隐私盾案后欧美数据的跨境流动监管及中国对策

——软数据本地化机制的走向与标准合同条款路径的革新*

李艳华

内容提要:《隐私盾协议》的失效与标准合同条款有条件的效力维持,反映了欧盟数据规则的布鲁塞尔效应与美国监控资本主义马太效应之间的对抗。欧盟在隐私盾案后形成了事实上的"软数据本地化"。然而,其"软数据本地化"机制从来不是也不应当是其追求的目标。标准合同条款作为欧盟最为重要的数据跨境传输机制,其基于"风险方法"的"基本+补充"的路径革新,具有深刻的国内与国际影响。中国最新的跨境数据流动条款秉承以数据安全为底线的跨境数据自由流动原则,遵循"硬数据本地化"的结构设计,参照了欧盟传输工具的基本框架。在具体规则的设计与落实中,中国应合理限制"硬数据本地化"的扩充,借鉴欧盟标准合同条款范本中的风险调控模块化方法,审慎设计标准合同条款,为本国参与全球数据竞争提供规则基础。

关键词:《一般数据保护条例》　跨境数据流动　数据本地化　标准合同条款

2020 年 7 月 16 日,欧洲法院对施雷姆斯 II 案(数据保护专员诉 Facebook 爱尔兰和 Maximillian Schrems 案,C-311/18,以下简称"Schrems II 案")作出裁决,认定欧美数据跨境传输机制《隐私盾协议》无效。标准合同条款(Standard Contractual Clauses,SCCs)作为欧盟数据跨境传输最为广泛的工具,其法律效力虽得到欧洲法院的认可,但在实践上却遇到重大障碍。该案裁决一年后,美国与其他贸易伙伴仍旧面临不确定的法律环境。尽管欧美间就新的替代性跨境数据传输框架的谈判仍在继续,但欧洲数

* 本文系 2021 年度司法部重点课题"习近平法治思想指导下涉外法治体系完善的结构化分析"(批准号:21SFB1006)的阶段性成果。感谢《欧洲研究》匿名评审专家对文章提出的宝贵修改意见,感谢厦门大学法学院博士研究生刘业提出的建议,文章仅代表作者本人观点,文责自负。

据保护委员会与欧盟委员会似乎缺乏推进一个新协定的政治意愿,反而继续贯彻数据本地化和数据保护主义。① 2021 年 6 月,欧美成立贸易和技术委员会,旨在通过关键技术数据出口、数据跨境流动等多方面的共同努力,达到牵制共同竞争对手的目的,但本计划于 9 月底推进的欧美隐私盾替代方案却因美法间的矛盾②变得岌岌可危。与此同时,为填补《隐私盾协议》缺失造成的企业数据传输法律真空,2021 年 6 月 4 日,欧盟委员会公布了《将个人数据从欧盟传输到第三国的新标准合同条款》。③ 欧洲数据保护委员会同样于 2021 年 6 月 18 日更新了《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传输工具补充措施的建议》(版本 2.0,以下简称"补充措施 2.0")。④

跨境数据流动监管本质上是一种国家间的竞争行为,遵循现实主义的博弈逻辑。Schrems II 案在某种程度上标志着欧盟数据保护制度的又一胜利,反映了欧盟在参与全球数据博弈中规则制定权的先发优势,由此扩大了制度上的"布鲁塞尔效应"(Brussels Effect)⑤。进一步而言,欧盟这一做法触及全球数据治理模式的深层问题,对未来多边"数据规制语境下的数字贸易治理"G20 与"贸易规制语境下的数据贸易治理"WTO⑥ 均产生不同程度的影响。因此,本文从 Schrems II 案入手,重点探讨私主体下的跨境数据处理:⑦首先,聚焦该案的两个争议点,剖析欧盟利用数据跨境流动监管制

① Nigel Cory, "How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime," ITIF, 8 July 2021, p.1, https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data.

② 《美英助澳造核潜艇,赤裸裸搞核扩散》,《浙江日报》,2021 年 9 月 15 日,第 3 版。

③ European Commission, Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Adopted on 4 June 2021.

④ EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data Version 2.0, Adopted on 18 June 2021. 在此之前,2020 年 11 月 10 日,欧洲数据保护委员会经公共咨询建议提出《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传输工具补充措施的建议》(版本 1.0)。

⑤ 美国学者布拉德福德(Anu Bradford)用该理论来解释欧盟单边立法的域外效力,参见 Anu Bradford, "The Brussels Effect," *Northwestern University Law Review*, Vol.107, No.1, 2012, pp.1-68。

⑥ 彭岳:《数字贸易治理及其规制路径》,载《比较法研究》,2021 年第 4 期,第 158-173 页。

⑦ Schrems II 案中的跨境数据流动(私主体的跨境处理)与公权力机关对数据调取的行为不同,前者是商业目的下的跨境数据传输,防止政府特别是情报机构访问一家公司已经传输到另一个司法管辖区的数据,后者为各国执法机构获取服务商提供的与刑事调查有关的证据,无论数据位于何处。参见 Theodore Christakis and Fabien Terpan, "EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options," *International Data Privacy Law*, Vol.11, No.2, 2021, p.104。

度与美国进行对抗的逻辑;其次,评估其产生的“软数据本地化”(Soft Data Localization)①效果,并探讨标准合同条款作为补充机制的制度设计;最后,结合中国《数据安全法》和《个人信息保护法》等法律,尝试从更为细化的规则设计视角为中国数据本地化制度的完善与标准合同条款的制定提出相关建议。

一 Schrems II 案:欧美数据跨境流动监管路径的再博弈

欧美间跨大西洋经济关系是世界上最为重要的经济关系,其产生的经济效益高达7.1 万亿美元。② 然而,数字和服务的全球化贸易既没有产生互联网法律的普遍统一,也没有推动数据保护和数据隐私法的趋同,欧美间的数据分歧便是例证。③ 在过去数十年间,欧盟一以贯之的“权利主导路径”与美国推崇的“市场主导路径”均在各自的双边与多边合作中不断推进,④而二者达成的《安全港协议》与《隐私盾协议》也先后经欧洲法院依据欧盟数据保护法,尤其是欧盟《一般数据保护条例》(以下简称 GDPR)与《欧盟基本权利宪章》,作出无效裁决。因此,GDPR 被认为是影响欧美数据跨境流动的关键障碍。而 Schrems II 案具有里程碑式的意义,它的判决结果将极大影响世界尤其是美国的数据保护走向。

(一)规范之争:隐私盾的废除与标准合同条款的效力维持

欧美在跨境数据流动规则上存在明显的分歧,历经多轮博弈,从 2000 年签订《安全港协议》双方展开较量,⑤到 2013 年斯诺登事件爆发后《隐私盾协议》的签署,美国通过设立数据保护原则,建立隐私盾监察员制度与其他救济措施,对欧盟隐私保护制

① 软数据本地化(Soft Data Localization)最初由钱德尔(Anupam Chander)教授提出,他认为欧盟虽并未直接要求数据本地化,但鉴于相关替代方案具有法律风险,如果数据没有本地处理,外国公司将很难在欧盟运营,所以 Schrems II 案裁决促成了“软数据本地化”的效果。参见 Anupam Chander, “Is Data Localization a Solution for Schrems II?” *Journal of International Economic Law*, Vol.23, Issue 3, 2020, p.2; UNCTAD, “Digital Economy Report 2021—Cross-border Data Flows and Development: For Whom the Data Flow,” 29 September 2021, p.107, http://www.environmentportal.in/content/471679/digital-economy-report-2021-cross-border-data-flows-and-development-for-whom-the-data-flow/。

② U.S. Department of Commerce of Commerce, “U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows,” Press Release, 16 July 2020, p.2, https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commercewilbur-ross-statement-schrems-ii-ruling-and.

③ W. Gregory Voss, “Obstacles to Transatlantic Harmonization of Data Privacy Law in Context,” *Journal of Law, Technology & Policy*, Vol.2019, Issue 2, 2019, p.458.

④ 如由欧盟主导的 OECD、108 号公约、欧日经济伙伴关系协定中的数据跨境流动条款等;由美国主导的 TPP(现为 CPTPP)、USMCA 与 APEC 下的 CBPR 中的数据跨境流动条款等。

⑤ Case C-362/14-Schrems, Maximillian Schrems v Data Protection Commissioner, Judgment of 06.10.2015.

度做出重大让步。[①]然而,上述补救措施并未弥合二者的根本性分歧。经施雷姆斯申诉,爱尔兰高等法院请求欧洲法院对《隐私盾协议》与标准合同条款的效力作出判决。2020 年 7 月,欧洲法院在经过调查后,最终判定《隐私盾协议》无效,也使得标准合同条款传输机制遭到严重质疑。正如美国著名隐私权活动家丹尼尔·索罗夫(Daniel Solove)所言:"《隐私盾协议》已死,而标准合同条款仍在苟延残喘。"[②]

在很多学者看来,欧美间数据保护框架的重大差异,使得欧盟依据 GDPR 第 45 条对美国数据保护水平的"总体充分性认定"从来都不是一个真正的选择。[③] 欧洲法院对《隐私盾协议》的无效判决使该问题再次凸显。一方面,欧洲法院在审查《隐私盾协议》时,对美国公权力下的政府监控项目进行了评估,并认为美国法律缺乏比例原则以确保政府仅在满足合法利益或"保护他人权利和自由"的"必要"情况下收集和使用数据;另一方面,美国未对欧盟数据主体提供"有效的行政和司法救济",《第 28 号总统政策指令》和《第 12333 号行政指令》均未授予欧盟公民在法庭上对美国当局提起诉讼的权利。[④] 而且,隐私盾监督员的独立性问题同样受到质疑,因为它并非《欧盟基本权利宪章》第 47 条意义上的法庭。

针对标准合同条款这一欧美数据跨境传输最广泛使用的法律工具,欧洲法院进一步裁定欧盟委员会关于标准合同条款的决定原则上有效,但均需逐案进行额外评估,以确保数据主体获得"基本上等同于"GDPR 根据《欧盟基本权利宪章》在欧盟范围内保证的保护水平。[⑤] 如果发现进口国法律存在瑕疵,则公司必须提供额外的安全措施。标准合同条款是私人间的契约机制,对其他政府并没有拘束力。因此,在第三国法律或实践与 GDPR 不一致的情况下,标准合同条款无法解决这一问题。事实上,欧洲法院指出,只要第三国处理个人数据超出了必要的范围,导致无法达到 GDPR 所要求的保护水平,数据控制者就必须暂停或终止向任何第三国进行数据传输。[⑥]

此次判决反映了斯诺登事件以来欧盟对美国极大的不信任。Schrems II 案判决后,尽管欧美开展了更加务实的对话,但一年来并未取得任何实质性的成果。一方面,

---

① 黄志雄、韦欣好:《美欧跨境数据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,第 35 页。

② Daniel Solove, "Schrems II: Reflections on the Decision and Next Steps," Teach Privacy, 23 July 2020, https://teachprivacy.com/schrems-ii-reflections-on-the-decision-and-next-steps/.

