大国竞争背景下欧盟数字主权的复合构建

——一种技术政治解读

张若扬　蔡翠红

内容提要:在大国竞争与技术焦虑驱动下,欧盟正将其“战略自主”抱负转化为具体的社会技术实践以构建数字主权。本文基于技术政治学视角,构建了一个以“战略自主”为元目标,涵盖规则、基础设施和身份维度的复合框架,通过比较 Gaia-X、数据法案及欧洲数字身份钱包等案例,发现欧盟的数字主权构建呈现出显著的非对称性与务实性。在规则维度,欧盟从市场规训向安全防御进行逻辑跨越,对美侧重柔性规训,对华则强化排他性防御;在基础设施维度,欧盟采取“增量建设”与“存量清理”并行的策略,在夺回数据和算力掌控权的同时,倾向于强制剥离高风险供应链;在身份维度,欧盟通过将欧洲价值观“编码”进技术架构,来划定数字共同体的信任边界。综上,欧盟数字主权的本质是通过将政治意志代码化和物质化,试图在深度依赖中强行开辟出受控的自主空间。三个维度相互交织,共同构成“对美规训、对华防御”差异化策略下的复合数字主权构建体系。

关键词:大国竞争　欧盟　数字主权　技术政治

一　问题的提出

21 世纪的地缘政治博弈,正在一个由数据、算法和云基础设施构成的数字空间中展开。面对美国巨头的技术垄断、中国产业链的快速追赶和自身数字经济竞争乏力的问题,在大国技术竞争加剧的背景下,欧盟发布了一系列战略文件,旗帜

鲜明地提出要追求数字领域的主权权利,以捍卫其“战略自主”、价值观和经济竞争力。近年来,欧盟在官方层面陆续提出“技术主权”(Technology Sovereignty)①、“数字主权”(Digital Sovereignty)②和“数据主权”(Data Sovereignty)③等概念,随着一系列政策和法律文件的出台,“数字主权”已经从一个单纯的学术话语、模糊的政治口号演变为欧盟在数字发展领域具体的战略议程。然而,一个核心的理论与实践难题随之而来:一个超国家政治实体,如何将这种宏大而抽象的地缘政治抱负,转化为可操作、可治理、可感知的社会技术现实?

本文的“数字主权”概念,特指欧盟在中美数字技术竞争的背景下,为追求“战略自主”而采取的一系列旨在降低关键性外部依赖、提升数字竞争力和规则影响力的社会技术实践。为洞悉这一具象化过程,本文引入技术政治学的理论视角。该视角强调技术与政治之间深刻的共生建构关系,将分析的焦点从布鲁塞尔的政策制定办公室转向“欧洲 Gaia-X 联邦式数据基础设施项目”(Gaia-X: A Federated Data Infrastructure for Europe,以下简称“Gaia-X”)的架构图、“欧盟高性能计算联合体项目”(European High Performance Computing Joint Undertaking,以下简称“EuroHPC”)的算力节点和“欧洲数字身份钱包”(European Digital Identity Wallet,以下简称“EUDI 钱包”)的代码库等具体的社会技术实践上。基于此,本文旨在提出并回答一个核心研究问题:在大国竞争背景下,欧盟在数字领域如何通过具体的社会技术和法律实践应对来自中美的竞争压力并寻求“战略自主”?面对不同的竞争压力,欧盟的技术政治实践采取了怎样的差异化策略?本文将以欧盟数据法案系列、外商直接投资审查框架、Gaia-X、EuroHPC 等为分析案例,力图通过技

① Ursula von der Leyen, “A Union That Strives for More: My Agenda for Europe,” European Commission, July 14, 2019, https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf.

② Tambiama André Madiega, “Digital Sovereignty for Europe,” European Parliament, July 2, 2020, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651992.

③ “Summary Report of the Public Consultation on the European Strategy for Data,” European Commission, July 24, 2020, https://digital-strategy.ec.europa.eu/en/summary-report-public-consultation-european-strategy-data.

术政治学的剖析,为理解大国战略竞争时代欧盟数字主权的复合构建提供一个批判性的分析框架。

二 理论框架:“战略自主”驱动下的数字主权复合构建

当前数字主权的研究正面临一种深刻的张力:宏观地缘政治的动力叙事与微观社会技术的建构过程之间存在显著的解释断层。为弥合这一理论裂隙,本文首先审视既有理论工具的解释边界与盲区,进而论证“战略自主”对于欧盟而言远非背景板式的口号,而是一个能够深刻重塑技术政治过程的核心变量。以此为基础,本文构建了一个全新的分析框架,旨在揭示欧盟如何通过规则、基础设施与身份三个维度的复合性策略,在主权诉求与依赖现实之间进行持续的战略校准。

(一)既有理论的视角及其局限

既有研究为理解数字主权提供了丰富的视角,分别从国际体系、国内或区域治理和社会技术网络的层次切入,根据其核心分析焦点,大致可分为三条泾渭分明的学术脉络。第一类研究聚焦体系层次,这一脉络根植于国际关系理论,将数字主权置于地缘政治博弈的宏观框架下审视,研究的是作为大国竞争与规范性权力的数字主权。学者或从现实主义出发,强调数字技术已成为国家核心权力要素,主权的核心在于对关键基础设施和数据的排他性控制,以防止战略依赖;①或从自由主义的视角出发,聚焦于通过国际制度和规则塑造来确立数字主权,②欧洲的“规范性权力”范式常常被引为例证,认为其通过《一般数据保护条例》(General Data Protection Regulation,GDPR)等法规对外输出规则,从而行使一种独特的“规

① Joseph Nye, “Cyber Power,” Harvard Kennedy School, May 2010, pp.3-4, https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf; Henry Farrell and Abraham L. Newman, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion,” *International Security*, Vol.44, No.1, 2019, pp.42-79.

② Rocco Bellanova, Helena Carrapico and Denis Duez, “Digital Sovereignty and European Security Integration: An Introduction,” *European Security*, Vol.31, No.3, 2022, pp.337-355.

范性主权”。[①] 这一层次的研究有力解释了数字主权兴起的外部动力和战略意图，并将其置于大国战略竞争的背景下，但其分析往往限于政策宣言与法律文本，将主权视为一个待实现的、整体的政治目标，却相对忽视了其实践过程本身的政治性，未能深入“主权是如何被具体建构”的内部过程“黑箱”。[②]

第二类研究聚焦治理层次，这一脉络把目光投向国家或超国家实体内部，关注如何通过立法、行政和司法手段来确立和行使数字领域的主权，将数字主权视为一种法律和监管秩序。研究集中于数据本地化立法、平台反垄断、网络安全审查、数字税等具体的政策工具。[③] 大量文献详述了欧盟数字单一市场战略下的法律体系，如 GDPR、《数字市场法》(Digital Markets Act)、《数字服务法》(Digital Services Act)等，分析其如何试图对内统一规则、对外设置壁垒。[④] 这一路径细致描绘了主权的制度框架和规制工具箱，但它通常预设了主权主体统一的意志和执行能力，相对忽视了法律文本和政策战略在转化为可治理、可操作的社会技术的现实过程中，所遭遇的复杂的技术约束和利益博弈。

第三类研究聚焦网络层次，这一脉络主要源于“科学技术研究”(Science and Technology Studies，STS)和技术政治学，它拒绝将技术视为中性的工具，转而探究主权如何通过具体的技术设计、基础设施部署和日常实践被“制造”出来，将数字

---

① Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020; 闫广、忻华：《中美欧竞争背景下的欧盟“数字主权”战略研究》，载《国际关系研究》，2023 年第 3 期，第 62-86 页；叶开儒：《数据跨境流动规制中的“长臂管辖”——对欧盟 GDPR 的原旨主义考察》，载《法学评论》，2020 年第 1 期，第 106-117 页。

② Jeanette Hofmann et al., “Between Coordination and Regulation: Finding the Governance in Internet Governance,” *New Media & Society*, Vol.19, No.9, 2017, pp.1406-1423.

③ Dan Svantesson, “Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines,” *OECD Digital Economy Papers*, December 22, 2020, https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/12/data-localisation-trends-and-challenges_d775fe8a/7fbaed62-en.pdf; Rogier Creemers, “China's Emerging Data Protection Framework,” *Journal of Cybersecurity*, Vol.8, No.1, 2022, pp.1-12.

④ Pierre Larouche and Alexandre de Streel, “The European Digital Markets Act: A Revolution Grounded on Traditions,” *Journal of European Competition Law & Practice*, Vol.12, No.7, 2021, pp.542-560; 郑春荣、金欣：《欧盟数字主权建设的背景、路径与挑战》，载《当代世界与社会主义》，2022 年第 2 期，第 151-159 页；陈菲、蒲文杰：《〈数字市场法〉：欧盟规制数字“守门人”的制度路径》，载《欧洲研究》，2024 年第 1 期，第 23-56 页。

主权视为一种社会技术建构。技术政治学并非一个单独的理论学派,而是一种跨学科的研究视角。其核心观点是,技术和政治是相互建构、深度交织的“共生体”,技术从设计之初就包含了特定的政治偏好,其本身具有重要的政治意涵。① 研究揭示了计算中心的地理政治②、互联网协议的标准之争③和数字身份系统的社会塑造如何影响权力关系。④ 这一视角提供了打开主权“黑箱”的精密仪器,擅长分析权力如何被“编码”进架构和标准。然而,其分析视角多聚焦于国内或跨国的社会技术网络的内部协商,却相对淡化了“大国间的战略竞争”此类至关重要的、结构性的外部变量。欧盟不是在真空中从无到有地构建自己的数字主权,而是在对外部数字技术存在全栈式深度依赖的背景下,为维护其“战略自主”而启动一场系统性、防御性的数字主权构建运动。

综上可见,当前对欧盟数字主权的研究存在宏观论述和微观过程之间的理论断层,体系与治理层次的研究揭示了数字主权的宏观政治动力和法律建构,技术政治学提供了观察内部主权构建的技术显微镜,但少有研究将二者连接起来,以解释战略压力如何具体地、差异化地影响和塑造欧盟内部的社会技术建构过程。为此,本文试图进行一种理论整合,将大国竞争的战略情境引入技术政治学的分析过程,构建一个战略情境下的技术政治分析视角,以理解大国博弈背景下欧盟数字主权的复合构建。

(二)分析框架:以“战略自主”为元目标的三维构建策略

在数字产业和数字经济领域,欧盟目前处于一种被美国和中国“双重挤压”的态势。美国对欧盟的竞争压力主要集中在数字经济的顶层逻辑和底层基础设施之上:欧盟的数字命脉高度依赖美国的云基础设施,这导致其在“数据主权”上感到严重焦虑;美国全球领先的社交媒体、搜索引擎和操作系统控制了流量入口和

① Langdon Winner, “Do Artifacts Have Politics?” *Daedalus*, Vol.109, No.1, 1980, pp.121-136.

