# 美欧数据跨境流动博弈中的欧盟技术主权战略及其实现

刘　业*

**摘　要：**与安全港框架不同，隐私盾框架的废止在涉欧数据跨境流动合规方面引起了较大的震动，这折射出欧盟在技术主权战略指导下趋向于严格规制数据跨境流动。欧盟法院在法律适用上存在采用双重标准的嫌疑，以及欧盟数据保护委员会偏离《一般数据保护条例》“基于风险”路径等吊诡现象，是欧盟以技术主权战略对抗美国侵略性技术控制战略并作用于法律层面的结果。凭借个人数据保护领域中的布鲁塞尔效应，欧盟牢牢掌控该领域的规则话语权，在隐私盾框架废止后的美欧后续谈判中处于主动地位，并迫使美国不断修改立法以符合欧盟的法规。欧盟意图在谈判中实现软数据本地化和限制境内外国科技企业市场竞争力的目的，为技术主权战略的实施提供数据与技术保障。中国应当关注欧盟数据跨境流动规制中的技术主权战略意图，避免陷入被动合规陷阱，并构建独立自主的数据跨境流动战略。

**关键词：**技术主权战略　数据跨境流动　隐私盾框架　布鲁塞尔效应　软数据本地化

## 引　言

2020 年 7 月，欧盟法院废止了美欧数据跨境传输的隐私盾框架。这并非欧盟法院首次废止美欧数据跨境传输的法律框架，早在 2015 年 10 月，欧盟法院便作出废止安全港框架（隐私盾框架的前身）的裁决。但 2016 年 7 月，美欧迅速完成谈判并通过了替代性的隐私盾框架。由于欧盟法院在废止安全港框架的同时设置了专门的谈判过渡期，因此美欧之间的数据跨境传输并未受到实质性影响。反观隐私盾框架却在废止后引发了以欧盟为中心、波及全球数据跨境流动的“大地震”。[①] 时间上，欧盟法院并未设置谈判过渡期，导致所有依靠隐私盾框架提供合法性支撑的美国企业，在隐私盾框架无效后瞬即陷入法律合规的不稳定状态。空间上，欧盟法院对依靠标准合同条款等替代性保障措施的企业施加个案充分性评估义务，要求企业只有经过数据保护机构的个案充分性审

* 刘业，厦门大学法学院国际法学博士研究生，荷兰乌特勒支大学联合培养博士研究生，厦门大学法学院网络空间国际法研究中心研究助理。本文系国家社科基金项目“网络强国战略下数据资源的国际法规制研究”（项目批准号：18CFX087）的阶段性研究成果，本文亦得到国家留学基金资助。本文所用网络资源的最后访问时间均为 2023 年 9 月 3 日。

① Xavier Tracol, “Schrems II: The Return of the Privacy Shield”, (2020) 39 *Computer Law & Security Review* 1, pp. 7 – 8.

查之后方可合法传输数据，由此动摇了标准合同条款等机制的合法性。[①] 不仅美国企业，所有依靠替代性保障措施的各国企业，其涉欧数据跨境传输业务均被置于合法性存疑的境地。

从安全港到隐私盾，为何欧盟法院裁决的严苛程度显著提升？虽然 2018 年 5 月号称全球最严数据保护法的欧盟《一般数据保护条例》（General Data Protection Regulation，下文简称 GDPR）正式生效，为欧盟法院作出严格裁决提供了法律依据，但 GDPR 承袭《数据保护指令》（Data Protection Directive），并未超出后者的基本框架，仅因 GDPR 的生效无法充分解释欧盟法院的此种转变。围绕隐私盾事件展开的讨论中，有学者在回顾美欧安全港和隐私盾等多轮博弈的基础上，深入细致地剖析了欧盟法院裁决《隐私盾决定》（Privacy Shield Decision）无效的司法逻辑。[②] 还有学者系统性比较美欧在数据保护理念与定位、法律规则体系、法律实施体系等层面的差异性，并适当评估了替代隐私盾的可能路径选择。[③] 另有学者从保护标准、适用工具、监管机构和国际规则等 4 个层面研究隐私盾事件对欧盟数据跨境流动法律监管产生的影响，反思欧盟此种防御式监管模式的合理性。[④] 这些讨论虽然从不同角度分析隐私盾事件，但大部分均局限于法律的单一维度，难以准确揭示欧盟法院立场转变背后的深层逻辑。有鉴于此，本文将从政治与法律的互动关系视角分析和解读隐私盾事件及其背后的技术主权战略。本文首先简要介绍美欧数据跨境流动规则博弈的舞台，接着分析隐私盾框架废止后欧盟法院、欧盟数据保护委员会以及欧盟委员会趋严适用数据跨境流动机制的现象，并借此引出欧盟的技术主权战略，紧接着全面剖析欧盟技术主权战略的动因、基本内涵和战略布局，随后分析欧盟如何在美欧数据跨境流动博弈中实现其技术主权战略，最后从中国视角审视欧盟的技术主权战略及其数据跨境流动法律机制，探寻中国的因应之策。

## 一　美欧博弈场域：欧盟 GDPR 数据跨境流动机制合规

围绕数据跨境流动议题，美欧展开了长达 20 余年的博弈。从 1995 年《数据保护指令》到 2016 年 GDPR，欧盟不断细化和完善数据跨境流动法律机制，美欧数据跨境流动的博弈舞台也始终圈定在欧盟的数据跨境流动法律机制之中。

欧盟 GDPR 第 5 章专章规定了数据跨境流动法律机制，为欧盟数据转移至第三国提供了一套多层次的数据跨境流动法律工具箱。第一层，充分性认定机制。由欧盟委员会对第三国或第三国特定区域进行充分性认定，第三国或第三国特定区域通过欧盟委员会的认定则可与欧盟自由进行数据跨境流动。充分性认定极为严格，包括对第三国人权与基本自由的尊重情况、政府部门访问个人数据的立法和实施情况、数据转移至第三国的规则和有效可执行的数据主体权利（尤其包括数据主体司

① Andraya Flor，“The Impact of Schrems II：Next Steps for U. S. Data Privacy Law”，（2021）96 *Notre Dame Law Review* 2035，pp. 2049 – 2050.

② 参见黄志雄、韦欣好：《美欧数据跨境流动规则博弈及中国因应——以〈隐私盾协议〉无效判决为视角》，载《同济大学学报（社会科学版）》2021 年第 2 期。

③ 参见单文华、邓娜：《欧美数据跨境流动规制：冲突、协调与借鉴——基于欧盟法院“隐私盾”无效案的考察》，载《西安交通大学学报（社会科学版）》2021 年第 5 期。

④ 参见杨帆：《后“Schrems Ⅱ案”时期欧盟数据跨境流动法律监管的演进及我国的因应》，载《环球法律评论》2022 年第 1 期。

法救济的权利）等方面的全面评估。[①] 第二层，适当保障机制。若无法取得欧盟委员会的充分性认定，境内企业必须确保提供适当的保障措施和可执行的权利、有效的法律救济措施。对此，欧盟提供了标准合同条款、可约束性公司规则、行为准则、验证机制等具体法律工具供企业选择。其中，标准合同条款和可约束性公司规则被广泛使用。[②] 第三层，克减机制。若以上两层次均无法适用，境内企业若符合 GDPR 第 49 条明确规定的特定情形，[③] 也可将数据传输至第三国。克减机制的设计理念是，个人数据受保护的权利并非一种绝对权，如果跨境流动的风险很小，抑或是此类风险被其他更为重要的权利或利益所覆盖，适当减损一部分数据主体权利是可接受的。为防止因滥用克减规则导致架空数据跨境流动法律保护机制的风险，实践中数据保护机构必须从严解释和适用克减机制。[④]

对美国而言，选择充分性认定作为数据跨境流动的法律机制具有必然性。原因在于，第二层次的适当保障机制，需要企业申请欧盟数据保护机构的个案审批同意后才能适用，一般的中小企业难以负担由此产生的跨境合规成本，[⑤] 实践中大型科技企业往往更青睐此种路径。而第三层次的克减机制，适用于临时的、非常态化、低风险的数据跨境流动场景，无法为开展常态化数字跨境经贸活动的企业提供合法基础。鉴于美国与欧盟之间每年约 7 万亿美元的数字经济规模，第一层次的充分性认定机制成为美国的必然选择。充分性认定机制主要适用于一国整体或部分区域的数据跨境传输，若该国或该区域与欧盟存在大体量的数字经贸活动，通过国家或区域范围内的充分性认定机制，企业仅需按照本地监管机关的要求合规即可。该机制下的隐私盾框架，为美国企业（尤其是美国的中小企业）与欧盟企业之间的跨大西洋数据传输搭建了便捷高效的制度桥梁。无须经过欧盟数据保护机构的个案合规审查，美国企业可自愿加入隐私盾框架，按照隐私盾框架中的数据保护规则进行自我认证，并接受美国联邦贸易委员会和商务部的监督与执法。这极大地简化了企业合规程序，降低了合规成本。仅 2017 年 9 月至 2019 年 6 月这段时间，加入该框架的企业从 2177 家猛增至 5348 家，[⑥] 美欧之间的数字经贸繁荣一时。但隐私盾框架的废止打断了这

① 目前，通过欧盟委员会充分性认定的国家或区域仅包括安道尔、阿根廷、加拿大（限于商业组织的数据跨境流动）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、韩国、瑞士、英国、乌拉圭以及美国（限于加入美欧数据隐私框架的商业组织的数据跨境流动）。这一名单动态更新，欧盟委员会至少每 4 年对其相关发展进行一次审查，并据此作出是否废止、修正或中止对该国的充分性认定。See "Adequacy Decisions", European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

② 标准合同条款由欧盟委员会制定发布，需要数据跨境传输的企业选择标准合同条款作为规定双方数据保护权利和义务的格式合同模板，但不得对标准合同条款进行任何可能减损数据保护水平的修改。可约束性公司规则由企业按照欧盟要求制定并得到欧盟批准才具有效力，其适用场景相比标准合同条款更为狭窄，仅适用于进行联合经济活动的企业集团内部，如分属不同国家的母子公司、总分公司之间的数据传输。

③ GDPR 规定的特定情形，除所列举的 7 类克减情形（包括数据主体自担风险而为同意、为保护数据主体利益所必要、数据主体客观上无法表达同意且为保护其关键利益、履行合同所必要、实现公共利益所必要、司法程序推进所必要，或制作登记册所需）外，还将符合转移非重复、仅涉及小部分数据主体权利、实现数据控制者压倒性正当利益所必要，且数据控制者已采取合适的安全保障措施的这类情形纳入克减情形之中。

④ Christopher Kunner, Lee A. Bygrave and Christopher Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), pp. 883-884.