③ Barbara Sandfuchs, "The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18-Schrems II," *GRUR International*, Vol.70, No.3, 2021, p.246.

④ C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, para.192.

⑤ Ibid., para.105.

⑥ Ibid., paras.141-142.

欧盟各国在实践中缩减向美国数据跨境传输的范围,如 2020 年 10 月法国卫生部对其法律进行了紧急修改,禁止在欧盟以外共享法国卫生数据。① 德国则要求尽量避免任何涉及向美国传输个人数据的活动。② 另一方面,欧洲数据保护委员会采用了对充分性"实质等同保护"的限制性解读,要求 GDPR 第 46 条保障措施中的第三国保证同等程度的保护,必要时需要使用"补充措施"。欧盟委员会也颁布了将《个人数据从欧盟传输到第三国的新标准合同条款》。从上述变化可以看出,《隐私盾协议》失效后欧盟数据监管实践趋向严格,这使得欧美数据跨境流动面临新的挑战,欧美间的矛盾难以调和。

(二)矛盾根源:数据规则布鲁塞尔效应与监控资本主义马太效应的对抗

表面上,Schrems II 案是欧盟"权利话语"与美国"市场话语"间的价值分歧与制度差异的结果,③但回顾美欧跨境数据流动机制博弈的历史不难发现,《隐私盾协议》的破产与标准合同条款的升级是美国监控资本主义的马太效应与欧盟规则布鲁塞尔效应对抗的产物,④未来将影响跨大西洋数据流动的走向。

尽管欧盟在全球 70 个最大的科技平台中市值占比不到 4%,但这个拥有超过 5 亿用户的地区贡献了谷歌和脸书四分之一的收入。⑤ 为了保护个人隐私与遏制大型企业的卡特尔化,欧盟试图通过增加制度成本产生"布鲁塞尔效应"来撬动其自身数据经济的发展。布拉德福德(Anu Bradford)将"布鲁塞尔效应"描述为欧盟在一系列监管领域建立的全球规则:反垄断、隐私和健康保护(包括化学品监管)、环境保护和食品安全。⑥ 在数据保护领域,欧盟的法律不仅对美国的公司进行严格监管,⑦还影响到美国之外全球其他地区的隐私法。此外,欧洲法院通过严格适用《欧盟基本权利宪

① Laura Bradford, Mateo Aboy and Kathleen Liddell, "Standard Contractual Clauses for Cross-Border Transfers of Health Data after Schrems II," *Journal of Law and the Biosciences*, Vol.8, Issue 1, 2021, p.16.

② "Berlin: Berlin Commissioner Issues Statement on Schrems II Case, Asks Controllers to Stop Data Transfers to the US," DataGuidance, 17 July 2020, https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schremsii-case-asks-controllers-stop-data.

③ 参见彭岳:《贸易规制视域下数据隐私保护的冲突与解决》,载《比较法研究》,2018 年第 4 期,第 179-181 页。不过单教授等具体将其分解为数据保护理念的差异、数据法律体系和模式的差异、数据法律实施体系的差异,参见单文华、邓娜:《欧美跨境数据流动规制:冲突、协调与借鉴——基于欧洲法院"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,第 96-98 页。

④ 参见单文华、邓娜:《欧美跨境数据流动规制:冲突、协调与借鉴——基于欧洲法院"隐私盾"无效案的考察》,第 98 页。

⑤ 欧盟地区主要是以美国(73%的份额)和中国(18%的份额)的高科技巨头为主。参见 G. Venkat Raman, "State Vs Big Tech: The Brussels Effect," FOUNDINGFUEL, 13 September 2021, https://www.foundingfuel.com/article/state-vs-big-tech-the-brussels-effect/。

⑥ Anu Bradford, "The Brussels Effect," pp.1-35.

⑦ 仅在 2019 年,谷歌就因在欧盟市场的各种违规行为被罚款 5700 万美元。2017 年早些时候,脸书被处以价值 1.1 亿欧元的罚款,原因是向欧盟提供了关于其将 WhatsApp 与其旗舰社交网络整合的错误信息。

章》对欧委会的《隐私盾协议》与《标准合同条款决定》进行司法审查,①承担了权利保护的终极裁判者的角色,事实上维持了布鲁塞尔效应的高标准。此外,欧盟秉承欧洲数字单一市场战略,通过发布《塑造欧洲数字未来》《欧洲数据战略》和《人工智能白皮书》战略文件,利用 GDPR 这一法律手段,将与市场相关的社会政策、经济政策和监管政策外部化,向国际层面输出标准,形成相较于竞争对手的制度优势。②

相反,美国科技公司的运营与发展源于对“监控资本主义”(Surveillance Capitalism)③的掌控,即通过互联网收集用户信息,分析用户偏好,再出售给精准投放的广告商,从而构成资本的原始积累。在这种模式下,美国科技公司不断发展强大进而形成垄断,并将触角延伸到全球,由此产生“马太效应”(Matthew Effect)④。监控资本主义易造成大量用户数据聚集,影响用户的数据保护水平和一国的经济安全与数据安全。此外,美国监控资本主义还通过对技术的控制,谋求政治、经济、文化等方面的利益,加剧全球范围内的数据鸿沟,引发全球数据安全危机。在美国,经济领域的数据可由政府无限制地监控与利用,因而影响到第三国的主权与国家安全。事实上,即使是美国人也很难质疑政府的监督。⑤ “9·11”事件发生后,美国织就了一张巨大的网络情报监视网。⑥ 其监视法对民事合同的权利保障也不够重视,⑦例如,关于《美国宪法第四修正案》第三方原则,⑧美国联邦最高法院认为,即使第三方在合同中承诺了他们的隐私,人们对第三方持有的个人数据也缺乏合理的隐私预期,因此,数据主体没有能力挑战政府的数据访问权。

鉴于此,欧盟在技术主权与个人权利保护的双重考量下,通过发挥欧洲数据隐私

---

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》,载《欧洲研究》,2021 年第 4 期,第 105-106 页。

② Sangeeta Khorana and W. Gregory Voss, “The Digital Single Market: Move from Traditional to Digital?” in Sangeeta Khorana and María García, eds., *Handbook on the EU and International Trade*, Elgar Edward Elgar Publishing, 2018, pp.384-389.

③ “监控资本主义”由哈佛大学教授肖莎娜·祖博夫(Shoshana Zuboff)提出,用以指称由 Google 以关键词方式崛起的一种寄生性的经济逻辑。参见[美]肖莎娜·祖博夫:《监控资本主义时代》,温泽元译,时报文化企业出版社 2020 年版。

④ “马太效应”由科学史研究者罗伯特·莫顿(Robert K. Merton)提出,后适用于经济、社会、垄断等领域,指一种强者越强、弱者越弱两极分化的现象。在本文中指美国科技公司监控资本主义的盛行导致其越来越强大,由此垄断全球数据市场,加剧全球范围内的数据鸿沟。

⑤ 在 Clapper v. Amnesty International 一案(568 U.S. 398,2013)中,美国最高法院认为,原告声称他们可能受到监视,并不得不采取昂贵的措施避免这种监视,但他们缺乏法律依据,因为只能猜测自己是否受到监视。

⑥ 如美国通过的《爱国者法案》《精确法案》与《外国情报监控法案》等。

⑦ Daniel Solove, “Schrems II: Reflections on the Decision and Next Steps”.

