美欧数据跨境流动的规则博弈及走向

□ 刘文杰

〔提　　要〕在数字经济时代，各国围绕数据跨境流动的合作与竞争成为全球治理领域的焦点议题。数据跨境流动引发的权力争夺、法律较量等问题日益突出，数据保护标准尤其是数据跨境流动规则主导权之争更趋激烈。美国与欧盟在数据跨境流动领域长期开展密切合作，但围绕数据跨境流动标准的确定，美欧均希望取得主导权，这导致双方发生多轮激烈博弈。欧盟以立法为数据跨境传输规定了严格条件，基本宗旨是确保其数据保护水平不会因数据向第三国或国际组织传输而下降，为此不惜宣告构成跨大西洋数据流动法律基础的“安全港决定”和“隐私盾决定”无效。造成美欧数据跨境流动协议失效的表层原因在于美国的数据收集制度偏离了欧盟秉持的个人数据保护原则，深层原因是双方对数据流动所持立场的差异以及美国将其国家安全诉求凌驾于他国利益之上的单边霸权思维。

〔关 键 词〕个人数据保护、数据跨境流动、隐私盾决定、全球治理

〔作者简介〕刘文杰，中国政法大学比较法学研究院教授

〔中图分类号〕D815

〔文献标识码〕A

〔文章编号〕0452 8832（2022）6 期 0065-14

进入数字经济时代，对数据跨境流动的规制在全球治理中所占分量越来越重。国家及国际组织在这一领域开展的合作与竞争成为近几年来全球治理领域的重要议题。综合来看，由于制度、文化、经济发展水平等方面的差异，

不同国家对数据保护的理解不同，围绕数据保护尤其是数据跨境流动存在着规则主导权之争。美国与欧盟是全球两大主要经济体，相互间存在着政治、经济、社会、文化等诸多领域的紧密联系。伴随着大西洋两岸货物和服务贸易的开展，数据跨境流动已经成为常态。但围绕数据跨境流动标准的确定，美欧均希望取得主导权，这导致双方发生多轮激烈博弈。深入探析美欧之间的数据保护标准之争，有助于更加清楚地认识围绕数据跨境流动形成的全球治理格局，为争取这一领域的规则创建权提供有益参考。

一、全球治理中的数据跨境流动议题

随着全球化和数字经济的发展，数据跨境流动已经成为全球治理领域的重要议题。围绕这一议题，各国及国际组织提出一系列治理方案，并致力于达成稳定的双边和多边安排。[1] 然而，基于不同的国情和利益诉求，这些治理方案不尽一致，相互间甚至存在较大的差异。总体而言，在数据跨境流动的全球治理领域，各国、地区之间将会长期呈现合作与竞争并存的态势。

（一）数据跨境流动的重要性和特殊性

电子化个人数据出现空前规模的增长并在全球范围频繁传输，是人类进入数字时代的一个标志性现象。包括电子商务、快递物流、地图导航等在内的现代服务诸多领域是以个人数据的采集和传输作为支撑的。个人数据的跨境流动在全球化时代已经变得不可或缺，其不但便利了个体，更有力推动了国际贸易与投资的发展。个人数据的跨境流动也是技术和商业模式创新的内在要求。各国企业、组织、个人广泛采用的云存储服务就是将服务器部署在不同的国家和地区，从而实现数据存储和传输的最优化，这其中也包含个人数据的跨境流动。在美国白宫 2022 年 3 月发表的声明中，数据跨境流动的重要性得到高度强调，“数据流动对跨大西洋经济关系和所有经济部门的大小公司都至关重要。事实上，在美国和欧洲之间流动的数据比世界上任何其他

[1] 参见孙南翔：《CPTPP 数字贸易规则：制度博弈、规范差异与中国因应》，《学术论坛》2022 年第 7 期，第 1-10 页；王欢雪：《从东盟数据跨境流动治理机制展望与中国的数据跨境流动合作》，《中国标准化》2022 年第 10 期（下），第 38-40 页，第 50 页。

地方都多，这促成美国和欧盟之间的经济关系达到 7.1 万亿美元”。[1]

