欧盟数据战略的目标冲突与中间道路*

王中美

[内容摘要] 欧盟数据战略认为,在数字时代应兼顾提高数据保护标准和便利国际贸易。欧盟模式在确保对数据的高度保护的同时,也通过允许多种机制的跨境传输实践了一种中间道路,为许多国家提供了一个以规则为基础、通过动态平衡协调多个相互冲突的目标的方案。全球数字经济发展需要数据开放和流动的支撑,需要更明晰的数据治理规则环境,因此欧盟的数据战略将产生深刻影响。

[关键词] 欧盟 数据战略 隐私保护 跨境流动

[作者简介] 王中美,上海国际问题研究院研究员

2020 年 2 月,欧盟委员会公布了《欧盟数据战略》,正式提出并描述了欧盟在未来五年打造数据经济的政策措施与投资战略。同时发布的还有《塑造欧洲的数字未来》和《人工智能白皮书》两份欧盟委员会报告。数据、数字经济、人工智能三者密切联系在一起,其中数据可能是赋能的基础要素,对欧盟来说也关涉人文精神与价值观。从过去十年欧盟的努力来看,欧盟数据战略仍然有很多冲突性的矛盾需要解决,其选择的道路较之美国和亚洲一些国家具有独特的中间模式特点。

一、欧盟数据战略的沿革与变化

(一)第一阶段:促进公共部门信息的再利用

欧盟数据战略的核心是“解锁各种类型数据的再利用潜能和创造欧洲数据

* 本文系国家社科基金重大专项课题“‘一带一路’建设与国际经贸规则研究”(项目编号:19VDL019)的阶段性成果。

共同空间”。[①] 欧盟初期的努力主要聚焦于“公共部门信息”(public sector information)的再利用。2002 年欧盟委员会建立了一个专门的“公共部门信息专家组”(PSI Group),2003 年发布了第 2003/98/CE 号指令(2013 年被 2013/37/UE 号指令修正),[②]其主要内容是要求成员国之间应该对公开信息的共享和再利用加以鼓励和提供便利。欧盟并就此制定了一套最低规则(minimum set of rules),但是否授权再利用的决定权仍然保留在各成员国。值得一提的是,欧盟之所以选择从公共部门信息入手,是因为早在 1995 年通过的第 95/46/EC 号指令[③]规定了对个人信息(personal information)的强有力的保护。按照 95/46/EC 指令的规定,个人信息不得被以与之最初被收集时特定的、明确的和合法的目的不一致的方式被进一步处理和收集。这基本上堵住了个人信息再利用的可能途径。

作为公共部门信息再利用的范本,欧盟委员会首先从自身做起,免费在线开放了其所拥有的统计数据、出版物和法律文件。2011 年欧盟委员会通过第 2011/83/EU 号决定[④],将其信息的共享再往前推一步,建立一个数据门户以进一步简化数据的再利用。欧盟委员会的决定仅为信息的商业和非商业使用设置了三个条件,即注明出处、不得扭曲和欧盟委员会不为信息使用的后果承担任何责任。2013 年欧盟发布了“数据供应链倡议”[⑤],其核心是建立“公私伙伴关系(public-private partnership,PPP)”,希望在公有部门努力的基础上,将更多的私人部门纳入到全欧数据生态圈中。但公共数据的共享问题在成员国层面推行的情况参差不齐,比较有成效的建设仍然集中在研究和教育领域,如建立了“泛欧研究与教育数据网络”。

---

① “Data Policies and Legislation,” https://ec.europa.eu/digital-single-market/en/data-policies-and-legislation.

② “Modifiant la Directive 2003/98/CE Concernant la Réutilisation des Informations du Secteur Public,” https://eur-lex.europa.eu/legal-content/FR/ALL/? uri=CELEX:32013L0037.

③ European Parliament and the Council, “Directive 95/46/EC of the European Parliament and of the Council,” https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:31995L0046&rid=5.

④ European Commission, “Commission Decision of 12 December 2011 on the Reuse of Commission Documents (2011/833/EU),” https://eur-lex.europa.eu/legal-content/en/TXT/? uri=CELEX%3A32011D0833.

⑤ European Commission, “A European Strategy on the Data Value Chain,” https://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm? action=display&doc_id=3488.

“数据供应链倡议”服务于欧洲“地平线 2020 计划”[①],特别鼓励科学数据在欧洲内部的共享和再利用,以促进欧洲整体科技与创新能力的提升。所谓“公私伙伴关系”实际上是希望将公共部门和私人部门动员起来,打造欧洲内部密切结合的数据生态系统。其具体措施包括鼓励大学、研究机构和企业的联合研发,促进成果转化;培养数据相关合格人才;对中小企业特别扶持;鼓励对数据领域新创或成长企业投资;加快电子政务建设;公有部门率先采购新数据服务;广泛的数据可得和再利用;基础设施建设,包括网络、存储器和便利研发的设备的建设;欧洲范围内云计算使用。通过这些措施,数据生产、存储、处理、采购和再利用的供应链能进一步通畅起来,直接作用于数据产业的发展。直到今天,这些措施仍是欧洲数据战略的重要组成部分。

(二)第二阶段:打造数据驱动的经济

2013 ~ 2016 年,欧盟又出台了一些政策和立法,基本上围绕“公私伙伴关系”,致力于发挥数字技术在欧盟经济中的推动作用。这一时期的关键词是“数据驱动的经济(data-driven economy)”[②],重心是全欧网络等基础设施的可用性、互联和速度。[③] “数据驱动的经济”被认为具有以下几个特点:(1)高质量的、可靠的和可互操作的数据资产(datasets)和高效的基础设施;(2)能够便利数据资产增值的完善的框架条件,包括人才、法律和公私合作等;(3)大数据能发挥作用的大量应用领域,既包括强大的信息与通信技术硬件系统,也包括公共部门通过采购、试用扮演数据产品的首批客户角色等。[④]

在这一阶段,欧盟已经发现自己在大数据时代远远落后于美国,而且缺乏产业能力,有竞争力的企业也比美国少得多。欧洲一方面已经暴露出在网络基础设施、代表性企业、产业运用、数据人才等方面的短板,另一方面其严苛复杂的法

---

① 欧洲地平线 2020 计划是目前为止最大的欧盟研究与创新计划,首期投入(2014 ~ 2020)预计达 800 亿欧元。该计划将鼓励具有突破性的世界一流的科技成果向市场转化。参见“What is Horizon 2020,” https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020。

② European Commission, “Digitising European Industry,” https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry.