⑤ Aaditya Mattoo and Joshua P. Meltzer, "International Data Flows and Privacy: The Conflict and Its Resolution", (2018) 21 *Journal of International Economic Law* 769, pp. 778-779.

⑥ Drew Medway and Jeremy Greenberg, "New FPF Study: More Than 250 European Companies are Participating in Key EU-US Data Transfer Mechanism", Future of Privacy Forum website, https://fpf.org/blog/new-fpf-study-more-than-250-european-companies-are-participating-in-key-eu-us-data-transfer-mechanism/.

一良好发展趋势，对合规不确定性的担忧笼罩于每个涉及欧盟数据跨境流动业务的企业头顶。此次事件，导致跨大西洋数据流动受到前所未有的冲击，跨大西洋数字贸易也受到严重影响。[①] 随后美欧经历长达 3 年的艰苦谈判，最终以欧盟委员会于 2023 年 7 月通过《关于欧盟—美国数据隐私框架的充分性决定》（Adequacy Decision for the EU-US Data Privacy Framework）为谈判画上了句点，但这一新的替代框架还将持续面临来自欧盟法院的司法审查。

## 二　欧盟趋严适用数据跨境流动法律机制

隐私盾事件中，欧盟法院的裁决标准趋于严苛，法律适用存在“双重标准”之嫌；而欧盟的数据保护机构，似偏离 GDPR“基于风险”路径（risk-based approach），而转向“基于权利”路径（rights-based approach）的规制理念。在新的谈判阶段，欧盟委员会在提升数据保护合规标准的同时，也意图将美国再度拉入欧盟规则场域之中。

### （一）欧盟法院裁决或存在“双重标准”之嫌

《隐私盾决定》是隐私盾框架的法律基础。根据欧盟法院的裁决，《隐私盾决定》无效的原因主要有两点：第一，美国情报部门获取个人数据的权力没有得到有效制约；第二，美国没有提供公正有效的司法救济机制。后续谈判中，美欧对后者的谈判取得较大进展，如美国承诺设置两级救济系统（two-tier redress system），其中包括设置专门的数据保护审查法院（Data Protection Review Court）。但关于前者，美欧之间的矛盾难以有效化解，谈判相关争议也主要围绕前者展开。

“隐私盾案”（也称“*Schrems II* 案”）中，欧盟法院审理认为，根据《欧盟基本权利宪章》（Charter of the Fundamental Rights of European Union）第 52 条，授权干涉基本权利的法律文件本身必须明确界定授权监控行为的行使范围与必要限制。并且，对个人数据基本权利的减损和限制必须严格控制在绝对必要的情形，如必须在法律上明确规定将在何种情形、何种条件下处理个人数据。[②] 在美国情报法律体系中，尽管美国试图通过《第 28 号总统政策指令》（Presidential Policy Directive－28，下文简称《总统指令》）来限制以《外国情报监控法》（Foreign Intelligence Surveillance Act，下文简称《监控法》）第 702 节和《第 12333 号行政命令》（Executive Order 12333，下文简称《行政命令》）为法律依据的政府情报监控行为，但这种限制并未达到欧盟标准。原因在于，《总统指令》允许情报部门以非特定方式大规模、大批量收集关于个人数据的情报信息且不加任何限制，这明显有违比例原则。而依据《行政命令》进行的情报监控，可在不受司法审查的情况下通过国际海底电缆收集来自欧盟的个人数据。[③]《监控法》第 702 节同样未限制依此进行外国情报监控的权力，也未对可能成为这些计划目标的非美国人提供担保。[④]

---

① Nigel Cory, Daniel Castro and Ellysse Dick, “Schrems II: What Invalidating the EU-U. S. Privacy Shield Means for Transatlantic Trade and Innovation”, Information Technology & Innovation Foundation website, https://itif.org/publications/2020/12/03/schrems－ii－what－invalidating－eu－us－privacy－shield－means－transatlantic/.

② *Data Protection Commissioner v. Facebook Ireland Ltd*, *Maximillian Schrems*, C－311/18 (2020), paras. 175－176.

③ *Data Protection Commissioner v. Facebook Ireland Ltd*, *Maximillian Schrems*, C－311/18 (2020), para. 183.

④ *Data Protection Commissioner v. Facebook Ireland Ltd*, *Maximillian Schrems*, C－311/18 (2020), para. 180.

对于欧盟法院的裁决理由，美国主张《行政命令》不应纳入数据保护的充分性评估之中。国家情报监控活动可区分为“直接”与“间接”两种情报监控模式：前者由政府情报部门直接对境外传输的数据进行监控，如在跨大西洋海底电缆中直接获取数据，《行政命令》为直接情报监控活动提供法律依据；后者通过行政令方式强制国内数据运营商向政府披露相关数据，《监控法》第 702 节为间接情报监控活动提供法律依据。根据欧盟法院的判例，[①] 对成员国的直接情报监控活动，并不在《隐私与电子通讯指令》（Privacy and Electronic Communications Directive）、GDPR 或是《执法指令》（Law Enforcement Directive）等欧盟法管辖之内。因此，对成员国的直接情报监控活动，欧盟法律实际上并未限制其成员国以国家安全目的为由直接访问个人数据，同时也未提供隐私与数据权利保护。在直接情报监控行为规制中，欧盟并没有相应的法律标准来评估第三国所提供的隐私和数据保护是否“基本等同于”欧盟法律保护水平。[②] 因而，无论是欧盟委员会、成员国数据保护机构还是数据跨境流动的企业，在进行充分性评估时，均应当排除直接情报监控所依据的《行政命令》。

有鉴于此，欧盟在法律适用上存在双重标准之嫌。有美国学者认为，欧盟选择性执法，存在明显地缘倾向，对欧盟成员国、俄罗斯、英国和以色列这些国家的情报监控行为无动于衷。[③] 在个人权利的救济方面，欧盟成员国所提供的个人救济与美国相比并无二致，甚至低于美国，可欧盟法院却唯独针对美国。[④] 也有部分欧盟学者持此类观点，其分析道，若将美国的情报监控法律与法国的进行比较，可以发现法国情报监控法所服务的目的同样非常广泛，包括重要外交利益、重要经济产业以及科学研究利益等。出于这类目的，法国情报法律授权情报机构可进行大规模自动监控和定向监控，但这些情报活动并没有法院或独立行政机构对其进行事前审查。虽然法国已设置国家情报技术控制委员会，但该委员会的监督职能依靠外界的触发。这种事后监管机制作用甚微，委员会虽可通知民众是否存在违法监控，但无权直接制止该违法监控行为，仅能以向总理建议的方式发挥监督作用。[⑤]

### （二）数据保护监管由“基于风险”向“基于权利”路径的转变

欧盟法院通过司法裁决的方式，向欧盟各数据保护监管机构释放了数据趋严保护的信号。2020 年 11 月，欧盟数据保护委员会（European Data Protection Board）快速反应，连续发布《关于为确保遵守欧盟个人数据保护水平而采用的对数据跨境转移工具补充措施的第 01/2020 号建议（征求意见稿）》［Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data—version for public consultations，下文简称

① See *La Quadrature du Net and Others*, C－511/18; *Privacy International*, C－623/17.

② The United States, “Comments on Proposed SCC Decisions”, Privacy Shield Framework website, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000YFcs.

③ Kenneth Propp and Peter Swire, “Geopolitical Implications of the European Court's Schrems II Decision”, Lawfare Blog website, https://www.lawfareblog.com/geopolitical－implications－european－courts－schrems－ii－decision.

④ Kenneth Propp and Peter Swire, “After Schrems II: A Proposal to Meet the Individual Redress Challenge”, Lawfare Blog website, https://www.lawfareblog.com/after－schrems－ii－proposal－meet－individual－redress－challenge.

⑤ Theodore Christakis, “Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)”, European Law Blog website, https://europeanlawblog.eu/2021/04/13/squaring－the－circle－international－surveillance－underwater－cables－and－eu－us－adequacy－negotiations－part2/.

《补充措施建议（征求意见稿）》］与《关于针对监控措施的欧洲基本保障的第 02/2020 号建议》（Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures，下文简称《监控措施建议》），将欧盟法院严格保护个人数据权利的意志落实为 6 步可操作性规则指南（如表 1 所示），指导涉欧盟数据跨境流动的企业合规和成员国数据保护机构执法。

**表 1　欧盟数据保护委员会数据跨境流动合规指南**

| 合规流程 | | 具体内容 | |
|---|---|---|---|
| 步骤一 | 了解数据跨境的具体场景 | 重点了解个人数据的去向、数据转移的充分性与必要性等 | |
| 步骤二 | 选择跨境转移工具 | 可选择的工具包括：充分性决定；标准合同条款、可约束性公司规则、行为守则、认证机制、特别合同条款；克减条款 | |
| 步骤三 | 转移工具充分性保护的全面评估 | 数据跨境转移法律风险评估因素包括转移目的、处理者类型、所在部门领域、数据类别、数据格式、数据存储地、数据再转移的可能性等 | |
| | | 特别关注与公共部门获取数据或要求披露数据的相关法律及救济权利，对此，《监控措施建议》提供具体标准以评估第三国情报监控活动是否构成对个人数据基本权利的过度干预 | 第一，情报监控所涉及的数据处理应以明确、准确和易懂的规则为基础，使公民充分了解在什么情形以及什么条件下公共当局有权采取监控措施 |
| | | | 第二，需要证明所追求合法目的的必要性和相称性 |
| | | | 第三，应有一个独立的监督机制 |
| | | | 第四，需要向个人提供有效的救济措施 |
| | | 是否有全面的数据保护法或独立的数据保护机构 | |
| | | 评估范围不仅仅包括公开的立法，如有必要还须立足既往先例、政府权力、技术、财力等 | |
| 步骤四 | 未充分保护的补充措施 | 仅凭双方的合同或组织管理措施，一般难以解决第三国公共当局获取个人数据的问题，只有技术性措施才能阻止数据访问或监控行为，加强对数据的整体保护 | |
| 步骤五 | 补充措施后的程序性要求 | 对标准合同条款而言，不需要取得数据保护机构的授权；对可约束性公司规则与特别合同条款而言，欧盟数据保护委员会还在进一步讨论 | |
| 步骤六 | 周期性再评估 | 如数据接收方违反或无法履行标准合同条款；补充措施在第三国不再有效 | |

［本表由笔者根据欧盟数据保护委员会发布的《补充措施建议（征求意见稿）》和《监控措施建议》制作。］

从个人数据的概念、数据处理的合法事由、数据控制者或处理者的影响评估义务，以及数据保护机构的处罚等方面来看，GDPR 采取了“基于风险”路径的数据保护策略。[①] “基于风险”路径的充分性评估，可根据风险大小采取不同程度的合规标准，如对于风险较小的场景采取合同或组织管理的补充措施即可，对于风险较大的场景，则必须通过安全性更高的技术性措施予以补充。美国政府极力主张充分性评估应当坚持“基于风险”的路径，但受欧盟法院裁决的影响，欧盟数据保护委员会似乎偏离了 GDPR“基于风险”路径的立场，而转向“基于权利”路径。[②] “基于权利”路径的充分性评估，过度重视数据权利的保护，对风险持零容忍态度，即使是风险系数极低的场景，亦一刀切地采取严格的保护标准。因此，当数据存在任何可能被政府非法获取的风险时，无论风险高低，均需要通过“步骤四”的补充措施加以消除。欧盟数据保护委员会

① 洪延青：《解锁 GDPR 的正确姿势：风险路径》，载《中国信息安全》2018 年第 7 期，第 38—40 页。

② Theodore Christakis，“Schrems III? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers（Part 2）”，European Law Blog website，https：//europeanlawblog. eu/2020/11/16/schrems – iii – first – thoughts – on – the – EDPB – post – schrems – ii – recommendations – on – international – data – transfers – part – 2/.

