从分歧到共识:欧美数据跨境流动合作的逻辑

韩关锋

[内容摘要] 在数据治理规则日益碎片化的国际趋势下,欧盟和美国拥有二十多年的数据跨境传输经验,体现出双方在弥合数据保护鸿沟方面采取的努力。本文通过对欧美数据跨境流动的三次合作经历进行总结,归纳出双方在价值考量、规制路径和责任分配方面所遵循的逻辑共性。欧美数据治理在价值理念和制度体系方面存在的"深层次"差异并不妨碍它们进行"浅层次"的合作,原因在于双方均认可对立统一的价值角力、内外结合的双重规制、控权授权的责任平衡。我国在与"一带一路"沿线国家开展跨境数据合作时,应转变过度强调数据流动保护的理念、慎重考虑政府参与监管的方式、塑造良好的外在形象。

[关键词] 数据跨境流动 价值考量 规制路径 责任分配 合作逻辑

[作者简介] 韩关锋,中国政法大学刑事司法学院博士研究生

[中图分类号]D871 [文献标识码] A [文章编号]2095-5715(2024)03-0135-20

数据已经成为比肩土地、劳动力、资本、技术的"第五要素",其价值的发挥高度依赖规模质量、多源融合和应用场景,因此必须通过流通才能创造出更大价值。习近平总书记在2022年11月9日的世界互联网大会上强调:"数据互联互通是网络空间的基本属性,共享共治是互联网发展的共同愿景"。[①] 在数据大航海时代,数据跨境流动治理已经成为时代发展的必然要求。相较于国境之内的数据治理,跨境治理的难度更高,因为数据所承载的信息包含多重价值取向,其深层次冲突难以轻易弥合。同时,数据跨境传输所带来的数字标准和规则更是

① 《携手构建网络空间命运共同体》,https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm。

地缘政治竞争的重要组成部分,因此治理数据跨境传输并不只是简单的规则制定,而是不同意识形态的调和妥协。

欧美自《安全港协议》签订以来,已有二十多年的数据跨境流动治理经验,而我国在数据流通领域的的双边、多边协作经验匮乏。因此,本文以欧盟和美国三次合作历程为出发点,总结数据跨境流动的治理逻辑。回顾已有研究,学者们一方面进行横向对比,开展欧美数据跨境流动治理分歧的溯源,即通过对比技术能力差异、法律文化冲突、价值主张分歧[①]等方面,将已有的《安全港协议》和《隐私盾协议》视为美国的数据自由流动规则向欧盟的严格保护规则的妥协。另一方面,学者们进行形式上的纵向对比,分析欧美数据跨境流动协议的演进历程,阐述前两代传输协议的立、废过程及具体规则异同。以上两种研究思路均是以欧美数据治理中的"差异"为出发点,将数据跨境传输协议视为两者博弈的产物,强调规则差异是造成跨境传输协议破裂的原因。然而,明确破裂的原因只是开始,重要的是探寻如何在求同存异的基础上达成共识。美欧双方的规则理念虽然有分歧,但双方也有共同的利益诉求,例如近似的意识形态背景、共同的经济发展需求和国家安全保障方面的相互依赖。这些共同诉求正是合意达成所需要的坚定基础。因此,本文进行实质上的纵向对比,在既有差异基础上探寻弥合分歧的方法,总结欧美数据跨境流动治理中秉承的价值考量、规制路径和责任分配逻辑,并以此提出对我国的启示。

一、数据跨境流动中的价值考量

欧美数据跨境传输合意的达成和终止从动机上看是美国监控资本主义的"马太效应"和欧盟"布鲁塞尔效应"对抗的结果,[②]实质上是欧盟"人权话语"和

① 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》,《情报杂志》2022 年第 11 期,第 90 页。

② 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 99 页。

美国“市场话语”间价值分歧引发制度冲突的结果。[①] 因此,合作与对抗只是表象,本质上是价值取向的嬗变和平衡。数据跨境流动会对国家安全、社会经济、个人隐私直接产生外部性影响,数据流通双方均希望增加正外部性而减少负外部性,这种趋利性选择并非总是零和博弈,在特定事件和历史因素影响下,双方会相互妥协从而在正负外部性上达成“帕累托最优”,为合作的形成预留斡旋空间。

(一)个人隐私

民众对隐私观念的认识形塑于社会中的法律传统和文化底蕴,美国和欧盟在个人隐私保护问题上的分歧来源于双方不同的社会、政治和法律传统。[②] 欧盟各国从法西斯主义和纳粹主义的毁灭经历中认识到捍卫人类尊严的重要性,将个人隐私保护视为一项基于尊严、人格和自决利益的基本权利,并将其上升至超国家的基本权利体系之中,镌刻在《欧洲人权公约》和《基本权利宪章》这两大支柱上,这种价值取向对制度设计的影响就是个人权利必须以成文法的形式予以保护,所有个人数据的处理都需要有法律依据。[③] 美国社会把自由主义奉为圭臬,其社会传统建筑在实用主义的意识形态上,自由主义就是在实用主义“树干”上开花结果,进而生成了自由、民主、人权等价值原则。[④] 因此,美国在个人隐私保护上排斥政府的过度干预,把个人数据更多视为一种商品,倡导以市场为主导、行业自律为中心的保护方式,国家保障数据的自由流动和公平交易。美国将“隐私警察”的职责分配给联邦贸易委员会,其目的在于维护个人数据交易的公平性和防止欺诈。

欧盟和美国虽然在个人隐私保护的内容和路径上有所差异,但均认可隐私保护的重要意义和既有保护路径的局限性。而且数据自由流动符合双方共同的政治经济利益。这种差异中的统一成为双方利益联结的纽带,促使双方不断以

---

① 彭岳:《贸易规制视域下数据隐私保护的冲突与解决》,《比较法研究》2018 年第 4 期,第 29 页。

② James Q. Whitman, “The Two Western Cultures of Privacy: Dignity Versus Liberty,” *Yale Law Journal*, Vol. 113, No. 6, 2003, p. 1160.

