中美欧博弈背景下的中欧跨境数据流动合作*

李墨丝

内容提要:数字时代,中美欧三方数字博弈是国际竞争的主战场。中美数字领域的对抗已成新常态,美欧呈现出竞争与合作的复杂互动,中欧数字关系也处于变化之中。为了拓展发展新空间,中国应以跨境数据流动合作为抓手,撬动整个中欧数字合作,避免双方演变成数字领域的"制度性对手"。中欧推进跨境数据流动合作,面临着双方数字关系变局以及数字领域信任缺失、价值理念和监管模式差异等障碍,合作是否能取得务实成果,最终取决于能否建立以双方认可的规则为基础的合作框架。中欧合作应跳出利益和制度博弈的思维定式,平衡反映双方关切,兼顾数据保护领域的布鲁塞尔效应以及中国总体国家安全观下的数据安全诉求,分别构建个人数据和非个人数据的跨境流动合作机制,着眼于长期合作,并争取早期收获,为数字领域提供制度性国际公共产品。

关键词:中美欧博弈　中欧数字合作　跨境数据流动

一　问题的提出

2020 年 9 月 14 日,习近平同德国及欧盟领导人共同举行会晤,将数字合作确定为下阶段中欧合作的重点领域,决定建立数字领域高层对话,打造中欧数字合作伙伴,推动制定全球数字领域标准和规则,促进全球数字经济治理的良性发展。这为中欧数字合作提供了重要战略指引。此前,中欧数字领域高层对话于 9 月 10 日在刘鹤同欧盟委员会执行副主席韦斯塔格的共同主持下启动。2020 年 12 月 30 日,《中欧全面投资协定》完成谈判,将为中欧在数字领域扩大相互投资提供新的机遇。然而,由于所

* 本文系国家社会科学基金一般项目"全球数字贸易规则新趋势及中国的政策选择研究"(项目批准号:17BFX148)的阶段性成果之一。感谢评审专家的宝贵建议,文责自负。

谓“新疆人权问题”,欧盟对华政策明显转变,中欧合作形势急转直下,欧洲议会冻结了中欧投资协定的审议过程,数字领域高层对话和中欧数字伙伴关系的合作氛围也受到了影响。

中欧数字合作出现波折,纵然是经贸问题政治化所致。但是,撇开地缘政治因素不谈,中欧要推动数字领域务实合作取得实际成效,也会面临诸多挑战,不仅涉及贸易投资利益的分配,还有隐私和安全的考量;既有价值观的分歧,又有法律制度的差异,各种问题相互交织,错综复杂。同时,中欧数字领域的双边合作,难免受到美国的影响。美国为了巩固数字霸权,采取“小院高墙”策略,加速“去中国化”,拉拢欧盟搞小圈子,扰乱中欧数字领域合作的进程。对中欧双方而言,数字领域要成为新的合作增长点,不仅需要化解矛盾和危机的政治智慧,也需要合作路径和机制层面的具体落实。

必须看到,合作仍然是中欧关系的大方向和主基调。在新冠肺炎疫情全球大流行和世界经济遭受严重冲击的特殊背景下,中欧双边的数字合作刻不容缓,也是各有所需,双方在诸多领域可以进行合作。其中,跨境数据流动是中欧数字合作最为核心的问题。中欧在数字领域开展贸易、投资和技术领域的合作都离不开数据流动。数据流动规则也是全球数字治理的核心内容,需要中欧加强合作,共同推动国际规则的制定。有鉴于此,本文以中美欧数字博弈为大背景,分析依托中欧跨境数据流动合作扩大发展新空间、谋求发展新动力的必要性,研判中欧数字关系变化对跨境数据流动合作带来的挑战和困境,探讨中欧跨境数据流动合作的主要路径,并剖析中欧跨境数据流动合作超越双边协调的全球意义。

二 数字领域的中美欧三方博弈

随着数字技术、数字经济对经济社会发展和全球治理体系的影响越来越深入,中美欧三方数字博弈将成为国际竞争的主战场。数字领域的问题往往是跨领域的前沿问题,其中贸易、科技、人权、安全等各种问题相互交叉。中美欧三极竞争格局已经基本形成,三方为了各自的战略利益,既有合作也有竞争,使数字关系趋于复杂。

(一)全球数字市场的中美交锋:对抗竞争成为新常态

近年来,中美关系的对抗性不断上升。作为促进经济复苏、重塑竞争优势的关键要素,数字领域无疑是美国与中国激烈竞争的前沿阵地。中美贸易战爆发之后,特朗

普政府不仅对半导体等信息通信技术(ICT)产品加征关税,[①]还将华为等中国科技企业列入出口管制实体清单,贸易战中的数字摩擦开始显露端倪。随后中美贸易战持续发酵,美国打压华为、封禁 TikTok、实施清洁网络计划、推出蓝点网络计划,遏制中国的手段不断加码,贸易战升级为科技战。拜登政府上台后,加紧通过国内立法和国际规则在数字领域进行全方位、系统性地遏制中国,数字"铁幕"正在落下。随着数字革命不断深入,中美之间的利益争夺还将不断加剧,即使局势偶有缓和,数字对抗已经成为中美博弈新常态。

第一,制华措施不断推陈出新。为了应对中国日益增长的数字影响力,美国的政策工具层出不穷,不仅大大强化了出口管制和外资审查等传统政策工具,还推出一系列制华遏华的新机制。

一是对外投资审查。拜登政府正在加快出台新的出口管制和投资审查制度,着眼于审查美国对外投资,特别是对中国的投资。[②] 与此同时,国会也在谋划制定相关立法。《2021 年国家关键能力防御法(草案)》(National Critical Capabilities Defense Act of 2021)旨在建立跨部门对外投资审查制度,要求公司披露关键供应链和能力外包给外国对手的情况。对外投资审查重点关注影响国家安全的制造业和关键技术,与数字领域有关的主要是通信、机器人、人工智能、半导体等行业。[③] 其实,对外投资审查,尤其是与中国有关的投资审查,一直备受争议。特朗普政府曾经主张在《外国投资风险审查现代化法案》(FIRRMA)中加入相应条款,将美国外国投资委员会(CIFUS)的管辖权扩张至技术转让的对外投资,但最终被否决。[④] 美国当时提出对外投资审查,重点是应对中国所谓的知识产权窃取和强制技术转让,而已有法律框架可以应对,制定新法并不必要。现在重提对外投资审查,主要是为了遏制中国日益增长的竞争力和影响力,这已经成为美国对华政策的优先事项和迫切需求,当然法案最终能否成形,要看美国如何在扩大对外投资与限制技术出口之间做出取舍,在自身发展与遏制对手之间进行平衡。

二是普惠制现代化改革。美国国会提议制定《数字贸易促进发展法案》(Digital Trade for Development Act),旨在通过将数字贸易作为普惠制资格标准下的法定考虑

① See USTR, "China Section 301-Tariff Actions and Exclusion Process—$16 Billion Trade Action (List 2)," https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-china/16-billion-trade-action.

② "Sullivan: White House Eyeing Outbound Investments That Undermine Export Controls," https://insidetrade.com/daily-news/sullivan-white-house-eyeing-outbound-investments-undermine-export-controls.

③ See National Critical Capabilities Defense Act of 2021, S1864, 117th Congress, Introduced on May 26, 2021.

④ "Treasury Considering Implementing Parts of CFIUS Reform Bill As Part of 301 Response," https://insidetrade.com/daily-news/treasury-considering-implementing-parts-cfius-reform-bill-part-301-response.