② Jukka Ruohonen, “Geospatial Insights on the EuroHPC Supercomputing Ecosystem,” *Digital Society*, Vol.4, No.2, 2025, pp.1-11.

③ Laura DeNardis, *The Global War for Internet Governance*, Yale University Press, 2014.

④ Silvia Masiero and Savita Bailur, “Digital Identity for Development: The Quest for Justice and a Research Agenda,” *Information Technology for Development*, Vol.27, No.1, 2021, pp.1-12.

数字市场的规则,通过平台经济和“守门人效应”垄断了欧盟的数字生态;美国在人工智能(Artificial Intelligence, AI)原始创新和算力上具有压倒性的优势,对欧盟而言,这意味着如果跟不上美国的节奏,其整个数字经济未来将被迫建立在美国的技术“黑箱”之上。相较之下,中国对欧盟的竞争压力则更多地体现在数字化应用、基础设施硬件和对传统优势工业的冲击之上:中国利用数字应用与先进制造融合方面的产业优势,在电动汽车、电池技术和智能制造领域实现了“换道超车”,中国不仅卖硬件,还卖整套数字化解决方案,这直接威胁到了欧盟的支柱产业;中国在通信基站和网络硬件上的高性价比,让欧盟在安全考量与建设成本之间陷入两难;此外,从 TikTok 到 Temu、Shein,中国数字企业在移动互联网应用层、算法推荐和跨境电商物流链条上的极高效率,正在重塑欧洲的消费市场,给欧洲本土零售和媒体产业带来巨大冲击。

在此背景下,“战略自主”这一诉求成为欧盟在数字领域应对竞争压力、加强主权建设的直接动力。因此,理解欧盟的数字主权实践,必须将“战略自主”这一地缘政治元目标确立为贯穿多层次分析的核心线索。它并非静态背景,而是一种能动的元规则,既定义了政治目标,又规制了立法议程,更直接介入了技术权衡。基于此,本文旨在融合上述多层次视角,提出一个新的、整合性的分析框架,将欧盟的数字主权实践理解为:在“战略自主”目标的驱动下,在规则、基础设施与身份三个关键社会技术场域展开的一场充满张力与妥协的、差异化的复合构建。

首先,规则维度是欧盟构建数字主权的总纲和蓝图。莱斯格(Lawrence Lessig)提出了“代码即法律”的著名论断,他认为技术标准和协议构成网络空间的“隐性宪法”,它们通过看似中立、理性的代码和规则,为网络空间划定了边界、设定了行为规范。① 德纳迪斯(Laura DeNardis)进一步论证,互联网治理的核心已演变为对技术规则和标准的争夺,这已成为地缘政治的新前沿。② 在数字时代,数字规则包括了数字领域相关的法律、法规和标准,它们为数字空间划定了具体的行

① [美]劳伦斯·莱斯格:《代码 2.0:网络空间中的法律》,李旭、沈伟伟译,清华大学出版社 2018 年版,第 6 页。

② Laura DeNardis, *The Global War for Internet Governance*, pp.1-33.

为边界和运行逻辑。其次,基础设施维度是欧盟构建数字主权的物理载体。技术政治学认为,权力不仅存在于政策文本的辩论中,更沉淀在技术架构的选型与算法的约束逻辑中。基础设施远非中性的技术平台,其物理部署、所有权结构和技术架构内嵌了治理模式、权力意志和文化价值观。① 爱德华兹(Paul N. Edwards)揭示了计算机技术如何内化了冷战时期的军事命令和控制逻辑。② 阿巴特(Janet Abbate)论证了早期互联网阿帕网(ARPANET)的技术架构如何反映了当时美国学术共同体的文化价值观。③ 在数字时代,数字基础设施在物理层包括数据中心、光纤电缆和超级计算机等,它们的地理分布和所有权结构是主权诉求的直接体现;在逻辑层或平台层则包括云服务平台、数据空间和操作系统等,它们的技术架构、接口标准和数据存储位置都包含了特定的治理理念。最后,身份维度是构建数字主权的认同边界和逻辑终点。从历史视角看,现代国家主权的行使与公民认同的塑造离不开诸如测绘、统计和身份认证等技术的支撑。④ 赫克特(Gabrielle Hecht)提出了"技术政治"(Technopolitics)的概念,她将其定义为"设计或使用技术来构成、体现或制定政治目标的战略实践",并以法国核技术发展为例,揭示了国家如何通过重大技术项目来重塑国家认同。⑤ 在数字时代,技术不仅是权力工具,更是政治共同体认同的物质载体,身份认证系统定义了"谁可以进入"以及"以何种身份进入"数字空间,是构建数字空间政治共同体的基础。

在此基础上,本文构建了一个以"战略自主"为核心目标,涵盖规则、基础设施与身份三个核心维度的技术政治学分析框架,旨在揭示欧盟在面对美中不同竞争压力时采取的非对称性实践路径。

---

① Susan Leigh Star, ed., *The Cultures of Computing*, Basil Blackwell, 1995.

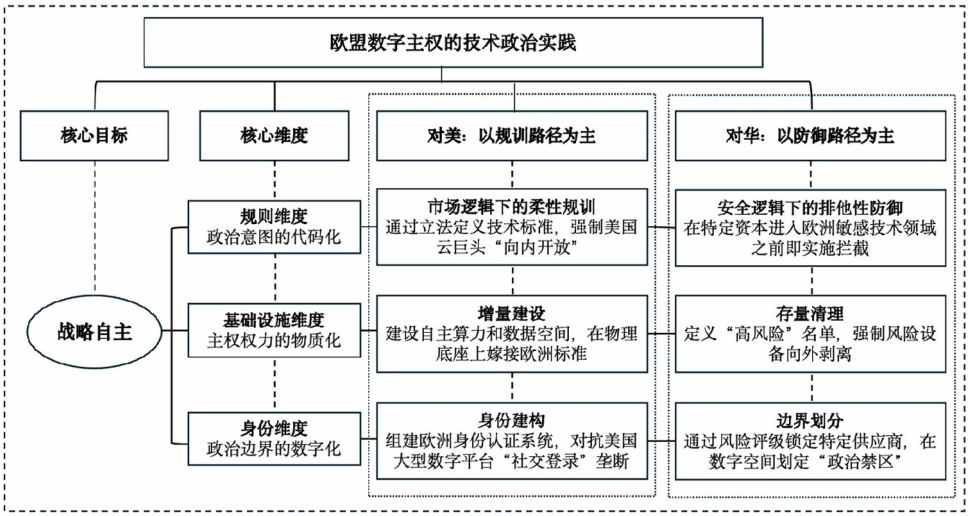
② Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*, The MIT Press, 1996.

③ Janet Abbate, *Inventing the Internet*, The MIT Press, 1999.

④ [美]詹姆斯·C. 斯科特:《国家的视角:那些试图改善人类状况的项目是如何失败的》,王晓毅译,社会科学文献出版社 2017 年版。

⑤ Gabrielle Hecht, *The Radiance of France: Nuclear Power and National Identity after World War II*, The MIT Press, 2009, p.15.

图 1 “战略自主”目标驱动下欧盟数字主权的技术政治实践



注:图由作者自制。

在规则维度,欧盟通过政治意图的代码化,实现了从内部合规向全球杠杆的“转译”。针对美中不同的压力源,欧盟采取了非对称的规则逻辑。针对美国,欧盟主要采取了基于市场治理逻辑的“规训路径”,面对美国平台的生态垄断,欧盟通过一系列法律规则进行“立法造市”,强制美资云巨头“向内开放”,来实现数据的互操作性,这不仅可以缓解数据受制于人的压力,还可以通过“布鲁塞尔效应”将欧洲标准转化为全球标准,赋予欧洲企业在公平规则下竞争的权利,从而缓解其在数字治理中沦为“二等公民”的规则焦虑。针对中国,欧盟则主要采取了基于安全逻辑的“防御路径”,通过外商直接投资审查框架等法律围栏建立硬性准入标准,从而实现对华技术投资的识别与隔离。

在基础设施维度,欧盟通过推动“主权权力的物质化”来构建可控的技术底座。一方面,通过 Gaia-X 和 EuroHPC 进行“增量建设”,以应对美中在云端和算力上的双重挤压。“增量建设”直接提供数字经济的燃料与引擎,在物理底座上“嫁接”欧洲标准,以对冲美式垄断,并且确保欧洲在 AI 与工业 4.0 时代的研发不因缺乏算力而停滞,从而增强实质性的数字竞争力。另一方面,针对关键领域试

图实施“存量清理”,即通过在物理层面剥离高风险设备,来纾解对底层设施被干预或切断的生存担忧,从而缓解深度依赖带来的安全焦虑、确保硬件基座的政治安全性,并通过提升底座的韧性构筑实质性的技术竞争壁垒。

在身份维度,欧盟试图通过“政治边界的数字化”来重塑数字空间的信任根基。通过建设 EUDI 钱包,对抗美国平台的“社交登录”垄断,重建公共信任;通过风险评级锁定特定供应商,在数字空间划定政治禁区,明确界定数字共同体的敌我边界。这种“数字围栏”的建构,不仅通过重建公共信任缓解了社会对隐私丧失的焦虑,更重要的是,欧盟希望通过统一身份标准来“缝合”碎片化的成员国市场,期望这种身份联邦化所产生的规模效应将欧洲转化为一个具备竞争潜力的统一数字单一市场,从而在根本上缓解欧盟面对美中巨头规模竞争力的焦虑。综上所述,这三个维度相互交织、动态互动,共同构成欧盟“对美规训、对华防御”的复合数字主权体系。