认为仅仅通过合同或组织管理措施，无法从根本上消除数据被政府恣意调取的风险，还必须通过技术性措施使数据不可被自身以外的其他实体解读，从而彻底消除潜在风险。

2021 年 6 月，欧盟数据保护委员会在吸收社会意见之后正式通过了《补充措施建议》。正式通过的版本中，欧盟数据保护委员会在追求“基于权利”的风险零容忍立场上有所松动。《补充措施建议》放弃征求意见稿坚持的纯客观因素的风险零容忍评估，而采取了包含主观因素的评估。步骤三中，若数据控制者或处理者认为第三国某部法律不可能适用于特定的数据跨境流动场景时，该法律可免于充分性评估。虽然欧盟数据保护委员会纳入了充分性评估的主观因素，但要排除对一部法律的评估，数据控制者或处理者需要承担非常繁重的证明责任，如需从法律上证明这部法律不适用此种场景，需结合自身实践证明是否收到过政府数据访问请求、是否被禁止披露政府请求，以及同行业是否存在类似经历等，最终形成详细的评估报告。这种风险零容忍立场的松动，一定程度上回应了美国关于数据保护充分性问题的抗辩，[①] 但实质上仍未改变欧盟数据保护委员会严格的充分性评估立场。欧盟成员国数据保护机构受其影响，在数据跨境传输场景下对“基于风险”的路径持否定立场，如奥地利数据保护机构认定企业在涉欧数据跨境场景中使用“谷歌分析”（Google Analytics）的行为违法。[②]

### （三）欧盟委员会“基于风险”路径的再谈判

不同于欧盟法院与欧盟数据保护委员会以保护个人数据基本权利为其核心职能，欧盟委员会因其偏重经济发展的职能定位，始终秉持着较为宽容的数据保护立场。欧盟委员会必须考虑美欧之间巨大的数字经济贸易体量在欧盟经济中的重要地位，而“基于权利”路径的数据保护明显不利于美欧数字经济的发展。在安全港与隐私盾事件之后，为尽快恢复跨大西洋数字经济贸易，欧盟委员会采取“基于风险”路径，积极促成与美国之间达成新的数据跨境传输框架。2022 年 3 月，欧盟委员会与美国达成跨大西洋数据隐私框架（Trans-Atlantic Data Privacy Framework）的原则性协议，同年 12 月，欧盟委员会便制定公布了《关于欧美数据隐私框架的充分性决定（草案）》，[③] 并于 2023 年 7 月 10 日正式通过该草案。

在美欧 3 年漫长的谈判中，正是因为欧盟委员会秉持“基于风险”路径的数据保护立场，谈判才可能得以进行并取得成功。受欧盟法院判决影响，欧盟委员会一般会适度拔高数据保护标准，限缩其对风险的容忍空间。美国也正是在欧盟委员会不断限缩的风险容忍空间中，提高其数据保护水平。例如，美国从最初仅设置非独立的隐私专员救济机制，到如今设置以数据保护审查法院为核心的双层救济机制。虽然欧盟委员会在数据保护方面更容易妥协，但在每一次谈判中，

---

① 2020 年 9 月，鉴于大部分中小企业自身并无能力详细评估国内数据保护法律制度，美国商务部、司法部以及国家情报部门联合发布针对标准合同条款等机制的合规参考文件，为企业进行充分性评估提供权威参考，以应对欧盟法院施加给企业对第三国进行充分性评估的义务。See “White Paper: Information on U. S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U. S. Data Transfers after Schrems II”, U. S. Department of Commerce, https://www. commerce. gov/sites/default/files/2020 - 09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT. PDF.

② “UPDATE on noyb's 101 complaints: Austrian DPA rejects ‘risk based approach’ for data transfers to third countries”, NOYB website, https://noyb. eu/en/update - noybs - 101 - complaints - austrian - dpa - rejects - risk - based - approach - data - transfers - third - countries.

③ “Adequacy Decision for the EU-US Data Privacy Framework”, European Commission, https://commission. europa. eu/system/files/2022 - 12/Draft%20adequacy%20decision%20on%20EU - US%20Data%20Privacy%20Framework_ 0. pdf.

欧盟委员会均切实提升了对流出至境外的个人数据的保护水平。

欧盟委员会以“基于风险”的相对宽松路径展开谈判，将第三国纳入其数据跨境流动法律机制之中，为欧盟法院与欧盟数据保护委员会适用更为严格的保护标准创造条件。欧盟委员会的“请君入瓮”，激活了欧盟法院的“裁判者”角色与欧盟数据保护委员会“执行者”角色。三者协同一体，牢牢掌握美欧数据跨境流动博弈中的主动权与话语权，共同服务于欧盟自身的战略利益。

## 三　重振欧洲：欧盟技术主权的战略布局

欧盟趋严适用数据跨境流动机制的原因，除为了增强对个人数据和隐私的基本权利保护力度之外，更是为了保障欧盟自身的政治和战略利益。美国等国家信息技术产业对欧盟市场的控制和侵蚀，威胁到欧盟在大数据、人工智能时代的技术自主权和发展权。凭借自身在规则领域的先发优势，欧盟力图利用其规制能力扭转逆局，夺回技术主权。

### （一）美国技术控制战略侵蚀欧盟技术主权

美国所实行的技术控制战略，主要以本国跨国科技企业对全球数据市场所形成的技术和产业控制力作为媒介，实现对另一国技术产业发展的控制和遏制。在大数据和人工智能时代，技术控制实现的底层逻辑是对数据的占有和控制，控制数据的供给无异于扼制技术发展的咽喉。因此，美国的技术控制，最直接表现为对全球数据的实际控制：一是假借数据跨境自由流动之名攫取他国数据；二是以“长臂管辖”为法律武器，变跨国科技企业对他国数据的技术控制力为国家控制权力。以下分述之。

数据跨境的自由流动呈现由技术洼地向技术高地流动的规律，并表现出数据规模聚集的“马太效应”现象。美国科技产业实力盘踞榜首，在互联网科技领域，美国拥有全球最具影响力的互联网科技公司以及雄厚的科技实力。早在 2018 年，全球排名前 20 的互联网公司中，属于美国的公司就有 12 家，且排名前 5 的公司均属于美国。[①] 2021 年 6 月统计称，苹果、亚马逊、字母表、微软、脸书等巨头各自的全球市场总值已经超越全球 90% 以上国家的 GDP 总值。[②] 跨国公司开展全球业务依赖数据跨境流动，而数据跨境的自然流动会造成全球数据以美国为中心汇聚的事实。为巩固和扩大此种事实局面，美国在双边和多边国际合作层面取得实质成效。[③] 例如，美国利用自身威势参与国际谈判，迫使他国签订《美日数字贸易协定》《美墨加协定》等为代表的国际协定，禁止他国设置阻碍数据跨境流动的数据本地化保护措施；借助亚太经合组织合作平

① 美国华尔街专家通过衡量全球各大互联网公司的市场估值，统计得出全球 20 大互联网科技公司中，美国占据 12 家之多，剩余 8 家为中国所占，苹果、亚马逊、字母表、微软、脸书位列榜单前五。See Jeff Desjardins, “Visualizing the World’s 20 Largest Tech Giants”, Visual Capitalist website, https://www.visualcapitalist.com/visualizing-worlds-20-largest-tech-giants/.

② 以苹果和微软为例，前者全球市场估值约为 2.1 万亿美元，仅次于美、中、日、德、印、英、法 7 国；后者估值为 1.9 万亿美元，仅次于以上 7 国和意大利。See Omri Wallach, “The World’s Tech Giants, Compared to the Size of Economies”, Visual Capitalist website, https://www.visualcapitalist.com/the-tech-giants-worth-compared-economies-countries/.