同时，个人数据跨境流动也具有特殊性，表现在个人数据涉及人格利益，这种利益并不因为信息“交割”而消失。与货物的流动相比，个人数据的流动通常采用电子传输方式，在瞬间完成，很容易转移到陌生人手中。由于个人数据是可以识别特定自然人的信息，是对自然人活动及行踪轨迹的记录，因此影响到数据主体的安全与自由。此外，个人数据流动往往由数据主体以外的人（数据控制人、数据处理人）实施，数据主体无法加以控制，甚至对自身数据的流动茫然不知，使其暴露在违法犯罪行为之下的风险大增。20 世纪 70 年代，计算机开始广泛应用于个人数据处理领域，导致存储、比较、选择和获取个人数据的可能性得到极大扩张。个人数据可以同时处于地理上分散的、成千上万的使用者支配之下，这一现象引发了公众对计算机处理个人数据所蕴含危险的关注。个人数据保护由此迎来第一波立法浪潮。

进入 21 世纪，互联网应用席卷全球，个人信息收集的普遍化和自动化、个人信息存储的无限量和无限期、个人信息转移的瞬间性和低成本，加之消费者与信息采集者在力量上的不对等，导致过度采集、长期存储而又缺乏安全措施之下的个人信息泄露风险、滥用风险较之以往大大增加。公众的诉求已经不限于简单的停止收集或者删除信息，而是希望对个人信息被利用的过程施加有效控制。因此，本世纪以来，全球掀起新一轮的个人数据保护立法浪潮。欧盟《一般数据保护条例》的出台即为代表，美国也有议员在联邦层面提出统一个人数据保护法案，中国继《民法典》规定有关个人信息保护条款之后，《个人信息保护法》及《数据安全法》也相继出台，反映出各国对新时代个人数据保护诉求的积极回应。

（二）围绕数据跨境流动的国际角力

鉴于个人数据跨境流动的重要性和特殊性，制定调整数据流动的国际规则有显著必要性。虽然双边协定是解决这一问题的选项之一，但其在实践层

[1] The White House, “FACT SHEET: United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework,” March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

面耗时耗力，收效也不明显，原因在于人员流动以及为人员提供的相关服务往往跨越多国，数据流动需求不限于两国之间。考虑到这一情况，更为现实的解决方案是多边规则进路，即通过区域贸易协定（专门的数字协定或包含在贸易协定中的数据流动条款）解决数据跨境流动问题。

美国作为世界最大经济体，拥有最发达的数字经济和数字产业，在数据的全球流动体系中，更多地扮演输入方和受益方的角色。例如，Statista 的统计数据表明，自 2017 年至今，在全球云基础设施服务市场排行榜上，美国的亚马逊、微软和谷歌公司所占有的市场份额始终名列前三。[1] 不受限制的数据流动更符合美国利益，推行数据本地化则会妨碍美国科技产业和信息产业的发展。因此，在数据跨境流动问题上，美国持一种相对自由的立场，不赞成他国以限制数据跨境的法律政策设置贸易壁垒。[2] 美国认同的数据跨境隐私规则体系建立在亚太经合组织隐私框架的基础上，而后者又以经济合作与发展组织的《隐私与个人数据跨境流动保护指南》为基础。该指南最初发布于 1980 年，更强调企业遵守个人数据保护诸项原则的承诺。2013 年，指南发布新版，增加了“建立数据保护机构”、“发生数据安全事件后通知数据保护机构和数据主体”以及“问责原则”，但其相对较低的个人数据保护门槛尤其是针对数据跨境流动相对宽松的立场并无改变。[3]

与美国立场不同，欧盟致力于更高水平的个人数据保护和对数据跨境流动的更严格监管。2016 年通过的《一般数据保护条例》确立了大数据时代数据跨境流动规则框架，目的是使数据主体在欧盟享受到的保护水平不因数据跨境流动而降低。通过《一般数据保护条例》，欧盟向全世界传递了个人数据保护和跨境流动规则应向欧盟看齐的意图。该条例规定，欧盟应对目标国进行个人数据保护充分性评估，评估对象包括目标国法律制度尤其是公权力

[1] “Cloud Infrastructure Services Vendor Market Share Worldwide from 4th Quarter 2017 to 1st Quarter 2022,” August 25, 2022, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.

