

中美欧竞争背景下的欧盟“数字主权”战略研究^{*}

闫 广 忻 华

[内容摘要] 数字技术正成为数字时代大国地缘战略竞争的关键抓手。欧盟改变了单纯对数字技术造成的问题进行治理的思路,转而从地缘政治、经济、技术民族主义出发制定数字发展战略。欧盟“数字主权”战略是中美竞争、新冠疫情冲击、数字地缘博弈等合力作用的结果。本文力图对欧盟“数字主权”进行概念化处理并为其搭建一个多层次解释性框架。本文提出,欧盟认知下的“数字主权”指在数字经济与安全领域中,欧盟掌握自主控制和运用数字技术的能力,以及对全球数字标准进行规范的权力。欧盟“数字主权”战略实践紧紧围绕自主与规范这两大内核展开,即通过数字基础设施的建设来构建自主性控制能力,通过数字的监管来塑造规范性权力。欧盟的目标是自主控制数字技术和战略性价值链,并向全球输出数字标准和规则。欧盟“数字主权”战略实践也面临着多重挑战。在数字地缘博弈愈演愈烈的背景下,作为“数字战略大三角”的中美欧如何以多边力量共同维护数字空间秩序和推动全球数字技术发展已成为全球数字治理面临的新课题。

[关键词] 欧盟 数字主权 大国竞争 数字地缘博弈 数字治理

[作者简介] 闫广,上海外国语大学上海全球治理与区域国别研究院博士研究生、上海外国语大学欧盟研究中心助理研究员;忻华,上海外国语大学欧盟研究中心主任、研究员,上海交通大学国际战略研究中心特聘研究员

大数据、人工智能等数字技术极大地重塑了经济业态,数字经济发展方兴未

^{*} 本文系2022年复旦大学博士生学术论坛之国务论坛获奖论文,感谢复旦大学潘忠岐、余博闻老师为本文提供的有益指导。同时,感谢《国际关系研究》编辑部和匿名评审专家为本文提出的宝贵修改建议,文责自负。

艾。数字技术已成为数字时代大国地缘战略竞争的关键抓手和衡量国家实力的关键性指标。当前,中美欧三足鼎立的全球数字地缘版图已初现端倪。^①但是,美国和中国在数字技术与数字市场领域总体领先于欧盟,欧盟数字市场更是被美国的高科技跨国公司(也被很多人称为“数字巨头”)所垄断。由此,欧盟担心沦为中美的“数字殖民地”。^②2019年,新任欧盟委员会主席冯德莱恩将打造一个“适应数字时代的欧洲”确定为其任期内的优先事项之一,称欧盟委员会将致力于通过新一代数字技术为欧洲赋能,让数字化转型惠及所有人。^③欧盟由此提出“数字主权”^④战略并陆续出台了多部有关“数字主权”战略的政策文件。由于越来越担心其公民、企业和成员国失去对数据、数字创新能力以及数字立法能力的控制权,欧盟改变了单纯对数字问题进行治理的思路,转从地缘经济政治出发制定数字发展战略。^⑤

随着美国对华芯片禁运、对华为和中兴公司产品全面禁售以及美欧各自芯片法案的出台,数字空间凸显其地缘战略意义。鉴于中美技术战的加剧对美欧和中欧关系的影响,特别是拜登上台以来美欧之间在高科技领域针对中国的战略协作的增加,对欧盟“数字主权”的本质特征与最新动态展开研究具有突出的理论价值与现实意义。但是,目前学界对欧盟“数字主权”战略及其相关政策架构的系统性阐释还较为缺乏。既有研究总体上可归纳为两类:一类是对欧盟数字政策文本的解读。有学者分析了《数字服务法》和《数字市场法》,指出这两部

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

② Nocetti Julien, “Is Europe a ‘Digital Colony’ of the United States?” *Politique étrangère*, Vol. 86, No. 3, 2021, p. 51.

③ Ursula von der Leyen, “Political Guidelines for the Next European Commission 2019 ~ 2024,” <https://op.europa.eu/publication-detail/-/publication/62e534f4-62c1-11ea-b735-01aa75ed7/a/>.

④ 当前学界存在“数字主权”与“技术主权”两种不同的表述方式。本文将二者进行了统一。本文认为,“技术主权”中的“技术”一词主要是指“数字技术”,即“技术主权”本质上等同于“数字主权”。欧洲议会研究中心等智库和西奥多·克里斯塔克斯等学者同样将“技术主权”视同“数字主权”,参见 European Parliamentary Research Service (EPRS), “Digital Sovereignty for Europe,” [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf); Theodore Christakis, “‘European Digital Sovereignty’: Successfully Navigating Between the ‘Brussels Effect’ and Europe’s Quest for Strategic Autonomy,” p. 9, <https://ssrn.com/abstract=3748098>.

⑤ 忻华:《“欧洲经济主权与技术主权”的战略内涵分析》,《欧洲研究》2020年第4期,第5页。

法案是欧盟数据治理的重要法案和欧洲“再主权化”的重要推动力。^①《欧洲数字议程》只强调“技术决定论”，未能满足各利益相关方的需求。^②还有学者指出，尽管《欧盟数据战略》在数据保护和数据跨境自由流动之间开拓了一条颇具特色的中间道路，但同时，欧盟在跨国数据保护与数据单一市场建立之间形成了战略冲突。^③另一类文献探讨了数字平台、数据保护等具体议题。有研究指出，欧盟个人数据跨境流动政策经历了从“公约”到“指令”再到“条例”的转变，这代表着欧盟的个人数据跨境流动政策从柔性规范上升到了刚性约束。^④还有学者指出，欧盟的数字监管模式旨在捍卫社会福利、民主、市场体系和自由价值观，欧盟已成为数字领域的“监管超级大国”。^⑤

区别于既有研究，本文尝试对欧盟“数字主权”战略展开系统分析。本文将首先从现实与理念两方面入手，通过探究欧盟“数字主权”建设的现实背景与理念基础来分析其背后的国际政治意涵。其次，本文将通过为欧盟“数字主权”战略搭建一个解释性框架来厘清其核心要义与目标指向，并进一步探讨欧盟“数字主权”的战略实践。本文最后的部分将探讨欧盟“数字主权”战略实践所面临的挑战。

一、欧盟“数字主权”建设的战略背景

欧盟“数字主权”战略的提出既与中美大国竞争因素有关，也与欧盟对自身数字技术发展不足的反思有关。面对世纪疫情，这些不足体现得尤为明显和棘手。

① Annegret Bendiek, “Integrationspolitische Bedeutung des Digital Service Act (DSA) und Digital Markets Act (DMA),” https://www.swp-berlin.org/fileadmin/contents/products/sonstiges/Bendiek_BT-Stellungnahme_Digitalpaket_der_KOM_02-2021.pdf.

② Sergey Kamolov and Igor Stepnov, “Sustainability through Digitalization: European Strategy,” *E3S Web of Conferences*, Vol. 208, 2020, <https://doi.org/10.1051/e3sconf/202020803048>.

③ 王中美：《欧盟数据战略的目标冲突与中间道路》，《国际关系研究》2020年第6期，第59页。

④ 方芳：《欧盟个人数据跨境流动政策的演变：市场统一与贸易规范》，《复旦国际关系评论》2020年第24辑，第16页。

⑤ Schneider Ingrid, “Democratic Governance of Digital Platforms and Artificial Intelligence? Exploring Governance Models of China, the US, the EU and Mexico,” *JeDEM - eJournal of eDemocracy and Open Government*, Vol. 12, No. 1, 2020, pp. 1 ~ 24.

