

美欧数据跨境流动合作机制的演进及其启示

彭德雷 杨莹泽

(华东理工大学, 上海 200237)

摘要: 发展数字贸易是中国建设贸易强国的必然要求。当前, 数据已成为重塑全球经济结构的关键资源, 数据跨境流动成为开展数字贸易的关键因素。在数据跨境流动合作议题下, 美欧先后签订《安全港协议》《隐私盾协议》和《数据隐私框架》, 虽历经波折, 但基本形成了数据跨境流动的跨大西洋合作机制。美欧在数据保护议题中的价值主张、立法体系等差异是双方合作存在的主要分歧, 而对行政措施监管以及权利救济的不足则成为影响双方合作发展的重要原因。由于美欧数字贸易市场相互深度依存, 双方近年来通过不断协商使得合作机制渐趋成熟与完善。观察美欧长达数十年的数据跨境流动合作机制的演进和主要特征, 有助于中国更好地推进数据跨境流动合作, 推动数字贸易发展, 更好地支撑贸易强国建设。

关键词: 数据跨境流动; 数字贸易; 《数据隐私框架》

中图分类号: D996.1

文献标识码: A

文章编号: 1006-1894 (2025) 05-0085-15

一、问题的提出

当前数据跨境流动的国际秩序正处于新旧交替时期, 数据跨境自由流动有助于降低交易成本、更高效地开展国际贸易, 推动数字经济发展, 但也带来一系列风险和挑战, 包括数据安全、个人隐私保护和数据合规监管等。构建数据跨境流动合作机制是保护数据安全和隐私、减少国际贸易壁垒、共享数字经济的关键路径。目前, 国际数据跨境流动合作格局呈现多样化发展的特点, 各国和地区根据自身发展需求和战略目标开展合作。美欧从签订《安全港协议》(Safe Harbor Framework)、《隐私盾协议》(Privacy Shield Framework)到《数据隐私框架》(Data Privacy Framework), 虽几经波折, 但基本形成了数据跨境流动的跨大西洋合作机制。该机制不仅为双方企业提供了广阔的市场空间, 促进双方投资和贸易便利化, 也为全球数据治理提供了一种合作框架。

在实践中, 数据跨境流动的安全与风险受到越来越多的关注。例如, 美国强制要求字节跳动剥离旗下应用程序 TikTok 在美国的业务。美国政府认为 TikTok 可能

作者简介: 彭德雷, 华东理工大学法学院教授, 博士生导师, 研究方向: 国际法、数字贸易、跨境数据流动; 杨莹泽 (通讯作者), 华东理工大学法学院博士研究生, 研究方向: 国际法、数字贸易。

基金项目: 国家社科重大课题“完善我国条约司法适用制度研究”(项目编号: 23&ZD167); 上海市高水平机构建设运行计划“软科学研究”项目“以制度型开放推进高水平国际科技合作的对策研究”(项目编号: 25692101700); 上海市人民政府决策咨询研究基地重点专项课题“上海完善促进数字贸易发展的制度体系研究”(项目编号: 2025-JD-11)。

会使中国政府获取并控制大量美国个人数据,从而使中国在数据跨境流动治理中处于优势地位。^①可见,数据跨境流动被卷入大国博弈的时代漩涡,成为中国企业海外投资无法回避的问题。构建数据跨境流动的信任和合作机制,对于企业跨国经营而言变得更加紧迫。

有鉴于此,中国政府正在积极开展数据跨境流动治理。在国内层面,出台《网络安全法》《数据安全法》《个人信息保护法》等相关法律,形成数据分类分级管理的顶层设计框架,以及数据出境安全评估、个人信息出境标准合同和个人信息保护认证3个维度的具体落实办法。在国际层面,中国与多个国家和地区签署了数据跨境流动备忘录,并在共建“一带一路”框架下推动数据跨境流动合作协议和国际规则的构建。当前,中国跨境数据治理水平与《全面与进步跨太平洋伙伴关系协定》(CPTPP)和《数字经济伙伴关系协定》(DEPA)等高标准国际经贸规则仍然存在差距。

美欧数据跨境流动的合作机制备受学者关注。目前有关研究主要有美欧跨境数据流动制度设计(Farrell, 2002; 曹杰和王晶, 2017; Mercurio and Yu, 2022; Lee et al., 2023; 周念利等, 2023)、参考域外经验为中国推进跨境数据流动国际合作提供政策建议(Li, 2021; 李俊等, 2023; 张倩雯和张文艺, 2023; Jiang, 2024; 单文华和邓娜, 2024; Voss and Pernot-Leplay, 2024)等。还有研究聚焦美欧跨境数据流动的风险防范机制,包括跨境数据流动场景中的风险识别、披露、分类和管理机制(Connolly and van Dijk, 2016; Voss, 2019; Batlle and van Waeyenberge, 2024)。

二、美欧数据跨境流动合作机制的演进

美国与欧盟数字贸易联系紧密,但两者关于数据跨境流动的国内立法路径却存在较大差异。为此,多年来双方一直就如何消除数据流动障碍进行谈判,并先后订立了《安全港协议》与《隐私盾协议》。尽管两份协议都被宣告无效,但不可否认的是,它们仍然为美欧维持了20多年较为稳定的数据跨境流动合作机制。

(一) 基于《安全港协议》的数据跨境流动合作机制

美欧数据保护立法差异是双方产生分歧的根源之一。欧盟于1995年发布了《个人数据保护指令》(Data Protection Directive)。该指令第25条规定跨境数据转移必须在达到欧盟认可的保护标准条件下进行,即“充分保护原则”。^②而彼时美国尚缺乏对个人隐私保护的全国统一立法,其数据隐私保护制度被描述为联邦和州法

^① The United States Court of Appeals for the District of Columbia Circuit. TikTok ByteDance Petition Review[EB/OL]. 2024, <https://fingfx.thomsonreuters.com/gfx/legaldocs/myymkdggbvr/TikTok-ByteDance-petition-review-20240507.pdf>. [2024-05-07](2024-07-25).

^② European Parliament. Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data. Article 25[EB/OL]. 1995, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046>. [1995-10-24](2024-04-28).