[2] 戴恩·罗兰德、伊丽莎白·麦克唐纳：《信息技术法》，宋连斌等译，武汉大学出版社 2004 年版，第 308 页。

[3] 洪延青：《推进“一带一路”数据跨境流动的中国方案——以美欧范式为背景的展开》，《中国法律评论》2021 年第 2 期，第 30-42 页。

部门访问个人数据的可行性和条件，实际上涵盖了目标国价值观、意识形态和政治制度等方面。[1]

在个人数据跨境流动的全球角力场上，还有其他相对折衷的方案。如中国加入的《区域全面经济伙伴关系协定》（RCEP）第 12 章“电子商务”只是要求缔约方应当在可能的范围内合作，以保护从一缔约方转移来的个人信息。就“通过电子方式跨境传输信息”，协定认可缔约方对通过电子方式传输信息有各自的监管要求，允许缔约方采取或维持其认为实现合法公共政策目标所必要的措施。协定还强调，此类合法公共政策的必要性由相关缔约方自己决定，从而更加尊重缔约方的主权和各自特点，给缔约方留出了较大政策设计空间。当然，这并不意味着 RCEP 忽略了个人数据安全。协定第 12 章第 8 条是关于线上个人信息保护的规定，要求每一缔约方在制定保护个人信息的法律框架时，应当考虑相关国际组织或机构的国际标准、原则、指南和准则。

此外，中国积极申请加入的《数字经济伙伴关系协定》（DEPA）在数据跨境流动问题上，对缔约方同样采取了一种相对灵活的态度。[2] 该协定第 4 章“数据问题”要求每一缔约方应允许为开展业务目的通过电子方式跨境传输信息，其中包括个人信息；与 RCEP 表述相同，协定认可缔约方有各自的监管要求，可以采取或维持合法公共政策目标所要求的措施。DEPA 同样设有个人信息保护规定，强调了个人信息保护的收集限制、数据质量、用途说明、使用限制、安全保障、透明度、个人参与以及责任原则，并敦促每一缔约方致力于制定机制，促进不同个人信息保护体制之间的兼容性和互操作性。

二、美欧数据跨境流动的博弈进程

2022 年 10 月，美国总统拜登签署《关于加强美国信号情报活动保障措

[1] Nigel Cory, Daniel Castro and Ellysse Dick, “‘Schrems II’: What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation,” Information Technology & Innovation Foundation Program, December 3, 2020, https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/.

[2] 周念利、于美月：《中国应如何对接 DEPA——基于 DEPA 与 RCEP 对比的视角》，《理论学刊》2022 年第 2 期，第 55-64 页。

施的行政命令》，以实施该国 3 月与欧盟最新达成的数据隐私框架协议——《跨大西洋数据隐私框架》。这是美欧围绕数据跨境流动监管开展的第三次尝试，此前双方已就该问题博弈多年，曾于 2000 年和 2016 年先后签订《安全港协议》和《隐私盾协议》，但二者均以欧盟法院认定无效告终。

（一）“安全港决定”和“隐私盾决定”的相继失效

1998 年，欧盟《关于个人数据处理及其自由流动的个人保护第 95/46/EC 号指令》（以下简称《个人数据保护指令》）正式生效，禁止将个人数据传输到未提供“充分保护”的第三国。出于商业利益考虑，美国与欧盟 2000 年 12 月达成有关个人数据跨境传输的《安全港协议》，欧盟委员会在此基础上作出第 2000/520 号决定（“安全港决定”），确认美国能够为欧盟公民的个人数据提供充分的制度保障。