(一) 国际技术竞争加剧背景下的大国博弈

安德鲁·芬伯格指出,当社会围绕着技术来组织时,技术力量就是社会中权力的主要形式。因此,技术是社会斗争的舞台,技术的设计本质上充满了政治后果。^① 在当前的大国博弈中,美国是将技术政治化与武器化的典型代表。过去几年间,美国不断地利用“技术武器”对中国进行技术打压,这一做法引起了欧盟的警觉与思考。欧盟认为,中美之间日益加剧的技术竞争为欧盟争取“数字主权”提供了参照,中美数字技术博弈已开始影响几乎每一个技术问题。

与此同时,“数字巨头”逐渐开始扮演“准主权者”的角色,表现出政治化和国家化的倾向。^② 当前,欧盟对“数字主权”的呼声明显在增加,原因是主权的真正挑战不只在数字空间的虚拟性,还在于“数字巨头”的市场势力,因为拥有垄断地位的美国数字企业掌握着重要的物质和非物质力量。肖莎娜·祖波夫认为,“数字巨头”不仅是数字中介和数字“守门人”,^③而且还掌握着巨量的资源。企业凭借市场地位行使控制权,进而成为主权的最大挑战之一。^④ “数字巨头”在高度敏感的地方干预国家事务,这在欧洲引发了对数字领域新的、更具结构性的、更为宽泛的思考。^⑤ 欧洲智库强调,欧洲已经“陷入了交叉火力之中”。^⑥ 因此,维护“数字主权”便成为了欧盟摆脱依赖、避免在未来大国竞争中失势的关键。

① [美] 安德鲁·芬伯格著,韩连庆、曹观法译:《技术批判理论》,北京大学出版社 2005 年版,第 1、16、18 页。

② 郝诗楠:《“自由”与“不自由”:高科技跨国公司的政治化与国家化》,《国际展望》2021 年第 3 期,第 126 页。

③ 欧盟《数字市场法》明确定义了“守门人”:对欧盟内部市场有重大影响、运营一个或多个重要的客户网关,以及在其运营中享有或预期享有牢固和持久地位的核心平台的提供商。达到“守门人”的标准有:1. 前 3 年年度营业额在欧洲市场平均达到 65 亿欧元,或 1 个财年市值达 650 亿欧元,且至少在 3 个成员国提供中介服务;2. 欧盟境内月活跃用户达到 4500 万或上一财年注册商户达到 1 万。参见 European Commission, “Digital Markets Act,” <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en>。

④ Sam DiBella, “Book Review: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power by Shoshana Zuboff,” <https://blogs.lse.ac.uk/usappblog/2019/11/10/book-review-the-age-of-surveillance-capitalism-the-fight-for-a-human-future-at-the-new-frontier-of-power-by-shoshana-zuboff/>。

⑤ José van Dijck, “Governing Digital Societies: Private Platforms, Public Values,” *Computer Law & Security Review*, Vol. 36, 2020, pp. 1~4.

⑥ Carla Hobbs, ed., “Europe’s Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry,” p. 8, https://ecfr.eu/archive/page//europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf.

(二) 欧盟在中美欧数字技术竞争当中的相对弱势地位

相较于欧盟,中国与美国总体处于数字技术和市场的优势地位。欧盟对美国的数字平台更是存在严重依赖,这加剧了欧盟的脆弱性。2015 年德国《明镜》杂志曾以《世界政府——硅谷如何控制我们的未来》为封面标题,将硅谷的数字企业称为“世界政府”,^①引起了一时的轰动。2018 年,中美两国占了全球区块链技术相关专利的 75%,全球云计算市场的 75% 以上和全球 70 个最大数字平台 90% 的市值份额。中美两国七个“独角兽”数字平台占据了总市值的三分之二,而欧洲在其中的份额仅为 4%。^②从智能设备操作系统来看,截至 2022 年 9 月,Android 在全球的市场份额为 42.96%,高居榜首。美国三大操作系统 Android、Windows 和 iOS 共同拥有全球市场份额的近 89.81%。^③

与中美相比,欧盟在数字创新、人工智能、芯片、云存储等技术方面较为落后(见图 1),且严重依赖美国企业。截至 2022 年 9 月,Android 和 iOS 在欧盟的市场份额达 99.24%。谷歌以 91.96% 的市场份额在欧洲市场占绝对主导地位,^④包括欧盟在内的西方国家 92% 的数据存储在美国。^⑤欧洲对外关系委员会主任杰里米·夏皮罗指出,“欧盟越来越担心美国滥用其数字主导地位,越来越感到对美国互联网公司的新殖民主义的依赖。这种依赖至少到目前为止远远超过了欧洲对中国的数字依赖。如果从数字主权的角度来看,美国是最大的问题,那么中国就成了最大的恐惧。”^⑥

① “Wie das Silicon Valley unsere Zukunft steuert,” <https://www.spiegel.de/spiegel/print/index-2015-10.html>.

② 联合国贸易和发展会议:《2019 年数字经济报告》,第 3 页, https://unctad.org/system/files/official-document/der2019_overview_ch.pdf。

③ “Operating System Market Share Worldwide (Dec 2021 ~ Dec 2022),” <https://gs.statcounter.com/os-market-share>.

④ “Mobile Operating System Market Share Europe,” <https://gs.statcounter.com/os-market-share/mobile/europe>; “Search Engine Market Share Europe,” <https://gs.statcounter.com/search-engine-market-share/all/europe>.

⑤ World Economic Forum, “What is Digital Sovereignty and Why is Europe so Interested in It?” <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>.

⑥ Carla Hobbs, ed., “Europe’s Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry,” p. 10, https://ecfr.eu/archive/page/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf.

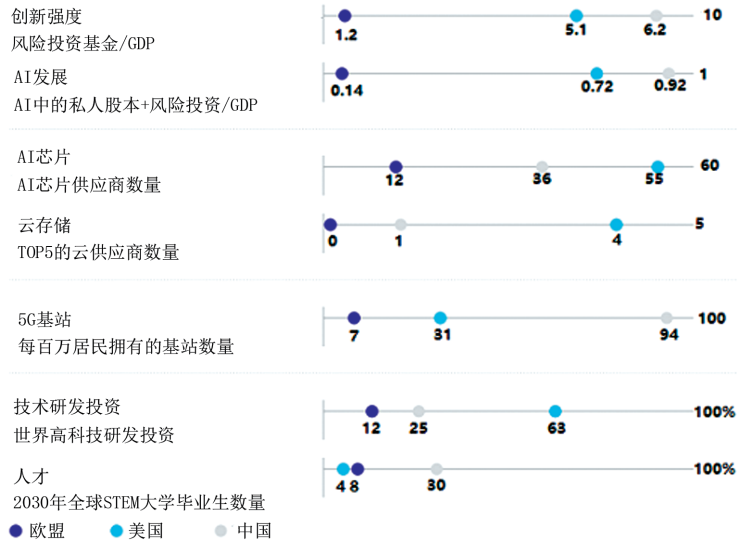


图1 美国、中国和欧盟数字能力记分卡

图表来源: Emmanuel Amiot et al., “European Digital Sovereignty — Syncing Values and Value,” p. 11, <https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf>.

(三) 新冠疫情凸显数字技术对经济和公共卫生体系韧性的重要性

新冠疫情凸显了数字技术对经济和公共卫生体系韧性^①的重要性。有学者直言,新冠疫情清楚地表明了数字化在当今世界应对全球危机的中心作用。^② 经合组织更是将新冠疫情称为发展数字技术的“巨大加速器”。^③ 强大的数字基础设施对国家的管理和疫情期间政府的反应能力至关重要。数字平台使得在线工作、在线教育和在线社会互动成为社会大部分人的生活方式,数字技术使公民有能力监测他们的健康状况,并提高护理以及医疗系统的效率。

新冠疫情暴露了欧盟及其成员国在数字技术上的弱点,抗疫的沉重代价迫

① 韧性通常是指在面对变化时能够坚持,在不断变化的环境中保持继续发展的能力,是关于人类、社区、社会、文化等在面对动态变化时适应以及转变发展道路的能力。在本文中,专指在新冠疫情中,经济与公共卫生体系应对、恢复和提升的能力。参见 Carl Folke, “Resilience,” *Ecology and Society*, Vol. 21, No. 4, 2016, p. 10.

② Frances G. Burwell and Kenneth Propp, “The European Union and the Search for Digital Sovereignty: Building ‘Fortress Europe’ or Preparing for a New World?” p. 3, <https://www.jstor.org/stable/resrep26697>.

③ OECD, “OECD Digital Economy Outlook 2020,” <https://dx.doi.org/10.1787/bb167041-en>.

