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*

金　晶

内容提要:个人数据保护标准是欧盟基本权利保护的制度体现。欧盟数据跨境传输规则和欧洲法院司法监管均以实现欧盟个人数据保护标准为要旨。数据传输的一般原则是针对出境数据的永久最低保护标准,充分性决定和标准数据保护条款是欧盟贯彻个人数据保护标准的法律工具。前者整体适用于特定国家,后者个别适用于特定商事主体,欧洲法院司法审查旨在实现对数据流动的全球监管。中国数据立法须全面研判欧盟数据保护立法模式的潜在风险,谨慎对待充分性决定、标准数据保护条款等具有欧盟特色的复杂法律工具,摆脱法律移植欧陆成文法的历史惯性,避免盲目借鉴《一般数据保护条例》而落入欧洲法院司法审查的长臂管辖。数据流动立法应全盘统筹个人数据与非个人数据流动立法方案,探寻价值中立规则以提供法律趋同新思路,引领数据立法的全球竞争。

关键词:数据跨境传输　数据自由流动　标准合同条款　个人信息保护　《一般数据保护条例》

数据的生命在于流动,数据跨境流动是数字经济全球化的命脉。数据流动突破了传统的国家疆界,往来于世界各国的机器云端。作为国家基础性战略资源,数据跨境流动带来了前所未有的风险:关键信息基础设施运营者和批量个人信息处理者在境内收集、产生的个人数据和重要数据一旦泄露或滥用,可能严重危害国家安全和公共利益;个人数据在境外遭到非法使用时,受害人无法向“千里之外”的第三国有效主张法律救济;各国主管机关囿于主权原则,难以监管处置境外的数据处理活动。如何发展

* 本研究受到以下基金项目的支持:中国政法大学科研创新项目“《民法典合同编》数字合同的规则建构与理论难点”(项目编号:10818438)、中国政法大学民法学青年学术创新团队项目(项目编号:19CXTD01)和国家社会科学基金项目“数字经济时代的合同法制度更新与制度供给研究”(项目编号:17BFX195)。感谢外审专家的宝贵意见,文责自负。

数字经济并确保数据流动的自由和安全,既是数字经济监管的全球挑战,也是各国数据立法的核心命题。

在数据流动领域,欧盟的数据保护立法呈现出一定程度的范式扩张。欧盟个人数据保护的基本价值随着“充分性决定”法律工具的运用融入日本、韩国的数据法律改革,①《一般数据保护条例》(General Data Protection Regulation,GDPR)立法模式一定程度上影响了中国《数据安全法》《网络安全法》和《个人信息保护法》的制度和概念。② 不仅东亚国家的数据法律受到欧盟法律的广泛影响,而且全球多国的数据立法现代化进程奉 GDPR 为圭臬,欧盟的“数据法律帝国”可以说已现雏形。③ 吊诡的是,欧盟并非数字经济“高地”,其数字市场与中美两国不可同日而语,这与数据立法的“欧洲中心主义”毫不匹配。④ 反之,中国作为数据资源大国,能否以及在多大程度上借鉴欧盟立法模式,亟须立法者审慎决断。

本文以“个人数据跨境传输的欧盟标准”为视角,在“欧盟基本权利保护”的宏观背景下,探索“欧盟数据法律范式”的扩张风险。文章首先考察欧盟个人数据保护标准在欧盟政策中的定位,随后从规则建构和司法推进两个维度,提炼个人数据跨境传输中欧盟个人数据保护标准的整体适用和个别适用以及欧洲法院的司法推动,最后反思中国数据立法借鉴欧盟数据法律范式的潜在风险。本文试图解决四个相互关联的问题:(1)欧盟个人数据保护标准的政策定位是什么?(2)欧盟个人数据保护标准如何嵌入个人数据跨境传输的法律规则之中?(3)欧洲法院如何推进欧盟个人数据保

