第 51 卷第 5 期
2024 年 9 月
Vol. 51, No. 5
September, 2024

四川师范大学学报(社会科学版)
Journal of Sichuan Normal University
(Social Sciences Edition)

外国数据法效力的域外扩张与中国范式研究

林福辰

摘要:数据已成为当今社会发展的重要因素,但目前全球尚未形成统一的数据跨境流动规则。在此背景下,美国与欧盟相继构建起“外向干涉型”和“内向保护型”数据法域外适用体系,以加强对网络空间的规制力。此举存在滥用数据法域外效力的隐忧,增加了各国数据的被动开放风险,也抬高了企业全球经营的合规门槛。作为数字产业大国,我国亦应加强数据立法,构建“能动回应型”数据法域外适用体系,既要顺应国内数字市场发展的内向性要求,也应兼顾互联网企业走出去的外向性需要,推动我国数据法域外效力的合理适度延伸,并完善外国数据法不当域外适用的阻断机制,以此探索全球数据治理的中国范式。

关键词:涉外法治;数据法;域外适用;数据流动

DOI: 10.13734/j.cnki.1000-5315.2024.0315

收稿日期:2024-05-02

基金项目:本文系四川大学博士后研发基金“外国数据立法不当域外适用的中国涉外法治应对”(skbsh2023-16)、教育部哲学社会科学研究重大课题攻关项目“加快推进自由贸易港建设研究”(23JZD27)、2023 年四川大学中央高校基本科研业务费(法学)研究课题(2023fxzy-04)的阶段性成果。

作者简介:林福辰,男,辽宁大连人,法学博士,四川大学法学院助理研究员、专职博士后,四川大学“自贸区暨‘一带一路’法律研究中心”助理研究员,E-mail: Linfc_SCU@163.com。

当前,数字革命几乎渗透到了社会经济关系的各个方面,数据经济成为重组全球经济要素资源、重塑全球经济结构、改变全球竞争格局的关键性力量①。大变局之下的当今世界,全球治理体系亟待改革与完善,国际竞争越来越体现为制度、规则、法律的竞争②。确保数字经济的供应链安全对提升国家竞争优势至关重要,因此,数据立法成为各国在国际社会争夺数据治理话语权、输出本国数据治理规则、扩大本国数据优势的主要路径③。以美国为代表的西方国家争相制定具有域外适用效力的数据法律法规,以期维护本国数据产业的竞争优势,争夺国际数据治理话语权。近年来,我国数据法律体系虽初具轮廓,国内数字经济治理体系和治理能力现代化水平显著提高,但尚未形成数据法域外适用体系,难以防控域外数据行为对国家安全、公共利益与个人权益的潜在危害,运用法治手段应对外国数据法不当域外适用的能力亟待提升。有鉴于此,本文拟在梳理美欧数据法域外效力规则体系的基础上,探究数据法域外适用体系的中国范式,并就外国数据法不当域外适用的中国应对方案进行探讨。

一 国家数据法效力域外扩张的理论归因

(一)规制数据跨境流动目标的合理性

①梅宏《大数据与数字经济》,《求是》2022 年第 2 期,第 28 页。

②周强《在习近平法治思想指引下 奋力推进新时代司法为民公正司法》,《求是》2022 年第 4 期,第 22 页。

③王燕《数据法域外适用及其冲突与应对——以欧盟〈通用数据保护条例〉与美国〈澄清域外合法使用数据法〉为例》,《比较法研究》2023 年第 1 期,第 187 页。

据统计,在2010至2019年间,全球数据跨境流量以每年45%的惊人速度增长,从45Tbps增长到1500Tbps①。数据作为新兴的生产要素,为全球经济增长提供新动能的同时,也改变了社会的责任配比②。

首先,大型互联网企业对用户数据的商业化利用,致使个人隐私保护问题尤为突出。当前,个体的社会生活在相当大的程度上被"数字化",在网络空间和存储设备中留下自身的"数字痕迹",随之而来则是个人数据跨境流动存在的隐私泄漏风险。例如,Facebook曾在用户不知情或"非自由"同意的情况下从第三方网站或应用搜集用户信息,对此,德国联邦最高法院曾于2020年6月裁定Facebook构成对公民隐私的侵犯,责令其调整服务条款和数据处理活动③。不仅如此,在数字技术的加持下,数据处理者对个人信息的大规模、自动化搜集弱化了传统匿名化技术的实际效果,进而加剧了个人数据被过度商业化利用的风险。因此,基于个人隐私信息保护的目的,规制数据流动是各国政府当前的重要责任。

其次,数据跨境流动,对公共安全利益带来挑战。公众在享受互联网便利性的同时,也面临着虚假信息泛滥、有害信息传播、网络犯罪发生等诸多危害。立足国家治理层面,各国往往基于一定的保护义务,推动网络空间规制的变革,强化网络空间架构的控制性。一般而言,网络空间的规制程度取决于网络空间的架构,而该架构的属性由价值观决定④。例如,德国通过限制数据跨境流动,禁止公民通过互联网平台售卖与纳粹有关的纪念品⑤;越南亦曾颁布立法,限制危及越南公共秩序的信息在网络空间中传播⑥。所以,各国对公共安全的维护,使规制数据流动有了天然的合理性。

最后,利用大数据分析等数据手段,一国可能有针对性地开展对他国信息情报的收集和处理工作,从而威胁到他国国家安全。例如,美国自2007年起启动了代号为"棱镜"的秘密监控项目,直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报,微软、雅虎、谷歌、苹果等在内的9家国际网络巨头参与其中⑦。可见,数据的自由流动对国家安全构成了新的挑战,各国对数据行为的监管需求更为迫切。

