海外智库观点要览
北京大学国际战略研究院
2021年12月24日 第78期

相互竞争的数据治理模式：欧盟、中国与美国

洪川[1]

编者按：随着数字贸易的飞速发展，数据治理日益成为全球经济和政治中的突出问题。本期摘译推荐的文章认为，当前以欧盟、中国和美国为代表出现了三种相互竞争的数据治理模式。欧盟模式强调保护个人数据隐私，中国模式重视捍卫主权与安全，美国模式介于两者之间。数据治理模式的分裂可能威胁全球信息流动，阻碍世界贸易发展。

货物、服务、资本和数据的跨境自由流动是全球经济的基本要素。随着反全球化浪潮的持续以及地缘政治竞争的升级，各国设置了越来越多的贸易壁垒，使全球贸易成本不断攀升，效率也随之下降。各国施加的阻碍措施包括提高关税、设置其他形式的贸易管制、加强投资审查以及收紧移民政策等，这些障碍也正在向数据领域扩散。近年来，数据流动对社会和经济发展越发重要。2019 年，包括电子商务和数字交付服务在内的全球数字贸易价值为 5.5 至 6 万亿美元，约占全球出口总额的 25%。

越来越多的公民、企业和决策者开始探讨建立数据治理框架。第三届联合国世界数据论坛强调了数据流动和共享在解决全球治理问题时不可或缺的作用，并提倡通过保护数据安全和隐私来增加信任，保持信息的自由流动。

数据供应链包括以下几个部分：数据的生成、收集、管理（包括质量管控）、

[1] 洪川（Hung Tran）是大西洋理事会地缘经济中心的非常驻高级研究员，曾任国际金融协会（The Institute of International Finance）执行总裁。本文英文原文题为“Competing Data-Governance Models Threaten the Free Flow of Information and Hamper World Trade”，发表于大西洋理事会官方网站：https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/competing-data-governance-models-threaten-the-free-flow-of-information-and-hamper-world-trade/。此为中文摘译版。

使用（包括营销、研究、政治和军事等），以及流通（国内和跨境）。另一个理解数据供应链的视角则关注数据生态系统中的行为体：谁拥有数据？谁从数据中获益？谁决定收集什么数据以及如何使用数据？谁来控制上述行为体？目前，大型平台运营商已经展现出了寡头或垄断性。基于网络效应和先发优势，它们能够攫取巨额利润，并产生重大社会与政治影响。因此，这些平台应当被纳入监管范围。

当前，世界上出现了三种不同的数据治理路径。欧盟推出了一个全面治理框架，以监管个人数据生成和使用的方方面面，突出个人数据安全和隐私。中国颁布了一系列法律，正式确立了其数据主权的愿景，认为公民的个人数据也应在政府管辖范围内，以保障经济发展、社会稳定和国家安全。美国一直坚持国内和跨境的数据自由流动，侧重于保护个人隐私免受政府侵犯（除涉及国家安全的情况外），但是，除个人健康信息等特定领域外，美国没有任何联邦法律来保护个人隐私不受私营企业（尤其是互联网企业）的侵犯。

随着这些地区/国家的数据治理框架逐渐成为法律，并在许多情况下产生域外影响力，全球的创意、信息和数据市场将走向分裂，这会提升跨境商务的合规成本，限制数据共享的潜力。

一、欧盟路径

欧盟制定了一个全面框架来监管数据流动的方方面面，包括个人在数据被收集、使用和流通时的相关权利、数据中间商和平台公司的行为规范、相关实体对在线服务的内容所负的责任，以及有关的税收规定。根据欧盟框架，即使数据公司的总部设在第三国，它们也需为在欧盟范围内的经营活动缴税。

在隐私条例的基础上，欧盟的《通用数据保护条例》（下称《条例》）于 2018 年 5 月 25 日正式生效。该条例旨在保护公民有关个人数据的基本权利。总体而言，数据中间商在收集或发送个人数据前，必须取得用户同意；同时，个人也有权浏览个人数据的内容，查询此类数据的使用方式，要求更正数据以及删除所有数据。《条例》具有重要的域外影响，适用于所有使用欧盟居民数据的数据中间商，不论这些公司的总部所在地。