因素,推动受惠国采取开放的数字贸易政策,并推动普惠制的现代化。[①] 理由是越来越多的受惠国在受益于普惠制下的美国市场免税准入的同时,又采取破坏美国价值观、就业和出口的数字政策,因此普惠制亟须更新和改革,以支持健全的数字贸易政策,促进美国在全球的战略利益。[②] 该法案的内容已经体现在《2021 年美国创新和竞争法案》(United States Innovation and Competition Act of 2021)中。其实,中国并不在美国的普惠制名单上,美国此举更多的是要削弱所谓"中国限制模式"对美国受惠国的影响,如中国《网络安全法》的数据本地化措施。虽然没有证据表明采取本地化措施的国家是受到中国影响,但是美国显然已经视之为全球势力范围的争夺战,认为普惠制标准现代化有利于争取尚未决定遵循中国模式的"摇摆国家",扩大美式数字圈,而美国及其盟友选择的数字发展道路将对未来美国国家安全发挥关键作用。[③]

第二,制华措施系统化和法制化。2021 年 6 月,美国国会参议院通过《2021 年美国创新和竞争法案》,推动实施系统化和法制化的制华举措。该法长达 2000 多页,整合了《无尽前沿法案》《2021 年战略竞争法案》和《2021 年迎接中国挑战法案》等众多法案,包含大量涉华条款,在美国历史上实属罕见。该法的通过释放出一个重要信号,即打击中国试图取代美国成为世界超级科技大国的努力越来越成为两党的共识。[④] 该法旨在通过加大对科技创新的投入,封堵技术和人才的外流,来加强美国在关键技术领域的领导地位,阻挡中国科技进步发展的步伐。其中有大量关于数字贸易以及数字技术与连接的规定,既要实施数字技术贸易联盟、数字连接和网络安全伙伴关系计划等新设机制,也要加强国际标准制定、数字贸易协定谈判等既有举措,企图拉拢盟友,切断中国与世界的数字连接。此外,区域技术中心计划、关键供应链弹性计划等重要计划的实施,也将在相当程度上挤压中国数字领域的发展空间。

① See Digital Trade for Development Act, H.R.3052, 117th Congress, Introduced on May 7, 2021.

② "Darin LaHood: LaHood Introduces Digital Trade for Development Act," https://lahood.house.gov/2021/5/lahood-introduces-digital-trade-development-act.

③ Siddharth Mohandas et al., *Designing a U.S. Digital Development Strategy*, Center for a New American Security, September 2020.

④ Jake Harrington and Riley Mc Cabe, "What the U.S. Innovation and Competition Act Gets Right (and What It Gets Wrong)," https://www.csis.org/analysis/what-us-innovation-and-competition-act-gets-right-and-what-it-gets-wrong.

表 1 《2021 年美国创新和竞争法案》数字领域的相关规定

法案	章节	主要目标	具体内容
《2021 年战略竞争法案》	数字技术与连接	建立数字技术联盟	• 数字技术的战略意识 领导国际标准制定：美国必须在为关键数字化技术制定治理规范和规则的国际机构中发挥领导作用，以确保这些技术在自由、安全、可互操作和稳定的数字化环境中运行。 反对数字权威主义：美国应与盟国和合作伙伴一起，利用其掌握的所有经济和外交工具，打击扩大使用信息通信技术产品和服务来监视、压制和操纵人口。 谈判数字贸易协定：美国贸易代表办公室应与欧盟、日本、五眼联盟成员国及其他国家，谈判有关数字产品的双边、诸边数字贸易协定或安排。 数字时代的信息自由：随着数字领域成为日益不可或缺的通信机制，美国应该领导全球努力确保信息自由得到维护。包括安全消费或发布信息而不必担心受到不当报复的能力。 形成数字技术贸易联盟：美国应当就形成有关数字化技术和服务的互利联盟进行外交谈判的机会开展评估。 • 数字连接和网络安全伙伴关系计划：保护数据等技术资产；在目标新兴市场扩大和增加安全的互联网接入；与伙伴国合作采取政策和监管立场，促进和鼓励开放、互操作、可靠和安全的互联网，包括数据自由流动；促进美国 ICT 产品和服务的出口，增加美国公司在目标市场的市场份额；与伙伴国合作建立网络安全能力并采用最佳实践。 • 美国国际发展金融公司的数字投资战略：鼓励私人部门的数字投资。
《2021 年贸易法案》	数字贸易的壁垒与审查	消除数字贸易壁垒	• 识别数字贸易壁垒：识别贸易伙伴采取的损害数字贸易的政策措施，并将做法最恶劣的国家或地区列入重点观察名单。 • 监督不公平贸易行为：在贸易代表办公室内指定官员，负责监督信息和通信设备供应商的不公平贸易行为。 • 谈判数字贸易协定：与志同道合的贸易伙伴谈判数字贸易协定，以解决数字壁垒、阻止审查、促进信息自由流动、保护隐私、保护敏感信息等。
	普惠制的再授权与改革	将受惠国是否采取数字贸易措施纳入考察范围	• 避免施加或消除数字贸易壁垒，包括不必要或歧视性的数据本地化或数据传输限制。 • 在数字环境中采取措施支持消费者保护、个人信息隐私和开放数字生态系统。

资料来源：作者根据《2021 年美国创新和竞争法案》整理。

第三,制华措施国内国际相互配合。印太地区是美国在国际层面围堵中国的主战场,在数字领域,美国主要通过国际规则谈判以及国际协调机制实现其遏制中国的目标。美国最新的战略举措是推动与澳大利亚、日本、新加坡等国缔结亚太地区数字贸易协定。① 美国制定印太地区数字贸易协定,不仅是为了对抗中国的数字影响力,也是为美国重返亚太铺路,并巩固其数字领域领导力。从国内因素看,美国退出《跨太平洋伙伴关系协定》以来,虽然先后与加拿大、墨西哥、日本缔结《美墨加协定》和《美日数字贸易协定》,但是并未达成覆盖整个区域的数字贸易协定,早期与澳大利亚、新加坡、韩国的自贸协定中的数字贸易规则也属于标准较低的前互联网时代规则,因此美国迫切需要达成新的协议,进一步确立美式数字贸易规则的领导地位。从中国因素看,中国正在成为亚太地区数字贸易领域的重要力量,其签署的《区域全面经济伙伴关系协定》(RCEP)包含数字贸易条款,但在跨境数据流动和禁止数据本地化等核心规则上与美国差异较大。此外,澳大利亚、新加坡等国正在积极推进数字贸易谈判,并敦促美国加入这些谈判。美国智库和学者也纷纷撰文,建议美国加入新加坡模式的《数字经济伙伴关系协定》(DEPA)。② 2021 年 8 月,美国宣布有意在 2023 年担任亚太经济合作组织(APEC)东道主,③意在重新参与亚太地区事务并加强其领导地位。这意味着中国参与区域合作时将面临来自美国更大的压力,尤其在隐私保护、跨境数据流动、开放政府数据等领域。

在美国看来,中美之间数字领域的博弈不仅是崛起大国与守成大国之间的对抗,也是两国不同的数字领域价值观和发展模式在全球范围内的势力范围争夺。不同于应对传统领域竞争的措施已经相对成熟,美国尚缺少有效应对数字领域新型博弈的政策工具,这也使美国感到前所未有的“恐惧”。因此,中美之间数字领域的矛盾将会越来越尖锐,即便可以避免跌入“修昔底德陷阱”,也可能会爆发彭博社所宣称的“数字冷战”或“冷战 2.0”。④ 然而,全球产业链的形成和发展是市场规律和企业选择共同作用的结果,数字领域更是如此。中国已经深度融入全球经济,中美数字领域密不可分。而美国打压中国数字技术和数字企业,人为地使数字领域成为中美关系中最严重

① “Tai: U.S. ‘Actively Working’ with Partners to Establish Digital Trade Rules,” https://insidetrade.com/daily-news/tai-us-%E2%80%98actively-working%E2%80%99-partners-establish-digital-trade-rules.

② Matthew P. Goodman, “DEPA and the Path Back to TPP,” https://www.csis.org/analysis/depa-and-path-back-tpp; Susan Aaronson, “The One Trade Agreement Biden Should Sign Up For Now,” https://www.barrons.com/articles/the-one-trade-agreement-biden-should-sign-up-for-now-51614607309.

③ “Harris Proposes U.S. as Next APEC Host, Backs Deeper Indo-Pacific Ties,” https://insidetrade.com/daily-news/harris-proposes-us-next-apec-host-backs-deeper-indo-pacific-ties.

④ Marc Champion, “How US-China Tech Rivalry Looks Like A Digital Cold War,” Bloomberg, 13 December 2019, https://www.bloomberg.com/quicktake/how-u-s-china-tech-rivalry-looks-like-a-digital-cold-war.