综上,放任国家数据的自由流动,会触及到该国经济和社会生活的核心部分,这与该国特定公共政策目标之间存在着不可避免的冲突。面对数据跨境流动对个人信息、公共利益和国家安全的冲击,各国近年来愈发重视数据安全风险的法律防范,并通过完善国内立法、参与国际合作等方式,强化对数据流动的规制,以此落实网络空间中的国家保护义务、满足规制数据跨境流动的合理性国家要求。

(二)数据法效力域外扩张的现实必要性与国际合法性

数据法效力域外扩张具有现实必要性。面对因数据跨境流动而产生的全球性威胁,各国目前难以在短期内形成具有统一性、全球性的数据跨境传输规则⑧。网络空间的出现,使法律属地主义被不断削弱,传统的国家界限变得愈加模糊,这使国际法成为应对数据跨境流动诸多现实挑战的理想平台。2003年,联合国信息社会世界峰会在《日内瓦原则宣言》中指出,"与互联网有关的公共政策的决策权是各国的主权"⑨。联合国相关专家组的报告亦明确了《联合国宪章》对网络空间的适用性⑩。据此,既有国际法体系重申了主权

---

①成政珉、华强森、Sven Smit等《全球流动:世界互联互通的纽带》,2023年1月发布,2024年3月18日访问,https://www.mckinsey.com.cn/wp-content/uploads/2023/02/MGI_Global-Flows_Dicsussion-paper-CN-20230215.pdf。

②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年第2版,第95页。

③The German Federal Supreme Court, Bundesgerichtshof bestätigt vorläufig den Vorwurf der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung durch Facebook, Juni 23, 2020, https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html.

④劳伦斯·莱斯格《代码2.0:网络空间中的法律》,第36页。

⑤Germany, Strafgesetzbuch [Penal Code] § 86a (2021).

⑥Vietnam, Decree No. 72/2013/ND-CP § 4(4) (2013).

⑦Barton Gellman, Laura Poitras, "U.S., British Intelligence Mining Date from Nine U.S. Internet Copmanies in Broad Secret Program," *Washington Post*, June 7, 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

⑧徐峰《网络空间国际法体系的新发展》,《信息安全与通信保密》2017年第1期,第75页。

⑨《日内瓦原则宣言》,《信息社会世界高峰会议成果文件》,国际电信联盟2005年,日内瓦,第19页,https://www.itu.int/net/wsis/outcome/booklet-zh.pdf。

⑩从国际安全角度促进网络空间负责任国家行为政府专家组《从国际安全角度促进网络空间负责任国家行为政府专家组的报告(A/76/135)》,联合国大会,2021年7月14日,中文版第16页。

原则对网络空间的适用性，各国享有对境内网络设施的管辖权。除此之外，国际法拓展有限，且多停留于倡议的层面，实践中可操作性欠佳。同样的叙事也体现在数字贸易的国际规制层面，CPTPP、RCEP 等协定确立了以数据跨境自由流动为原则、本地化为例外的规制进路①，但就数据跨境流动例外条款的具体适用，各区域一体化协定缺乏明确指引。传统的国内立法管辖权是以属地管辖为基础，以属人管辖、保护性管辖和普遍性管辖等为补充。然而，互联网具有虚拟性、开放性和无边界的特征，大规模的数据跨境流动对以属地为基础的国际管辖秩序形成了严重挑战。同时，一个借助互联网实施的行为不仅在地理空间上难以界定行为发生地，其影响范围也非地理意义上的领土边界所能阻隔，这进一步削弱了属地管辖的规范意义。对此，以美国和欧盟为代表的国家或实体探索创新立法管辖模式，延伸数据法域外效力，希冀提升其对数据跨境流动的规制力。由此，各国开始将注意力转向国内，尝试通过强化涉外立法以监管数据跨境流动。

数据法效力域外扩张具有国际合法性。一般认为，法律属地主义式微是社会、技术等一系列因素叠加的结果②。1927 年，国际常设法院在“荷花号”案中对国家实施域外管辖的行为进行了阐明，认为：“国际法非但远没有设立一般禁止性规定以要求各国不得将其法律的适用及其法院的管辖权扩展至领土外的人、财产和行为，反而在这方面为各国留下了广泛的自由权利，仅在特定情形中以禁止性规则限制之；除特定情形，各国皆得自由采取其认为最好与最适合的原则”③。据此，国际常设法院确立了“国际法不禁止即为允许”的原则，奠定了国内法域外适用的合法性基础。目前，全球并未形成具有普遍约束力的数据保护国际规则，没有对国家管辖权向域外延伸进行过多限制，宽松的国际环境为各国扩张数据法域外效力奠定了合法性基础④。

二　美欧数据法域外适用体系的范式考察

（一）美国“外向干涉型”数据法域外适用体系

美国在全球互联网产业拥有近乎垄断的市场地位，凭借数字技术与产业规模的巨大优势，美国数据法域外适用体系秉持“外向性”姿态，致力于获得调取全球数据的能力。以 2018 年《澄清域外合法使用数据法案》（Clarifying Lawful Overseas Use of Data Act，以下简称 CLOUD 法案）为代表的数据立法就试图突破美国域外取证瓶颈，赋权政府可以调取本国企业在境外存储的数据信息。

1. 依托全球数字市场垄断地位的“外向性”姿态

作为美国数据立法的基础性法案，1986 年《存储通信法案》（Stored Communications Act，以下简称 SCA）主要关注发生在其国内的数据行为，但未明确美国政府是否有权要求通信服务商提交存储在境外的数据。在微软案中，美国当局试图获取存储于境外的数据。对此，微软公司认为涉案数据存储在爱尔兰境内，基于属地管辖的限制，美国当局搜查令的效力不能及于该数据。区别于微软所主张的“数据存储地标准”，美国政府认为微软是数据的实际控制者，其在本土通过互联网即可完成数据的调取；作为美国境内企业，微软公司应当执行美国当局依据 SCA 签发的搜查令。美国法院最终裁判，搜查令的实施地点是决定该案能否援引 SCA 的重要因素，微软公司在美国境内的情况不足以替代对数据位置的关注⑤。