③ Paul M. Schwartz and Karl-Nikolaus Peifer, “Structuring International Data Privacy Law,” *International Data Privacy Law*, Vol. 21, 2019, pp. 5 ~ 8.

④ 赵可金、倪世雄:《自由主义与美国的外交政策》,《复旦学报(社会科学版)》2006 年第 2 期,第 11 页。

搁置争议或折中的方式寻求最优解。一方面,数据流动和权利保护并不应寻求平衡,因为平衡这个词本身暗含着零和关系,自由流动和权利保护是一体两面,密不可分的关系,应该同等重视,而不是厚此薄彼过分追求某一目标。因此数据规则的制订应当是实现多目标优化,将数据流动限制在可控范围。另一方面,知情同意原则虽然是实现个人信息自决的重要手段,但美欧双方也深刻认识到该手段具有结构化缺陷并且容易陷入认知障碍,因此美国通过对公司施加披露要求来创造信息隐私的不可剥夺性,欧盟对个人交易或放弃这些权利的能力加以限制,将重要数据的隐私权置于个人交易能力之外,[①]双方的保护路径虽然不同但目的是一致的。

(二)国家安全

数据跨境传输后对个人隐私最大的威胁来源于企业滥用,对国家安全最大的威胁来源于数据流入国的情报部门。欧美数据跨境传输的单向性使欧盟各国的国家安全暴露在美国的监视和威胁之下,2013 年的“棱镜门”事件将这种担忧推向顶点,直接导致《安全港协议》的破裂。表面上看这种不平等关系使得数据跨境传输难以为继,实际上,对国家安全的共同关切有助于弥合双方的利益差异。

一方面,对监督情报机构权力的文化认同是消除双方分歧的内生动力。这种文化传统体现在三个方面:一是公众对政府权力固有的不信任感。以美国为例,美国民众认为政府权力具有天然的侵犯性和扩张性,不受制约的权力极易导致滥用和腐败,因此情报机构也是会滥用权力的怪胎,必须用正式或者非正式的约束机制来规范其活动,防止其凌驾于法律之上。[②] 二是对知情权、政府透明度,以及政府责任的捍卫和追求。在西方民主理论中,知情权是提高政府透明度的有力武器,透明度是确保政府承担责任的前提,三者环环相扣,相互依存,因而情报机构在保卫国家安全的同时不能损害公民的自由民主权利和国家的民主法治秩序,必须主动履行告知义务、对民众负责、接受民众监督。[③] 例如,欧盟鼓励企

① Paul M. Schwartz and Karl-Nikolaus Peifer, “Structuring International Data Privacy Law,” *International Data Privacy Law*, Vol. 21, 2019, pp. 8 ~ 9.

② 汪明敏:《美国情报监督机制研究》(第 1 版),光明日报出版社 2013 年版,第 91 ~ 97 页。

③ 同上,第 94 页。

业定期发布透明度报告以说明情报机构请求访问个人信息的数量,要求美国情报机构的手段和目的必须符合比例原则,受到第三方的监督和控制。三是对情报文化的秘密传统感到不安和质疑。秘密性是情报工作与生俱来的特点,在民众看来,秘密是民主的敌人,[①]容易滋生欺骗和蒙蔽,在民主法治的社会中,公开才是社会的主基调,因此在欧盟和美国的个人数据保护过程中,公民的知情权和选择权是最基本的权利。

另一方面,抵御共同外部风险的安全需求是双方跨境合作的外在压力。冷战结束后,欧亚大陆的地缘政治竞争更加激烈,国家安全观发展为包含多元诉求的"综合安全观",开始从强调建立在"战争与和平"之上的"传统安全"向"非传统安全"转变,安全的覆盖范围也由单一的军事和政治安全向社会、环境、经济、反恐领域扩展。[②] 欧盟和美国是推动和影响全球治理进程的重要行为体,二者近似的意识形态和密不可分的经济贸易联系促使双方形成安全共同体,尤其是面对俄罗斯军事威胁以及地区重大安全问题时,两者保持高度一致,结成紧密盟友关系,以西方阵营的身份团结一致,捍卫共同价值观。然而,这种联盟不是一种静态结构,在回应自身内在动力以及政治、经济和社会环境的变化时,会经历不断的转变。正如苏珊·斯特兰奇的结构性权力理论所述:安全关切处于核心地位,谁在安全上受制于人,谁就会在政治经济等方面失去权力和自主性。[③] 当欧盟需要美国的军事庇护以应对外部威胁时,双方内部矛盾暂时被忽视,其他利益关切就会减弱,一旦外部威胁发生变化,安全关切的地位下降,双方的内部矛盾又会显现。

(三)社会经济

数据跨境自由流动虽然会对个人隐私和国家安全造成威胁,但对双方经济发展的促进作用也是显而易见的。工业4.0驱动的新一轮工业革命的核心特征是人—物的互联互通,其严重依赖互联网技术来降低产销之间的信息不对称,实

① Pat M. Holt, *Secret Intelligence and Public Policy: A Dilemma of Democracy*, Washington, D. C.: CQ Press, 1994, p. 9.