的“断层线”,并不能彻底改变市场规律和企业选择。因此,即便出现中美数字“冷战”,这场冷战可能也只发生在有限范围内。

(二)全球数字治理的美欧角力:竞争与合作的复杂互动

1.欧盟数字主权与美欧数字裂痕

美欧之间在数据流动、数字税、数字平台监管等问题上的分歧由来已久。这种分歧很大程度上源于欧洲对美国科技企业带来的经济社会影响有强烈担忧,这些企业威胁到了欧盟公民对其个人数据的控制,限制了欧盟数字经济和创新的发展,影响了欧盟和成员国在数字环境中的立法和执法能力,这也是欧盟提出“战略自主”和“欧洲主权”等概念的重要动因之一。在数字领域,欧盟提出“数字/技术主权”,意在打造促进数字创新的保护性机制和防御性工具,强化欧洲在数字世界中自主行动的能力。① 正如欧盟委员会主席冯德莱恩所言:“欧洲必须根据自己的价值观做出自己的选择,尊重自己的规则”。②

欧委会于 2020 年 2 月发布了三份重要的数字战略文件——《塑造欧洲的数字未来》《人工智能白皮书》和《欧洲数据战略》,将数字/技术主权的概念制度化。为了实现在数字基础设施、关键技术等方面的“自主可控”,欧盟正在对现有的法律、监管和金融工具做出一系列调整。数字主权战略提出后,德法两国合作推出欧洲云基础设施计划“盖亚云”(Gaia-X),以改变目前欧洲严重依赖美国云服务提供商的局面。2021 年 3 月,欧委会发布“数字罗盘”路线图,围绕数字人才、可持续数字基础设施、商业数字化转型、公共服务数字化四个方面,制定了 12 项具体政策指标。③ 随后,欧委会公布“地平线欧洲”(Horizon Europe)战略规划,总资金规模为 955 亿欧元,旨在确保欧盟科研和创新行动服务于欧盟优先事项,包括“适应数字时代的欧洲”“通过引领关键的数字、赋能和新兴技术,以及行业和价值链的发展,推动开放战略自主”。④

欧盟有关欧洲数字主权战略的一系列举措不容忽视,但它也面临着相当的现实困境。一方面,欧盟要赢得这场游戏,仅有规范性力量是不够的。⑤ 为了获得更大的主

① Tambiama Madiega, “Digital Sovereignty for Europe,” European Parliamentary Research Service Ideas Paper, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

② European Commission, “Shaping Europe's Digital Future: Op-ed by Ursula von der Leyen, President of the European Commission,” Brussels, 19 February 2020.

③ See European Commission, “2030 Digital Compass: The European Way for The Digital Decade,” COM(2021) 118 final, March 2021.

④ European Commission, “Horizon Europe's First Strategic Plan 2021-2024: Commission Sets Research and Innovation Priorities for A Sustainable Future,” https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1122.

⑤ Konstantinos Komaitis and Justin Sherman, “US and EU Tech Strategy Aren't as Aligned as You Think,” https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/.

权,欧洲必须成为经济创新方面的全球领导者,而不仅仅是在监管方面发挥引领作用;①另一方面,欧盟不可能完全切断与美国数字企业的联系。欧盟专注于规范大型科技公司的市场行为、塑造其商业模式的行事方式,也表明欧盟并无此意。更为重要的是,冯德莱恩欧委会数字主权战略的推进,将会面临内外交织的挑战:对内是欧委会构建数字主权的决策会在政治逻辑与经济理性之间艰难摇摆,其推进数字政策同样可能遭遇此前欧盟其他产业政策类似的困境;②对外则是全球数字经济图景中,中美两极格局逐步趋于固化,虽然《欧洲数据战略》指出欧洲在数据的工业化应用和专业领域应用中(主要是日常生活中的物联网应用和公共利益相关领域的应用)具有优势,③但要想短期内实现弯道超车并降低对中美两国的依赖并不容易。美国科技巨头已经占领欧洲市场,只要欧盟数字主权战略不走向过度保护主义,不排除美国科技企业的参与,美欧之间的数字裂痕并不会因此陡然加深。

2.拜登时期美欧关系调整与数字合作

拜登政府上台后,致力于重振美欧关系,与“民主”国家一起捍卫所谓“共同价值观”。美欧在七国集团(G7)峰会和美欧峰会就经贸、外交、科技等领域达成一系列共识,并重启了美日欧贸易部长三方会议,继续推进联合应对中国崛起的议题。其中,数字合作是美欧合作的新核心。美欧意图借 G7 数字和科技部长会议、美欧贸易和技术委员会(EU-U.S. Trade and Technology Council, TTC)等新机制,为数字世界制定新规则。

G7 将自己定位为“世界领先的民主国家和技术强国联盟”,④以意识形态划线、针对中国的色彩十分浓重。2021 年 4 月,G7 数字和科技部长签署联合声明,同意就数字、电信和 ICT 供应链、数字技术标准、数据流动、网络安全、数字竞争以及电子可转让记录等议题开展合作。⑤ 会议批准了《可信数据自由流动合作路线图》,将以《G20 领导人大阪宣言》及后续成果为基础具体推动数据流动,并确定了四个合作领域,包括

① Matthias Bauer and Fredrik Erixon, “Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls,” ECIPE Occasional Paper 02/2020.

② 忻华:《“欧洲经济主权与技术主权”的战略内涵分析》,载《欧洲研究》, 2020 年第 4 期,第 22 页。

③ European Commission, “A European Strategy for Data,” COM(2020) 66 final, February 2020, p.3.

④ See “G7 Tech Leaders Agree Bold New Proposals to Boost Online Safety Worldwide,” https://www.gov.uk/government/news/g7-tech-leaders-agree-bold-new-proposals-to-boost-online-safety-worldwide.

⑤ See “G7 Digital and Technology—Ministerial Declaration,” 28 April 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/981567/G7_Digital_and_Technology_Ministerial_Declaration.pdf.

数据本地化、监管合作、政府访问数据以及重点部门数据共享。①

美欧贸易和技术委员会的最终目标同样是确保数字技术和数字治理遵循西方的民主价值观,而不是遵守由中国决定的规则。TTC 是双方在 2021 年 6 月美欧峰会上成立的,是推动跨大西洋伙伴关系重回正轨的重要举措。其主要目标是促进美欧之间的贸易与投资、强化技术和产业的领导地位、保障和促进关键和新兴技术。它将形成高级别、跨部门、全政府的工作机制,成立十个工作组,重点推进人工智能、物联网和其他新兴技术的标准合作、半导体等信息通信技术和服务(ICTS)的供应链安全、数据治理、出口管制和投资审查合作,以及共同应对全球贸易挑战。尽管欧盟方面指出 TTC 不是反华同盟,②但不可否认其部分目的是就如何限制中国在关键和新兴技术领域的挑战达成欧美一致立场。

毋庸置疑,就数字合作而言,美欧有明显的共同利益,也具备合作的基础。美欧数字合作以数字技术作为核心,围绕数字技术的标准、安全、供应链等方面的合作将是重点领域。值得关注的是,TTC 将设立工作组审查和加强关键供应链,建立美欧伙伴关系来实现全球半导体供应链的再平衡,以增强美欧各自的供应安全以及半导体的设计生产能力。③ 近年来,美国和欧洲各国高度重视供应链安全,强调提高关键技术供应链弹性,供应链审查已经逐步趋势化,并被用作打压中国数字企业的手段。④ 可以说,美欧有着共同的政治动机来解决 ICTS 供应链安全这一紧要问题。当然,美欧之间长期以来未能填补固有的数字裂痕,导致数字合作存在相当的不确定性,特别是监管一致性等长期合作的前景并不明朗,但是美欧可能就技术标准、半导体供应链等紧迫问题达成一致,而且合作机制的创设也是数字合作的重要推动因素。

(三)中美欧博弈背景下中欧跨境数据流动合作的必要性

随着数字领域的战略价值不断凸显,为了维护发展和安全利益,未来中美欧数字博弈还会持续升级。其中,三方博弈的主要矛盾是中美竞争,因为美国在数字技术和数字市场上的霸主地位正在受到中国的挑战。因此,中国和美国都希望借助与欧洲的合作来改变全球竞争格局,即使与之合作不足以撼动中美欧三足鼎立之势,却可以通

① See "G7 Digital and Technology Track—Annex 2 Roadmap for Cooperation on Data Free Flow with Trust," 28 April 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf.

② "China Check-in: Trade and Tech Council Isn't about China, But It Looms," https://insidetrade.com/trade/china-check-trade-and-tech-council-isn%E2%80%99t-about-china-it-looms.

③ The White House, "U.S.-EU Summit Statement," https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement/.