③ “Connectivity for a European Gigabit Society,” https://ec.europa.eu/digital-single-market/en/policies/improving-connectivity-and-access.

④ European Commission, “Towards a Thriving Data-driven Economy,” pdf, pp.5 ~ 6.

律环境加大了数字资产接入的难度并制造了创新的障碍。[①] 但是,欧盟也认为,促进数据驱动的经济的条件是提高数据的保护水平和信任,因为这对数据驱动的经济至关重要。

这一时期与数据战略密切相联系的是欧洲“数字单一市场”(digital single market,DSM)战略。[②] “数字单一市场”战略提出在欧洲实现人员、服务和资本流动的自由化之外,推动网络和在线活动的无缝接入,以促进欧洲内部竞争条件的公平。这一战略要求高效的基础设施,包括云计算、超级计算器、5G 网络、物联网和公共数据设施。在 2014 ~ 2019 年期间,欧洲战略投资基金(EFSI)向数字经济领域投入了 413 亿欧元,同时与成员国共同投入 10 亿欧元建立世界级的欧洲超级计算机设施;[③]约 2800 个欧洲城市被挑选获得价值 15000 欧元的 WIFI4EU 免费券,该项目在城市的公共区域(市政厅、图书馆、博物馆、公园等)建立 WIFI 热点;欧洲 5G 项目正在推进;同时还希望在 2020 年对所有市民和企业提供“一键进入”的行政手续办理,即“单一数字门户”(sing digital gateway)。除了基础设施的改进外,“数字单一市场”战略还聚焦于法律与规则的保障。欧盟委员会提出了 30 项法案,其中 28 项获得通过,涵盖了包括电子商务、在线平台、电子合同和签名、价格透明度、无障碍电子阅读等方方面面的细小领域,以推动从商务到生活的数字经济的便利化。

尽管迫切希望推进以数据驱动的经济和数字单一市场,欧盟也认识到由此产生的规制问题。这些规制问题为数据战略的推进消除障碍的同时也可能形成新的阻碍和限制。2014 年以来,欧盟对于数据规制的关注主要聚焦于四个方面。(1)个人数据保护和消费者保护。这一问题在欧洲是广泛关注的社会问题,涉及价值观和人权,因此是非常复杂的社会、政治、经济、法律和技术问题。(2)数据挖掘(data mining)。这主要涉及著作权。(3)由大数据引起的信息安全问题。

---

① European Commission, “Towards a Thriving Data-driven Economy,” pdf, pp. 2 ~ 3.

② European Commission, “A Digital Single Market for the Benefit of All Europeans,” https://ec. europa. eu/digital-single-market/en/news/digital-single-market-benefit-all-europeans.

③ 欧洲超算项目(The Euro HPC Joint Undertaking)建立于 2018 年,目标是在 2020 年底前建成世界级的超算中心,用以支持包括医药、生物工程、气候、新材料、油气开发、飞机和汽车设计以及智慧城市方面的产业发展,目前已有 30 个欧洲国家参加了这一项目。

这涉及基础设施要求、责任分割、数据使用等方面。(4)所有权和数据传输。数据的本地存储在一些领域的要求限制了数据的跨境流动,进而对欧盟在云计算和大数据方面形成单一市场构成障碍。欧盟特别关注物联网技术获得的数据的所有权和相关责任。

(三)第三阶段:在高保护前提下推动私人部门数据的再利用

2018 年以后,欧盟开始将数据再利用的触角向私人部门(private sector)持有的数据延伸,其重点是在线收集的数据和物联网(IoT)技术运用后产生的数据。欧盟提出大数据分析工具和人工智能运用将是重要的技术引擎,这都离不开数据的共享和再利用。[①] 对于私人部门数据的再利用,欧盟提出了 B2G(business to government)和 B2B(business to business)两种模式。B2G 强调私人部门为公共部门提供数据收集、分析和处理等服务,帮助公共部门提高在城市规划、疫情防控、道路和交通管理、环境保护、市场监控和消费者保护方面的能力。B2B 则主要针对物联网产生的数据的再利用,是机器产生的非私人的数据在企业之间的共享,其出发点是为了公平竞争和鼓励后续创新。

从实际的成效来看,B2G 在政府的推动下先行一步。欧盟委员会公布的最佳实践案例也主要集中在 B2G。[②] 例如,在芬兰,森林每年提供约 84 亿欧元的国内生产总值,而大多数与森林相关的数据可以从 Metsään. fi 网站上获得。这一门户网站联结森林所有者和第三方服务提供者,网站上的数据都以隐名的形式提供,如果要获得具名的信息,则要依法通过特定的注册程序获得。在 B2G 模式下,芬兰森林中心(芬兰农业与森林部下属的公共机构)也在建设一个重要的新数据平台,推动数据(包括气候、环境、规划、木材等)在私人部门的运用,如向私人部门提供木材的采购和成本核算等信息,同时政府也能获得更多渠道的数据。芬兰于 2018 年 3 月开始正式推动森林相关数据的开放,到 2020 年 3 月数据下载

① European Commission, "Guidance on Private Sector Data Sharing," https://ec. europa. eu/digital-single-market/en/guidance-private-sector-data-sharing.

② European Commission, "Good Practices and Pledges on B2G Data Sharing," https://ec. europa. eu/digital-single-market/en/good-practices-b2g-data-sharing.

