

DOI: 10.14015/j.cnki.1004-8049.2024.01.004

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”，《太平洋学报》，2024年第1期，第44-56页。

SHAN Wenhua, DENG Na, “A View of Conflict and Coordination of Cross-border Data Flow between the EU and the U.S. through Data Privacy Framework”, *Pacific Journal*, Vol.32, No.1, 2024, pp.44-56.

# 从“数据隐私框架”看欧美数据 跨境流动的规则博弈

单文华<sup>1</sup> 邓娜<sup>1</sup>

(1. 西安交通大学, 陕西 西安 710049)

**摘要:** 欧美《隐私盾协议》失效后, 双方为了恢复数据跨境流动秩序, 于2022年底达成了“数据隐私框架”。该框架旨在回应欧盟法院在“《隐私盾协议》无效案”中提出的主要关切。2023年7月, 欧盟委员会基于该框架对美国的个人数据保护水平发布了充分性认定决议。然而, 该框架并未对美国情报机构大规模收集数据与窥探隐私的行为施加实质性限制。此外, 框架建立的双层救济机制由于缺乏独立性, 也无法给数据隐私权益受损的欧盟公民提供充分有效的救济。与《隐私盾协议》相比, 该框架在本质上并没有明显的突破。欧盟和美国在双方数据跨境流动制度安排上的博弈, 表面上是两种数据保护理念和治理模式的碰撞, 实际上反映出了欧盟实施“数字主权”战略与美国维护“数字霸权”地位之间存在的根本利益冲突。欧美凭借各自优势, 在数字经济时代争夺全球数字治理话语权。通过深入研究欧美之间关于“数据隐私框架”的规则博弈, 可以为我国在选择适合本土的数据监管模式和提升数据治理规则话语权方面提供重要的思考和启示。

**关键词:** 《隐私盾协议》; 数据跨境流动; “数据隐私框架”; 充分性认定决议; 数字主权; 数字霸权  
**中图分类号:** D913 **文献标识码:** A **文章编号:** 1004-8049(2024)01-0044-13

欧美《隐私盾协议》(EU-US Privacy Shield Framework)失效后, 双方经过两年多的深入谈判, 终于达成了新的“数据隐私框架”(EU-US Data Privacy Framework), 并由美国总统拜登签署《关于加强美国信号情报活动保障措施的行政命令》(Enhancing Safeguards for U.S. Signals Intelligence Activities, 又称“第14086号行政命令”)加以落实。“数据隐私框架”旨在替代先

前的《隐私盾协议》, 为跨大西洋数据自由流动提供新的法律基础。2023年7月, 欧盟委员会以“数据隐私框架”为基础, 发布了关于美国个人数据保护水平的充分性认定决议。至此, 经过长达三年的悬而未决, 欧美数据跨境流动安排终于尘埃落定。

在美国签署第14086号行政命令后, 欧洲议会第一时间作出了回应。他们认可了美国在

收稿日期: 2023-06-26; 修订日期: 2023-09-23。

基金项目: 本文系国家社科基金重点项目“境外投资保护和促进法律问题研究”(21AZD065)的阶段性研究成果。

作者简介: 单文华(1970—), 男, 湖南株洲人, 西安交通大学校长助理、法学院院长、二级教授、博士生导师, 法学博士, 主要研究方向: 国际经济法; 邓娜(1989—), 女, 湖南衡阳人, 西安交通大学法学院2018级博士研究生, 主要研究方向: 网络空间和数据治理。

\* 作者感谢《太平洋学报》编辑部匿名审稿专家提出的建设性修改意见, 文中错漏由笔者负责。

提升数据保护水平方面所做的努力,但同时也表达了对这一措施是否能达到欧盟标准的担忧。<sup>①</sup>许多欧洲学者持有与欧洲议会相似的观点,如伊丽莎白(Elizabeth)强调,尽管美国情报法律体系有所改进,但大规模监控的可能性仍然存在;<sup>②</sup>阿什利(Ashley)分析了该行政命令建立的救济机制,并质疑其是否满足欧盟法律对于“有效司法保护”的基本要求。<sup>③</sup>而美国学者普遍认为欧盟的法律要求过于苛刻,并认为该行政命令已经是“在美国成文法和宪法框架内可行的最佳方式”。<sup>④</sup>国外对欧美之间数据跨境流动规制矛盾根源的深入分析普遍较为缺乏。国内关于欧美数据跨境流动的研究成果丰富,主要集中在《安全港协议》无效案、《隐私盾协议》无效案、欧美对个人数据保护和数据跨境流动规制模式的比较、双方分歧和博弈的根源分析,以及对我国的借鉴意义等方面。然而,从“数据隐私框架”角度切入的研究较为稀缺,目前仅有陈丽娜对双层救济机制的制度形式和制度成效进行了探讨。<sup>⑤</sup>深入剖析欧美“数据隐私框架”,有助于洞察欧美数据跨境流动之争存在的深层次问题,为我国在全球数字战略竞争中更好地把握国际数字治理趋势并选择适合本土的数据监管模式提供有益启示。

## 一、背景:欧美《隐私盾协议》无效案

自2015年10月欧盟法院宣布欧美《安全港协议》(EU-US Safe Harbor Framework)失效后,美国互联网巨头脸书(Facebook)转而采用“标准合同条款”(Standards Contractual Clauses)<sup>⑥</sup>作为向美国传输欧盟用户数据的依据。然而,在2015年底,奥地利法学学生麦克斯·施雷姆斯(Max Schrems)以脸书在向美国传输其个人数据时未能提供充分保护为由,向爱尔兰数据保护委员会提出投诉,要求暂停脸书使用标准合同条款。在案件审理期间,欧美为恢复双方数据的自由流动重新签订了《隐私盾协议》,并于2016年7月开始实施。因此,爱尔兰高等法院在向欧盟法院移交该案时,同时

对《隐私盾协议》的有效性提出了质疑。经过调查,欧盟法院认为美国当局将国家安全与法律执行置于公民隐私保护原则之上,其国内庞杂的情报法律体系并未充分考虑对公民数据隐私权利的保障,而且欧盟公民对此缺乏有效的司法救济途径。2020年7月,欧盟法院认定美国未能提供与欧盟“实质等同”(essentially equivalent)的数据和隐私保护水平,判定《隐私盾协议》失效。由于“《隐私盾协议》无效案”与判定《安全港协议》失效的“施雷姆斯第一案”(Schrems I)一脉相承,故又称“施雷姆斯第二案”(Schrems II)。欧盟法院判定两份协议失效的理由如出一辙,可见数据隐私保护问题是欧美数字经济往来的症结所在。

在《隐私盾协议》失效后,众多欧盟境内的外国企业为了应对欧盟愈发严格的数据跨境传输合规要求,不得不选择成本更高、流程更复杂的方式,如使用标准合同条款或其他替代工具,作为暂时性的解决方案。其中,约有10%的此类企业选择将数据存储在本地,或者干脆放弃

<sup>①</sup> Hendrik Mildebrath, *Reaching the EU-US Data Privacy Framework: First Reactions to Executive Order 14086*, European Parliament, 2022.