本文将从“欧盟如何在战略自主目标驱动下,在规则、基础设施、身份三个维度开展差异化的复合主权构建”这一核心问题出发,在每一个案例分析中,首先明确其面对的具体的外部竞争压力,其次分析欧盟为此设定了怎样的自主目标,再次论述其在对应维度采取何种差异化策略进行构建,最后剖析在这一过程中暴露出的核心张力。本文目的是为欧盟数字主权研究提供一个将宏观地缘政治动力与微观社会技术建构过程相结合的整合性分析框架,从而更全面、更动态地理解数字时代主权的复杂实践。

三 规则维度的主权构建:从柔性规训到排他性防御

欧盟的数字主权,首先是一场以法律为战场、以规则为武器的制度性权力争夺。在规则维度上,欧盟的数字主权实践并非遵循单一逻辑,而是针对不同威胁来源演化出两套并行且截然不同的治理范式。本文通过分析这两套法律实践,揭示欧盟数字主权在规则维度的双重面向及其内在张力。

(一)市场逻辑下的柔性规训:《数据法案》和《数据治理法案》

欧洲发达的数字市场创造了丰富的数据资源,但并未及时转化为欧洲在数字

竞争中的优势。尽管 GDPR 等法律在隐私保护层面实现了统一,但共同信任框架的缺乏和成员国在具体操作层面的规则不一阻碍了欧洲整体的数据流动,影响泛欧数据空间的形成,欧洲单一数字市场的愿景难以实现。欧盟意识到,单靠 GDPR 的“隐私保护”范式已经不足以赢得竞争,必须通过强制性共享释放欧洲的数据潜力,《欧洲数据战略》(A European Strategy for Data)明确指出,“目前少数大科技公司拥有世界上大部分数据”,导致欧洲企业缺乏竞争公平性,而“中国和美国等竞争对手正在全球范围内推广他们的数据访问和使用理念”。① 在此背景下,为维护欧盟的“数据主权”,2020 年,欧盟的法律体系建设进入“数据战略阶段”,即欧盟开始制定数据战略并依此构建全面的数据治理法律体系。② 2020 年 11 月,欧盟委员会通过了《数据治理法案》(Data Governance Act,DGA)的提案,确定了一系列增加数据共享信任度的机制,旨在消除各部门与成员国之间因缺乏信任所产生的数据共享壁垒。③ 2023 年 12 月,欧盟理事会批准了《数据法案》(Data Act),④该法案于 2024 年 1 月 11 日正式生效,⑤并于 2025 年 9 月正式实施。⑥ 作为《欧洲数据战略》中的一项关键立法措施,《数据法案》是对《数据治理法案》和 GDPR 的重要补

① “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data,” European Commission, February 19, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

② 林梓瀚:《基于数据治理的欧盟法律体系建构研究》,载《信息安全研究》,2021 年第 4 期,第 337 页。

③ “Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act),” European Commission, November 25, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020PC0767.

④ “Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance),” European Commission, December 22, 2023, https://eur-lex.europa.eu/eli/reg/2023/2854/oj.

⑤ “European Data Act Enters into Force, Putting in Place New Rules for a Fair and Innovative Data Economy,” European Commission, January 11, 2024, https://digital-strategy.ec.europa.eu/en/news/european-data-act-enters-force-putting-place-new-rules-fair-and-innovative-data-economy.

⑥ “EU Data Act Gives Users Control over Data from Connected Devices,” European Commission, September 12, 2025, https://digital-strategy.ec.europa.eu/en/news/eu-data-act-gives-users-control-over-data-connected-devices.

充,旨在推动更多数据在符合欧盟规则和价值观的前提下流动和利用,以此构建欧洲单一数据市场。

《数据治理法案》与《数据法案》构成欧盟利用其单一市场规模,主动塑造全球数字游戏规则的“法律组合拳”,旨在通过强制性立法,在破除内部数据流动壁垒的同时,迫使依赖欧洲市场的美中科技企业遵守一套体现欧洲价值观的数据流动与竞争规则,以此行使一种不对称的“规则性权力”,实现对技术依赖的战略再平衡。其中,《数据治理法案》侧重于构建信任基础和激活非市场数据流,它并非直接规制科技巨头,而是“厚植”欧洲数据经济的“土壤”。它有三个核心机制:一是公共部门数据的再利用机制。该机制对数据进行分类,并为敏感公共部门数据的安全再利用建立了统一的规则,允许企业和研究机构在保护隐私和商业利益的前提下,将数据应用于 AI 训练等创新活动;二是数据利他主义机制。该机制通过建立官方认可的“利他主义”组织资质认证体系和标准化流程,鼓励个人和企业为了科研、环保等公众利益自愿分享数据;三是数据中介服务机制。该机制对提供数据共享服务的中介机构提出了中立性和透明度的要求,使之成为可信的数据交换“守门人”。这三大机制的目的是系统性激活欧盟内部被锁闭的数据资源,特别是公共部门和公益领域的数据,从而为欧洲本土的 AI 创新培育一个受欧洲规则保护、相对安全可控的数据训练池,降低对外部数据的依赖。同时,通过确立“数据利他主义”等概念输出欧洲在数据伦理上的话语权,与美中的数据治理模式进行竞争。

与之形成互补的是,《数据法案》更侧重于破除垄断和重塑 B2B(Business-to-Business)数据关系,是一部更具进攻性的法律,它针对的是美中数字企业在欧洲市场的主导模式,直接瞄准了美中企业主导的物联网设备制造商和以美国企业为主的超大型云服务商的“数据垄断”和“用户锁定”。它同样包含三个核心机制。其一是开放物联网数据访问权的机制,此举主要针对美国的物联网和硬件制造商、中国的智能设备厂商,以及依赖平台数据的美国互联网巨头们。《数据法案》强制联网设备的制造商向其用户共享设备所产生的数据,并规定用户有权将这些数据提供给第三方(通常是欧洲中小服务商)。这一规定延续和强化了 GDPR 所规定的“数据可携带权”,对美国而言,旨在打破其“硬件—服务—数据”的一体化

闭环。例如,该规定迫使特斯拉向第三方维修商开放车辆诊断数据,打破其售后垄断;要求苹果健康数据可以被欧洲医疗科技公司使用。对中国而言,该规定则是为了防范其通过 IoT 传感器此类智能设备大规模采集欧洲数据并回传分析的风险。同时,法律并不直接禁止,而是要求企业必须开发并开放标准化的、安全的实时数据应用程序编程接口(Application Programming Interface,API)。这迫使企业必须投入高额成本改造产品架构,并接受其数据接口按欧盟标准被审计和认证,本质上是将企业的私有数据协议改造为符合欧洲公共技术标准的"数据通道"。此举旨在打破美中设备制造商的数据闭环,为欧洲中小型服务商创造进入市场的机会,扶植本土数字产业。

其二是云服务切换保障机制,《数据法案》力图为用户切换云服务提供商消除合同壁垒、技术障碍和降低费用门槛,包括取消不合理的最低合同期限或自动续约条款、解决数据格式不兼容的问题、明确要求云服务商向用户公开披露与切换相关的所有费用构成,并计划逐步取消切换费等。这一机制主要针对美国的超大规模云提供商,其直接战略意图是降低欧盟政府和企业从美国云迁出的经济成本和技术障碍,为 Gaia-X 等欧洲主导的互操作生态扫清法律障碍。法律的要求被转化为"合规性证明"负担,云服务商必须在技术架构上实现数据与元数据的标准化导出,其管理平台必须集成并公开"切换功能模块",且该模块的性能将成为合规审计的一部分,这意味着将强制美国云巨头为自己的客户开发一套将数据迁移到竞争对手的工具,并将其服务质量置于欧洲监管机构的持续监管之下。2025 年 11 月,欧盟《数字综合监管提案》(Digital Omnibus Regulation Proposal)提出,给予中小企业和中型上市公司云服务切换规则的定向豁免,[①]这一机制精准锁定美国

① "Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)—Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)," European Commission, November 19, 2025, https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

超大规模云服务商,监管靶向性愈发显著。

其三是互操作性要求机制,《数据法案》希望推动欧盟内部数据处理服务之间的互操作性,包括鼓励云服务商采纳共同标准和接口等,以实现不同服务之间更顺畅的连接和交换数据。此举同时针对拥有主导地位的美国操作系统和软件平台,以及潜在形成生态垄断的中国应用平台,目的是在操作系统层面为欧洲开源或为小众软件创造公平竞争环境,在应用层面削弱美国社交平台因网络效应形成的垄断,并防范中国的超级应用和平台通过封闭生态在欧洲获得市场支配地位。欧盟通过授权或指定欧洲的标准化组织制定具体的互操作性技术细则,这意味着非欧盟企业若想进入欧洲市场就必须在产品设计阶段植入这些欧洲标准。欧盟的法规文本,实际上化身为一份强制性的技术设计规范书,试图深度介入全球产品的技术路线图。

表 1 《数据法案》对科技巨头与欧洲中小企业的影响及其核心机制

《数据法案》的核心机制	法律要求的技术转化	对科技巨头(主要是非欧盟企业)的预期影响	对欧洲中小企业的预期影响
开放物联网数据访问权	要求企业必须开发并开放标准化的、安全的实时数据 API	迫使企业投入高额成本改造产品架构,接受其数据接口按欧洲标准被审计和认证	经用户许可后可以获得大设备制造商生成的海量数据
云服务切换保障	“合规性证明”要求	为自己的客户开发一套将数据迁移到竞争对手的工具,并将其服务质量置于欧洲监管机构的持续监管之下	降低了数据迁移成本
互操作性要求	通过授权或指定欧洲标准化组织(如欧洲电信标准化协会,ETSI)制定具体的互操作性技术细则	想进入欧洲市场,就必须在产品设计阶段植入这些欧洲标准	开源或小众软件获得相对公平的竞争环境

注:表由作者自制。

《数据法案》系列是欧盟以规则制衡技术、寻求“规则性主权”的典型实践,即欧盟在无法于物联网硬件和云基础设施上立即替代美中产品的前提下,试图通过法律强制力穿透技术产品的外壳,以夺取其内部数据资产的控制权和再分配权。这种以规则“造市”的实践诠释了政治和法律如何主动地、前瞻性地塑造技术市场的架构和生态。通过这种立法组合拳,欧盟试图主动设定数据市场的基本运行逻辑,并将其主权意志通过法律形式嵌入未来数字经济的根基当中,通过法律强制力塑造一个符合欧洲愿景的数据市场。