《条例》还规定，只有在欧盟认为某非欧盟国家的隐私保护制度在作用上等同于欧盟的情况下，有关欧盟公民的数据才能被转让给该国实体。这一规定导致美欧商业关系严重破裂：2020 年 7 月，欧盟法院裁定，在政府出于国家安全目

的获取个人数据以及欧盟公民在美国接受司法审查和赔偿等问题上，美国没有与欧盟对等的保护制度。这项裁定意味着《欧美隐私盾协议》（EU-US Data Privacy Shield）失效，该协议原本旨在促进美国和欧盟间的数据自由流动。由此，跨大西洋关系在数据传输方面遭到破坏，双方企业都面临巨大的不确定性。如果不能及时解决这一问题，那么在欧盟区域内开展服务的跨国公司将不得不接受数据本地化的要求，因为在欧盟内部建立数据服务器和处理设施远比处理法律不确定性更加简单。

欧盟委员会已经承认了十三个具备对等数据隐私保护框架的国家和地区。但欧盟法院对美国监管框架的最终裁决使人产生疑虑：在剩下的十二个国家或地区里，有多少最终将被认定为拥有与欧盟同等的隐私保护框架？如果这种不确定性持续存在，欧盟的数据流动将受到限制，其在线业务和创新将受到负面影响。

近年来，欧盟法院还加强了《条例》的执法力度，措施之一是：允许成员国的隐私委员会直接起诉违规的数据公司，而不用依赖欧盟框架下的隐私保护机构来提起诉讼。这可能扩大各国在解释和适用《条例》时的分歧，使成员国统一遵守《条例》变得困难。

除《条例》外，《数字市场法（DMA）》由欧盟委员会于 2020 年 12 月提出，目前正在通过成员国以及欧盟议会的相关立法程序。该法案旨在解决大型数字公司（所谓的“守门人”）市场份额过于集中的问题，要求这些公司在部分情况下允许其他企业访问其平台，并制止它们针对商业用户和消费者的排他性和不公平行为。这一举措有望给数字服务市场带来更多的公平竞争。

与《数字市场法》同期推出的《数字服务法（DSA）》也在经历同样的立法过程。该法案旨在改进数字机制，保障在线平台用户的基本权利，包括言论自由和删除非法信息等。其重要目的之一是加强公众对平台的监督，尤其是那些覆盖 10%以上欧盟人口的大型平台。公民和监管机构将帮助在线平台运营商识别和警示不法信息，而这些平台必须通过“用户友好型”的透明程序来解决不法信息问题。

最后，截止 2021 年 3 月，已经有 11 个欧盟成员国制定或提议了数字服务税（DST）。该税适用于全球收入和服务所在国当地收入超过某一阈值的跨国数字服务公司，是解决跨国公司在低税率地区设立办事处来逃税的有效方法。然而，这项措施也存在争议。从美国的角度看，其偏离了传统的税收概念，并有歧视美国

跨国科技巨头之嫌。美国威胁要对单方面征收数字服务税的国家采取报复措施。

尽管上述措施尚处在不同的颁布和实施阶段，但它们已经构建起欧盟针对数据和数字服务的全面监管框架。总体而言，欧盟路径的主旨在于保护个人免受企业和政府对其数据的入侵和滥用，努力维持一个充满竞争的数字市场，并要求数字公司负责任地处理有关其内容的争议。

二、中国路径

通过中国近期出台的一系列法律、官方声明与行动，我们可以总结出数据治理的中国路径。2017 年的《网络安全法》是中国在数据监管方面的基本法。该法明确了数据主权的概念，并详细规定了互联网产品和服务的提供商以及运营商在数据收集、本地化、使用和传输方面的义务。该法还规定，在收到有关要求时，互联网运营商必须同政府合作，将有关的用户数据移交给公共和国家安全机关。该规定是对 2017 年《国家情报法》中的一项关键条款的强化。此外，互联网公司还需对通过其网络传输的内容负责。该法律也提及了个人隐私问题。

其次是 2021 年 9 月通过的《数据安全法》。该法加强了对中国数据在境外传输的限制，并对私营企业施加了广泛的数据安全义务。该法增加了一项“国家核心数据”类别，包括了影响国家安全、国内经济、人民民生以及公共利益的数据。这样宽泛的界定为政府官员解释和实施法律提供了充足的空间，一定程度上增加了企业运营的不确定性。