规的“拼凑”，几乎不可能被列入欧盟认可名单。^①因此，为避免数据流动壁垒对双方经济往来造成负面影响，美欧于2000年签署了《安全港协议》。为了妥善处理个人数据，^②《安全港协议》规定了通知原则、选择权原则、再传输原则、安全原则、数据完整性原则、访问原则和执行原则。^③

如果商业机构想要从欧盟传输数据，它们需要申请加入《安全港协议》并遵守所规定的原则与义务。美国商业机构需要履行高于美国本土立法的数据传输保护标准，以弥补美国隐私法规的不足。这实际上代表了商业机构在数据保护规则中做出让步以获取欧盟对美国数据跨境传输的部分认可，使得双方隐私保护法律的冲突暂时得以缓和（黄志雄和韦欣好，2021）。同时，应看到《安全港协议》对维持美欧数据跨境流动的积极意义。

首先，《安全港协议》促进了美欧之间数据流动，暂时解决了跨大西洋数据传输的法律困扰。尽管该协议增加了跨境传输数据的成本，但极大地促进了美国企业在欧盟市场的扩张，在《安全港协议》名单上超过5,000家商业机构使用该协议进行数据传输，使美国在数字贸易飞速发展的15年间抢先占据了优势市场地位。另外，得益于该协议构建的数据流动机制，2014年美国 and 欧洲之间的跨境数据流是世界上最高的——几乎是美国和拉丁美洲之间数据流的两倍，比美国和亚洲之间的数据流高出50%。^④

其次，《安全港协议》有利于国际数据隐私保护标准的统一与提升。《安全港协议》对欧盟“充分保护原则”的认定进行了创新，即充分性判断并不需要延伸到整个美国数据隐私法律体系，只需要延伸到自愿接受隐私原则的公司。这被证明是欧盟潜在妥协的基础，网络运营商能够忽略美欧隐私立法差异进行数据传输。^⑤推而广之，符合对应国家数据保护标准的企业皆可适用此类协议进行数据传输，而不必强求双方乃至区域之间在数据隐私保护立法领域的完全一致（马芳，2015）。而且，《安全港协议》规定了数据保护的七大原则，有助于提升数据保护和隐私权的标准。

然而，美国基于国家安全原因对个人隐私数据的频繁访问引发了欧盟的质疑，且《安全港协议》相关规则已经远不能覆盖其后10余年网络技术迅速发展所产生的需求。2013年，棱镜计划被曝光，美国国家安全局和联邦调查局被指控对所有向美国传输的即时通信和既存资料进行深度监听，包括苹果、微软在内的众多美国巨头公司

① Weiss, M. A., Archick, K. US-EU Data Privacy: From Safe Harbor to Privacy Shield [EB/OL]. 2016, <https://sgp.fas.org/crs/misc/R44257.pdf>. [2016-05-19] (2024-05-27).

② 根据《安全港协议》的规定，个人数据是指任何形式记录的由美国机构从欧盟收到的在本指令范围内的任何已识别或可识别到具体个人的数据。

③ Federal Trade Commission of the U.S. Safe Harbor Privacy Principles [EB/OL]. 2016, <https://www.ftc.gov/business-guidance/resources/information-eu-residents-regarding-us-eu-safe-harbor-program>. [2016-07-25] (2024-06-15).

④ Meltzer, J. P. The Importance of the Internet and Transatlantic Data Flows for U.S. [EB/OL]. 2014, <https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf>. [2014-10-15] (2024-06-18).

⑤ 商务部国际贸易经济合作研究院、上海数据交易所.《全球数据跨境流动规则全景图》[EB/OL]. 2023, <https://voestatic.chinadep.com/group1/voe/447b6ccabfb42e9a33ba6b8ebd63861.pdf>. [2023-11-26] (2024-05-12).

皆参与其中。^①在此背景下，2015 年奥地利律师马克斯·施雷姆斯（Max Schrems）就脸书（Facebook）数据传输保护不充分一事向爱尔兰法院寻求救济（Schrems I 案）。欧盟法院认为本案关键在于美国长期以国家安全为由违背《安全港协议》的核心原则，个人数据可能会在侦查犯罪和间谍活动的过程中不被区分地被访问。^②《安全港协议》被欧盟法院判定为欧盟居民提供的保护并不充分，并被宣布无效。

在 Schrems I 案判决作出时，已有超过 5,000 家机构通过《安全港协议》在美欧之间传输电子数据。协议的失效将严重扰乱它们的正常生产经营，并重创美欧跨境数字贸易市场。因此，双方通过紧急磋商达成了新的数据传输协议，即《隐私盾协议》。

（二）基于《隐私盾协议》的数据跨境流动合作机制

在《安全港协议》失效至《隐私盾协议》生效前，美欧双方主要通过“标准合同条款”（SCCs）与“约束性公司规则”（BCRs）暂时维持数据传输。《隐私盾协议》于 2016 年 7 月正式实施，其实质是对《安全港协议》的补充与升级（表 1）。基于前车之鉴，除了丰富七大原则的细节与注意事项之外，《隐私盾协议》不仅适用于私人商业主体，还对美国政府施加了义务并设立救济机制。

表 1 《隐私盾协议》对《安全港协议》的补充与升级

补充事项	《安全港协议》	《隐私盾协议》
企业义务	需要遵守 7 项隐私原则	更严格的隐私原则，包括新的责任原则、补充原则；涉及数据安全的更多方面，如敏感数据的处理、新闻行业的例外情况以及数据保护机构的作用等
隐私保护标准	/	要求美国企业提供与欧盟同等水平的隐私保护
年度审查	/	要求每年进行一次联合审查
监察员机制	/	设立了独立的隐私盾监察员，负责处理涉及政府部门监控、获取个人信息的投诉
对美国政府监控的限制	/	要求美国政府在获取欧盟公民个人信息时，必须限于特定目的，并且承诺不再进行大规模任意监控
救济机制	/	多种救济渠道，包括直接向美国企业提出请求和投诉、提供免费的替代性纠纷解决机制（ADR）、向本国数据保护机构进行投诉以及仲裁程序
法律效力和执行	由美国联邦贸易委员会（FTC）监督执行，但主要依赖于企业的自我认证和自律	除 FTC 的监督外，还增加了美国商务部的参与以及与欧盟委员会的合作

