美欧跨大西洋数据流动的重启及其前景

程海烨　王 健

[内容提要] 2023年7月生效的《欧美数据隐私框架》是跨大西洋数据流动的第三次重大实践，意在进一步强化美欧数字联盟关系，扩大双方数字市场规模，并通过统筹两大法域法律规制的双向兼容性，制定有利于美欧利益诉求与监管偏好的跨大西洋数据流动规则。此次跨大西洋数据流动将为全球数字合作贴上“民主化”政治标签，挑战其他法域的数字规则话语权，加剧与中国数字市场竞争态势，并对多边机制参与全球跨境数据流动治理提出更高的要求。然而，该协议未对美国情报机构信息收集活动的必要性、相称性和补救机制的独立性作出规定，也未回应美国情报机构与欧洲数据保护机构间的利益冲突。由于美欧在数据保护机构的制度设计、跨国监管权力和技术可操作性等方面并不匹配，对其他跨大西洋数据流动机制存在的问题不够重视，跨大西洋数据流动前景还具有不确定性。

[关键词] 《欧美数据隐私框架》 跨大西洋数据流动 全球数字治理

[作者介绍] 程海烨，上海社会科学院国际问题研究所助理研究员，主要研究全球数字治理；王健，上海社会科学院国际问题研究所所长、研究员，主要研究中美关系、中国外交。

跨境数据流动与数据共享是各国发展数字经济市场的重要组成部分，也是促进颠覆性技术创新的关键来源。跨境数据流动的规则制定已成为全球数字治理的核心议题之一。然而，全球尚未形成统一的跨境数据流动规

制体系，跨境数据流动的全球治理呈现出监管规则多极化和规制标准俱乐部化，美欧两大数字经济体正在该领域扮演规则制定者和实践推动者等重要角色。《欧美数据隐私框架》（EU-U.S. Data Privacy Framework）是继《美欧安全港框架》（U.S.-EU Safe Harbor Framework）和《欧美隐私盾框架》（EU-U.S. Privacy Shield Framework）失效后，美欧通过联合政府部门和企业开展跨国协商与谈判，统筹关于数据存储、个人隐私保护、国家安全等国内外法律法规兼容性，促成跨大西洋数据流动的第三次重大实践。《欧美数据隐私框架》不仅是一份关于数据保护的重要政治声明，而且具有一定的法律效力，是美欧跨大西洋数据流动重启的标志。本文将在梳理《欧美数据隐私框架》主要内容的基础上，分析美欧跨大西洋数据流动重启的原因、影响及前景。

一、《欧美数据隐私框架》的主要内容

美欧跨大西洋数据流动可以追溯自2000年11月生效的《美欧安全港框架》，这是全球首个商用数据跨境流动协议，也是跨大西洋数据流动的首次重大实践。该协议提出7项关于数据保护的基本原则，是美国为兼顾《1995年欧盟数据保护指令》而实现商业数据跨大西洋流动专门设置的折中原则。[①] “棱镜计划”（Prism）和“施雷姆斯诉讼案I”（Schrems I）发生后，欧洲法院于2015年10月6日宣布该协议失效。2016年7月生效的《欧美隐私盾框架》是在《美欧安全港框架》基础上，通过新增16项具有同等约束力的补充性原则、新增跨国公司应承担的数据保护责任、明确参与

① 《美欧安全港框架》有3大支柱：一是包括涉及数据保护的7项基本原则；二是跨国公司和其他组织等应自愿并公开承诺遵守数据跨境流动的相关原则，并向美国商务部申请加入该协议，实施自我监管；三是由美国联邦贸易委员会受理并解决欧洲公民或企业的争端冲突，欧盟委员会将有权撤回欧洲数据保护机构的充分性调查结果。参见“U.S.-EU Safe Harbor Framework,” https://legacy.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf.

监督的责任主体、建立争端解决机制和联合审查制度等，解决美欧双方关于数据保护和国家安全等方面的平衡困境。[①]“剑桥分析事件”（the Cambridge Analytical Affair）发生后，欧洲法院对“施雷姆斯诉讼案II”（Schrems II）再次审查，指出“由于美国跨国企业脸书（Facebook）和谷歌（Google）等受到美国政府相关部门的过度监控，《欧美隐私盾框架》未对欧洲公民个人隐私提供充分性保护”，于2020年7月16日判决该协议无效。

《美欧安全港框架》和《欧美隐私盾框架》的两次失效，暴露了美欧就跨大西洋数据流动规则谈判亟待解决的三项重要问题：关于欧盟强调公民个人隐私保护和美国主张国家安全的优先性；关于美国情报机构应承担的监管责任，以及美国相关部门对数据充分性保护责任的划分；关于跨国企业自我认证模式合法性的质疑。鉴于跨大西洋数据流动对美欧数字经济稳定、包容和持续发展的重要性，双方继续为促成制度合作而努力。2023年5月11日，欧洲议会以306票赞成、27票反对、231票弃权，通过了《欧美数据隐私框架》所提供的充分性保护决议草案，该协议于7月10日生效。这意味着欧盟再次认同了美国对公民个人数据的保护能力与欧盟相当，美欧将再次实现跨大西洋数据流动、重建跨大西洋数字合作。

《欧美数据隐私框架》在原先两份协议的基础上做出改进与调整。一是新增具有约束力的7项补充原则，包括对数据获取和使用方的目的限制与选择、对个人数据按特殊类别处理的要求、确保数据使用的准确性和最小化原则、数据处理过程的透明度、个人权利的保障、对再次使用数据的限制以及事后问责等重要方面，弥补了之前原则中对数据处理细则模糊、缺少保障个人权利、未限制数据二次使用和转移等问题。

① “Safe Harbor Is Dead; Long Live the Privacy Shield?” https://www.americanbar.org/groups/business_law/publications/blt/2016/05/09_alvarez/.