使欧盟反思自身数字技术发展的不足。对欧盟来说,新冠疫情除了造成大量的人员死亡外,还揭示了欧洲经济和社会的严重混乱。预警系统和协调机构处于紧张状态表明欧盟对大规模危机情况进行管理的不足。疫情初期,由于信息的不对称、不畅通,许多医院不堪重负,基本药品和设备短缺,人员和货物的自由流动受到严重限制;许多学校因无法提供替代教室的数字化教学方式被迫关闭。^①韧性的提升要求具备有效的信息系统以及能够及时评估影响的监测系统。^②而欧盟面临的矛盾是,一方面不得不过度依赖美国的信息平台、信息技术以及监测系统,另一方面则是对隐私和数据泄漏的担忧。疫情期间,供欧洲各国使用的数字解决方案基本都源自欧洲之外:Gmail、Zoom 提供了视频通话服务;Skype、亚马逊、微软提供了云服务;脸书、Instagram 提供了社交服务;优步提供了送货和通勤服务等。因此,通过加强创新使欧盟自身掌握数字技术便成了必要选择。新冠疫情警示了欧盟的数字化转型和掌握“数字主权”是一个关乎生死存亡的问题。^③为了应对新冠冲击,2021 年欧盟建立了“恢复与韧性基金”,计划为其成员国提供 1270 亿欧元的资金以专门支持数字化转型。^④

二、欧盟“数字主权”战略的理念基础

欧盟“数字主权”战略的提出既有现实因素的考量,也有理念的塑造。欧盟“数字主权”的理念基础包括技术民族主义与“欧洲主权”愿景。

① European Commission, “2020 Strategic Foresight Report,” p. 6, https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight/2020-strategic-foresight-report_en.

② Steve Thomas et al., “Strengthening Health Systems Resilience: Key Concepts and Strategies,” WHO Regional Office for Europe, 2020, p. 4, <https://apps.who.int/iris/bitstream/handle/10665/332441/Policy-brief%2036-1997-8073-eng.pdf>.

③ Carla Hobbs, ed., “Europe’s Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry,” p. 1, https://ecfr.eu/archive/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf.

④ 关于“恢复与韧性基金”,参见 European Commission, “Regulation (EU) 2021/241,” <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0241>; European Commission, “Digital Economy and Society Index 2022,” p. 8, <https://digital-strategy.ec.europa.eu/en/policies/desi>.

(一)“数字主权”的理论基础:技术民族主义

工业化时代以来,国家间经济竞争形式总体上经历了从贸易竞争到产业竞争再到技术竞争的发展路径。贸易竞争是国家间经济竞争的初始形态;产业竞争是贸易竞争的高级形态;技术竞争则是产业竞争的延伸。^①与此相对应的是,国家间经济竞争理念经历了从重商主义到经济民族主义再到技术民族主义的演化路径。重商主义于16~18世纪在西欧盛行,主张通过贸易保护等国家干预的手段实现贸易顺差以进行资本原始积累,最终达到国家富强的目的。在吸取重商主义将货币看作国家财富的唯一形态和将顺差看作是财富的唯一来源的教训后,工业国家开始关注本国的产业竞争力问题。作为贸易竞争高级阶段的产业竞争,是民族主义经济学发展的初始领域。^②其中,关于经济民族主义理念的阐释,尤以德国学者李斯特最具代表性。^③而中美欧数字技术竞争推动下的欧盟“数字主权”战略本质上体现的是技术民族主义思想。^④

技术民族主义最早于1987年由加州大学罗伯特·莱克教授提出。他认为,日本在短短几十年的时间里通过“技术立国”从战争的废墟中站立起来,对美国的技术霸权构成严重威胁,美国应该对技术优势进行保护和强化。^⑤之后,多位学者对技术民族主义展开研究。概而言之,技术民族主义通常被认为是与技术全球主义相对的概念,强调科学技术的进步对提升竞争力的重要作用,技术实力被视为是国家兴衰最重要的决定因素之一。政府旨在通过市场干预与保护的手

① 王玉柱:《发展阶段、技术民族主义与全球化格局调整——兼论大国政治驱动的新区域主义》,《世界经济与政治》2020年第11期,第147~148页。

② 民族主义经济学也被称为“李斯特主义”,参见贾根良:《新李斯特主义:替代新自由主义全球化的新学说》,《学习与探索》2012年第3期,第101~109页。

③ 关于李斯特经济民族主义,参见Friedrich List, *The National System of Political Economy*, New York: Longmans, Green, and Co., 1909, pp. 159~263。

④ 参见崔宏伟:《重启搁置8年的自贸谈判,欧盟为何加速推进对印新战略?》, <https://wenhui.whb.cn/third/baidu/202105/13/404540.html>;余南平、戢仕铭:《西方“技术联盟”组建的战略背景、目标与困境》,《现代国际关系》2021年第1期,第52页。

⑤ Robert Reich, “The Rise of Techno-Nationalism,” *Atlantic Monthly*, Vol. 1, No. 5, 1987, p. 31.

段培育行业竞争优势与“行业冠军”,实现技术赶超。^①

但是,欧盟“数字主权”战略所呈现出的技术民族主义与传统技术民族主义相比,二者既有共性,也存在明显的差异。相同点主要表现在二者都把非市场力量(政府等公共权力部门)对高科技市场的干预、规制、保护视为实现自身技术进步与经济、技术安全的手段,具有保护主义色彩。而不同于传统技术民族主义的是,“数字主权”战略所呈现的技术民族主义有如下新变化:第一,新一轮技术民族主义主要由西方发达国家所推动,而传统的技术民族主义被认为是技术落后的国家(一般指发展中国家)旨在培养本国的冠军企业、寻求技术赶超而特有的现象。^②第二,技术政治化,尤其是意识形态化。传统技术民族主义聚焦于技术进步所带来的比较优势等经济指标,而“数字主权”不仅着眼于经济科技竞争力,而且关注欧盟整体的地缘政治战略利益和价值观。第三,对技术的负外部性(也被称为“科技反冲”^③)的反思。传统的技术民族主义主要是对技术的正外部效应的追求,而在新一轮技术民族主义中,技术所带来的负面问题被渲染为“安全威胁”,成为欧美不断强调和利用的“噱头”。第四,突出反垄断监管。反垄断监管是欧盟“数字主权”战略实践的重要内容,欧盟通过对域外数字巨头企业(主要是美国企业)的反垄断规制来保护内部数字平台,通过严厉的惩罚措施来规范域外企业的市场行为以符合欧盟自身的市场规则和经济利益。

(二)“数字主权”的思想基础:“欧洲主权”愿景

近年来,学界关于“欧洲主权”的争论甚嚣尘上。现代主权的观念发端于欧洲,以《威斯特伐利亚和约》为标志确立了主权的实体,即民族国家在国际关系当中的主体性与合法性地位。随着欧洲一体化的持续推进,欧盟的超国家性凸显。因此有学者认为,所谓的“欧洲主权”概念是不存在的,因为欧盟不是民族国家,

① 关于技术民族主义的定义,参见 Robert A. Manning, “Techno-Nationalism vs. the Fourth Industrial Revolution,” *Global Asia*, Vol. 14, No. 1, 2019, p. 15; Shigeru Nakayama, “Techno-Nationalism versus Techno-Globalism,” *East Asian Science, Technology and Society*, Vol. 6, No. 1, 2012, p. 11; 王玉柱:《发展阶段、技术民族主义与全球化格局调整——兼论大国政治驱动的新区域主义》,《世界经济与政治》2020年第11期,第144页。

② 李峥:《新一轮技术民族主义危害更甚》,《环球时报》2021年4月21日,第14版。

③ 李峥把技术进步所带来的社会和安全问题称为“科技反冲”现象。参见李峥:《全球新一轮技术民族主义及其影响》,《现代国际关系》2021年第3期,第35页。

并非具有独立的、至高无上的国家主权的属性。^① 但不可忽略的是,主权议题是贯穿欧洲一体化的核心议题之一,欧盟也正是成员国主权让渡的结果。欧盟作为超国家组织,是主权国家的集合。赵怀普教授指出:“欧洲一体化的经验表明,国家已不再是唯一的主权实体,超国家组织可以是集合主权实体”。^②

