施，鼓吹数据自由流动以扩大乃至蚕食他国数据市场；而受到安全威胁的数据小国则采取防御性数据流动政策，如印度实施高压数据本地化措施。随着中国等新兴国家在信息技术领域崛起，传统数据大国为巩固既有红利，也开始采取相对保守的跨境数据流动政策，如欧盟规定数据保护影响评估、设立数据保护官，美国禁止 “受关注国家” 及相关主体访问敏感数据等。

互联网未缓和地缘政治冲突，反而加剧其复杂性。面对数据流动引发的领土紧张等地缘政治问题，无论是传统数据大国还是新兴国家，都加强了对数据流动的政府干预与监管。基于数据的双重属性，主权国家为维护国家安全，必须确保数据治理权力不无限度流失。在应对跨境数据流动这一全球性挑战时，处于不同发展阶段、数字经济产业链不同位置的国家，基于自身发展需求及国际环境变化，呈现出不同程度的政策反应：欧盟、美国等数据强势国家依托全球信息领域优势，整体采取相对开放的跨境数据流动政策，但面对新兴国家冲击，针对性实施 “双重标准”；许多发展中国家受技术和资源限制，选择相对限缩的策略，如要求数据本地存储和处理。无论数据大国还是发展中国家，在制定数据本地化政策时，均从维护自身国际体系利益出发，规避数据流动无边界性对国家安全造成的潜在威胁。

3 结语

数据本地化的内涵分化与立法实践，是数字时代国家主权诉求、隐私保护需求与地缘政治博弈交织的必然结果。从存储要求的独占与非独占之分，到规制方式的法律与事实之别，再到地缘驱动下的利益共同体导向，其多元形态折射出全球数据治理的复杂格局。各国推行数据本地化政策，核心是在数据双重属性下寻求平衡：既需应对数据无边界流动带来的安全风险，又要兼顾数字经济发展的效率诉求，本质是维护自身在国际数据竞争中的核心利益。未来，全球数据治理的关键在于摒弃阵营对立思维，在尊重各国主权与发展差异的基础上，通过多边协商构建包容高效的规则体系。唯有平衡安全与开放、公平与效率，才能破解数据流动与本地化的张力，推动数字经济实现可持续的全球发展。

参考文献

[1]邵怿.网络数据长臂管辖权——从“最低限度联系”标准到“全球共管”模式[J].法商研究,2021,38(06):73-87.

[2]陈爱飞.“数据控制者标准”取证模式及中国因应[J].法商研究,2024,41(03):60-74.

[3]范婴.数据本地化的内涵分化与模式选择[J].情报杂志,2022,41(06):86-91+79.

[4]金晶.个人数据跨境传输的欧盟标准——规则建构、司法推动与范式扩张[J].欧洲研究,2021,39(04):89-109+7.

[5]邵怿.跨境数据流动规制的自由化与本地化之辩[J].政法论丛,2023,(05):139-148.

[6]单文华,邓娜.欧美跨境数据流动规制：冲突、协调与借鉴——基于欧盟法院“隐私盾”无效案的考察[J].西安交通大学学报(社会科学版),2021,41(05):94-103.

[7]高志宏.隐私、个人信息、数据三元分治的法理逻辑与优化路径[J].法制与社会发展,2022,28(02):207-224.

[8]封帅,薛世锟.跨境数据流动政策偏好的全球分布：国家维度的治理模式比较研究[J].俄罗斯学刊,2024,14(03):8-28.

[10]张生.美国跨境数据流动的国际法规制路径与中国的因应[J].经贸法律评论,2019,(04):79-93.

作者简介：刘蕙华（2000.09-），广东省梅州市，在读法学硕士，华南理工大学法学院，研究方向：国际经济法。