量达到 10.5TB。[①]

事实上,私人部门持有数据的分享问题一直没有取得突破性的进展,其原因之一是涉及个人信息的数据保护问题。欧盟的《通用数据保护条例》(GDPR)是 1995 年第 95/46/EC 号指令的修订版,其基本原则并没有实质性的变化,只是应信息时代的特点作了具体规则上调整。2018 年 5 月这一条例生效,被认为是欧洲数据战略的重要组成部分。如前所述,欧盟坚持认为,只有在提供充分保护并建立信任的基础上才可能谈个人数据的再利用和流动,因此《通用数据保护条例》也被认为是目前世界上对个人数据保护力度最大的立法。例如,依据《通用数据保护条例》,被界定为个人数据的数据是指可以识别个人的信息,包括姓名、性别、电话号码、住址、身分证字号或是社会安全号码等,以及其他可以直接或间接过滤出特定对象数据的数据类型,如网络浏览器中的 Cookie、网络 IP 地址,或是包括其他足以识别特定个人身份或性别的基因、生物特征或医疗数据等。

简单概括《通用数据保护条例》的内容,可以归结为以下三个原则:(1)所有涉及个人信息收取、处理和利用的活动都必须事先取得当事个人的明确同意;(2)数据持有企业分为"数据控制者"和"数据处理者",二者都负有数据保护的直接责任,需要满足欧盟在硬件、程序和人员配备上提出的一系列要求;(3)在确立安全和充分保护的前提下,鼓励数据,特别是非个人数据在欧盟内部的自由流动;在严格的条件下,可以允许个人数据转移到经欧盟认定具备充分保护水平的第三国、[②]第三国的某个区域或特定部门以及国际组织;同时也允许跨国企业内部在具备"有约束力的公司规则"(binding corporation rules,BCR)[③]下进行数据转移。《通用数据保护条例》被称为最严的数据保护法主要体现在对违反行为的巨额罚金,但该条例也明确规定,不能以保护个人数据中的相关自然人为由,对欧

① "Good Practices B2G Data Sharing Finnish Forest Data Ecosystem," https://ec.europa.eu/digital-single-market/en/news/good-practices-b2g-data-sharing-finnish-forest-data-ecosystem.

② 截至 2020 年 2 月,欧盟已对 13 个国家给予安全认定,包括安哥拉、阿根廷、加拿大(商业组织)、法罗群岛、格恩西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、乌拉圭和美国(仅限于隐私盾框架)。参见 "Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection," https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en。

③ 在《通用数据保护条例》之前,已有部分欧盟成员国的监管机构接受"有约束力的公司规则",包括埃森哲、宝马汽车、惠普、摩托罗拉等 72 家跨国公司获得了"有约束力的公司规则"的认可。

盟内部个人数据的自由流动进行限制或禁止。《通用数据保护条例》是以建立保护为前提推动数据的流动,但也在公共利益、个人其他重大利益、数据控制者的正当利益等方面进行了一定的平衡,设定了许多限制条件。

《通用数据保护条例》的实施对欧盟的数字经济带来了巨大的影响。所有在欧盟经营或从欧盟获取数据的企业都需要遵守《通用数据保护条例》,因此这一法令较之过去任何一次指令、行动和倡议,都更为私人部门所重视。从这个意义上来看,欧盟的数据战略上了一个新的台阶。随后 2018 和 2019 年欧盟又密集出台了《非个人数据自由流动条例》、[①]《网络安全法》、[②]《公开数据指令》[③]等法律法规。在这样的背景下,2020 年 2 月欧盟委员会公布的《欧盟数据战略》报告[④]继续列明欧盟在未来五年将要采取的政策措施和投资。报告提出,全球数据总量将从 2018 年的 33ZB 增长至 2025 年的 175ZB,这将带来巨大的机遇,因此为欧盟设定了三个 2025 年数据目标(基于 2018 年的数字),即(1)数据经济的产值从 3010 亿欧元增长到 8290 亿欧元;(2)数据专业人员数从 570 万人增长到 1090 万人;(3)欧盟具有基本数字技能的人口占比从 57% 增长到 68%。[⑤] 报告特别提出,希望通过一系列的政策和措施使得欧盟在数据经济中的份额至少与其经济体量相当。

---

① European Parliament and of the Council, "Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-personal Data in the European Union," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri = CELEX:32018R1807.

② European Parliament and of the Council, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)," https://www.legislation.gov.uk/eur/2019/881/contents#.

③ European Parliament and of the Council, "Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-use of Public Sector Information (Recast)," https://www.legislation.gov.uk/eudr/2019/1024/contents#.

④ European Commission, "A European Strategy for Data," https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

⑤ European Commission, "European Data Strategy: Making the EU a Role Model for a Society Empowered by Data," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy.

二、欧盟数据战略的目标冲突:一体化、隐私保护、流动和竞争力

尽管欧盟从 2002 年开始关注公共部门信息的共享问题,但是将数据问题上升到战略角度不过是近十年时间的事。事实上,在美国 20 世纪 90 年代开始的数字经济创新浪潮中,一大批美国企业崛起并垄断了社交媒体、在线购物、网络游戏和智能手机等消费领域。进入 21 世纪,日本、韩国、中国等亚洲国家的企业也陆续成长起来后,欧盟发现自己在信息技术设施、设备、网络和内容各方面都落后了。根据麦肯锡报告,目前欧洲数字经济占国内生产总值的比例约为 1.7%,大大低于美国的 3.3% 和中国的 2.1%。[①] 特别是数据方面,欧洲企业的数据基本上都存储在亚马逊、谷歌和微软的云服务。在人工智能技术的催化下,欧盟对这些数据增值服务的依赖可能继续加大,因此这对欧洲来说是关涉政治、经济、社会、文化的重要问题。

依据 2020 年 2 月欧盟委员会发布的《欧盟数据战略》,欧盟数据战略的目标是确保欧盟在数据赋能的经济中成为领导者,为此,它希望通过建立一个真正的欧盟数据空间(data space)、一个单一数据市场(single market for data)去解锁更多未经使用的数据,允许这些数据在欧洲内部和各部门间自由流动,以促进经济增长和创新。虽然在很多场合,欧盟表达了对数据控制权和竞争力的担忧,但其公布的数据战略仍然是比较宽泛和灵活的,并未有非常细致、具体的安排,这是因为欧盟希望保留数据市场的活力和自由。欧盟委员会主席乌尔苏拉·冯德莱恩说:“今天我们展示了塑造欧洲数字未来的雄心壮志。它涵盖了从网络安全到关键基础设施、从数字教育到技能、从民主到媒体的一切。我希望数字欧洲反映出欧洲最好的一面,即开放、公平、多样化、民主和自信。”[②]