为破解域外数据的可及性限制，美国出台了 CLOUD 法案，引入“数据控制者标准”来弱化数据与物理空间的关联性。CLOUD 法案规定，只要互联网企业拥有、监控或控制用户数据，那么无论该数据是否存储在美国境内，相关企业作为数据控制者都应承担向美国政府披露数据的义务⑥。在实践中，微软、谷歌、苹果等美国科技企业占据着全球绝大多数数字市场的份额，获得了海量数据资源，这让它们成为美国获取域外数据的关键桥梁。尽管这些公司仍必须服从所在国的数据监管规则，但是借助“数据控制者标准”，CLOUD 法案可以让美国在事实上具备获取全球数据的能力，并且不需要考虑数据的实际存储地。

为进一步提升调取全球数据的有效性，CLOUD 法案还设置了严格的责任豁免条件。CLOUD 法案规

---

①杜玉琼、罗新雨《RCEP 数据跨境流动规则例外条款的适用及中国应对》，《四川师范大学学报（社会科学版）》2023 年第 5 期，第 75 页。

②蒋小红《欧盟法的域外适用：价值目标、生成路径和自我限制》，《国际法研究》2022 年第 6 期，第 106 页。

③S.S. Lotus (Fr. V. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

④孔庆江、于华溢《数据立法域外适用现象及中国因应策略》，《法学杂志》2020 年第 8 期，第 86 页。

⑤United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

⑥Clarifying Lawful Overseas Use of Data Act § 103.

定域外数据控制者如欲免除数据披露义务,需同时满足三个条件:第一,法案对域外数据控制者施加的数据披露义务违反了"适格外国政府"法律;第二,美国法院根据案件情况和公平理念,依国际礼让原则主动放弃CLOUD法案的域外适用;第三,数据控制者所服务的用户不是美国人且不在美国居住①。然而,美国法院在实践中认定的"适格外国政府"相当有限,目前,仅英国和澳大利亚获得了认定并签订了数据调取协议②,也缺乏明确的国际礼让分析思路③。同时,作为法律概念的"美国人"的涵盖范围相当宽泛。在美国对外制裁中,"美国人"不仅包括美国公民、合法获得永久居住的外国人以及在美注册的公司等主体④,甚至还覆盖了美国公司的外国子公司和美国人管理的外国公司⑤。对此,美国政府曾毫不掩饰地表示,CLOUD法案代表着一种新的范式,一种高效获取电子数据的保护办法⑥。

2.致力于获得调取全球数据能力的"干涉性"追求

作为美国行使域外管辖的合法性依据,CLOUD法案的"数据控制者标准"虽具有客观属地原则或效果原则的特征⑦,但是,法案的调整对象十分宽泛,适用也具有相当程度的灵活性,这对干涉他国数据监管权的正常行使以及削减其他国家保护公民隐私、国家安全的能力造成了影响。例如,CLOUD法案规定的数据控制者涵盖了电子通信服务和远距离计算服务提供者⑧,这意味着提供电子邮件、社交媒体、云存储等服务的相关企业,甚至电商平台都是数据披露义务的承担者。不仅如此,美国司法部认为,域外的数据控制者如与美国有足够的联系也可触发CLOUD法案的适用⑨,此种联系包含了拥有、监控和控制等数据处理活动的全周期⑩。这进一步扩大了法案的潜在适用范围,体现了美国对数据法域外效力的极致追求。

同时,美国与其他国家间的数据调取具有非互惠性。SCA规定通信服务商不得向外国政府提供有关通信内容的数据,导致他国在侦查打击犯罪时,难以通过双边司法协助请求而从美国当局获得涉案数据。相比之下,CLOUD法案虽规定"适格外国政府"也可通过数据控制者获取存储于美国境内的数据⑪,但是,"适格外国政府"的构成标准非常严苛,相关国家不仅被要求与美国签订数据调取协定,同时还要为数据控制者免除数据披露义务提供实质性或程序性的救济途径,这让外国在实践中近乎无法获取美国境内存储的数据。不仅如此,"适格外国政府"还要给予美国同等的数据访问权,并面临美国定期的单边审核与"随时开除"的压力。非互惠性的标准,加上调取全球数据的干涉性追求,会在客观层面几乎造成"全球→美国"的数据单向流动,折射出"美国优先"的立法思路和主导全球数据流动秩序的野心。

(二)欧盟"内向保护型"数据法域外适用体系

1.服从于欧洲数字市场统一需要的"内向性"姿态

---

①Clarify Lawful Overseas Use of Data Act §103.

②U.S. Department of Justice, U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, October 3, 2019, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists; U.S. Department of Justice, United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime, December 15, 2021, https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime.

③郭烁《云存储的数据主权维护——以阻断法案规制"长臂管辖"为例》,《中国法律评论》2022年第6期,第78页。

④18 U.S.C. § 2523 (2018).

⑤覃俊豪《国内法域外适用:研究路径、美国实践与中国应对》,《学术论坛》2024年第2期,第144页。

⑥U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, (April, 2019). https://www.justice.gov/opa/press-release/file/1153446/dl.

⑦客观属地原则是指当试图管辖之行为的构成因素出现在领土国境内时,一国可对其领土外的人、财产或行为行使管辖权;效果原则是指一国可以根据外国国民于一国领土外发生的行为,却在该领土上产生重大影响而主张管辖权。参见:联合国《国际法委员会报告——第五十八届会议》(2006年5月1日至6月9日和7月3日至8月11日),联合国2006年版,第393页。

⑧18 U.S.C. § 2510(15) (2018).