⑧ 第三方原则是美国的一项法律原则。该原则认为,自愿向银行、电话公司、互联网服务提供商和电子邮件服务器等第三方提供信息的人“没有合理的隐私预期”。由于缺乏隐私保护,美国政府可以在没有法律许可证的情况下从第三方获取信息,也不必遵守《美国宪法第四修正案》中禁止无正当理由搜查和扣押的规定。

规则的布鲁塞尔效应,形成制度竞争,以此遏制美国监控资本主义的过分发展与国家监控制度的过度扩张。欧洲数据保护委员会在《针对监控措施的关于欧盟重要保障的建议》中明确了四项重要保障,①以确保相关方对公民数据隐私权和个人数据的保护符合欧洲联盟法院及欧洲人权法院判例所要求的标准。

总而言之,Schrems II 案《隐私盾协议》判决无效引发的法律效果具有较强的指向性与针对性。而对于标准合同效力的确认,尽管在具体认定上需遵循个案原则,但仍可能从美欧之间发酵到全球,直接影响欧盟与全球的数据跨境流动。就充分性认定而言,由于美欧存在根本分歧,未来的谈判将重点围绕美国的权利救济体系与监控制度展开。即便美国可以设计独立的隐私盾监督机制,②未来在数据保护水平层面达到前所未有的高度,③但拥有强大的消费者隐私保护法律并不意味着美国的法律就达到了欧盟的充分性保护标准。④ 因为充分性认定也需考虑美国联邦监督法。基于"国家安全"的考量,美国的情报监控制度似乎没有改变的余地,由此导致欧美新的跨境数据流动谈判困难重重。相反,美国还借鉴欧盟"经验",于 2021 年 4 月提出《保护美国人的数据免受外国监视法案》。⑤ 对于标准合同条款而言,鉴于标准合同的保障性、补充性与私法性特征,标准合同与 GDPR 所要求的充分性必然存在一定的距离,而且隐私盾案对美国监控制度的否决同样会影响到标准合同条款的效力。但欧洲法院选择了要求采取保障措施补强标准合同条款的路径,而非使其归于无效。既避免欧美《隐私盾协议》失效后出现规则真空,又防止在标准合同条款失效后产生蝴蝶效应辐射全球。

---

① 数据处理应当基于清晰、准确和公开的规则;所采取的措施必须是为了达到合理目的,并需要说明该措施的必要性和适当性;应当具备独立的监督机制;数据主体应获得有效救济。

② 例如由普罗普(Kenneth Propp)等人提出的由已有的隐私与公民自由官员进行实况调查,由一名独立的联邦法官对事实调查进行评估,欧盟公民可以向外国情报监督审查法院提出上诉,最终向美国最高法院提出上诉。参见 Kenneth Propp and Peter Swire, "After Schrems II: A Proposal to Meet the Individual Redress Challenge," LAWFARE, 13 August 2020, p.5, https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge。

③ 在州层面,2021 年,弗吉尼亚州和科罗拉多州跟随加利福尼亚州,颁布"全面"隐私立法,扩大消费者的权利和增加企业的义务。在联邦层面,2021 年 8 月美国统一法律委员会(ULC)投票通过了《统一个人数据保护法》,这是一项旨在统一州隐私立法的示范法案。经过最终修订后,该法案预计在 2022 年 1 月被州立法机构引入。此外,2021 年国会还提出 30 项隐私法案,涉及消费者权利保护、紧急健康数据的使用、执法部门技术使用与网络/国土安全等。参见 Müge Fazlioglu, "Privacy Bills in the 117th Congress," IAPP, 24 August 2021, https://iapp.org/news/a/privacy-bills-in-the-117th-congress/。

④ 例如,加利福尼亚州希望得到类似于加拿大的部分充分性决定,《加州消费者隐私法案》(CCPA)采用了与《一般数据保护条例》(GDPR)类似的"个人信息"定义,为消费者提供了与 GDPR 类似的个人知情权等。参见 Andrei Gribakov, "Road to Adequacy: Can California Apply Under the GDPR?" LAWFARE, 22 April 2019, https://www.lawfareblog.com/road-adequacy-can-california-apply-under-gdpr。

⑤ Ron Wyden, "Wyden Releases Draft Legislation to Protect Americans' Personal Data from Hostile Foreign Governments," Gorge Country Media, 15 April 2021, https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments.

二 数据本地化:后 Schrems II 时代跨境数据流动监管的可行出路?

20 世纪 90 年代以来,美欧间的信息流动稳步增长。美国凭借强大的信息技术优势,吸引大量的欧盟公民个人数据正向流入,而欧盟则以早期的《第 108 号公约附加议定书》、后来的《欧共体数据保护指令》与最近的 GDPR,[①]并结合《欧盟基本权利宪章》,逐步升级对个人数据权利的有效保护。欧洲法院最近对《隐私盾协议》的无效判决使得欧美跨境数据流动恢复到原有状态,产生了数据本地化的间接效果。然而,"数据本地化"的机制设计从来不是也不应当是欧盟最终追求的目标。

(一)Schrems II 案形成事实上的"软数据本地化"

数据本地化重申主权国家对于境内数据的控制权,标志着威斯特伐利亚主权传统在网络空间的回归。[②] 迄今为止,全球 62 个国家实施了 144 项数据本地化的限制措施。[③] 从规制内容来看,相关规则包括限制政府数据、地图和地理空间数据、健康和基因数据、传统电信和通信相关数据、金融数据、个人数据等特定类型的数据出境。[④] 从规制结构上看,相关规则主要体现为相应的数据跨境规制条款原则上禁止数据出境,在本地储存和处理数据,只有经数据主体同意或规制机构许可才能构成例外。[⑤] 从政策产生的效果看,主要有硬数据本地化与软数据本地化。"硬数据本地化"体现为直接的物理性的数据存储要求,典型代表是全面数据本地化的俄罗斯与特定类型数据本地化的中国与印度(两种数据本地化在欧美相关研究中被视为同一类型的数据本地化模式),[⑥]而"软数据本地化"机制是指相关规则条款中没有明确的数据本地化表述,但要求个人信息跨境传输满足相关严苛条件,并造成事实上的数据本地化,典型代表如欧盟。Schrems II 案背景下《隐私盾协议》的废除,使得事实上的数据本地化的效果更为显著。

---

① 张舵:《略论个人数据跨境流动的法律标准》,载《中国政法大学学报》,2018 年第 3 期,第 98-100 页。

② 刘晗、叶开儒:《网络主权的分层法律形态》,载《华东政法大学学报》,2020 年第 4 期,第 67-82 页。

③ Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," *ITIF*, 19 July 2021, p.3, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

④ Ibid., pp.3-4 .

⑤ 彭岳:《数据本地化措施的贸易规制问题研究》,载《环球法律评论》,2018 年第 2 期,第 179 页。

⑥ 在国内法律政策中明确规定数据本地化的国家,以俄罗斯、中国、马来西亚、印度、伊朗、土耳其、越南、印度尼西亚、尼日利亚等国为典型代表。转引自刘金河、崔保国:《数据本地化和数据防御主义的合理性与趋势》,载《国际展望》,2020 年第 6 期。ITIF 最新的报告书则认为中国是对数据限制最为严格的国家,其次是印度尼西亚、俄罗斯和南非。参见 Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," p.3。

欧盟虽然在内部治理(GDPR)[①]与对外谈判中(WTO 电子商务诸边谈判、G20 大阪数字经济宣言、欧日经济协定、欧盟与新西兰及澳大利亚的贸易谈判)均禁止数据本地化措施。然而,欧盟法律框架下数据跨境的多层传输机制,实际上变相产生了数据本地化的效果。第一层的充分性保护认证机制过于烦琐与严苛,目前仅有 13 个国家[②]得到充分性保护认证,欧盟委员会正在考虑的国家是韩国,[③]英国继脱欧后于 2021 年 6 月获得欧盟的充分性认定。不过,《隐私盾协议》的寿终正寝使得这一机制更难以运行。第二层的标准合同条款也因 Schrems II 案增加了额外措施的限制。而约束性公司规则因仅限于调整跨国公司的内部数据传输行为,并且企业合规成本较高,因此适用较少。另外,虽然 GDPR 引入了认证机制和行为准则作为其他保障性措施,但相关机制尚未正式建立。而第三层的保护源于 GDPR 第 49 条规定的特殊情形下义务的克减,尽管欧洲法院认为该条款可避免规则真空,然而,关于同意[④]与必要性的解释非常有限,后者只能适用于"偶尔的、非经常性的、数量较少的"数据传输行为,且其他出境制度均不适用的情况,因此有着严格的情境限制。

由上可见,《隐私盾协议》失效后,在事关欧盟的数据传输问题上,数据控制者与处理者可用的传输路径极其有限,尽管欧洲法院并未也从未要求个人数据在本地存储,但一些公司为了防止巨额罚款,减少商业风险,其数据传输策略事实上形成了"软数据本地化"。此外,从欧洲数据保护先锋德国的态度来看,其数据保护当局曾呼吁在法律框架改革以前,数据不应传输到美国。[⑤] 由施雷姆斯担任荣誉主席的数据保护团体甚至要求避开美国供应商,禁止使用美国的云服务器,[⑥]而这种措施极有可能违反贸易中的非歧视性原则。

(二)"数据本地化"并非欧盟数据跨境传输最为可行的监管机制

① 参见 GDPR 前言第 101 行:"欧盟与欧盟以外国家和国际组织之间的个人数据流动对于扩大国际贸易和国际合作是必要的"。

② 安道尔、阿根廷、加拿大(限于商业组织)、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、乌拉圭与英国。

③ European Commission, "Adequacy Decisions," 30 March 2021, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-dataprotection/adequacy-decisions_en. 2021 年 3 月,欧韩完成关于数据保护同等水平的谈判并得出"充分性"结论,6 月欧盟委员会正式启动关于向韩国传输数据的充分性认定程序。

④ 首先,同意必须是强有力的,鉴于有效同意的门槛很高,且该同意必须能够撤销,这可能意味着同意不是可行的解决方案;其次,每个数据主体所需要的充分同意可能既昂贵又耗时;最后,欧洲当局对同意和相关减损的早期解释往往具有相当大的限制性。

⑤ "Berlin: Berlin Commissioner Issues Statement on Schrems II Case, Asks Controllers to Stop Data Transfers to the US," DataGuidance, 17 July 2020, https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schremsii-case-asks-controllers-stop-data.

⑥ "Next Steps for EU Companies & FAQs," NOYB, 20 July 2020, https://noyb.eu/en/next-steps-eu-companies-faqs.