事实上,将“欧洲主权”概念与“国家主权”进行类比从而认为“欧洲主权”概念不成立的推导逻辑是有失偏颇的。^③ 这是因为:第一,“欧洲主权”所追求的不是欧盟在法律意义上的主权合法性,而是欧盟在大国地缘战略竞争当中的实际战略能力和自主性诉求;第二,以“欧洲主权”为基础和依托的“数字主权”本身超越了经典国家主权的“属地属人”原则。需要强调的是,“数字主权”之所以以“欧洲主权”为基础和依托,是因为近年来欧盟的重大政治话语表述基本是建立在“欧洲主权”愿景的基础之上的。^④ 从2016年欧盟正式提出“战略自主”概念^⑤到2017年马克龙公开提出“主权欧洲”的目标^⑥再到2019年的“数字主权”,其实质都指向“欧洲主权”。战略自主是当前欧盟实现“欧洲主权”愿景的战略重点与政策抓手,欧盟还为这一战略搭配了“欧洲主权基金”^⑦等配套政策措施。而“数字主权”和“经济主权”等概念是在“战略自主”之下,为了应对来自不同领域的问题与挑战而衍生出来的。简言之,“数字主权”属于“欧洲主权”框架下的二级子集。另外,之所以说“数字主权”超越了国家主权的“属地属人”原则,是因为欧盟《一般数据保护条例》第3(2)条规定,新的数据保护法适用于非欧盟设立的数

① Antoine Bailieux, “The Two Face of European Sovereignty,” *European Papers*, Vol. 5, No. 1, 2020, pp. 303 ~ 306; Maxime Lefebvre, “Europe as a Power, European Sovereignty, Strategic Autonomy: A Debate that is Moving Towards an Assertive Europe,” <https://www.robert-schuman.eu/en/doc/questions-d-europe/qe-582-en.pdf>.

② 赵怀普:《欧盟政治与外交》,世界知识出版社2021版,第147页。

③ 曾向红、孟祥毅:《愿景政治视角下的“欧洲主权”构想》,《德国研究》2022年第1期,第6页。

④ 同上,第8页。

⑤ European Union, “Shared Vision, Common Action: A Stronger Europe,” https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

⑥ “President Macron Gives Speech on New Initiative for Europe,” <https://www.elysee.fr/en/emmanuel-macron/2017/09/26/president-macron-gives-speech-on-new-initiative-for-europe>.

⑦ 冯德莱恩在欧盟2022年度国情咨文中称将推动建立一个新的“欧洲主权基金”,确保欧洲未来的工业是“欧洲制造”,参见“2022 State of the Union Address by President von der Leyen” https://ec.europa.eu/commission/presscorner/detail/ov/speech_22_5493;欧盟内部市场专员蒂埃里·布雷顿指出,“欧洲主权基金”对涉及“欧盟主权”的任何工业领域项目提供支持,参见Thierry Breton, “A European Sovereignty Fund for an industry ‘Made in Europe’,” https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_5543。

据控制器和处理器,如果它们处理与欧盟数据主体有关的数据或者监测欧盟境内个人的行为,就必须接受监管。^① 这表明欧盟找到了不限于领土边界的方法来行使主权,由此,数据也可以是主权的一部分。欧盟在一个原本没有边界的数字世界建立管辖权,通过确定数字边界重新控制数据和数字基础设施。^②

法国总统马克龙是“欧洲主权”的坚定倡导者,他在接受巴黎高等师范学院地缘政治研究小组专访时曾对“欧洲主权”愿景作出明确回应。他强调,欧洲作为一个真正的民主国家的雏形已现。他表示坚决支持在欧盟委员会、欧盟理事会和欧洲议会之间出现一种主权形式,这种主权不是国家主权,而是“欧洲主权”,在战略自主中也许可以以一种更为中立的方式找到主权。马克龙指出,欧洲必须找到自决、摆脱依靠他人的方式,在所有“技术”上欧盟都实现自主。当在欧洲之外时,欧洲人是一个集体身份,欧洲是一个包含集体身份的凝聚的地理空间。^③ 由此可见,“欧洲主权”勾勒出一个源于现实又高于现实的愿景世界,其目标可被理解为:一是欧盟作为一个凝聚的地理空间维护欧盟整体发展利益和价值观;二是提升欧盟自主性,减少对外依赖并增强欧盟内生性根基。

三、欧盟“数字主权”的内涵界定与战略实践

在欧盟层面,2019 年之前“数字主权”很少被提及,更倾向于使用“战略自主”来间接映射数字技术方面的自主性。^④ 2019 年至今,除冯德莱恩之外,包括德国前总理默克尔、法国总统马克龙、欧盟“反垄断沙皇”玛格丽特·维斯塔格等在

① “General Data Protection Regulation,” <https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html>.

② Edoardo Celeste, “Digital Sovereignty in the EU: Challenges and Future Perspectives,” in Federico Fabbrini, eds., *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford: Hart Publishing, 2021, pp. 211 ~ 228.

③ “The Macron Doctrine: A Conversation with the French President,” <https://geopolitique.eu/en/macron-grand-continent/>.

④ Julia Pohle, “Digital Sovereignty: A New Key Concept of Digital Policy in Germany and Europe,” pp. 12 ~ 13, <https://www.kas.de/en/web/guest/single-title/-/content/digitale-souveraenitaet>.

内的越来越多的欧洲政治家公开支持欧盟“数字主权”。^①“数字主权”已成为一个强大且流行的话语,但是究其内涵却模糊而广泛。因此,本节在界定“数字主权”内涵的基础上着重对欧盟“数字主权”战略实践展开分析。分析发现,欧盟“数字主权”战略实践紧紧围绕自主性与规范性展开,即通过数字基础设施的建设来构建自主性控制能力,通过数字的监管来塑造规范性权力。

(一) 欧盟“数字主权”的内涵界定

2020年7月,欧洲议会研究服务中心发布了《欧洲数字主权》研究报告,报告认为“数字主权”是“欧洲在数字世界中独立行动的能力,应从保护机制和积极发展数字创新工具两方面来理解”。^②2020年9月,欧盟委员会欧盟内部市场专员蒂埃里·布雷顿撰文指出,“数字主权依赖于三个不可分割的支柱:计算能力、数据控制能力和安全连接能力,”并强调“欧洲现在必须将自己的战略利益掌握在自己手中以保护主权。在一个竞争日益激烈的世界里,自主权的争夺正在如火如荼地进行。面对美国和中国正在发动的‘技术战争’,欧洲现在必须为其未来20年的主权奠定基础”。^③同年10月举行的欧盟理事会特别会议提到:“要实现数字主权,欧盟层面必须建立一个真正的数字单一市场,加强自己制定规则、自主选择技术以及开发和部署战略性数字基础设施的能力。在国际层面,欧盟将继续向所有符合欧洲规则和标准的公司开放,利用工具和监管权力来帮助塑造全球规则和标准。”^④

从上述表述可看出,“自主性”和“构建全球规则和标准”是欧盟“数字主权”的应有之义。鉴于此,本文试图将欧盟“数字主权”概念化,并为其搭建一个多层次的解释性框架(见图2)。本文认为,欧盟“数字主权”是指在数字经济与安全领域中,欧盟自主控制、运用数字技术的能力以及对全球数字标准进行规范的权

① Theodore Christakis, “‘European Digital Sovereignty’: Successfully Navigating Between the ‘Brussels Effect’ and Europe’s Quest for Strategic Autonomy,” p. 9, <https://ssrn.com/abstract=3748098>.

② European Parliamentary Research Service, “Digital Sovereignty for Europe,” [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

③ Thierry Breton, “Europe: The Keys to Sovereignty,” https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en.

④ European Council, “European Council Conclusions EUCO 13/20 of 1st/2nd October 2020 Special Meeting,” <https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf>.