二是设置一套新的规则和有约束力的多重监督机制，强化对美国情报机构的事后监管力度，进一步平衡保护公民隐私与国家安全之间的关系。《欧美数据隐私框架》的第3部分从法律基础、监管和补偿等三个方面，对美国公共机构以刑事执法和国家安全为目的收集与使用个人数据的行为加以限制和防范。据此，美国情报部门获取数据的权力接受以下三方面的约束。(1) 设置具有约束力的保障措施，将美国情报机构对数据的访问权限制在保护国家安全必要性 (necessity) 和相称性 (proportionality) 范围内；(2) 加强对美国情报机构活动的监督，确保对其监视活动进行限制；(3) 设置独立公正的“双层补救”机制，负责调查和处理关于美国情报机构获取数据而面临的投诉问题。美国相关部门以国家安全为目的收集和使用个人数据的法律基础，不仅包含《1978年外国情报监视法案》《第12333号美国情报行动行政命令》，还新增了拜登总统签署的《关于加强美国信号情报活动保障措施的行政命令》（简称《第14086号行政命令》），它将取代《第28号总统政策指令：信号情报活动》，成为美国确保对欧洲公民数据充分保护的另一项重要法律依据。同时，美国情报机构的活动将由多重机构负责监督，其中包括：每个情报机构内部设有负责定期监督的部门与保护公民隐私的官员、一名负责监督外国情报活动的独立监察长、在总统情报咨询委员会内成立的情报监督委员会、隐私和公民自由监督委员会，以及美国国会的情报与司法部、《1978年外国情报监视法案》规定的其他监管机构等。[①]

三是建立具有独立性和约束力的“双层补救”机制，为数据主体维护自身权益提供合法途径。美国政府建立了一个新的“双层补救”机制，具有

① “Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (Notified under Document C (2016) 4176) (Text with EEA Relevance),” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016D1250.

独立性和约束力。第一层是由美国国家情报总监下属的公民自由保护办公室对涉及侵犯公民隐私的行为进行初步审查，主要任务包括确保对公民自由和隐私保护已适当纳入美国情报机构的决策程序，监督美国情报总监遵守对公民自由和隐私的充分性保护要求，并进行相应的隐私保护评估等。审查完成后，美国国家情报总监公民自由保护办公室将发布需要适当补救的决定。若该决定不被违规者接受，则移交至数据保护审查法院进行第二次审查。数据保护审查法院是由美国司法部长根据《第14086号行政命令》设立的一个独立法庭，至少由6名法官组成，由美国联邦司法部长与商务部长、国家情报局长、隐私和公民自由监督委员会协商任命，任期4年。数据保护审查法院为保证裁决过程的独立性，不仅制定了多数投票表决等确保公正裁决的程序性规则，而且要求涉事的美国各行政部门都禁止干扰审查过程和结果。数据保护审查法院将对情报活动是否涉及公民个人隐私、公民自由保护办公室的判决是否合理以及其他补救问题等做出最终判决。此外，“双层补救”机制还将接受隐私和公民自由监督委员会年度审查。审查内容主要包括投诉情况的处理与评估、资料获取的充分性、执法的合法性以及情报机构遵守“双层补救”机制的审查结果情况等。该项年度审查报告将同时向美国总统、美国司法部长、美国国家情报总监和公民自由保护办公室、美国情报机构负责人、美国国会等提交，公开部分将提供一年一次的公众认证和监督。

四是将美国企业的自我认证机制和强制性承诺等引入跨大西洋数据流动规则，推广美国企业自我认证机制的国际合法性。自我认证机制包括初始自我认证 (initial self-certification) 与年度再认证 (annual re-certification) 两部分，需要满足的合规要求主要有：每年向美国商务部证明对《欧美数据隐私框架》原则的遵守情况、发布符合协议原则的企业隐私政策、提供独立的补救机制途径等，并允许美国联邦贸易委员会、美国运输部和其他

欧盟认可的美国机构调查与执法，监督其对规则的遵守情况。此外，美国商务部将推出“数据隐私协议计划网站”，帮助符合申报自我认证机制条件的美国跨国企业能够实现认证，促进其内部的个人数据跨境流动符合欧盟法律。同时，美国商务部将加入自我认证机制的跨国企业列入《欧美数据隐私框架》名单，并定期核实其提供的相关隐私政策与相关原则的相称性，还将提供相关的替代性争端解决机制。

五是进一步明确相关主体开展定期联合审查的分工和责任等细则。美欧双方对该协议执行情况展开定期审查的主体机制包括：主要负责管理和监督的欧盟委员会、欧洲数据保护机构和美国商务部，负责监督美国企业对协议执行情况的美国联邦贸易委员会等。美国商务部还将设置一个专门与欧洲数据保护机构的联络点，以便欧洲数据保护机构接到投诉时，能够与其立即展开联合审查。美国联邦贸易委员会将与欧洲数据保护机构交换审查信息并向相关涉事部门和企业做出回应，为欧洲数据保护机构提供执法援助。同时，还会优先考虑来自美国商务部和欧盟成员国，以及来自隐私和公民自由监督委员会和其他独立争端解决机构的隐私诉求和分歧等。[①]

二、美欧跨大西洋数据流动重启的动因

在全球数字规则制定中，跨境数据流动是数字地缘政治角力的主要焦点之一。[②]美国与欧盟作为引领全球数字规则与数字地缘政治走向的两大重要力量，迫切地推动跨大西洋数据流动重启，主要动因如下。

① “Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (Notified under Document C (2016) 4176) (Text with EEA Relevance),” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016D1250.