⑨U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, (April, 2019). https://documents.un.org/doc/undoc/gen/g06/636/19/pdf/g0663619.pdf?token=QziVvJEmXouUsyVOJd&fe=true.

⑩数据全生命周期包括数据处理者进行数据收集、存储、使用、加工、传输、提供、公开、删除等环节。参见:王玎《论数据处理者的数据安全保护义务》,《当代法学》2023年第2期,第44页。

⑪18 U.S.C. § 2523 (2018).

不同于美国庞大数字产业对 CLOUD 法案实施的支撑，欧盟数字市场的发展整体滞后，对外国技术的依存度较高，因而加剧了欧盟加强内部数据保护的现实紧迫性。欧盟内部几乎没有大型数字平台，数字产业规模仅占全球 70 个大型数字平台市值的 4%[①]。谷歌、脸书和微软等美国互联网企业几乎垄断了欧盟数据市场，收集大量用户数据，并通过精准推送创造了海量广告收入。不仅如此，上述企业还可能妨碍欧洲国家政府开展工作。如在新型冠状病毒流行期间，法国当局曾开发出“Stop Covid”的病毒密接者追踪程序，但遭到苹果和谷歌公司的技术阻拦，致使软件无法实际投入应用。在此背景下，欧盟数据监管的自主性面临严峻挑战，欧盟公民对个人数据和隐私保护的担忧与日俱增。

针对由外国互联网企业主导的在线环境，欧盟试图通过数据法的域外适用，强化内部市场监管，调整数据主体和数据控制者之间的力量对比。欧盟早在 1995 年便颁布了数据相关立法，即《关于个人数据处理及其自由流动的个人保护第 95/46/EC 号指令》(Directive 95/46/EC of the Enropenan Parlianment and of the Council: on the protection of individuals with regard to the processing of personal data and on the free movement of such data，以下简称《数据保护指令》)。但遗憾的是，《数据保护指令》需经欧盟成员国转化为国内法后方可实施，这导致了欧盟内部数据保护水平的差异。因此，欧盟于 2016 年通过了《一般数据保护条例》(General Data Protection Regulation，以下简称 GDPR)，并将其作为一项直接适用的数据基础性立法。与《数据保护指令》相比，GDPR 加重了数据控制者义务，力求切实落实数据主体权利的保护。

在域外管辖权方面，GDPR 首先承继了《数据保护指令》的“设立机构标准”。其第 3.1 条规定，不论数据处理行为实际是否在欧盟内进行，GDPR 都适用于在欧盟内部设立机构的数据控制者。这虽未明确 GDPR 能否进行域外适用，但实际上保证了 GDPR 规制域外数据处理行为的可能。在此基础上，欧盟通过“目标指向标准”拓宽了数据法的域外效力。得益于数据的无边界属性，现实中数据控制者在境外亦可完成对欧盟用户数据的收集、分析和处理。因此 GDPR 第 3.2 条规定，即使数据控制者未在欧盟设立机构，GDPR 依然适用于为欧盟内的数据主体提供商品或服务的数据控制者，以及对发生在欧盟内部的数据主体活动进行监控的数据控制者。这就是“目标指向标准”。可见，相较于“设立机构标准”，“目标指向标准”在事实上更具有域外效力扩张的色彩。

晚近以来，“设立机构标准＋目标指向标准”的管辖权模式也被吸收到欧盟新近颁布的数据立法之中。2022 年 7 月，欧盟委员会颁布的《数字服务法》(Digital Services Act，以下简称 DSA)第 2.1 条规定，该法案适用于向拥有其设立地或位于欧盟的服务接受者提供的中介服务，而服务提供者的设立地点不受限制。欧盟 2023 年 5 月生效的《数字市场法》(Digital Markets Act，以下简称 DMA)也遵循相似进路，其第 1.2 条规定，面向欧盟境内用户或平台提供服务的互联网企业，都是该法案的调整对象，至于企业的设立地或营业地并非该法案是否适用的因素。

2.致力于强化保障数据主体权利的“保护性”追求

就数据权利保护的限度而言，欧盟始终围绕《欧洲人权公约》第 8 条展开，将个人数据权利理解为一项基本人权，认为数字技术的发展并不能影响对个人隐私权利的保护。在此观念指导下，GDPR 创设了用户删除权、被遗忘权等新型数据权利，强化个人信息保护水平。同时，为确保相关规则能够在实践中发挥实效，欧盟通过扩大解释延伸“设立机构标准”和“目标指向标准”的涵盖范围，拓宽数据法域外适用的场景。

关于“设立机构标准”，欧盟数据保护委员会曾指出，只要域外的数据控制者与其在欧盟境内的“设立机构”之间存在真实有效的联系即可认定为满足该标准[②]。在 Google Spain 案中，位于美国的谷歌公司负责处理西班牙的用户数据，而位于西班牙的谷歌分公司仅负责当地的搜索引擎业务。针对此种情况的法律适用问题，欧盟法院认为，分公司的创设为总公司的广告业务提供了盈利空间，谷歌公司也与分公司之间存在真

①“Communication on Online Platforms and the Digital Single Market {SWD(2016) 172 final}，” accessed March 18, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288.

②Article 29 Data Protection Working Party, “Opinion 8/2010 on Applicable Law (0836-02/10/EN WP 179),” accessed March 18, 2024, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf.