② 许可:《自由与安全:数据跨境流动的中国方案》,《环球法律评论》2021年第1期,第31页。

③ 宋芳:《地缘政治竞争中的"软制衡"与"新遏制"》,南京大学博士学位论文2020年,第55页。

现供求双方的联系和反馈。欧美数据跨境传输协议消除了法律缺失造成的合作障碍,为数据流动提供一个新的安全框架,可以确保欧盟与美国企业能够持续稳定的开展跨境电子商务活动,这有助于双方数字经济持续稳定增长。美国白宫表示:“跨大西洋的数据流动对于促成价值 7.1 万亿美元的经济关系至关重要,超过 5000 家欧美企业——其中 70% 是中小型企业——依赖于之前的隐私盾协议,数据跨境传输框架将是恢复跨大西洋数据流动的重要法律基础。”①

除了繁荣国内经济,数据跨境流动还有助于强化欧美数字联盟关系,共同应对以中国为代表的新兴国际经济力量崛起带来的挑战。欧盟贸易总司长萨宾·韦恩德表示:国际秩序已经从基于规则的体系向基于权力的体系转变,欧盟、美国和其他志同道合的民主政府应该团结合作,共同应对那些通过技术和数字规则来强化自身威权的国家所带来的挑战。② 在西方看来,中国和俄罗斯等其他一些国家正在推进一个以国家为中心的威权体制,其对内以国家政权参与甚至主导数字技术的发展,排斥国外数字企业,有违自由市场经济所尊崇的公平、公正原则,对外把“数字威权主义”治理模式推向发展中国家,输出有关治理的意识形态原则和实施这一意识形态观念的威权剧本。“数字威权主义”不但破坏了民主和开放社会的基本原则,而且还要重塑数字时代的国际秩序和国际规则。③ 因此,欧美只有携手合作打造“科技联盟”,利用统一市场的力量,才能在开放的数字经济竞争中获胜,而数据的无缝跨境转移和法律的确定性是在全球数字化经济中实现民主参与的关键,同时也是推进新兴技术、数字安全,以及市场导向原则的关键。因此为了跨大西洋安全、繁荣和共同的价值观,欧美必须在数字领域建立更加紧密的联系。

(四)逻辑关系

欧美数据跨境流动在合作与冲突之间的不断摇摆反映了双方在个人隐私、

---

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

② Frances Burwell and Kenneth Propp, “Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy”, https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-in-practice-the-eus-push-to-shape-the-new-global-economy/, p. 1.

③ 刘国柱:《“数字威权主义”论与数字时代的大国竞争》,《美国研究》2022 年第 2 期,第 36 页。

国家安全、社会经济三方面的对立统一关系,即三者在欧美立法者和决策者那里并没有割裂,相反却始终并行不悖,只要政治需要且可行,任何一个理由都可以被选择并亮出,且这个理由既可导向矛盾,也可导向合作。[①] 双方并没有将某一价值目标绝对化和神圣化,而是以共同认可的基础为桥梁,在特定技术条件和时代背景下不断平衡不同主体利益和立法目标。[②] 例如,在"9.11"事件后,打击恐怖主义、重塑国家安全成为小布什政府的首要目标,[③]欧盟也在随后的伦敦暴恐事件中深刻认识到恐怖袭击的严重危害,在《欧洲安全战略》中指出欧洲面临新的、多元的、更隐蔽且难以预测的三大战略威胁,并将恐怖主义列为首要威胁。[④] 此时,双方均把国家安全诉求上升到首位,强化情报系统的地位和运作效能,因此,第一代数据传输协议《安全港协议》对情报机构的数据滥用行为关注度不多。"斯诺登事件"引发了欧美民众对情报界的信任危机,这种情报活动与西方所宣扬的"自由""人权"等理念背道而驰,极大提升了人们对情报监控的关注和争论,此时,美欧双方在个人隐私和国家安全方面的分歧就得到放大,直接导致第一代和第二代数据传输协议的破产。又如,受新冠疫情和俄乌冲突的影响,欧美受到经济下行和通货膨胀的压力,数字经济是全球要素资源重组、经济结构重塑、竞争格局改变的关键动力,自然成为欧美经济合作的新高地和中美战略博弈的制高点,此时东西方之间则是"敌我矛盾",[⑤]欧美之间虽然在个人隐私和国家安全等方面理念相悖,但仍属于"内部矛盾",因此在发展数字经济的共同需求下,欧美再次合作形成《跨大西洋数据隐私框架》。

二、数据跨境流动的规制路径

三代数据跨境流动协议的最终目标均是要求数据接收国能给予欧盟个人数

① 张丽娟:《美国贸易政策的政治经济学》(第1版),经济科学出版社2017年版,第185页。

② 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106页。

③ 谢海星、钟思礼:《美国国家情报战略研究》(第1版),时事出版社2020年版,第44页。

④ 陈洁:《欧盟反恐战略的发展与挑战》,《世界经济与政治论坛》2016年第1期,第70页。

⑤ 李墨丝:《中美欧博弈背景下的中欧跨境数据流动合作》,《欧洲研究》2021年第6期,第10页。

据与《通用数据保护条例》“实质性等同”的保护水平。为保障个人数据得到充分保护,欧美数据传输协议均采取两条规制路径以防止企业和政府滥用:第一条是在公平信息实践原则指导下的“个人—企业”规制路径,第二条是在元规制理念指导下的“政府—企业”规制路径。两条路径的基本结构显现为一种内外结合的双层嵌套结构(如图 1 所示)。一方面,企业和个人通过“告知—同意”工具获得数据跨境传输的正当依据,并通过隐私设计技术将数据保护措施嵌入到产品开发过程中;另一方面,政府通过程序性制度框架,为企业和个人之间的合意提供约束性架构,也为企业产品设计提供外围指引。