资料来源：作者根据《安全港协议》与《隐私盾协议》内容整理。

首先，《隐私盾协议》详细规定了救济与仲裁机制。违背隐私原则的美国企业将被索赔以及受到其他惩罚，如果其持续不遵守原则，则将被从隐私盾名单中除名，并且必须归还或删除相关数据。^③同时，美国国务院设立了隐私盾监察员岗位，负责

① The Guardian.NSA Prism Program Taps in to User Data of Apple,Google and Others[EB/OL].2013,https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.[2013-06-06](2024-06-15).
② European Parliament.The CJEU's Schrems Ruling on the Safe Harbour Decision[EB/OL].2015,https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/569050/EPRS_ATA(2015)569050_EN.pdf.[2015-10-06](2024-06-13).
③ European Parliament.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[EB/OL].2016,https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.[2016-07-12](2024-07-23).

审查有关投诉。美国国家情报总监承诺国家安全情报活动将会有明确的限制范围和保障措施。另外,美欧双方将对国家安全部门介入情况进行年度审查,在《隐私盾协议》生效之后,2017年至2019年间已经进行过3次审查。

《隐私盾协议》对《安全港协议》救济机制的重大改革提升了美欧数据传输框架的执行力。《安全港协议》遭受的质疑很大程度上来自其宽松的监管模式与执行水平,其生效的大部分时间没有任何执法活动。^①罕见的执法活动也通常是由隐私保护倡议者直接发起的,而不是当局的任何常规监督或调查。据统计,15年间消费者向联邦贸易委员会提出的1,300多起投诉中只有40起被执行调查,在这些案件中也只有两家公司被罚款。《隐私盾协议》的索赔与惩罚机制使欧盟进一步延伸了数据保护权利,重建了美欧双方对数据跨境流动的信任关系。

其次,《隐私盾协议》推动了美国国内立法和执法体系的完善。为应对欧盟的监管压力,美国通过了第28号总统政策指令《信号情报活动》,意在限制情报机构对个人数据的获取与使用,并将保护对象扩展至美国公民以外。此外,《隐私盾协议》谈判中欧盟的价值导向再次明确了隐私权是人权不可缺少的一部分,这对其他国家和地区的相关立法具有积极影响。同时,《隐私盾协议》的规定较《安全港协议》具有更强的执行力,这促进了国际数据跨境流动机制规范化发展。美欧之间的数据流动机制几经波折,使得越来越多的国家与地区意识到数据传输合规的重要性(刘碧琦,2016)。在此背景下,计算机设施的位置、数据存储本地化等问题成为重要议题。后续达成的区域贸易协定等就上述议题达成共识,促进了国际数据跨境流动机制的合作。

(三) 美欧数据跨境流动合作机制再遇挫折

自《隐私盾协议》生效以来,共有5,394家商业机构通过认证。^②然而,《隐私盾协议》对个人隐私保护条款的补充与升级并非一劳永逸。一方面,它并未要求美国修改本国隐私立法,导致监察员机制无法独立于行政机关运行,其监管处罚力度让人质疑,无法从根本上限制情报机构对个人数据的窥伺;另一方面,2018年欧盟《通用数据保护条例》(GDPR)正式实施以取代《个人数据保护指令》。根据该指令第25条制定的《隐私盾协议》与GDPR的兼容性也令人担忧。在Schrems II案审查过程中爱尔兰高等法院发现《隐私盾协议》有效性存疑,将其提交欧盟法院。2020年7月欧盟法院宣布《隐私盾协议》因不能提供充分保护而失效。^③

究其直接原因,首先,美国对监控计划进行严格限制的承诺并无法律依据。根

① 《安全港协议》在2000~2008年、2010~2011年和2012~2013年之间没有任何执法活动。

② Data Privacy Framework Program. Privacy Shield Lists of U.S. Companies[EB/OL].2020,https://www.privacyshield.gov/list.[2020-07-20][2024-07-14].

③ European Parliament.The CJEU Judgment in the Schrems II Case[EB/OL].2020,https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.[2020-07-16][2024-06-13].

据《欧盟宪章》第7条,欧盟法院认为允许干涉基本权利的法律依据本身必须界定限制范围以及保障措施,并且必须满足比例原则的要求。^①然而,美国《外国情报监视法》(FISA)第702条未明确规定对监视实施机构的任何权力限制,也没有为相关非美国公民提供任何保障。^②因此,该承诺本质上不能达到《欧盟宪章》第7条要求的保护水平,并且被视为对数据和隐私权的过度干涉。

其次,美国缺乏对数据主体有效的救济措施。根据《欧盟宪章》第47条规定的原则,GDPR第104条指出,第三国“应确保有效的独立数据保护监督,并应向数据主体提供有效和可执行的权利以及有效的行政和司法救济”。^③美国为此承诺设立监察员机制以弥补其在救济途径上的缺陷。然而,经过调查后欧盟委员会认定其非但没有弥补,反而加剧了这些缺陷。这是因为监察员机制不能被认定为合格的司法救济途径。根据《欧盟宪章》第47条及其相关要求,救济途径要求数据主体必须有可能向独立公正的法院提起法律诉讼,以便获取其个人数据,或获得对此类数据的纠正或删除。^④然而,监察员不能被视为《欧盟宪章》第47条含义内的法庭,他的决定也不可上诉,这表明该制度缺乏欧盟主体针对美国当局的可诉权利。而且,欧盟对监察员机构的独立性与其决定的可执行性也令人担忧。尽管美国声称监察员“独立于情报系统”,但事实上由国务卿任命并且从属于国务院。《隐私盾协议》也没有任何内容表明其有权做出对情报机构具有约束力的决定。

最后,美欧数字经济基础差异导致双方数据保护价值诉求不同,并进一步成为双方数据保护机制分歧的深层原因。全球信息与通信技术产业(ICT)作为数字经济领域重要产业之一,2022年欧盟占ICT全球市场收入份额为11.3%,在10年间下降超过10%,而美国的份额则高达36%。^⑤另外,欧盟数字企业不发达,中小企业发展十分缓慢且不均衡。截至2024年,欧盟只有263家独角兽公司^⑥(占全球总数的13%),而中国有387家,美国有1,539家。^⑦这表明欧盟在全球数字贸易市场中的困境,一方面,欧盟人口众多,经济发达,数字贸易市场潜力巨大;另一方面,欧盟本土相关企业与高新技术产业竞争力不足,数字产品高度依赖进口。而美国数字经济在产业

① Official Journal of the European Communities.Charter of Fundamental Rights of the European Union(2000/C 364/01),Article 7[EB/OL].2000,https://www.europarl.europa.eu/charter/pdf/text_en.pdf.[2000-12-18](2024-06-13).