② 鲁传颖：《全球数字地缘政治的战略态势及其影响》，《当代世界》，2023年第5期，第37—43页。

其一，强化美欧数字联盟关系，形成合力以求主导全球数字地缘政治发展态势。“现在正是建立一个西方数字联盟，以应对相互联系却日益分裂的21世纪。”[①]从国家层面，美欧正统筹双边数字贸易规则，为重新整合全球跨境数据流动规则展开制度合作。除了联合国（UN）、经合组织（OECD）、亚太经合组织（APEC）和世贸组织（WTO）等，二十国集团（G20）、七国集团（G7）、《全面与进步跨太平洋伙伴关系协定》（CPTPP）和《区域全面经济伙伴关系协定》（RCEP）等多边机制也成为美欧推动双边数字规则合作的重要平台。同时，《美日数字贸易协定》和《美墨加协定》并行，美国正不断加强与盟友的跨境数据流动合作；“英美数据桥”（UK-US Data Bridge）将在2023年10月21日生效，英国组织能够将个人数据传输到获得“欧美隐私框架的英国扩展”认证的美国组织，也不必再接受风险评估。欧盟与日本也将跨境数据流动规则纳入了经济伙伴关系协定谈判。此外，美欧各情报机构在打击恐怖主义、打击跨国刑事与金融犯罪等领域实现了跨大西洋情报机构数据共享与合作机制，形成了跨大西洋情报机构联盟关系。在美国国家安全局和欧洲刑警组织推动下，美欧签署了3份《乘客姓名记录协议》，要求欧盟向美国国土安全部提供乘坐客运航班的旅客个人信息等，确保国土安全；《追踪恐怖分子融资计划》将帮助美欧情报与安全部门提取国际银行通过SWIFT系统传输的部分数据；《保护伞协议》则为美欧警察和刑事司法等执法合作建立了全面与高水平的数据保护框架。欧洲刑警组织还与美国签署关于个人数据调查与互换的补充性协议，加强双方数字战略和通信技术的交流与合作。

其二，扩大美欧两大经济体的数字市场规模。2021年，美国数字经济规模达15.32万亿美元，蝉联世界第一；中国、德国、英国、法国等数字经济

① “Time for a U.S.-EU Digital Alliance,” https://www.brookings.edu/articles/time-for-a-us-eu-digital-alliance/.

体规模分别为7.06万亿美元、2.88万亿美元、2.17万亿美元和1.37万亿美元，排在全球第2—5名。[①]跨大西洋数据流动也正不断为美欧创造超7.1万亿美元的经济价值，所在地为欧洲的超过90%的公司都需要与美国接收或传输数据，涉及包括推特、谷歌、脸书和亚马逊等科技巨头在内的5300多家公司。[②]据估计，每年持续的数据流动将支撑跨大西洋9000亿美元的贸易额。[③]美国数字企业占全球前100个数字平台总价值份额的67%，欧洲仅占3%。[④]美国既是欧洲数字化服务的最大市场，也是欧洲最大的数字产品与服务提供商。美国和欧洲大约一半的数据需要通过跨大西洋进行传输流动。在美欧数字贸易中，美国进出口分别占39%和32%。[⑤]2018年，跨大西洋数字贸易总额约为2950亿美元。其中，美国分别向欧盟出口和进口的金额为1880亿美元和1070亿美元。[⑥]《欧美隐私盾框架》的终止导致欧盟出口减少约4%、每年约降低GDP增长1%左右。累计至2030年，欧洲将损失达1.5万亿美元，影响130万个工作岗位。相比之下，如果欧盟和主要贸易伙伴采取措施促进跨境数据流动，欧盟整体出口额将增长2%以上，每年GDP增加0.6%，即约增加70万个就业岗位，到2030年将累计价值达8520亿美元。[⑦]

① 英国脱欧后，欧盟数字经济规模总量与中国相当。参见《全球数字经济白皮书（2022年）》，中国信息通信研究院，2022年12月，第13—14页。

② Daniel S. Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2023: Annual Survey of Jobs, Trade and Investment between the United States and Europe,* Foreign Policy Institute, Johns Hopkins University, 2023, p.72.

③ "Trans-Atlantic Data Privacy Framework," https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.

④ *Digital Economy Report 2021 Cross-border Data Flows and Development: For Whom the Data Flow,* UNCTAD, 2021, p.22.

⑤ Daniel S. Hamilton and Joseph P. Quinlan, *The Transatlantic Economy 2020: Annual Survey of Jobs, Trade and Investment between the United States and Europe,* Foreign Policy Institute, Johns Hopkins University, 2020, p.33.