(二)安全逻辑下的排他性防御:外商直接投资审查框架及其修订

在欧盟数字主权的规则版图中,法律不仅是调节市场的技术杠杆,更是地缘政治意志“代码化”的实践工具。在对华政策逻辑中,这一特征呈现出从“市场规训”向“安全防御”的显著转向。与主要针对美国平台权力的规训逻辑不同,欧盟对华技术投资奉行的是基于安全考量的排他性防御策略。这一逻辑转型在《欧洲经济安全战略》(European Economic Security Strategy)中得到了系统阐述,该战略确立了“去风险”(De-risking)而非“脱钩”的政策基调,并强调须严防由于外国投资导致的敏感技术流失。① 在此背景下,2020 年建立并在 2024 年开启制度升级的外商直接投资审查框架,已演变为一种前瞻性的、边界性的主权防御机制。其本质是在资本进入敏感领域前筑起规则堤坝,以缓解其深层的竞争力焦虑——防止竞争对手利用欧洲市场的开放性,通过资本渗透实现技术高地的“换道超车”。

一方面,欧盟外商直接投资审查框架及其 2024 年的修订,反映了欧盟对华威胁认知的变化。自 2019 年以来,欧盟陆续通过了《欧盟外商直接投资审查框架条例》(Establishing A Framework for the Screening of Foreign Direct Investments into the Union)及一系列配套文件,构建起欧盟首个统一的外资审查框架,其话语体系仍以经济竞争中立为外壳,强调公共秩序与安全,审查标准聚焦于“是否为外国政府所有或受其控制”。② 中国虽未被点名,但“国有企业”“国家补贴”等描述已构成隐晦指认。

① “An EU Approach to Enhance Economic Security,” European Commission, June 20, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3358.

② “Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 Establishing A Framework for the Screening of Foreign Direct Investments into the Union,” European Commission, March 21, 2019, https://eur-lex.europa.eu/eli/reg/2019/452/oj.

在此基础上,该框架2024年的修订提案,将威胁认知从“竞争扭曲”升级为“技术安全”。修订案明确将审查范围扩展至绿地投资,并强化了对关键技术、关键基础设施、敏感数据的审查门槛。① 这反映了近年来欧盟对华威胁认知的变化:中国投资不再被界定为需要监管的市场行为,而是被重构为需要防御的安全威胁。这一认知重构,为后续审查标准的泛化与裁量权的扩张提供了合法性基础。

另一方面,法案的修订反映了欧盟治理模式的深层强化。从2019年《欧盟外商直接投资审查框架条例》的出台到2024年修订提案的稳步推进,以及后续相关的战略升级,欧盟外资审查制度正经历从“软协调”向“强干预”的范式变化。首先,这一变化体现为法律强制性的提升。2019年,该框架侧重于成员国间的自愿协作与信息交换,而2024年的提案则显著强化了欧盟委员会的规则引导权,要求成员国在立法标准上强制趋同,使审查逻辑从分散的国家裁量向布鲁塞尔定义的统一安全标准对标,并强制要求所有成员国必须建立、维护并强化其外资审查机制。其次,这一范式变化体现在适用范围的全口径覆盖之上。修订提案明确将绿地投资纳入审查范畴,使尚未形成交易结构的资本布局亦须接受合规评估,审查权边界由“存量控制权转移”前移至“增量投资意图”。最后,范式的变化还体现为审查标准从模糊宣示转向精准锚定。以“公共秩序与安全”为核心的抽象条款被细化为对关键技术、关键基础设施及敏感数据安全的结构化审视。这一变革的核心逻辑在于,欧盟正试图将地缘政治意志“编码”为“去政治化”的法律程序,通过在资本进入敏感技术领域之前构筑起一道动态可调、深度穿透的制度性边界,在制度实践中实现对特定地缘政治风险的识别与隔离。

2024年1月提出的《欧盟外商直接投资审查条例》修订草案已于2025年12月达成政治协议,并于2026年2月24日获得欧洲议会相关委员会通过。② 目前,

---

① “Proposal for a Regulation of the European Parliament and of the Council on the Screening of Foreign Investments in the Union and Repealing Regulation (EU) 2019/452 of the European Parliament and of the Council,” COM/2024/23 final, European Commission, January 24, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024PC0023.

② “Revision of the FDI Screening Regulation,” European Parliament, February 24, 2026, https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-revision-of-the-fdi-screening-regulation.

该修订案正处于正式批准前的最后阶段,预计将于 2026 年上半年正式颁布。外商直接投资审查框架及其修订提案,是欧盟规则主权在资本维度上的物质化体现。它通过法律审查程序,在资本进入欧洲敏感技术领域之前筑起一道制度性边界。与物理边界不同,这道边界是可调节、可裁量、可溯及的,可以根据威胁认知的变化随时收紧,也可以根据经济需求的变化适度放松。但由于欧盟在技术领域吸引投资的需求和安全诉求之间的冲突,这一规则本身也存在不稳定性与争议性。一方面是成员国之间的利益分化,德国、法国等传统引资大国对过度审查可能吓退外资保持警惕。2024 年修订提案草案在成员国谈判中遭遇阻力,正是这一张力的直接反映。另一方面是替代供给的可行性问题,欧盟之所以敢于收紧对华资本准入,前提是在关键技术与创新融资领域,它仍可依赖美日盟友及内部市场资本。但这种替代并非无限供给,过度审查可能伤及欧洲自身创新生态。

将外商直接投资审查框架的演进脉络与《数据法案》《数据治理法案》对比可以发现,欧盟在面对美国与中国不同的数字竞争压力时,分别动用了两套不同的规则工具箱。面对 AWS、Azure、Google Cloud 等美国云巨头,欧盟的选择是柔性规训:不寻求将美国云巨头从欧洲市场排除,而是通过强制性互操作、数据可携、公平竞争条款,将其纳入欧洲规则体系,在承认依赖的前提下行使规则主导权。而面对中国对欧在 5G、半导体、人工智能、新能源等敏感领域的技术投资,欧盟的选择是排他性防御:通过审查门槛下沉、适用范围扩张、权力向上集中,在资本进入欧洲敏感技术领域之前筑起制度性边界。综上,对美规则工具箱通过规则将外部力量内化为合规参与者,是一种连接性主权;对中规则工具箱通过审查将特定资本外化于技术边界之外,是一种壁垒性主权。二者不仅是价值选择的分野,也是结构性约束下的策略分化。

四 基础设施维度的主权构建:建设与“清理”并行

数字基础设施是欧盟数字主权从制度理念转化为现实能力的关键媒介,负责将法律文本和战略文件赋予的抽象权能,转化为可运行、可感知、可倚仗的物质性力量。在数据存储与处理领域,美国云巨头的服务器承载着半数以上的欧洲数字

服务;在通信网络领域,中国设备商在过去十余年间深度参与了欧盟成员国 5G 基础设施的规划与部署。欧盟委员会经评估发现,在处理器、网络平台和云基础设施等关键技术领域,欧洲企业的地位远远低于欧盟在全球经济中的权重。① 对这种非对称依赖的深度焦虑让欧委会意识到,基础设施并非中立,而是数字经济的生命线,因此,欧委会在《2030 数字指南针:欧洲数字十年之路》(2030 Digital Compass: the European way for the Digital Decade)中明确提出,"弹性、安全和值得信赖的基础设施和技术是确保尊重欧洲的规则和价值观的必要条件"。② 其政策考量不仅是通过"增量建设"补短板,更在于通过实施"去风险化"来进行"存量清理",以保护欧洲能源、交通等核心产业的底座安全。这两条路径并行展开,构成了"建设"与"清理"的复合数字主权构建逻辑。

(一)增量建设:Gaia-X 和 EuroHPC 的自主算力和数据空间尝试

在基础设施维度的增量建设中,面对美国云服务商的市场霸权,欧盟选择以柔性规制应对。Gaia-X 不寻求建造替代性超大规模云平台,而是通过联邦架构与标准制定,在依赖中建立规则主导权。而面对算力这一战略制高点,欧盟则采取硬性占领。EuroHPC 以公共投资直接建造并拥有自主超级计算设施,在物理层面直接兑现主权承诺。这一路径分化的背后反映了欧盟基础设施主权的务实逻辑。

1. Gaia-X:对美式云垄断的柔性规制

欧盟的 Gaia-X 是技术政治的一个典型案例,即欧盟通过技术架构设计这一具象化的手段来追求"数字主权"的政治经济诉求,以对抗域外云服务商的技术殖民并追求"战略自主"。以 AWS、Microsoft Azure、Google Cloud 为代表的美国云服务提供商主导了全球市场,欧洲大量政府、企业和公民数据存储在美国公司的服务器上,受美国《云法案》(CLOUD Act)的管辖,这导致了欧洲数据控制权外流。而欧洲企业对美国云服务的深度依赖限制了欧洲数字产业的创新和竞争力,而且由于全球数据治理规则由技术事实标准主导,欧洲推崇的基于规则的治理模式形

① "2030 Digital Compass: The European Way for the Digital Decade," European Commission, March 9, 2021, https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/.

② Ibid.