② 美国《外国情报监视法》第702条允许政府强制美国公司协助针对位于美国境外的非美国人收集情报,并且每个目标都不需要来自外国情报监视法院(FISC)的单独命令。

③ European Parliament.Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data,and Repealing Directive 95/46/EC(General Data Protection Regulation)[EB/OL].2016,https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.[2016-05-04](2024-07-13).

④ Official Journal of the European Communities.Charter of Fundamental Rights of the European Union (2000/C 364/01),Article 47[EB/OL].2000,https://www.europarl.europa.eu/charter/pdf/text_en.pdf.[2000-12-18](2024-06-13).

⑤ European Commission.2023 Report on the State of the Digital Decade[EB/OL].2023,https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade.[2023-09-27](2024-10-13).

⑥ 独角兽公司指全球成立于2000年之后价值10亿美元以上的非上市公司。

⑦ European Commission.Report on the State of the Digital Decade 2024[EB/OL].2024,Communication_from_the_Commission_State_of_Digital_Decade_2024_main_report_lzDSxHZ5UBFrQggK1aDTiHkz0vQ_106687%20.pdf.[2024-07-02](2024-10-13).

规模和完整度、企业竞争力、核心技术等方面都处于世界前列。^①

数字经济实力差异塑造了美欧在数据保护方面的价值取向。因其强大的数字经济，美国在全球数据跨境流动体系中属于数据流入国，数据隐私泄露至境外的担忧更少，从而确立了“市场本位”的数据保护价值导向，更倾向于较少限制的数据流动规则。数据自由流动迎合了美国本土数字企业巨头的需要，有利于维护其在全球数字经济中的领导地位。另外，较为自由的数据流动规则也为美国情报系统收集海外目标的通信信息提供方便（程海桦和王健，2023）。作为数据流出地区，欧盟采取了更为审慎的“权利本位”态度。这既与欧盟一如既往的个人隐私保护传统有关，也表达了其希望通过 GDPR 增强对数据流动控制权的诉求。GDPR 严格的数据保护机制既提高了来自欧盟以外的数字企业进入欧盟市场的门槛，保护欧盟本土企业发展；又迫使其他国家与地区向 GDPR 标准看齐，提高了其在全球数据治理规则制定中的话语权。由此可见，美国的“市场本位”价值观与欧盟的“权利本位”价值观冲突，本质上体现的是双方对于“数据主权”的争夺。

价值取向分歧进一步影响了美欧双方构建数据跨境流动机制的路径选择。欧盟通过统一立法对个人隐私权利采取充分保护，注重事前预防与控制，并通过“外严内松”的规制形式构建内部统一的数字市场，以增强其在世界上的数字竞争优势（郑淑凤，2024）。欧盟对国家安全例外的限制较为严格，要求必须在真实、紧迫且可预见的威胁下才可进行相关活动，并且需要有独立的审查机制。而美国尚未形成专门法律，其主要通过事后问责制对个人隐私数据进行监管，而且《外国情报监视法》等法律赋予情报机构广泛的监控权限，缺乏对非美国公民的充分法律保障，美国政府得以借国家安全为由频繁违反比例原则窥探他国公民隐私。对国家安全例外范围的不同定义也是双方争议的焦点。

总之，由于数字经济基础差异、价值取向分歧与数据主权博弈等种种原因，美国在数据传输中的实际做法与《欧盟宪章》和 GDPR 的基本规定并不兼容，其缺乏后两者规定的所必需的法律限制与救济手段，导致欧盟法院认为美国没有提供它在《隐私盾协议》中所保证的与 GDPR 基本同等的、充分的保护水平。这直接影响了《隐私盾协议》整体的有效性，所以被欧盟法院宣告无效。

三、美欧数据跨境流动合作机制的重建

尽管《安全港协议》与《隐私盾协议》均以失效告终，但美欧数字贸易市场的深度依存关系决定了它们必须尽快进行新一轮磋商。双方于 2023 年 7 月达成了第 3 份协议——《数据隐私框架》。该框架由两部分组成：美国商务部发布的《数据隐私

^① 中国信息通信研究院.全球数字经济白皮书2023[EB/OL].2024,http://www.caict.ac.cn/english/research/whitepapers/202404/P020240430470269289042.pdf.[2024-01-09][2024-10-12].

框架原则》以及规范美国情报机关活动的相关配套行政指令。作为目前美欧之间数据传输谈判的最新成果，其主要对《隐私盾协议》存在的上述缺陷作出了回应。这些回应主要体现在《数据隐私框架》第3章中，由获取数据的法律依据、监督程序以及救济机制3个部分组成。另外，美欧近年来也分别与周边国家探索数据跨境流动合作机制。

（一）基于《数据隐私框架》的数据跨境流动合作新机制

首先，该框架对美国公共机构为国家安全利益等公共利益收集使用的个人数据规定了更为严格的限制和保障措施。例如，对个人隐私保护权利所施加的任何限制都必须通过法律规定。^①在《隐私盾协议》实施过程中，美国情报系统的做法被批评为过度执法，而《数据隐私框架》将比例原则确立为主要规定之一。为满足比例原则的要求，对个人数据保护的例外和限制只能在为达到类似欧盟确认的一般利益目标时，在严格必要的范围内适用。美国情报系统在获取欧盟公民的数据信息时需要遵循程序，承诺将在内部建立一套新的数据保护规则，对数据收集实施分类分级与限制数据收集范围。此举加强了对美国情报系统的限制，使得美国情报机构对个人数据的访问不仅需要满足“必要性”，在访问过程中还需遵循“合理性”的要求。