2013 年，“安全港决定”的效力遭遇来自欧盟内部的挑战。这一挑战不是来自双方行政部门的质疑，而是通过个案受到欧盟法院的司法审查。斯诺登“棱镜门”事件同年曝出后，奥地利国民马克西米利安·施雷姆斯（Maximillian Schrems）[1] 向爱尔兰个人数据监管机构提出申诉，认为美国关于个人信息保护的保护强度远低于欧盟，请求禁止脸书爱尔兰公司将其个人信息传输至美国境内。监管机构依据欧盟委员会“安全港决定”，认为美国确保了足够的保护水平，驳回了投诉。施雷姆斯随即向法院起诉。经过层层审理，欧盟法院 2015 年 10 月作出判决，宣布欧盟委员会“安全港决定”无效（“Schrems Ⅰ判决”）。[2]

“安全港决定”被判无效后，美国与欧盟展开紧急磋商。美国政府向欧盟委员会出具书面承诺，保证将对其“出于公共利益获取和使用个人数据”的行为加以限制并提供救济措施，建立独立于美国情报部门的“隐私盾监察员”等。同时，《一般数据保护条例》于 2016 年 4 月经欧洲议会投票通过。在此背景下，美欧于 2016 年 7 月达成第二份数据跨境传输协议，即《隐私盾协议》。

[1] 施雷姆斯自 2008 年以来一直是脸书公司的用户。与居住在欧盟国家的其他用户一样，施雷姆斯的部分或全部个人数据被脸书爱尔兰公司转移到位于美国的脸书公司服务器上，并在那里进行处理。

[2] “Case: C-362/14 – Schrems I,” https://www.europeansources.info/record/judgment-in-case-c-362-14-maximillian-schrems-v-data-protection-commissioner/.

欧盟委员会据此再次作出美国可以对传输至美国的个人数据提供充分保护的第 2016/1250 号决定（“隐私盾决定”）。考虑到上述新情况，审理施雷姆斯与脸书公司诉讼的爱尔兰法院请求欧盟法院裁决第 2016/1250 号决定是否有效。

2020 年 7 月，欧盟法院作出判决，宣布第 2016/1250 号“隐私盾决定”无效。[1] 法院的审查主要围绕“隐私盾决定”第 1 条第 1 款进行，欧盟委员会在该款中认定美国为欧盟个人数据提供的保护水平实质上等同于欧盟的保护水平。但欧盟法院认为，美国对外国人数据的情报收集制度不符合欧盟法律规定的比例原则。[2] 一方面，美国《外国情报监视法》第 702 条没有对其赋予的、为获取外国情报目的实施监视计划的权力有任何限制，也没有对可能成为这些计划目标的非美国人给予保障，因此没有满足比例原则要求。另一方面，基于美国第 12333 号行政命令开展的监控允许情报机关对流动到美国的数据进行“批量”收集，且不受任何司法审查的限制。因此，该行政命令也不符合比例原则。

欧盟法院还认为，尽管“隐私盾决定”规定了美国当局在实施有关监视计划时必须遵守的要求，但美国《外国情报监视法》第 702 条和第 12333 号行政命令都没有赋予数据主体可在法院起诉美国当局的权利，数据主体没有获得有效救济的机会。“隐私盾决定”中的美方隐私盾监察员虽然被描述为“独立于情报部门”，却是由美国国务卿任命的，是美国国务院的一个组成部分。“隐私盾决定”中也没有任何内容表明监察员相对于行政部门的独立性。[3] 因此，“隐私盾决定”提到的监察员机制并没有提供相当于《欧盟基本权利宪章》第 47 条所要求的保障。[4]

[1] “Case: C-311/18 - Schrems II,” https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en/.

[2] 《欧盟基本权利宪章》要求，对行使基本权利的任何限制必须由法律规定，必须特别指出在什么情况和什么条件下可以对个人数据保护进行减损和限制，并规定最低限度的保障措施，以便数据主体在其个人数据免受滥用方面获得足够的保障。

[3] “Case: C-274/14 - Banco de Santander,” https://ec.europa.eu/newsroom/comp/items/667196/en.