同虚设。

在此背景下,欧盟将重新掌握对数据的控制权视为实现欧盟数字主权的三大支柱(计算能力、对数据的控制和安全连接)之一,[①]并推出了 Gaia-X 这一数字基础设施建设重点项目,作为实现这一目标的重要措施。Gaia-X 始于 2019 年 10 月,是德国和法国当时的经济部长发起的一项建设欧洲安全数据基础设施的联合倡议。[②] 欧盟成员国在 2020 年 10 月发表联合声明,表示 Gaia-X 旨在创建一个欧洲数据基础设施,通过为欧洲数据共享提供安全和可互操作的环境来促进数字主权和技术创新。[③] 2021 年 1 月,包括 11 家法国企业和 11 家德国企业在内的 22 家创始会员企业正式成立了“Gaia-X 欧洲数据与云国际非营利协会”(Gaia-X European Association for Data and Cloud AISBL,Gaia-XAISBL),负责该项目的具体运作。可见,Gaia-X 是由法德政府牵头、法德企业联动,经由欧盟层面的议程设置而成为欧盟的一项核心数字战略。其设想是以法德两国领先的数字企业为支撑,逐步纳入其他欧盟成员国的数字企业,使之成为一个安全且具有主权属性的欧盟数据基础设施。[④] Gaia-X 明确否认要构建一个单一的、庞大的“欧洲云”以取代现有的云服务提供商,而是作为一个“连接器的连接器”,创建一个基于共同规则和标准的联邦,将现有的云服务提供商、数据中心和企业用户连接起来,形成一个统一的数据生态系统,其终极目标是实现数据的可发现、可信任和可互操作,让数据在欧洲规则下安全、自由地流动。

为减少对美国云巨头的依赖,夺回数据控制权,Gaia-X 设计了一套联邦式的技术架构,通过分布式节点的架构直接对抗像 AWS 这种中心化的模型,通过去中

---

① “Europe: The Keys to Sovereignty,” European Commission, September 11, 2020, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ac_20_2885/.

② “Press Release on Franco-German Common Work on a Secure and Trustworthy Data Infrastructure,” *Global Security Mag*, October 29, 2019, https://www.globalsecuritymag.fr/Press-Release-on-Franco-German,20191029,92222.html.

③ “Member States Joint Declaration on Cloud: Building the Next Generation Cloud for Businesses and the Public Sector in the EU,” Le Gouvernement Luxembourgeois, October 15, 2020, https://gouvernement.lu/dam-assets/documents/actualites/2020/10-octobre/MS-Joint-Declaration-Cloud-20201015-Final.pdf.

④ 宫云牧:《数字时代主权概念的回归与欧盟数字治理》,载《欧洲研究》,2022 年第 3 期,第 39 页。

心化的技术逻辑强制实现权力的分散,以打破单一中心的垄断控制权。[①] 这种技术架构本身即是一种政治选择,它强调现有的市场结构和成员国多样性,避免自上而下的强制性统一。同时,Gaia-X 还将欧洲的规则和标准(如 GDPR、网络安全标准等)进行了技术化嵌入,其核心是一套极其严格的合规性框架和共同规则,它定义了成为 Gaia-X 成员所需要遵守的"规则集",包括技术、操作和法律规则,并通过合规性自我声明和标签系统等形式来体现。这一系列设计的目的是使欧洲的规则和标准不再是单纯的法律条文,而是将法律要求直接"编码"到技术平台的操作规则中,是一种典型的"布鲁塞尔效应"的技术强化。此外,Gaia-X 还强调互操作性和数据可移植性,它试图创造一个数字单一市场,让欧洲的中小云提供商可以凭借特色服务而非规模优势参与竞争,这事实上是在通过技术架构来培育符合欧洲产业政策的市场环境。Gaia-X 的诞生,正是欧盟试图将"数字主权"这一政治概念转化为"技术—法律—经济"复合体的一次尝试。

表 2 Gaia-X 对《数据法案》等法律条文的技术"转译"

来自《数据法案》和《数据治理法案》的法律原则	Gaia-X 的技术响应和具象化
B2B 数据共享	建立数据空间,定义标准化 API,提供共享的技术流程
避免云服务锁定	通过强制性的自我描述文件和标签系统,将符合法律精神的服务标识出来
互操作性	采用开放标准和开源参考实现,通过开源组件连接异构云环境
数据利他主义	构建基于公共利益的安全、受控的数据空间,通过使用策略和策略执行点实现目的限制和可审计

注:表由作者自制。

① Gaia-X European Association for Data and Cloud AISBL, Gaia-X Compliance Document - (25.10 Release); Gaia-X Architecture Document, https://docs.gaia-x.eu/.

Gaia-X 的技术架构体现了对《数据法案》等法律规则的技术“转译”。法律要求和具体实践之间往往存在一个巨大的鸿沟。例如,法律规定了数据共享是一项强制性法律义务,然而,法律本身无法规定数据应以何种格式、通过何种安全通道、在何种信任基础上进行共享,这就产生了一个巨大的“治理真空”。而 Gaia-X 的技术架构正是为了填补这些真空而设计的,抽象的法律条款通过 Gaia-X 的技术架构,被“转译”成一套针对非欧盟服务商的、机器可读的、自动执行的技术性市场准入壁垒。首先,合规标签为外部企业进入欧洲数据生态设立了一套技术签证系统。境外企业若想加入 Gaia-X 主导的欧洲数据空间,必须生成自我描述文件,用机器可读语言声明自己如何具体满足《数据法案》的每一条要求。其次,官方提供的开源参考实现成为外部企业必须接受的合规基准。Gaia-X 推动、认证的“数据空间连接器”等开源组件,本质上是一个默认合规的技术“黑箱”,企业部署此类组件便自动获得了与欧洲系统互操作的能力。开源方案将极大地降低中小企业接入欧洲数据空间的成本和难度,也能防止形成新的锁定。但对已经占据主导地位的美中企业而言,这将倒逼它们要么接受并集成这套欧洲主导的开源堆栈,而这意味着技术路线的部分归化;要么只能投入巨大成本以自证其私有方案能达到同等合规水平。最后,审计与认证的自动化使非欧盟企业将处于一种常态化的、穿透式的技术合规监督之下。未来的合规审计很可能通过自动化的“合规性机器人”,持续扫描企业 API 和服务状态,与它们提交的自我描述文件进行比对,法律条款由此转化为持续运行的技术监管流程。

Gaia-X 成功吸引了大量的欧洲企业和组织,形成了制造业、能源、医疗等多个行业数据空间的雏形,并且成功地将“欧洲数据空间”和“联邦式主权”这样的概念推向了政策与产业辩论的中心。以汽车行业的 CATENA-X 为例,该计划以欧洲汽车以及汽车零件制造商为核心,旨在围绕汽车价值链建立一个开放协作的数据生态系统,自 2023 年年中投入服务至今,全球会员已增长至近 200 家。当然,Gaia-X也面临多种困境。一方面是治理模式的妥协,该计划采取的是多利益相关方的治理模式,虽然由法国和德国政府牵头,但其核心运营实体 Gaia-X AISBL 是一个由企业、研究机构和协会组成的国际非营利协会,且鼓励包括美国云巨头在内的全球企业参与,这种国际成员的深度参与引发了“主权稀释”的争议。以亚马

逊、微软和谷歌为代表的美国数字巨头公司长期垄断欧盟市场,加之欧盟头部电信公司的主要合作伙伴均为美国数字企业,Gaia-X 不仅在架构上依赖现有超大规模云服务商的底层服务,而且从商业利益的角度考虑,也需要吸引美国巨头参与以增强其吸引力和实用性。① 在此背景下,Gaia-X 难以有效培育和扶植欧洲本土的云服务商取代原本的垄断商,反而可能因为欧盟层面的云服务市场进一步整合而巩固美国大型数字企业的市场份额。② 另一方面,成员国之间的竞争、商业利益分歧导致的实施阻力,也是当前 Gaia-X 面临的主要障碍。③ 截至目前,Gaia-X 的正式成员已超过 300 个,尽管体现了这一计划的开放性和包容性,但也增加了成员国之间沟通协调的成本,导致 Gaia-X 项目的整体进展缓慢。利益相关者的多样性和国家间的路径分歧拖慢了行动的同步性,除了技术方面的分歧外,国家间在治理议题层面的协商成本同样突出,特别是在定义公共标准方面,④这也解释了为什么目前 Gaia-X 的项目进展不及预期。

2. EuroHPC:对战略高地的硬性占领

2025 年 11 月 17 日,第 66 届 TOP500 超级计算机榜单正式发布,排名前三的超算仍然是来自美国能源部的实验室 El Capitan、Frontier 和 Aurora。第 4 名是空降的欧洲超算 JUPITER Booster,将 2024 年榜单的第 4-9 名依次向后挤了一位。位于德国的 JUPITER Booster 为 EuroHPC 所有,它实现了 1000Petaflop/s 的运算性能,现已是欧洲排名第一、世界第四的超算。此外,EuroHPC 旗下芬兰的 LUMI、意大利的 Leonardo 和西班牙的 MareNostrum 5 也分别位列第 9、10、14 名,皆为全球超

① 调研机构“Synergy Research Group”的数据显示,欧洲云提供商的市场份额从 2017 年的 29%下降到 2022 年的 15%,并在此后一直保持在 15%左右,亚马逊、微软和谷歌占据了欧洲 70%的云服务市场。参见“European Cloud Providers' Local Market Share Now Holds Steady at 15%,” Synergy Research Group, July 24, 2025, https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15。

② 宫云牧:《数字时代主权概念的回归与欧盟数字治理》,第 39 页。

③ Clothilde Goujard and Laurens Cerulus, “Inside Gaia-X: How Chaos and Infighting Are Killing Europe's Grand Cloud Project,” POLITICO, October 26, 2021, https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/.

④ Francesca Musiani, “Gaia-X: The Bid for a Sovereign European Cloud,” *Polytechnique Insights*, June 18, 2025, https://www.polytechnique-insights.com/en/columns/digital/Gaia-X-the-bid-for-a-sovereign-european-cloud/#note-4.