<sup>②</sup> Elizabeth Goitein, “The Biden Administration’s SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance”, *Just Security*, October 31, 2022, <https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/>.

<sup>③</sup> Ashley Gorski, “The Biden Administration’s SIGINT Executive Order, Part II: Redress for Unlawful Surveillance”, *Just Security*, November 4, 2022, <https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/>.

<sup>④</sup> Paul Rosenzweig, “The ‘Three Rs’ of President Biden’s Trans-Atlantic Privacy Outreach”, *Lawfare*, October 21, 2022, <https://www.lawfareblog.com/three-rs-president-bidens-trans-atlantic-privacy-outreach>.

<sup>⑤</sup> 陈丽娜:“美欧跨境数据隐私保护双层审-诉救济机制析解——基于 Executive Order 14086”,《商丘师范学院学报》,2023年第8期,第67-73页。

<sup>⑥</sup> “标准合同条款”是欧盟进行数据跨境传输的常用方式。这种条款通过内容的强制性和强制使用机制,确保将欧盟的监管要求融入每次单独的数据传输中。2021年6月,欧盟委员会发布了最新版本的标准合同条款,这一版本不仅涵盖了欧盟《一般数据保护条例》的核心规则,还吸收了“施雷姆斯第二案”的裁决精神。

在欧盟的业务。<sup>①</sup> 美国数字企业巨头“元”(Meta,前身为脸书)在2022年2月向美国证券交易委员会提交的年度报告中明确指出,欧盟的《一般数据保护条例》(General Data Protection Regulation)严重阻碍了其将欧盟用户数据传输和存储至美国服务器。《隐私盾协议》的失效无疑给欧美数字经济关系带来了明显的冲击。双方亟需就数据跨境流动问题展开深入协商,寻找合适的解决方案。

## 二、欧美“数据隐私框架”的主要成果和意义

《隐私盾协议》的失效严重扰乱了欧美之间正常的流动秩序,如何确保个人数据安全高效地流动成为双方的重大关切。自2020年7月“施雷姆斯第二案”判决生效以来,欧美双方一直在积极磋商新的数据流动规则和隐私保护方案,终于在2022年3月达成了“数据隐私框架”原则性协议。同年10月,美国颁布行政命令,正式落实这一框架。这标志着历时两年多的跨大西洋数据流动之争终于取得了实质性的成果。

### 2.1 达成跨大西洋“数据隐私框架”原则性协议

2022年3月,美国总统拜登和欧盟委员会主席冯德莱恩共同宣布,双方已就全新的跨大西洋“数据隐私框架”达成原则性协议。这一框架旨在解决欧盟法院在“施雷姆斯第二案”判决中提出的核心关切,重建欧盟个人数据传输至美国的重要法律机制。美国承诺对本国信号情报活动实施新的限制措施,以加强对数据隐私和公民自由的保护。改革后的情报部门在追求国家安全目标时,其行动是必要且相称的。此外,美国将加强信号情报活动的分层监督,并建立独立的双层救济机制。欧盟委员会与美国政府将继续合作,将这一协议转化为双方正式签署的法律文件,从而落实新的跨大西洋“数据隐私框架”。这份原则性协议不仅体现了欧盟与美国为恢复稳定、可信赖的数据流动所做的努

力,也凸显了双方之间紧密的数字经贸往来对商业数据安全、高效流动的迫切需求。

### 2.2 美国颁布行政命令(EO14086)限制信号情报活动

为了确保美国在“数据隐私框架”原则性协议中的承诺得以落实,美国总统拜登于2022年10月签署了《关于加强美国信号情报活动保障措施的行政命令》。这一行政命令对美国情报机构的信号情报活动设定了严格的限制,强调在处理个人数据时应充分尊重个人的合法隐私利益。

《关于加强美国信号情报活动保障措施的行政命令》规定了美国情报机构在获取个人数据时应遵循的总体原则,即只有在法律允许或经总统授权,且为实现法定的国家安全目标所必需的情况下,才能进行必要且相称的数据收集活动。此外,该行政命令还强调了对相关机构的监管要求。具体来说,该行政命令明确了可以收集信号情报的12项合法目标,包括评估外国政府的能力、防范恐怖主义和间谍活动、维护选举和政治程序的公正性等。美国国家情报总监办公室的公民自由保护官(Civil Liberties Protection Officer)将以上述合法目标为基础,对《国家情报优先框架》(National Intelligence Priorities Framework)<sup>②</sup>中的“情报优先级别”进行“验证”,确保情报活动的推进在于实现一个或多个合法目标。而且,实施情报活动应当符合必要性和比例性原则的要求。情报活动必须基于对所有相关因素的全面和合理评估,确保只在必要的情况下进行,并以与“经过验证的情报优先级别”(validated intelligence priority)相匹配的方式进行,避免对隐私和公民自由造成不成比例的影响。此外,情报收集应当“尽可能量身定制”(as tailored as feasible),优先考虑有针对性而非批量收集数据。原则上,只有在认定无

<sup>①</sup> Müge Fazlioglu, *IAPP-EY Annual Privacy Governance Report 2021*, International Association of Privacy Professionals, 2022, p.2.

<sup>②</sup> 《国家情报优先框架》是在总统指示下、由国家情报总监发布,用于确定国家情报活动的优先级、管理风险和评估任务绩效的政府文件。



法通过定向收集方式合理获取有效情报信息后,情报部门才能被授权实施大规模的情报收集活动。而且,大批量收集个人信息只能适用于防范恐怖主义、间谍活动、网络安全威胁等六项特定目标。当情报机构处理通过信号情报活动收集的个人信息时,必须遵循数据最小化原则,并在保护数据安全、限制数据访问等方面遵循特定要求和程序。

《关于加强美国信号情报活动保障措施的行政命令》作为践行“数据隐私框架”的核心法律文件,为之后欧盟委员会对美国数据隐私保护状况发布充分性认定决议奠定了基础。这一行政命令明显加强了美国信号情报活动中对数据隐私和公民自由的保护力度,有效避免了外国公民遭受不受限制的监控。尤其是12项合法目标的确立,不仅约束了美国情报机构之前不受实质限制的监控行为,还缩小了美国《外国情报监视法案》(Foreign Intelligence Surveillance Act 1978)第702条中“外国情报”的定义范围,代表着美国在保护外国公民隐私方面的重大进步。