在欧盟强有力的监管下,市场经济主体会基于趋利避害的考虑选择“软数据本地化”机制,但它会给欧盟带来较高的制度成本,亦无法解决欧美跨境数据流动过程中的关键性障碍——国家监控制度。

首先,欧盟“软数据本地化”政策会产生较高的制度成本。自 Schrems II 案发生后,根据跨境数据论坛 2021 年 4 月的一份报告,①相当多的社会反响都聚焦于《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传输工具补充措施的建议》(版本 1.0)(以下简称“补充措施 1.0”)导致数据本地化的担忧。其一,数据本地化成本高昂,建立额外的存储设备会对贸易和投资产生负面影响,最终其负担将不成比例地落在规模较小的公司身上。美国科技创新智库信息技术与创新基金会(ITIF)研究发现,一个国家的数据限制指数(DRI)在 5 年间每增加 1%,其贸易量将减少 7%,生产率将降低 2.9%,下游产品价格将上涨 1.5%。② 其二,数据本地化破坏了欧盟的贸易增长目标,并与欧盟自身倡导的全球数据流动主张相矛盾。其三,数据本地化还会招致报复,其他国家可能会做出同样的反应。其四,数据本地化会影响网络安全,额外设备的增加易成为更多黑客攻击的对象,分散公司的网络安全能力。其五,数据本地化虽有利于一些本地企业,但会牺牲其他本地企业的利益。③ 例如,截至 2020 年 10 月,美国共有 5211 家公司得到隐私盾的认证,数据本地化将损害这些与美国合作的从事数据跨境传输企业的利益。此外,从欧洲与世界的经济来看,数据自由流动政策和数据本地化政策的经济红利差距非常显著,每年超过欧盟国内生产总值的 1.5%。④ 因此,“软数据本地化”机制只能成为欧盟的暂时选项,而非长久之策。实际上针对非个人数据,欧盟《非个人数据在欧盟境内自由流动框架条例》提出了限制成员国数据本地化的要求。

其次,除了制度成本,欧盟“软数据本地化”政策对遏制美国监控他国行为的效果存疑。事实上,美国国家安全局和联邦调查局的对外监视并未因为欧盟的交涉而有所减少,美国国会与法院也未能针对这一问题提供充分与适当的救济手段,美国立法机

① DeBrae Kennedy-Mayo and Peter Swire, “Prominent Theme of Data Localization in Comments to EDPB Guidance on Implementing Schrems II Has New Urgency with the Portuguese Decision,” *CROSSBORDER DATAFORUM*, 29 April 2021, https://www.crossborderdataforum.org/prominent-theme-of-data-localization- incomments-to-edpb-guidance-on-implementing-schrems-ii-has-new-urgency-with-the-portuguese-decision/.

② Nigel Cory and Luke Dascoli, “How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,” p.3.

③ Anupam Chander, “Is Data Localization a Solution for Schrems II?” pp.12-14.

④ Frontier Economics, “The Value of Cross-Border Data Flows to Europe: Risks and Opportunities, Report Prepared for Digital Europe,” DIGITALEUROPE, June 2021, p.6, https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf.

构也无意在监控法上做出任何变更。相反,美国政府还认为,相较于《外国情报监控法》中政府可强制要求公司披露数据,《第 12333 号行政指令》中政府基于国家安全目的直接访问个人数据的行为不应成为欧盟的审查对象。①

总之,在 Schrems II 案发生后,欧盟虽并未直接要求数据本地化,但鉴于相关替代方案具有法律风险,因此事实上对公司施加了本地化的压力。这一"软数据本地化"机制非但不能解决欧美间不可调和的监控矛盾,还会增加企业成本、破坏贸易增长目标、招致报复、破坏网络安全与损害相关企业利益等。然而,GDPR 数据跨境传输条款的日益严苛,以及最近发布的《欧洲数据治理法案》和 GAIA-X 云专案②似乎表明,欧盟在数据本地化问题上的立场不会轻易后退。正如欧盟委员会所言,针对跨境数据传输与禁止数据本地化要求,欧盟将基于欧洲价值观与利益,采取开放且自信的路径……在保留数据保护与隐私领域监管自主权的同时,解决数据流动中的不合理障碍。③ 当然,也需要看到,为从跨境数据传输中获益,尽可能消减数据本地化的不利影响,欧盟对标准合同条款路径进行了革新。

三 标准合同条款:后 Schrems II 时代跨境数据流动监管路径的革新

1995 年的《欧共体数据保护指令》与 2001 年的《第 108 号公约附加议定书》④规定了诸如标准合同条款的保障措施,作为对充分性保护的补充适用。而 GDPR 第 46 条⑤保留了这种"适当保障"的结构,根据国内法向"有问题"的司法管辖区传输数据提供了单独的路径。Schrems II 案发生后,一方面,鉴于旧版标准合同条款无法与 GDPR 的部分内容相衔接,亟待更新;另一方面,欧盟委员会需要调和商界与民间隐私保护组织的利益诉求,并根据欧洲法院的裁决,寻求在数据风险最小的情况下继续实现

① U.S. Department of Commerce, "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," September 2020, https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF; U.S., "Comments on Proposed SCC Decisions," 10 December 2020, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000YFcs.

② 德法发布 GAIA-X 云专案,拟建立云基础设施,从而降低对其他国家大型云服务商的依赖。参见 EU, "GAIA-X. A Federated Data Infrastructure for Europe," http://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html。

③ UNCTAD, "Digital Economy Report 2021—Cross-border Data Flows and Development: For Whom the Data Flow," 29 September 2021, p.107, http://www.environmentportal.in/content/471679/digital-economy-report-2021-cross-border-data-flows-and-development-for-whom-the-data-flow/.

④ Additional Protocol Article 2.

⑤ GDPR 第 46 条:在缺乏根据第 45 条第 3 款所作决定的情况下,仅当在控制者或处理者提供了适当的安全措施,以及在可强制执行的数据主体权利和对数据主体的有效法律补救措施就绪的条件下,一个控制者或处理者可以将个人数据传输到第三国或国际组织。

国际数据的跨境传输,新的标准合同条款由此应运而生。

(一)标准合同条款仍为最重要的数据跨境传输机制

标准合同条款是欧盟委员会预先批准的法律机制,包括从数据控制者到数据控制者的两套合同,以及从数据控制者到数据处理者的一套合同。数据提供方与数据接收方需要将条款嵌入合同中,并且对合同的数据与隐私保护负责。作为充分性保护的替代性机制,标准合同条款显示了一定的公法特征,私人签订的标准合同条款仍需以欧盟委员会的版本为蓝本,并且受到欧洲数据保护机构的监督。不过,标准合同条款的最大缺陷在于并不限制政府强制访问个人数据。因此,在 Schrems II 案中,欧洲法院要求依赖标准合同条款的公司有责任自行确定接收国关于政府获取数据的法律是否提供了符合欧盟法律标准的隐私保护,否则需要额外采取"补充措施"。对于 Schrems II 案的结果,克里斯托弗·库勒(Christopher Kuner)教授认为,欧洲法院并未对何为"补充措施"做出说明,他还进一步指出,所有标准合同条款已然成为"小型的充分性决定"。① 这些决定使得法院和监管机构的监管成本更高,中小企业会遭受不成比例的负担,因而易造成事实上的数据本地化。尽管该案的判决结果增加了企业适用标准合同条款的不确定性,但标准合同条款仍是欧盟最为重要的数据跨境传输机制。

首先,在实践层面,标准合同条款仍是欧盟公司使用最为频繁的数据跨境传输工具。在全球数据治理过程中,企业合规能力对于当今数字经济能否最大限度地发挥数据与数字技术的优势至关重要。随着各国纷纷制定新的数据保护法规,标准合同条款的制定将为跨国数据传输提供一个各国都能接受的制度安排。通过对欧洲近 300 家公司调查发现,Schrems II 案发生后,近 85%的公司使用标准合同条款,只有 9%的公司没有将数据传输至欧盟境外。② 几乎所有公司都使用标准合同条款向美国传输数据,近 60%的公司使用标准合同条款向亚洲或英国传输个人数据。③ 涉及数据传输的行业包括信息技术、媒体、通信、制造业、科学技术、金融保险和零售等。近三分之二以上的中小企业都在使用标准合同条款。90%的公司将标准合同条款用于企业对企业

① Christopher Kuner, "The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation," EUROPEAN LAW BLOG, 17 July 2020, https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

② BusinessEurope, DIGITALEUROPE, ERT and ACEA, "Schrems II: Impact Survey Report," 26 November 2020, p.5, https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2020-11-26_schrems_ii_impact_survey_report.pdf.

③ Ibid. 许多受访者还选择其他国家,如澳大利亚、俄罗斯等。瑞士、加拿大与日本是欧盟委员会认可的提供充分保护的第三国,因为向这些国家传输数据不需要 SCCs,因而不会出现在此列表中。具体来说,欧盟通过标准合同条款(SCCs)进行数据跨境传输的企业中,欧美为 94%,欧英为 56%,欧亚为 59%,欧盟与南美为 10%,欧盟与中东和非洲为 18%。

的销售和服务,而不仅仅是为互联网消费者服务的工具。①

其次,在制度设计层面,新标准合同条款弥补了欧美充分性保护认定的缺位,降低了数据跨境传输的不确定性,得到了欧盟委员会的支持与美国的被动回应。尽管欧美间的第一层传输机制"充分性保护"被判无效,但问责制标准合同条款通过法律、技术和组织手段弥补了部分法律的漏洞。欧盟委员会副主席薇拉·乔洛娃(Vera Jourova)强调:"在欧洲,我们希望保持开放性并允许数据的流动,但数据的流动与保护须并驾齐驱。标准合同条款将有助于我们实现这一目标,这些条款可以保证企业的数据活动在欧盟乃至国际范围内的传输符合法律规定。"因此,标准合同条款仍为其他国家与欧盟进行数据跨境传输唯一可广泛访问的法律工具。② 针对欧洲法院的指控,美国总结了政府基于国家安全目的访问个人数据的现行法律与实践,并出具初步意见《白皮书:Schrems II 案后欧美数据跨境传输机制中美国隐私监管的信息说明》(以下简称《白皮书》),为个人数据从欧盟传输到美国提供参照。③ 可见,美国以被动合规的角色继续履行标准合同条款。

(二)标准合同条款基于风险方法的"基本+补充"的路径革新

相较于针对国家整体适用的充分性认定工具,标准合同条款成为适用商事主体的个别适用工具,为达成与前者相一致的效果,标准合同条款主要以合同义务"补强"域外数据保护水平之不足,以合同条款"固定"欧盟个人数据保护标准。④ 而新的标准合同版本与补充措施"基本+补充"的二重路径将强化这一"补强"功能,以灵活应对个人数据跨境后的损害风险。

1. 基于风险方法下的标准合同条款 2.0

2021 年 6 月 4 日,欧盟委员会通过《将个人数据从欧盟传输至第三国的新标准合同条款》(以下简称"标准合同条款 2.0"),⑤有跨境数据传输需求的企业可在 18 个月的过渡期内,采用新版标准合同条款。新的标准合同条款保留了欧盟委员会 2020 年

① Nigel Cory, Daniel Castro and Ellysse Dick, "The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade," *ITIF*, 17 December 2020, p.6, https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade.