算竞争中的有力竞争者。[①] EuroHPC 于 2018 年成立,是欧盟推动高性能计算战略的核心机制,目的是在欧洲范围内开发、部署和拓展世界级的协调一致的高性能计算及数据基础设施生态系统。与 Gaia-X 这种充满市场妥协的路径相对,欧盟在战略计算领域选择了一条以超国家公共投资进行“硬性占领”的主权路径,其目标是通过直接拥有和运营世界级的超级计算设施,从根本上确保欧洲在人工智能、科学研究等关键领域的长期技术自主性,这是数字主权在物质层面的终极体现。

EuroHPC 的创立及其地理部署、治理模式和技术选择都体现并服务于欧盟特定的政治意图和价值观。它并非因市场需求自然产生,而是欧盟及其成员国出于对“算力差距”的地缘政治焦虑,通过政治决策主动创建,其战略目标是提升欧洲的算力自主性,确保欧洲在数字时代拥有独立的算力支撑,以支持其在药物研发、新材料和人工智能等关键领域的创新。[②] 其部署地点同样是成员国间政治博弈的结果,将机器放置在芬兰、德国、意大利、西班牙等地,不仅考虑了经济和技术因素(如能源、冷却等),也有平衡欧盟内部发展、强化区域科技枢纽的政治意图。[③] 在治理模式上,不同于 Gaia-X 的产业联盟模式,EuroHPC 呈现出强烈的公共性和国家干预色彩。EuroHPC 是一个由欧盟(以欧盟委员会为代表)、37 个参与国和第三方合作伙伴共同组成的独特法律实体。在决策机制上,EuroHPC 的管理委员会由各参与方代表组成,资金和战略决策由公共利益主导,这确保了项目与欧盟的战略高度绑定。在资金来源方面,EuroHPC 由其成员共同资助,在 2021—2027 年期间的预算约为 70 亿欧元,其中大部分来自当前的欧盟长期预算,其余部分由成员国根据本国 GDP 规模共同出资,还有部分参与的企业或机构也会提供实物或资金

① “TOP500 List—November 2025,” Top 500 The List, November 2025, https://top500.org/lists/top500/list/2025/11/.

② “Council Regulation (EU) 2021/1173 of 13 July 2021 on Establishing the European High Performance Computing Joint Undertaking and Repealing Regulation (EU) 2018/1488,” European Commission, July 13, 2021, https://eur-lex.europa.eu/eli/reg/2021/1173/oj.

③ Jukka Ruohonen, “Geospatial Insights on the EuroHPC Supercomputing Ecosystem,” *Digital Society*, Vol.4, No.2, 2025, pp.1-11.

贡献。[①] 此外,技术路径的选择也体现了欧盟在追求“战略自主”和现实性之间的政治权衡。一方面,EuroHPC 通过“欧盟处理器计划”(European Processor Initiative,EPI)投资“欧洲芯”,旨在设计并开发完全由欧洲自主的低功耗微处理器,展现了对长期技术自主的雄心;另一方面,EuroHPC 又在建立初期务实地采购了整合美国技术(AMD、Intel、NVIDIA)和欧洲技术(Atos)的系统,以快速跻身第一梯队。这种混合架构本身就是一种政治选择,即在短期性能需求和长期自主目标之间寻求战略平衡,反映了欧洲在无法立即实现纯粹自主的领域,试图通过公共投资确保所有权和控制权、逐步推进技术替代的战略意图。

EuroHPC 的核心成果是直接部署和运营一批世界顶级的超级计算机,使欧洲正式进入全球算力竞赛的第一梯队。它不仅关注传统的超级计算机,还拓展至量子计算机和人工智能基础设施等领域,目前已在 7 个国家部署了量子计算机。[②] 当前,EuroHPC 框架下由欧洲公司自主研发的 Rhea-1 处理器已进入流片阶段,首批测试芯片计划于 2026 年年初交付合作伙伴,[③]这一里程碑标志着欧盟在构建自主可控的高性能计算生态系统中迈出实质性步伐。这是欧盟摆脱对美国公司依赖的长期战略投资,也是其技术主权最底层、最基础的体现。此外,作为一个强大的象征性项目,EuroHPC 还有助于培养一种“欧洲科技共同体”的集体认同,将成员国在数字领域的利益和命运更紧密地捆绑在一起。

(二)存量清理:从自愿性 5G 工具箱到强制性供应链审查

无论是 Gaia-X 还是 EuroHPC,都体现了欧盟在基础设施领域进行“增量建设”的逻辑,即通过公共投资建设新的、欧洲自主的战略基础设施,是从无到有的积极建构;而从“欧盟 5G 安全工具箱”(EU Toolbox for 5G Security,以下简称“5G

① “Discover EuroHPC | Budget,” The European High Performance Computing Joint Undertaking, July, 2024, https://www.eurohpc-ju.europa.eu/about/discover-eurohpc-ju_en#budget.

② “New EuroHPC Quantum Computer to Be Hosted in the Netherlands,” The European High Performance Computing Joint Undertaking, October 22, 2024, https://www.eurohpc-ju.europa.eu/new-eurohpc-quantum-computer-be-hosted-netherlands-2024-10-22_en.

③ Timothy Prickett Morgan, “With Money and Rhea1 Tapeout, SiPearl Gets Real about HPC CPUs,” The Next Platform, July 9, 2025, https://www.nextplatform.com/2025/07/09/with-money-and-rhea1-tapeout-sipearl-gets-real-about-hpc-cpus/.

工具箱”)到新近《欧盟网络安全法》(EU Cybersecurity Act)的修订提案,则体现了欧盟试图对基础设施进行“存量清理”的逻辑,即对既有基础设施中的“高风险供应商”组件进行物理清除,以构筑欧洲数字基础设施的技术边界。

2026 年 1 月 20 日,欧盟委员会发布了一份《欧盟网络安全法》的修订草案,包含了一揽子新的网络安全政策方案。① 欧盟委员会副主席汉娜·维尔库宁(Henna Virkkunen)表示,新规旨在强化供应链保护、应对网络攻击,筑牢欧洲技术主权与安全韧性。② 修订草案的公布,标志着欧盟基础设施主权逻辑的重大范式转移:它将 2020 年 5G 工具箱的自愿性指南升级为强制性的供应链审查,将治理范围从 5G 单一领域泛化至十几个关键基础设施领域,将管控措施从“限制新增”延伸至“存量清理”。它试图通过法律性质的强制化、适用领域的泛化、管控措施的追溯化等策略,将地缘政治意志“编码”为一套“去政治化”的、可执行的“技术—法律”排除机制。

首先,从 5G 工具箱到新的《欧盟网络安全法》修订草案体现了欧盟对华技术威胁认知的再政治化。作为欧盟对华技术限制的开端,2020 年出台的 5G 工具箱首次提出了“高风险供应商”的概念,并要求成员国采取限制措施。③ 其话语体系仍以技术风险为核心外壳,强调“供应链多元化”“网络韧性”等“去政治化”的通用表述。相比之下,新版草案的技术中立性被明显削弱。草案不仅将管控对象从 5G 领域扩张至能源、医疗、半导体供应链等十几个关键领域,更将措施追溯化,要求成员国在 36 个月内从移动通信网络中拆除已部署的高风险供应商设备。此外,新版草案提出认定“高风险供应商”的核心标准是“依赖风险”和“外部干预风险”,而非具体的技术漏洞清单,还特别强调了应对“非技术风险”的重要性。④ 这使得排除决定在本质上将成为一项政治判断,而非技术评估。通过以上这些手

① “Proposal for a Regulation for the EU Cybersecurity Act,” COM(2026)11 final, European Commission, January 20, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act.

② “Remarks by Executive Vice-President Virkkunen on the Cybersecurity Package,” European Commission, January 20, 2026, https://ec.europa.eu/commission/presscorner/detail/de/speech_26_152.

③ “The EU Toolbox for 5G Security,” European Commission, January 29, 2020, https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

④ “Proposal for a Regulation for the EU Cybersecurity Act”.

段,新版草案完成了一次威胁认知的再政治化。它试图将 2020 年 5G 工具箱中隐晦的、以技术话语包装的地缘焦虑,转化为法律语言和行政程序。通过“高风险供应商”这一法律虚构,成功地将排除中国技术设备这一政治决定,“编码”为一个看似程序正义、技术中立的法律机器。这种威胁认知的泛化,为排除措施的激进化和普遍化提供了合法性基础。

其次,修订草案的发布也意味着欧盟规制权力从“自愿指南”到“行政算法”的强制化转变。从技术政治学视角看,此次修订的核心在于将政治上的不信任感通过法律手段转化为技术化的硬约束,即将政治意志从软性的政策倡议固化为具有强制力的“技术—法律”架构。2020 年的 5G 工具箱作为一份自愿性指南,意味着对技术风险的评估权和最终裁量权仍掌握在各欧盟成员国手中。然而,新《欧盟网络安全法》修订草案的发布,意味着原本仅具软性约束的 5G 工具箱可能将被升格为具有法律强制力的统一信息与通信技术(Information and Communications Technology,ICT)供应链安全框架。修订草案一旦通过成为直接适用的条例,将在所有成员国具有直接的法律效力。5G 工具箱时代,成员国尚可基于本国经济利益与对华关系,对“高风险供应商”认定持保留态度;而新草案通过欧盟委员会和至少三国联合发起风险评估机制,实质上剥夺了单个成员国否决排除决定的能力。如果获得批准,该提案将触发各国强制电信运营商逐步淘汰已被多个成员国认定为存在安全风险供应商(如华为和中兴)的约束性规则。通过将自愿指南升级为统一法规,欧盟实现了权力的向上集中,成员国在安全和主权话语下,将被迫让渡原本属于国家层面的供应链自主权,这将是欧盟“技术主权”在规则维度激进的自我授权。此外,通过在法律中设定“高风险供应商”认定流程,特别是风险评估机制的发起形式,[①]欧盟实际上在数字生态的底层逻辑中植入了一套“地缘政治过滤算法”。法律将不再仅仅处理事后的违规行为,而是转变为一种事前的结构性排斥,将供应商的政治背景转化为技术准入的硬性门槛。

尽管该草案在规则层面构建了完美的防御闭环,但在其实施过程中也面临巨大的行业争议和内部协调难题。5G 工具箱时期,运营商仅需在新增投资中规避高

① “Proposal for a Regulation for the EU Cybersecurity Act”.