③ 许多奇：《治理跨境数据流动的贸易规则体系构建》，载《行政法学研究》2022 年第 4 期，第 53 页。

台，将以《APEC 隐私框架》为核心的低水平保护标准嵌入 APEC 跨境隐私规则（Cross-Border Privacy Rules，下文简称 CBPR）体系，力图将低门槛数据跨境流动规则从区域推向全球，[①] 以降低全球各国数据高标准保护壁垒。

美国立法、执法和司法三位一体的“长臂管辖”，将企业对境外数据的控制力转化为国家的控制力。立法上，通过《澄清境外合法使用数据法》（Clarifying Lawful Overseas Use of Data Act），将《存储通讯法》（Stored Communication Act）的“数据存储地”管辖标准变为“数据控制者”标准，赋予执法机构域外执法管辖权；执法上，执法机构通过行政令等方式强令国内的跨国科技企业配合调取境外数据，以实现对海外存储数据的控制，跨国公司不得再以数据存储于境外为由拒绝执法机关的数据调取命令。[②] 司法上，在“雅虎法国案”[③]“谷歌加拿大知识产权案”[④] 等案件中，雅虎、谷歌等科技企业的美国身份，导致法国、加拿大等国法院的涉数据判决执行受到美国法限制，而美国法院判决的域外效力则可以凭借跨国科技公司的美国身份而得以实现。[⑤]

面对美国等国家的跨国科技企业在欧盟数字市场份额的日趋增长，欧盟境内数据不仅加速外流，更受到他国国家权力的渗透与控制。本土科技企业的生存与创新空间受到严重挤压，欧盟对本土数据和技术的控制能力逐渐被美国削弱。受欧洲实力相对衰弱、世界地缘政治重心从大西洋转向亚太的影响，欧盟强烈意识到自身在世界政治舞台上正逐渐被边缘化。为重整欧洲实力，以冯德莱恩（Ursula von der Leyen）为首的一届欧盟委员会开始尝试有限偏离单纯依赖规则力量的原初轨道，逐步转向地缘现实主义，着重提升自身的科技硬实力。[⑥] 欧洲地缘政治上的战略定位体现在数据和技术等领域则催生出“数据主权”“技术主权”等理念，其战略目标是使欧洲摆脱美国等国的“数字殖民”，[⑦] 夺回对本土数据和技术的自主控制权力。换言之，实施技术主权战略不仅仅为了争取更多数字贸易利益，也是为了在互联网时代取得有利于国家安全所需的位置，对于拥有数字技术能力的欧盟来说，这是其提出技术主权战略的重要动机。[⑧]

### （二）欧盟技术主权战略布局

2020 年 2 月，冯德莱恩正式提出“技术主权”概念，其意指欧盟“根据自己的价值观并遵守自己的规则来做出自己选择”的能力。[⑨] 欧盟希望在人工智能、量子计算、网络安全、电池、氢能源等关键性或颠覆性领域，减少依赖外来技术，占据制定标准的领导地位，培育和支持欧洲

---

① 2022 年 4 月 21 日，美国与参与亚太经合组织 CBPR 体系的经济体宣布建立“全球跨境隐私规则体系”（Global Cross-Border Privacy Rules System），其实质是将区域性的 CBPR 体系转变为全球所有国家或经济体均可加入的体系。See “Global Cross-Border Privacy Rules Declaration”, U. S. Department of Commerce, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

② Miranda Rutherford, “The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access”, (2019) 34 *Berkeley Technology Law Journal* 1177, p. 1178.

③ See *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181 (2001).

④ See *Google LLC v. Equustek Sols. Inc.*, 2017 U. S. Dist. LEXIS 182194.

⑤ 杨永红：《美国域外数据管辖权研究》，载《法商研究》2022 年第 2 期，第 151 页。

⑥ 解楠楠、张晓通：《“地缘政治欧洲”：欧盟力量的地缘政治转向?》，载《欧洲研究》2020 年第 2 期，第 5 页。

⑦ 刘皓琰：《当代左翼数字殖民主义理论评介》，载《当代世界与社会主义》2021 年第 2 期，第 114 页。

⑧ 沈玉良：《数字贸易发展转折点：技术与规则之争——全球数字贸易促进指数分析报告（2021）》，载《世界经济研究》2022 年第 5 期，第 10 页。

⑨ Ursula von der Leyen, “Shaping Europe's Digital Future”, Modern Diplomacy website, https://moderndiplomacy.eu/2020/02/21/shaping-europes-digital-future/.

的创新企业。实现技术主权战略，需要欧盟通过定义并捍卫自身的规则和价值观，在数字时代牢牢掌握全球数据保护的规则话语权和塑造力，以规则话语权为武器保障技术发展。

鉴于本文立足数字经济与数据跨境流动背景，下文将主要以人工智能技术为例展开论述。2020年2月，欧盟同时发布《塑造欧洲的数字未来》（Shaping Europe's Digital Future）、《欧洲数据战略》（European Strategy for Data）和《人工智能白皮书》（White Paper on Artificial Intelligence）。这3份文件奠定了数字时代人工智能领域欧盟的“技术主权”战略路线。①

1. 战略目标：培育人工智能技术产业

欧盟的技术主权战略，是以规则和价值塑造为先导和武器推进实施的。因此，在发展人工智能技术产业上，欧盟首先通过构建和完善本土人工智能技术的法治规范环境，抢占该领域的规则话语权，再运用规则话语权削弱外国企业在本土的市场竞争力，为本土人工智能与数据企业创造良好的市场竞争环境。

一方面，欧盟为培育本土人工智能技术产业营造良好的法治环境。政策上，自2018年发布《欧洲人工智能战略》（Artificial Intelligence for Europe）以来，欧盟通过了一系列政策性战略文件，典型如2018年和2021年陆续发布的两版《人工智能协调计划》（Coordinated Plan on Artificial Intelligence），2019年《可信人工智能伦理指南》（Ethics Guidelines for Trustworthy AI），以及上文提及的《人工智能白皮书》等。这些政策文件及其配套举措勾勒出欧盟在坚持以人为本、可信任、可持续等价值和规则基础上，力图成为人工智能领域执牛耳者的野心。与之相呼应，法律上，欧盟在2021年制定《人工智能法（草案）》（Proposal for an Artificial Intelligence Act）。② 为促进AI的发展与应用，该法案采取“基于风险”的规制路径，将AI系统按照应用场景的风险高低分为4个等级：最低风险、有限风险、高风险和不可接受的风险。实践中大部分AI系统会被划入前两个风险等级，法律仅对这类AI系统施加少量限制或不做限制。针对可能严重影响人们安全与生活的高风险场景AI系统，如交通基础设施、教育或职业培训、移民管理、医疗辅助等场景下的AI系统，只有在具备符合规定的风险管理系统、透明度、人力监督、数据质量和网络安全条件下才能使用。对于利用潜意识技术或操纵欺骗技术、利用个人弱点或人格特征、利用社会评分等造成个人损害的场景，以及在公共场所进行实时远程生物识别的场景，则禁止使用AI系统。此外，AI归责是横亘在AI大规模应用之前必须予以解决的问题。2022年9月欧盟委员会发布了《人工智能责任指令（草案）》（Proposal for an AI Liability Directive）和《缺陷产品责任指令（草案）》（Proposal for a Directive on Liability for Defective Products）。前者对因个人过错致使AI系统对他人造成的损害，适用“过错责任”的归责原则；后者对因人工智能系统缺陷而非个人过失造成损害的归责，确立“无过错责任”的归责原则。明确人工智能的归责机制，可增强公众对人工智能技术的信任，并为参与开发这些系统的企业提供法律上的确定性。③

---

① 洪延青、朱玲凤、张朝、谢晨曦：《欧盟提出“技术主权”概念，引领欧盟数字化转型战略》，载《中国信息安全》2020年第3期，第70—74页。

② European Commission, “Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative ACTS”, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

③ Samar Abbas Nawaz, “The Proposed EU AI Liability Rules: Ease or Burden?”, European Law Blog website, https://europeanlawblog.eu/2022/11/07/the-proposed-eu-ai-liability-rules-ease-or-burden/.

另一方面，欧盟借“公平贸易”之名打击外国寡头科技企业的市场垄断，扶植欧盟企业。[①] 考虑到欧盟数字服务市场中以美国企业为代表的外国科技企业拥有巨大统治力，挤压本土数字企业的生存与发展空间，欧洲议会 2021 年 12 月表决通过《数字市场法》（Digital Markets Act），又于 2022 年 1 月通过《数字服务法》（Digital Services Act），这凸显了欧盟保护自身企业发展、打击外国科技巨头的战略意图。[②] 虽然两部法律的立法目的是通过规制网络平台，创造更加安全、公平、更具有创新活力的数字服务市场，但前者为 4 类在线中介服务平台逐级累加繁重的合规义务（尤其是超大型平台），后者明确对具有“守门人”资格的大型平台列举了要求其实施的事项和禁止其实施的事项，此类监管规则具有鲜明的目标导向，直指脸书、谷歌和亚马逊等美国互联网巨头。两部法律针对大型平台设置繁重的合规义务和严苛的罚则，为欧盟战略性执法铺平了道路。欧盟可以借此打击美国科技巨头在欧盟单一市场的势力，扶持欧盟内部的中小型科技企业。

根据《人工智能白皮书》，为弥补欧盟在人工智能技术领域的短板，欧盟在注重监管的同时，也将重点从加强对该领域的投资、加大人工智能人才的汇聚和培养、加快人工智能技术的实践应用、增强计算基础设施的建设保障等方面推进人工智能技术的迭代更新。

2. 战略支柱：掌控海量的数据资源

人工智能技术作为数字时代的领先技术，其发展速度与算法训练的数据体量呈正向关系。缺少《欧洲数据战略》构建的巨量数据资源池，《人工智能白皮书》所力求实现的技术突进愿景便难以实现。为增加可用数据体量和质量，欧盟采取“内外有别”的数据流动规制策略，对内促进共享和利用，对外严格限制数据流出。

一方面，对内开源。欧盟通过 GDPR 和《非个人数据自由流动条例》（Regulation on the Free Flow of Non-Personal Data）形成欧盟层面关于个人数据与非个人数据流动的单一法律空间，消除因成员国之间法律差异造成的数据跨境流动制度壁垒，最大限度促进数据流动，汇聚数据资源。欧盟在《欧洲数据战略》中强调，要建立包括工业、环境、出行、健康、金融、能源、农业、公共管理、技能等九大公共领域在内的欧洲单一数据空间，以充分发掘欧盟数据的聚合价值。欧盟通过《数据治理法》（Data Governance Act）和《数据法》（Data Act）进一步完善境内数据流动和利用制度。前者通过框定公共部门数据再利用机制、数据中介机构制度和数据利他主义制度这三大数据共享机制，为公共数据与社会数据的共享利用打下制度根基；后者则进一步聚焦非个人数据，通过强制互联网产品的制造商和数字服务提供商（如亚马逊、微软、特斯拉等科技巨头）共享数据，将巨量的商业与工业数据释放于数据资源池，供中小企业和用户开发利用。

另一方面，对外节流。根据《欧洲数据战略》要求，在规制数据跨境流出时，欧盟必须保证所涉行为符合欧盟立法和价值观。在个人数据跨境流出场景中，欧盟通过 GDPR 第五章数据跨境流动法律机制，前置性从严审查第三国是否能提供与欧盟等同的充分性保护。在非个人数据流出场景中，欧盟通过《数据治理法》和《数据法》同样设置了事前的严格审查，重点对第三国

① 金晶：《欧盟的规则，全球的标准？——数据跨境流动监管的“逐顶竞争”》，载《中外法学》2023 年第 1 期，第 51 页。

② 《数字市场法》已于 2022 年 11 月 1 日生效，2023 年 5 月 2 日起实施；《数字服务法》也已于 2022 年 11 月 16 日生效，2024 年 2 月 17 日起全面实施。