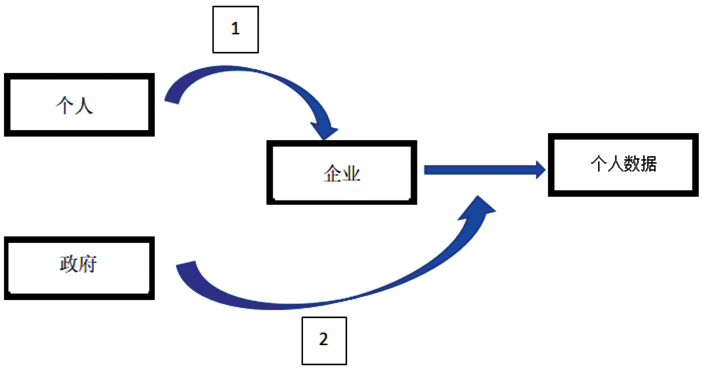

图 1:规制路径

资料来源:作者自制。

(一)“个人—企业”规制路径

该路径来源于公平信息实践原则。公平信息实践原则起源于 20 世纪 70 年代,是现代个人信息保护的基石。从思想渊源与制度架构来说,公平信息实践提供了个人信息保护法或信息隐私法的思想渊源,奠定了现代信息隐私法的框架。[①] 该原则主要指导信息收集和使用,并不针对具体技术和产品,具有很强灵

① 丁晓东:《论个人信息法律保护的思想渊源与基本原理——基于“公平信息实践”的分析》,《现代法学》2019 年第 3 期,第 97 页。

活性和适应性。[①] 其一方面强调个体的自我管理,赋予个体一系列权利,例如个人信息访问权、更正权、修改权等,另一方面对信息处理者施加对应的义务,例如目的限制、数据最小化、透明等。公平信息实践原则在三代传输协议中有鲜明体现,欧盟的《数据保护指令》《通用数据保护条例》和美国的《隐私法》《公平信用报告法》均体现公平信息实践的各项子原则。即使各国对该原则有不同的认识,在个人的权利类型及刚性程度、信息处理者的附加义务和管理义务等方面的具体规定不尽相同,[②]但相关立法总体上包括以下五个方面:通知/意识、选择/同意、访问/参与、完整性/安全性、执行/补救。[③]

该路径以告知与选择机制为主,充分尊重个人的信息自决权,同时注重企业自我规制,将企业作为个人信息传输安全的第一责任人。因此,对主体赋予权力和对企业施加义务是该路径的主要内容。在传输协议中,早期的个人权利主要包括:(1)知情权,获得企业发送的说明书;(2)选择权,当企业向第三方披露、传输敏感信息、信息用途与最初收集目的不同时,个人有权选择退出;(3)救济权,个人具有独立追偿和投诉的渠道。经过三代传输协议的发展,在原有基础上又增加了几项权利:(1)访问权,个人有权访问企业收集的个人信息;(2)更正、修改或删除权;(3)仲裁,获得一个公平、独立且迅速的争议解决渠道。总体而言,这些权利的核心目标是加强个人对自身信息的控制,保证对企业传输行为的知情,并拥有介入的权利,同时通过救济渠道反向约束企业行为。企业的义务主要包括三个方面:(1)针对数据主体享有的权利,企业有配合、响应、协助的义务;(2)传输协议的原则和补充原则中要求采取的实质性义务,例如安全保障和数据继续转移责任;(3)为通过政府认证而履行的程序性义务。“个人—企业”规制路径既可以保障个人不同的信息偏好,又促进了数据合理流动,有学者将其视为一种企业自我规制。同时,该路径镶嵌在隐私政策和设计代码之中,因而也可以被看

① 张涛:《大数据时代“通过设计保护数据”的元规制》,《大连理工大学学报(社会科学版)》2021 年第 2 期,第 80 页。

② 丁晓东:《论个人信息法律保护的思想渊源与基本原理——基于“公平信息实践”的分析》,《现代法学》2019 年第 3 期,第 103 页。

③ 张涛:《大数据时代“通过设计保护数据”的元规制》,《大连理工大学学报(社会科学版)》2021 年第 2 期,第 81 ~ 83 页。

做产品的内部规制。

但是,随着大数据时代的来临,该路径已经逐渐偏离公平信息实践的初衷,显现出形式化和单一化的弊端。美国学者詹姆斯·鲁尔就批判该原则已经沦为“效率”原则,其目的是最大程度消除数据控制者与数据主体之间的冲突,而不是实质性的保护数据控制者利益。[①] 该路径的困境主要体现在两个方面:对企业而言,隐私政策的设计面临结构性挑战,且严格的告知义务导致高昂的合规成本;对个人而言,其有限理性会导致认知障碍,且信息不对称导致其难以预判相关风险。因此,“个人—企业”规制路径虽然为个人信息保护奠定了良好的制度框架,但难以充分满足大数据时代个人合理利用与保护信息的需求,尤其是数据跨境传输过程中,政府角色的缺位导致情报部门滥用职权,这实际上架空了整个个人信息保护体系。

(二)“政府—企业”规制路径

为有效解决企业自我规制的弊病,欧美政府吸收元规制理念,在跨境传输协议的迭代中不断强化政府责任,采取更为复杂、抽象和间接的干预路径。元规制是指对自我规制予以规制的过程,[②]澳大利亚学者克里斯汀·帕克将其总结为“对规制者的规制”。[③] 元规制介于自我规制和政府规制之间,外部规制者并不直接针对问题提出解决方案,而是通过法律设置价值引导,刺激规制对象对问题作出内部式、自我式应答。[④] 元规制适用于“需要解决的问题过于复杂,或者受规制的行业非常特殊且处于动态演进之中”的情况。尤其是信息技术行业,规制者缺少必要的信息资源或者专业技术,对特定市场、行业的运行模式缺少必要的理解,且僵化的规则也难以适应新技术的高速发展。在元规制模式下,政府将其角色定位于掌舵而非划桨,保留有限职责,间接参与治理。政府一方面给予企业一定的自由裁量权,使其能在政府预设的框架内根据自身情况量体裁衣,制订符合