风险供应商,而新草案要求拆除已稳定运行多年的存量设备。欧洲电信组织 Connect Europe 警告,仅移动网络领域的强制淘汰将产生数十亿欧元的额外成本。[①] 此外,成员国在排除中国设备上也存在利益分歧。2019—2020 年,在 5G 工具箱谈判期间,德国、西班牙、匈牙利等国正是基于经济理性抵制了对华为的强制排除,最终促使 5G 工具箱被设计为“自愿性指南”。[②] 五年之后,这些国家的技术依赖程度并未根本改变。[③] 对于这些国家而言,36 个月的淘汰期限意味着数十亿欧元的额外支出、网络服务的中断风险以及与重要贸易伙伴的政治摩擦。

从 5G 工具箱到新《欧盟网络安全法》修订草案是欧盟基础设施主权一次激进的实践尝试。修订草案的治理对象是已经物质化的 5G 基站、电力控制系统、自动驾驶平台、医疗成像设备,这些设备在过去五年到十年间被采购、安装、调试,已深度嵌入欧洲关键基础设施的日常运行。该治理手段不是通过市场竞争的优胜劣汰,也不是通过技术迭代的自然更替,而是通过法律命令的直接干预来实现。该治理目标是在物理层面重塑欧洲关键基础设施的技术构成,让“高风险”技术从欧洲的数字疆域中被系统性地、不可逆地清除出去。与 Gaia-X 和 EuroHPC 的“增量建设”相比,它属于“存量清理”,二者共同构成欧盟基础设施主权的完整光谱。然而,这一激进实践也受制于基础设施主权的根本性约束:主权意志不能替代物质基础。当法律强制拆除的速度快于替代供应链的建设速度时,主权的激进性将不得不向现实妥协,5G 工具箱的实施状况也证明了这一点。《欧盟网络安全法》修订草案最终的落地形态,将不是布鲁塞尔单方面意志的简单投射,而是主权愿景与技术依赖、安全诉求与经济代价、欧盟统一与成员国差异之间持续博弈的结果。

---

① “Connect Europe Statement on the Cybersecurity Act,” Connect Europe, January 20, 2026, https://connecteurope.org/news/connect-europe-statement-cybersecurity-act.

② 吴白乙等主编:《欧洲蓝皮书:欧洲发展报告(2019~2020)》,社会科学文献出版社 2020 年版,第 156-158 页。

③ 根据丹麦咨询公司“Strand Consult”在 2025 年发布的 5G 市场报告的数据,截至 2024 年第四季度,欧洲 32 个国家(欧盟 27 国+5 个非欧盟国家)中,近三分之一的 5G 站点由中国的供应商提供,这一比例自 2022 年第二季度以来没有下降。参见“The Market for 5G RAN in 2024: Share of Chinese and Non-Chinese Vendors in Europe,” Strand Consult, January 10, 2025, https://strandconsult.dk/get-your-free-copy-of-strand-consults-new-study-the-market-for-5g-ran-in-2024-share-of-chinese-and-non-chinese-vendors-in-europe/。

五 身份维度的主权构建:构建“可信欧洲”的数字围栏

在技术政治学的视野下,身份是主权行使的逻辑终点。如果说规则提供了蓝图,基础设施提供了物理底座,那么身份维度则确立了数字空间中的政治主体与信任边界。欧盟在这一维度的实践呈现出一种双面一体的逻辑:对外的边界划分和对内的身份建构。首先,数字主权的边界通过确认外部风险来实现。正如上文在规则与基础设施维度中所述,欧盟通过《欧盟网络安全法》等工具建立了“高风险供应商”认定机制。这些机制本质上是一种外向的身份识别实践,它将地缘政治中的不信任转化为技术系统中的风险标签,从而在数字空间划定了清晰的信任场域。通过这种方式,欧盟完成了对数字主权边界的初步勾勒,即通过对技术源进行识别并“去风险化”,为内部信任环境的建立扫清了障碍。然而,仅仅依靠外部排除并不能支撑起独立的主权人格,数字主权的深度建构,最终取决于如何定义并凝聚其内部的政治共同体。因此,本文的分析重点将转向欧盟最具主动性的身份主权实践——EUDI 钱包。

(一)EUDI 钱包的出台及其背景

在数字时代,控制公民访问在线服务的身份认证体系已成为同控制物理领土同等重要的主权新前沿。欧洲公民与数字服务的连接,正被美国大型科技平台通过其便捷的“社交登录”所垄断。[①] 这些平台的身份认证系统本质上是一种私人主权的行使,相当于数字时代的“出入境管理”,大型科技平台以此获得了巨大的权力,它们可以利用积累的行为数据施加前所未有的商业和政治影响力。将数字身份生态建立在境外科技巨头的基础上,意味着巨大的战略风险:不仅仅是数据流向外部,更是将整个数字经济的信任基石“外包”出去。同时,数字身份认证体系也代表了数字空间的通行规则,谁掌握了它,谁就掌握了定义隐私、安全、数据权利和商业模式的权力。对境外平台的依赖不仅带来了数据安全危机和经济风险,更意味着欧盟在定义其数字空间的准入规则、隐私标准和公民权利方面主权的严

① 例如,网站上常见的“通过 Google 登录”“通过 Apple 登录”或“通过 Facebook 登录”的按钮。

重流失。正如欧委会主席乌尔苏拉·冯德莱恩(Ursula von der Leyen)所言,“当一个应用或网站要求我们创建一个新的数字身份或通过一个大平台轻松登录时,我们不知道我们的数据在现实中发生了什么”。①

欧盟数字主权在身份维度上的缺失不仅体现在对外依赖上,在内部维度,也从未真正存在过一个统一的欧洲数字公共领域和一个互操作性的数字身份系统。欧盟及其成员国的主权身份系统在数字领域是碎片化的,德国的 eID、意大利的 SPID、法国的 FranceConnect 等系统互不联通,形成了一个“数字巴别塔”。为什么欧洲没有数字巨头?欧洲通过内部政策讨论达成的共识为 27 个成员国身份系统的互不联通导致了巨大的交易成本,一个统一的欧洲数字身份系统对于欧洲数字“单一市场”的建设是至关重要的。② 因此,关于欧洲统一数字身份的考量不仅是隐私,更是“规模主权”的重组,即通过统一底座,将碎片化的小市场“缝合”成一个足以与美中大厂抗衡的统一数字空间,从而找回缺失的规模竞争力。

在此背景下,EUDI 钱包正是欧盟和成员国为了在 21 世纪有效行使主权、追求“战略自主”而构建的信任基石。2014 年,欧盟委员会出台《电子身份识别和信任服务法规》(Electronic Identification and Trust Services,eIDAS),以加强整个欧盟的安全数字交互。③ 这一法规旨在使欧盟公民能够使用各自的电子身份(eID)认证和参与整个欧盟成员国的在线服务。2024 年 2 月,欧盟通过了修订后的 eIDAS 2.0 法规。该法规赋予个人对其数据更大的控制权,并提出要在欧盟范围内实施 EUDI 钱包。④ EUDI 钱包是一个用户控制的应用程序,允许欧洲公民存储和管理

① Ursula von der Leyen, “State of the Union Address 2020,” European Commission, September 16, 2020, https://commission.europa.eu/strategy-and-policy/state-union/state-union-2020_en.

② “Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity,” European Commission, June 3, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0281.

③ “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC,” Official Journal of the European Union, July 23, 2014, https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng.

④ “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework,” European Commission, April 30, 2024, https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng.

他们的数字证书。这些凭证可以包括个人识别数据(如验证个人身份的身份证)和各种电子属性证明(如移动驾驶执照和确认特定属性或资格的教育证书等)。[①] EUDI 钱包并非要取代成员国各自的身份认证系统,而是要通过一个“身份联邦”的模型构建一个互操作层,它承认成员国身份系统的权威,但通过共同的欧盟规则和技术标准将它们编织在一起。

(二)EUDI 钱包对欧洲价值观的技术编码

与上文所述的防御性措施不同,EUDI 钱包是一次内化的、建设性的技术政治尝试。它不再仅仅关注“谁是敌人”,而是通过一套精密的技术架构,回答了“什么是欧洲定义的数字公民”。本文将从技术编码的视角,解析 EUDI 钱包如何将隐私保护、自主可控等欧洲核心价值观转化为可执行的代码逻辑,从而在数字时代重塑公共信任的基石。

首先,EUDI 钱包以“自我主权身份”(Self-Sovereign Identity,SSI)模型对抗境外科技巨头的平台中心化范式。EUDI 钱包摒弃了美国科技平台和欧盟自身由单一中心集中存储和管理用户身份数据的传统架构,采用了去中心化的“自我主权身份”模型,用户凭证以加密形式存储在个人设备上的数字钱包中,数据交换通过点对点的可验证凭证完成。这种技术架构的战略潜力通过 eIDAS 2.0 得到了法律维度的深度激活:该条例在序言中明确要求,超大型在线平台负有接受 EUDI 钱包作为身份验证手段的义务。[②] 这一“技术架构+行政强制”的组合,试图在根本上阻止美国科技巨头成为欧洲公民数字身份的“中间人”,直接挑战其通过控制身份层来积累数据、锁定用户的商业模式,这是对科技巨头“身份即服务”垄断的一次技术反击。同时,这一架构也旨在防范任何外部中心化的控制,即使是欧盟机构自身也无法在未经用户同意的情况下集中访问所有身份数据。这在技术上预防了未来因政治压力或安全漏洞导致的大规模身份数据被外部力量获取或操控的风险,体现了“战略自主”中的安全维度。

---

① Zahra Ebadi Ansaroudi et al., “Navigating Secure Storage Requirements for EUDI Wallets: A Review Paper,” *EURASIP Journal on Information Security*, No.1, 2025, pp.1-17.

② “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework”.

其次,EUDI 钱包架构强调开放标准和互操作性,以确保规则制定权和技术选择自由。EUDI 钱包不创建欧盟私有的、封闭的技术标准,而是基于“万维网联盟”(World Wide Web Consortium,W3C)等标准组织制定的开放标准来构建。一方面,欧盟旨在摆脱对单一技术供应商的锁定,无论是美国还是中国的技术公司,都无法通过其专利技术将欧盟捆绑在其商业生态中,以保持选择任何符合开放标准的技术供应商的主动权;另一方面,欧盟也希望以此争夺全球规则的制定权,通过率先在大规模公共应用中实施这些开放标准,试图将这些标准与诸如隐私和用户控制等欧洲价值观深度绑定,并将其树立为全球数字身份的“事实黄金标准”。这实质上是将欧洲的规制偏好通过技术标准进行全球化输出,以实现规则自主。此外,互操作性是激活欧洲单一数字市场的关键。eIDAS 2.0 法规明确指出,这一实践的核心意图在于“消除跨境使用电子识别手段的既有障碍”,并确立了强制性的跨境互认框架,要求各成员国签发的数字身份钱包必须在全欧范围内获得无障碍的法律认可与技术对标。① 欧盟希望通过这样的技术手段,将分散的欧盟成员国市场整合为一个拥有 4.5 亿用户的统一数字空间,从而获得能与美中相抗衡的“规模主权”。

最后,EUDI 钱包设置了国家背书的信任层级,将国家作为信任的终极锚点。作为一项信任基础设施,EUDI 钱包的最终信任源不是钱包本身,而是成员国政府根据 eIDAS 法规认证的官方身份源,钱包只是呈现和管理这些由国家背书的凭证容器。同时,EUDI 钱包的技术架构划分了清晰的信任层级,明确区分了不同等级的身份保证,确保高风险交易需要更高级别的身份验证,并将美国科技公司和中国可能的方案都排除在最高信任层外。通过这套由国家主导的信任体系,欧盟得以清晰界定数字政治共同体的边界。此外,这也为跨境数字治理奠定了基础,统一的数字身份层使欧盟能够跨越成员国边界,直接、有效地实施数字政策,如跨境福利发放和企业监管,这将大幅增强欧盟作为一个超国家实体的整体行动能力和内部治理的自主性。

① “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework”.