② "An Early Analysis of Schrems II—Key Questions and Possible Ways Forward," DIGITALEUROPE, 31 August 2020, https://www.digitaleurope.org/wp/wpcontent/uploads/2020/08/DIGITALEUROPE_An-early-analysis-of-Schrems-II_Key-questions-andpossible-ways-forward.pdf.

③ U.S. Department of Commerce, "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," p.2.

④ 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》,第 97-98 页。

⑤ 现行标准合同条款将于 2021 年 9 月 27 日废止,但废止日期前依据现行标准合同条款所签订的跨境数据传输协议仍将被视为符合欧盟 GDPR 的规定,直至 2022 年 12 月 27 日。

11 月 12 日发布的《将个人数据从欧盟传输至第三国的标准合同条款的实施决定(草案)》①中使用的“一般条款+模块化”②的创新结构设计,用于控制者到控制者的传输、控制者到处理者的传输、处理者到处理者的传输以及处理者到控制者的传输,实现了通过一套标准合同条款解决广泛的数据传输问题。实际上,旧标准合同条款仅包括数据控制者向数据控制者,以及数据控制者向数据处理者跨境传输的两种情形,Schrems II 案也揭示了旧标准合同条款存在安全性缺陷。因此,标准合同条款 2.0 的发布不仅可以暂时填补欧美跨境数据流动的规则真空,还可满足企业的现实需求。相比旧版标准合同条款,标准合同条款 2.0 在两个方面有所改良。

首先,标准合同条款 2.0 衔接 GDPR 内容,新增若干数据处理要求。其一,增加了更多的数据跨境传输场景,如数据处理者之间的传输与处理者至控制者的传输。此外,为协调解决 GDPR 第 3(2)条的域外范围,③标准合同条款 2.0 明确承认数据提供方本身可为一个非欧盟实体,④数据接收方需要设立在第三国且在 GDPR 地域适用范围之外;其二,新增多方条款与对接条款,多个数据提供方可签订合同,并允许随着时间的推移增加新的缔约方;⑤其三,增加一系列数据接收方的义务,⑥譬如对隐私声明的要求义务、数据泄露通知义务、数据处理活动记录/合规记录义务、不准确数据的通知义务、保障数据主体权利的义务等。

其次,标准合同条款 2.0 不仅旨在更新当前版本,还旨在遵守欧洲法院的裁决,并将这些额外的保障措施内置于合同中。如标准合同条款 2.0 第 3 节将 Schrems II 案欧洲法院的建议“影响遵守条款的当地法律和做法”⑦与“数据接收方在公共当局访问情况下的义务”⑧嵌入条款设计中。标准合同条款 2.0 第 14 条规定,合同各方必须针对

① “Data Protection-Standard Contractual Clauses for Transferring Personal Data to Non-EU Countries (Implementing Act),” https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

② 除一般条款外,控制者与处理者应选择适用于其情况的模式,以规范他们在数据处理中的角色和责任,调整他们标准合同条款下的义务。

③ 目的地原则的适用,根据 GDPR,向欧盟数据主体提供商品或服务或监控他们的行为,均为 GDPR 的调整范围。

④ 例如,如果一个非欧盟的数据提供方想把数据传输到另一个非欧盟方(如美国的云处理器),从技术上讲,SCCs 不能作为它在这种特定情况下合法传输数据的手段,新的 SCCs 则解决了这种需求。

⑤ 依赖 SCCs 进行集团内部传输的组织,可能会随着时间的推移而设立或收购新的公司,因此需要在 SCCs 中加入这些公司。参见 Phillip Lee, “The Updated Standard Contractual Clauses—A New Hope?” IAPP, 7 June 2021, https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope/。

⑥ 具体义务一般因传输类型而异,模块一规定了数据接收方的义务,具体包括目的限制、透明度要求、准确性、数据最小化和保留原则、安全性、继续转让、数据主体的权利以及投诉机制、提交至司法管辖区等。

⑦ 第 14 条,影响遵守本条款的地方法律。

⑧ 第 15 条,在公共部门提出查阅数据请求时数据进口方的义务。

此类传输进行全面风险评估,[①]包括:传输的所有事实;数据接收方的当地法律和惯例(执法机构与国家安全机构获取数据的法律和惯例);任何相关的技术、合同或组织措施。针对政府机构访问数据这一行为,鉴于欧洲法院无法对美国政府的监控行为直接进行规制,只能在合同中对数据接收方的行为予以限制。数据接收方应将此类请求告知提供方,并在可能的情况下告知数据主体,如若当地法律禁止数据接收方告知数据提供方或数据主体,导致数据接收方无法发出该通知,则数据接收方须尽"最大努力"取得对法律禁令的豁免。此外,数据接收方仍需定期向数据提供方提供尽可能多的、有关数据访问请求数量和类型的透明度报告。数据接收方必须审查任何此类请求的合法性,并在具备合理理由的情况下对非法请求提出质疑,还需用尽现有上诉的可能性,以获得充分救济。此外,在回应披露请求时,数据接收方只提供法律强制规定所需的最低限度的信息。上述法律规定增加了数据接收方的义务,由此表现出欧盟在数据保护上的谨慎态度。

2. 基于风险方法下的补充措施 2.0

为协助接收方采取"补充措施"达到欧盟"实质同等"的保护水平,识别、确定和实施适当的额外保障措施,欧洲数据保护委员会于 2020 年 11 月 11 日就《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传输工具补充措施的建议》(版本 1.0)[②]公开征求意见。征求的意见认为,政府数据访问规定导致一些国家的隐私保护水平达不到欧盟要求,欧盟国家因此无法传输数据到美国、俄罗斯与印度等国。此外,征求的意见还认为,补充措施 1.0 排除了"数据提供方认为数据接收国公共机构访问此类数据可能性"的主观因素,而要求数据提供方仅需考虑在客观上数据接收国的法律是否符合欧盟要求,这一规定过于严苛,仍需再行考量。

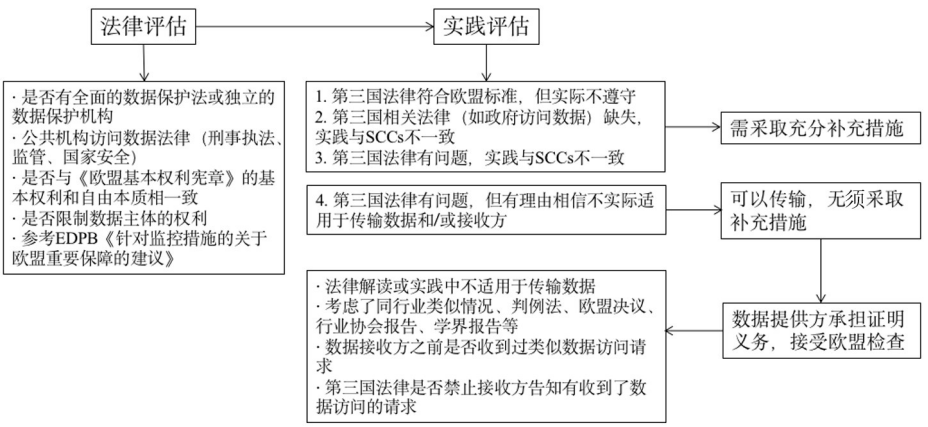
在上述背景下,2021 年 6 月 18 日,欧洲数据保护委员会最终更新了《关于为确保遵守欧盟个人数据保护水平而采用的对数据跨境传输工具补充措施的建议》(版本 2.0,以下简称"补充措施 2.0")。补充措施 2.0 采用了基于风险的方法,来考察第三国现行有效的相关措施是否有效保护了个人数据。相较于补充措施 1.0,补充措施 2.0 放弃了前者严格的"基于风险"路径,而是纳入了包含主观因素的风险评估。补充措施 2.0 包括 6 项审查步骤,要求进行跨境数据流动的企业首先梳理数据跨境传输情

① Tanguy Van Overstraeten, "EU: New Standard Contractual Clauses—From Theory to Practice," LINKLATERS, 4 June 2021, https://www.linklaters.com/en/insights/blogs/digilinks/2021/june/eu-new-standard-contractual-clauses-from-theory-to-practice.

② EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data, Adopted on 10 November 2020.