① 张涛:《大数据时代“通过设计保护数据”的元规制》,《大连理工大学学报(社会科学版)》2021 年第 2 期,第 81 页。

② 金健:《德国食品安全领域的元规制》,《中德法学论坛》2018 年第 1 期,第 152 页。

③ 高秦伟:《社会自我规制与行政法的任务》,《中国法学》2015 第 5 期,第 83 页。

④ 程莹:《元规制模式下的数据保护与算法规制》,《法律科学》2019 年第 4 期,第 50 页。

实际的内部行为规范。[①] 另一方面,政府对企业自我规制予以监督和救济,弥补个人与企业之间的权力不平等。相较于传统的“命令—控制”型政府规制,政府角色由自上而下的调控向平行决策转变,把具体规制责任转移给企业,充分发挥企业自我规制所具有的信息优势,利用程序上、组织上、权限上的规范,促使企业在预设的价值目标上实现自我规制,因此能更加灵活、有效地应对市场波动变化,并减少企业合规成本。

在欧美合作过程中,元规制理念的应用主要体现为政府通过设定具体义务推动企业强化内部治理,将数据跨境流动治理的价值取向传输到企业内部的自我规制系统中。因此在构造上存在企业自我规制和政府规制双重面向。为了达到“实质性等同的保护水平”,政府需要为企业预设标准化的程序和框架要求,这些要求的核心是正当程序、透明、可问责。[②] 首先,正当程序主要体现在政府为企业设立了一系列程序要求,用以证明企业满足执行、追偿和救济规则,政府由实质审查转为程序审查,要求企业将需要履行的义务以自我报告或者外部合规审查的形式提交,证明企业已经采取有效机制以确保遵守传输协议所列举的要求。政府为国家情报部门查询和使用个人数据的行为设立了程序保障,确保情报活动的范围和方式符合必要性、相称性和监督原则。其次,透明主要体现在信息披露,用以破除技术壁垒,解决信息不对称问题,企业需要按照透明原则要求通知个人所参与的数据传输协议,还需要定期发布透明度报告说明政府请求查询的信息数量。最后,可问责主要体现在问责和补救机制的建立上,政府规制并不关注个案公正,而是强调企业内部、独立第三方、欧盟数据保护机构的追偿和投诉机制是否合理,能否保证欧盟公民的合法权益得到补救。

(三)逻辑关系

总体上看,两条路径呈现为一种内外结合的双层次嵌套结构,“个人—企业”规制路径作为内部装置直接影响企业的数据保护措施,鼓励企业根据自身行业特点和信息技术优势主动采取措施。措施包括两个方面,一是以隐私政策为代

① 韩新华:《平台时代网络内容治理的元规制模式》,《中国出版》2022 第 5 期,第 51 页。

② 同上,第 52 ~ 53 页。

表的程序性保护,强调信息主体的知情同意权,并对最少必要、目的明确、安全利用等规则也以清晰易懂的方式加以确定。二是以“通过设计保护隐私”为代表的实体性保护,将个人信息保护措施嵌入到技术、商业准则和基础设施的设计标准中。[①] “政府—企业”规制路径作为外部装置间接约束企业的数据保护措施,政府的规章制度和行政命令起到引导、补充和辅助性功能,为企业自我规制提供制度约束和目标激励,引起企业的高度重视和内部回应,相当于为企业自我规制增加了一道“保险阀”,在自我规制不足或目的落空的情况下仍能给于用户最基本的保障,总体上呈现事前指引和事后监督的面貌。因此,在既定价值观的支配下,两条规制路径相互耦合、补充和支持,致力于同一目标的达成,保证个人数据在流出欧盟域外后仍然得到实质等同的保护水平。

三、数据跨境流动中的责任分配

如果说规制路径是数据跨境流动治理的宏观设计,那么责任分配则是微观维度,即在具体操作层面实现双方合意。欧美三代数据跨境合作遵循一个渐进式发展的过程,通过不断的复杂化和精密化的革新来满足日益多元化的需求。每一代的细化责任和落实主体会随着价值取向而变化,但责任分配的逻辑脉络是具有延续性的。根据前文所述,该合作采用两条相互耦合的规制路径,在责任分配上由企业自我规制责任和政府规制责任两部分构成,个人只享有权利而不承担数据的保护责任。

(一)企业规制责任

企业处于两条规制路径的交汇点,要对欧洲公民的权利予以回应,也要承接政府转移的部分监管职能。因此,企业责任处于责任分配的中心地位。

1. 自我认证

需要数据跨境传输的公司应每年通过美国商务部的自我认证及审核程序,

① 高秦伟:《个人信息保护中的企业隐私政策及政府规制》,《法商研究》2019 年第 2 期,第 22 页。

向美国商务部提交相关文件,并通过自我评估或第三方评估的方式证明所做的保护实践是真实存在的。企业即便在主动退出协议后也需要每年提交问卷,以便美国商务部持续追踪其数据保护实践。这种认证方式属于一种“软性”约束工具,用以证明企业的数据保护能力符合一定的法律规范和技术标准,其实质就是通过技术手段和程序控制评判不同企业的数据合规情况及数据保护能力,实现企业数据保护质量的可视化评定。[①] 这种认证方式的优点不仅在于便捷灵活,能有效降低企业的合规成本,还在于其可以消解因信息不对称、政府技术和专业能力欠缺等客观因素而导致的监管困境。