尽管理想高远、道德标杆立得很高,欧盟可能无法同时实现这么多商用和非

① 《默克尔急了!三季度 GDP 仅增 0.1%,敦促欧盟夺回数据控制权》,https://news.hexun.com/2019-11-16/199292480.html。

② 《欧盟发布人工智能白皮书,计划每年吸引 200 亿欧元 AI 投资》,https://new.qq.com/omn/20200220/20200220A0PENI00.html?pc。

商用的目标。欧盟的数据战略与数字经济、电子商务、人工智能等问题密切相联,但又更为敏感复杂,在实践中一直以来就存在一些自相矛盾和自我冲突的问题。如前文所展示,过去三个阶段的欧盟数据战略的推进基本上仍然局限于数据在公共部门的共享和公共部门如何更好地利用数据服务上,法规法令则主要是提高私人数据的保护,以建立流动的信心。这些还都是基础工作,关键是下一步数据如何流动和更好地应用于经济。欧盟仍然要解决下述三个重要矛盾或冲突,才可能推动欧盟数据赋能的经济的实质变化。

(一)欧盟数据单一市场与成员国数据主权的冲突

欧盟数据战略提出,首先应当建立恰当的数据治理、接入和再利用的法规框架,以促进数据在欧盟内部的自由流动。以《通用数据保护条例》为例,在强调个人数据保护的前提下,该条例特别规定了"一站式(one-stop)"数据保护监管模式。简单来说,企业如在欧盟多个成员国有业务营运的,可以选择一个成员国的监管机关作为带头监管机关(lead supervisory authority,LSA),企业只需要与这个带头监管机关对接《通用数据保护条例》中的数据保护监管事务,而无需分别与多个成员国的监管机关打交道。原则上,企业应选择其主要机构(main establishment)所在地的监管机关为带头监管机关。[①] 如果涉及对该企业的投诉递交到其他成员国监管机关的,其他成员国监管机关应当不迟延地报告给带头监管机关,而带头监管机关应当在三周内决定具体由哪家监管机关处理该投诉,所有监管机关应当加强合作。

这一看似理想的一站式架构却也反映了欧盟内部仍然存在多国监管的难点。虽然通过《通用数据保护条例》的实施,各成员国在数据保护方面实现了法规框架的基本一致,但各成员国在具体规定、程序、效率等方面仍然存在诸多的不一致。[②] 而且《通用数据保护条例》第56(2)条明确规定,如果一项侵权行为发

① European Commission, "Guidelines on the Lead Supervisory Authority (WP 224 rev. 01)," https://ec.europa.eu/newsroom/article29/item-detail.cfm? item_id=611235.

② 以德国为例,德国的数据监管权不在联邦层面,而是交由16个州政府,为了协调执法,联邦层面成立了"数据保护会议"。同时,德国联邦数据保护与信息自由委员负责电信服务中的数据保护问题,并作为德国代表参加欧盟数据保护委员会。

生在其境内或实质性影响了其境内数据当事人,成员国监管机关有权执法。这一规定使得带头监管机关的作用也很有限。为了进一步解决多国监管的问题,欧盟又成立了“欧盟数据保护委员会”(European Data Protection Board,EDPB)。该委员会由各成员国监管机关的代表组成,负责监督《通用数据保护条例》在全欧的实施,可以对跨国数据处理问题作出有约束力的决定,同时发布相关指南,指导全欧对条例的一致解释。①

《通用数据保护条例》对违反行为规定了高昂的罚金——最高达该企业全球营收的 4% 或 2000 万欧元,但这在各自为政的多国监管体系下也存在实施的冲突问题。在《通用数据保护条例》出台之前,跨国数据保护问题可能由多国监管机关依照本国法律进行执法并处以罚金,这可能存在同一行为的叠加调查或叠加惩罚。《通用数据保护条例》出台之后,类似跨国案件可能提交给欧盟数据保护委员会,由涉案成员国的监管机关代表共同选择一个牵头机关,此牵头机关作出的调查决定或者经所有涉案成员国同意或经所有成员国多数表决通过,可以对所有涉案成员国有约束力。这就一定程度地避免了叠加和冲突。

但是这是理想情况,即多国监管机关同时发现涉案行为,并决定提交给欧盟数据保护委员会。在实践中,情况要比假设的理想情况复杂得多。数据当事人所在地、主要侵权行为发生地、数据控制者主营地等可能在不同的成员国,执法时间可能有先有后,重点和角度也千差万别。尤其是在涉及法院司法程序的情况下,问题可能更多。各成员国法院遵循的国内数据侵权法律与《通用数据保护条例》在欧盟层面的实施之间也存在协调问题。总的来看,由于未能建立统一的执法与司法体系,跨国数据的保护关涉各成员国的数据主权(data sovereignty)问题,目前相互间的权限冲突并不能依靠欧盟数据保护委员会完全解决。而且,由于数据跨国收集和处理在欧盟广泛存在,数据归属始终是个突出的问题。

(二)隐私保护与数据再利用的冲突

按照欧盟数据战略的基本思路,首先应当建立个人数据得到充分保护的信

① European Commission, “EU Data Protection Reform: Ensuring its Enforcement,” https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-role-edpb_en.pdf.

任,才有可能推动个人数据的流动和再利用。在2020年的《欧盟数据战略》中,欧盟提出将特别关注以下领域数据的应用:工业制造、“绿色”数据、可持续发展、流动、健康、金融、能源、农业、公共行政等。[①] 这些领域的发展可能涉及两方面活动产生的数据,一是物联网数据,即由机器产生的数据;二是人的数据,即由消费者或使用者产生的数据。物联网数据由私人部门所有和控制,共享和流动的问题还相对简单,而人的数据的所有者、控制者和利用者都可能不同,且因为可能涉及隐私,在欧盟引起特别大的关注。另外,由于第二方面人的数据大量被收集和掌握在美国公司手中,这更引起欧盟的忧虑,因此才有了《通用数据保护条例》的出台。