### 2.3 美国为保护数据隐私权利建立双层救济机制

《关于加强美国信号情报活动保障措施的行政命令》的第三部分创建了一套双层救济机制,以处理在特定范围内违反美国法律与信号情报活动相关的“合格申诉”(qualifying complaints),为受到美国情报机构行为影响的欧盟公民提供了一种维权途径。若欧盟公民发现其个人数据在向美国传输的过程中,存在违反美国法律(包括《关于加强美国信号情报活动保障措施的行政命令》)的情况,他们有权向该救济机制提出申诉。

第一层救济机制由美国国家情报总监办公室的公民自由保护官组成。该官员将对“合格申诉”进行调查和审查,并在必要时下令采取适当的补救措施。第二层救济机制由数据保护审查法庭(Data Protection Review Court)构成。该法庭由美国司法部按照《关于加强美国信号情报活动保障措施的行政命令》的要求在其内部

组建。为了确保公正性,司法部长必须根据特定的遴选标准任命至少六名法官和两名特别辩护人。申诉人和情报机构人员均可就公民自由保护官的决定向法院申请复审。通常,由三名法官组成审查组对申请进行审查。此外,每一起申诉案件都会选任一名特别辩护人,该辩护人不仅应协助审查组开展工作,还应代表申诉人的利益进行抗辩。法庭在审查过程中,将参考公民自由保护官的审查记录以及申诉人、特别辩护人或情报机构所提供的信息或意见书。同时,其作出的决定必须遵循美国最高法院的相关判例。最后,公民自由保护官应按照法庭的要求行事,而情报机构也须遵守公民自由保护官和法庭审查组作出的决定。

新的双层救济机制相对于以前的隐私盾监察员制度有了一定进步,其独立性得到了明显提升。《关于加强美国信号情报活动保障措施的行政命令》通过明确美国国家情报总监的职责界限和限定罢免公民自由保护官的理由,提高了第一层救济机制的独立性。并且,通过制定数据保护审查法庭法官的选拔、任命、监督和罢免标准,降低了司法部长对第二层救济机制的影响,进一步确保了机制的独立性。该行政命令还赋予法庭调查和获取信息的权力,以及作出有约束力裁决的权力,这在一定程度上保障了法庭的独立性。

## 三、欧盟委员会的充分性认定决议及其争议

在“数据隐私框架”的推动下,美国针对本国的信号情报活动制定了新的限制措施,并为欧盟数据主体的隐私权利和自由提供了更完善的保障措施和救济机制。欧盟委员会强调“数据隐私框架”相比于《隐私盾协议》的重大改进,在综合评估美国当前的数据保护状况后,于2023年7月发布了一份肯定性的充分性认定决议。美国改进后的数据保护水平能否达到欧盟法律要求的“实质等同”标准,是其能否重新获得欧盟充分性认定的关键问题,也是双方博弈

的焦点。

### 3.1 对美国当前数据保护状况的评估和结论

根据欧盟《一般数据保护条例》第45(2)条的规定,欧盟委员会在作出充分性认定时,必须对第三国或地区的法律秩序进行全面评估,考察内容包括法律法规、人权保护、司法救济、国防及国家安全等方面。在对美国的充分性认定决议中,欧盟委员会明确指出,《关于加强美国信号情报活动保障措施的行政命令》所建立的限制、保障和救济机制是美国法律框架的重要组成部分,为欧盟委员会作出充分性认定提供了基础。欧盟委员会审视了欧美“数据隐私框架”的各项原则、加入框架的美国企业的承诺和认证义务,以及美国商务部对框架的管理和执行责任等,认为美国的法律体系总体上能够保障这些原则的有效实施。美国的监督机制和救济机制确保了实践中违反数据保护规则的行为能够被及时发现和处罚,并为数据主体提供了访问、纠正或删除个人数据的法律救济途径。此外,针对美国当局为刑事执法和国家安全等公共利益而干预欧盟公民基本数据权利的行为,《关于加强美国信号情报活动保障措施的行政命令》已将其严格限制在实现相关合法目标的必要范围内,并为欧盟公民免受此类干预提供了有效的法律保障。<sup>①</sup> 综上所述,欧盟委员会认为,在“数据隐私框架”下,美国可以为从欧盟传输至美国境内的个人数据提供与欧盟《一般数据保护条例》标准“实质等同”的保护。同时,欧盟公民根据《欧盟基本权利宪章》享有的基本权利在美国也能得到充分尊重和保障。因此,欧盟委员会作出决议,允许欧盟境内的个人数据根据《一般数据保护条例》第45条的规定传输至美国,而无需额外的授权。

### 3.2 博弈焦点:当前美国数据保护水平是否达到欧盟“实质等同”要求

欧盟的充分性认定决议引发了各利益相关方和学者的广泛关注与讨论。自“施雷姆斯第二案”以来,许多学者认为美国必须对其本国的监控法律体系进行实质性改革,这是其重新获

得欧盟充分性认定的先决条件。尽管《关于加强美国信号情报活动保障措施的行政命令》对美国当局的信号情报活动施加了一些新的限制,但美国的法律框架总体上仍然为大规模监控保留了广阔的空间。此外,美国为数据权益受损的外国公民提供的救济并不充分。实际上,美国只是在表面上遵循了部分欧盟法律的形式要求,但并未真正落实欧盟从根本上限制大规模监控、保护人权的精神。<sup>②</sup>

#### (1) 未实质改革的美国信号情报法律体系

在错综复杂的美国情报法律体系中,与外国个人隐私数据保护冲突最为明显的是《外国情报监视法案》第702条和总统第12333号行政命令《美国情报活动》(United States Intelligence Activities)。《外国情报监视法案》第702条允许情报部门进行大规模监控,包括对美国境外的非美国公民。该法条为美国的“棱镜”(PRISM)和“上游”(UPSTREAM)监控计划提供了法律依据。而《美国情报活动》行政命令则为美国国家安全局超出公共安全目的的监控行为提供了法律基础,例如允许其通过跨大西洋水底电缆拦截来自欧盟的在途数据,从而规避美国国内数据隐私保护法律的监管。值得注意的是,“数据隐私框架”并未对这两项关键法律进行修订或实质限制。相反,《关于加强美国信号情报活动保障措施的行政命令》在很大程度上只是替代了美国《第28号总统政策指令》,而该指令的部分规定已被撤销。<sup>③</sup> 此外,该指令因对美国情报活动的限制过于简单笼统,而被欧盟法院诟病流于形式,而《关于加强美国

<sup>①</sup> “Commission Implementing Decision Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data under the EU-US Data Privacy Framework”, European Commission, July 10, 2023, [https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework\\_en.pdf](https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf).

<sup>②</sup> Hendrik Mildebrath, *Reaching the EU-US Data Privacy Framework: First Reactions to Executive Order 14086*, European Parliament, 2022, p.6.