2. 隐私保护

企业应当在产品生产的源头融入价值设计导向,将隐私保护贯穿数据传输前后的整个生命周期,在数据采集、存储、访问、使用、转移、销毁等各环节,采取有针对性的安全防护措施。传输协议中共有 7 条原则,其中 4 条涉及该责任,如第 2 条要求企业在收集信息时提供清晰明确的选择机制以获得个人授权,第 3 条要求企业在数据继续转移的过程中承担延续性保护责任,第 4 条要求企业对出境的数据采取合理或适当措施,防止数据丢失、滥用和未经授权的访问、披露、更改和破坏,第 5 条要求企业必须在授权范围内使用数据,并保障数据的完整性。以上 4 条保护措施不仅需要基于“知情—同意原则”获得授权,还需要在“风险控制理念”下对预期风险进行预判、评估和排序,在产品设计之初或数据流动之前就自动设置防御措施。换言之,授权是数据跨境传输的核心,风险管理是辅助性或补充性的保障措施。

3. 信息透明

信息透明可以定义为个人有效获取企业在运营和决策过程中所使用个人数据的能力,[②]其在西方规则制定者的议程中占有重要地位。美国上世纪 60 年代的

① 张继红:《数据认证:模式选择与应用规范》,《中国政法大学学报》2021 年第 2 期,第 66 页。

② Elisa Bertino et al., “Redefining Data Transparency: A Multidimensional Approach,” *Computer*, Vol. 52, No. 1, 2019, p. 17.

《阳光法案》中正式将公开披露作为监督和问责的重要手段。[①] 根据传输协议要求,企业公开的内容包括:(1)企业参与的传输协议;(2)收集数据的类型;(3)处理的目的;(4)可能向第三方披露的个人数据类型及目的;(5)数据主体享有的权利;(6)企业的联系方式;(7)有效的补救途径;(8)包含以上信息的隐私政策及指向执法机构的网站链接;(9)政府访问个人数据的数量和原因。信息公开是履行保护义务最重要的手段,目的在于消除信息不对称而产生的误解和欺诈行为,是个人理性选择的前提。信息公开的有无和程度决定了企业和用户之间能否充分的互动。虽然隐私政策只是企业的单方承诺,但可以展示企业在自我规制方面的努力,[②]也可以对国家情报机构访问个人数据的行为形成威慑和监督,因此信息公开成为数据跨境传输过程中兼具告知功能和监督功能的制约工具。

(二)政府规制责任

政府角色的引入主要是为了防止国家滥用情报监视权和解决企业自我规制的弊病,因此其责任主要包括以下三个部分:

1. 审核确认

美国商务部的国际贸易管理局负责数据跨境流动的行政管理,对企业的初始认证和年度认证进行审核,总体上采用形式审查加联合评估的方式开展。一方面,政府通过企业提交的自我评估报告或外部合规审查报告确定企业是否严格遵守了原则和补充原则中所列举的各项义务。另一方面,商务部与执法机构、替代性争议解决机构、第三方机构合作,共同验证企业是否积极履行了法定义务。审核后定期公布权威的正面清单(顺利完成初始认证、年度认证的企业)和负面清单(被强制移除的企业及原因)。对于审核中出现的任何问题,政府有权要求企业限时解决,否则依照职权移交联邦贸易委员会或美国交通部等执法机构。对于自愿或被动退出协议的企业要监督其删除任何暗示继续参与协议的表述,并禁止该企业通过协议继续接收欧盟个人数据。事后,商务部还持续追踪企

① Philipp Hacker and Bilyana Petkova, "Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers," *Northwestern Journal of Technology and Intellectual Property*, Vol. 15, 2017, p. 15.

② 冯洋:《从隐私政策披露看网站个人信息保护——以访问量前 500 的中文网站为样本》,《当代法学》2019 年第 6 期,第 64 页。

业的数据跨境传输实践,要求退出企业填写问卷,申报之前获得数据的使用情况、负责数据合规的联络人等。

2. 程序控制

为解决欧盟法院在驳回《隐私盾协议》时所提出的关切,美国于 2022 年 10 月通过《第 14086 号行政命令》,目的是加强对美国情报活动的程序保障,使美国政府能保证通过跨境传输协议获得的数据得到“充分性保障”。该行政命令也成为跨境传输协议达成的重要前提。为确保情报活动的范围和方式符合必要性、相称性和监督原则,该行政命令规定:(1)情报收集前必须对所有可能因素进行评估,确保用于执行行政命令所列举的十二项合法目的,坚决禁止用于行政命令所列举的四项目的;(2)情报收集活动要贯彻比例原则,方案尽可能量身定制,合比例地影响公民隐私和自由;(3)情报活动要受到严格的监督,每个情报机构内部都要有合规官员确保情报活动遵守美国的法律,其在外部必须接受公民自由监督委员会和外国情报监视法院的监督。[①]

3. 权利救济

权利救济措施由两部分构成,一部分是传输协议的直接规定:(1)执法机构(商务部、联邦贸易委员会)与替代性争议解决机构、欧盟成员国的数据保护当局合作,协助调查欧洲公民未解决的投诉;(2)联邦贸易委员会和交通部分别对商业领域和航空运输领域的不公平或欺诈行为采取执法行动。另一部分由美国其他现行有效的法规规定,例如《第 14086 号行政命令》,目的是针对有关美国情报活动的投诉建立一个两级补救机制。第一级由国家情报总监办公室的公民自由保护官员对收到的合格投诉进行初步调查,以确定行政命令或美国其他法律中的保障措施是否被违反,并决定是否采取适当的补救措施;第二级由总检察长建立一个数据保护审查法院,这是一个具有准司法职能的独立行政机构,根据个人或情报界成员的申请,对国家情报总监办公室的决定进行独立的审查。[②]

① “Executive Order 14086—Enhancing Safeguards for United States Signals Intelligence Activities,” https://www.presidency.ucsb.edu/documents/executive-order-14086-enhancing-safeguards-for-united-states-signals-intelligence.