此外，还有自 2021 年 12 月 1 日起生效的《个人信息保护法》。该法适用于个人信息处理实体（PIPEs），对个人信息的跨界传输施加了严格要求，包括必须通知并取得用户的同意、确保数据接收者（无论位于境内还是境外）符合《个人信息保护法》要求等。该法赋予中国政府处理个人信息的广泛权利。此外，《个人信息保护法》还规定了个人针对互联网企业的权利。例如，这些企业必须在收集个人信息前取得使用者的同意，并且提供撤销此类同意的方式。因此，《个人信息保护法》在这一方面同欧盟的《通用数据保护条例》有相似之处。

总体而言，中国路径的目标是规范数据的使用以保护国家安全，这不仅涵盖数据的对外传输，也涉及信息的内部传播。中国已经建立起一整套系统来实施有效的数据监管。上述法律被政府用作约束网络平台、社交媒体和运输公司的有力手段。

在参与制定国际技术标准时，中国一直积极推动对数据主权的国际承认。例如，在国际电信联盟（ITU）中，中国提出了新的互联网协议，使各国政府能够控制互联网的发展和活动，以取代当前全球性的开放但分散的协议。此外，中国已经能够将数据主权的概念以及相关的硬件系统出口到其他国家。值得注意的是，中国并不是唯一一个推动数据主权概念的国家。虽然印度同中国在许多政策领域持相反意见，但在数据领域采取了与中国几乎相同的做法。

三、美国路径

美国没有类似于《通用数据保护条例》的全面联邦数据保护法，主要通过一系列具体的联邦法律和部分州的消费者隐私法来保护个人数据不受政府（而非私营企业）侵害。1972 年的《美国隐私法》规定了政府机构使用个人数据所受的限制，并确认公民有权访问、复制和更正政府持有的数据。然而，特朗普政府时期通过的《澄清域外合法使用数据法》允许美国执法机构通过签发许可证来获取受美国管辖的组织所持有的数据，即使这些数据存储于美国之外或涉及美国公民以外的个人。还有部分法律保护了特定类型的个人数据隐私和安全，包括个人健康数据、未成年人数据以及金融交易中产生的非公开个人信息等。

在联邦法律的真空中，部分州已经提出了保护消费者数据隐私的立法。《加利福尼亚州消费者隐私法》将于 2021 年 1 月 1 日正式生效，《弗吉尼亚州消费者数据保护法》的生效日期被推迟到了 2023 年，另有六个州正在制定类似法案。这些州法在确保个人有权访问、纠正和删除公司个人数据以及公司合规使用数据方面与《通用数据保护条例》有相似之处。

四、总结：三种路径的不同之处

总体而言，欧盟和中国代表了两种不同的数据治理模式，美国介于两者之间，但更接近于欧盟。欧盟模式强调公民对个人数据隐私的权利，保护个人免受私人企业和政府的侵扰。该模式旨在解决大型公司的市场力量过于强大的问题，要求这些公司对其平台上的内容负责，并着手对跨国公司在其管辖范围内的商业活动征税。欧盟框架内的一个标志性组成部分——《通用数据保护条例》——吸引了大量在欧洲开展经营的非欧盟公司遵守该规范，展现了“布鲁塞尔效应”。许多国家都将《通用数据保护条例》作为制定本国数据隐私法的模板。迄今已有 16

个国家效仿该《条例》立法。

相比之下，中国模式侧重于捍卫主权与安全，赋予政府针对个人数据广泛的访问和处理权限。中国还严格控制境内和境外的数据传输，要求数据本地化，并通过高科技基础设施来加强数据监管。许多国家，特别是发展中国家，已经部分采纳了中国模式，主张数据主权，并通过从中国进口硬件和软件来实现这一愿景。

美国的联邦法律旨在保护公民隐私免受政府侵害，但并未针对私营企业采取类似措施。美国国会目前正在考虑对大型平台和社交媒体公司采取反垄断措施，并加强对未成年人的隐私保护。此外，一些州已经采取单独行动，遵照欧盟《通用数据保护条例》的思路立法。如果越来越多的州朝着这个方向发展，联邦政府可能会认为有必要通过联邦立法来实现各州法律的统一。美国联邦制的独特性使得很多其他国家难以效仿其数据治理的混合模式。

（陈泽均摘译，归泳涛校）