④ 美国第 13942 号有关 TikTok 的行政令、第 13943 号有关微信的行政令都将应对 ICTS 供应链的紧急状况作为封禁的理由。参见美国商务部网站,https://www.commerce.gov/issues/ict-supply-chain。

过全球数字领域标准和规则的制定,为各自争取更大的主导权或发展空间。

近年来,中国数字企业快速成长,但市场主要在国内,海外份额仍然有限;中国积极进军人工智能、区块链、云计算、5G网络、无人驾驶汽车以及更多尖端技术领域,但在许多核心关键技术上还落后于美国;中国数据圈迅猛扩展,预计到2025年将成为全球数据量最大的区域,①但与全球数据圈相对割裂是实际存在的问题。中国要更好地参与全球数字竞争、获取全球数字资源、畅通国内外经济循环、掌握数字治理话语权,应当积极推动中欧数字合作。中欧在数字领域既有合作也有竞争,但双方没有重大利害冲突和地缘政治矛盾。中欧可以合作的领域很多,需要找准符合共同利益、立场相对接近、具有关键作用的突破口。由于中美欧在不同层面的数字博弈都会聚焦到跨境数据流动问题上,中欧双方应当以此为支点,撬动整个中欧数字合作,进而打造中欧数字伙伴。

第一,跨境数据流动是发展道路之争的新爆发点。全球数字领域已经基本上是中美欧模式分而治之。美国强调数字市场开放,重视企业的商业利益。欧洲强调数字主权,重视个人的数据权利。中国强调总体国家安全观,重视数据的安全管理权,不仅在数字经济和数字技术上正成长为与美国相抗衡的一极,在数字治理上也在寻求与美欧不同的路径。近五年来,中国正在加快数字领域立法进程,以《网络安全法》《数据安全法》和《个人信息保护法》为核心的法律框架已经初步形成。对于数据跨境流动,中国提出了《全球数据安全倡议》,建立起以出境安全评估为主要机制的监管体系,并规定了广泛的数据本地存储和处理要求,与美国的事后问责制有巨大差异。中国还出台了《出口管制法》《阻断外国法律与措施不当域外适用办法》等,为反击美国制裁以及阻断美国法律不当适用提供法律依据。对此,美国将数字领域的监管体制与"民主"价值观直接联系在一起,以此为依据划分阵营。特别是在跨境数据流动问题上,尽管美欧之间矛盾深重,仍然属于"内部"矛盾,中美之间则是"敌我"矛盾。实际上,美国在数字经济方面具有鲜明的扩张性偏好,一直谋求拓展其商业利益和势力范围;由于整体实力的差距,中欧与美国数字利益的抵触面更大,甚至就数据应否跨境自由流动形成了二对一的局面,反而有利于中欧双方在其中寻求利益共同点。

第二,跨境数据流动是规则主导权之争的核心点。21世纪的贸易规则说到底是数字贸易规则。中美欧互不相同的数字发展模式决定了三方对规则制定的争夺异常激烈。美国凭借在全球数字市场的绝对主导地位,最先布局并已经确立了一整套美式

① David Reinsel, John Gantz and John Rydning, "Digital Age 2025: The Digitization of the World from Edge to Core," IDC White Paper, http://book.itep.ru/depository/dig_economy/idc-seagate-dataage-whitepaper.pdf.

数字贸易规则,以充分发挥“互联网和其他数字技术在加强和支持美国经济各个部门的公司方面的至关重要的作用”。① 而且美式规则还通过日本、澳大利亚等贸易伙伴得以传播和推广,在全球数字贸易规则网络中呈现出明显的传导性。欧盟依靠其强大的规范性力量,大力弘扬其数据保护价值观,已经成为事实上的数据领域全球标准制定者。中国也在尝试数字领域国内法的国际化,RCEP 缔约实践就是典型例证。RCEP 跨境数据流动和计算设施位置条款首次纳入安全例外,②表明中国承认数据自由流动的基本理念,但也为保障网络安全和数据安全等基本安全利益预留了相当的政策空间。当然,虽然中国提升话语权和规则制定权的诉求越来越强,也已具备影响国际规则制定的能力,现实情况是规则主导权主要还是在美欧手中,但近年来美欧之间对隐私盾后续协议和 WTO 电子商务联合声明谈判等问题展开的争斗更加白热化,这样的利益矛盾显然有利于中欧共同推进数字领域全球标准和规则的制定,特别是多边规则的形成。

第三,跨境数据流动是数据资源之争的落脚点。中美欧三方在数字领域的博弈无论是贸易摩擦还是科技竞争,都绕不开对数据的争夺。如果说 20 世纪各国博弈的重点是石油资源,在当今数字时代各国争夺的则是数据资源。因为数据是数字领域的原材料,是国家的基础性战略资源,也是数字经济扩张的首要驱动因素。③ 而且数据价值的实现来源于数据的流动,包括跨境流动。数据流动不仅是数字时代的生产和交易手段以及全球价值链的组织方式,④也是数字技术持续创新的核心要素,高端制造、物联网、云计算、大数据、人工智能等技术的广泛应用无一不有赖于海量数据的累积并形成数据循环。⑤ 美国数字贸易规则的核心是数据跨境自由流动和禁止数据本地化,并通过《存储通信法案》《澄清域外合法使用数据法案》(CLOUD 法案)等立法强化获取全球数据的能力。欧盟数字主权的基本要义是对个人数据的保护,并试图通过组建欧盟从业数据、边缘计算和云计算联盟⑥等举措将其控制范围延伸至非个人数据。中国从总体上强化数据安全保护,为的是在技术能力和治理能力有待强化的现实国情下,

① USTR, “2021 Trade Policy Agenda and 2020 Annual Report,” March 2021, p.121.

② See RCEP, Art 12.14(3), 12.15(3).

③ See UNCTAD, “Digital Economy Report 2019—Value Creation and Capture: Implications for Developing Countries,” 2019, p.xv.

④ Javier López González and Marie Agnes Jouanjean, “Digital Trade: Developing A Framework for Analysis,” OECD Trade Policy Papers, No.205, TAD/TC/WP(2017)4/FINAL, 2017, p.11.

⑤ UNCTAD, “The ‘New’ Digital Economy and Development,” UNCTAD Technical Notes on ICT for Development, No.8, TN/UNCTAD/ICT4D/08, October 2017, p.12.

⑥ See European Commission, “European Alliance for Industrial Data, Edge and Cloud,” https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance.

保障数据资源的安全。尽管中欧有不同关切,但都有保护自身数据资源的诉求,而与美国的分歧更加明显。

必须承认,一方面,中欧在推动数字经济增长和数字技术发展方面越来越相互依赖,中欧数字合作有着巨大的潜力和需求。《中欧全面投资协定》降低了数字领域的投资准入壁垒,中国对欧盟开放云计算等数字服务市场,①就是中欧数字合作需求的实际反映。中欧跨境数据流动合作,有利于实现中欧两大数字市场、两方数字资源的更好联通、更大效益,推动中欧数字化转型更加强劲,数字红利更可持续。另一方面,由于欧盟数字主权战略以及地缘政治因素,加之美欧之间在数字领域的复杂互动,欧盟仍然面临着与中国是合作还是竞争的方向选择。这一选择不仅是欧盟的内部决策,也取决于中欧之间的战略互信,尤其是数字领域的战略互信。如何通过具体措施增强战略互信,进而推动跨境数据流动合作落到实处,是摆在双方面前的难题。

三 中欧数字关系下跨境数据流动合作的挑战

当前,中欧数字关系正处在关键的十字路口,推进中欧跨境数据流动合作既有机遇,也有挑战。中欧数字关系变化带来的不确定性,中欧在数字领域的信任缺失,以及价值理念和监管模式的差异,都是双方需要直面的问题。

(一)变化中的中欧数字关系

在中欧关系上,中国始终认为合作是大方向和主基调,将欧洲视为伙伴而非对手。② 不过,欧洲却有两种力量在较量:一种是维护中欧关系继续朝着合作共赢的大方向发展;另一种是企图把中欧关系引向对立对抗甚至脱钩。同时,对于中欧之间竞争性大于互补性,还是互补性大于竞争性的问题,也有不同声音。2021 年 9 月,欧洲议会表决通过《新欧中战略报告》,称中国是欧盟的合作和谈判伙伴,同时在越来越多的领域也是欧盟的经济竞争者和制度性对手。③ 欧盟对中国的这一战略定性并非首

① See EU-China Comprehensive Agreement on Investment (CAI)- Schedule of China, Annex I Entry 12. 根据《中欧全面投资协定》规定,互联网数据中心服务的外商投资者持股不得超过 50%。这意味着包括云计算在内的互联网数据中心服务对欧盟的开放水平已经与《〈内地与港澳关于建立更紧密经贸关系的安排〉服务贸易协议》持平,超越了《自由贸易试验区外商投资准入特别管理措施(负面清单)(2020 年版)》。这将打破长期以来该项业务不对港澳以外的其他外商投资者开放的限制,为欧盟云服务商进入中国市场提供更大的机遇。

② 《王毅出席慕尼黑安全会议"中国专场"活动并发表演讲》,中国政府网,http://www.gov.cn/xinwen/2021-05/26/content_5612172.htm。

③ European Parliament, "A New EU-China Strategy, European Parliament Resolution of 16 September 2021 on a New EU-China Strategy (2021/2037(INI))," September 2021, para. 1(a).