<sup>③</sup> “National Security Memorandum on Partial Revocation of Presidential Policy Directive 28”, The White House, October 7, 2022.

信号情报活动保障措施的行政命令》也存在类似问题。

首先,《关于加强美国信号情报活动保障措施的行政命令》规定了12项合法目标,这些目标表面上看似限制了情报活动的实施,但实际上对监控过程和结果的限制并不一定有效。至少在某些情况下,确定特定目标并不能有效地缩小监控和数据收集的范围。以其中一个合法目标“防范外国对网络安全的威胁”为例,保护网络安全涉及的范围非常广泛,该目标理论上可以作为持续监控所有人的所有互联网活动的正当理由。此外,合法目标的设定还存在诸多细节问题。例如,《关于加强美国信号情报活动保障措施的行政命令》允许情报部门以“保护政府财产和防范跨国犯罪威胁”为由实施监控。按照常理推测,轻微破坏公物或者轻微犯罪的案件应当不属于此类,但目标本身并没有明确严重程度这一门槛。更令人担忧的是,行政命令规定总统可以授权更新合法目标清单。而且,如果公布更新的清单会对美国的国家安全构成风险,总统可以选择秘密修改。这一规定直接导致合法目标的限定形同虚设。如果目标清单连自身内容都失去了确定性和公开性,其对情报机构活动的限制与规范则更是无从谈起。

其次,实施信号情报活动应当遵循的必要性和比例性原则存在主观性较大、容易受到自由解释影响的问题。而且,这两个原则比较模糊宽泛,较难在实践中为信号情报活动提供具体指引。必要性和比例性原则是起源于国际法的关键术语,除非美国能够依照国际判例法来解释和应用相关条款,否则将它们纳入行政命令只不过是法律上装点门面。<sup>①</sup>美国司法部在《数据保护审查法庭》条例中明确规定,法庭在解释《关于加强美国信号情报活动保障措施的行政命令》时必须完全根据美国法律及法律传统,而不包括任何其他法律来源。这使得人们难以相信,必要性和比例性测试能够以一种对美国监控活动有实质检查意义的方式进行。<sup>②</sup>此外,比例性原则要求监控活动以与“经过验证

的情报优先级别”相称的方式进行。由于美国国家情报优先级别是保密的,对此只能参考美国国家情报总监发布的非机密的《全球威胁评估》(Worldwide Threat Assessment)。美国国家情报当局倾向于用高度概括的措辞描述威胁,例如“有组织犯罪”和“移民”等,从而给当局进行扩大解释并采取更宽泛的措施提供基础。因此,若情报机构以“更重要的优先事项”为由实施更广泛和更具侵入性的监控,比例性原则反而可能为其提供合理辩护。

综上所述,《关于加强美国信号情报活动保障措施的行政命令》在事实上容纳了大规模收集数据的行为。该行政命令的必要性标准主要考虑合法目标所需,适用于所有形式的监控,并未对大规模收集数据这种高风险的监控形式施加进一步限制。行政命令试图通过约束情报机构收集数据以后的查询、使用、传播、保留等行为来减轻侵犯隐私的问题,这种后端的数据隐私保护方式其实收效甚微,具体可参考已经公布的《外国情报监视法案》法庭意见和监控透明度报告。而根据《美国情报活动》行政命令进行的情报收集活动不受司法监督和审判,其存在的合规问题很可能会更加严重。批量收集不可避免会导致与实现合法目标无关的私人通信或者其他数据被情报机构收集,这种任意的监控形式被欧盟法院谴责为侵犯了隐私权本质,“允许公共当局在普遍基础上获取电子通信内容的立法,必须被视为对《欧盟基本权利宪章》第7条所保障的尊重私人生活的基本权利的精神的违背。”<sup>③</sup>

## (2) 救济机制的局限性

① 欧盟数据主体难以在美国司法救济体系中获得充分的“诉讼资格”。

<sup>①</sup> Elizabeth Goitein, “The Biden Administration’s SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance”, *Just Security*, October 31, 2022, para.16.

<sup>②</sup> Hendrik Mildebrath, *Reaching the EU – US Data Privacy Framework: First Reactions to Executive Order 14086*, European Parliament, 2022, p.7.

<sup>③</sup> “Maximilian Schrems vs. Data Protection Commissioner”, CJEU, Case C-362/14, October 6, 2015.



美国宪法第三条规定的普通联邦法院,理论上可以满足《欧盟基本权利宪章》第47条规定的“独立、公正”法庭的标准。如果欧盟公民能够向此类法院提起诉讼以保护数据隐私权利,那么是可以达到《欧盟基本权利宪章》规定的“获取有效救济”要求的。然而,根据美国宪法第三条,原告在向联邦法院提起诉讼之前,必须证明自己具备“诉讼资格”(standing),即要求其证明已经遭受“事实损害”(injury in fact)。<sup>①</sup>但是,行政部门往往会援引保密条款来阻止诉讼当事人获取相关证据,这使得原告难以证明在情报机构的活动中遭受了事实损害,即使原告已经委托了具有安全许可证明的律师。在少数情况下,即使原告确立了诉讼资格,行政部门又会根据国家机密特权提出驳回起诉的诉讼请求,法院通常会予以支持。美国情报体系的多重保密制度给欧盟公民向联邦法院寻求数据隐私权益救济造成了实质困难,甚至也给美国本国公民带来了类似难题。在美国法院涉及情报机构非法监控的案件中,很少有原告的起诉被法官或陪审团审理。实际上,美国政府通过实施多层保密制度,成功阻止了所有在美国法院提出的质疑情报监控合法性的民事诉讼,因而美国法院从未对《外国情报监视法案》第702条和《美国情报活动》行政命令下监控的合法性问题作出裁决。<sup>②</sup>在美国法律体系中,宪法第四修正案是美国公民对抗非法监控最重要的诉因和最有效的武器。然而,对于与美国没有“重大自愿联系”(significant voluntary connection with the U.S.)的欧盟公民来说,宪法修正案并不适用。

## ② 新的双层救济机制缺乏独立性。

尽管“数据隐私框架”创建的双层救济机制对现状有所改进,但是由于其隶属于美国行政部门,不免被视为隐私盾监察员制度的升级版,而后者已经在“施雷姆斯第二案”中被欧盟法院否定。<sup>③</sup>由于缺乏独立性,新救济机制不能满足《欧盟基本权利宪章》第47条所规定的法庭标准。欧盟法院在2018年的一起判例中,对法庭“独立”的含义作出了具体解释:“有关机构应完全自主地行使其司法职能,不受任何等级限制