其次，《数据隐私框架》完善了情报机构的多重监督机制。第一，要求每个机构都设有合规审查官员，并确保他们拥有权力处理投诉。这些官员需要定期向国会、隐私和公民自由监督委员会（PCLOB）就投诉数量、类型以及处理结果作报告。第二，在每个情报机构设立独立的监察长职位与监察办公室，主要负责对情报机构的工作进行调查，并具有向检方起诉以及向情报机构提出改正建议的权力。监察长提出的改正建议虽然不具有强制约束力，但其报告会被公开并发送至国会。第三，设立隐私和公民自由监督委员会等行政监督机制。值得注意的是，根据美国《外国情报监视法》第702条收集的个人信息，不仅需要向情报委员会和司法委员会提交法定报告和举行听证会，向司法部长每半年提交一次合规报告，还需要受涉外情报监控委员会的监督。在年度审查时，数据也会受到情报监督委员会的严格合规审查与认证。

最后，美国首次承诺建立司法途径的双层救济机制。第一层是在美国的情报系统中设立“公民自由保护官”（CLPO），用于监管其在获取欧盟公民个人数据时符合流程与范围限制，并在欧盟居民投诉时做初步调查。第二层是根据《第14086号行政命令》设立“数据保护审查法庭”（DPRC）。^②欧盟居民可以通过该法庭提起诉讼。DPRC有权对投诉进行独立调查、获取证据以及进行有约束性的决策。在审查过程中，有特别律师代表申诉人的利益表达诉讼请求。如果DPRC发现情报系统或

①② Adequacy Decision EU-US Data Privacy Framework[EB/OL].2023, https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf. [2023-07-10] (2024-07-26).

者商业公司有违《数据隐私框架》原则，可以要求对方删除该数据。鉴于法庭成员独立于行政系统以外，DPRC 的独立性与监管力度较《隐私盾协议》中的监察员机制有大幅提升。

总体上，相较于《安全港协议》与《隐私盾协议》，美国企业在《数据隐私框架》的背景下面临更为严格与具体的要求。《数据隐私框架》进一步规定了美国企业参与数据跨境传输的行为，并设立了“数据保护审查法庭”等机构。美国企业若出现违反规定的行为，不仅需要删除不符合要求的数据，而且在经营中受到更大的监管力度。《数据隐私框架》既是美欧双方就数据跨境传输进行 20 余年长期博弈的具体体现，也是双方就该议题不断协调的最新成果。该框架对美欧以往数据跨境传输中存在的不足进行了修正。双方在数据隐私、国家安全、监督与救济程序等长期存在争议与实施障碍的关键领域取得进展，这表明双方在数据领域的合作机制正在走向规范化与成熟。

（二）美欧与周边国家的数据跨境流动合作机制

在与欧盟达成上述协议之外，美国也在探索与其他国家和地区建立数据跨境流动互相认可机制。目前美国主要着力点是亚太经济合作组织（APEC）的《跨境隐私规则体系》（CBPRs）。CBPRs 基于《APEC 隐私框架》诞生，是一个自愿的、基于问责制的体系，为 APEC 成员之间的跨境数据交流提供单一框架以弥合它们在国内隐私法方面的差异。它有 4 个主要组成部分：申请加入 CBPRs 体系的最低认可标准；问责机构的选择；问责机构的评估标准；监管合作安排（CPEA）。自 2011 年成立以来，目前有 9 个国家与地区参与了 CBPRs。

除了互相认可机制之外，美国在自由贸易协定（FTA）中也体现了数据跨境流动合作机制。美国最早引入数据跨境流动规则的 FTA 是 2012 年的《美国—韩国自由贸易协定》。^①《跨太平洋伙伴关系协定》（TPP）出现之后，数据跨境流动条款开始成为美国缔结的 FTA 的重要内容。2018 年达成的《美墨加协定》（USMCA）和 2019 年达成的《美日数字贸易协定》基本沿用了 TPP 的有关规定，任何缔约方不得禁止或限制包括个人信息在内的数据跨境流动以及禁止强制的个人数据本地化存储。尽管该规定不得违背合法公共政策目标，但 USMCA 又为实现公共政策目标的措施增加了限制，以最大限度实现数据自由流动。^②USMCA 还在个人信息保护条款中认可了 CBPRs，即缔约国可以使用 CBPRs 作为统一的个人数据保护标准。^③但值得注意的是，上述规定均未涉及对美方情报系统的限制与救济措施。除此之外，美国新近缔结的 FTA 以及数字贸易专项协定都纳入了数据跨境流动规则，但总体上都

① 《美国—韩国自由贸易协定》第15.8条。

② USMCA第19.11条。

③ USMCA第19.8条第2款。

沿用了 TPP 的规定，以强制性条款促进数据跨境自由流动，尽可能地实现美国先进数字技术带来的巨大经济利益。

欧盟一直尝试在 FTA 的谈判过程中纳入数据跨境流动相关规则，并在 FTA 的基础上进一步建设数字伙伴关系。2019 年 2 月 1 日，《欧盟—日本经济伙伴关系协定》正式生效，旨在消除贸易壁垒。在此基础上，双方启动了数字伙伴关系谈判，并于 2023 年 6 月达成《欧盟—日本数字贸易原则》，包括取消数据本地化要求、消除数据跨境流动中的不合理障碍、开放数字市场等内容。^①2022 年 11 月 30 日，欧盟签订了《欧盟—韩国数字贸易原则》，内容涵盖了数字贸易便利化、数据治理、消费者信任等。2023 年 2 月，欧盟与新加坡在《欧盟—新加坡自由贸易协定》的基础上签署了《欧盟—新加坡数字伙伴关系协定》，就可信任的数据流动、数据中心建设等议题进行深入合作。^②