② Ibid.

(三)逻辑关系

企业和政府各自的三个责任两两对应(见图 2),将数据跨境传输协议视作“控制企业和政府权力的法律”,既保障企业和政府获得境外数据以维护正常功能的运转,又严格限制公私权力的使用,以保障公民的基本权利。因此,授权与控权的动态平衡成为跨境数据治理中责任分配的逻辑主线。

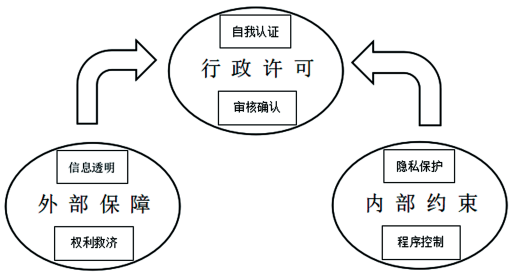

图 2　责任分配

资料来源:作者自制。

从授权角度看,企业的自我认证和政府的审核确认在本质上属于行政许可。企业提出申请是行政许可的前提条件,是从事数据跨境传输之前必须履行的法定义务,申请程序因相对人行使申请权而开始。企业开展的自我评估或者第三方评估是申请行政许可的必要条件。美国政府审核确认是对申请权的应答,通过形式审核加联合评估的方式确定企业是否满足协议要求,其法律结果是赋予企业从事数据跨境传输活动的法律权利。

从控权角度看,一方面,治理者在企业和政府的内部形成约束。对于企业而言,“代码即法律”,产品的整个生命周期都是按照事先设计的程序执行,在产品设计和技术开发中融入数据保护理念,隐私保护可成为默认设置。对于政府而言,正当程序是执法所依据的重要原则,对执法手段和目的施加比例原则的限制符合个人最低的公正标准。另一方面,治理者在企业和政府的外部建立保障措施。对于企业而言,以隐私政策为代表的信息透明机制向政府和用户展示了个人数据保护措施,以外在监督的方式推动企业履行承诺。对于政府而言,独立的

权利保障机制是针对情报权力运作过程中消极后果的法律补救,情报部门在收集情报时更加忌惮被投诉的风险,使其自身监督的主动性和积极性与承担的责任强行捆绑,避免了权力使用的随意性和偶然性。

四、对我国数据跨境流动治理的启发

大数据时代,数据跨境流动是经济全球化的必然结果,也是当下和未来经济发展的常态,在数据流动规则多极化和标准俱乐部化的发展趋势下,[①]双边协议在处理国家间数据保护标准不一的问题上属于比较可行的解决路径。欧盟和美国通过三代跨境传输协议缩小了双方在个人信息保护标准上的差异,[②]用较小的立法成本推动了双方数字经济一体化发展。我国在数据跨境传输方面的双边协议还处于起步阶段,欧美跨境数据治理在价值考量、规制路径、情报监督方面的经验对我国有很强的启示和借鉴意义。

(一)价值考量趋同:从数字主权到数字贸易

数字主权是信息化时代的新型权力,从《个人信息保护法》可以看出,我国在数据流动规制过程中蕴含着极强的国家安全考量,对数字主权的维护被认为是数据跨境流动的首要目标。对数字主权的强调是因为我国的数据信息产业起步晚、底子薄,相较美国处于弱势地位,而且我国与美国的意识形态背景和文化传统差异较大,彼此间身份认同感弱,数字主权的强化可以保证我国数据信息的基本安全和初步发展。但是,随着我国信息产业的飞速发展,我国互联网企业已经成为除美国外独一档存在。另外,随着美国对华"脱钩"逐渐成为"基本国策",中美之间的贸易日益减少,2023 年中美两国双边贸易额为 4.67 万亿元人民币,同比缩减 6.6%。[③] 相反,在 2023 年,中国与东盟经济融合持续加深,双边贸易规模

① 刘宏松,程海烨:《跨境数据流动的全球治理——进展、趋势与中国路径》,《国际展望》2020 年第 6 期,第 78 页。

② 张继红:《个人数据跨境传输限制及其解决方案》,《东方法学》2018 年第 6 期,第 40 页。

③ 《重磅!俄罗斯成为中国第四大贸易国,超过越南、澳大利亚、德国》,https://new.qq.com/rain/a/20240112A069VX00。

达 6.41 万亿元人民币，东盟连续 4 年成为中国第一大贸易伙伴，中国也连续多年为东盟第一大贸易伙伴。[①] 新形势下，数据流动的方向逐渐发生变化，数据主权的外延和保护理念也应重新审视，尤其是对过于宽泛化的数据保护主义则需要加以警惕。

共同利益是国际合作的前提和基础，为数据跨境流动提供动力。2017 年“一带一路”国际合作高峰论坛上中国政府提出的“数字丝绸之路”为东南亚沿线国家的经济发展创造了新机遇和增长点，成为弥合数字鸿沟和发展数字经济的重要契机。因此，沿线国家，尤其是东南亚国家与我国在数字发展领域的价值追求更具有趋同性，是数据跨境流动的主要目标。为此，我国应作出相应的政策应对。第一，对于经贸合作、政商往来密切的区域要淡化数字主权这个具有浓厚权力政治色彩的理念，搁置双方的理念分歧，寻求发展合作的最大公约数，并且大力推动跨境电商、教育、医疗等领域的数字贸易合作，将经济利益与数据流动深度捆绑，让其充分享受到数据时代的经济红利。第二，积极参与区域性合作治理平台，商讨数据合作中的共同标准，逐步取消跨境数据流动中“不必要的阻碍”和国别间差距。第三，加强对“一带一路”沿线国家传统基础设施的数字化改造，夯实沿线国家数字产业发展的基础，通过缩小“数字鸿沟”解决经济、文化、数字资源发展不协调的问题，消解沿线国家的信任危机，从而增进国家间的政治互信，营造良好的合作环境。