当前,EUDI 钱包正处于大规模试点过程中,并且计划于 2026 年年底在成员国全面推出。① EUDI 钱包的测试已经超出了政府和公共服务范畴,在旅游、金融等关键行业展开了真实的应用场景测试。例如,Amadeus 与汉莎航空成功测试了 EUDI 钱包在线上值机、行李托运、登机的全流程中的应用。② 德国储蓄银行集团宣布将 EUDI 钱包集成到其主要的银行 APP 中,以大幅提高用户便利性并巩固数据主权。③ 在快速推进的同时,EUDI 钱包项目也面临协调复杂的生态系统、赢得公众信任和被市场采纳等难题。例如,EUDI 钱包的项目涉及欧盟 27 个成员国、众多私营合作伙伴以及非欧盟参与者,如何确保所有钱包都遵循共同规范以保障互操作性,这将是一项持续性的挑战。

EUDI 钱包通过去中心化、标准开放化和信任国家化的技术架构,构建了一个自主性闭环,它将欧盟的“战略自主”诉求和规范性价值观从布鲁塞尔的法律文本,深刻嵌入每一位欧洲公民的日常数字生活,从而塑造一种基于欧洲价值观的数字身份认同,代表了欧盟在个体层面实践“数字主权”的最深层尝试。这也体现了技术政治学的核心要义:技术和政治并非两个独立的领域,而是持续共同塑造着我们所处的数字世界。

六 数字主权实践的差异化指向

从本文对规则、基础设施与身份三个维度的分析中可以看出,欧盟数字主权的构建并非整齐划一的“技术孤立”,而是呈现出一种非对称的、具有高度针对性的实践逻辑。这种差异化指向揭示了欧盟在面对美中两种不同竞争压力时,对威

① Réka Vékás-Kovács, “EU Digital Identity Wallets are Set to Transform Online Privacy. Here Is How,” TechUK (The UK's Technology Trade Association), October 17, 2025, https://www.techuk.org/resource/eu-digital-identity-wallets-are-set-to-transform-online-privacy-here-is-how.html.

② Monica Hansen, “Tap to Fly: Amadeus and Lufthansa Test EU Digital Identity Wallet for Seamless Travel,” *Amadeus*, September 16, 2025, https://amadeus.com/en/newsroom/press-releases/amadeus-lufthansa-eu-digital-identity-wallet.

③ Bo Harald, “Sparkassen Showing the Way for Wallets in E-banking,” *Finextra*, October 18, 2025, https://www.finextra.com/blogposting/29615/sparkassen-showing-the-way-for-wallets-in-e-banking.

胁性质与依赖深度的动态校准。

在数字主权的实践逻辑上,通过对《数据法案》系列、Gaia-X、EuroHPC、5G 工具箱和《欧盟网络安全法》修订草案等案例的跨维度考察,可以发现欧盟在处理美中竞争压力时呈现出显著的“对美规训、对华防御”的差异化策略倾向。欧盟对美路径更倾向于在功能性依赖中行使规训权力,美国对其技术压力主要源于其软件生态与云服务的垄断。因此,欧盟的主权实践更侧重于规则维度的“转译”。通过《数据法案》和 Gaia-X 设定互操作性 API,欧盟并不寻求物理上彻底切断美方服务,而是通过市场治理逻辑进行规训,促使美资巨头在欧洲定义的标准轨道内运行。其核心目标是打破数据锁定,实现一种“受控的依赖”。而欧盟的对华路径则更倾向于在地缘政治风险中构建排他性的防御。针对中国,欧盟的焦虑更多地指向底层硬件的系统性风险与路径依赖。因此,其主权实践侧重于基础设施维度的“存量清理”。从外商直接投资审查框架、5G 工具箱到强制性的新《欧盟网络安全法》修订草案,欧盟采取的是一种排除逻辑。其核心目标是通过对关键技术领域设备和投资的剥离,从投资和供应链层面强行开辟出地缘政治的安全区,实现一种“物理的隔离”。

这种差异化指向并非偶然,而是由压力源的本质特征所决定。一方面是美中威胁认知的差异。美国被视为经济上的霸权、政治上的盟友,其压力主要体现在市场垄断和私人主权扩张,因此,欧盟动用法律杠杆对其进行市场规制;而中国则被视为技术上的挑战和制度性的对手,这意味着对中国技术的风险评估从基于事实的风险转向了基于身份的风险,欧盟对中国技术的排斥,本质上是对非盟友政体及其法律环境下“技术武器化”风险的系统性担忧。另一方面,这也反映了欧盟对产业支柱的生存焦虑。与美国占优的虚拟服务不同,中国在工业数字化和能源转型领域表现出极强的软硬一体化竞争力,直接挑战了欧洲传统的工业根基。排除中国设备,不仅是出于网络安全的考虑,更是为了在物理工业数字化转型的关键期,利用行政壁垒为西门子、爱立信、诺基亚等欧洲本土工业巨头清场,剥离中企设备可以被视为防止欧洲工业“空心化”的一种保护主义手段。

尽管存在明显的逻辑倾向,但必须指出,欧盟数字主权的差异化指向并非绝对的技术脱钩,也不代表规则仅针对单一国家。在规则维度,欧盟的法律框架在

文本形式上保持中性,其针对“守门人”平台或数据共享的硬性限制,在规训美国巨头的同时,同样适用于具有相似市场地位的中国企业,如 TikTok、阿里巴巴等。在阐述《欧盟网络安全法》修订草案时,欧委会副主席维尔库宁同样提到云服务和卫星技术是两个潜在的安全风险领域,[①]而这两个领域几乎完全被美国公司所垄断。这种规则中性确保了欧盟在世界贸易组织框架下的法律正当性,也体现了其作为规则大国对数字市场整体权力的重构。在实践中,欧盟数字主权的差异化指向同样存在不同程度的交叉渗透现象。在基础设施维度,EuroHPC 虽然旨在对冲美式算力霸权,但其对供应链自主可控的要求同样排除了其他非欧盟的硬件供应。在身份维度,EUDI 钱包对隐私算法的强制“编码”,既阻断了美式“私人主权”的数据收割,也通过数字围栏防御了其他技术体系的潜在渗透。

综上所述,欧盟的数字主权实践展现出一种“嵌入式自主”的特质,它在规则维度利用市场力量进行柔性规训,在基础设施维度利用行政力量进行硬性防御,在身份维度则利用隐私算法进行双向阻隔。这种差异化指向揭示了欧盟最真实的战略意图,它并非追求与全球供应链的全面决裂,而是通过精准的技术政治实践,在依赖美国生态的同时保住市场自治权,在利用中国制造的同时守住安全生命线。这种非对称的策略组合,共同支撑起欧盟在数字时代“战略自主”的总目标。

七 结论

本文通过对欧盟数字主权实践的系统考察发现,欧盟正试图将其追求“战略自主”的地缘政治抱负,精准地转化为一套涵盖规则、基础设施与身份维度的社会技术实践。这并非一次简单的技术脱钩,而是一场在深度依赖的全球技术生态中进行的非对称性权力重构。

欧盟数字主权的构建呈现出极强的务实主义与技术政治化特征:在规则维度,它通过“立法造市”将政治意志代码化,对美资平台进行柔性规制,对中国技术资本实施排他性防御;在基础设施维度,它通过“增量建设”与“存量清理”的双轨

① “Remarks by Executive Vice-President Virkkunen on the Cybersecurity Package”.

并行,加强其对核心底座的物理掌控,特别是针对中国高科技企业进行系统性剥离的政策倾向,标志着其安全逻辑已从风险治理走向身份排除;在身份维度,它通过对内建构信任锚点与对外划定政治禁区,完成了数字共同体边界的闭环。这一复合防御系统不仅缓冲了来自美中技术博弈的外部压力,更试图系统性地缓解其技术落后的竞争力焦虑,定义一种不同于美中的第三种数字文明模式。

欧盟这一态势对中国的启示体现在应对策略与借鉴经验两个层面。一方面,在应对策略上,中国需高度警惕欧盟数字主权逻辑中“安全焦虑身份化”的倾向,即欧盟对中国企业、技术和资本的风险评估从基于事实的风险转向基于身份的风险。面对欧盟从 5G 工具箱向全赛道供应链审查的硬性转变倾向,中国科技企业应通过提升技术底层架构的透明度、积极参与欧洲开源生态建设,尝试在技术逻辑上对冲基于身份的不信任。同时,应利用欧盟内部经济利益与地缘诉求的张力,在非敏感领域寻求务实的第三方市场协作,延缓系统性排除的连锁反应。另一方面,从借鉴的角度来说,中国可适当汲取欧盟将主权嵌入技术架构的建设经验。欧盟将法律条文“转译”为 API 标准、将价值观“编码”为身份协议的做法,为数字时代的社会治理提供了新范式。中国在推进数字主权建设时,亦可强化将法律“编码”为技术治理能力,不仅要在硬件底座上实现自主,更要学习如何将宏观政策目标转化为微观的技术架构约束,通过构建主权内生的技术生态,实现数字空间治理效能与地缘政治韧性的双重提升。

(**作者简介**:张若扬,复旦大学国际关系与公共事务学院博士研究生;蔡翠红,复旦大学美国研究中心教授。**责任编辑**:蔡雅洁)