⑥ "Table 3.3. U.S. Trade in ICT and Potentially ICT-Enabled Services, By Country or Affiliation," https://apps.bea.gov/iTable/?reqid=62&step=9&isuri=1&6210=4#eyJhcHBpZCI6NjIsInN0ZXBzIjpbMSw5LDZdLCJkYXRhIjpbWyJQcm9kdWN0IiwiNCJdLFsiVGFibGVMaXN0IiwiMzU5Il1dfQ==.

⑦ *The Value of Cross-Border Data Flows to Europe: Risks and Opportunities,* Frontier Economics Ltd, June 2021, p.6-7.

其三，统筹美欧两大法域关于数据跨境流动规则的内部与涉外法律法规双向兼容性，塑造更加持久和稳定的跨大西洋数字合作。如何平衡数据主权、数据自由流动、个人隐私保护和国家安全是美欧两大法域统筹国内与涉外法律法规的关键。美国重视数字经济和国家安全，依赖市场自由竞争、跨国公司自我监督和消费者自我保护。美国信奉的是“私人诉讼和市场自我监管”体系，对监管行动的成本更为敏感，普遍适用的美国联邦法律难以得到民众的支持。[①]由政府部门开展事中与事后审查、行业自律是美国情报部门维护数据安全、科技巨头在欧洲市场扩张的政策导向。迄今为止，美国尚未从联邦层面制定统一的隐私保护法案，主要通过行业立法和州立法规范特定行业、特定类别或各州的隐私权力，《美国数据隐私和保护法案》距离正式立法还有一定距离。此外，美国并未设置专门的数据隐私监管机构，以分散的“多重叠加监管模式”为主。例如，美国国土安全部、美国商务部下属的国际贸易管理局、美国联邦贸易委员会、美国国家情报办公室等都是跨境数据流动机制的监管主体。与之相比，欧盟将保护个人隐私放在首位，监管是迄今为止欧盟最重要的手段。欧盟充分依赖严苛法律下的“政府干预和监管机构执法”模式，要求数据跨境流动去向为第三国，应保证其拥有符合欧盟规定的充分数据保护能力。[②]此外，欧盟还制定了《数字服务法案》《数字市场法案》《数据法案》《数据治理法案》等其他对数字市场规制的法律，并成立欧洲数据保护委员会、欧洲数据保护机构等专门监管机构。因此，《欧美数据隐私框架》是美欧两大法域将不同监管模

① Tom Romanoff, “Comparison of Competition Law and Policy in the U.S., EU, UK, China, and Canada,” https://cubeworldwide.com/uk-and-eu-competition-policy.

② 最鲜明地体现在《1995年欧盟数据保护指令》（EU Data Protection Directive 1995）第25条和《一般数据保护条例》（General Data Protection Regulation）第24条“充分性决定”（an adequacy decision）。参见“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/legal-content/EN/TXT/?uri=celex%3A31995L0046. “General Data Protection Regulation, GDPR,” https://gdpr-info.eu/.

式再次碰撞的实质性成果，将有助于美欧诸多机构开展多方位监管合作，更进一步了解双方的利益诉求。在不断完善本法域安全机制、司法机制、监管机制等顶层设计的同时，逐步获得跨大西洋信息情报、数据保护、司法救济等重要机构的跨国合作与协调经验，提升美欧数字合作的持久性和稳定性。

其四，加强跨境数据流动规则的主导权和控制权，并通过跨大西洋数据流动实现双方利益诉求。美国将“美式民主”价值观置于国际数字合作首位，将实现美国国家安全和数字霸权看作重要战略目标，将数据流动视为重塑全球数字经济的关键支柱。欧盟则将尊重并保护公民隐私权置于国际数字合作首位，将形成统一的数字化单一市场和实现欧洲数字主权看作重要战略目标，将强化监管权力作为延伸其数字战略的手段之一。美欧对于数据跨大西洋流动的利益诉求、数据安全观和监管机制均存在明显差异，最终形成不同的数据流动监管机制。因此，双方都希望促成有利于自身监管偏好的跨大西洋数据流动规则。《欧美数据隐私框架》兼顾了欧盟强调数据保护和美国重视国家安全的双重目标。例如，《美欧安全港框架》《欧美隐私盾框架》和《欧美数据隐私框架》都应确保符合欧盟《一般数据保护条例》对数据的“充分性保护”要求。与此同时，《欧美数据隐私框架》也将《第14086号行政命令》提倡的三项重要改革内容纳入其中，即“对美国情报机构收集信息情报活动增加进一步的限制措施”“创建一个独立且具有约束力的两级审查和纠正机制，分别是国家情报总监办公室的公民自由保护官和数据保护审查法院”“赋予专门的隐私监督委员会参与监督审查机会”等。[①]

① *Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*, White House, October 7, 2022.