次提出,而是最早出现在 2019 年 3 月欧委会发布的《欧中战略前景》①中。新战略更加突出近来的事态发展以及中国带来的全球挑战,并强调双方竞争领域越来越多,凸显的是对中国快速增长的经济实力和政治影响力的深切忧虑。

中欧数字关系是中欧总体关系的缩影。撇开其妄评中国内政不论,欧盟《新欧中战略报告》提出的三分法,即将中国同时视为合作伙伴、经济竞争者和制度性对手,不仅会影响广义上的中欧关系,也会影响中欧数字关系。数字领域是中欧各自的战略重点。客观地看,中欧作为数字领域的两大力量,数字连接、数字经济、隐私保护、网络安全等越来越成为双边关系中日益突出的问题。一方面,在人工智能、大数据、云计算、区块链等领域双方有强化科技创新国际合作以及扩大互惠市场开放的巨大需求;②另一方面,在 5G 等下一代技术、关键基础设施等方面双方有不同利益,在个人数据和隐私保护、标准和互操作性、知识产权等方面也有不同诉求。这就使得中欧数字合作面临机遇与挑战并存的局面。

中欧数字合作最早可以追溯到 2009 年的中欧高科技对话,重点是信息技术、电信和互联网使用。2013 年《中欧合作 2020 战略规划》也将最初的合作重点放在互联网和信息化上,明确要加强中欧信息技术、电信和信息化对话机制,开展相关战略、政策、法规的交流与对话。2015 年,作为中欧经贸高层对话的重要成果,中欧 5G 战略合作联合声明签署。在联合声明框架下,中欧共同推进 5G 国际标准制定、技术研发、试验等方面的合作,特别是物联网领域的 5G 应用。③ 中欧还开展了其他有关数字技术研究创新和标准化的合作项目,涉及智慧城市和互联网治理等领域。更重要的是,中欧 ICT 企业之间的合作迅速扩大并日益密切。《中国对欧盟政策文件》以及《欧亚互联互通战略》④这两份中欧于 2018 年分别发布的战略文件中也都重申了中欧数字领域的相互支持与交流合作。

然而,近年来欧盟对加强中欧数字对话的立场逐渐变得谨慎,特别是《欧中战略前景》发布之后。欧盟提出了保护产业竞争力和保障战略自主的若干行动,大部分都

---

① European Commission, "European Commission and HR/VP Contribution to the European Council, EU-China—A Strategic Outlook," 12 March 2019, p.1.

② DIGITALEUROPE, DIGITALEUROPE Statement on the EU-China Comprehensive Agreement on Investment (CAI), https://www.digitaleurope.org/news/digitaleurope-statement-on-the-eu-china-comprehensive-agreement-on-investment-cai/, visited on 18 September 2021.

③ 参见中欧物联网和 5G 研究项目网站,EU-CHINA Study on IoT and 5G, https://www.euchina-iot5g.eu/about/project/index.html。

④ See European Commission, "Connecting Europe and Asia: Building Blocks for an EU Strategy," Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, JOIN(2018) 31 final, September 2018.

与数字领域有关。尽管此后有中欧数字领域高层对话、《中欧全面投资协定》完成谈判等重要转机,但最近中欧关系再度出现变局。《新欧中战略报告》则明确强调“欧盟应通过解决欧中关系的其他方面,特别是数字和技术主权,来提高战略自主”,在此背景下,欧盟要在微芯片和半导体生产、云计算和电信技术等领域制定具有竞争力的主权产业战略,减少对中国的依赖。① 欧盟立场转变是受到诸多错综复杂因素的影响,其中影响最为显著的是两个方面。

一是中国数字竞争力和影响力逐步增强,正在对欧洲数字领域的政治和经济各个方面带来挑战。欧盟一方面担心丧失对华技术优势,另一方面担心中国科技的安全威胁。特别是新冠疫情以来,欧洲越来越警惕中国的数字技术,希望摆脱华为的 5G 技术、TikTok 和微信的社交应用软件、阿里的云服务、同方威视的安检系统、海康威视的视频监控和大疆的无人机等中国企业和技术。实际上,由于高科技竞争已经被高度政治化了,欧盟的担心更多地来自政治层面。欧洲围绕中国科技的政治担忧既涉及数据保护问题和贸易投资问题,也涉及所谓人权问题和安全利益,背后的核心问题则是信任缺失。较之传统领域的中欧互信问题,中欧数字合作的信任危机更为突出。

二是中美关系日趋紧张,欧盟面临着成为中美数字对抗的战场的风险。美欧同属所谓“民主”国家阵营,而且欧盟对美国科技和互联网公司的依赖,远远超过对中国的数字依赖。美国对华发动的打击和制裁,也会给欧盟带来外部冲击。如美国要求欧盟排除中国的 5G 设备供应商,会限制欧洲各国大力发展 5G 网络。即便欧盟宣称战略自主和数字主权,不在中美之间“选边站”,也难免不陷入交火之中。中国欧盟商会的一份报告预测,许多欧盟公司将不得不借助双供应链体系来应对数字困境,即以美国为中心的部分和以中国为中心的部分,因此面临极大的不确定性和高昂的成本。② 而美国主动修复美欧关系,欧盟也出现了追随美国的迹象,因此有可能会进一步抑制欧盟与中国合作的深化。

必须承认,中欧在数字领域既有合作又有竞争是客观事实,中美、美欧关系的外溢效应也不容忽视。中欧跨境数据流动合作须在中美欧博弈大背景下推进,以合作为契机积极解决双方在经济、政治等方面长期存在的问题,引领中欧数字关系积极向好,避免双方演变为数字领域的“制度型对手”。

---

① European Parliament, “A New EU-China Strategy, European Parliament Resolution of 16 September 2021 on a New EU-China Strategy(2021/2037(INI)),” para.41.

② 中国欧盟商会:《脱钩:全球化何去何从》, https://europeanchamber.oss-cn-beijing.aliyuncs.com/upload/documents/documents/Decoupling_CN[869].pdf。

（二）中欧跨境数据流动合作的主要挑战

在跨境数据流动的具体层面，中欧合作面临一系列挑战。第一，跨境数据流动国际合作中的信任缺失问题普遍存在。由于数字领域是由具有多重身份的多个参与者相互作用的分层结构，这种分层结构是极其错综复杂和快速变化的。这使得数字环境的信任问题愈发重要，不仅消费者和企业的参与和受益取决于信任程度，信任关系也是国际合作的基石。跨境数据流动合作尤其依赖于参与方之间的信任。然而，跨境数据流动问题特别复杂和敏感，增强互信并非易事。因为数据流动首先是一个复杂的技术问题，通过互联网发送的数据以“数据包”的形式传输，跨越不同的国家到达目的地，很难先验地确定数据流动的地理位置。① 事实上，数据和数字活动本质上是无国界的，但监管不是，当数据跨越不同管辖区域时，隐私保护、数据安全、国家安全、监管影响力等问题都会变得更加复杂。② 这导致各国管理跨境数据流动的规则成了大杂烩，由此加剧了中美欧之间的监管竞争，以及中欧监管层面的信任缺失。

第二，中欧跨境数据流动合作的信任缺失根源在于双方价值理念的差异。数字技术创新和数字经济发展给中国和欧盟的政策制定者带来了相似的挑战，但是由于法制传统、数字生态环境、数字化转型进程等的不同，中欧数据保护的基本理念存在不小的差异。欧盟数据保护模式以严格保护隐私和个人数据著称，对个人数据跨境流动持谨慎态度，某种程度上甚至可以说坐在数据流动议题国际谈判桌上的是欧盟公民个人。中国的数据保护则着眼于总体国家安全观下的数据安全，重视对总体国家安全具有重要意义的数据的保护，从国家安全、经济运行、社会稳定、公共健康等角度审视数据重要与否，而非对于特定组织和个人是否重要或敏感。由于立法价值序列的不同，尽管中国已有严格的法律规定，欧盟仍然对中国的个人数据和隐私保护状况抱有疑虑，甚至担心在欧洲的中国科技企业必须依据中国国内情报安全立法向有关部门提供欧盟公民的数据。③

第三，中欧之间监管模式的差异也导致了跨境数据流动合作的信任缺失。不仅中国自上而下的监管框架以及执法机构设置与欧盟明显不同，许多具体监管方法也有区别。中欧有关数据本地化的监管差异就是典型的例证。中国有明确的数据本地化要

① Francesca Casalini and Javier López González, “Trade and Cross-Border Data Flows,” OECD Trade Policy Papers, No.220, 2019, pp.9-10.