况,在此基础上识别数据传输工具充分性保护路径、标准合同条款与约束性公司规则等,若满足充分性保护或符合 GDPR 第 49 条“克减措施”,则可直接进行数据跨境传输,否则需要对第三国的法律与实践状况予以评估(如图 1),①根据评估结果来决定是否采取必要的补充措施②,补充措施应遵循正式程序性步骤,并定期重新进行评估。评估过程含实质与形式上的严苛义务。其中,补充措施具体包括组织措施、附加合同措施与技术措施三种方式,以达到所需的数据保护水平。③ 此外,确定的补充措施不得直接或间接与标准合同条款相抵触,并确保 GDPR 所保证的保护水平不被削弱。

图 1 法律评估与实践评估的具体内容



资料来源:作者根据欧洲数据保护委员会“补充措施 2.0”相关内容及其附件 3 整理。

① 附件 3 为数据提供方提供了一份非常简短的清单,其中列出了评估第三国数据保护水平的部分信息来源:欧洲联盟法院和欧洲人权法院的判例法、欧盟委员会的充分性认定、政府间组织和区域机构(如欧洲委员会和联合国机构)的决议和报告、相关的国家判例法、贸易协会的报告,以及学术机构和民间社会组织(如非政府组织)的报告等。

② “补充措施”是对 GDPR 第 46 条转移工具以及 GDPR 的其他适用安全要求(例如技术安全措施)已经提供的保障措施的补充。参见 EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data Version 2.0, para.50。

③ EDPB, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data Version 2.0, Annex 2: Examples of Supplementary Measures, Adopted on 18 June 2021; 组织措施包括企业通过适当的数据传输治理的内部政策,明确分配相关责任、定期公布政府要求获取数据的透明度报告、尽量减少不必要的操作,以限制个人数据在未经授权的情况下被访问、根据欧盟认证或国际准则制定严格的数据安全和隐私政策等。补充措施 2.0 还建议采用附加合同条款,规定使用具体技术措施的合同义务、增强透明度义务(提供第三国公共当局获取数据的情况,包括在情报领域的情况)、赋予数据主体行使权利的合同义务。除了组织与附加合同要素之外,技术措施也成为补充措施的方式之一,加密/匿名化/假名化技术作为示例且为暂时的解决方案,需要满足加密足够强大且接收国的公共当局无法访问加密密钥的要件。

(三)标准合同条款的对内与对外影响

对欧盟而言,尽管数据外流时可能面临重重阻碍,短时间会造成欧盟数据传输国际贸易合作的减少,但新版标准合同与补充措施回应了欧洲法院对于标准合同条款作为跨境传输工具合理性的质疑,暂时弥补了欧美间《隐私盾协议》失效后的规则真空,提高了欧盟数据保护水平,细化了数据准确性原则,增强了 GDPR 的操作性,满足了欧盟企业商业模式日益复杂化的诉求,实现了 GDPR 制定后欧盟数据治理的又一次进步。

就国际社会而言,新版标准合同与补充措施将倒逼美国等国家完善数据立法,提高国家的数据保护水平。如美国在 Schrems II 案发生后提出有关保护个人数据的立法提案,以及在《白皮书》中对强制披露欧洲公民数据的情况进行澄清。实际上,日本、东盟、中国等国家或国际组织在跨境数据传输的框架设计上都不同程度上借鉴了欧盟的标准合同,因此,欧盟这一机制的革新有可能会影响到其他国家具体规则的制定或革新。值得注意的是,新版标准合同与补充措施的适用会形成不同国家的规则对抗:其一,对于"问责制"条款,数据提供方有可能与数据接收方所在国家形成法律冲突,如中国并没有将"第三方受益制度"纳入该种合同,不过这将取决于中国未来标准合同条款的具体设计;其二,对于数据报送制度,不同的国家在程序措施与救济途径上差别很大,中国政府机关调取企业数据的措施与欧盟所要求的"重要保障"标准差别较大。对从事数据跨境的企业而言,问责制使境内企业承担了更多更严格的连带责任,而数据报送制度将增加企业的合规成本。目前,企业纷纷更新原有标准合同条款,及时做好企业合规。某种程度上,随着各个国家个人数据保护法的完善,企业合规成本将不断提升。

综上所述,标准合同条款仍是欧盟最为重要的数据跨境传输机制,为欧盟数据保护提供了替代性与多层次的工具。鉴于其本身指向数据提供方与数据接受方签订的数据传输合同机制,当与欧盟第三方受益人合同相结合时,可一定程度上保护基本隐私权益。Schrems II 案发生后,新版标准合同条款与补充措施重点评估数据进口国法律与实践状况,并针对政府访问公民数据向数据接收方提出新的要求,加之,法律、技术、组织补充措施可降低欧盟公民数据被侵犯的可能性。然而,一个值得关注的问题是,欧洲法院通过对标准合同条款的司法审查与效力控制,确立了"实质等同"标准,数据提供方仍需个案审查是否维持了适当的数据保护水平。在此情况下,一方面,数据提供方俨然成为"第三国法律方面的专家",这便意味着 GDPR 第 45 条的充分性测试可能吞并其余的传输机制。在无充分性决定时,数据保护监管机构有权质疑数据提

供方与数据接收方签订的合同。另一方面,数据接收方面临更为严苛的义务与国内监管和国外监管的双重压力,尤其在政府访问欧盟公民数据的情况下,数据接收方的通知行为可能构成对本地法律有关保密规定的违反,接收方对政府的要求进行合法评估也增加了企业的合规成本与守约难度,因而导致其倾向于进行个人数据本地化存储与处理。此外,一般跨国合同中关于责任豁免的"当地国家法律有强制性规定的除外"规则,在数据跨境传输中很难发挥作用,尤其是来自多法域数据混同在一起快速流动的情况下。

四 数据本地化与标准合同条款:中国数据跨境流动监管的最优解?

数据跨境流动对促进数字创新、提高经济增长与增进社会福祉至关重要。《全球数字经济白皮书——疫情冲击下的复苏新曙光》显示,2020 年,中国数字经济规模位居世界第二,高达 5.4 万亿美元,数字经济同比增长 9.6%,位居世界第一。数据产量占全球 9.3%,居世界第二。① 近年来,跨境数据流动已经成为推动数字经济发展的重要力量。② 一方面,在数据跨境流入的情景模式下,随着中欧经济、文化、政治与教育交流的增加,大量欧盟公民数据流入中国。③ 2021 年 9 月 14 日,欧盟主要数据隐私监管机构已针对 Tik Tok 处理儿童个人数据以及向中国传输个人数据是否遵循欧盟数据法两个问题启动调查。④ 另一方面,在数据跨境流出的情景模式下,中国形成了由法律、行政法规和规章构成的完备的法律构架。⑤《个人信息保护法》第三章具体规定

① 中国信息通信研究院:《全球数字经济白皮书——疫情冲击下的复苏新曙光》,2021 年 8 月,http://www.caict.ac.cn/kxyj/qwfb/bps/202108/t20210802_381484.htm。

② Center for Strategic and International Studies (CSIS), "Governing Data in the Asia-Pacific," April 2021, p.1, https://www.jstor.org/stable/resrep31139? seq=1#metadata_info_tab_contents.

③ Bo Zhao and Jeanne Pia Mifsud Bonnici, "Protecting EU Citizens' Personal Data in China: A Reality or A Fantasy?" *International Journal of Law and Information Technology*, Vol.24, No.2, 2016, p.129.

④ Sarah Harford, "Ireland's DPC to Probe TikTok over Handling of User Data," Siliconrepublic, 15 September 2021, https://www.siliconrepublic.com/enterprise/tiktok-dpc-user-data-children-china.

⑤ 如《网络安全法》(2016 年 11 月 7 日发布、2017 年 6 月 1 日实施),《数据安全法》(2021 年 6 月 10 日发布、2021 年 9 月 1 日实施),《个人信息保护法》(2021 年 8 月 20 日发布、2021 年 11 月 1 日实施),《关键信息基础设施安全保护条例》(2021 年 7 月 30 日发布、2021 年 9 月 1 日实施),《网络安全审查办法(征求意见稿)》(2021 年 7 月 10 日发布),《数据出境安全评估办法(征求意见稿)》(2021 年 10 月 29 日发布),《网络数据安全管理条例(征求意见稿)》(2021 年 11 月 14 日发布)。

了个人信息跨境提供的规则,①其中,硬数据本地化体现在“规定关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者收集和产生的个人数据本地化存储,确有必要仍需安全评估的基准”;②标准合同条款则要求“个人信息处理者向境外提供个人信息应按照国家网信部门制定的标准合同与境外接收方订立合同,约定双方的权利与义务”。③ 在上述背景下,本部分试图探讨的是硬数据本地化与标准合同条款是否为中国数据跨境流动监管的最优解,以及具体应如何优化相关制度设计。

(一)规则正当性基础:以数据安全为底线的跨境数据自由流动原则

中国《数据安全法》第 11 条规定了国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作,参与数据安全相关国家规则和标准的制定,促进数据跨境安全、自由流动。④ 中国高度重视数据安全保护,数据的跨境自由流动以数据安全为底线。数据的固有属性、数据流动的空间结构与经济基础决定了数据自由流动原则的正当性。作为全球数字经济的受益者与引领者,中国在《G20 大阪数字经济宣言》《区域全面经济伙伴关系协定》(RCEP)⑤等多边场合承认跨境数据流动的基础性地位,与此同时,在国内先行先试“数据跨境流通自由港”试点,加快探索香港大湾区的跨境数据自由流通。然而,为保护个人、国家与公共安全利益,对数据自由流动的安全规制是中国数据流动规则的另一个面向。中国数据安全既包括静态的安全,即对数据固有形态及其权益的保护,如技术安全(《数据安全法》第 3 条),也包括动态的安全,即对数据流动过程及其权益的保护,包括重要数据自主可控的综合安全(《国家安全法》第 25 条)与非重要数据可信的合作安全(《数据安全法》第 3 条)。⑥ 综合安全的保护可有力钳制外国情报监控制度的不当扩张,而合作安全可实现个人数据保护与数据自由流