三、美欧重启跨大西洋数据流动的影响与前景

《欧美数据隐私框架》是美欧进一步将“本法域政策需求”与“其他法域监管规则”相匹配的产物，也是双方再次为跨大西洋监管机制差异性作出协调与让步，塑造同时满足数据自由流动、个人隐私保护和国家数据安全的新型数字合作机制，将再次影响全球跨境数据流动的治理与实践。

（一）为全球数字合作贴上“民主化”政治标签，用意识形态挤压其他法域数字发展空间。当前，全球数字地缘政治正加速形成区域多极化分散博弈的态势，北美、东亚和欧洲地区在数字发展战略上取得领先优势，中东、非洲等地区正加快缩小与发达经济体的数字鸿沟。鉴于数字发展对数字基础设施、数据存储、数字技术、人才培训等方面的依赖，数字发展弱的区域将更加依赖于数字发展强的地区或国家。区域性国家借助与数字大国开展多领域数字合作的方式，成为参与全球数字空间规则制定、获得数字发展支持的重点。在此背景下，跨大西洋数字合作的首要目的是建立基于“美式民主”的数字联盟伙伴关系，核心内容涉及科技创新发展、数据共享与流动以及数字安全三大支柱。[①]根据《数字战略（2020—2024）》，美国已与盟友和伙伴国家共建“数字民主俱乐部”，为全球数字合作贴上“美式民主”的政治合作标签。同时，欧盟也将塑造以欧洲人权为中心、以欧洲民主为基础的数字秩序，确保欧盟与其他合作伙伴在全球数字地缘政治合作中的安全性。部分国家要求对数据实现本地存储的行为则被西方国家看作是“数字铁幕制度”和“数字保护主义”。[②]跨大西洋数据流动的重启在一定程度上是追求西方民主和人权的国家之间寻求合作的一种政治表态，意在用西方民主国家的价值观重塑全球数字地缘政治格局，承认西方民主化

① 郎平：《全球数字地缘版图出现端倪》，《信息安全与通信保密》，2021年第3期，第9—15页。

② “The Geopolitics of Technology: How the EU Can Become a Global Player,” https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/.

意识形态则是美欧今后在全球数字规则博弈中要求其他国家或地区选边站的首要态度。

（二）进一步提升美欧制定全球数字规则权力，形成两大法域驱动下的全球跨境数据流动规则，挑战其他法域制定数字规则话语权。美欧已从国家层面实现塑造跨境数据流动规则的两条路径：一是制定与本法域偏好一致的数据保护机制，凭借庞大的市场规模优势向其他法域推行该规则，形成全球监管影响力，如欧盟《一般数据保护条例》通过建立“白名单”制度扩大域外法律适用范围等；二是向多边机制输出倾向其自身利益偏好的治理理念与模式，提升规则的适用性与国际认可度，如美国在APEC下设置跨境隐私规则（Cross Border Privacy Rules）体系，向其他国家或地区输出禁止数据本地存储、实施企业自我监管认证机制等偏好的跨境数据流动规则。此次美欧之间再次就跨大西洋数据流动达成共识性协议，标志着双方启动第三条路径，即摒弃两大法域不同的利益诉求和数据规则优先项，促成求同存异的双边共识性协议，建立相互信任、包容与持久的跨大西洋数据流动规制体系。上述三条路径均成为他国模仿的对象，对于不符合美欧数据流动规则的法域将受到反对与抵制。例如，加入欧盟“白名单”的法域应遵从欧盟数字市场法律法规，否则无法与之开展跨境数据流动；加入APEC跨境隐私规则体系也应与美国同样支持数据自由流动的优先性；跨大西洋数据流动规则也将成为国家间跨境数据流动“模板”，甚至影响《区域全面经济伙伴关系协定》《数字经济伙伴关系协定》《全面与进步跨太平洋伙伴关系协定》等多边机制相关规则。

（三）《欧美数据隐私框架》将美国推崇的企业自我认证模式和欧盟严苛的监管规则相结合，是美欧两大法域间软法与硬法碰撞的又一次海外实践，这将加剧与中国数字市场竞争态势。美国已将私营企业主导、获取数字资产和建立开放的数字市场等看作与他国开展数字竞争的三种重要手

段。少数占主导地位的数字科技企业在行业规则制定中占主导权，它们将隐私视为个人私有可交易财产，而私营企业和自由市场则是保护隐私正常交易的最有效机制。因此，依托消费者自我保护和企业自我认证等软法，是美国认为促进行业发展且最具吸引力的有效机制。科技行业自我认证实践已在美国内部取得显著成效。2022年全球领先科技企业前10排名中，美国科技巨头企业共7家。[①]其中，谷歌、微软、推特等数字科技企业已加入“数字信任和安全伙伴关系”（Digital Trust and Safety Partnership）。《欧美数据隐私框架》也意味着美国推崇的企业自我认证模式得到欧盟的认可，跨国科技企业可以合理合法地在欧洲市场“复制”该模式，降低合规成本、提升投资份额、赢得更多的数字经济收益。

与此同时，该协议打破了欧盟坚持欧洲标准的严苛监管模式，承认美国推崇的企业自我认证模式也体现出欧盟愿意探索更加灵活、开放和自由的数字市场环境，吸纳更多数字经济体开展数字合作。相较美国与中国，欧洲科技企业相对发展较慢。美国科技企业已占据欧洲市场大部分份额，在数字科技企业全球排名前10中也较少出现欧洲科技企业。2020年，美国的数据存储量位列世界第一，占全球39%；中国占10%位列第二。[②]欧盟意识到依赖监管权力和市场规模无法最终赢得全球科技竞争。中美紧张的数字竞争局势成为欧洲提升自身数字发展的额外动力，欧洲还将成为中美争夺数字技术和数字经济发展的重要市场。对此，欧盟选择先与美国共同促进跨大西洋数据流动，加快推动欧洲企业的数字化转型，并通过获得美国跨国企业在欧洲本地数据存储机会，提升欧洲数字市场的数据资产。此外，美欧两大法域间不同监管模式的尝试还将吸引美国主导的APEC、OECD、G7等成

① 台积电（TSMC）、腾讯（Tencet）和三星（Samsung）分别位于第6、8、10位，其余均为美国科技企业。参见“Leading Tech Companies Worldwide 2022, By Market Capitalization (in Billion U.S. Dollars),” https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/.