《通用数据保护条例》规定,个人数据的采集只能用于指定的、明确的、合法的目的,不得采用与这些目的不相符的方式进行进一步处理。数据当事人必须能够访问其个人数据,且有权对违反指令要求进行处理的个人数据进行整改、擦除或屏蔽。数据控制方必须采取适当的技术和组织措施,防止个人数据遭受意外或非法破坏、意外丢失、篡改、越权披露或访问。关于个人数据的保护,《通用数据保护条例》为控制和处理数据的企业创设了很多实体和程序上的义务,这些繁复的义务及严厉的罚金设定的出发点就在于保护个人隐私。这被认为是欧洲人文精神和价值观的体现。

但是,在个人数据保护非常严格的情况下,究竟数据可能因为安全和信任而更广泛地流动,还是因为障碍过高而不能有效地流动,是一个并没有定论的假设前提。欧盟选择相信以保护为前提、以信任为基础的流动在欧洲这样的社会里会得到更多的接受。但从实践效果来看,初始收集和利用个人数据阶段的责任设置已经很复杂,如果进入再利用渠道,责任划分可能更加具有不确定性。在这样的情况下,企业很可能因为担心承担个人数据泄露的责任而不愿意公开和共享有关数据。如何促进私人部门所掌握的个人数据的再利用一直是个难题,而

① “Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence,” https://ec.europa.eu/eip/ageing/sites/eipaha/files/news/shaping_europe_s_digital_future_commission_presents_strategies_for_data_and_artificial_intelligence.pdf.

提高隐私保护并不能破解。简言之,加重隐私保护责任与数据流动之间本身就存在天然的冲突。

在欧盟,这个冲突还会被进一步放大。欧洲的个人数据大多数由美国的互联网或云服务公司控制,所以欧盟既想对这些跨国公司加诸责任,又希望个人数据最终服务于欧盟产业和市场,其本身能调用的工具已经捉襟见肘。欧盟规定,个人数据不得传输到欧洲经济区以外的国家或地区,除非该国家或地区能确保与个人数据处理相关的数据当事人的权利和自由得到充分的保障。与美国达成的"隐私盾(privacy shield)协议"在很大程度上是因为欧盟处于较为被动的位置,虽然有一系列美方政府承诺、[①]争端解决程序安排和年度联合审查的安排,但在欧盟内部仍然有社会团体以隐私保护不力为由加以反对。[②] 尽管如此,欧盟已经认识到,如果一味强调保护个人数据,将个人数据固守在欧盟内,不允许传输或流动,从长远来看,欧盟就不可能获得在数据驱动的经济中的领导者角色。因此,欧盟对数据跨境流动问题一直持中立态度,既不完全支持美国的激进立场,也不赞同中国等国家坚持的绝对数据主权立场。

(三)数据垄断与公平竞争的冲突

从《通用数据保护条例》公布之时起,关于数据接入(access)的问题就一直被认为可能成为该条例与竞争法之间的重叠领域。[③] 在数字经济下,拥有某一领域海量数据本身可能成为重要的资产和竞争优势,因此涉及大数据的限制竞争行为就可能触发竞争法的约束机制。以搜索引擎为例,越多的检索使用数据越能

---

① 美国政府向欧盟出具了书面承诺,公开表示以国家安全为由进行的访问都必须受到约束和监管,保证不会对根据"隐私盾"协议转移到美国境内的个人数据进行不加鉴别的、大规模的监视,批量收集的公民数据只能用于反恐、防扩散、网络安全等六个特定目的,且不得破坏"隐私盾"协议的原则。另外,美国建立了独立于国家安全部门之外的监察专员机制,专门负责跟踪和处理个人提出的投诉和咨询。

② 互联网新技术新业务安全评估中心:《隐私盾:欧盟—美国数据转移规则的最新状态》, https://www.secrss.com/articles/8067。

③ 被广为提及的施雷姆斯(Schrems)案中,原告施雷姆斯就脸谱将欧盟个人数据传递到美国、侵犯个人隐私一事提出申诉。2016 年就隐私盾更新后的申诉书可见 Mag. Maximilian Schrems, "Complaint Against Facebook Ireland Ltd," http://www.europe-v-facebook.org/comp_fb_ie.pdf; 欧盟法院之前就欧美安全港的意见可见"Opinion of Advocate General Bot," http://curia.europa.eu/juris/document/document.jsf?docid=168421&doclang=EN; 关于稳私盾的更多争议,可参考 Hayley Evans and Shannon Togawa Mercer, "Privacy Shield on Shaky Ground: What's up with EU-U.S. Data Privacy Regulations," https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations。

促进后台算法的改进,帮助搜索引擎服务的提供者找到最能匹配相应关键词的内容,这也是谷歌被使用得越多就越拥有压倒雅虎、必应(BING)等其他引擎的优势的原因。在欧盟对脸谱和微信、谷歌和双击这两个重要的互联网公司合并案件的反垄断审查中,欧盟竞争委员玛格丽特·维斯塔格(Margrethe Vestager)指出,尽管一些兼并不涉及很大的营业额(turnover),但是却涉及有巨大商业价值的数据,因此也有必要纳入审查中。[①]

对于中小企业来说,接入和利用大企业所掌握的大数据将有利于它们的成长和创新,但也可能因为数据优势上的不对称,中小企业在与大企业的竞争中处于弱势或被盘剥(exploit)的地位。[②] 这对欧盟而言尤为重要,也是其更关心的问题。福布斯排名前20位的数字企业全部在美国和亚洲,[③]世界营收排名前十名的互联网公司全部来自美国和中国,[④]欧盟的企业确实已经处于数据弱势地位。所以对欧盟来说,当务之急是增强数字经济的竞争力,而数据受制于人是需要突破的瓶颈之一。以反垄断的手段介入数据市场的竞争,要求强制接入大企业所掌握的数据,目前在欧盟层面暂无先例,但欧盟竞争委员在多个公开场合表示了这一可能性。[⑤]

另外,对欧盟来说还有另一个扭转局势的抓手,即"物联网数据"。依据《欧盟数据战略》,未来五年数据的处理和存储方式会发生巨大变化。目前80%的数据存储和数据处理发生在数据中心和中心化的云设施,20%是在智慧联结物品上,如汽车、家居和制造机器人,以及靠近使用者的计算设施,这又称之为边缘计算(edge computing)。但是2025年这两个比例可能会发生对调。欧盟在机器制

---

① Margrethe Vestager, "Big Data and Competition," http://ec.europa.eu/commission/20142019/vestager/announcements/big-data-and-competition_en.