（二）规制路径多元：从企业规制到政府规制

在法律实践方面，我国的规范性文件并不算少，但存在形式不统一、内容多矛盾、执行难到位等现实难题，尤其是缺少统一的数据跨境标准规范和权威的内容审核监督机构。[②] 正因为监管机制的混乱和缺失，被资本裹挟的滴滴公司才能将包含所有用户数据、沟通文件、问题汇总的审计底稿传给美国。2022 年，国家互联网信息办公室对滴滴全球股份有限公司处以人民币 80.26 亿元罚款，充分展

① 《2023 年中国与东盟、RCEP 成员国及“一带一路”沿线国家贸易情况》，http://asean.china-mission.gov.cn/dmdt/202401/t20240112_11222856.htm。

② 易永豪，唐俐：《我国跨境数据流动法律规制的现状、困境与未来进路》，《海南大学学报（人文社会科学版）》2022 年第 6 期，第 142 页。

现了国家对网络安全、数据安全、个人信息保护等领域的保护力度和执法决心。中国政府正以“政府—企业”规制路径引导互联网企业依法合规运营,防止资本的无序扩张,促进企业健康、规范、有序发展。

重构政府、企业和个人之间的权力平衡机制已经成为数据跨境流动中不可回避的事项,欧美数据流动治理中“内外结合的双层嵌套式”规制路径具有深刻的启示作用。一方面,政府需要在法律层面设定目标和原则,在技术标准层面提供指引,促进企业对隐私保护问题作出内部式、自我规制性质的回应。法律层面的《网络安全法》《数据安全法》《个人信息保护法》对数据出境管理已经搭建起了四梁八柱,现在的重点是制订技术指引和操作指南,将社会期待、法律规定和伦理要求以技术化的形式表达出来。因此,需要全国信息安全标准化技术委员会参照国际标准化组织发布的《隐私信息管理体系标准》,将现有法律转换为系统工程任务中的等价要求。另一方面,完善事前评估加持续监督的监管模式,在评估环节加快出台统一的配套规则,明确评估流程的触发机制、评估执行主体、评估工具的使用、评估结果的应用、评估流程的闭环等问题。在监督环节,构建多元主体协同参与的管理体制,在国家数据局的统一部署之下,加快探索形成数据跨境流动治理“宏观发展—安全监管—具体领域”的三元协同格局。[①]

(三)情报程序公开:从自我封闭到开放透明

为使欧盟认可美国已经满足“充分性保护”条件,美国以行政命令的方式加强对自身情报活动的控制,坚持情报活动符合比例原则和监督原则,并设立第三方救济渠道。与之相比,我国的情报活动呈现出“只做不说”或者“做多说少”的沉默样态,尤其是情报活动的监督机制不成体系且较为粗放,没有公开明确的执行部门和执行流程。因此,西方国家和媒体对我国数字技术发展、治理和传播模式贴上“数字威权主义”的意识形态标签,认为我国以构建“平安社会”“智慧城市”“智慧警务”等名义,在国内建立严密的监控体系,使用数字信息和通信产品

① 徐拥军,王兴广:《总体国家安全观下的跨境数据流动安全治理研究》,《图书情报知识》2023 年第 6 期,第 25 ~ 26 页。

和服务来监视、压制和操纵国内外的民众。[①] 因此,我国必须加强情报监督,公开表明情报活动的价值追求、监督方式和救济渠道,消解对方在情报滥用方面的关切。

第一,树立情报机构的良好形象,强调情报活动会遵守法律规定、尊重个人隐私,不会肆意侵犯他国公民的个人权利,并通过立法或行政法规的方式表现出积极的姿态,向外界表明情报界将主动加强内部监督。第二,加强情报活动的程序控制。相比美国监督机构明确、监督内容具体、监督方式清楚,我国《国家情报法》对情报监管的内容显得太过于原则化。有必要细化《国家情报法》中对情报监管的相关条款,使其具体化、可操作化。[②] 另外,我国对情报机关的审查主要为内部审查与监督,需要增加外部制约和权利救济机制。第三,增加情报工作的透明度。出于国家安全的需求,情报活动要有足够的“隐蔽性”,这种保密文化容易引起民众对情报机构的质疑和不安,因此情报部门应保持适当的透明度,通过法定渠道积极主动且清晰地向社会公开必要的信息,展示出我国情报理念和手段的法治化、程序化进程。[③]

五、结　　语

当前世界形势复杂多变,反全球化浪潮兴起,数据领域治理规则碎片化的趋势日益加深,欧美以其二十多年的数据跨境传输合作经验为我国提供了现实参照,体现出欧美在弥合双方个人信息保护鸿沟方面采取的策略和努力。其权利保障、程序控制等方面的规定为我国未来跨境传输协议的签订提供了经验指南。在这个数据大航海时代,数字经济正渗透到社会发展的每个环节,推动经济社会进行深层次变革,如何有效协调各国在数据保护立法上的差异性成为摆在各国面前的现实难题,我国应当以双边或多边数据流通协议为契机,推动构建网络空间命运共同体,为数字经济合作中实现互联互通、共享共治提供“中国方案”。

① 刘国柱:《“数字威权主义”论与数字时代的大国竞争》,《美国研究》2022 年第 2 期,第 38 页。

② 林鑫,刘跃进,杨建英:《关于〈中华人民共和国国家情报法〉的若干思考》,《情报杂志》2022 年第 1 期,第 29 页。

③ 韩关锋,陈刚:《后台前置:美国情报透明原则的发展、实践及启示》,《情报杂志》2024 年第 5 期,第 27 页。