力。自主与规范是“数字主权”的“双内核”，其目标是自主控制数字技术和战略性价值链，并向全球输出数字标准和规则。

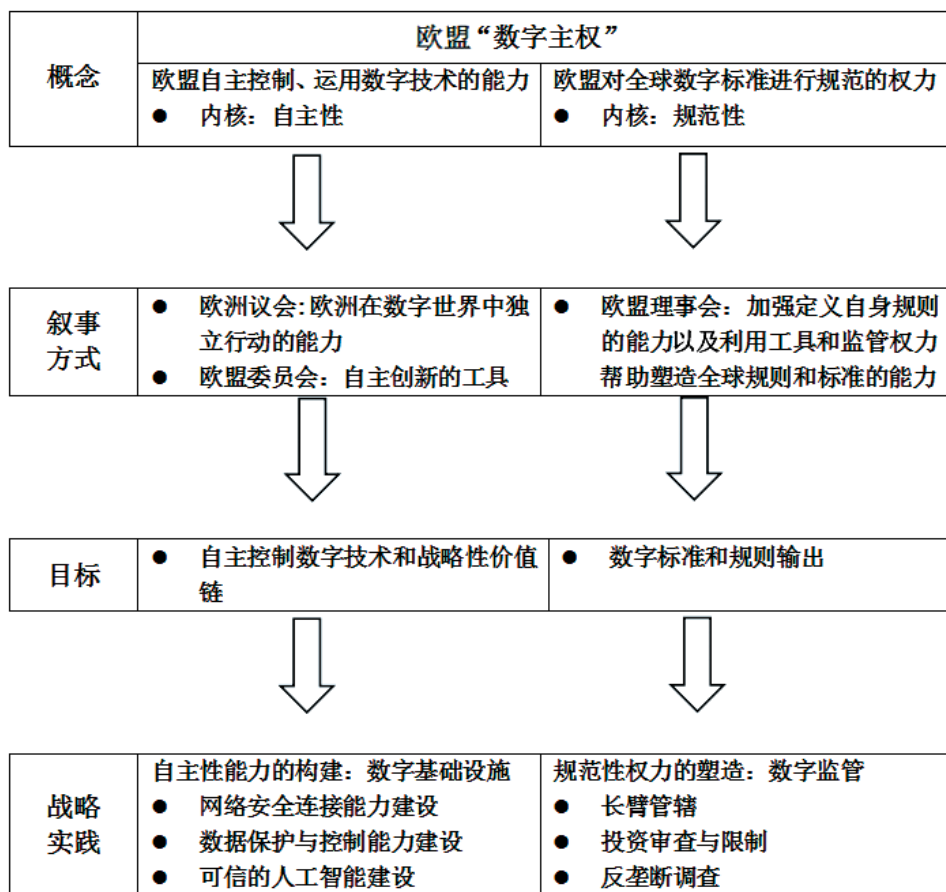


图 2 欧盟“数字主权”解释性框架

图表来源：笔者自制。

第一，“数字主权”指的是欧盟通过数字基础设施建设提升数字技术竞争力，自主掌控战略性技术和价值链的能力，其内核为自主性。欧洲议会和欧盟委员会所表述的“欧洲在数字世界中独立行动的能力”和“促进数字创新的工具”正是欧盟追求自主能力的直接反映。第二，“数字主权”是指欧盟对数字空间监管以及对数字标准进行规范的权力，其内核为规范性。欧盟理事会所说的欧洲“利用

工具和监管权力帮助塑造全球规则和标准的能力”同样是欧盟追求规范权力的直接反映。这是“布鲁塞尔效应”^①在数字领域的集中体现。从目前来看,获得欧盟数据充分保护认定的有包括日本在内的 14 个国家或地区。^②截至 2019 年底,全球有 66% 的国家已经通过立法保护网络数据和隐私,法律内容很大程度上受到了欧盟相关立法的影响。显然,数字“布鲁塞尔效应”已经奏效。

(二) 欧盟“数字主权”战略实践

1. 自主性能力的构建:数字基础设施

(1) 网络安全连接能力建设。2013 年的“棱镜门”事件让欧盟充分认识到了网络安全的重要性和网络威胁的严峻性。之后,欧盟通过实施一系列重要举措来维护网络安全。2016 年,欧盟委员会发布第一部网络安全立法文件《网络和信息安全指令》。^③《网络和信息安全指令》主要包含三个部分:一是国家能力,即强调欧盟成员国必须具备一定的网络安全能力,如组建国家计算机应急响应小组、进行网络演习等;二是跨境合作,即要求加强欧盟成员国之间的跨境合作,如战略网络和信息安全合作组等;三是关键行业的国家监管,即强调欧盟成员国必须对其本国关键市场运营商的网络进行监管,加强对关键行业(能源、交通、水、卫生、数字基础设施和金融行业)的事前监管和对关键数字服务提供商(在线市场、云和在线搜索引擎)的事后监管。2018 年 7 月,欧洲议会通过了《网络安全法》,为信息与通信技术产品、服务和流程创建了一个网络安全认证框架。在欧盟开展业务的公司需对其信息与通信技术产品、流程和服务进行一次认证,以确保消费者和企业免受网络安全威胁。^④同年 11 月,在法国巴黎举办的互联网治理论坛

① “布鲁塞尔效应”是由哥伦比亚大学教授阿努·布拉德福德提出,指欧盟正在通过其法律制度和标准行使前所未有的全球权力,欧盟无需诉诸国际机构或寻求其他国家的合作便能够颁布已根深蒂固于发达市场和新兴市场法律框架中的法规,从而导致全球商业的重要方面呈现“欧洲化”。参见 Anu Bradford, “The Brussels Effect,” *Northwestern University Law Review*, Vol. 107, No. 1, 2012, p. 271。

② 关于数据保护充分认定情况,参见 European Commission, “Adequacy Decisions,” https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en。

③ “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for A High Common Level of Security of Network and Information Systems Across the Union,” <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>。

④ “The Cybersecurity Act,” <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN>。

上,马克龙发起了“巴黎呼吁网络空间的信任和安全”的倡议,呼吁建立一个互联网监管框架,同时在国际上进一步扩大《一般数据保护条例》的使用。^①

欧盟委员会于2019年3月通过了《关于欧盟对5G网络安全采取共同办法》的建议,指出所有成员国都须对5G网络基础设施的风险进行评估。在此基础上,鼓励成员国更新对网络提供商的现有安全要求,特别是在授予5G频段无线电频率使用权时,如果公司不符合标准和法律框架,欧盟成员国有权出于国家安全原因将公司排除在其市场之外。^②2020年1月欧盟委员会公布了《欧盟5G网络安全工具箱》,通过在欧盟层面和成员国层面建立一个强有力的执行框架,确保整个欧盟的5G网络安全水平和成员国之间的协调。工具箱具体包括:《网络和信息安全指令》《网络安全法》和《外国直接投资审查条例》等多种审查和规制手段。欧盟委员会强调,各成员国制定解决5G安全问题的共同方法是欧盟在数字环境中战略自主性的重要考验。^③欧盟《2030数字罗盘》提出,到2030年,欧盟的通信技术专家将达到2000万,拥有基本数字技能的人口占80%。所有欧洲家庭都将被千兆网络覆盖,5G将覆盖所有人口密集的地区。欧盟将为欧洲公民和企业提供100%的在线公共服务,100%的欧洲公民可以获得医疗电子记录,80%的公民将使用数字身份证。^④截至2021年,欧盟平均网络覆盖率为70%,5G覆盖率达到66%。^⑤

(2)数据保护与控制能力建设。欧盟的数据保护倡导者长期以来一直在呼吁主权的必要性,不断重申对数据的控制能力。《一般数据保护条例》规定了“充

① “IGF 2018 Speech by French President Emmanuel Macron,” <https://www.intgovforum.org/en/content/igf-2018-speech-by-french-president-emmanuel-macron>.

② “Questions and Answers - Commission Recommends Common EU Approach to the Security of 5G Networks,” https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_1833.

③ NIS Cooperation Group, “Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures,” <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

④ European Commission, “2030 Digital Compass: The European Way for the Digital Decade,” <https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/>.

⑤ European Commission, “Digital Economy and Society Index (DESI) 2022—Digital Infrastructures,” <https://digital-strategy.ec.europa.eu/en/policies/desi-connectivity>.