实有效的联系,进而认定谷歌公司的域外个人数据处理行为应适用《数据保护指令》①。可见,欧盟对"设立机构标准"的理解十分宽泛,域外的数据控制者可能因为域外的个人数据处理活动而适用欧盟的数据法。

在"目标指向标准"中,GDPR 着眼于欧盟范围内数据的保护,而不仅停留在欧盟公民数据保护的层面。关于 GDPR 第 3.2 条中"数据主体"的界定,欧盟采用了与美国 CLOUD 法案相近的规制方式,指出"GDPR 提供的保护应适用于个人数据受到处理的自然人,无论其国籍或居住地如何"。同时,欧盟力图保持数据处理行为定义的宽泛性,GDPR 在序言中规定,该法中的"监控"是指在互联网对自然人进行的追踪,包括后续个人数据处理技术的潜在使用,此类个人数据的技术处理包括对个人进行特征分析,并预测个人的偏好、行为和态度。由此表明,实践中域外数据控制者若以欧盟为对象进行相关的数据处理活动,那么其行为很有可能构成 GDPR 第 3.2 条中"对欧盟内数据主体进行监控",从而触发欧盟数据法的域外适用。例如,在 Judith VIdal-Hall, Robert Hann, Marc Bradshaw v. Google Inc 案中,欧盟法院曾认定谷歌公司通过 Cookie 存储用户数据并推送个性化广告的行为构成对用户的监控追踪②。

三 美欧滥用数据法域外效力规则的消极影响

数据法域外效力的扩张有其内在合理性,但未经来源国允许的数据跨境调取,将被视为对一国数据主权的侵犯,而被界定为外国数据法的不当域外适用。美国意欲绕过各国监管实现对全球数据的调取,其数据法的域外适用呈现恣意扩张的态势,各国亟须重视并加以应对。相较之下,欧盟的数据法域外适用体系虽呈现"内向性"姿态,但设立高标准权利保护机制的原因是欧盟对外输出数据监管模式的政策需求,以此寻求影响全球数据流动规则的话语权。

(一)增加各国数据被动开放的风险

随着信息技术的迅猛发展,互联网活动呈现远程化、全球化和虚拟化的特点,极大地冲击了传统立法的管辖模式。然而,数据的存储仍要依托计算机实体,这为国家主权原则向网络空间治理领域拓展提供了基础。在 2023 年 11 月召开的首届全球人工智能安全峰会上,中国、欧盟等多个国家代表共同签署《布莱切利宣言》,在宣言中表示要携手合作应对人工智能所引发的相关风险,并尊重各国规制数据活动的自主权和灵活性③。可见,数据主权是国家主权在网络空间的自然延伸和表现,国家主权原则依然是全球数据规则治理的基础。在数据主权原则的指引下,各国普遍主张不能以严格的自由流动义务或完全禁止本地化的要求来限制主权国家出于正当理由治理互联网的能力。截至目前,已涉及 32 个国家的 27 项自贸协定包含了有关数据本地化的条款④。

然而,数据的本地化存储并不能削减互联网企业对数据的现实支配力。鉴于微软、谷歌、苹果等美国企业近乎掌控了全球数据设备终端和传输通道,美国倾向于将数据支配力作为数据监管权力行使的边界。美国司法部认为,只要可以从美国领土访问到有关数据,这些数据就属于美国法律可以轻松"领土化"的地区⑤。这无疑是对他国数据主权的否定,并为自身数据霸权的行使提供依据。

数字产业的强大竞争力叠加 CLOUD 法案的"数据控制者标准",致使美国政府的数据调取之手可方便地延伸到国境之外,实现了"境内外一盘棋"。从寻求国家间司法协助到要求企业提供数据,数据提供主体的转变极大地减少了美国获取域外数据的阻力。加之调取全球数据的干涉性追求,美国数据法存在恣意滥用

---

①Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12 Court of Justice of the Europeon Union (2014).

②Judith Vidal-Hall, Robert Hann, Marc Bradshaw v. Google Inc, Case No: A2/2014/0403 Court of Appeal (2014).

③GOV.UK, The Bletchley Declaration by Countries Attending the AI Safety Summit, November 1, 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

④Chiara Del Giovane, Janos Fcrencz, Javier López-González, "The Nature, Evolution and Potential Implications of Data Localisation Measures," *OECD Trade Policy Papers*, no. 278 (November 10, 2023): 16.

⑤U.S. Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act", accessed March 18, 2024, https://www.justice.gov/d9/pages/attachments/2019/04/10/doj_cloud_act_white_paper_2019_04_10.pdf.

的趋向，这势必会加剧美国与他国数据管辖权的冲突，增加他国境内存储数据被动开放的风险。在此背景下，由于缺乏与美国数字产业相抗衡的经济实力，大部分国家尤其是最不发达国家难以通过双边谈判达成双向数据流动安排，只能被迫遵循 CLOUD 法案的“适格外国政府”标准和美国政府的审查。

欧盟数据法虽致力于内部市场的统一化建设，但也存在侵犯他国数据主权的隐忧问题。例如，欧盟在《电子证据条例（草案）》中规定了与美国 CLOUD 法案相似的“数据控制者义务”，以期单方面获取域外数据①。另外，GDPR 的域外适用以数据行为构成“设立机构标准”或“目标指向标准”为要件，但面对纷繁复杂且日新月异的网络空间，从事实要件到构成要件的投射过程存在高度的不确定性。例如，针对域外数据控制者提供商品或服务的行为，GDPR 还要求判断域外数据处理者是否有向欧盟数据主体提供商品、服务的主观目的。对此，欧盟数据保护委员会认为，应结合具体的案件事实加以判断，并综合考虑其他因素②。由于立法措辞的模糊性，欧盟执法机关或法院可以在实践中放宽境内主体与域外数据处理行为的实际联系要求，采取相关措施，进而影响他国的监管自主性。