美欧开展数据跨境流动合作机制采取的路径具有一定的相似性，均提出了符合自身利益诉求的数据保护标准，并积极通过在 FTA 谈判中纳入数据跨境流动规则的方式对外推广各自的数据保护价值观。尽管 CBPRs 与 GDPR 在基本框架设置等方面非常相似，但两者在基本目标与保护标准上存在本质区别。CBPRs 本质上是一个 APEC 区域内部的数据保护标准系统，旨在促进 APEC 内部国家与地区间的数据跨境流动；GDPR 作为欧盟法规，促使欧盟以外的国家与地区在试图进入欧盟市场时遵守相关规定。另外，CBPRs 仅规定了数据保护最低标准，在个人数据识别、数据收集与处理等领域没有具体明确的规定，对于通过认证的企业也缺乏共同的管理标准和要求。在规则制定上，CBPRs 与 GDPR 的侧重点不同，欧盟更侧重对个人隐私权利的保护，CBPRs 更体现美国对数据自由流动的诉求。美国试图通过 CBPRs 在亚太地区推广美式数据流动规则，以对抗欧盟 GDPR 的强大影响力。

值得注意的是，欧盟与其他国家通过双边协议开展跨境数据流动合作的方式与《数据隐私框架》也存在差别。欧盟与其他第三方进行谈判时更加重视基于双边关系进行磋商，提出基于贸易伙伴关系进一步发展与日本、韩国、新加坡的“数字伙伴关系”，而非形成单独的跨境数据合作协议。欧盟在与其他第三方的协商中淡化了对情报部门干涉的相关措施，强调对于隐私保护的一般做法。《数据隐私框架》则进一步升级对美国情报机构的监管措施，作为政府间的合作机制，在其宣称的救济与监管措施没有执行的情况下，未来不排除与《安全港协议》和《隐私盾协议》一样，需要受到欧盟法院等司法机构的审查。

① European Commission. EU and Japan Conclude Landmark Deal on Cross-border Data Flows at High-Level Economic Dialogue[EB/OL].2023,https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378.[2023-10-28][2024-07-26].

② Ministry of Trade and Industry Singapore.The European Union (EU)-Singapore Digital Partnership[EB/OL].2023,https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/EUSDP.[2023-02-01][2024-07-26].

四、美欧经验对中国数据跨境流动合作机制构建的启示

尽管美欧数据跨境流动合作机制历经挫折，但已渐趋成熟与完善。相比而言，中国数据跨境流动合作机制建设起步较晚，上述分析有助于中国探索后续如何更好推进数据跨境流动合作机制。

（一）完善国内数据保护体系和权利救济机制，为推动数据跨境流动合作做铺垫

美欧数据跨境流动规则的频繁变动，引发了对双边协议治理效力的广泛审视。此前美欧数据跨境流动双边协议接连失效的核心原因在于欧盟对美国数据隐私保护机制缺乏足够的信任，具体表现为美国国内统一数据保护体系与救济机制的缺失。美国数据监管机制存在滞后性，无法充分预防数据风险的发生。此外，当个人数据被美国情报机构非法窥探时，非美国公民缺乏有效且独立的救济手段。

有鉴于此，中国应当吸取美欧经验，完善国内数据保护体系和权利救济机制，增强与合作伙伴的互相信任，为开展数据跨境流动合作做铺垫。（1）完善数据保护相关法律法规。中国仍需修订国内立法相关内容，针对数据保护的各个环节、重点行业、分级分类等制定具体规范。（2）建立全面的监管体系。在政府层面，兼顾事前预防机制与事后处罚机制以确保相关法律有效执行。同时，推动行业自律，鼓励行业协会等组织制定数据保护的具体行业标准。（3）加强数据安全技术的研究和应用。加大对数据保护技术的科研投入，通过推广先进的加密技术、访问控制技术等手段，为数据保护体系提供技术支持。（4）为数据主体提供多种救济途径。包括向数据控制者提出申诉、向监管部门投诉、寻求司法救济等；同时鼓励数据主体通过协商、调解等方式解决数据纠纷，在符合条件的情况下开展线上诉讼，降低维权成本。

（二）继续借助区域贸易协定，完善数据跨境流动合作机制

美欧双方由于数字经济基础差异与数字主权博弈等原因，在数据跨境流动中存在不同的价值导向与利益诉求，但二者都不约而同地采取了通过 FTA 谈判加强与域外国家或地区数据跨境流动合作的路径。在法律实施层面，FTA 为数据跨境流动构建了一个相对自由的法律框架。这种框架不仅降低了数字贸易壁垒，同时也为数据流动的国家安全、公共政策考量等例外情况提供了法律确定性。在全球治理层面，美欧通过 FTA 推广数据跨境流动规则的“美式模板”与“欧式模板”，构建其数据跨境流动治理秩序，并进一步扩大其在全球数据跨境流动规则制定中的优势与话语权。

有鉴于此，中国应当积极参与 FTA 谈判，并重点商议数据跨境流动合作条款。当前，在中国加入的一些 FTA 中，涉及的电子商务条款主要包括在线消费者保护、网络安全以及电子商务合作等。例如，《区域全面经济伙伴关系协定》（RCEP）电子商务章节强调各自负责消费者保护的主管部门间在电子商务相关活动中开展合作，

以增强消费者保护的重要性；通过交流最佳实践，利用现有合作机制，在网络安全相关事项方面开展合作；要求各方应在适当时就帮助中小企业转型、确定合作领域、信息和经验共享等问题开展多边合作。《中国—澳大利亚自由贸易协定》规定，在开展电子商务的研究培训等合作活动中，可以共享管理框架、网络消费者保护等信息。《中国—韩国自由贸易协定》鼓励企业间的交流、合作活动和联合电子商务项目，以促进电子商务发展。

目前，中国正在申请加入的 CPTPP 和 DEPA 都设置了数据跨境流动相关条款。二者均包含缔约方认识到在网络安全、在线消费者保护方面开展合作的重要性的表述。DEPA 还特别指出数据创新的重要性，提出缔约方应努力在数据共享项目和机制、数据新用途的概念验证（包括数据沙盒）方面开展合作，以促进数据驱动的创新。