② European Commission, "Online Platforms and the Digital Single Market Opportunities and Challenges for Europe," http://eur-lex.europa.eu/legal-content/EN/TXT/? uri = CELEX:52016DC0288.

③ "Top 100 Digital Companies," https://www.forbes.com/top-digital-companies/list/#tab:rank.

④ 依据Worldatlas的统计,年度营收前25名的互联网企业中,欧盟企业仅占三席。Joyce Chepkemoi, "The 25 Largest Internet Companies in the World," https://www.worldatlas.com/articles/the-25-largest-internet-companies-in-the-world.html。

⑤ 参见European Commission, "Competition Policy for the Digital Era," https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf。

造业方面领先,德国的西门子、法国的阿尔斯通以及一众历史悠久的汽车企业都积累了相当多的工业数据,因此边缘计算将可能是欧盟极力推进的重要领域。

欧盟也没有放弃在云设施方面的追赶。Synergy Research Group 2020 年初发布的新闻称,过去十年企业花费在云服务上的支出从 0 增长到 1000 亿美元,而且增长空间仍然巨大。[①] 目前全球排名前三的亚马逊、微软、谷歌均为美国云服务商,占据了半数以上的全球市场。欧盟数据战略中提出的重点推进工作就是要建立节能、高效和可信的欧盟自有的云设施和服务。《欧盟数据战略》特别提出将与 Gaia-X[②] 协同推进这项工作,并预计于 2020 年第三季度与各成员签署备忘录,避免在云设施上碎片化和重复的建设。对欧盟来说,通过政府推动甚至投资来建立为其所控的云设施,某种意义上就是试图争夺在欧洲市场上的数据垄断地位,特别是在下一轮物联网和边缘计算所需的云设施中胜出。[③] 在此之前,欧盟仍然将举着促进公平竞争的大旗,试图通过竞争法让来自美国和亚洲的云服务企业进行数据分享或通过破除垄断对这些企业进行干预。

三、基于规则的中间道路

从各项指标来看,欧盟要实现成为数据赋能的经济的“领导者”这一愿望还有很长的路要走。如前所述,欧盟既无领先的拥有大数据的企业,也无高额的数据贸易,其自有的云服务设施也仍在建造中。而且,欧盟数据战略本身也并不着眼于数据产业的发展,而是将数据作为重要的要素市场来培养,希望通过推动数据的共享和再利用,充分发挥数据对经济增长及创新的支持功能。因此,欧盟数据战略的立足点是促进数据的流动和充分利用。这又包括两方面,一是数据在

① Synergy Research Group, “The Decade's Megatrends in Numbers-Part 1: Cloud Goes from 0 to 100 in Ten Years while Enterprise Data Center Spending Stagnates,” https://www.srgresearch.com/articles/the-decades-megatrends-in-numbers-part-1.

② 2019 年 10 月 29 日,德国经济部长彼得·阿尔特迈尔(Peter Altmaier)在联邦政府数字峰会(Digital Gipfel)上宣布了一项针对泛欧洲市场的云计划——“Gaia-X”,旨在建立一个安全的数据基础架构,以减少欧洲对亚马逊、阿里云等外国云厂商的依赖,具体的技术和组织构造细节在 2020 年初提交给各欧盟成员国。

③ Fabian Schmidt, “Gaia-X: The Rise of Europe's Connected Data Infrastructure,” https://homo-digitalis.net/gaia-x-the-rise-of-europes-connected-data-infrastructure/.

欧盟内部的流动;二是数据进出欧盟的流动。前者是欧盟极力推动的,从鼓励公用部门数据的再利用到私人部门数据的共享,欧盟希望打造“欧盟单一市场”。欧盟对后者则相对谨慎,但并不完全禁止,欧盟也一直希望在双边和区域层面建立安全认证的框架。

其实,这两方面的数据流动都涉及数据的跨境传输(cross-border data transfer),关涉多个国家的数据主权。因此,对于欧盟来说,数据战略首要解决的问题就是数据主权之间的协调,而为了加强主权之间的互信,必须建立统一的管制框架和统一标准。《通用数据保护条例》的出台就是基于这样的逻辑。通过加强保护建立起彼此的信任,才有可能谈数据的跨境流动。但这样还不够。由于数据多掌握在共享意愿最弱的私人部门手上,必须促进公共部门与私人部门之间的数据共享以及私人部门相互之间的数据共享,才可能真正让数据流动起来,让其效能发挥到最大。因此欧盟通过投资设立公私合作项目,通过竞争执法破除数据垄断和壁垒,最终就是要让私人部门的数据成为具有流动性的要素。

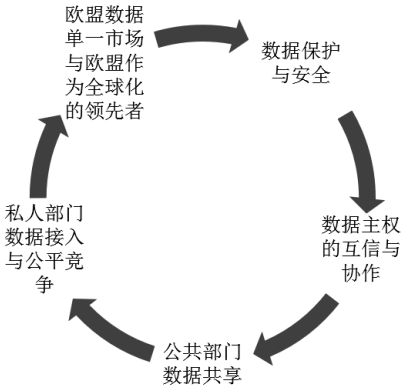

图1　欧盟数据战略的推进逻辑

图表来源:作者整理自制。

综上,对欧盟来说,推动数据战略的过程中需要解决三个冲突,即单一市场与数字主权的冲突、隐私保护与数据再利用的冲突、数据垄断与公平竞争的冲突。这三个问题是嵌套在一起的,而欧盟解决的逻辑或方法也是嵌套在一起的,

形成相互衔接的环形关系(如图 1 所示)。从近十年欧盟数据相关行动的成效来看,主要难点和症结仍然在三点:一是数据主权,即使是欧盟内部的互信与协作也没有完全达成;二是私人部门数据的再利用,仅仅依靠严格的数据保护制度只是创设了前提,并没有提供共享的动力,特别是在大数据企业都是欧盟以外企业的情况下难度更大;三是欧盟的领导力,如果没有领先的云设施和云服务企业,欧盟在数据赋能的下一轮全球竞争中的领导力是没有充分保障的。因此可以预见,欧盟下一阶段战略的重中之重是对自有云设施和以工业数据为基础的物联网的建设。