（二）抬高企业全球经营的合规门槛

近年来，欧盟数据立法不断更新迭代，对公民数据权利的保护力度渐次加大。通过数据法域外适用，欧盟能够塑造其他国家及市场行为主体的议程设置和偏好界定，进而重塑各国的相对优势与国际竞争格局。例如，高标准的权利保护搭配数据法的域外适用，容易在事实上造成数据本地化的效果，即造成间接型数据本地化③，大幅增加企业的合规成本。2023 年 4 月，欧盟依据 DSA 要求 17 个超大在线平台和两个超大型在线搜索引擎承担更严格的平台义务，否则相关企业将面临全球年营业额 6％的罚款④。迫于巨大的监管压力，许多大型在线平台开始有针对性地调整其数据合规政策。例如，TikTok 推出“三叶草项目”，花费 12 亿欧元在爱尔兰和挪威新建三个数据中心，用于存储 1.5 亿欧洲用户的个人数据，以满足欧盟的合规要求⑤。

同时，欧盟数据法的域外适用可能加重境外企业的法律责任。在 Google Spain 案后，谷歌公司遵循判决结果，有针对性地调整了在欧盟境内的搜索程序，但欧盟数据保护机构认为，谷歌公司应在全球范围内删除链接，实现用户的被遗忘权。在 Schrems II 案中，欧盟法院同样认为，无论是否在欧盟境内，欧盟用户的个人数据保护水平应实质等同⑥。为了强化与欧盟的实际联系，GDPR 还要求域外互联网企业在欧盟境内设立代表处⑦。相关代表处即便不进行具体的经营活动，也可以作为欧盟数据保护机构调查执法的对象。如此一来，欧盟数据保护机构在依据 GDPR 域外效力规则认定域外数据控制者违反欧盟数据保护标准时，可以通过代表机构提高执法的有效性。

不仅如此，域外企业始终在被动适应欧盟的数据保护标准。随着数据立法的完善，欧盟数据保护标准不断提高。为实现“保护性”追求，欧盟强势地将其数据保护标准全球化，从而导致欧盟与其他国家的数据跨境流动合作具有较强的不确定性。以欧盟与美国间的数据传输合作为例，安全港协议（Safe Harbor）、隐私盾协议（Privacy Shield）曾于 2015 年和 2020 年被欧盟相继宣告无效，此种反复给美国企业带来了极大的数据合规压力。更值得关注的是，美欧前两次合作的失效源自欧盟法院 Maximillian Schrems v. Data Protection Commissioner 案和 Schrems II 案的判决，这意味着欧盟法院是通过司法审查的方式实现对数据流动的全球

---

①European Commission, “Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters,” accessed March 18, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

②European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, November 12, 2019: 7.

③Organization for Economic Co-operation and Development, Data localisation trends and challenges, December 22, 2020, https://www.oecd.org/sti/data-localisation-trends-and-challenges-7fbaed62-en.htm.

④European Commission Questions and answers on the Digital Services Act, February 23, 2024, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.

⑤Beth Maundrill, “TikTok Initiates Project Clover Amid European Data Security Concerns”, accessed February 23, 2024, https://www.infosecurity-magazine.com/news/tiktok-initiates-project-clover/.

⑥Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18.

⑦General Data Protection Regulation, Chapter 4, Article 27.

监管[①]。在这一过程中,美国更多的是在被动地面对欧盟数据保护标准的变化。2023 年,新达成的"欧盟—美国数据隐私框架"(EU-U.S. Data Privacy Framework,以下简称 EU-U.S. DPF)协议生效,该协议是美欧第三次尝试建立稳定的跨大西洋数据流动安排所作的努力。美国企业的数据合规责任再次加码,在个人权利保护方面,框架内企业应向欧盟用户告知收集数据的类型与使用的目的,给予个人访问其数据的权利,为个人提供限制其个人数据的使用和披露的选择和手段。与此同时,为满足国家安全的需要,企业仍要承担向当局披露用户信息或转移给第三方的责任,相关企业还需每年向美国主管部门提供材料以证明其合规性,否则将受到美国商务部、联邦贸易委员会(FTC)等机构的制裁。根据附件的规定,EU-U.S. DPF 还构建了独立的纠纷解决程序,允许欧盟个人提起仲裁,以解决"任何 EU-U.S. DPF 其他机制未解决的违反该框架的行为"[②]。值得注意的是,EU-U.S. DPF 的实施也不影响 GDPR 对欧盟成员国个人数据处理行为的适用性。可见,欧盟对外开展数据跨境流动合作的前提,是域外企业充分遵守欧盟的数据保护标准,并以此作为域外企业进入欧盟市场的条件。而随着欧盟数据保护标准的提升,强调数据自由流动的美国公司不得不调整原有的数据运营模式[③]。

四　数据法域外适用的中国范式及其建构路径

2022 年,我国数字经济规模达 50.2 万亿元,总量稳居世界第二,占 GDP 比重提升至 41.5%[④],数字经济已成为实现创新发展、重塑国民生活的重要力量。为规范引导数字产业发展,我国现已出台《网络安全法》、《数据安全法》、《个人信息保护法》等基础性法律,国内数字经济治理体系和治理能力现代化水平显著提升。然而,相较于欧美的数据立法,我国数据法仅有个别条款涉及域外适用,规则的体系性不足,可适用性有待提高。我国《数据安全法》第二条规定,在我国境外开展数据处理活动,损害我国国家安全、公共利益或个体合法权益的,依法追究法律责任。在境外处理我国境内自然人个人信息的活动应受《个人信息保护法》调整。同时,针对欧美数据法的不当域外适用,我国也缺乏必要的应对措施。对此,我国亟须在现有分散式立法的基础上,省思数据法域外适用体系的中国范式。