① 2019 年 1 月 23 日,欧盟通过对日本的“充分性认定”;2021 年 6 月 14 日,欧盟和韩国公布“充分性认定”决定(草案)。欧盟对日本的“充分性认定”,参见 European Commission, “Commission Implementing Decision (EU) 2019/419 of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan under the Act on the Protection of Personal Information,” C(2019) 304, OJ L 76, 19.03.2019, pp.1-58; https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC; 欧盟对韩国的“充分性认定”草案,参见 https://ec.europa.eu/info/sites/default/files/draft_decision_on_the_adequate_level_of_protection_of_the_republic_of_korea_with_annexes.pdf。

② 《个人信息保护法》的诸多概念、原则和规则都一定程度地借鉴了 GDPR。例如,区分个人信息和敏感个人信息、专章规定个人信息的跨境提供、将标准合同作为个人信息跨境提供的合法方式,确立删除权等个人主体权利。学界关于个人信息保护的比较法研究,参见周汉华:《〈个人信息保护法(草案)〉:立足国情与借鉴国际经验的有益探索》,载《探索与争鸣》,2020 年第 11 期,第 9-11 页;周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,载《法学研究》,2018 年第 2 期,第 3-23 页;高富平:《制定一部促进个人信息流通利用的〈个人信息保护法〉》,载《探索与争鸣》,2020 年第 11 期,第 12-14 页;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 30-36 页;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 22 页。

③ 例如,GDPR 对智利、韩国、巴西、日本、肯尼亚、印度、加利福尼亚、印尼等其他地区国家产生了影响。参见 European Commission, “Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital transition—Two Years of Application of the General Data Protection Regulation,” COM(2020) 264 final, 26.06.2020, p. 3。

④ 法律领域欧洲中心主义的相关论述,参见朱明哲:《中国近代法制变革与欧洲中心主义法律观》,载《比较法研究》,2018 年第 1 期,第 155 页。

护标准并监管全球数据流动？(4)欧盟数据法律范式有何扩张风险？

一 欧盟个人数据保护标准的政策定位

保护基本权利和建设欧盟内部市场，可谓欧洲一体化进程中最为古老的两项目标。从1995年《数据保护指令》到2016年的《一般数据保护条例》，直至2020年的《欧洲数据战略》，上述双重目标在数据跨境流动领域表现为：保护基本权利，尤其保障与数据保护相关的基本权利；建设欧盟内部市场，尤其是实现数据的自由流动，建构单一数据市场。①

建构和推广欧盟个人数据保护标准是欧盟数据立法的一项重要政策内容。以欧委会通讯为例，早在2010年，《欧盟个人数据保护整体方案》就提出要制定个人数据保护的国际法律标准和技术标准，将高度统一的欧盟数据保护水准视为推广欧盟标准的最佳方法。② 2012年，《在互联世界中保护隐私：面向21世纪的欧盟数据保护框架》表明，个人数据跨境传输时，无论处理者是否位于欧盟，无论何时向欧盟公民提供商品，应适用欧盟的标准和规则，创建高水平的欧洲数据保护标准。③ 2017年，《全球化世界中个人数据的交换和保护》提出，GDPR提供多种数据跨境传输机制，将国际数据流动和个人保护最高水准相结合，应推广欧盟高水平的数据保护标准。④ 2020年，在《数据保护作为公民赋权的支柱和欧盟数字化转型路径：GDPR两年适用》中，欧盟委员会认为，GDPR广受国际社会欢迎，欧盟在数据保护领域的领导地位表明其可以成为数字经济监管的标准制定者。⑤ 以冯德莱恩(Ursula von der Leyen)领衔的新一届欧委会在发展欧盟数据法律标准上更为积极。2020年，欧委会在《欧洲数据战略》《塑造欧洲的数字未来》和《人工智能白皮书》中提出，应制定欧洲标准，推进欧洲方法，制

① European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union," COM(2010) 609 final, 04.11.2010, p.1.

② Ibid., pp.15-19.

③ European Commission, "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century," COM(2012) 9 final, 25.01.2012, pp.10-13.