[4] 《欧盟基本权利宪章》第 47 条第 1 款要求，每个受欧盟法律保障的人有权在权利和自由受到侵犯时向法庭获得有效救济。根据该条第 2 款，每个人都有权得到一个独立和公正的法庭的审理。

（二）围绕《跨大西洋数据隐私框架》的磋商

由于“安全港决定”和“隐私盾决定”归于无效，美欧不得不就个人数据跨境流动开展新一轮磋商。2022 年 3 月，美欧发表联合声明，承诺建立一个新的跨大西洋数据隐私框架，并解决欧盟法院在 2020 年“隐私盾决定”无效判决中提出的关切。美方承诺推行新的保障措施，以确保其在追求国家安全目标时开展的信号情报活动是“必要”和“成比例的”，并为欧盟个人建立新的针对信号情报活动的救济机制。[1]

根据《跨大西洋数据隐私框架》，美方的承诺包括加强对美国信号情报活动中的公民隐私和自由的保障、建立独立和有约束力的新救济机制以及加强对信号情报活动的分层监督。新的框架旨在确保：美国只有在为达到合法的国家安全目标所必需的情况下，才可以进行信号情报收集，并且不得对个人隐私和自由造成不成比例的影响；欧盟公民可以向多层新救济机制寻求法律救济，该机制包括一个独立于美国政府的数据保护审查法庭，其将有充分的权力对索赔进行裁决并根据需要指导补救措施；美国情报机构将实施程序，监督公民隐私和自由新标准得到有效遵守。同时，参与到该框架中的公司和组织将被要求继续遵守隐私盾原则，可通过美国商务部对其遵守该原则进行自我认证。欧盟公民将继续拥有多种救济渠道，包括通过替代性争议解决方案和有约束力的仲裁来解决其对参与方的投诉。2022 年 10 月，美国总统拜登签署行政命令，将上述承诺落实于纸面，作为欧盟委员会进行保护充分性认定的评估基础。[2]

三、美欧数据跨境流动之争的原因

无论在欧洲还是美国，个人数据保护都起源于隐私权制度，在数据保护规则的创建上，美国甚至呈现出某种向欧洲靠拢的态势。尽管如此，双方仍然就数据跨境流动问题发生了激烈的冲突，乃至出现两次政府间协议被欧盟法院否决的结果，个中原因需深入探究。

（一）数据跨境保护在欧盟内部的制度定位

1. 个人数据保护：从隐私权到独立的基本权利

梳理历史可以发现，在个人数据保护兴起之初及以后的相当长时间里，其在欧洲都被视为隐私保护在新技术条件下发展出的新维度，或者隐私权制度向信息处理尤其是自动化信息处理领域的延伸。欧洲理事会 1981 年《关于个人数据自动化处理的个人保护公约》（又被称为欧洲《第 108 号公约》）规定了个人数据质量、敏感数据、数据安全、数据保护与限制、个人数据跨境传输等个人数据保护制度。欧盟 1995 年《个人数据保护指令》第 1 条第 1 款即明确，在符合本指令规定的前提下，成员国应当对自然人的基本权利和自由，尤其是对与处理个人数据相关的隐私权加以保护。指令强调，调整个人数据处理国内法的目标是保护自然人的基本权利和自由，特别是《欧洲人权公约》第 8 条所确认的隐私权。隐私权的使命是捍卫个体生活的自主决定权，而个人数据保护所捍卫的信息自决权乃是其中不可或缺的组成部分。[1]

本世纪以来，伴随着互联网的高速发展，人工智能与大数据技术应用日益普及，欧盟立法者对个人数据保护的态度进一步强化。2000 年《欧盟基本权利宪章》第 8 条在第 7 条“隐私权”之外，单独将个人数据保护确认为一项基本权利。该条规定，任何人享有就与其相关的个人数据获得保护的权利；个人数据必须基于本人同意或法定事由得到公平处理，任何人有权查询其个人数据，并有权要求更正；个人数据处理的合规应当由一个独立机构负责。取代《个人数据保护指令》的《一般数据保护条例》指出，自然人在个人数据处理方面获得保护属于一种基本权利。该条例第 1 条第 2 款规定，保护自然人的基本权利与自由，尤其是其个人数据受保护的权利。

2. 欧盟的数据跨境流动调整机制

《一般数据保护条例》第 5 章对欧盟向第三国或国际组织转移个人数据

[1] The White House, “United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework,” March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/united-states-and-european-commission-joint-statement-on-trans-atlantic-data-privacy-framework/.