② Francesca Casalini, Javier López-González and Taku Nemoto, “Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers,” OECD Trade Policy Papers, No.248, 2021, p.7.

③ “Chinese Tech Companies Could Face Trouble in Europe,” POLITICO, https://www.politico.eu/article/meet-china-inc-s-firms-that-could-face-trouble-in-europe-2/.

求,主要适用于关键信息基础设施运营者产生和收集的重要数据和个人信息。① 尽管《一般数据保护条例》(GDPR)被指是事实上的“个人数据出口禁令”,②而且施雷姆斯第二案(Schrems II)之后,欧洲数据保护委员会发布的关于将个人数据从欧盟传输至第三国的指南草案实际上可能会导致数据本地化,③但是欧盟相关立法并未明确要求数据本地化。再如,中国允许为了维护公共安全在公共场所安装图像采集、个人身份识别设备,要求必须设置显著的提示标识,所收集的个人图像、身份识别信息只能用于维护公共安全的目的。④ 而欧盟数据保护机构认为,应当全面禁止使用人工智能在公共空间中自动识别人类特征,如识别人脸、步态、指纹、DNA、语音、按键和其他生物识别或行为信号。⑤

由此看来,中欧跨境数据流动合作是否能够取得进展,最终取决于能否弥补双方的信任缺失,具体而言则是能否接受各自的监管体系。如果说中欧监管层面信任缺失是由监管差异引发的,那么弥合监管差异将是中欧合作的核心。建立充分信任的中欧跨境数据流动合作框架需要以规则为基础,中欧以相互认可的规则为基础共同推动中欧跨境数据流动合作,有助于双方避免在价值体系和监管模式上发生冲突,克服可能危及双方数字市场发展和数字技术创新的挑战,最终建立互信、互惠、互利的双边数字关系。

四 中欧跨境数据流动合作的基本路径

鉴于价值理念和监管模式的差异,中欧跨境数据流动合作应当兼顾双方的利益和诉求,在个人数据和非个人数据跨境流动合作基本路径的构建中,建立以双方认可的规则为基础的合作框架。

(一)个人数据的跨境流动

1.数据保护领域的布鲁塞尔效应

布鲁塞尔效应(Brussels effect)一词最早由哥伦比亚大学法学院教授阿努·布拉德福德(Anu Bradford)于 2012 年提出,主要是指欧盟单方面控制全球市场的力量欧盟

① 参见《网络安全法》第 37 条。

② European Center for Digital Right, Comment 169 on EDPB Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, R01/2020-0169, p.2.

③ EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Adopted on 10 November 2020.

④ 参见《个人信息保护法》第 26 条。

⑤ See EDPB, EDPB-EDPS Joint Opinion 5/2021 on the Proposal for A Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 18 June 2021, p.11.

通过颁布塑造国际商业环境的法规,提升全球标准,导致全球商业的许多重要方面显著欧洲化。欧盟拥有重要的、独特的和高度渗透的力量来单方面改变全球市场,包括在竞争政策、环境保护、食品安全、隐私保护或者社交媒体仇恨言论监管方面制定标准的能力。因此,尽管人们普遍认为欧盟在经济和政治上正走向衰落,但是布鲁塞尔效应使得欧盟在未来很长一段时间内都是并且很可能仍然是全球经济的主要力量。①

布鲁塞尔效应在数据保护领域体现得尤为突出,特别是《一般数据保护条例》及一系列相关立法,确立了全球数据保护标准的基调,使数据保护成为全球监管环境欧洲化的有力体现。② 随着跨国公司自愿遵循 GDPR 管理全球业务,欧盟仅凭自身市场规模的力量便足以将欧盟标准转化为全球标准。在法律层面,欧盟的数据保护规则正在成为许多国家和地区遵循的范本,特别是 GDPR 树立了数据保护的"黄金标准"。从亚洲的日本、韩国、印度、印度尼西亚,到拉美的巴西、智利、哥伦比亚,再到非洲的南非、肯尼亚,效仿欧盟数据保护制度可以说是一种全球趋势。③ 欧盟模式的数据保护制度在世界范围内扩散的另一个重要原因是各国希望从欧盟获得充分性认定、获得充分性认定将使个人数据可以从欧盟流向第三国,无须任何进一步的保护,否则会导致跨境数据传输的难题,欧盟正是借此牢牢掌握美欧之间数据流动博弈的主动权。

鉴于欧盟数据保护领域的布鲁塞尔效应以及欧盟视个人数据保护为基本权利④的价值观取向,在中欧个人数据跨境流动合作中欧盟也将坚持其一贯标准,即 GDPR 第五章的规定,当个人数据得到充分保护时,才可进行国际传输。GDPR 为国际数据传输提供了多种传输机制,包括充分性决定、标准合同条款、约束性公司规则、认证机制、行为准则、减损的使用等。其中,充分性认定是最重要的传输机制。但是,考虑到充分性认定的考察标准⑤和严苛程度⑥,目前中国几乎不可能获得欧盟的完全充分性认定。因此,长期

① Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020, p.14.

② Ibid., p.216.

③ European Commission, "Communication from the Commission to the European Parliament and the Council, Data Protection as A Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation," COM(2020) 264 final, June 2020; Mark Scott and Laurens Cerulus, "Europe's New Data Protection Rules Export Privacy Standards Worldwide," POLITICO, January 31, 2018, https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.

④ See Charter of Fundamental Rights of the European Union, Art. 8.

⑤ 在评估第三国对个人数据的保护水平时,GDPR 第 31 条规定了相关考虑因素,包括法治和基本人权的保护程度,是否存在独立且有效运作的监管机构以及承担有关个人数据保护的国家责任或国际承诺。

⑥ 迄今为止,获得欧盟充分性认定的国家和地区仅有 12 个,分别是安道尔、阿根廷、加拿大(商业组织)、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士和乌拉圭。2021 年 6 月,欧盟委员会分别根据 GDPR 和《执法指令》正式通过了英国的充分性决定,此外还启动了根据 GDPR 通过韩国充分性决定的程序。See European Commission, "Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection," https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

来看,中欧合作的重点可聚焦于推动部分充分性协议,即类似美欧隐私盾协议或者欧盟给予加拿大的充分性认定,近期则可以寻求替代性的国际传输机制。

2.中欧部分充分性协议

尽管中欧对于个人数据的理念差异较大,但是国际合作更重要的是协调国内规制的冲突。而中欧部分充分性协议符合双方数据保护的基本方向。对欧盟而言,给予中国部分充分性认定有利于扩大欧盟数据保护制度的全球版图。欧委会通讯文件《在现代化世界中交换和保护数据》指出,欧委会鼓励其他国家寻求部分充分性决定或者特定部门的充分性决定,例如金融服务或信息通讯部门。① 对难以获得欧盟完全充分性认定、但欧盟数据流动对其特定部门或地理区域又是至关重要的国家来说,部分充分性决定提供了一种选择。对中国而言,寻求获得欧盟部分充分性认定有利于中国企业更好地进入欧盟市场。近年来,中国企业在欧洲正以后起之势加速发展,但欧盟严苛的数据法规和标准也是企业面临的重要挑战之一,运营成本增加,开展业务受限,市场准入受阻。如果中欧部分充分性协议能够达成,将为中国企业在欧投资运营提供更加稳定的营商环境,并有助于中国企业以欧盟为重要战略支点开展全球化布局。

美欧隐私盾框架是部分充分性决定的典型例子,虽然已经被判无效,但其基本架构对中欧达成部分充分性协议仍有参考价值。美国秉持不同于欧盟综合立法的部门方法,主要针对金融、医疗等特定部门数据立法,也没有独立的政府数据保护机构,因此美国数据保护法本身不符合欧盟的充分性标准。美欧隐私盾框架主要包括适用于美国企业和政府两个层面的制度设计,目的是对美欧双方的数据保护制度做折中处理,填补监管差距。

企业层面,为了进入隐私盾,美国企业和其他组织必须向美国商务部自证且公开声明其遵守隐私盾原则,包括补充原则,根据这些原则公布隐私政策,完全实施这些原则,完成年度重新认证,向欧盟公民提供免费的独立争议解决机制,并接受美国联邦贸易委员会、运输部及其他法定机构的监管。美国商务部经与欧盟委员会磋商形成的隐私盾原则包括通知原则、选择原则、对外传输原则、安全原则、数据完整和用途限制原则、获取原则以及追索、执行和责任原则;隐私盾补充原则包括适用于敏感数据、人力资源数据、旅行信息、公共记录和公开信息等特定数据的原则,以及适用于互联网中介、数据保护机构、公共机构等不同组织的原则。② 隐私盾原则及补充原则是针对美国企业的实体义务,旨在提高企业的隐私保护水平,而非谋求改变美国的数据保护制

① European Commission, "Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World," COM(2017) 7 final, October 2017, p.8.