或隶属于任何其他机构,并且不受任何来源的命令或指示”。<sup>④</sup>在2019年的一起判例中,欧盟法院进一步强调法庭的独立是提供“有效司法保护”(effective judicial protection)的基本要求。尽管拜登政府采取了一些措施来确保救济机制的独立性,但是组成救济机制第一层的公民自由保护官隶属于国家情报总监办公室,第二层数据保护审查法庭隶属于司法部,这两层救济机制实际上都是美国行政部门分支的组成部分。而且,根据规定,公民自由保护官还必须“适当尊重国家安全官员作出的任何相关决定”。而对于法庭的运转,事实调查由国家情报总监办公室而非法庭进行,法官由司法部长而非情报机构之外的第三方挑选任命,而且总统可以推翻法庭的裁决。可见,法庭并非如欧盟法院所要求的那样“完全自主”运作,也没有摆脱“等级限制”。欧盟法院还强调,必须“保护法官免受可能损害其独立判断或影响其决定的外部干预或压力”,并指出有关法官任职期限和解职规则必须“消除个人心中关于该机构是否受外部因素影响及能否在利益面前保持中立的任何合理怀疑”。<sup>⑤</sup>然而,《关于加强美国信号情报活动保障措施的行政命令》及其配套法律并未限制总统对法官免职的权力。法官四年任期期满以后的续任,也依赖于行政部门。这些情况都与欧盟法院保护法官免受干预、保持法官独立自主的精神相悖,可能导致产生有偏见的裁决。

① 巩固:“美国原告资格演变及对公民诉讼的影响解析”,《法制与社会发展》,2017年第4期,第123页。

② Ashley Gorski, “The Biden Administration’s SIGINT Executive Order, Part II: Redress for Unlawful Surveillance”, Just Security, November 4, 2022, <https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/>, para.11.

③ 刘文杰:“美欧数据跨境流动的规则博弈及走向”,《国际问题研究》,2022年第6期,第78页。

④ “Associação Sindical dos Juizes Portugueses vs. Tribunal de Contas”, CJEU, Case C-64/16, February 27, 2018.

⑤ “European Commission vs. Republic of Poland”, CJEU, Case C-619/18, June 24, 2019, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=215341&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=224379>.

### 3.3 各利益相关方评价

美国的数据隐私保护状况尽管获得了欧盟委员会的肯定,但是各方对其评价不一。欧洲多国的地区数据保护机构在认可美国进步的同时,对其是否能像欧盟一样将公民数据隐私权利作为基础权利进行保护表示担忧;大多数字权利组织和隐私保护组织也认为美国的数据隐私保护水平未能达到欧盟标准,两者之间仍然存在明显差距;甚至有学者提议美国国会从根本上修订情报法律体系以符合欧盟的“实质等同”要求。<sup>①</sup> 国际商会数据保护工作组主席库勒(Christopher Kuner)指出,欧盟希望通过《隐私盾协议》、其他充分性认定或标准合同条款这类程序性机制,在美国的法律实践中达到保护数据与隐私权利的目标,这只是一种不切实际的想象。因为这些机制无法为个人数据提供能够对抗美国情报收集活动与政府监控的保护。<sup>②</sup> 而考虑到欧美之间恢复个人数据自由流动所带来的巨大经济收益,如为企业节约合规成本、降低数据转移至美国后的潜在风险、创造更加稳定的商业环境等,部分行业协会如数字欧洲和信息技术工业委员会则高度肯定了充分性认定决议的意义。<sup>③</sup>

欧盟和美国在数据跨境流动问题上的立场不同,因此很难找到根本的解决方案。随着国际数字贸易蓬勃发展,双方在此领域的竞争和妥协将持续存在。虽然美国在最新达成的“数据隐私框架”中并未真正改革其信号情报法律体系,并且创建的双层救济机制存在明显的独立性问题,但是美国在本次博弈中已经作出了几次重大让步,进一步协商弱化其国家安全法律将更加不符合美国的利益。<sup>④</sup> 有学者认为,使用行政命令和司法部法规相结合的非法定方法来取代《隐私盾协议》是目前美国成文法和宪法结构中最切实可行的方案。<sup>⑤</sup> 因为无论是要求美国实质性改革本国的信号情报法律体系,以更有效地限制信号情报的收集使用,还是颁布相应法律,允许欧盟数据主体就美国情报机构的不当监控行为向联邦法院提起诉讼,都将面

临巨大的政治和法律障碍。<sup>⑥</sup> 虽然美国当前的数据隐私保护水平与欧盟的期望可能还存在一定的差距,但是考虑到高效的数据跨境流动对跨大西洋数字经济关系至关重要,欧盟委员会仍然通过了关于美国数据保护水平的充分性认定草案,为跨大西洋数字贸易注入了新的活力。

## 四、欧美数据跨境流动规制矛盾的根源分析

欧美双方就“数据隐私框架”的谈判,表面上是两种数据保护理念和治理模式的碰撞,实际上反映了欧盟“技术主权”意识觉醒以后,试图打破美国数字技术垄断地位,摆脱对美国的依赖,实现真正的自主的强烈愿望。欧美关于数据跨境流动规则的博弈,本质上源于欧盟实施“数字主权”战略与美国维护“数字霸权”地位之争,是双方在数字经济时代凭借各自优势争夺全球数字治理话语权。

### 4.1 监控资本主义促进美国互联网巨头崛起

美国互联网巨头的崛起离不开“监控资本主义”(Surveillance Capitalism)。监控资本主义

<sup>①</sup> “New Biden Executive Order on EU-US Data Transfers Fails to Adequately Protect Privacy”, ACLU, October 7, 2022, <https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy>, para.7.

<sup>②</sup> Christopher Kuner, “Reality and Illusion in EU Data Transfer Regulation Post Schrems”, *German Law Journal*, Vol. 18, No.4, 2017, pp.881-918.

<sup>③</sup> Hendrik Mildebrath, *Reaching the EU-US Data Privacy Framework: First Reactions to Executive Order 14086*, European Parliament, 2022, pp.6-8.

<sup>④</sup> Oliver Patel and Dr N. Lea, *EU-U.S. Privacy Shield, Brexit and the Future of Transatlantic Data Flows*, University College London European Institute, 2020, p.15.

<sup>⑤</sup> Paul Rosenzweig, “The ‘Three Rs’ of President Biden’s Trans-Atlantic Privacy Outreach”, *Lawfare*, October 21, 2022, <https://www.lawfareblog.com/three-rs-president-bidens-trans-atlantic-privacy-outreach>, para.25.

<sup>⑥</sup> Theodore Christakis and Kenneth Propp, “EU/US Adequacy Negotiations and the Redress Challenge: How to Create an Independent Authority with Effective Remedy Powers”, *European Law Blog*, February 26, 2022, <https://europeanlawblog.eu/2022/02/16/eu-us-adequacy-negotiations-and-the-redress-challenge-how-to-create-an-independent-authority-with-effective-remedy-powers/>, para.2.