数据保护水平评估指标、机密数据与受知识产权保护数据流出要求、高度敏感性数据流出的特殊限制等予以严苛的规定和审查。[①]

## 四　美欧数据跨境流动中欧盟技术主权的实现路径

美欧数据跨境流动博弈中，欧盟技术主权战略昭然若揭：最大限度将数据留存于欧盟境内，迫使美国科技巨头释放数据，并削弱其市场竞争力，以数据培育本土数字技术企业发展，从而牢牢掌握数据与技术的控制权。欧盟强大的规则制定和影响能力，成为实现此种战略的重要工具。《隐私盾决定》无效事件，无疑是实现该战略的一个微观缩影和代表性案例。

### （一）掌控数据领域的规则话语权

据数据保护权威学者格林利夫（Graham Greenleaf）教授统计，截至2023年3月，全球已有162个国家制定了数据隐私法律，[②] 其中大部分国家均效仿和移植欧盟数据保护法，如巴西、日本、南非、韩国等这类大型经济体国家和区域强国，哥伦比亚、泰国等中等经济体国家，甚至如百慕大群岛这类小岛地区。[③] 这种欧盟数据保护法律的全球扩散现象彰显和强化了欧盟GDPR的统治地位。[④] 2020年2月，欧盟在《塑造欧洲的数字未来》中宣告："世界上多数国家都已将自己的立法朝着欧盟强大的数据保护制度接轨。"[⑤] 欧盟数据保护规则的全球影响力为世界所公认。[⑥] 布拉德福（Anu Bradford）教授指出，欧盟正利用其法律制度与标准将欧盟的规则影响力成功输向世界，获得一种前所未有的、被世人严重低估的全球性规制力量。这一现象也被布拉德福教授称之为"布鲁塞尔效应"（Brussels Effect）。[⑦]

欧盟何以规制世界，可以初步从以下5个角度作一系统解读。第一，市场规模（market size）。欧盟单一市场规模庞大，人口5.16亿，人均GDP为4万美元，消费市场前景广阔。[⑧] 第二，规制能力（regulatory capacity）。欧盟单一市场的建设赋予了欧盟机构制定和执行市场规则的广

---

① 黄钰：《非个人数据跨境流动监管模式研究》，载《情报杂志》2022年第12期，第114页。

② See Graham Greenleaf, "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills", (2023) 181 *Privacy Laws & Business International Report* 1.

③ Mark Scott & Laurens Cerulus, "Europe's New Data Protection Rules Export Privacy Standards Worldwide", Politico website, https://subscriber.politicopro.com/article/2018/01/europes-new-data-protection-rules-export-privacy-standards-worldwide-318721.

④ Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance (February 11, 2021)", (2021) 169 *Privacy Laws & Business International Report* 3, p. 5.

⑤ "Shaping Europe's Digital Future", European Commission, https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278.

⑥ See Paul M. Schwartz, "Global Data Privacy: The EU Way", (2019) 94 *New York University Law Review* 771.

⑦ See Anu Bradford, "The Brussels Effect", (2012) 107 *Northwestern University Law Review* 1.

⑧ 2018年，欧盟占全球国内收入总值超20%，欧盟区域内生产总值17万亿美元（美国为19万亿、中国12万亿、日本5万亿），世界第二大货物进口区和最大服务进口区。欧盟区域人口5.16亿（消费者市场），人均GDP为40900美元；美国3.27亿人，人均GDP为59500美元；中国14亿人，人均GDP为16700美元；印度12亿人，人均GDP为7200美元。欧盟市场占俄罗斯、南非、中国、美国、印度和巴西的出口比例分别是43%、31%、22%、21%、19%和18%。See Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020), pp. 27-29.

泛权力，欧盟机构职员数量的增长、专业素质以及共同的使命感和身份认同感，保证了欧盟具有强大的规则制定和执行能力。第三，严格规制（stringent regulations）。在规制理念上，欧盟更信任政府干预，以“事前风险预防”作为指导原则实行严格的行政规制，制定全球高水平数据保护标准。第四，非弹性目标（inelastic targets）。若要进入欧盟市场，域外企业无法规避适用欧盟的数据保护法律。第五，不可分性（non-divisibility）。域外企业为遵守欧盟高标准规则，出于法律、技术和经济等考虑只能在全球范围内提升合规标准：在法律层面，跨国公司为顺利开展全球业务，规避不确定性的法律风险，会统一公司内部的合规政策，以域外业务中合规标准最高的国家的法律为基准；[①] 在技术层面，跨国公司将产品或服务的合规模式根据市场的不同进行分割在技术上是困难的；经济层面，跨国公司如果区分不同国家的市场进行差异化合规，从规模经济视角评判，这种合规模式的成本会非常高昂。且品牌和商誉上，跨国公司统一采用世界公认最高的合规标准，有利于增强消费者信心。[②] 经济上无法放弃欧盟市场，且忌惮于欧盟高昂违法成本，欧盟这种市场强制力量最终使欧盟规则通过私人法律移植方式输送至全球其他国家。[③] 概言之，欧盟凭借市场力量（market power）、[④] 规范性力量（normative power）[⑤] 以及《个人数据自动化处理中的个人保护公约》（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data，通称《108 号公约》）等发挥的观念性力量（ideational power）[⑥]，将其高标准数据保护规则施加于跨国公司，并借此渗透至其他国家，实现欧盟规则的全球化扩张和话语权的增强。

因其主要依赖于跨国企业主动推进本国市场法律规则向高标准靠拢，故欧盟的布鲁塞尔效应并未表现出明显的强制性。欧盟增强规则话语权的另一重要途径——通过 GDPR 适用范围条款扩大数据保护法的域外效力，则具有明显的强制性。[⑦] 以 2014 年“谷歌西班牙案”为契机，[⑧] 2016 年 GDPR 在 1995 年《数据保护指令》基础上大幅扩张其域外适用范围：第一，进一步加强“管辖境内实体”的属地管辖原则，即使数据处理行为发生于境外，亦划归 GDPR 管辖；第二，以客观属地原则为补充，即使境内无实体，但其数据处理行为旨在为境内数据主体提供商品或服务，或者监控境内数据主体，GDPR 均可管辖；第三，管辖对象不仅限于数据控制者，还包括数据处理者。欧盟法域外效力的扩张在实现更好保护欧盟利益的同时，还能增强欧盟规则的强制输出，不断提升该领域规则制定的国际话语权。以 2018 年“英国数据保护机构 ICO 对加拿大公司 AIQ 域外执法案”为例，[⑨] AIQ 涉嫌帮助剑桥分析（Cambridge Analytica）处理欧盟公民的脸书账号信

① Thomas Schultz，“Carving up the Internet：Jurisdiction，Legal Orders，and the Private/Public International Law Interface”，（2008）19 *European Journal of International Law* 799，pp. 813 – 814.

② Anu Bradford，*The Brussels Effect*：*How the European Union Rules the World*（Oxford University Press，2020），pp. 56 – 62.

③ 金晶：《欧盟的规则，全球的标准？——数据跨境流动监管的“逐顶竞争”》，载《中外法学》2023 年第 1 期，第 57 页。

④ See Chad Damro，“Market power Europe”，（2012）19 *Journal of European Public Policy* 682.

⑤ See Manners Ian，“Normative Power Europe：A Contradiction in Terms?”，（2002）40 *Journal of Common Market Studies* 235.

⑥ See Lee A. Bygrave，“The ‘Strasbourg Effect’ on Data Protection in Light of the ‘Brussels Effect’：Logic，Mechanics and Prospects”，（2021）40 *Computer Law & Security Review* 1.

⑦ 《人工智能法（草案）》同样设置了域外管辖条款，无论人工智能产品的提供者身处何处，只要其生产的人工智能系统运用于欧盟境内，就落入其管辖范围。

⑧ See *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos*（*AEPD*）*and Mario Costeja González*，C – 131/12.

⑨ 俞胜杰、林燕萍：《〈通用数据保护条例〉域外效力的规制逻辑、实践反思与立法启示》，载《重庆社会科学》2020 年第 6 期，第 73 页。

息并进行民意分析，ICO 认为其构成对欧盟境内公民的监控，并勒令停止处理并删除所有英国公民的个人数据，最终 AIQ 迫于高额违法成本不得不服从 ICO 的执法要求。此案作为 GDPR 域外执法第一案具有深远意义，GDPR 或将成为全球数据科技企业挥之不去的“梦魇”。

### （二）利用规则话语权实现软数据本地化

美国依托其技术实力优势，尽可能降低他国数据保护水平，扫清数据流动壁垒，实现数据向美国汇聚；在巩固和强化美国公司对全球数据掌控的同时，压缩了各国自主选择数据保护水平的规制空间。[①] 作为回应，欧盟利用其数据保护规则解释的话语权，掌控博弈主导权，控制美欧数据跨境流动朝符合欧盟战略利益的方向发展。

1. 非平等博弈：美国陷入合规陷阱

美欧博弈场域框定于欧盟搭建的 GDPR 数据跨境流动法律机制之中，欧盟借此将国家之间的数据跨境流动，转化为欧盟内部的数据传输。[②] 为何美国会陷入欧盟主导的规则体系之中，一方面是因为美国的互联网科技产业虽然大幅领先欧盟，但却高度依赖欧盟单一市场。例如，脸书在欧盟拥有 2.77 亿的日活用户，远多于美国本土，欧洲的广告收入占其全球收入总额的 24%；谷歌在欧盟搜索市场的份额超 90%，而其在美国的份额只有 67%—75%；欧洲、中东、非洲的广告收入占谷歌 2017 年总收入的 33%；亚马逊的网络销售额仅德国和英国就贡献了 280 亿美元，约占亚马逊全球销售额的 16%。[③] 即便作为合规者被迫迎合欧盟高标准规则，美国也毫不减损帮助其科技企业进军欧盟数字市场的意愿。另一方面，欧盟委员会不同于欧盟法院与欧盟数据保护委员会对数据保护的严苛立场，对数据保护风险持更为宽容的态度，使得美欧谈判的进行以及后续的成功得以成为可能。换言之，正是欧盟委员会采取“基于风险”路径的谈判策略，使美国进入欧盟主导的博弈场域成为现实。欧盟委员会的此种策略，既避免了美欧之间数字经贸的中断，又为欧盟法院与欧盟数据保护委员会保护个人数据基本权利提供了靶标。

值得指出的是，在数据跨境流动领域，国内部分学者可能会倾向使用安全港或隐私盾“协议”来指代美欧之间的数据跨境流动框架。[④] 本文认为“协议”一词的使用可能有失妥当，易掩盖数据跨境流动领域美欧之间不平等博弈的事实。国际法上，“协议”一般是指平等主体的国家之间签订的双多边条约。严格意义上，隐私盾框架并非美欧基于平等国际主体地位而缔结的确立其相互权利、义务的国际书面协议，[⑤] 而是以美国作为合规者、内嵌并依附于欧盟委员会作出的

---

① 洪延青：《推进“一带一路”数据跨境流动的中国方案——以美欧范式为背景的展开》，载《中国法律评论》2021 年第 2 期，第 42 页。

② 赵精武：《数据跨境传输中标准化合同的建构基础与监管转型》，载《法律科学（西北政法大学学报）》2022 年第 2 期，第 153 页。

③ Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020), p. 29.