分保护认定”原则,对个人数据的许可和使用限制有严格的要求。^① 2020年2月欧盟出台了《欧洲数据战略》,^②这是欧盟用数据为经济赋能的重要战略举措,其核心是要创建单一数据市场,使更多的非个人数据在欧盟内部市场和跨部门之间流动,以用于经济和社会发展,激励公共部门之间数据共享,通过跨部门治理框架来避免内部市场的撕裂。同年11月,欧盟发布的《数据治理法》旨在建立一个促进数据共享的框架,以安全地共享公共机构持有的敏感数据,规范个人的数据共享行为。^③

除了已有的法律手段外,欧盟还建立了专门的执行机构来保障各成员国数据存储与控制能力建设的落实。欧盟先后成立了欧洲数据保护委员会和欧洲数据保护专员公署。欧洲数据保护委员会根据《一般数据保护条例》而建立,由各成员国数据保护机构和欧洲数据保护专员公署的代表组成,致力于在整个欧盟范围内协调一致地应用数据保护规则,并促进欧盟数据保护机构之间的合作,确保《一般数据保护条例》和《欧洲执法指令》在欧盟得到一致应用。欧洲数据保护委员会除了可采用一般指导来阐明欧洲数据保护法的条款,还可以对成员国监管机构做出具有约束力的决定。^④ 欧洲数据保护专员公署是欧盟的独立数据保护机构,实质是欧洲数据保护委员会的常设秘书处,负责在法律和实践方面加强欧盟数据保护和隐私标准,确保对个人数据和隐私的保护,监视可能危害个人信息的技术。^⑤ 《欧洲数据保护委员会和欧洲数据保护专员公署之间的谅解备忘录》^⑥规定,欧洲数据保护专员公署具有独立性,不受欧洲数据保护委员会的干预,以保证其能在数据监管与隐私保护方面做到高效、独立和公正。

① Frances G. Burwell and Kenneth Propp, “The European Union and the Search for Digital Sovereignty: Building ‘Fortress Europe’ or Preparing for a New World?” <https://www.jstor.org/stable/resrep26697>.

② European Commission, “The European Data Strategy,” https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283.

③ European Commission, “Data Governance Act,” <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN.2020.11.25>.

④ European Data Protection Board, “Who We Are,” https://edpb.europa.eu/about-edpb/about-edpb_en.

⑤ European Data Protection Board, “About Us,” https://edps.europa.eu/about/about-us_en.

⑥ European Data Protection Board, “Memorandum of Understanding between the European Data Protection Board and the European Data Protection Supervisor,” https://edpb.europa.eu/sites/edpb/files/files/file1/memorandum_of_understanding_signed_en.pdf.

对欧盟而言,建立一个安全的覆盖整个欧盟的数据框架,加大对云存储等前沿技术的投资是至关重要的。为此,德法合作建立了“欧洲云”,计划自 2020 年起在欧洲层面建立一体化的数据基础设施以提升数据保护水平,并改变数据存储市场几乎完全由非欧洲供应商主导的现状。有学者认为,从“数字主权”的角度来看,它是一个合乎逻辑和有希望的举措。^① 2030 年之前,欧盟计划部署 10000 个高度安全的边缘节点,以保证个人或企业无论位于何处都能安全地、以低延迟(几毫秒)的速度访问数据服务。

(3)可信的人工智能建设。冯德莱恩在施政方针中提到,数据和人工智能是创新的要素,是可以帮助欧盟应对社会挑战的解决方案。2020 年 2 月,欧盟发布了《人工智能白皮书》,^②其中最主要的内容是构建“卓越生态系统”和“信任生态系统”。“前者是瞄准市场价值,调动资源以获得人工智能价值链上的最大收益;而后者是人工智能的监管框架。欧盟不仅要投资下一代数字技术,还要投资“支持创建可信人工智能的欧洲数据池”的基础设施建设。白皮书通过引入“值得信赖的人工智能”指南,对人工智能进行严格的评估,以防“变坏”。^③ 2021 年 4 月,欧盟委员会审议的《人工智能法》是继《人工智能白皮书》之后又一重量级法案。该法从“维护欧盟的技术领先地位,并确保欧洲人民可以按照欧盟价值观从人工智能中受益”的原则出发,在区分“禁止类人工智能”和“高风险类人工智能”的基础上进行风险管理。该法提出要确保投放到欧盟市场的人工智能系统是安全的,并尊重现行法律中的基本权利和欧盟价值观,要加速对安全、可信赖的人工智能应用的开发,促进欧盟单一数字市场的发展等目标。^④《人工智能协调计划》则指出,在创新的同时,推进道德议程有可能使欧洲企业在全全球市场上取得竞争

① Lokke Moerel and Paul Timmers, “Reflections on Digital Sovereignty,” pp. 24 ~ 25, <https://ssrn.com/abstract=3772777>.

② European Commission, “White Paper on Artificial Intelligence - A European Approach to Excellence and Trust,” https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

③ Andreas Aktoudianakis, “Fostering Europe’s Strategic Autonomy: Digital Sovereignty for Growth, Rules and Cooperation,” p. 14, https://www.epc.eu/content/PDF/2020/Digital_SA_paper_EPC_and_KAS.pdf.

④ European Commission, “Artificial Intelligence Act,” https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

优势。^① 上述法案展示了欧盟想要成为开发和部署尖端可信人工智能的世界领先地区的雄心。预计欧盟将在 10 年内投入 2000 亿欧元用于人工智能的开发。^② 欧盟力争到 2030 年,75% 的欧盟企业能使用云计算、大数据和人工智能,90% 以上的中小企业至少达到基本的数字强度。欧盟将扩大人工智能创新规模,改善人工智能融资的渠道,最终使人工智能独角兽数量翻一番。^③

2. 规范性权力的塑造:数字监管

汉斯·摩根索曾言,“当个人间的交往还主要停留在技术的可能性上,政府的控制则已变为技术和政治上的现实了”。^④ 欧盟对全球数字标准的规范主要是通过严密的数字监管,旨在实现规则主导,形成异于中美技术与市场主导的竞争优势。

(1) 长臂管辖。长臂管辖常被用于反垄断、贸易及知识产权等领域,其实质就是用本国的法律制度来管理和规制域外国家的事物,以达到“主权延伸”的目的。^⑤ 在数据保护方面,美国和欧盟也利用“长臂管辖”权力在域外国家谋求特权。美国《澄清合法使用境外数据法案》规定美国电子通信服务提供商和远程计算机服务提供商储存在境外的数据可以被美国执法机构“合法”地调取。^⑥ 而欧盟《一般数据保护条例》的第 3 条同样也有类似规定。这也就意味着,在未经他国同意的情况下,欧盟赋予了其执法监督机构对所有涉及欧盟业务的企业直接行使执法的权力。^⑦ 欧盟通过长臂管辖从两个方面规范全球数字标准:一方面以

① European Commission, “Coordinated Plan on Artificial Intelligence 2021 Review,” <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>.

② European Commission, “White Paper on Artificial Intelligence - A European Approach to Excellence and Trust,” p. 6, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

③ European Commission, “2030 Digital Compass: The European Way for the Digital Decade,” p. 10, <https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/>.

④ [美]汉斯·摩根索著,徐昕、郝望、李保平译:《国家间政治:权力斗争与和平》,北京大学出版社 2012 年版,第 299 页。

⑤ 屈文生:《从治外法权到域外规治——以管辖理论为视角》,《中国社会科学》2021 年第 4 期,第 44 ~ 45 页。

⑥ The United States Department of Justice, “Division V-Cloud Act,” <https://www.justice.gov/criminal-oia/page/file/1152896/download>.