② 参见隐私盾框架文本,https://www.privacyshield.gov/EU-US-Framework。

度。加入隐私盾的美国企业通过自证其符合隐私盾原则,将被欧盟视为能够提供充分的隐私保护,解决跨大西洋数据传输的法律基础问题。

执行机制方面,美国商务部全面负责隐私盾框架的执行,发布隐私盾名单,有权将不遵守隐私盾原则的企业从名单中删除。美国政府专门向欧盟委员会递交书面声明,确保行政机关在监督和执行过程中,有明确的权力范围和保障措施。美国还任命了下设于国务院的监察员,独立于国家安全机构,由其专门负责向欧盟数据主体提供救济措施。① 相比此前的安全港协议,隐私盾框架更加强化美国政府的执行机制和权力界限,而隐私盾被判无效也是出于对美国政府访问和使用欧盟个人数据的关切,②反映出对于有关数据的公私权利,欧盟的天平明显倾向于私权利。

中国可以参考美欧隐私盾框架,与欧盟开展部分充分性谈判。企业层面,中国企业依据《个人信息保护法》等法律规定开展合规工作,使其具备加入中欧双方认可的数据保护框架的基础。《个人信息保护法》在一定程度上借鉴了 GDPR,对企业全面保护个人信息做了较为严格的规定,在敏感信息处理、未成年人个人信息处理等方面与 GDPR 基本一致,在同意规则、信息主体知情权等方面的严厉程度甚至超过 GDPR。行政监管层面,不同于欧盟及各国均采取独立的数据保护机构机制,中国仍然维持多部门执法机制,这一重要区别可能是中欧充分性谈判的焦点之一。中国也可以仿效美欧隐私盾框架下美国行政权力设置的相应安排,特别是监察员制度,以强化对个人数据的保护。

同时,中欧部分充分性谈判必须符合中国的相关法律规定。《网络安全法》第 37 条确立了关键信息基础设施运营者产生和收集的个人信息跨境流动的基本制度,即原则上要求本地存储,必要时出境须进行安全评估。《个人信息保护法》第三章专门规定了个人信息跨境提供的规则,构建了以安全评估、个人信息保护认证、标准合同等为主的跨境传输机制,并要求个人信息处理者取得个人的单独同意;同时还规定了关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者的数据本地化要求。③ 中国的安全评估和欧盟的充分性认定同属有条件的流动机制,前者是个案审查,后者是统一认定,比较而言,前者对数据传输的限制程度更高。④ 因

① See Privacy Shield Framework, "EU-U.S. Privacy Shield Ombudsperson Mechanism," https://www.privacyshield.gov/servlet/servlet.FileDownload? file=015t00000004q0g.

② CJEU, "The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield," Press Release No 91/20, July 2020.

③ 参见《个人信息保护法》第 38-40 条。

④ Francesca Casalini, Javier López-González and Taku Nemoto, "Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers," pp.9-10.

此,中欧部分充分性协议应在根据中国法律要求进行本地存储的前提下,对出境安全评估机制做出便利化的安排,例如,部分充分性协议即可被视为符合安全评估要求。

3.替代性国际传输机制

除了充分性决定,GDPR 还规定了标准合同条款、约束性公司规则、认证机制等替代性传输工具。中国《个人信息保护法》第 38 条也对个人信息保护认证、标准合同做了规定。这就为中欧就认证机制和标准合同开展合作、争取早期收获奠定了基础。

认证机制方面,作为 GDPR 和《个人信息保护法》引入的新机制,中欧双方开展合作有较大空间。认证机制是由第三方认证机构对企业的数据保护能力进行认证,评估企业的 ICT 产品和服务、数据保护政策及实践是否符合个人信息和数据安全的法律法规。认知机制的核心是企业对数据保护的自我监管,目的是在企业与用户之间建立起收集、处理、使用、传输数据的信任关系,以解决跨境数据流动中信任缺失的问题。在欧洲,认证机制已经实际应用,例如,欧洲隐私印章"EuroPriSe"获得欧盟资助,作为独立第三方为符合欧盟隐私和数据安全保护要求的企业颁发信任标章。① 在中国,尽管已有法律规定,《中国(上海)自由贸易试验区临港新片区总体方案》也曾提出要建立数据保护能力认证管理机制,但个人信息保护认证机制建设尚未真正启动。GDRP 和《个人信息保护法》的认证机制均须经政府认可,双方可就相互承认、对等或协调等进行正式合作,也可开展主管机关之间的信息交流、对话或会议。此外,中欧双方还可合作建立认证机构。

标准合同是 GDPR 应用最为广泛且较为成熟的数据传输机制,可以为中国具体建构标准合同传输机制提供借鉴和参考。2021 年 6 月,欧盟委员会根据 GDPR 发布了新的标准合同条款,分别适用于处理者和控制者②以及国际传输③,取代了原来依据《数据保护指令》发布的标准合同条款。新条款通过单一的入口涵盖了广泛的传输场景,而且模块化方法为可能出现的多方数据传输情形提供了更多样化的选择,为复杂的数据处理链提供了更大的灵活性。中欧双方可就标准合同开展正式和非正式合作,包括分享信息、经验和最佳实践,以及共同帮助中小企业克服使用标准合同的障碍。

---

① EuroPriSe, "European Privacy Seal Fact Sheet," https://www.euprivacyseal.com/EPS-en/Fact-sheet.

② Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on Standard Contractual Clauses between Controllers and Processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA Relevance).

③ Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA Relevance) C/2021/3972.

(二)非个人数据的跨境流动

1.欧盟的传输机制

欧盟层面规范非个人数据流动的主要是《非个人数据自由流动条例》,于 2018 年 11 月通过,2019 年 5 月 28 日生效。该条例旨在通过禁止数据本地化要求,进一步促进欧盟内部的跨境数据流动。该条例所指的"非个人数据",是指 GDPR 第 4.1 条定义的个人数据以外的数据。①但是,《非个人数据自由流动条例》仅限于处理欧盟的非个人电子数据,不适用于在欧盟以外进行的处理以及与此类处理有关的数据本地化要求,主要包括两种情形:②(1)作为服务提供给居住在欧盟内或在欧盟内设有机构的用户,不论该服务提供者是否在欧盟内设立机构。例如,在美国设立的云服务商通过位于欧盟境内的服务器,向在欧盟的客户提供处理服务,则属于适用范围。如果服务器在欧盟之外,所有处理活动均在欧盟之外进行,则不适用于这种情况。(2)由居住在欧盟或根据自己的需要在欧盟设立机构的自然人或法人进行。例如,一家来自欧盟成员国 A 的小型初创企业决定通过在成员国 B 开设一家企业来扩大业务,为了成本最小化,该初创企业选择将新企业的数据存储和处理集中在原有服务器中,成员国不得禁止此类 IT 集中化工作,除非有公共安全的正当理由并符合比例原则。但是,当非个人数据是混合数据集的一部分,该条例仅适用于非个人数据的部分;如果混合数据集中的非个人数据和个人数据密不可分地联系在一起时,③非个人数据的跨境流动仍然必须遵守 GDPR,④包括 GDPR 有关向第三国或国际组织传输个人数据的规则。

目前,所有处理活动都在欧盟以外进行的非个人数据的跨境流动,须以欧盟与其他国家签署的协定为准。迄今为止,除了《欧盟—英国贸易与合作协定》之外,欧盟签署的其他贸易协定均未对跨境数据流动做出实质性承诺。英国脱欧前适用的是欧盟数据保护法律,所以双方能够在贸易协定中就跨境数据流动和个人数据保护达成一致,⑤而且欧委会已经分别根据 GDPR 和《执法指令》⑥正式通过了英国的充分性决

① The Regulation on the Free Flow of Non-personal Data, Art. 3.1.

② Ibid., Art. 2.1.

③ 《非个人数据自由流动条例》和 GDPR 都没有定义"密不可分地联系"的概念。在实践中,可以是指这样的情况,即混合数据集既包含个人数据又包含非个人数据,并且将两者分离是不可能的,或者被控制者认为在经济上效率低下或在技术上不可行。See European Commission, "Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union," COM(2019) 250 final.