[2] The White House, “FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework,” October 7, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

[1] “BVerfGE 65, 1 - Volkszählung,” https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Gerichtsurteile_und_-beschluesse/bverfge_65_1_-_volkszaehlung.pdf.

作出规定，基本宗旨是确保自然人的数据出境后受到的保护水平不会被减损。为实现这一目标，条例作了详细规定，创立了复杂的机制。

在这套机制中，“保护充分性认定”居于首要位置。如果欧盟委员会认定第三国、该国的一个或多个特定部门或有关国际组织可确保充分（即与《一般数据保护条例》水平相当）的保护水平，则数据处理人可将个人数据从欧盟转移到该第三国或国际组织。这种基于“保护充分性认定”发生的数据流动不再要求任何具体的授权。为作出认定，欧盟委员会应当对目标国或国际组织进行全面评估并定期审查，评估时应特别考虑以下因素：相关领域的一般性和部门立法以及这些立法的实施、包括数据跨境流动规则在内的数据保护规则、专业守则和安全措施、判例法等，有效和可执行的数据主体权利、个人数据转移场合对数据主体的有效行政和司法救济；负责确保和强制遵守数据保护规则的一个或多个独立的监督机构的存在和有效运作，具有充分的执法权协助和建议数据主体行使其权利，并与欧盟成员国的监督机构合作；目标国或国际组织已作出的国际承诺，或因参加的有法律约束力的公约或文书、多边或区域机制而产生的其他义务，特别是在保护个人数据方面。

如果未获取欧盟委员会的“保护充分性认定”，那么只有在提供了适当保障措施的情况下，数据控制者或处理者才可以将个人数据转移到第三国或国际组织，且要满足数据主体权利可执行以及存在有效法律救济的条件。适当保障措施存在多种形式，最为重要的是依据《一般数据保护条例》第 47 条所规定的有约束力的公司准则、欧盟委员会或监管机构审核、采用的标准数据保护条款或根据《一般数据保护条例》第 42 条批准的认证机制进行的认证。

“隐私盾决定”的无效意味着欧洲企业不能以“保护充分性认定”为依据向美国传输欧盟的个人数据，美欧双方均难避免受到负面影响。美国跨国科技企业无法自由传输欧盟客户的数据，而欧盟企业在利用境外服务方面也可能遭遇明显障碍。早在“安全港决定”无效判决作出时，就有研究认为，因此导致的数据流通受阻会造成欧盟区内的国内生产总值下降 0.8%~1.3%。[1] 美欧双方存在努力寻求（例如通过《跨大西洋数据隐私框架》方式）重新达

[1] Yann Padova, “The Safe Harbour Is Invalid: What Tools Remain for Data Transfers and What Comes Next?,” *International Data Privacy Law*, Vol.139, 2016, p.140.

成合作的动力。

（二）美国个人数据保护制度的特点及问题

在美国，无论是立法还是司法审判层面，无论在公法还是私法领域，个人数据保护都是隐私权制度的组成部分。进入计算机与电信时代，个人数据保护被单独提上立法议程。在美国联邦和州一级的立法中，个人数据保护大多被冠以隐私保护之名。在晚近的司法判决中，诸如手机定位信息等个人数据被美国联邦最高法院认定为隐私信息。[1] 迄今为止，美国并不存在类似于欧盟《一般数据保护条例》或成员国个人数据保护法那样的联邦统一立法，有关个人数据保护制度分散于联邦或州的部门性法律中。近些年来，在个人数据保护的制度设计尤其是保护强度上，美国一定程度上显现出向欧盟看齐的态势。