④ 参见马芳：《美欧跨境信息〈安全港协议〉的存废及影响》，载《中国信息安全》2015 年第 11 期；曹杰、王晶：《数据跨境流动规则分析——以欧美隐私盾协议为视角》，载《国际经贸探索》2017 年第 4 期；黄志雄、韦欣妤：《美欧数据跨境流动规则博弈及中国因应——以〈隐私盾协议〉无效判决为视角》，载《同济大学学报（社会科学版）》2021 年第 2 期；丁汉韬：《大数据时代下个人信息保护法的域外效力边界》，载《中国国际私法与比较法年刊》第 24 卷，法律出版社 2019 年版。

⑤ 《关于国家和国际组织间或国际组织相互间条约法的维也纳公约》第 2 条关于“条约”的定义是：“‘条约’指一个或更多国家和一个或更多国际组织间，或国际组织相互间以书面缔结并受国际法支配的国际协议，不论其载于一项单独的文书或两项或更多有关的文书内，也不论其特定的名称为何。”

《隐私盾决定》的一套特殊的数据跨境流动制度框架。使用“协议”一词可能掩盖隐私盾框架的不平等性和单边性本质，也无法解释欧盟法院得以单方裁决具有“双边条约”性质的“隐私盾协议”无效这一有违国际法的事件。有学者也指出，尽管裁决欧盟委员会决定无效这一事实，实质造成了欧盟法院对外国法律进行评估的客观后果，但这并非国际法问题。①

2. 欧盟利用规则解释的主动权

欧盟作为数据跨境流动博弈规则的制定者、解释者与实施者，对博弈进程持有主导权。哈特曾指出，法律语言本身是一种开放结构，法律语言在含义上有一个确定的核心，但同时也具有边缘的不确定性。② 因此，在既定规则体系之下，欧盟个人数据保护标准作为司法审查的基准，非常灵活且具有较大的自由裁量空间，欧盟法院以及数据保护机构可通过对“实质同等”概念边缘的宽严解释，以实现特定的政治目的。③ 从美欧谈判博弈发展历史可探知，欧盟通过立法、司法与执法的协同作用，正不断推动美国国内数据保护标准的提高。这种现象，可借用经济学术语“棘轮效应”描述，其原指人的消费习惯形成之后具有不可逆性，易向上调整，而难以向下调整。若将数据隐私视为奢侈品，一旦美国开始接受欧盟数据隐私保护高标准，惠及每一位公民的数据隐私保护标准将难以降低。④ 面对欧盟不断升级的数据保护要求，无论是觊觎欧盟巨大数字单一市场，还是满足民众对数据隐私高标准保护需求，美国以自身实践表明，其会继续以被动的合规者身份寻求同欧盟合作。

美欧谈判进展显示，为回应欧盟法院在《隐私盾决定》裁决中提出的无效理由，2022 年 10 月，美国总统专门发布《加强美国情报活动监管的行政命令》（Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities），⑤ 该命令针对情报监控活动的限制问题，采用“白名单 + 黑名单”的方式，严格限制政府部门开展情报活动的目的范围；针对缺乏有效权利救济问题，建立两级补救机制，欧盟居民可向新设的公民自由保护官投诉，对处理结果不满，可向数据保护审查法院寻求司法救济。这些制度最终反映在欧盟委员会《关于欧盟—美国数据隐私框架的充分性决定》之中。与安全港废止后的隐私盾谈判阶段相比，这一阶段美国承诺的数据保护标准得到进一步提升。

3. 导向软数据本地化

技术主权战略之下欧盟对规则的运用，可能隐藏着欧盟“数据本地化”的战略意图。有学者将这种实践称之为软数据本地化（soft data localization），⑥ 即虽然欧盟规则和欧盟法院均没有明确主张数据本地化，但其一系列的规则解释和适用使得数据本地化成为企业唯一可选的道路。除数据本地化外，企业的其他任何合规措施均存在违法风险，这种合规的不确定性最终会导致企

① Theodore Christakis and Fabien Terpan, “EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options”, (2021) 11 *International Data Privacy Law* 81, p. 100.

② H. L. A. Hart, *The Concept of Law* (Clarendon Press, 2nd edn, 1994), p. 134.

③ 金晶：《欧盟的规则，全球的标准？——数据跨境流动监管的“逐顶竞争”》，载《中外法学》2023 年第 1 期，第 54 页。

④ Gregory Shaffer, “Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of US Privacy Standards”, (2000) 25 *The Yale Journal of International Law* 1, p. 83.

⑤ “Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities”, The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

⑥ Anupam Chander, “Is Data Localization a Solution for Schrems II?”, (2020) 23 *Journal of International Economic Law* 1, p. 6.

业不得不选择本地化留存数据，以消除跨境合规风险。[①]

与欧盟进行数据跨境流动，美国必须在情报监控立法等层面妥协，依欧盟标准重塑其国内法体系。美国若无法达到欧盟的充分性认定标准，企业虽可采取替代性的适当保障措施，但仍负有评估本国数据保护水平是否达到欧盟的充分性认定标准的义务。若企业经评估无法达到标准，欧盟留给企业唯一合规的道路便是跨境传输过程中采取技术保障措施，即任何人皆不可读的加密措施，但此种加密措施会导致数据失去再利用价值。第三国企业与欧盟的数据跨境流动业务将持续处于法律合规上的非稳定状态，欧盟数据保护机构的执法之剑时刻高悬于顶。为了摆脱这种非稳定状态，企业或考虑放弃欧洲的市场，或将数据存储于欧盟境内。据“*Schrems II* 案”后的最新进展，数据跨境传输失去隐私盾框架的庇护之后，脸书于 2023 年 5 月 12 日被爱尔兰数据保护机构处以 12 亿欧元的 GDPR 史上最高罚款，并被要求限期中止涉欧数据跨境传输。在长达两百多页的处罚决定书中，爱尔兰数据保护机构经详细论证后认为，美国法律并未提供实质等同于欧盟的保护标准，脸书所采用的各版本标准合同条款均无法弥补美国法律充分性保护之不足，且脸书也并未采取适当的补充措施。[②] 作为软数据本地化的另一现实例证，为应对隐私盾框架废止后的合规风险，微软于 2021 年 5 月 6 日宣布了一项名为“微软云的欧盟数据边界”（EU Data Boundary for the Microsoft Cloud）的新项目，其承诺欧盟客户的数据将在欧盟境内存储和处理。这一计划适用于微软核心云服务，包括 Azure、Dynamics 365 和 Microsoft 365 等。[③]

## 五　中国的因应之策

欧盟数据跨境流动法律机制在技术主权战略和欧盟法院的影响之下，呈现出武器化的政治工具色彩。[④] 欧盟善用其规则话语权，作出有利于实现其政治与经济目的的规则解释与适用。美国坚持在 GDPR 规则体系下开展与欧盟的数据跨境流动谈判合作，实质上处于“合规者”的被动地位，不断迎合欧盟的诉求，陷入棘轮效应的泥淖。中国数字经济产业发展兴盛，同样可能面临与美国类似的处境，对此应予以高度警惕和重视。

### （一）警惕欧盟技术主权战略下的数据跨境合规陷阱

由于双方价值理念以及监管模式的差异，中欧在数据跨境流动国际合作中存在较严重的信任缺失问题。[⑤] 依欧盟法院的裁决，无论采取欧盟提供的何种跨境转移法律工具，只要涉及欧盟居民数据处理，都必须对第三国整体的数据保护法制环境进行充分性评估。结合“隐私盾案”的

① 刘金瑞：《迈向数据跨境流动的全球规制：基本关切与中国方案》，载《行政法学研究》2022 年第 4 期，第 85 页。

② “Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation”, European Data Protection Board, https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission_en.

③ Brad Smith, “Answering Europe's Call: Storing and Processing EU Data in the EU”, Microsoft website, https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/.

④ See Jeffery Atik and Xavier Groussot, “A Weaponized Court of Justice in Schrems II”, (2021) 4 *Nordic Journal of European Law* 1.

⑤ 李墨丝：《中美欧博弈背景下的中欧数据跨境流动合作》，载《欧洲研究》2021 年第 6 期，第 15 页。

裁决逻辑，检视中国是否满足欧盟的充分性认定标准，结论通常是消极的。

一国情报监控法律是欧盟重点关注和评估的领域。中国情报监控领域的立法起步较晚，很长一段时间中国几无法律规范政府收集情报信息和秘密监控的行为，直到近年来《中华人民共和国国家安全法》（下文简称《国家安全法》）、《中华人民共和国国家情报法》（下文简称《国家情报法》）、《中华人民共和国反间谍法》（下文简称《反间谍法》）、《中华人民共和国反恐怖主义法》（下文简称《反恐怖主义法》）、《中华人民共和国网络安全法》（下文简称《网络安全法》）等法律的陆续颁布才初步搭建了一套法律框架。但这些法律中的相关规则多为概括性条款，[①] 对情报收集和秘密监控的一系列程序规范、适用对象和范围、救济与监督机制等缺乏具体规定，[②] 无法匹配欧盟数据保护委员会《监控措施建议》的 4 条审查标准。此外，由于欧盟等西方国家与中国在意识形态和政治体制方面存在显著差异，西方对中国法治的极端化误解短期难以消除。即便中国情报监控法律制度日渐完善，西方固有的偏见会成为充分性认定的意识形态障碍。欧盟充分性认定具有较大的主观性和强烈的政治色彩，中国极有可能受到欧盟的不合理对待。[③]