以收集大量用户个人数据为基础,通过数据挖掘与算法分析产出经济效益。这种数据收集与市场化运作已经逐渐成为当今全球数字企业默认的主要商业运行模式。“个人数据的商品化使其成为地球上最具价值的资源之一”。<sup>①</sup>从通讯信息、网页浏览、购物记录、在线支付、运动轨迹到睡眠质量,被监测到的个人数据源源不断地被送回互联网科技平台。通过对这些海量数据的实时收集、存储、深度挖掘及算法分析,企业能够更精准地锁定潜在消费者,以及开发更多符合消费者需求的产品与服务,更好地为广告营销及扩大再生产服务。<sup>②</sup>广泛收集海量数据是大数据分析、机器学习训练、人工智能开发等数字技术发展的基础,过度监管可能会妨碍相关技术进步、造成相关产业萎缩。从根本上讲,欧盟严格的个人数据权利保护制度与监控资本主义的要求是相背离的。

目前美国数字科技巨头凭借技术优势,在全球数字产业链中处于垄断地位,既缺乏有力竞争,也缺乏有效监管。<sup>③</sup>美国大规模监控活动的实施,与其互联网科技巨头的垄断地位息息相关。虽然监控活动名义上只为维护国家安全,但是其获取的各种情报数据可以在国际竞争中转化为技术、经济、政治甚至军事等各方面的优势。美国《澄清域外合法使用数据法》(Clarify Lawful Overseas Use of Data Act,即“云法案”)确立了“数据控制者标准”,打破了他国的主权疆域界限,为其全球“数字霸权”的确立奠定了基础。<sup>④</sup>当前,世界范围内的数据正越来越向美国的数字科技巨头集中,这进一步挤压了各国互联网和数字企业的生存空间,甚至可能威胁到各国的国家安全与独立自主。<sup>⑤</sup>

#### 4.2 欧盟“数字主权”与美国“数字霸权”之争

美国依靠其互联网通信技术的先发优势以及丰富的人才储备,培育了谷歌、微软、脸书、亚马逊四大互联网科技巨头。这四家企业在全世界数字领域确立了行业标准,并占领了巨大的市场份额。随着国家间数字竞争日益政治化,美国采取了多种经济和政治手段来遏制其他国家

的数字信息技术发展,在全球范围内形成了“数字霸权”。<sup>⑥</sup>凭借这种“数字霸权”,美国在国际经济活动中享有特权,并形成了一种更为高效隐蔽的新型财富掠夺方式。<sup>⑦</sup>作为美国第三大数字贸易伙伴的欧盟,虽然拥有强大的科技实力与发达的制造业,却未能孕育出大型的数字科技企业。这使得欧盟在全球数字经济市场所占份额与其经济实力并不相称。而且,美国国家安全利益至上的单边霸权思维给双方的战略合作造成难以弥合的裂痕。<sup>⑧</sup>欧美之间关于数字主权的分歧由来已久,欧洲以增强技术自主为核心实施的“数字主权”战略与美国巩固“数字霸权”以持续攫取利益之间存在明显的结构性冲突。<sup>⑨</sup>虽然欧盟当前的数字经济实力有限,但是其标准和规则在国际经济规制中仍然具有独特和重要的影响力。<sup>⑩</sup>欧盟试图依靠其完善的数据隐私保护制度来主导国际数字治理话语权,维护其在数字时代的利益。这在一定程度上反映了欧盟数据治理规则的布鲁塞尔效应与美国监控资本主义的马太效应之间的对抗。<sup>⑪</sup>为了限制美国数字科技巨头在欧盟的无序扩

① Shoshana Zuboff, “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization”, *Journal of Information Technology*, Vol.30, No.1, 2015, pp.75-89.

② 戴陆:“数字化、控制社会与监控资本主义”,《世界美术》,2021年第4期,第57页。

③ 徐宏潇:“国际数字资本主义的发展动向及其内在悖论”,《经济学家》,2020年第2期,第57页。

④ 冯硕:“美国数据霸权的建构与法律应对”,《太平洋学报》,2023年第8期,第48页。

⑤ 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”,《西安交通大学学报(社会科学版)》,2021年第5期,第98页。

⑥ 钱爱兵:“信息化进程中的数字霸权现象分析”,《情报科学》,2003年第5期,第545页。

⑦ 刘皓琰:“数据霸权与数字帝国主义的新型掠夺”,《当代经济研究》,2021年第2期,第28页。

⑧ 刘文杰:“美欧数据跨境流动的规制博弈及走向”,《国际问题研究》,2022年第6期,第65页。

⑨ 闫广、忻华:“中美欧竞争背景下的欧盟‘数字主权’战略研究”,《国际关系研究》,2023年第3期,第83页。

⑩ Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020, p.68.

⑪ 李艳华:“隐私盾案后欧美数据的跨境流动监管及中国对策——软数据本地化机制的走向与标准合同条款路径的革新”,《欧洲研究》,2021年第6期,第25页。

张,并为本土互联网科技企业的成长创造空间,欧盟采取了多项措施,并颁布了一系列数据相关法案。除了推行数字服务税试图将美国科技巨头攫取的数字红利留在欧洲以外,欧盟还在2022年先后通过了《数据治理法案》(Data Governance Act)、《数字市场法案》(Digital Markets Act)和《数字服务法案》(Digital Services Act)。随后,欧盟进一步完善了《数据治理法案》,将其修订为《数据法案》(Data Act)。

《数字市场法案》主要针对大型互联网企业滥用市场支配地位的不公平竞争行为。该法案根据特定标准认定部分大型在线平台为“守门人”企业,对其规定了具体的“应为”和“不应为”义务,对违反规定的企业规定了明确的惩罚措施,包括罚款甚至“行为性或结构性救济措施”,例如剥离部分业务。欧盟认定的“守门人”企业多数来自美国,因此该法案也被视为针对美国数字科技巨头制定的最新义务清单。《数字服务法案》旨在创造更加安全的数字空间与保障用户的基本权利,为此加强了对互联网平台问题的治理,尤其强调平台对于内容的监管义务。而且,该法案要求互联网平台向欧洲监管机构公开其进行内容推荐的算法,以增强欧盟对内容自主管控的力度。《数字服务法案》规定的许多义务仅适用于在欧洲拥有超过4500万用户的大型平台,多数为美国企业(脸书、推特和优兔等都包含在内),违者可能面临高至全球年营业总额6%的罚款。<sup>①</sup>《数据法案》旨在按照欧盟的规则和价值观为数字市场提供更多可用数据,以激发欧盟数字经济活力。