② “Geopolitics of Digital Power Infographics,” https://www.tni.org/en/geopolitics-of-digital-power.

员国，以及《一般数据保护》“白名单”国家加入，再次增加数据向中国流动的合规成本、增加中国开展跨境数据流动规则协调的可操作难度。

（四）跨大西洋数据流动呈现参与主体多元化、涉及规则多样化等特点，对多边机制参与全球跨境数据流动治理提出了更高的要求。美国情报部门和欧洲数据保护机构是两大参与主体，包括欧盟委员会、欧洲数据保护机构和美国商务部等在内的多个部门还需参与定期跨国审查与监督。同时，跨国数字巨头在美欧两大法域内的游说作用也不可忽视。苹果、爱立信、诺基亚、飞利浦和三星等“数字欧洲”（Digital Europe）游说团体成员是推动欧盟向美国传输数据的重要支持力量。此外，跨境数据流动涉及包括数据主权、网络安全、个人隐私保护、跨国平台监管、数字技术等多项具体规则的制定、落地与实行。基于美欧推进跨大西洋数据流动的实践经验，以UN、WTO、OECD、APEC等为代表的多边机制不仅要为相关部门提供跨国跨域协商的机制平台，而且要为代表不同利益诉求主体提供相应的解决方案、为不公平案件提供合理的上诉途径，并塑造更加独立的监督机制等。这对上述多边机制治理全球跨境数据流动是一次重要考验。

然而，《欧美数据隐私框架》仍存在诸多不可忽视的缺陷，也为跨大西洋数据流动的前景增添不确定性。

第一，《欧美数据隐私框架》是为了解决“施雷姆斯诉讼案II”中的两个关键性问题，即美国是否对情报收集活动进行“必要且相称”的行动，以及如果公民认为其个人数据被不合法地收集或使用，是否有向美国政府寻求一个客观且独立机制进行相应补救的渠道。[①]针对第一个问题，尽管该协议对美国情报机构收集公民个人数据和信息等活动进一步提出限制，但对于收集与保护数据的必要性与相称性判断定义模糊，相关机构的主观判

① “Privacy-Heading for Schrems III,” https://www.csis.org/analysis/privacy-heading-schrems-iii.

断权更大。这意味着收集欧洲公民信息的主动权仍在美国情报机构，不同的监管机构还将产生差异性决策结果。针对第二个问题，数据保护审查法院的独立性也令人质疑。尽管美国在第二层补救机制中设置了独立的数据保护审查法院，但其任命的法官大多由美国司法部长、美国隐私与公民自由监督委员会、商务部长和国家情报局局长等协商任命，其部门与欧洲数据监管机构均有对接和联系，所涉及的事务也牵涉相关部门实际利益，因而该补救机制难以做到判决独立。这一缺陷将引起双方涉事部门的数字信任危机。

第二，《欧美数据隐私框架》未对以维护公民隐私权为首的欧洲数据保护机构、以保护国家安全为主的美国情报机构两者之间不同的利益诉求和监管冲突予以充分且明确的回应，也尚未设置实质性惩罚措施。欧盟的核心关切是如何在保护个人数据隐私的前提下实现数据跨境流动，而美国的首要目标则是兼顾数字经济发展和维护国家安全，该目标远胜于对公民个人隐私的保护。美国情报机构参与跨大西洋数据流动的目的，就是获得更多欧洲公民的数据并实施监控，而这种行为则被欧洲数据保护机构看作是侵犯公民隐私权。此次《欧美数据隐私框架》借鉴了《第14086号行政命令》对美国情报机构收集信息活动进一步限制，但未明确阻止此类行动，也尚未提及此类行动对公民隐私权的侵犯。尽管该协议通过了“充分性决定”，但欧洲数据保护委员会认为，美国通过前置性地为情报机构收集信息活动而建立符合欧洲要求的隐私和公民自由保障措施，目的是达到后期与欧洲开展更加信任、稳定的跨大西洋数据自由流动。即便《欧美数据隐私框架》提及对美国情报机构收集欧洲公民个人数据作出限制，但其涉及与欧盟“基本等同”的数据保护能力、符合欧盟“必要与相称”的标准等，并没有从法律意义上对欧洲公民的数据实施相应保护。此外，该协议仅提及监管机制和“双层补救”机制，却忽视了对美国情报机构和数据监管与执法部门

访问数据的具体行为等进行必要的规制，也没有明确对数据处理者的惩罚措施或原则等。当相关行为违背或侵犯公民隐私保护时，欧盟仍将会单边实施《一般数据保护条例》以及其他数字监管法律，致使《欧美数据隐私框架》对侵犯公民隐私的行为不具备实质性威慑作用。