(一)构建我国"能动回应型"数据法域外适用体系

1.秉持"能动性"姿态

美国数据法域外适用体系的"外向性"姿态与其互联网企业在全球的产业优势密切相关,欧盟的"内向性"姿态则是其加强内部数字市场统一化监管的结果。相比之下,我国数字产业的发展兼具欧美的特点。一方面,我国数字市场日新月异,但互联网企业的经营行为仍需加强规范引导。2021 年,在对滴滴公司的网络安全审查中,国家网信办查明滴滴公司存在违法收集用户手机相册中的信息、人脸识别信息、乘客地址信息等 16 项违法事实[⑤]。在国家安全领域,2023 年,我国在对美光公司进行网络安全审查时发现,该公司在华销售的产品和提供的服务涉及对我国基础设施相关关键信息数据的收集,存在严重涉外网络安全隐患[⑥]。另一方面,自 2017 年习近平总书记提出"数字丝绸之路"倡议以来,我国持续加强与"一带一路"共建国家在数字经济前沿领域的合作,国内数字产业的发展成果正惠及全球。当前,我国已与 17 个国家签署"数字丝绸之路"合作谅解备忘录,与 23 个国家建立"丝路电商"双边合作机制,与周边国家累计建设 34 条跨境陆缆和多条国际海缆[⑦]。"在尼日利亚,中尼两国企业合作成立的电子商务及支付企业 OPay,已成为该国最大的移动

---

①金晶《个人数据跨境传输的欧盟标准——规则建构、司法推动与范式扩张》,《欧洲研究》2021 年第 4 期,第 99 页。

②International Trade Administration and U.S. Department of Commerce The U.S. Department of Commerce, EU-U.S. Data Privacy Framework, https://privacyshielddev.blob.core.windows.net/publicsiteassets/Full%20Text_EU-U.S.%20DPF.pdf, April 2024, 25.

③安怡宁、田野《数字经济多赛道竞争的权力机制——以美国和欧盟数字经济政策为例》,《国际关系研究》2023 年第 6 期,第 34 页。

④《国家互联网信息办公室发布〈数字中国发展报告(2022 年)〉》,中国网信网,2023 年 5 月 23 日发布,2024 年 1 月 30 日访问,http://www.cac.gov.cn/2023-05/22/c_1686402318492248.htm?eqid=e964285800089bd4000。

⑤《国家互联网信息办公室有关负责人就对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定答记者问》,中国网信网,2022 年 7 月 21 日发布,2023 年 12 月 24 日访问,http://www.cac.gov.cn/2022-07/21/c_16600215343064976.htm。

⑥《美光公司在华销售的产品未通过网络安全审查》,中国网信网 2023 年 5 月 21 日发布,2023 年 12 月 24 日访问,http://www.cac.gov.cn/2023-05/21/c_1686348043518073.htm。

⑦林子涵《中国"数字丝绸之路"创造新机遇》,《人民日报海外版》2022 年 10 月 10 日,第 10 版。

支付网络之一，拥有700万用户和30万家合作商户，每月交易额达30亿美元”①。因此，我国数据法域外适用体系的建构应秉承兼收并蓄的理念，积极参与全球数据治理，既要顺应引导本国数字市场发展的内向性要求，也应兼顾保障互联网企业走出去的外向性需要，保护企业的海外合法权益，推动“数字丝绸之路”的高质量发展。

2.致力“应对性”追求

一方面，应对域外数据控制者的不当行为影响，维护国家安全、公共利益与公民权益。在实践中，以逐利为目的的数据控制者存在过度收集、使用和处理数据的倾向。对此，我国近年来不断完善数据法律体系，总结数据治理的中国经验。不同于欧盟以人格与身份为核心的“保护性”数据立法，我国《个人信息保护法》更加具有实用主义的特点，其保护的法益涵盖了人格与人身财产安全等多项权益②。同时，作为发展中国家，我国强调数据的跨境流动不能有损国家安全。在此基础上，我国应协调内外部数据市场，探寻中国特色数据法域外效力的系统性延伸方案。不仅如此，通过完善数据法域外适用体系，我国亦可与全球数据治理建立内外联动模式，推动数据流动国际规则的形成，为全球数据治理贡献中国方案。

另一方面，主动解决外国数据法域外效力规则的滥用问题，积极有效地应对外部风险挑战。习近平指出，在信息领域没有双重标准，各国都有权维护自己的信息安全，不能牺牲别国安全谋求自身所谓绝对安全③。我国于2020年提出《全球数据安全倡议》，呼吁“各国应尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人获取位于他国的数据”④。然而，以美国CLOUD法案为代表的“干涉性”数据域外适用体系存在较高的滥用风险，我国应充实数据法律工具箱，建立完善阻断制度，赋予企业国内救济途径，以避免我国境内数据的被动开放风险。

（二）推动我国数据法域外效力的合理适度延伸

目前，我国《个人信息保护法》与《数据安全法》采用数据处理的“行为发生地标准”，即无论数据处理者是否在中国境内，只要其数据处理行为发生在我国，就应受我国数据法的调整。“行为发生地标准”看似适用范围广泛，但数据在传输过程中，可能会涉及多个位于不同位置的服务器以及遍布全球的网络线路，致使在实践中数据处理行为地难以被准确认定。同时，我国《个人信息保护法》第三条规定的具有域外效力的条件，包括“以向境内自然人提供产品或服务为目的”或“分析、评估境内自然人的行为”等情形，在表达上具有模糊性，在实践中较难界定。对此，我国可借鉴域外立法模式，完善数据法域外效力规则。

首先，采用“设立机构标准”的域外适用模式。相较“行为发生地标准”，欧盟数据法的“设立机构标准”作为客观的连接点，在实践中更容易聚焦物理地点的关联性。为保障数据法调整范围的周延性，“设立机构标准”应包含域外企业在我国境内设立的分支机构或具有法人资格的子公司。