事实上,欧盟面临的问题与世界上大多数国家是一致的。同样是面对内部的信息共享需求和外部的跨境数据流动问题,全世界至少存在三种以上的模式。一是美国模式。美国既具有强大的科技与产业基础,也具有世界上最大的数据服务贸易量,同时美国着力促进内部和跨境的数据流动,在一系列国际协定和安排中倡导取消数据存储本地化的要求。二是中国模式。中国模式突出信息安全的重要性。中国一方面推动国内数据产业和数字经济的发展,另一方面又严格限制数据跨境流动。三是欧盟模式。欧盟的战略选择可能代表具有典型特点的中间道路,即在数据硬件受制于人的情况下,希望通过提高数据保护水平促进数据的内部和外部流动,以期在下一阶段的全球化中也能受益于数据丰富性带来的创新动力。

上述三种模式,对大多数国家来说,最可能接受和参照模仿的是欧盟模式。美国和中国都具有很突出的特殊性。二者作为数字经济的领先者,都具有坚实的产业基础和广大的国内市场,因此在数据战略实施上占据主动地位。不仅如此,由于在技术和市场上的优势,中美两国以国家安全为名的强势干预都加大了其他国家的疑虑。[①] 所以,大多数国家和欧盟一样,既不想被隔绝在数字经济发展的洪流之外,需要促进数据的流动,又担心被动地接受数据垄断,成为被盘剥

① 以美国 2018 年《澄清境外数据的合法使用法案》(Clarifying Lawful Overseas Use of Data Act, CLOUD)法案为例,该法案允许美国执法机关调取美国企业存储在境外服务器中但由其控制的用户数据,也允许适格的外国企业通过双边或多边司法协助条约调取在美国存储的数据。中国则要求数据必须本地存储,在中国获取的数据除非用户同意,一律不得出境。

(exploit)的对象。欧盟提供的这套方案,如果从静态来看,有许多的目标冲突,如既要高保护,又要促进共享,既要反数据垄断,又要拥有能为己用的关键设施或服务的垄断优势。但是,从动态来看,正如前文所展示的,在矛盾中通过相反的作用力相互修正、相互限制并不断向前推进是一种积极的选择。

表 1　　欧盟关于个人数据跨境传输的多种机制

将个人数据传输至第三国的机制	实施情况
1. 数据当事人的明确同意并用于指定的目的	公布相关指南,作严格的条件限定①
2. 适格决定(Adequacy Decision):获得适格决定后,对该第三国的数据传输不再需要额外许可,等同于欧盟内部传输	目前已有 13 个适格国家或地区,其中对美国的适格决定按专门的"隐私盾协定"执行
3. 标准合同条款(standard contractual clauses):供数据出口方与进口方采用,明确双方在数据安全和保护上的义务	已发布两套标准合同条款和一套非标准合同条款
4. 有约束力的公司规则(binding cooperation rules,BCR):针对跨国公司或关联公司内部的数据传输,经欧盟认证(向带头临管机关申请)在公司内部建立了相应保护水平的传输规则	在欧洲经营的许多知名公司申请了有约束力的公司规则认证②
5. 适当的安全保障(appropriate safeguards):数据的控制者或处理者可以通过采用经批准的行为准则或认证机制(如隐私封口或标记)达到对个人数据的适当保护以进行跨境传输	这项 2016 年新增的传输机制具有很大的灵活性,可以针对行业或个体特点量身定制。该机制也可用于在国际协定或行政安排下公有部门之间的数据传输

图表来源:作者整理自制。

事实上,欧盟方案还通过两个重要因素发挥示范性影响,一是全球跨国企业都不能忽视的欧盟市场;二是欧盟在规则制定上具有的优势。欧盟从立意实施数据战略以来便致力于规则化道路并密集制定了一系列与数据相关的规则,包括数据保护、公有部门数据再利用、非个人数据自由流动、网络安全等相关法规。

① 参见"Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679," https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf。

② 欧盟委员会网站上公布了截至 2018 年 5 月 24 日建立有约束力的公司规则名单。European Commission, "Binding Corporate Rules (BCR): Corporate Rules for Data Transfers within Multinational Companies," https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en。

单以数据跨境传输问题为例,欧盟规定了至少五种可以将个人数据传输至第三国的机制(如表 1 所示),每一条件都有较为公开透明且能为企业所运用的规则和程序。这一强调对等保护前提下开放跨境传输的规则模板也被欧盟之外许多国家,如新加坡、日本、印度等纷纷效仿。正由于欧盟《通用数据保护条例》和其他一系列法律法规标准比较高,在按欧盟的要求调整公司合规操作后,如果世界上其他主要市场也能有较为一致的要求,跨国公司将不再增加额外的合规成本。[①]

所以,欧盟的数据战略可以被视为一种中间道路,如欧盟委员会自己描述的兼合对跨国数据流动的开放性与对个人数据的高保护。欧盟因此有潜力成为"数据服务的中心节点(hub),这样的节点同时需要自由流动和信任"。值得一提的是,欧盟并未在自由贸易协定中推广《通用数据保护条例》模式,而更多地强调非歧视原则。欧盟认为,数据保护和贸易谈判是分开的两个轨道,只有"适格决定(Adequacy Decision)"是建立在彼此信任基础上允许数据跨境传输的最佳通道。[②] 言下之意,欧盟不会因贸易利益牺牲或交换在数据保护和跨境传输上的原则和标准。欧盟也认为,目前国际贸易协定谈判中涉及的两方面内容——电子商务和跨境数据流动的根本问题是关于这两方面的国内规定或国际安排(无论是便利化措施还是限制措施)都不应构成对贸易的扭曲,[③]不是强求对方接受《通用数据保护条例》的相应标准或直接要求对方取消数据的跨境流动限制。通过将数据保护标准和贸易谈判问题分离,欧盟试图在尊重各国数据主权的前提下,以温和的方式处理数据跨境流动。[④] 这也不失为一种中间道路。

---

① European Commission, "Exchanging and Protecting Personal Data in a Globalised World," https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vkaybywjxhzg.