第三，美欧在数据保护机构的制度设计、跨国监管权力和技术可操作性等方面不匹配，将造成美欧各部门对跨大西洋数据流动监管混乱的局面。已有31个欧洲国家设置独立的数据保护机构，专门对跨国企业数据保护行为的合法性进行监管。[①]而美国则将数据保护行为纳入各政府部门管辖，并未设置专门的数据保护机构与欧洲数据保护机构进行对接。根据《欧美数据隐私框架》，为确保双方的监管差异不会阻碍跨大西洋数据流动，该协议强调行业的自发性监管，却未设置专门与欧洲数据保护机构对接的特殊部门，也未赋予数据保护机构对违反隐私保护规则企业的跨国监管权力。美国仅在联邦贸易委员会和商务部下属的国际贸易管理局等配置与欧洲数据保护机构的联络点，向欧洲数据保护机构回应相关审查与投诉的情况。同时，面对美国不合规的数据保护行为，欧洲数据保护机构并没有跨国监管权，依据“双层补救”机制，只能向美国国家情报总监下属的公民自由保护办公室提议初步审查。美国联邦贸易委员会和商务部就欧洲数据保护机构起诉的调查都将基于《美国安全网络法案》等国内法律法规，与欧洲数据监管机制建构并不一致。此外，美欧对于数据安全和隐私保护的可操作性技术行动侧重点不同。美国强调技术服务于有效监管的操作性。试图借助全球跨境隐私规则论坛，推广“保护隐私数据共享和分析”（PPDSA）技术，并借助其数字技术优势实现跨境数据自由流动的技术霸权。欧盟则重视监管机构在合规情况下用技术手段执法的重要性。欧盟正

① “Our Members,” https://edpb.europa.eu/about-edpb/about-edpb/members_en#member-at.

在《一般数据保护条例》基础上强化欧洲数据保护委员会的更多监管职责，包括对公共部门使用“云服务”的协调执法、加强数据监管战略合作、协助开展执法活动等。这将造成美欧双方监管机构在技术审查中的混乱。

第四，《欧美数据隐私框架》是跨大西洋整体性适用协议，忽视了其他数据流动机制存在的问题。除《一般数据保护条例》第45条“充分性决定”，欧盟还根据第46条确立了标准数据保护条款、公司规则、行为准则和认证机制等四类替代性数据跨国传输的工具。当第三国未通过欧盟充分性保护认定时，可在提供适当保护的前提下通过替代性方案实现从欧盟向境外传输数据。[①]此前，欧洲法院判决《欧美隐私盾框架》失效，但支持标准合同条款（Standard Contractual Clauses）作为有效的替代性数据流动机制。至少有20项标准合同条款（草案）等涉及跨境数据流动，涵盖约71个国家和地区。标准合同条款也成为美国、欧盟和其他法域向第三国传输个人数据的最广泛使用的法律机制之一。据估计，通过标准合同条款从欧盟向美国传输数据达94%，信息通信技术行业占37%。美国数字科技企业是签订该条款最大的用户。一旦跨国公司无法在美欧运营地区间顺利传输数据，将极大影响其提供服务的质量和方式，大量依赖跨大西洋数据流动的美国数字产品和服务企业也将面临合规成本高涨、与欧盟本土企业相比竞争力下降、遭遇更多数字经济损失等局面。因此，美国数字企业更依赖通过标准合同条款进行跨境数据流动实践，且更加关注这一替代性方案的执行风险。部分美国数字企业质疑标准合同条款存在数据保护机构过度监管、缺乏独立的上诉与补救机制等问题，认为标准合同条款逐渐提高了欧盟向境外输出与分析数据的成本和制度复杂性，欧洲正进一步向数据保护本地化倾斜。爱尔兰数据保护机构曾以脸书传输个人数据未符合《一般数据保护

① 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》，《欧洲研究》，2021年第4期，第89—109页。

条例》为由，向爱尔兰高等法院提起诉讼，要求其暂停向美国传输欧盟用户数据。[①]谷歌、亚马逊（Amazon）、苹果（Apple）等美国科技公司也因被列入欧盟“超大型”在线平台或搜索引擎名单而面临欧洲数据保护机构更加严苛的监管。亚马逊还向爱尔兰高等法院提起诉讼，表达对美欧间数据流动机制的监管环境不满，并抵制欧盟对数字内容的过度监管行为。[②]然而，上述诉求未在此次跨大西洋数据流动谈判中得到回应。

结语

《欧美数据隐私框架》标志着跨大西洋数字合作步入新阶段，也为制定全球跨境数据流动规则贡献了更多的实践经验。该协议主要回应了“施雷姆斯诉讼案II”的两个关键问题：一是要求美国情报机构对信息收集活动进行“必要且相称”的行动，二是如果公民认为其个人数据被不合法地收集或使用，美国政府应提供一个客观且独立的机制进行相应补救。对此，该协议在前期共识的基础上，主要提出了五项改进内容。美欧重启跨大西洋数据流动，不仅进一步深化美欧双方数字联盟关系、扩大数字市场规模，而且能够统筹两大法域法律规制的双向兼容性，建立有利于美欧利益诉求与监管偏好的跨大西洋数据流动规则。与此同时，跨大西洋数据流动的重启也为全球数字合作贴上西方“民主化”政治标签、挑战其他法域制定数字规则话语权、加剧美欧与中国数字市场竞争态势，并对多边机制参与全球跨境数据流动治理提出了更高的要求。不过，执行《欧美数据隐私框架》仍存在一定缺陷，例如该协议并未确保美国对情报收集活动的必要性、相

① “The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade,” ITIF, December 17, 2022.