综上所述,欧盟力图通过各种政策手段压制互联网数字巨头广泛存在的赢家通吃局面,为本土中小企业参与竞争和创新创造公平友好的环境。同时,欧盟还致力于塑造数字经济和数据治理规则,使欧盟成为数据驱动型社会的领导者。欧盟迫切希望掌控数字技术主权,减少欧盟成员国对外关键技术依赖,提升欧盟在数字时代设定自身规则与价值观的能力,最终重新定义更为对等的跨大西洋伙伴关系。面对欧盟利用数字规则发出的挑战,美国一方面在

“数据隐私框架”磋商中坚定维护本国的信号情报法律体系,一方面凭借其数字技术优势和数字科技巨头的国际垄断地位推动相关国际标准和规则的制定。此外,美国还加快了国内综合性数据隐私保护立法的进程。美国参议两院在2022年6月共同发布了《美国数据隐私和保护法》(American Data Privacy and Protection Act)草案,这是美国首次在联邦而非单个州的层面提出此类立法。

### 4.3 争夺全球数字治理话语权

欧美都力图将各自的数据治理理念和模式推广为全球范本,不仅在双方的数据跨境流动安排中展开了直接交锋,而且在国际层面展开了关于数据保护和数据跨境流动标准制定的博弈,争夺全球数字治理话语权。欧盟和美国分别借助国内规则的向外流动打造出符合各自利益的数据流动圈,在国际上形成了由欧盟和美国两大规制体系主导的数字治理基本格局。<sup>②</sup>

欧盟凭借其数据隐私保护立法的先发优势,不断向国际社会输出规则,扩大其数据治理规则的国际影响力。欧盟一方面通过《一般数据保护条例》为其成员国的数据跨境流动提供统一标准,着力打造内部数字单一市场;另一方面凭借《一般数据保护条例》的“充分性保护水平认定”机制建立了数据跨境自由流动的白名单,将加拿大、日本、阿根廷等诸多国家和地区纳入其数据治理阵营。由于欧盟《一般数据保护条例》域外适用广泛且法律模式可移植性高,已经在事实上成为全球数据保护的标杆,俄罗斯、日本、韩国、巴西、智利等国家在制定本国数据保护法律时都以其为参照范本。为了扩大与欧盟的数字经贸合作空间,部分国家还按照欧盟标准提升了本国的数据保护水平。

<sup>①</sup> 朱兆一、陈欣:“美国‘数字霸权’语境下的中美欧‘数字博弈’分析”,《国际论坛》,2022年第3期,第66页。

<sup>②</sup> 王佳宜、王子岩:“个人数据跨境流动规则的欧美博弈及中国因应——基于双重外部性视角”,《电子政务》,2022年第5期,第101页。

美国则主要通过多边和双边协议强化其对规则的主导权。首先,美国利用其在经济合作与发展组织(OECD)、二十国集团(G20)、亚太经济合作组织(APEC)等国际组织中的优势地位,大力推行其倡导的数据跨境自由流动和反对数据本地化理念,主导发布在信息化背景下国际上首份关于数据跨境流动的法律文件《关于隐私保护与个人数据跨境流动的指南》(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data),并且借助亚太经济合作组织建立的跨境隐私规则体系(Cross-Border Privacy Rules System)扩大了美国在亚太地区制定规则的话语权。此外,美国将数据流动议题纳入自由贸易协定规制范围,利用其在谈判中的传统主动地位,借助一揽子协议将其数据治理理念与模式向经贸合作国家强势推广,并且试图在全球推进具备法律约束力的跨境数据流动规则体系。<sup>①</sup> 美国在今后的自由贸易协定谈判中还将继续深化数据跨境流动条款,谋求制定更高水平的数据跨境流动规则。<sup>②</sup>

## 五、欧美数据跨境流动的规则 博弈带给中国的思考

数据监管已成为国际竞争的新领域。欧美都力图将各自的数据治理理念和模式推广为全球范本,在双方的数据跨境流动安排中展开了直接交锋。数据治理话语权的博弈已经超出经济范畴,与政治甚至意识形态问题交织。如何选择适合本土的数据监管模式,如何应对欧美在数据治理话语权方面的博弈,是值得我国思考的重要议题。

### 5.1 注重我国数字经济与欧盟的差异,兼顾数据进出口的平衡发展

“施雷姆斯第二案”是欧盟输出数据法律规则的又一成功实践。欧盟立法者有意在数据流动监管中嵌入具有扩张功能的概念和规则,旨在将其数据治理理念和模式推向全球,这其中也包括我国。我国的数据治理法律体系,包括

数据跨境流动规则,在很大程度上借鉴了欧盟《一般数据保护条例》的核心概念和典型制度。这种法律移植短期内填补了国内数据法律体系的空白,具有积极意义。然而,每个国家的经济、政治、社会、文化、价值观和优先发展事项等情况都不尽相同,因此数据监管模式也应当因地制宜,没有普适的“黄金标准”。在数字治理法律体系已经形成的情况下,我国应更加注重结合本国具体国情,选择更适合本土的数据监管模式。

我国的数字经济发展情况与欧盟存在显著差异。在欧盟这一数字经济的“洼地”,未能培育出大规模的互联网企业,而中国孕育了诸如字节跳动、腾讯和阿里巴巴等具有国际竞争力的互联网企业。欧盟数据治理的重点在于通过实施严格的数据流出政策来保护数据主体的权利,深层次的经济动机在于遏制外国互联网巨头的扩张,为本土中小企业的发展创造空间。相比之下,我国在考虑数据流出风险的同时,还需顾及本国互联网企业在海外运营时将数据传输回国内的需求。当前,我国和欧盟都高度重视防范跨境数据流出的风险。但是,过于严格的数据跨境流动政策可能引发他国的反制措施,不利于我国互联网企业在海外运营的数据回流,从而制约其进一步发展。因此,我国应避免盲目采纳欧盟模式的立法惯性或立法惰性,而应适度放宽对商业数据跨境流动的审查限制,兼顾数据进出口的平衡发展。<sup>③</sup>

### 5.2 培育我国的数据市场规模,提升数据治理规则制定的话语权

欧盟成熟的数据市场对于“布鲁塞尔效应”(欧盟凭借市场力量单方面监管全球市场的能力)的发挥起到了关键作用,而跨国企业在其中扮演了不可或缺的角色。欧盟的数据法律主要

<sup>①</sup> 蔡翠红、郭威:“中美跨境数据流动政策比较分析”,《太平洋学报》,2022年第3期,第32页。

<sup>②</sup> 李墨丝:“欧美日跨境数据流动规则的博弈与合作”,《国际贸易》,2021年第2期,第83页。

<sup>③</sup> 徐程锦:“WTO电子商务规则谈判与中国的应对方案”,《国际经济评论》,2020年第3期,第49页。



目的在于规范内部市场,由于跨国企业无法舍弃欧盟市场,它们不得不接受欧盟的监管,并按照欧盟的规则调整其运营行为。并且,为了便于内部管理和节约运营成本,跨国公司有动力在全球分支机构中推行符合欧盟标准的统一规则。<sup>①</sup>此外,为了确保与国内非出口型企业竞争的优势,跨国企业还有动力游说本国采纳欧盟的数据立法模式。而且,它们不仅有资本,还有能力在制度的支持下实现这一目标。最终,欧盟标准不仅在经济层面上,而且在法律层面上转化为全球标准。可见,欧盟数据治理模式的全球扩张高度依赖于欧盟市场的全球影响力,这是全球数据监管竞争的基础逻辑。<sup>②</sup>美国在“施雷姆斯第二案”后作出让步,与欧盟达成“数据隐私框架”,主要原因正是看重欧盟的市场规模。因此,我国若想在数据全球规制中拥有话语权,最有效的途径之一就是进一步培育本土的数据市场规模。随着跨国企业在我国市场的数据产品和服务出口比例增加,我国在全球数据规则制定方面的影响力也将逐步提升。