在数据跨境流动领域，美国以《澄清境外合法使用数据法案》（简称 CLOUD 法）规定，美国企业在境外的经营活动只要与美国有足够的联系，执法部门即可以在一定条件下调取企业存储在境外的数据。如果外国监管部门想要调取美国本土数据，则需要达到法案规定的“适格外国政府”标准。对外国政府发出的调取数据的命令，CLOUD 法案有严格限制，包括不得侵犯言论自由、向美国提供相互访问数据的准入权利等，且美国保留停止外国政府调取数据命令的权力。简言之，该法案为美国本土监管部门调取他国数据规定了宽松的条件，却没有给予外国监管部门调取美国境内数据的同等权力，实际上是单边主义的霸权思维在数据跨境流动领域内的扩张。[2]

此外，在电子数据的监视和调取方面，美国存在着两套法律体系，即以 1978 年通过的《电子通信隐私法》（ECPA，后经过多次修正）为核心、适用于一般执法情形下的数据调取规定，以及以《外国情报监视法》（FISA）和第 12333 号行政命令（里根总统签署）等为核心、面向国家安全的数据监视和调取制度。后一套制度与数据跨境流动关系更为密切，因而成为欧盟法院“隐

[1] Carpenter v. United States, “138 S.Ct. 2206 (2018),” https://supreme.justia.com/cases/federal/us/585/16-402/ .

[2] 许可：《数据主权视野中的 CLOUD 法案》，《中国信息安全》2018 年第 4 期，第 40-42 页。

私盾决定”诉讼的审查对象。

《外国情报监视法》与第 12333 号行政命令等构成美国获取外国情报的制度框架。执法部门广泛援引的《外国情报监视法》第 702 条来源于该法 2008 年的修正法案，其授权美国情报机构出于保障国家安全目的，向美国企业收集、查阅外国人的通信，而提供信息的企业无需通知受影响的用户。该条同时规定了定位程序和伤害最小化程序，以确保监视仅针对外国公民，减少对美国公民数据的附带收集。美国政府称，第 702 条对保障国家安全、打击恐怖主义至关重要。[1] 第 12333 号行政令则授权美国国家安全局访问大西洋海底电缆，在数据抵达美国之前收集和保留传输的数据；根据该行政命令开展的活动不受成文法的约束。

《外国情报监视法》第 702 条没有对其赋予的、为获取外国情报目的实施监视计划的政府权力施加限制，也没有对可能成为这些计划目标的外国人提供充分的法律保障。第 12333 号行政命令和第 PPD-28 号行政命令（奥巴马总统签署）均未赋予数据主体在法院起诉美国当局的权利。因此，这两项行政命令给予外国人的保护亦未达到《欧盟基本权利宪章》所要求的水平。事实上，《外国情报监视法》及第 12333 号行政命令对数据监视和调取的规定相对宽泛和不透明，且缺乏司法监督，这一点即使在美国国内也受到人权组织的诟病。[2] 例如，依据《外国情报监视法》创设的外国情报监视法庭（FISC）负责批准情报部门的监视计划，但该法庭对监视项目进行年度整体性批准，而非个案审批，年度计划里只需说明监视的数据类别而非具体的目标个人的信息，且年度计划内容和 FISC 裁决均默认保密。据统计，FISC 从 1979—2019 年间共批准了 42947 项年度监视计划，仅否决了 135 项，其中 123 项还是在 2013 年“棱镜门事件”后予以否决的。[3]

[1] The Federal Bureau of Investigation, “Defending the Value of FISA Section 702,” October 13, 2017, https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702.

[2] American Civil Liberties Union, “Warrantless Surveillance under Section 702 of FISA,” November 1, 2022, https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa.

[3] The Administrative Office of the U.S. Courts, “The U.S. Courts Statistics & Reports,” November 30, 2020, https://www.uscourts.gov/statistics-reports/analysisreports/directors-report-foreign-intelligence-surveillancecourts.