其次，吸纳“目标指向标准”作为补充。当前中国网络用户人数已位居世界首位，数字经济规模位列全球第二，这既反映出我国数据产业的强大实力，也对数据保护提出了更高要求，因此，以效果原则为连接点，对拥有巨型数据市场的我国尤为重要。在此基础上，发挥我国司法的能动作用，也有助于提高数据法域外适用的灵活性。作为技术日新月异的新兴领域，与数据相关纠纷的产生，往往也会创设一个部分或者全部不受规范所约束的新场域，冲突成为促使新规范建立的催化剂，致使新规则不断地被创造、旧规则不断地被改进⑤。因此，我国法院应秉持能动司法的姿态，将行为对国家安全和利益的影响作为连接点，探寻域外数据处理行为与我国的实际联系方案。同时，不仅应关注个案的审理，更应积极评估纠纷所涉及的各方利益与多元价值，分析阐释数据跨境流动治理的中国立场。

再次，我国数据法域外适用体系的建构应坚守国际法治轨道。美国“外向干涉型”数据法域外适用体系

①科菲·库阿库《携手共建“数字丝绸之路”（观点）》，《人民日报》2023年5月29日，第17版。

②丁晓东《〈个人信息保护法〉的比较法重思：中国道路与解释原理》，《华东政法大学学报》2022年第2期，第73页。

③习近平《弘扬传统友好 共谱合作新篇——在巴西国会的演讲》（2014年7月16日，巴西利亚），《人民日报》2014年7月18日，第3版。

④《全球数据安全倡议》，《人民日报》2020年9月9日，第16版。

⑤林福辰《全球治理体系变革视域下的中国国际商事法庭：功能承载与发展展望》，《四川大学学报（哲学社会科学版）》2024年第2期，第196页。

是“美国优先”理念下的产物,存在滥用倾向。因此,我国应防范美国 CLOUD 法案不当适用所引发的消极影响,而不是将“数据控制者标准”作为借鉴模板。构建我国域外适用的法律体系,应以得到国际法认可的管辖原则或与相关国家缔结的国际条约作为依据,从而与美式“长臂管辖”划清界限。如出现法律冲突,应秉持多边主义,考虑其他国家的合理利益与关切,通过协商谈判予以妥善解决。

(三)完善外国数据法不当域外适用的阻断机制

我国《数据安全法》第三十六条规定,非经我国主管机关批准,境内主体不得向外国司法或执法机构提供存储于我国境内的数据。然而,在外国强制数据调取的证据开示要求和我国数据监管的双重压力下,企业履行任何一方的义务都会遭到另一方的惩罚,进而陷入左右为难的境地。为避免给企业带来不必要的合规义务,衡平关键数据本地化监管与外国数据披露要求的内在张力,成为当前亟待解决的问题。

针对外国数据法的不当域外适用,我国应完善阻断立法,丰富企业救济途径。通常而言,阻断法是指在管辖权冲突的情况下,禁止在本国管辖范围内适用外国具有域外效力的法律并消除其影响的一类国内法的统称①。广义的阻断法包含了应对不当域外证据开示的法律,以及应对次级经济制裁的法律②。目前,我国《阻断外国法律与措施不当域外适用办法》(以下简称《阻断办法》)的适用前提仅限于在“违反国际法和国际关系基本准则”的条件下,不当禁止或者限制我国主体与第三国(地区)进行正常的经贸及相关活动的情形,即针对次级制裁的阻断,无法涵盖外国滥用数据法域外效力规则要求数据控制者开示证据的情形。因此,在《阻断办法》基础上,我国可从公力阻断与私人救济两方面建构数据法阻断规则。其一,以美国 CLOUD 法案为代表的数据法域外效力规则,本质上是借助单边手段获取电子化的司法证据,符合广义阻断语境下的损害他国司法主权的取证情形。对此,法国 2022 年修订的《阻断法》,明确企业在面对外国数据披露要求时,有向法国政府报告的义务③。目前我国《阻断办法》的法律位阶偏低,考虑到外国数据法不当域外适用的现实威胁,应打破《阻断办法》规则供给不足及法律位阶低的掣肘,推动制定《阻断法》④,并将外国数据法不当域外适用所涉及的证据开示纳入阻断范围。同时,考虑到数据无边界的属性,数据传输阻断禁令的申请主体可由“中国公民、法人或者其他组织”,扩展为“在中国有经常居所地的公民和在中国有营业地的法人或者其他组织”。其二,拓展私人救济途径,突破企业的“两难困境”。《阻断办法》第十一条规定,我国企业因未遵守外国法律受到重大损失的,我国政府可以根据具体情况给予必要的支持。针对数据产业的特殊性和敏感性,我国应细化企业申请政府支持的标准以及政府提供补偿的形式。2023 年 9 月,我国颁布《外国国家豁免法》,其第四条授权我国法院在特定情形下管辖以外国国家为被告的民事案件。在此背景下,我国应完善追偿程序,明确追索求偿诉讼的请求权基础和案件的管辖范围,准许因外国滥用数据法域外效力规则而遭受损失的我国自然人、法人或者其他组织在国内法院起诉并要求赔偿。

[责任编辑:苏雪梅]

①叶研《欧盟〈阻断法案〉述评与启示》,《太平洋学报》2020 年第 3 期,第 53 页。

②徐伟功《论次级经济制裁之阻断立法》,《法商研究》2021 年第 2 期,第 188 页。

③French Law No. 2022-207.

④王淑敏、李倩雨《中国阻断美国次级制裁的最新立法及其完善》,《国际商务研究》2021 年第 4 期,第 27 页;郭烁《云存储的数据主权维护——以阻断法案规制“长臂管辖”为例》,《中国法律评论》2022 年第 6 期,第 81 页。