我国拥有庞大的网民基数,这是我国发展大规模数据市场的比较优势。为了培育我国的数据市场规模,需要建立高效的数据流通和交易制度,重点在于尊重自由市场原则和合同自由原则。在自由市场中,数据作为商品可以进行自由交换和流通,从而促进数据共享。企业可以根据市场需求自主决定数据的收集、处理和使用方式,从而提高数据的质量和价值。自由市场原则还有利于激发市场主体的活力和创造力,推动数据市场的竞争和创新。此外,自由市场原则可以促进数据的跨境流动和国际合作,推动全球数据市场的形成和发展。合同自由原则在培育数据市场中也可发挥重要作用。通过合同约定,交易双方可以明确数据权属、使用范围、保密义务等事项,减少纠纷和冲突的发生。同时,合同自由原则有助于提高市场的透明度和可预测性。总之,在培育数据市场的过程中,应充分尊重和发挥自由市场原则和合同自由原则的作用,为数据市场的健康发展提供有力的支持。

### 5.3 完善立法机关和企业之间的沟通机制,助力我国数字企业发展

欧盟法院虽然先后判定《安全港协议》和《隐私盾协议》失效,但是在美国并未对本国情报法律体系作出根本改革的情况下,欧美又达成了“数据隐私框架”,恢复了双方之间的数据流动秩序,足见数字经济实力和技术实力在数字经济体国际交往中的决定性作用。美国数字科技巨头的成长与其国内法律体制的保障密不可分。无论是达成“数据隐私框架”和签署《关于加强美国信号情报活动保障措施的行政命令》以满足美国互联网企业在欧盟开展业务的需求,还是2018年颁布《澄清域外合法使用数据法》为美国获取境外数据提供法律基础,都充分体现了美国数字企业的利益。这些法律文件的及时发布与美国政治中的游说制度紧密相关。美国的经济利益集团通过游说制度影响立法进程,确保立法能够充分回应企业的需求并保障其利益。

我国互联网企业在海外发展面临诸多挑战,如何将这些实际需求及时、高效地传达给立法机关,以增强立法的科学性和针对性,为企业的海外发展保驾护航,为其与美国互联网企业之间的竞争提供助力,是一个值得深思的问题。为了加强我国立法机关和企业之间的沟通,可以从以下几个方面进行尝试:一是加强立法前的调研和论证,深入了解数字企业的需求和痛点。可以通过问卷调查、实地走访、座谈会等方式收集数字企业的建议,并邀请相关领域的专家学者和数字企业代表等参与立法前的论证,对数字企业的发展需求进行充分讨论和评估,以确保法律法规的科学性和合理性。二是健全反馈机制,及时收集数字企业在法律法规实施后的意见和建议,对法律法规进行相应完善和调整。这些措施有助于优化立法机关和企业之间的沟通机制,助力我国数字企业发展。

<sup>①</sup> Anu Bradford, “The Brussels Effect”, *Northwestern University Law Review*, Vol.107, No.1, 2012, p.159.

<sup>②</sup> 金晶:“欧盟的规则,全球的标准?数据跨境流动监管的‘逐顶竞争’”,《中外法学》,2023年第1期,第64页。

## 六、结 语

从《安全港协议》到《隐私盾协议》，再到2022年的“数据隐私框架”，欧盟和美国二十多年以来就双方的数据跨境流动制度安排展开了多轮博弈。《隐私盾协议》的失效，本质上是欧盟在“数字主权”战略下凭借其数据隐私规制话语权对美国牵制的一种反制。而“数据隐私框架”的达成，则是欧盟考虑到“跨大西洋数据流

动对于促成欧美之间价值7.1万亿美元的经济关系至关重要”而作出的妥协<sup>①</sup>。随着数字技术政治化趋势的加剧以及中美战略竞争的升级，我国需要更加谨慎妥善地处理与美国和欧盟的数字博弈关系。作为数字地缘版图中的重要经济体，中美欧如何在数字网络空间进行相互尊重、合作共赢的包容性竞争，如何以多边力量共同推动全球数字技术进步和维护数字空间秩序，是全球数字治理面临的新课题。

责任编辑 邓文科

## A View of Conflict and Coordination of Cross-border Data Flow between the EU and the U.S. through Data Privacy Framework

SHAN Wenhua<sup>1</sup> DENG Na<sup>1</sup>

(1. Xi'an Jiaotong University, Xi'an 710049, China)

**Abstract:** After the invalidation of the Privacy Shield, the EU and the U.S. established the Data Privacy Framework in late 2022 to restore the order of cross-border data flow between them. The Data Privacy Framework was designed to address the main concerns raised by the Court of Justice of the European Union (CJEU) in the Schrems II case, and the European Commission issued a decision on the adequate level of protection of personal data based on the framework in July 2023. However, the Data Privacy Framework has failed to impose significant constraints on the capabilities of the U.S. intelligence agencies to conduct large-scale data collection and mass surveillance. Additionally, the two-tier relief mechanism does not provide adequate and effective relief to the EU citizens whose data privacy rights are violated in the U.S. due to a lack of independence. In fact, the Data Privacy Framework doesn't make an essential breakthrough compared to the Privacy Shield. On the surface, the divergence in the arrangement of the cross-border data flow between the EU and the U.S. is a collision of two different concepts and governance models of data protection, reflecting the fundamental conflict of interest between the European digital sovereignty and the U.S. maintenance of digital hegemony. The two sides are competing for the right to speak on global data governance in the era of digital economy by virtue of their respective advantages. The competition between the EU and the U.S. over the Data Privacy Framework offers valuable insights for China in selecting an appropriate model of data supervision and enhancing its influence in the field of rules of data governance.

**Key words:** Privacy Shield; cross-border data flow; Data Privacy Framework; digital sovereignty; digital hegemony

<sup>①</sup> “Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework”, The White House, October 7, 2022.