在未来 FTA 谈判中，中国应重点考虑数据跨境流动合作，为探寻数据跨境流动全球规制的兼容性框架提供新思路 and “中国方案”。加强数据跨境流动技术领域的合作，例如数据加密、区块链、云计算等领域的技术合作，确保数据跨境流动的安全性，建立信息共享和互信机制，共同应对数据跨境流动带来的挑战。

（三）围绕重点内容和重要行业，签署数据跨境流动合作备忘录

美欧数据跨境流动合作机制频频出现分歧，双方跨国数字企业实力不对等是重要原因之一。发达的数字产业经济是美国推崇数据自由流动的信心来源与经济依托，也正是欧盟的担忧所在。同时，美欧数据跨境流动合作机制的多次失效也阻碍了双方跨国数字企业发展业务。可见，跨国数字企业的发展与数据跨境流动合作机制相互影响，息息相关。

有鉴于此，中国应当尽快与相关国家签订数据跨境流动合作范本或备忘录，营造跨国数字企业良好的发展氛围。备忘录内容可重点考虑以下方面。（1）构建数据跨境流动的对话机制。例如，围绕数据跨境流动的个人信息保护和网络安全合作与保障等内容开展对话，有效化解可能存在的分歧，为双方企业提供稳定的数字营商环境。（2）试点重点产业领域的的数据跨境流动。可根据双方国际贸易和投资往来现状，围绕重点行业的数据跨境流动开展试点。（3）数据跨境流动的风险防范与争议解决。当前国家数据安全备受关注，数据跨境流动风险较高。为此备忘录应该设置相应的一般例外和安全例外条款，防范国家安全风险，同时设立必要的争议解决机制，例如双方成立联合委员会具体处理潜在的分歧等。

在具体实施中，缔约方可在单独备忘录中列出合作活动的详细安排，通过联合委员会报告合作机制的计划和进展，力争通过各自渠道最大限度提供资源。具体合作的内容可以参照中国正在积极争取加入的 FTA，这样有助于释放 FTA 的“溢出效应”。例如，2024 年 6 月，中德签署《关于中德数据跨境流动合作的谅解备忘录》，旨在建立“中德数据政策法规交流”对话机制，加强数据跨境流动议题交

流。^①一直以来，中德两国在汽车等制造业领域具有深厚的合作基础，数据跨境流动合作机制的建立，有助于在汽车数据领域为双方建立一套共同的标准和规则，为两国企业营造良好的营商环境。

（四）围绕重点区域，推动构建数据跨境流动合作机制

为应对美欧积极开展与周边国家和地区的合作以及它们已经构建的数据跨境流动秩序，中国应当循序渐进地构建具有中国特色的互惠开放的数据跨境流动合作机制。

首先，中国应当优先考虑与那些政治互信度高且经贸往来密切的国家和地区开展数据跨境流动合作。如充分利用“一带一路”倡议，推进数据跨境流动对外合作。借助“一带一路”沿线国家既有的合作基础，既可以降低政治阻力，又有助于构建全球数据流动的示范效应。考虑到各国和地区在制度需求、发展水平上的差异，中国应采取渐进式的合作举措，在确保互信基础上逐步拓宽合作领域，稳步构建安全高效的数据流通环境。例如，2022年华为在新加坡的子公司华为国际获得新加坡资讯通信媒体发展局授予的数据保护信任标志（Data Protection Trustmark），以证明其业务合规，遵从新加坡《个人数据保护法》，这种实践值得借鉴推广。^②在数据跨境流动领域，实现“以点带面”的突破，为企业的国际经营提供保障。

欧盟作为中国重要的贸易伙伴，推动双方达成数据传输框架具有重要的意义。未来中欧要达成统一的数据传输框架，仍然需要在法律法规和政策方面进行多方面的调整和协调。GDPR对数据跨境传输设定了严格的“充分性认定”，中国可与欧盟就更加清晰的跨境数据评估标准商谈合作。鉴于欧盟对于数据隐私保护的重视，需要重点关注数据保护监管机构的独立性与实施能力。探索数据管理机构与多部门之间的协作，建立综合监管机制，给予数据保护机构一定的权力并加强其独立性。中国可以借鉴美欧跨境数据合作经验，特别要注意欧盟以数据隐私保护为由产生的外部干预风险。同时，中国可以利用现有的国际合作与调解平台，化解数据传输过程中的具体矛盾。

其次，由双边合作逐步过渡到多边以及区域数据跨境流动国际合作。中国应以双边协议为基础，积极构建涵盖范围更广的多边数据流动机制，通过采取“以双边带多边、以区域带整体”的推进举措，逐步构建一个更广泛的数据跨境流动圈。近年来，中国先后提出或签署《全球数据安全倡议》《“一带一路”数字经济国际合作倡议》《金砖国家数字经济伙伴关系框架》《中国—东盟关于建立数字经济合作伙伴关系的倡议》《“中国+中亚五国”数据安全合作倡议》等数字经济领域合作与行动倡议，

① 中央网络安全和信息化委员会办公室、庄荣文会见德国数字化和交通部部长维辛 双方共同签署《关于中德数据跨境流动合作的谅解备忘录》[EB/OL].2024, https://www.cac.gov.cn/2024-06/26/c_1721081180089753.htm. [2024-06-26] (2024-06-28).

② 华为获新加坡资媒局授予数据保护信任标志[EB/OL].2022, <https://www.huawei.com/cn/news/2022/3/singapore-imda-award-huawei-data-protection-cert>. [2022-03-16] (2024-07-23).