由于上述法律和行政命令给予情报部门的宽泛授权，美国政府实施了数项大规模数据监听计划。按照《外国情报监视法》第 702 条开展的情报监视包括“上游计划”和“下游计划”（原“棱镜计划”）等。“上游计划”涉及美国情报部门对全球互联网骨干网的数据复制和过滤，包括元数据和通信内容；“下游计划”则要求美国企业向情报部门披露目标账户接收和发送的通信和数据。根据第 12333 号行政命令，美国情报部门也开展了大规模监视计划，收集数以亿计的移动电话位置记录、个人电子邮件中的通信录和地址簿等。此外，无论《外国情报监视法》第 702 条还是第 12333 号行政命令对情报的定义都相对宽泛，造成收集、保存和使用大量与国家安全无关信息的风险。[1]

综上，造成欧盟方面否定美国个人信息安全保证的原因，并不在于双方制度或价值观有所差异。恰恰相反，二者在这些方面并不存在本质区别。美欧个人数据跨境保护协议遭到否定也并非源于经济竞争中相互排挤的冲动，而是在于美国方面在保护个人数据免于来自公权力部门的不当干预上存在制度缺陷，尤其是对于境外个体数据保护的歧视性对待，基于惯有的霸权思维，将所谓美国国家安全片面地置于境外个体的基本权利之上。

四、美欧数据跨境流动之争的走向

结合欧盟法院作出的两次无效判决来看，美方关于数据跨境保护的新承诺仍然不无问题。虽然新的行政命令使用了欧盟法律的措辞即《欧洲基本权利宪章》第 52 条中的“必要”和“成比例的”，而不是第 PPD-28 号行政命令第 1（d）中使用的“尽可能量身定制”，以此向欧盟方面表明向其靠拢的诚意，但新行政命令并没有从制度上改变美方电子监控法律的内容，正在实施的大规模电子监控计划恐难有所改变。尽管欧盟法院两次宣布美国有关监控的法律和做法不构成“合比例”，然而新的行政命令并不禁止所谓的“批量监视”，从境外发送给美国网络服务商的数据仍将最终进入“棱镜计划”

[1] 参见张春飞、杨筱敏：《从＜欧美隐私盾＞协议失效看美国政府电子数据调取体系》，《信息通信技术与政策》2021 年第 1 期。

或“上游计划”收集范围。此外，行政命令中的“法院”也不是欧盟方面期待的真正意义上的法院。按照新行政命令的规定，个人数据救济机制将是一个两步程序，第一步由国家情报总监的官员进行处理，第二步由“数据保护审查法庭”加以裁决。但是，两者均非《欧洲基本权利宪章》第 47 条或美国宪法意义上的法院，而只是美国行政部门内的一个机构。新系统只是以前的“监察员”机制的升级版本，后者已被欧盟法院否定。基于以上理由，作为个人数据保护社会活动家的施雷姆斯表示，如果欧盟委员会对新行政命令给予肯定，可能再次引发诉讼。[1]

综观美欧围绕数据跨境流动议题博弈的全过程，可以得到的启示是，在数字全球治理领域，围绕数据跨境流动规则主导权而展开的各方博弈将日益突出，并将在较长一段时间内存在。在围绕数据跨境流动展开的美欧博弈中，欧盟一方握有一定的主导权，从每一次协议失效后美方均积极作出新的承诺即可看出。美国哥伦比亚大学法学院教授布拉德福德于 2012 年提出著名的“布鲁塞尔效应”理论。该理论认为，总部设在比利时布鲁塞尔的欧盟通过一系列调整市场经济的指令、规定，例如竞争政策、环境保护、食品安全、隐私保护或者社交媒体仇恨言论监管等领域的立法，使其影响力向全球市场渗透，相当程度上实现了单方面为国际商业环境确立标准的效果。所谓“布鲁塞尔效应”，就是全球商业市场的诸多重要方面呈现出行为标准欧洲化。这一现象也显示出欧盟依然拥有重要和独特的影响全球经济规制政策的力量。[2]2020 年 2 月，欧盟委员会连续发布了《塑造欧洲数字未来》、《欧洲数据战略》和《人工智能白皮书》三份数字转型战略文件，显示出争取国际数字经济规则主导权的强烈愿望，从一个侧面印证了“布鲁塞尔效应”的存在。

【完稿日期：2022-11-10】

【责任编辑：肖莹莹】

［1］ “First Reaction: Executive Order on US Surveillance Unlikely to Satisfy EU Law,” NOYB Organization, October 7, 2022, https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law.

［2］ Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020, p.14.