与欧盟严苛的数据保护立法相比，中国缺少专门的数据保护机构，在个人救济保障机制方面仍存在不足。《中华人民共和国个人信息保护法》（下文简称《个人信息保护法》）的出台弥补了中国在个人信息保护领域统一性立法的缺失，但与欧洲自 1970 年德国黑森州第一部数据保护法开始的长达半个世纪的立法经验相比，中国个人数据保护法治仍处于起步阶段。《个人信息保护法》与其他法律的关系定位、各项条款的具体实施细则、执法体系和救济路径的建设等仍有待进一步研究和探索。特别是在数据保护机构层面，实践中负责个人信息保护执法的主要是网信部门、公安部门、市场监管部门和工信部门，执法模式大多属于政策驱动式的运动性执法，未能形成常态化的执法机制，且各部门之间权责不清，执法效果大打折扣。[④] 若以欧盟已建立的专业化的独立数据保护机构及其“一站式”（one-stop-shop）执法机制为评估标准，[⑤] 中国难免遭到欧盟的批评和指责。

对中国出海企业而言，由于数据跨境流动国际规制的政治化[⑥]和阵营化，企业不得不采取切割市场的方式，规避因数据跨境流动带来的高额执法风险。实践中，如百度、阿里巴巴、腾讯、字节跳动、华为等大型科技企业均在欧盟境内设立分支机构，在欧盟本地存储各自所获取的欧盟

① 参见《国家安全法》第 51—54 条、第 81—82 条，《国家情报法》第 8—14 条，《反间谍法》第 13—17 条，《反恐怖主义法》第 43—48 条，《网络安全法》第 28 条等。

② 程雷：《大数据背景下的秘密监控与公民个人信息保护》，载《法学论坛》2021 年第 3 期，第 17—18 页。

③ 杨帆：《后“Schrems II 案”时期欧盟数据跨境流动法律监管的演进及我国的因应》，载《环球法律评论》2022 年第 1 期，第 186—187 页。

④ 杨帆、刘业：《个人信息保护的“公私并行”路径：我国法律实践与欧美启示》，载《国际经济法学刊》2021 年第 2 期，第 49—52 页。

⑤ 数据保护机构制度和“一站式”执法机制分别由 GDPR 第 6 章“独立监管机构”（independent supervisory authorities）与第 7 章“合作与一致性”（cooperation and consistency）专章设置。各成员国可设置一个或多个数据保护机构，专门负责推进 GDPR 实施。为增强 GDPR 在各成员国执法的一致性和有效性，GDPR 建立了各成员国数据保护机构的沟通合作机制，并由欧盟委员会和欧盟数据保护委员会统筹协调。针对存在管辖权积极冲突的案件，选定牵头数据保护机构，以其为中心协调解决案件，避免因“踢皮球”现象而使案件得不到及时有效处置。

⑥ 例如，在中概股赴美上市议题上，美国监管机构对涉及中国企业涉数据流动的审查标准存在明显政治化倾向。参见包柠榛：《中概股赴美上市的数据安全审视：风险来源、中美监管与应对》，载《东北师大学报（哲学社会科学版）》2023 年第 4 期，第 149—151 页。

居民个人数据。但这种切割经营模式会导致国内外数据、技术资源无法实现全球配置，容易削弱中国科技企业的全球竞争力。[①] 如果不进行切割，企业即使积极参与欧盟体系下的跨境合规，采取必要的合同、组织乃至技术措施，最大限度接近欧盟保护水平，仍无法消除欧盟的执法威胁。[②] 切割模式的经营成本高昂，实力较弱的中小型企业难以维持涉欧数据业务。因为欧盟配置的执法资源难以支撑自身在实践中全面贯彻法律，中小型企业的短期理性策略可能是在法律灰色区域内静待事态发展，维持其原有经营活动。[③] 但这并非企业发展长久之计，亟需在国家层面与欧盟协调数据跨境流动合作机制。

### （二）布局独立自主的数据跨境流动战略

隐私盾框架被废止后，有美国学者极力主张美国政府应当采取强硬姿态，与英国、澳大利亚、印度等国在数据领域达成统一战线以对抗欧盟，在国际法层面与欧盟达成平等的数据跨境流动国际协议，且欧盟应作出承诺不再因这些理由而威胁数据跨境流动的稳定性。[④] 这一论点揭示了欧盟的规则运作逻辑，对中国具有一定的启发意义。

1. 完善国内数据跨境流动法律制度

中国必须首先打造和完善自身的数据跨境流动法律体系，增强规则制定能力。欧盟通过《欧盟基本权利宪章》和 GDPR 在数据主体权利、数据控制者或处理者义务、数据监管机构等方面树立全球数据保护规则标杆，在此基础之上建构多层次、多样化的跨境数据流动法律工具箱，实现欧盟数据在域外享有实质等同于欧盟数据保护标准的目标。而美国虽未如欧盟一般构建专门的跨境数据流动规则，但通过外资国家安全审查制度、国家紧急状态制度及清洁网络计划等一系列灵活配置的组合拳，打击他国科技企业的发展，牢牢控制数据的跨境流出。[⑤]

中国互联网产业强势崛起，跨国性互联网平台对数据跨境流动的需求日益强烈，财务、人员管理、跨国运营网络效率与服务的提升等，均无法脱离数据的跨境流动。近年来中国也愈加意识到数据跨境流动的重要性，在短短数年间构筑起自身的数据跨境流动法律框架，其中以《网络安全法》《中华人民共和国数据安全法》（下文简称《数据安全法》）和《个人信息保护法》为顶层制度设计，以《数据出境安全评估办法》《网络安全审查办法》《关键信息基础设施安全保护条例》《个人信息出境标准合同办法》《个人信息保护认证实施规则》等为具体实施规则。具体而言，中国为企业数据出境提供了以数据出境安全评估、标准合同和个人信息保护认证为主的法律工具箱。数据出境安全评估适用于可能威胁国家安全和公共安全的高风险数据跨境流动场

---

① 洪延青：《数据跨境流动的规则碎片化及中国应对》，载《行政法学研究》2022 年第 4 期，第 71 页。

② Kenneth Propp and Peter Swire, “Geopolitical Implications of the European Court’s Schrems II Decision”, Lawfare Blog website, https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision.

③ Theodore Christakis, “Schrems III? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 3)”, European Law Blog website, https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-EDPB-post-schrems-ii-recommendations-on-international-data-transfers-part-3/.

④ Stewart Baker, “How Can the U.S. Respond to Schrems II?”, Lawfare Blog website, https://www.lawfareblog.com/how-can-us-respond-schrems-ii.

⑤ 以技术产业快速崛起的中国为例，美国一方面利用国际影响力联合他国抵制华为等中国科技企业布局国际市场，切断华为芯片的供应链，全方位打压华为企业；一方面封禁国际版抖音和微信在美运营并强制其出售，清除美国互联网领域与中国相关的一切威胁其数据控制权的因素。

景；个人信息保护认证更适合常态性、相对稳定且属于基础信息处理活动的跨境流动场景，如跨国企业集团内部的数据流转；相对而言，标准合同的适用场景可能更为广泛，可适用于各类低风险、非常态化的数据跨境流动场景。[①] 同时，标准合同可以作为数据出境安全评估和个人信息保护认证要求数据出口方与数据接收方签订法律文件的范本，因此，标准合同也是更为基础和底层的法律工具。通过自我评估数据出境的安全风险，企业可从中选择适合自身的数据出境法律工具。

但问题在于，数据出境安全评估的三大适用场景——关键信息基础设施提供者或处理 100 万人个人信息处理者、重要数据出境和累计传输 10 万人个人信息或 1 万人个人敏感信息的个人信息处理者——中，“关键信息基础设施”“重要数据”“个人敏感信息”等核心概念的界定存在非常弹性的自由裁量空间。在国家以“安全目标”为数据出境首要价值考量的背景之下，网信等相关部门在实践中判断特定数据出境是否属于安全评估情形时，往往倾向扩大解释安全评估的适用范围。企业在自评估出境风险时，为消除合规的不确定性风险，也会倾向选择最保险的安全评估。由此，数据出境安全评估的适用场景会呈现扩张和泛化，挤压企业本可适用更合适的个人信息保护认证或标准合同的选择空间。此外，数据出境安全评估属于国家事权，安全评估的实质审查和批准权力由国家网信部门行使，地方网信部门仅具有形式上审核申请材料完备性的权力。[②] 此种制度设计可能会降低安全评估的运作效率。同时，该制度与国家从严审查数据出境的因素相叠加，更容易导致事实上的数据本地化。[③] 跨国企业可能不得不继续花费巨额成本在境外各个法域创设独立的分支机构与数据处理中心，尽量避免数据的跨境流动。对此，中国的数据跨境流动制度还需通过立法进一步明确数据出境安全评估的适用范围，增强适用的确定性，为网信等部门和企业提供更加确定的监管和操作指引，真正实现低风险场景下的数据自由出境。值得注意的是，2023 年 9 月，国家网信办发布《规范和促进数据跨境流动规定（征求意见稿）》，释放出国家意图在实践中进一步推进落实低风险场景下数据自由流动的政策信号。

国家安全是国家生存发展的基本前提，数据跨境流动不能以危害本国安全利益为代价。在国际层面，《区域全面经济伙伴关系协议》（RCEP）、《全面与进步跨太平洋伙伴关系协定》（CPTPP）和《数字经济伙伴关系协定》（DEPA）等新一代国际经贸协议，实际上已通过数据跨境流动规则中的“合法公共政策目标”和“基本安全利益”等例外条款，将这一共识法律化。中国的数据出境安全评估正属于对例外条款的恰当阐释，中国也已经与国际初步接轨。[④] 同样需注意的是，新一代经贸协定均采取以数据跨境“自由流动”为原则、“限制流动”为例外的基本立场。中国在主张安全评估等例外时，应当加以严格限制，避免因安全评估泛化而使“限制流动”这一例外喧宾夺主，成为事实上的原则。

2. 加强中国数据保护法律的域外法治建设

互联网时代地理主权边界日益模糊，固守传统的属地主义管辖原则已不足以维护一国安全利

① 谢登科：《个人信息跨境提供中的企业合规》，载《法学论坛》2023 年第 1 期，第 93 页。

② 《数据出境安全评估办法》第 6—10 条。

③ 据不完全统计，从《数据出境安全评估办法》2022 年 9 月生效至 2023 年 6 月，通过数据安全评估的企业仅有 13 个，其中北京 3 个，上海 2 个，浙江 3 个，广东 3 个，山东和江苏各 1 个。所涉企业主要集中在电商、零售、汽车、电子技术等领域。参见“截至目前已超过 10 家企业通过数据出境安全评估”，https：//mp. weixin. qq. com/s/fexv032v1VCzpcLKB7KDEQ。