① 如规定了在数据主体同意前提下安全评估、个人信息保护认证与标准合同文本三种方式(《个人信息保护法》第 38 条、第 39 条);规定数据本地化条款(《个人信息保护法》第 40 条);要求跨境数据调取遵循平等互惠原则(《个人信息保护法》第 41 条);规定境外侵害境内个人信息权益的保护原则(《个人信息保护法》第 42 条);规定歧视性措施的对等原则(《个人信息保护法》第 43 条)。除此之外,《个人信息保护法》总则第 12 条还规定国家积极参与个人信息保护国际规则的制定,促进个人信息保护方面的国际交流与合作,推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

② 《个人信息保护法》第 40 条。在此之前,中国《网络安全法》与《数据安全法》即确立了关键信息基础设施产生的个人数据出境的该种基本框架。

③ 《个人信息保护法》第 38 条第 1 款第 3 项。

④ 类似表述的还有《数据出境安全评估办法(征求意见稿)》第 1 条:为了规范数据出境活动,保护个人信息权益,维护国家安全和社会公共利益,促进数据跨境安全、自由流动,根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规,制定本办法。

⑤ 相较于 TPP“公共目标政策例外+本国监管例外”与 USMCA“公共目标政策例外”,RCEP 中发展中国家首次引领了关注基本安全利益的数据流动立场,给缔约方留有更多自由裁量权,并通过与发达国家合作开创了多元共治的数据流动解决方案。

⑥ 许可:《自由与安全:数据跨境流动的中国方案》,载《环球法律评论》,2021 年第 1 期,第 32 页。

动的动态平衡。相比美国以数据流通为原则、数据安全保护为例外,欧盟以个人数据保护为本位的数据治理模式,大数据安全与流动的双轨制更符合中国的国情,有利于兼顾和平衡各种利益。

一方面,数据本地化是维护中国数据主权与数据安全的必然选择,易于实现重要数据可控的综合安全。面对全球信息技术强弱不均的国家实力结构以及数据往往向强势国家流动的现状,不同于美国数据自由流动与欧盟数据权利保护工具的逻辑,中国与一些发展中国家采取的是一种国家战略上防御主义的数据本地化策略,①通过对数据的控制来保护自身的数据安全。以美国为代表的部分西方发达国家反对主权原则直接适用数据领域。不过,基于国家安全的考量,当前不少发达国家也出现数据出境传输收紧的趋势。需要指出的是,鉴于数据跨境传输具有广泛的国际性,跨境信息控制这一“互赖主权”的适当弱化,推动了网络经济和网络政务的发展,反过来增强了“国内主权”。② 相对的数据本地化设置也因此具有了正当性与合理性。此外,数据本地化与数据自由流动绝非彼此对立,鉴于中国的数字经济地位正在发生改变以及包容性的数据治理理念,中国在解释与具体设计数据本地化出境条款时,应在维护本国数据主权的同时保持适度的开放性。

另一方面,标准合同条款的设置为个人数据更为自由传输提供了法律工具,还易于实现非重要数据可信的合作安全。从标准合同条款的性质来看,它是私主体之间采用政府主体提供的格式合同,并在此基础上而达成的数据跨境传输协议。由此观之,标准合同条款通过企业与企业间、企业与国家间的信赖与合作,实现个人数据的动态安全。标准合同条款有益于为企业提供更多的法律可预测性,帮助中小企业确保数据安全传输的要求,且更有效率。实际上,从中国数据跨境传输的设置构造来看,除关键信息基础设施的个人信息和重要数据与达到规定数量的个人信息处理者的个人信息需要本地存储与网信办安全评估之外,中国更多的是将权力下放到私主体上。《个人信息出境安全评估办法(征求意见稿)》中提供的“标准合同”尽管还处在概念化的阶段,却为中国继续推行该工具提供了良好的契机。

(二)规则构想:合理限制数据本地化与审慎设计标准合同条款

1. 数据本地化

相较于欧美隐私盾失效后 GDPR 所产生的“软数据本地化”的规制效果,中国跨境数据流动规则从建立之初就呈现出明显的“硬数据本地化”的规制特征,即遵循以

① 刘金河、崔保国:《数据本地化和数据防御主义的合理性与趋势》,第 89 页。

② 张新宝、许可:《网络空间主权的治理模式及其制度构建》,载《中国社会科学》,2016 年第 8 期,第 145 页。

数据本地化为原则,安全评估为例外的路径,由此为欧美诟病。《网络安全法》第 37 条为中国法律框架引入了针对“关键信息基础设施”运营者在中国境内收集个人信息或“重要数据”的数据本地化规定,并对跨境数据传输采用了有限的和安全的评估方案,因业务需要确需向境外提供个人信息的,按照网信部门与国务院有关部门制定的办法进行“安全评估”。① 此外,《个人信息保护法》还要求个人信息达到国家网信部门规定数量的个人信息处理者仍需境内存储个人信息。其中,“关键信息基础设施”“重要数据”与“安全评估”是数据本地化与跨境数据传输评估的三个重要切入点。

首先,刚刚生效的《关键信息基础设施安全保护条例》第 2 条解决了第一个切入点的问题,即明确了关键信息基础设施的定义与调整范围。② 其次,于 9 月 23 日公布的《信息安全技术 重要数据识别指南(征求意见稿)》旨在针对第二个切入点,以明晰重要数据的核心概念。此处的重要数据为“以电子方式存在的,一旦遭到篡改、破坏、泄露或者非法获取、非法利用,可能危害国家安全、公共利益的数据”,③并排除了个人信息与国家秘密,其识别基准聚焦安全影响、综合考虑风险,且定性与定量相结合。不过,《数据安全法》扩大了“重要数据”的出境限制对象,不再仅限于关键信息基础设施,而是扩展到所有的数据处理者。最后,从数据本地化的例外要求来看,《网络安全法》生效 4 年以来,安全评估仍为跨境数据传输的重点与难点之一。④ 其一,在设置理念上,相较于欧美国家只针对个人信息的数据保护评估,中国将关键信息基础设施重要数据与个人数据的出境评估合并设置在《网络安全法》中,这有可能会增加与国际社会的对话成本,影响数据的利用效率。此外,中国重要数据与个人数据出境评估制度历经从合并到分离再至合并方式的频繁变更,其更多的是数据立法逐渐明朗的产物,反映了当时的立法需求,但同时增加了相应的制度成本。其二,在评估方式上,尽管《数据出境安全评估办法(征求意见稿)》规定了企业数据风险的自评估,⑤但中国

① 张金平:《跨境数据转移的国际规制及中国法律的应对——兼评我国〈网络安全法〉上的跨境数据转移限制规则》,载《政治与法律》,2016 年第 12 期,第 151 页。

② 《关键信息基础设施安全保护条例》第 2 条。本条例所称关键信息基础设施,是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

③ 《信息安全技术 重要数据识别指南(征求意见稿)》第 3.2 条。在此之前已经颁布关于征信业信息、人类遗传资源、人口健康信息、位置和地图信息、网络出版信息的相关规则。

④ 中国于 2017 年 4 月 11 日发布了《个人信息和重要数据出境安全评估办法(征求意见稿)》,2019 年 6 月 13 日发布了《个人信息出境安全评估办法(征求意见稿)》,2021 年 10 月 29 日发布了《数据出境安全评估办法(征求意见稿)》。关于出境评估的制度设计,2017 年 4 月 11 日发布的《个人信息和重要数据出境安全评估办法(征求意见稿)》最初分为无须提供给主管部门的自评估与达到特定标准需要交由行业主管部门或网信办的安全评估。而后《个人信息出境安全评估办法(征求意见稿)》与《个人信息保护法》均转变为需由国家网信部门组织安全评估。《数据出境安全评估办法(征求意见稿)》现又规定企业自评估与行业主管部门或网信办安全评估两种方式。

⑤ 《数据出境安全评估办法(征求意见稿)》第 5 条。

的评估机制更多侧重“一事一议”与网信办等国家各部门安全评估相结合的模式。而欧盟 GDPR 中充分性保护是对第三国、地区与国际组织进行的广泛评估,标准合同条款与有约束力的公司准则侧重对组织内部保护水平的评估,美国《跨境隐私规则》(简称 CBPR)旨在依赖企业的自评与测评机构的合规审查。因此,部分国家对中国加入《全面与进步跨太平洋伙伴关系协定》(CPTPP)的数据出境条款已经提出异议,它们认为既有的数据跨境流动机制没有安全评估的先例。① 其三,在评估内容上,新近发布的《数据出境安全评估办法(征求意见稿)》第 4 条②就个人信息规制主体与规制对象进行了量级规定,即处理个人信息达到 100 万的个人信息处理者与累计向境外提供超过 10 万人以上个人信息或者 1 万人以上敏感个人信息。然而,这种定量基准与方式是否合理?一方面,《互联网平台分类分级指南(征求意见稿)》将大型平台的用户数量定为不低于 5000 万,与办法所要求的数量相冲突。该办法的数量基准是否过低,导致小型平台亦需出境安全评估,形成事实上的数据流动障碍?另一方面,纯粹的定量分析方式是否会忽视个人信息的定性结果?例如,尽管出境的特殊敏感数据尚未达到 1 万人,但结合信息主体身份、用途、处理方式实质上已达到应当安全评估的标准,这种情况该如何处理?此外,为了确保公共安全与促进监管便利,中国实施多项针对特定行业的数据本地化规定。③ 由于制度以及规则存在一定的碎片化问题,即使《个人信息保护法》出台,短期内也无法改变国外对中国“数据本地化”的刻板印象。④

为实现中国数据保护与数据自由流动的动态平衡,未来更加顺利地开展区域与多边数字谈判,笔者认为,有必要对中国的“硬数据本地化规则”进行合理限制。为此,可从“关键信息基础设施”“重要数据”与“安全评估”三个方面做出如下改进。

首先,《关键信息基础设施安全保护条例》虽对何为“关键信息基础设施”、相关程序与主体责任做出明确规定,但囿于中国数据保护多部门监管的特点,没有独立的数

① 洪延青:《数据出境安全保障的中国路径》,世界互联网大会,2021 年 9 月 28 日,https://mp.weixin.qq.com/s/nSMB0nGLwAijYmtbCzvXjw。