⑦ 李海敏:《“数字丝路”与全球网络空间治理重构》,《国际论坛》2019 年第 6 期,第 23 页。

市场为杠杆和筹码,利用自身的国际地位与实力行使全球权力;另一方面则是以保障公民基本权利为借口,强行扩大自身法律的适用范围以实现法律规制标准与规则的全球适用。

(2)投资审查与限制。2019年3月欧盟发布了《欧盟外商直接投资审查条例》(下称“条例”),条例旨在阻止外国投资者对其战略性行业和企业进行投资和收购等危及到欧盟安全的商业活动。纵观整个条例的内容,可发现其审查目的十分明确。条例以“政治”“国家安全”为由,限制和排除重点高科技领域的外来投资,直指中美两国。条例规定了影响安全或公共秩序的投资范围,为成员国提供了一份提示性清单。审查主要聚焦于四个领域:关键技术和军民两用产品、关键基础设施、关键材料的供应、敏感信息的获取,重点包括人工智能、网络安全、通信、媒体、数据处理或存储、个人数据或控制信息的能力等。^①

(3)反垄断调查。欧盟不断加强数字经济领域的反垄断监管,^②对非欧盟(主要是美国)的数字巨头采取反垄断措施,且处罚的力度之大、金额之高,不断刷新纪录。欧盟的高压监管手段在全球处于“领先地位”。^③迄今为止,谷歌共遭到了欧盟三次反垄断罚款,累计罚款超过了80亿欧元,是欧盟最大的罚款对象。2020年底,欧盟曾指控亚马逊涉嫌利用其市场权力牟取对第三方卖家的不正当竞争优势,对其开出370亿美元的天价罚款。^④

2020年12月欧盟出台的《数字服务法》和《数字市场法》都强化了反垄断规则。《数字服务法》明确定义了“超级数字平台”。^⑤如果欧盟委员会认定超级平台存在垄断等不当的竞争行为,那么对这些平台的最高罚款可达其全球年收入

① European Commission, “Regulation (EU) 2019/452 of the European Parliament and of the Council: Establishing a Framework for the Screening of Foreign Direct Investments into the Union,” <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN>.

② 王晓晔:《数字经济反垄断监管的几点思考》,《法律科学(西北政法大学学报)》2021年第4期,第49页。

③ 杨洁:《数字经济背景下的反垄断应对:欧盟经验与中国路径》,《西华大学学报(哲学社会科学版)》2021年第4期,第70页。

④ 余颖:《加强反垄断监管是国际惯例》,《经济日报》2020年12月22日。

⑤ “超级数字平台”指拥有4500万用户或占有欧盟人口10%的在线平台。参见“Digital Platforms - New EU Regulations and Competition Law Tools,” <https://www.Antitrustlawblog.com/2020/12/articles/eu-competition-regulator-digital-platforms-eu-regulations-competition>.

或营业额的6%。按照《数字市场法》规定,欧盟对“守门人”的罚款最高可达其全球年收入或年营业额的10%;如果“守门人”存在持续性的违法行为,可按照最高额为其全球日平均收入5%的“日罚款”进行处罚;在“守门人”出现系统性违法的情况下,欧盟委员会除了可采用如罚款等行为性救济方式,还可采用诸如企业拆分或者业务剥离等结构性救济方式。^① 反垄断一方面可以通过多种惩罚或制裁的手段保护欧盟内部的数字平台,另一方面又通过这些严厉的惩罚措施倒逼超级数字平台按照欧盟制定的标准进行合规运营,进而达到规范的目的。

四、欧盟“数字主权”战略实践所面临的挑战

对欧盟来说,无论是自主性能力的构建,还是规范性权力的塑造都不可能一蹴而就,仍存在诸多限制性因素掣肘,“数字主权”建设之路可谓道阻且长。

(一) 欧盟内部的数字鸿沟与立场分歧

欧盟成员国之间数字发展不平衡,存在较大的数字鸿沟。欧盟《2022 数字经济与社会指数》报告指出,欧盟企业对人工智能和大数据等关键数字技术的采用仍然很低,数字技能水平不足阻碍了未来增长的前景,加深了数字鸿沟。芬兰、丹麦、荷兰和瑞典是欧盟的数字领跑者。2021年,在欧盟总人口中,具备基本数字技能的人口约占54%。同期,欧盟成员国罗马尼亚约为29%,而芬兰约为80%。欧盟55%的中小企业在数字化程度方面达到了欧盟认定的基本水平,瑞典高达86%,而罗马尼亚和保加利亚的中小企业数字化程度则最低。^② 不仅如此,欧盟成员国内部的州、城市与农村之间也存在着较大的数字鸿沟。2021年,欧盟城市宽带覆盖率与农村宽带覆盖率相差近30%,荷兰农村宽带覆盖率超过90%,而希腊仅有约20%。^③ 这些数字鸿沟增加了政策协调的难度,是欧盟数字

^① European Commission, “Digital Markets Act,” <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en>.

^② European Commission, “Digital Economy and Society Index 2022,” pp. 14 ~ 20, <https://digital-strategy.ec.europa.eu/en/policies/desi>.

^③ Ibid.

市场一体化的潜在障碍。

欧盟数字市场的碎片化。过去 10 年,欧盟在数字网络上的人均投资比美国少 40%。一个主要原因是市场的分裂,有多达 90 家欧洲运营商为 4.45 亿居民提供服务,而在美国只有 4 家运营商为 3.2 亿居民提供服务。因此,欧盟较为饱和的电信运营市场对投资者不具有很大的吸引力,而且运营商投资资金的不足反过来又限制了电信基础设施的改善。^①此外,欧盟的数据环境存在多种缺陷,数据互操作性标准不完善,缺乏相应的基础设施来支持数据池的建设。

欧盟成员国在数字政策上缺乏共识。以数字税为例,荷兰与法国在征收数字税方面表现最为积极。2018 年,法国在欧盟率先提议征收数字服务税,但遭到爱尔兰、瑞典和丹麦的反对,导致倡议失败。最终法国还是在国家层面实施了数字服务税,并于 2020 年 1 月生效。法国对广告商(如脸书或谷歌)、服务中间商(如优步或 Airbnb)以及数据交易平台征收年度营业额 3% 的税。这项税收将适用于大约 30 家大型跨国公司,每年可增加约 5 亿欧元的税收。^②由于苹果、脸书等数字巨头的欧洲总部位于爱尔兰,爱尔兰出于保护自身总部经济利益的考虑,对欧盟征收数字税忧心忡忡,担心其市场吸引力受到损害。除了爱尔兰,其它低税国家(地区)如卢森堡等都是亚马逊、谷歌等跨国数字企业的“避税天堂”,这极大地制约了欧盟数字税的执行力度和监管效力的发挥。

(二)“数字主权”与“自由开放的数字市场”之间的张力

欧盟强调,通过“数字主权”战略打造数字化的欧盟,以彰显欧盟开放、自由、公平和更加自信的一面,《数字市场法》等法律的出台是为了确保欧洲数字市场的公平和开放。^③但事实上,“数字主权”与“自由开放的数字市场”之间存在较大的张力。同时,欧盟在政策实践过程中注意力过分集中于规则,而弱化了对数字

^① Emmanuel Amiot et al., “European Digital Sovereignty—Syncing Values and Value,” p. 14, <https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf>.

^② Nicola Bilotta, “Beyond the Digital Tax: The Challenges of the EU’s Scramble for Technological Sovereignty”, *Istituto Affari Internazionali (IAI) Papers*, Vol. 20, 2020, p. 8.

^③ Natasha Lomas, “European Parliament Backs ‘Historic’ Reboot to EU’s Digital Rulebook,” <https://techcrunch.com/2022/07/05/dma-dsa-eu-parliament-vote/>.