旨在凝聚多方共识,弥合各国(地区)在数据安全、隐私保护、经济发展之间的分歧,携手构建数字命运共同体,为后续推进数据跨境流动合作提供基础。为此,中国应秉承合作共赢的理念,明确与相关国家(地区)在跨境数据领域的共同利益与机制互补的可能性,在平等互利的基础上,寻找更广泛的数字合作空间。

五、结论

在全球数字治理领域,美国、欧盟和中国呈现“三足鼎立”的格局,数字规则正成为改变全球贸易竞争格局的关键制度性力量。自2000年以来,美欧数据跨境流动合作历经《安全港协议》《隐私盾协议》和《数据隐私框架》。究其原因,美欧数字经济基础差异导致双方数据保护价值诉求不同,并进一步导致数据保护机制出现分歧。美国为进一步维护其在全球数字经济中的领导地位,确立了“市场本位”的数据保护价值导向,倾向于促进数据的自由流动;欧盟作为数据流出国采取更为审慎的“权利本位”价值观,一方面是出于保护个人隐私权的立法传统,另一方面是以严格的数据跨境流动规则提高其在全球数据治理规则制定中的话语权。由此可见,美欧双方价值观冲突,本质上体现的是双方对“数据主权”的争夺与博弈。价值取向分歧影响了美欧国内数据保护立法的差异。美国缺乏数据跨境流动监管必需的法律限制与救济手段,政府以国家安全为由频繁违反比例原则窥探他国公民隐私,使欧盟认为美国没有达到与GDPR基本同等的充分性保护水平。尽管美欧数据跨境流动合作体系历经波折,但却不断完善,基本形成了数据跨境流动的跨大西洋合作机制。这为美欧数据跨境流动提供了相应的保障机制,加强了双方在数据跨境流动议题上的交流合作,为双方跨境数据企业营造了公平的营商环境,具有积极的意义。

数字贸易对数据跨境流动具有很强的依赖性,数据跨境流动为数字贸易发展提供前提条件。中共二十大报告提出要“发展数字贸易,加快建设贸易强国”。当前,中国规范数据跨境流动的国内法律制度正不断完善,内外资企业数据出境的需求也更加强烈。美欧数据跨境流动合作演进机制为中国更好参与数据跨境流动国际合作提供借鉴。诸如在实践中,如何更好平衡个人隐私保护和国家数据安全,如何完善配套的国内立法和执行机制等。中国可以通过FTA谈判和升级、签署数据跨境流动合作备忘录、双边合作协议等方式,探索数据跨境流动国际合作。

参考文献:

- [1] 曹杰,王晶.数据跨境流动规则分析——以欧美隐私盾协议为视角[J].国际经贸探索,2017,33(4).
- [2] 程海烨,王健.美欧跨大西洋数据流动的重启及其前景[J].现代国际关系,2023,(10).
- [3] 黄志雄,韦欣好.美欧数据跨境流动规则博弈及中国因应——以《隐私盾协议》无效判决为视角[J].同济大学学报(社会科学版),2021,32(2).
- [4] 李俊等.我国数据跨境流动治理成效、问题与完善建议[J].国际商务研究,2023,44(6).
- [5] 刘碧琦.美欧《隐私盾协议》评析[J].国际法研究,2016,(6).

- [6] 马芳. 美欧跨境信息《安全港协议》的存废及影响[J]. 中国信息安全, 2015,(11).
- [7] 单文华, 邓娜. 从“数据隐私框架”看欧美数据跨境流动的规则博弈[J]. 太平洋学报, 2024,32(1).
- [8] 张倩雯, 张文艺. 欧美跨境数据流动合作的演进历程、分歧溯源与未来展望[J]. 情报杂志, 2023,42(1).
- [9] 郑淑凤. 美欧外资数据安全审查的特点、影响与我国因应[J]. 国际贸易, 2024,(5).
- [10] 周念利等. 我国自贸区(港)数据跨境流动试点制度创新研究[J]. 国际商务研究, 2023,44(4).
- [11] Battle,S.,van Waeyenberge,A.EU-US Data Privacy Framework:A First Legal Assessment[J].European Journal of Risk Regulation,2024,15(1).
- [12] Connolly,C.,van Dijk,P.Enforcement and Reform of the EU-US Safe Harbor Agreement[J].Enforcing Privacy Law, Governance and Technology Series,2016,25.
- [13] Farrell,H.Negotiating Privacy Across Arenas:The EU-US Safe Harbor Discussions[C].Héritier,A.Common Goods: Reinventing European and International Governance.Lanham,Maryland: Rowman & Littlefield Publishers, 2002.
- [14] Jiang,F.China's Legal Efforts to Facilitate Cross-border Data Transfers: A Comprehensive Reality Check[J]. Asia Pacific Law Review,2024,32(1).
- [15] Lee,K. Y.,et al.Network and Text Analysis on Digital Trade Agreements[J].World Economy Brief,2023,13(3).
- [16] Li,Y.La Disciplina Cinese del Trasferimento Transfrontaliero dei Dati[J].Rivista Italiana di Informatica e Diritto,2021,(1).
- [17] Mercurio,B.,Yu,R.Regulating Cross-border Data Flows: Issues, Challenges and Impact[M].London:Anthem Press,2022.
- [18] Voss,W. G.Cross-border Data Flows, the GDPR, and Data Governance[J].Washington International Law Journal,2019,29(3).
- [19] Voss,W. G.,Pernot-Leplay,E.China Data Flows and Power in the Era of Chinese Big Tech[J].Northwestern Journal of International Law & Business,2024,44.

The Evolution and Implication of the Cooperation Mechanism of Cross-border Data Flow between the US and EU

PENG Delei YANG Yingze

Abstract: The development of digital trade is an essential requirement for China to become a strong trading nation. Currently, data has become a key resource for reshaping the structure of the global economy, and cross-border flow of data has become a key factor in promoting digital trade. Under the cooperation on cross-border flow of data, the US and EU have gone through the Safe Harbor Agreement, the Privacy Shield Agreement and the Data Privacy Framework. Despite numerous setbacks, these efforts have gradually established a transatlantic cooperation mechanism for cross-border data flows. However, significant differences between the U.S. and the EU—particularly in terms of their value orientations and legislative systems for data protection—remain major obstacles to deeper cooperation. Nevertheless, given the high level of mutual interdependence between the U.S. and EU digital trade markets, ongoing negotiations have progressively refined and institutionalized their cooperation framework. A comprehensive examination of the evolution and key features of the U.S.–EU cross-border data flow cooperation over several decades can offer valuable insights for China as it seeks to enhance its own mechanisms for international data flow governance, advance digital trade, and further support the strategic goal of becoming a major trading power.

Keywords: cross-border data flow; digital trade; Data Privacy Framework

(责任编辑: 梁丽华)