④ 谭观福：《数字贸易中跨境数据流动的国际法规制》，载《比较法研究》2022 年第 3 期，第 184 页。

益和民众数据权益。正因如此，欧盟 GDPR 放弃以数据处理行为作为确定管辖范围的标准，选择“实体标准”和“针对性标准”进一步扩张其域外适用范围，并以“代表制度”确保其域外效力的执行落实，[①] 同时配合其数据跨境流动的规则输出，增强欧盟在全球的规则塑造力。美国自 20 世纪以来为确保对外政策的实现，赋予越来越多国内法以域外效力，并逐渐形成一套立法、执法与司法紧密配合的对外制裁法律机制，[②] 在数据领域则以《澄清境外合法使用数据法》为核心将美国法律强制推向他国。

相较于个人信息保护的国内法治建设，中国数据跨境流动的涉外法律体系建设存在短板。[③] 数据保护立法的域外法治建设，应当在坚持安全与地点相挂钩的基础之上，在数据保护立法中突出客观属地原则。若境外数据处理者的数据处理行为之后果直接危及或可能危及国家和个人的数据安全和隐私利益时，中国应积极将其纳入数据保护法律的管辖范围，《数据安全法》第 2 条第 2 款以及《个人信息保护法》第 3 条第 2 款已经体现这一动向。在执法层面，执法机关依据国内法的域外管辖条款，以落入管辖范围的境外实体为执法对象行使管辖权，保障中国国家和公民利益。但执法管辖权严格遵循属地原则，中国执法部门无法直接进入他国领土执法。对此，可采用间接的境内执法方式将中国法的效力传导至境外执法对象。以《个人信息保护法》第 53 条的代表制度为例，通过代表代为承担责任的模式，代表制度可以将公权力的直接域外执法转化为代表对境外数据处理者的民事追偿，既可实现域外执法之目的，又能避免突破执法管辖权的属地限制。在司法层面，标准合同作为国家公法意志的私法表达，其合同履行效果直接影响中国数据域外保护机制运作的实效，对此，作为标准合同履约的重要争端解决机制，中国法院在审理此种争端时应当具有更广阔的国际视野，保障境外实体的诉讼参与，让审理程序更为便捷、公开与透明，在程序正义基础上最大程度保障结果正义，使境外实体内心信服并自愿履行其义务、承担其责任。立法、执法和司法三位一体协同推进涉外法治建设，在更好保障中国政策和利益的同时，逐渐增强国内数据保护法律的域外影响力和国际话语权。

3. 共建“一带一路”数据跨境自由流动圈

目前国际公共产品供给不足，中国适时提出“一带一路”倡议，为国际社会提供公共产品。[④] 此外，中国适时在国际舞台提出《全球数据安全倡议》，化解各方在数据安全、隐私保护、经济发展之间的分歧，以倡议为规则蓝本凝聚各方共识，构建各方普遍接受的数字和网络国际规则框架，携手打造数字命运共同体。[⑤] 但考虑到美欧等国在数据跨境流动领域对中国数据跨境流动的限制对待，并日渐朝着“阵营式”脱钩方向演化，[⑥] 现阶段中国应依托“一带一路”倡议和《全球数据安全倡议》，凝聚沿线国家数据跨境流动的战略共识，加强区域性数据治理和数

① 俞胜杰、林燕萍：《〈通用数据保护条例〉域外效力的规制逻辑、实践反思与立法启示》，载《重庆社会科学》2020 年第 6 期，第 68—75 页。

② 霍政欣：《国内法的域外效力：美国机制、学理解构与中国路径》，载《政法论坛》2020 年第 2 期，第 175—181 页。

③ 蔡翠红、郭威：《中美数据跨境流动政策比较分析》，载《太平洋学报》2022 年第 3 期，第 39 页。

④ 石静霞：《“一带一路”倡议与国际法：基于国际公共产品供给视角的分析》，载《中国社会科学》2021 年第 1 期，第 157—158 页。

⑤ 《外交部官员：〈全球数据安全倡议〉为全球治理注入新动力》，人民网，http://world.people.com.cn/n1/2020/1124/c1002-31942744.html。

⑥ 洪延青：《数据跨境流动的规则碎片化及中国应对》，载《行政法学研究》2022 年第 4 期，第 69 页。

字经济合作,[①] 打造“一带一路”数据跨境自由流动圈。首先,中国可放权地方先行先试,通过自贸区、自贸港的政策和地理区位优势,推进北京海淀区数字贸易港、雄安新区跨境电商综合试验区、海南自贸港、上海临港新片区国际数据港和粤港澳大湾区等各具特色的数据跨境流动实践,积累和探索跨境数据流动的成功经验和制度模式,为跨境数据流动的国际合作积累制度和实践经验。其次,借助“一带一路”倡议及“数字丝绸之路”所创造的国际合作新舞台,在《全球数据安全倡议》《中阿数据安全合作倡议》《“中国 + 中亚五国”数据安全合作倡议》等理念共识之上,逐步推进与中亚、中东、东盟、金砖国家等沿线国家和地区的数据治理合作,共建一批以“中国—东盟信息港”为样板的数据跨境流动合作新模式。通过“以双边带多边,以区域带整体”的推进策略,逐步形成面向全球的、开放和包容的“一带一路”数据跨境自由流动圈。[②] 最后,在全球数据跨境流动国际格局中,以“一带一路”自由流动圈、欧盟自由流动圈和北美自由流动圈三足鼎立之态势为谈判基础,中国可与欧盟、美国等展开数据跨境流动国际协定的平等谈判,而不必以减损国家主权利益为代价的合规者姿态参与同西方的国际谈判。

## 六 结语

欧盟不断提升内部的数据保护标准,并借助多种路径将内部标准向全球输出。现今,欧盟的数据保护法律已成为全球数据保护立法之标杆。以捍卫人的基本权利与尊严为价值导向,欧盟始终将自身放置在以规则为载体的价值制高点之上。但隐私盾事件所折射出的欧盟司法适用双重标准与偏离基于风险路径的法律解释与适用,揭示出欧盟潜藏在“正义”的规则外衣下软数据本地化的政治性意图。在数字经济时代,欧盟数字经济产业已经落后于美国与中国,为了重振本土数字经济产业,欧盟提出技术主权战略,以对抗美国等国家依托其互联网跨国企业对欧盟市场实施的技术控制,保护、培育和发展欧盟本土的数字产业。受此种战略的影响,公正、中立的欧盟法院也表现出其政治性或者武器性的一面。欧盟委员会最终通过《关于欧盟—美国数据隐私框架的充分性决定》,代替被欧盟法院宣布无效的《隐私盾决定》,重新接续起跨大西洋数据流动法律框架。但考虑到充分性决定的通过程序中缺少欧盟法院意志参与这一关键环节,后续仍有可能因欧盟法院的介入而出现类似于“*Schrems I* 案”和“*Schrems II* 案”的“*Schrems III* 案”,新建立起来的数据隐私框架存在被废止的制度隐患。[③] 届时,若美国继续遵循合规路径,在美欧重新谈判中,欧盟委员会对美国数据保护标准的要求可能进一步提高。此种发展趋势,可能正好契合欧盟技术主权战略的推进意图。

中国作为后发国家,较长一段时期受到欧美等西方国家规则话语体系的影响,容易形成一种将自身作为被动合规者和接受者的路径依赖。但随着综合国力日渐强盛,中国开始创设具有自身特色的规则话语体系,摆脱对西方叙事的依赖。在国际法领域,中国正逐渐打造中

① 赵龙跃、高红伟:《中国与全球数字贸易治理:基于加入 DEPA 的机遇与挑战》,载《太平洋学报》2022 年第 2 期,第 23 页。

② 何波:《中国参与数据跨境流动国际规则的挑战与因应》,载《行政法学研究》2022 年第 4 期,第 102 页。

③ “‘Privacy Shield 2.0’? – First Reaction by Max Schrems”, NOYB website, https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems.

国特色国际话语体系，加强涉外法治理论体系建设，增强中国的国际规则话语权。[①]《隐私盾决定》无效事件侧面印证了中国坚持走独立自主道路的战略的正确性。在数据跨境流动国际舞台上，中国应充分认识欧盟技术主权战略的实现逻辑，把握数据跨境流动国际谈判的主动权，切勿让自身陷入如美国一般的被动合规者境地。在完善自身数据保护和数据跨境流动规则体系的基础上，中国可依托《全球数据安全倡议》凝聚价值共识，借助“一带一路”倡议和“数字丝绸之路”增强与沿线国家的数据跨境流动国际合作，形成以中国为核心的区域性数据跨境自由流动圈。在此基础上，中国可探索与欧盟乃至美国就数据跨境流动合作议题开展平等对话与谈判的路径。

## EU's Technological Sovereignty Strategy and Its Realization in the US-EU Gaming on Cross-Border Data Flows

*Liu Ye*

**Abstract**: Distinguishing from the Safety-Harbor Framework, the abolishment of the Privacy-Shield Framework shocked the compliance of cross-border data flows concerning EU, which reflects transformation of EU to regulating on cross-border data flows more stringently because of the newly technological sovereignty strategy. The suspicion to double standards in the law application of the Court of Justice of European Union, as well as the odd measures taken by European Data Protection Board that deviate from the intent of the "risk-based" approach of General Data Protection Regulation, are the results of which EU's technological sovereignty strategy responded to US's aggressive technological control strategy in the legal field. By virtue of the Brussels Effect in the field of data protection, EU has controlled the rules-making power and possessed in a privileged status when negotiating with US after the abolishment of the Privacy Shield Framework, forcing US to constantly revise its legislation for passive compliance. EU has been managing to realize the target of soft data localization, limit the competitiveness of foreign tech enterprises in EU's single market, and finally support the implementation of the technological sovereignty strategy in data and technology. China should keep a watchful eye on EU's regulation of cross-border data flows under the guidance of the technological sovereignty strategy, avoid falling into the trap of passive compliance, and plan an independent strategy on cross-border data flows.

**Keywords**: Technological Sovereignty Strategy, Cross Border Data Flows, Privacy-Shield Framework, Brussels Effect, Soft Data Localization

（责任编辑：谭观福）

① 参见黄进：《论统筹推进国内法治和涉外法治》，载《中国社会科学》2022 年第 12 期；何志鹏：《国内法治与涉外法治的统筹与互动》，载《行政法学研究》2022 年第 5 期；张曩：《涉外法治的概念与体系》，载《中国社会科学》2022 年第 2 期。