技术本身的关注。

“数字主权”战略捍卫了一个封闭和重商主义版本的数字时代,与当今文化和经济发展趋势格格不入。^① 欧盟基于“数字主权”而设定的多重规则屏障与自由开放的数字市场目标相斥,如何协调自由开放的市场以免陷入保护主义和维护“数字主权”是欧盟面临的一大挑战。欧洲国际政治经济中心高级研究员马蒂亚斯·鲍尔认为,在一个价值链全球化的数字世界里,自主不能简单地意味着独立于他人。贸易限制不能代替欧盟从开放的技术和数字中获得好处。^② 因此,如何妥善解决“数字主权”与“自由开放的数字市场”之间的矛盾是欧盟面临的难题。

迄今为止,欧盟更关心的是如何成为“游戏规则制定者”,而不是成为“游戏玩家”。“数字主权”不应该成为欧盟法律适用范围、欧洲规范性权力过度扩张的理由。^③ 欧盟希望通过设定技术标准和规则,降低成员国之间由于信息和政策不对称而造成的交易成本,塑造地区乃至全球的标准和偏好,在数字领域提高影响力和话语权。然而,只靠规则设定似乎不足以实现欧盟的地缘政治野心,也无助于数字技术本身的进步以及缩小欧盟与中美的数字差距。欧盟捍卫自身在数字领域的价值和利益的最好方法就是真正从监管者转变为技术主导者,创新产品和改进技术流程等才是保持产业竞争优势的唯一办法。^④ 欧洲学者呼吁,欧盟必须通过大力对数字基础设施、数字技能和产业进行投资来补充其监管影响力,以便凭借自身实力成为“数字玩家”。

(三) 外部压力:美国的牵制与约束

从中美技术竞争基本可以延伸出以下结论:美国对既有技术霸权的维护意味着其不能接受欧盟想成为数字规则制定者与数字标准规范者的雄心,也不会

^① Luciano Floridi, “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU”, *Philosophy & Technology*, Vol. 33, 2020, pp. 374 ~ 375.

^② Matthias Bauer and Fredrik Erixon, “Europe’s Quest for Technology Sovereignty: Opportunities and Pitfalls,” p. 6, https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf.

^③ Celeste Edoardo, “Digital Sovereignty in the EU: Challenges and Future Perspectives”, in Federico Fabbrini, ed., *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford: Hart Publishing, 2021, pp. 211 ~ 228.

^④ [美]迈克尔·波特著,李明轩、邱如美译:《国家竞争优势(上)》,中信出版社2012年版,第61页。

乐见欧盟对独立于甚至是超越于美国的数字技术能力的追求。

美国数字企业在欧盟的主导地位意味着欧盟严密的监管将更多地触及美国的利益。为此,美国多措并举对欧盟进行牵制。首先,美国利用关税大棒和国际议程的设置权来对欧盟的数字议程进行替代。数字税问题一直都是横亘于欧美之间难以弥合的利益分歧点。针对欧盟数字服务税议程,美国通过单边报复性关税威胁与全球最低企业税率倡议^①成功掌握了议程设置的主导权。^② 2019 年当法国批准对在其国内市场运营的跨国数字企业征收 3% 税时,美国贸易代表办公室声称法国的数字服务税具有歧视性,其目的是惩罚特定的美国技术公司。^③ 为此,美国对自法国进口的 24 亿美元商品征收了高达 100% 的关税。2021 年 6 月,美国宣布对来自包括英国、意大利和西班牙等 6 国总价值约为 21 亿美元的商品征收 25% 的报复性关税,并且明确表示此举是作为对这些国家向脸书、谷歌等美国数字企业收取数字税的回应。特朗普曾多次强烈批评欧盟的监管激进主义,抨击欧盟的反垄断调查是在赚“快钱”。^④ 奥巴马也曾抨击欧盟对美国数字企业的政策,称这些行动是商业利益驱动的针对美国公司的技术保护主义。^⑤ 2021 年 10 月 30 日,随着由美国倡议的全球最低企业税率得到二十国集团成员国的支持并达成历史性协议,美国成功地掌握了数字税收议程的主动权。

其次,美国通过美欧联合的方式对欧盟“数字布鲁塞尔效应”形成牵制,如美欧贸易和技术委员会下设“技术标准合作”和“数据治理和技术平台”等 10 个工作小组,以期强化美欧在关键和新兴技术标准方面的协调与合作。其中“技术标准合作”工作组包含“人工智能小组”和“战略标准化信息机制”,以实现双方在

① 全球最低税率是指为了应对“数字经济的税收挑战”,即数字时代下,大型跨国公司和数字科技巨头将利润转移到低税收地区所造成的税基侵蚀和利润转移问题,各国所达成设置全球最低企业税率为 15% 的协定。参见 OECD, *Tax Incentives and the Global Minimum Corporate Tax: Reconsidering Tax Incentives after the GloBE Rules*, Paris: OECD Publishing, 2022, p. 6.

② 宫云牧:《数字时代主权概念的回归与欧盟数字治理》,《欧洲研究》2022 年第 3 期,第 46 页。

③ Office of the United States Trade Representative, “Conclusion of USTR’s Investigation Under Section 301 into France’s Digital Services Tax,” <https://ustr.gov/node/10052>.

④ Makena Kelly, “Donald Trump on Tech Antitrust, There’s Something Going On,” <https://www.theverge.com/2019/6/10/18659619>.

⑤ Murad Ahmed et al., “Obama Attacks Europe Over Technology Protectionism,” <https://www.ft.com/content/41d968d6-b5d2-11e4-b58d-00144feab7de>.

与技术 and 经济利益相关的国际标准开发方面的信息共享。^① 总之,美国以联欧的方式来弱化和牵制欧盟对数字规则主导权的塑造。

最后,美国的“数字巨头”对欧盟机构的游说在一定程度上迟滞了欧盟“数字主权”的政策实践。^② 在欧盟,数字技术领域已经成为最大的游说对象,超过了制药、化石燃料、金融或化工等其它领域。据欧盟内部监察机构报告统计,有 612 家公司、团体和商业协会就欧盟的数字经济政策对欧盟机构展开游说,每年的游说花费超过 9700 万欧元。其中,美国的企业最多,占比超过了 20%。在游说支出排名前 10 的数字企业中,除中国华为与英国沃达丰外,其余皆为美国企业,游说支出约为 2800 万欧元。自 2019 年 12 月以来,从“数字巨头”与欧盟委员会举行的会议数量来看,谷歌以 46 次会议领先,脸书和微软紧随其后,各开了 40 场会议,亚马逊以 20 场会议排名第三。^③ 这足以反映出美国的“数字巨头”对欧盟数字政策的影响之深和牵制之大。

五、结 语

面对世纪疫情的冲击和自身在数字技术领域的相对弱势地位,为了抓住数字技术发展的机遇并整合欧盟内部各成员国在数字空间的不同利益诉求,欧盟提出“数字主权”战略并以此为依托加强自身在数字空间领域的规范性力量,提升欧盟在数字技术能力和欧盟整体价值观的影响力,寻求获得技术带来的经济 and 地缘政治方面的利益,塑造一条具有欧盟特色的数字发展之路。欧盟作为当前全球数字版图中的重要组成部分,“数字主权”战略无疑会对今天及未来数字空间领域的格局有重要影响。欧盟“数字主权”战略深刻地揭示了数字技术与地缘政治因素的相互交织,数字空间成为了一个新的地缘政治博弈空间。谁拥有

① The White House, “U. S. -EU Joint Statement of the Trade and Technology Council,” <https://www.whitehouse.gov/wp-content/uploads/2022/05/TTC-US-text-Final-May-14.pdf>.

② 官云牧:《数字时代主权概念的回归与欧盟数字治理》,《欧洲研究》2022 年第 3 期,第 45 页。

③ Max Bank et al., “The Lobby Network: Big Tech’s Web of Influence in the EU,” pp. 4 ~ 14, <https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu>.

未来的数字技术、谁制定技术标准已经成为地缘政治竞争的重要内容。

“数字主权”战略代表了欧盟对自身国际角色的新定位,反映了欧盟谋求成为全球数字版图中的战略参与者与“角斗士”的愿景,以更加积极、更加自主的姿态来参与数字地缘竞争与博弈。也正是这种愈演愈烈的数字地缘博弈,使得当前的全球数字治理格局并没有呈现出明显的“网络化”和“互动性”特征,而是在非对称竞争中呈现霸权性,全球数字治理各行为体呈现“权力流散”态势。^① 中美欧作为当前数字地缘版图中的战略大三角,如何进行包容性竞争,如何以多边力量共同推动全球数字技术发展与维护数字空间秩序,是全球数字治理面临的新课题。全球数字治理作为数字时代特有的新产物,涉及多主体、多层次、多方面的问题,因此需要在未来持续、深入、系统地展开研究。总之,数字空间不应是地缘政治博弈的新策源地,而应该是充分发挥大国之间相互尊重、合作共赢的新舞台。

^① 蔡翠红:《数字治理的概念辨析与善治逻辑》,《中国社会科学报》2022 年 10 月 13 日,第 5 版。