② Ibid.

③ 参见"EU Provisions on Cross-border Data Flows and Protection of Personal Data and Privacy in the Digital Trade Title of EU Trade Agreements," https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157129.pdf。

④ 例如,贸易协定中建议可以规定,如果成员方要求保留对数据跨境处理的限制,如数据本地存储要求,那么这样的限制措施不应构成对第三方公平贸易机会的损害。开放措施亦然。

四、结　语

总的来看,欧盟的数据战略历经20年并在近五年时间里真正成熟并形成完整的规则框架。在大数据时代被夹在中间的欧盟,试图在坚持数据高标准保护和推动数据跨境流动自由化两端之间开拓一条颇具特色的中间道路。通过《通用数据保护条例》及一系列法律法规的出台,面对市场融合和数据主权之间、隐私保护和数据流动之间、数据垄断和公平竞争之间的固有冲突,欧盟通过动态平衡创造了一种首尾衔环的驱动模式。从公权力层面来看,欧盟的数据战略已经极尽各种手段调动多个方面的要素。尽管在市场培育和产业成长来看,欧盟还有较长的路要走,但欧盟对全球数据规则形成的影响将是深刻的。

相比之下,中国也已经意识到数据的重要性,并在许多领域推广大数据的运用,但还没有制定成体系的数据战略。与欧盟相似,中国对数据战略也关心以下几方面:(1)提高数据再利用,促进数据赋能经济的发展;(2)加强数据基础设施建设,特别是拥有自主能力的关键设施的建设;(3)数据安全问题,中国《信息安全法》明文规定了个人数据和重要信息的保护;(4)通过鼓励数据共享,促进本土市场内的数据一体化;(5)反对美国依据本国法律对本国互联网公司所持有的数据拥有司法调取权。

但是,中国与欧盟在数据战略的一些关键问题上也存在截然不同的理念和方式。中国和欧盟最重要的不同在于,中国将数据安全(主要是国家安全)放在第一位,强调数据主权(data sovereignty)概念,认为数据应首先适用被收集地法律和管辖。[①] 由数据主权延伸出"数据本地存储要求",即要求在中国收集的数据应存储在设于中国境内的服务器上,而且个人信息和重要数据非经监管部门批准不得跨境输出。因此,与欧盟选择的在法定条件下有限自由化的中间道路相

① Stephanie Carroll Rainie et al.,"Data as a Strategic Resource: Self-determination, Governance, and the Data Challenge for Indigenous Nations in the United States," *The International Indigenous Policy Journal*, Vol. 8, Issue 2, 2017, pp. 1 ~ 29.

比,中国在数据治理上走的是保守道路,与美国针锋相对。

2020 年 9 月,中国外交部发布的《全球数据安全倡议》[①]重申了中国的立场,其基调仍然是“安全第一”,针对的也是美国对全球数据安全可能造成的威胁。其中提出的八大倡议归结起来重申了三个方面的诉求:(1)维护数据安全,既要防止窃取和滥用个人信息和重要数据,也要维护全球信息技术产品和服务供应链的开放、安全、稳定;(2)维护数据主权,企业要遵守所在国法律,各国应尊重其他国家法律和管辖权;(3)强化企业责任,不得设置后门,不得滥用优势地位侵犯消费者利益。

所以,世界主要国家对数据治理的协调目前存在三种立场:具有信息技术优势的美国,要求数据流动自由化,日本、韩国、加拿大、墨西哥、智利、巴西等国家将追随美国;中国、俄罗斯、印度、印尼等国要求数据本地存储,原则上不得进行跨境传输;处于信息技术弱势的欧盟则坚持在数据高保护的条件下允许有序流动。

“棱镜门”事件后,全世界对数据安全都提高了警惕性。欧盟《通用数据保护条例》的出台很大程度上是为了应对美国利用美国互联网公司调取全球个人数据。中国在《全球数据安全倡议》中提出的很多诉求应当能得到大多数国家包括欧盟的支持。但是,是否促进数据流动和共享才是数据经济的核心问题。对此,目前中美之间尚无协调方案。2019 年 1 月,包括中国在内的 76 个世界贸易组织成员在达沃斯召开的非正式部长级会议上签署了《关于电子商务的联合声明》,共同发起电子商务议题的诸边谈判,其中将涉及数据跨境流动和数字贸易等核心问题。由于分歧巨大,谈判进展缓慢。

值得一提的是,与欧盟在互联网经济上的相对落后不同,中国许多信息技术企业的产品和服务都已经全球化,因而在数据基础设施和获益能力上远远超过欧盟。[②] 近期美国针对字节跳动和微信这两个中国软件发出总统封杀令,提出的

① 中国外交部:《全球数据安全倡议》,https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml。

② AlphaBeta, “The Data Revolution: How China can Capture the Digital Trade Opportunity at Home and Abroad,” https://alphabeta.com/wp-content/uploads/2019/03/digitaltrade_china-en-1-pg-view_hi-res.pdf.

主要理由是中国企业可能滥用其收集和获取的美国公民个人数据。[①] 在云存储设施上,全世界最强的国家现在只有美国和中国。在《全球数据安全倡议》的第一条中,中国即提出信息技术产品和服务供应链的开放、安全和稳定。这一条指出,对信息产品和服务供应链的阻断和干预都是出于各国宣称的“国家安全”目的,中国的企业和贸易也深受其他国家政府“以数据安全”为名的干预之害。

因此,对中国来说,除了安全考虑之外,也要关注两项重大利益:一是不能成为“数据孤岛”,未来全球供应链的发展必然需要数据的共享和流动,中国必须置身其中;二是要帮助企业走出去,对等开放可能是无可回避的命题。欧盟提供的中间道路方案的关键点是以提高数据保护标准来允许数据有条件流动,提出了明确的企业可以跨境传输数据的标准,相较中国模糊的审批制更具透明度和操作性。数据分类和保护框架的认证也基本能解决中国所关心的数据安全问题。简言之,在数据治理问题上,中国应当认真考虑中间道路的可行性,与欧盟形成盟友关系。

① 参见 Donald J. Trump, “Executive Order on Addressing the Threat Posed by TikTok,” https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/。