② “Amazon Launches First U.S. Challenge to EU Content Rules and Says It Would Be ‘Unfairly Singled Out’,” https://www.cnbc.com/2023/07/11/amazon-launches-first-us-challenge-to-eu-content-rules.html.

称性和补救机制的独立性，也尚未回应欧洲数据保护机构和美国情报机构两者间利益冲突。美欧在数据保护机构的制度设计、跨国监管权力和技术可操作性等方面并不匹配，以及对其他跨大西洋数据流动机制存在的问题不够重视，跨大西洋数据流动前景还具有不确定性。

未来，跨大西洋数据流动是竞争与合作并存的发展趋势。但总体上，美国仍在重塑全球数据治理体系中占据较大优势，中国与美欧在跨境数据流动治理的立场上有相似之处，并非完全对立。当前，中国的跨境数据流动规制体系尚处于调整与优化阶段，如何在保护数据安全和发展数字经济两者中实现平衡，既是当前中国探寻跨境数据流动规则的重要考量，又是在跨境数据流动治理新格局变化中保持国际竞争力的核心议题。对此，中国可做以下应对。一是基于《全球数据安全倡议》，打破以西方民主意识形态谈合作的思维模式，提出全球跨境数据流动治理倡议。二是持续向既有多边机制APEC、G20和WTO等输入有利于中国跨境数据流动的规则偏好，并在《区域全面经济伙伴关系协定》《数字经济伙伴关系协定》和《全面与进步跨太平洋伙伴关系协定》等多边机制中争取更多的跨境数据流动规则谈判机会。三是拓宽数据流动“朋友圈”，同建设“数字丝绸之路”的国家（地区）以及金砖国家等推进跨境数据流动规则协调与合作。四是与美欧畅通双边或多边数字经济合作，明确在数字经济领域的共同利益与机制互补可能性，寻找更广泛的数字合作空间。五是形成与本国数字经济市场规模相匹配的数据监管机制，强化对数据出境后的监管审查机制，并加快统筹国内法治和涉外法治双向兼容性，为跨境数据流动营造更加安全、包容、可持续的规制环境。■

（责任编辑：王锦）

commercial space sector, the continuous incubation of lunar technologies and capabilities, the success of the COTS program, and the launch of Artemis program. As a double-edged sword, it not only impacts the traditional pattern and paradigm of lunar exploration, extends the space economy from earth orbit to cislunar space and promotes internationalization of lunar commercialization, but also poses risks to NASA, commercial lunar companies and the international community.
Keywords:
US, Lunar, commercialization, space

Prospects for Reactivating Transatlantic Data Flows between the US and Europe

Cheng Haiye and Wang Jian

Abstract:
The EU–US Data Privacy Framework is the third major exercise in transatlantic data flows. The relaunch of the transatlantic data flow is intended to further strengthen the US–EU digital alliance, expand the scale of the US–EU digital market.By integrating the two-way compatibility of legal regulation, it is possible to establish rules for cross-border data flows that are conducive to the interests and preferences of the United States and Europe. The transatlantic data flow will label global digital cooperation as democratization politics, challenge the right of other jurisdictions to make digital rules, intensify the competition with China's digital market, and put forward higher requirements for multilateral mechanisms to participate in the governance of global cross-border data flow. However, the agreement does not ensure the independence of US Intelligence Agencies' information-gathering activities and remediation mechanisms, nor does it address the conflicting interests of European Data Protection Authorities and US Intelligence Agencies. The mismatch between the United States and Europe in terms of the institutional design of data protection agencies, transnational regulatory powers and technical operationalization, as well as the neglect of the problems of other transatlantic data flow mechanisms, will add further uncertainty to the prospects for transatlantic data flows.
Keywords:
EU–US Data Privacy Framework, Transatlantic Data Flows, global digital governance

The US–Japan Semiconductor Cooperation and Its Limits

Li Jinfeng

Abstract:
The Biden Administration has comprehensively strengthened its cooperation with Japan. The United States and Japan have established several high-level semiconductor cooperation mechanisms. At the bilateral level, the governments of the US and Japan have expanded cooperation fields. Multilaterally, the two countries wooed developed countries and China's neighboring countries to formulate key technical standards. In addition, the United States and Japan have substantially deepened their cooperation with Chinese Taiwan on semiconductor industry and jointly intervened in the Taiwan question. The motivationsbehind is that the both United States and Japan urge to reshape the semiconductor industry chain and supply chain, and donot want to see the rapid development of China's semiconductor industry.Besides, the global nature of the semiconductor industry determines that the United States and Japan must cooperate to achieve their goals. The essence of US–Japan semiconductor cooperation is to weaponize industrial issues, which not only has a bad impact on the stability of the global semiconductor industry chain and supply chain, but also threatens China's economic interests and national security. However, the US–Japan cooperation is restricted by multiple factors, including the conflict of US–Japan's identical goals of reviving domestic semiconductor manufacturing, the US–Japan divergences on the goals and implementation of their China policies, and the constraints from the third parties such as Chinese Taiwan, South Korea, and the European Union. To mitigate the adverse impacts, China needs to strengthen external strategic dialogues, deepen cooperation with the global semiconductor supply chain, and enhance the resilience and competitiveness of domestic semiconductor industry.
Keywords:
US–Japan alliance, economic security, semiconductor supply chain, Sino–US strategic competition