④ The Regulation on the Free Flow of Non-personal Data, Art. 2.2.

⑤ See EU-UK Trade and Cooperation Agreement, Part 2 Title III Chapter 2.

⑥ Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA.

定。欧英协定条文的表述与欧委会于 2018 年 4 月批准的跨境数据流动和个人数据保护规则范本①基本一致,其要旨是个人数据是一项基本权利,在贸易协定中是不可谈判的,贸易协定在不影响欧盟数据保护和隐私规则的前提下,禁止跨境数据流动的保护主义壁垒。欧盟这一立场也体现在与澳大利亚②、新西兰③的贸易协定谈判以及 WTO 电子商务谈判④中。可见,未来欧盟有关非个人数据跨境流动的贸易协定谈判或数据治理国际合作也将继续遵循上述基本立场,即除了个人数据和隐私保护,欧盟对非个人数据跨境自由流动并没有特别考虑。那么,在非个人数据并非欧盟首要关切的情况下,中欧之间非个人数据跨境流动的合作将留给中国更大的空间。

2.中欧重要数据的跨境流动机制

中国对非个人数据跨境流动的管理主要围绕重要数据展开,以数据安全为要义。《网络安全法》首次在法律层面提出重要数据的概念以来,中国已经开始高度重视数据安全保护。《数据安全法》将重要数据作为核心概念,要求建立国家数据分类分级保护制度。《网络安全审查办法(修订草案征求意见稿)》将重要数据的风险作为重要考虑因素之一。不同于其他国家大多对具体部门、特定场合的数据进行管理,中国把重要数据作为一个大类提出统一要求,体现出从战略高度审视重要数据保护及数据安全问题。其中,本地存储和出境安全管理是重要数据保护制度的核心内容。

中国除依法要求重要数据在境内存储外,还构建了以出境安全评估为核心的出境安全管理制度,包括两个层面:一是关键信息基础设施的重要数据的出境安全管理,适用《网络安全法》的规定。关于关键信息基础设施的范围,《关键信息基础设施安全保护条例》将公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的重要网络设施、信息系统等纳入其中,并规定由行业主管部门认定关键信息基础设施。关于重要数据,2021 年 9 月发布的《信息安全技术 重要数据识别指南(征求意见稿)》明确了识别重要数据的基本原则和流程。二是其他重要数据的出境安全管理办法,由国家网信部门会同有关部门制定。⑤ 此外,《关于汽车数据安全管理的若干规定(试行)》等行业数据管理规定也涉及所在行业重要数据出境的相关规则。

① See EU's Horizontal Provisions for Cross-border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements).

② See EU-Australia Free Trade Agreement, Initial Text Proposal Tabled by the EU Side on Digital Trade, Chapter II Data Flows and Personal Data Protection, 10 October 2018.

③ See EU-New Zealand Free Trade Agreement, Initial Text Proposal Tabled by the EU Side on Digital Trade, Chapter II Data Flows and Personal Data Protection, 25 September 2018.

④ WTO, "Communication from the European Union, Joint Statement on Electronic Commerce—EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce," INF/ECOM/22, 26 April 2019, para. 2.8.2.

⑤ 参见《数据安全法》第 31 条。

针对重要数据出境安全评估制度的实施,2021 年 10 月发布的《数据出境安全评估办法(征求意见稿)》确立了风险自评估与安全评估相结合的机制,①并适用于所有数据处理者,②较之《网络安全法》规定的关键信息基础设施运营者而言更加宽泛,且安全评估基本属于个案评估,③进一步反映出强化数据安全监管的大趋势。

当然,重要数据本地存储和出境安全评估并非绝对要求。《数据安全法》规定要开展数据领域国际交流与合作,参与数据安全相关国际规则和标准的制定,促进数据跨境安全、自由流动。④《关于汽车数据安全管理的若干规定(试行)》也明确中国缔结或者参加的国际条约、协定有不同规定的,适用该国际条约、协定,但中国声明保留的条款除外。⑤ 上述规定为中欧之间以合作协议或备忘录的方式,就重要数据跨境传输做出特殊安排提供了法律依据。

中欧重要数据跨境传输协议或备忘录应以中国已有的重要数据出境安全评估制度为基础,以提升跨境数据流动便利性为宗旨,建立合规成本更低的评估制度,实现保障安全与有效利用的合理平衡。考虑到重要数据的特殊性和敏感性,双方可以采用监管数据沙盒的形式,在特定行业或者特定地理区域内先行先试,通过便利跨境数据流动来促进数据驱动型创新。

总体而言,中欧跨境数据流动合作以不改变各自国内法律体系为前提,以规则为基础,构建对另一方数据保护制度的信任,打通个人数据和非个人数据跨境传输的通道。中欧推进跨境数据流动合作,将在很大程度上惠及中欧数字企业,实现两方数据资源、两大数字市场的进一步联通,并为广泛开展数字领域其他合作奠定基础、树立标杆。

五 中欧跨境数据流动合作:超越双边协调的全球意义

在全球范围内,数据流动对数字技术和数字经济的重要作用已经得到越来越广泛的认同。特别是新冠疫情暴发以来,数字技术和数字经济对全球抗击疫情和经济复苏发挥着至关重要的作用,更凸显出数据流动不可或缺。随着数字化转型不断推进,数据流动还会继续增加。跨境数据流动所引发的网络安全、数据安全、隐私保护等问题是跨国界的,没有一个国家可以单独解决,因此需要开展强有力的多边合作。

① 参见《数据出境安全评估办法(征求意见稿)》第 3 条。
② 同上文,第 2 条。
③ 同上文,第 12 条。
④ 参见《数据安全法》第 11 条。
⑤ 参见《关于汽车数据安全管理的若干规定(试行)》第 11 条。

然而,数字经济的起步阶段恰逢国际秩序深度调整期。单边措施和区域协调并行,导致数据领域的治理规则面临严重碎片化的风险,中美欧激烈博弈又进一步加剧了全球数据圈的“巴尔干化”趋势。一方面,各国采取的跨境数据流动限制措施和数据本地化要求在不断增加。据美国信息技术与创新基金会统计,数据本地化措施正在全球蔓延,2017-2021 年间本地化措施的数量翻了一番,62 个国家/地区实施了 144 项限制,还有数十项正在考虑中。① 另一方面,越来越多的区域贸易协定和数字经济协定包含个人信息保护、跨境数据流动等数据相关条款,呈现出“意大利面碗”效应;隐私和数据保护的诸边框架也相互交叉重叠,目前至少有 96 个经济体参与了经济合作与发展组织(OECD)隐私指南、欧洲委员会(Council of Europe)《关于个人数据自动化处理的个人保护公约》、APEC 跨境隐私规则体系等一系列安排。②

在这样的背景下,推动中欧跨境数据流动合作取得切实成果,不仅将促进中欧双方共享数字经济红利,使中欧数字关系迈向更高水平,也将展现出超越双边协调的全球意义。第一,中欧跨境数据流动合作将为全球数字领域标准和规则的制定提供制度性国际公共产品,在一定程度上填补国际公共产品供给的缺口,缓解国际社会集体行动的困境;第二,中欧跨境数据流动合作将证明不仅所谓志同道合的“民主”国家可以共同制定全球数字规则,价值体系、监管模式不同的经济体也能就这一充满争议的议题达成一致,完全可以避免零和博弈;第三,中欧跨境数据流动合作也可能会反过来影响中美数字博弈,促使美国为了其数字企业在中国市场的利益,调整对华数字策略,令中美数字对抗得到缓解。

有鉴于此,推进中欧跨境数据流动合作,要站在统筹中华民族伟大复兴战略全局和世界百年未有之大变局的高度,既要认识到合作带来的广泛利益和广阔机遇,也要看到面临的阻力和困难。对此,中欧双方既要对中美欧数字博弈的发展态势、中欧之间的监管差异及其政治经济影响进行全面、深入分析,以便共同克服可能危及合作的挑战,也要跳出中欧之间利益博弈、制度博弈的思维定式,以尊重各自的价值理念和监管要求为前提,以发展破除难题,建立跨境数据流动合作机制,平衡反映双方关切,形成基于规则的、充分信任的、互利互惠的数字合作伙伴关系。

(**作者简介**:李墨丝,上海对外经贸大学国际经贸研究所研究员;**责任编辑**:张海洋)

① Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,” https://itif.org/sites/default/files/2021-data-localization.pdf.

② Francesca Casalini, Javier López-González and Taku Nemoto, “Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers,” p.20.