② 《数据出境安全评估办法(征求意见稿)》第 4 条 数据处理者向境外提供数据,符合以下情形之一的,应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估:(1)关键信息基础设施的运营者收集和产生的个人信息和重要数据;(2)出境数据中包含重要数据;(3)处理个人信息达到一百万人的个人信息处理者向境外提供个人信息;(4)累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息;(5)国家网信部门规定的其他需要申报数据出境安全评估的情形。另外,《网络数据安全管理条例(征求意见稿)》第 37 条做出了相似的规定。

③ 包括健康信息、征信机构信息、商业银行信息、互联网地图信息、出租车平台经营者业务数据、邮递快件服务信息等,如《人口健康信息管理办法》第 10 条、《征信业管理条例》第 24 条、《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第 6 项、《地图管理条例》第 34 条、《网络预约出租汽车经营服务管理暂行办法》第 27 条、《邮件快件实名收寄管理办法》第 16 条等。

④ 例如,OECD 数字服务贸易指数将中国列为限制程度最高的国家,USTR《国别贸易壁垒评估报告》之《数字贸易主要壁垒》批评中国的数据保护主义措施,欧美日数据治理合作也对抗中国。转引自李墨丝:《欧美日跨境数据流动规则的博弈与合作》,载《国际贸易》,2021 年第 2 期。

据保护机构,为防止追责,监管部门容易出现应本地尽本地的情况。因此,未来可考虑直接建立独立的数据保护机构,以解决上述难题。

其次,有关重要数据,亦应分级分类,这一机制的合理设置有益于中国在未来国际合作中,将“安全例外条款”或“基本安全利益条款”更为顺利地纳入双边或区域经济协定中的数字条款。

最后,中国数据出境安全评估基于数据安全、国家安全与个人数据保护的三个维度而设置,这符合数据出境管控的国际趋势。不过,在设置理念上,应在数据安全为底线的跨境数据自由流动原则的基础上,坚持重要数据与个人数据出境评估制度的合并立法方式,合理设置个人信息与重要数据的出境评估条款,避免立法的频繁变更。在评估方式上,中国的安全评估与其他国家的数据出境评估其实并无实质性差异,只是立法技术的不同。因此为消解 CPTPP 部分国家对中国出境安全评估制度的疑虑,中国谈判代表可对本国的立法模式做出澄清。另外,加强行业自律可降低数据跨境传输风险。未来,随着中国数据治理体系日益完善,对于企业的数据自评估也亟须国内在此方面加以引导。在评估内容上,针对上文提及的《数据出境安全评估办法(征求意见稿)》第 4 条的量级规定,主管部门仍需注意立法协调的问题与量级立法方式可能忽视的定性标准,以做出更为合理的规定。在具体设计数据出境评估场景时,评估机构应结合数据类型区分管制,对于个人数据和重要数据,评估机构要遵守评估中的比例原则,前者应强化个人对数据的控制权,后者则注重数据出境后的国家安全风险。评估机构均应对数据进口国进行法律与实践评估。评估方案应强化数据提供方的义务,完善救济渠道,而纯粹的商业数据应鼓励流动。

2.标准合同条款

《个人信息保护法》的数据跨境传输工具参照了欧盟 GDPR 第五章的基本框架,并谨慎删除充分性保护的认证路径,在数据主体同意的前提下,保留了安全评估、认证机制与标准合同条款的规定。目前,三种机制还处于制度设计阶段。其中,机制一与机制三已具体出现在现有的法律文本之中,机制二认证制度借鉴欧盟的认证制度,上海自由贸易试验区临港新片区、北京和浙江的自由贸易试验区在总体实施方案中均提出建立数据保护认证制度。[①] 此外,《个人信息保护法》第 38 条第 3 款还增加了补充性的个人信息处理者的义务性规定,即需要采取必要措施,以使境外接收方的个人信息处理活动达到本法规定的标准。此处的必要性措施适用上述三种机制,并且同样需

① 周念利、姚亭亭:《中国自由贸易试验区推进数据跨境流动的现状、难点及对策分析》,载《国际商务研究》,2021 年第 3 期,第 6 页。现已有国家认证(如美国 FedRAMP、德国 C5、澳大利亚 IRAP)和全球认证(ISO 27001 和 ISO 27018)。

要有关部门的解释。

实际上,《个人信息出境安全评估办法(征求意见稿)》(以下简称《办法》)已涉及中国式标准合同条款工具的设计思路。《办法》注重发挥“网络运营者与接收者签订合同”的工具性价值,合同结构性分配网络运营者(第 14 条)与接收者(第 15 条)的责任和义务与个人信息主体的权利,①并针对个人信息的再次传输实施选择退出(opt-out),个人敏感信息的再次传输要求个人选择同意(opt-in)。② 上述制度设计有力保护了诸多数据跨境场景中的个人信息安全、网络空间主权与国家安全。然而,《办法》中的条款设计仍过于原则化。此外,《数据出境安全评估办法(征求意见稿)》第 9 条③也仅是简单规定数据处理者与境外接收方订立合同的内容。因此,仍需对标准合同条款的具体设计提出方案,域外制度经验或许可为中国提供一定的借鉴。

目前来看,除了上文所述欧盟的新标准合同条款之外,东盟数字部长会议于 2021 年 1 月 22 日批准了《东盟数据管理框架》(ASEAN Data Management Framework -DMF)与《东盟跨境数据流动标准合同条款》(ASEAN Model Contractual Clauses for Cross Border Data Flows -MCCs)。《东盟数据管理框架》提供的全数据生命周期④保障措施为数据企业赋能并确保了数据安全。《东盟跨境数据流动标准合同条款》从微观规定数据传输的实操规则,相较于欧盟新标准合同条款,在传输地点与方式上,限于在东盟内部传输,仅包含从数据控制者传输个人数据,而不涉及从数据处理器传输个人数据。在法律属性上,《东盟跨境数据流动标准合同条款》为数据企业自愿选择条款,是一种灵活的且仅仅作为最低要求的非约束性条款,而欧盟新标准合同条款为必选条款,为确保符合输出国的数据法律法规要求,有时仍需进行修订和补充。欧盟新标准合同条款还要求新纳入条款不得与已有标准合同条款相抵触。

对于欧盟与东盟两个区域经济体的跨境数据规则工具进行审视与利弊研判,有益

① 个人信息主体可查询的内容包括:网络运营者与接收方之间签署的合同副本、个人信息主体网络运营者和接收者的基本情况,以及向境外提供个人信息的目的、类型和保存时间等内容。在保障知情权的前提下,个人信息主体能够更好地行使其权利。

② 洪延青:《解析〈个人信息出境安全评估办法(征求意见稿)〉实体保护规则背后的主要思路》,中国网信网,2019 年 6 月 15 日,http://www.cac.gov.cn/2019-06/15/c_1124628000.htm。

③ 第 9 条 数据处理者与境外接收方订立的合同充分约定数据安全保护责任义务,应当包括但不限于以下内容:(1)数据出境的目的、方式和数据范围,境外接收方处理数据的用途、方式等;(2)数据在境外保存地点、期限,以及达到保存期限、完成约定目的或者合同终止后出境数据的处理措施;(3)限制境外接收方将出境数据再转移给其他组织、个人的约束条款;(4)境外接收方在实际控制权或者经营范围发生实质性变化,或者所在国家、地区法律环境发生变化导致难以保障数据安全时,应当采取的安全措施;(5)违反数据安全保护义务的违约责任和具有约束力且可执行的争议解决条款;(6)发生数据泄露等风险时,妥善开展应急处置,并保障个人维护个人信息权益的通畅渠道。

④ 从 DMF 的生命周期来看,主要包括六个组成部分:治理和监督;政策和程序性文件;数据清单(数据识别和归类);影响/风险评估;控制;监控和持续改进。

于中国做出更为缜密的制度设计,以便于未来与区域经济体进行合作与互认。相较于欧盟通过“宪法审查”来保障数据主体的基本权利,中国应在数据安全的前提下,注重谨慎协调的立法设计。

第一,在模式选择上,标准合同文本宜借鉴欧盟标准合同条款范本中的风险调控模块化方法,重点区分个人信息处理者和受托处理者之间的多种传输模式,因而可满足跨境传输企业的现实需求;还应区分中国与欧盟在数据处理者与数据控制者的定义上的不同之处。① 第二,在条款补充上,数据提供方与数据接收方可签订更为具体的合同,但不得修改标准合同文本条款,增加条款不得与标准合同文本相冲突。第三,在生命周期设置上,在数据出境前,数据处理者无须进行国家网信办安全评估,只需将数据安全风险与保障措施报告向当地机关备案。数据合同的内容应具体规定多种场景下当事人的义务条款,确保从出境到入境的全生命周期的数据安全,并且根据数据的敏感性来界定保障措施的安全性。在数据出境后,数据接收方需告知数据提供方和数据主体政府机构的数据访问请求,并可质疑政府机构的非法数据访问请求。此外,如果数据接收方国内监管政策发生重大变化,接收方也应及时告知数据提供方与数据主体。通过上述措施,中国可限制他国公权力对本国个人数据的访问,确保本国公民的数据主体权益得到有效、合理与及时的保护。第四,在救济路径上,采用“问责制”进路,要求个人数据接收方承担连带责任,以实现《个人信息保护法》的域外效力,并规定其他违反合同义务时的权利救济条款。第五,在管辖法院上,数据提供方与数据接收方产生的争议应接受中国管辖,以维护中国的数据主权。

(**作者简介**:李艳华,厦门大学法学院博士研究生;**责任编辑**:张海洋)

① 《个人信息保护法》中个人信息处理者的范围与 GDPR 的“控制者+处理者”的范围,并没有实质的区别。