④ European Commission, "Exchanging and Protecting Personal Data in a Globalised World," COM(2017) 7 final, 10.01.2017, pp.2-3; European Commission, "Data Protection Rules as a Trust-enabler in the EU and beyond - taking Stock," COM(2019) 374 final, 24.07.2019, pp.1-3, p.11, 19.

⑤ European Commission, "Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation," p.3, 10, 14, 18.

定全球标准。① 欧盟内部市场委员布雷顿(Thierry Breton)甚至提出,要让欧盟占据标准制定领域,成为标准的制定者。②

在数据流动的制度供给上,欧盟通过立法和司法,将欧盟个人数据保护标准融入顶层设计。在规则建构上,GDPR 专章规定个人数据跨境传输规则,将欧盟个人数据保护水准作为数据保护是否得到"充分保障"的评判标准。在司法推动上,2015 年 Schrems I 案和 2020 年 Schrems II 案形塑了数据跨境流动中欧洲法院的强监管角色。③ 在 GDPR"确保欧盟公民个人数据传输到境外时,欧盟个人数据保护随数据流动到域外"的宗旨之下,欧盟个人数据保护标准随着数据流动流向世界。

二 规则建构:数据跨境传输标准的整体适用与个别适用

在规则建构层面,GDPR 确立了数据跨境传输的欧盟立法范式,欧盟个人数据保护标准融入数据跨境传输的规范体系之中:数据传输的一般原则(GDPR 第 44 条)是针对出境数据的永久最低保护标准;充分性决定(GDPR 第 45 条)是针对特定国家"整体适用"欧盟个人数据保护标准的法律方案;标准数据保护条款(GDPR 第 46 条)是针对特定商事主体"个别适用"欧盟个人数据保护标准的法律工具。

(一)数据传输一般原则:出境数据的永久最低保护标准

欧盟立法者认为,一旦超出 GDPR 的适用范围,就存在数据接收国(第三国)无限制使用数据的风险,因此,GDPR 对数据跨境传输采取了"原则禁止+例外允许"的基本模式。在规范构造上,立法者将数据传输的一般原则(GDPR 第 44 条)设计为"附许可保留的预防性禁止规定",以禁止数据传输作为一般原则,仅在符合 GDPR 第五章的特定前提时,方才允许数据跨境传输。一般原则的功能在于:一方面为欧盟的出境数据确立了以欧盟保护水平为准的数据保护永久最低标准;另一方面蕴含了对数据

① European Commission, "On Artificial Intelligence—A European Approach to Excellence and Trust," White Paper, COM(2020) 65 final, 19.02.2020, pp.8-9; European Commission, "A European Strategy for Data," COM(2020) 66 final, 19.02.2020, p.5; European Commission, "Shaping Europe's Digital Future," COM(2020) 67 final, 19.02.2020, p.2, 13, 16.

② Thierry Breton, "The Geopolitics of Technology," 27.07.2021, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/geopolitics-technology_en; "Europe: The Keys To Sovereignty," 11.09.2020, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en; "Digital Sovereignty: Commission Kick-starts Alliances for Semiconductors and Industrial Cloud Technologies," 19.07.2021, https://ec.europa.eu/cyprus/news/20210719_2_en.

③ C-362/14-Schrems, Maximillian Schrems v Data Protection Commissioner, Judgment of 06.10.2015; C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020.

传输的二阶审查,将数据传输合法性审查的管辖范围延长到出境数据,实现了欧盟数据保护标准的域外扩张。

首先,数据传输的一般原则(GDPR 第 44 条第 2 句)确立了数据保护的永久最低标准(Perpetuiertes Schutzniveau),实现了个人数据保护水平的地域扩张。① 结构上看,GDPR 第 44 条共两句,第 1 句明确:"就正在处理中的个人数据或拟在传输到第三国或国际组织后进行处理的个人数据,包括从第三国或国际组织再传输到其他第三国或国际组织的个人数据,控制者和处理者仅在满足 GDPR 的第五章的规定后方可传输";第 2 句规定:"GDPR 第五章的所有规定都应适用,以确保 GDPR 所保障的对自然人的保护程度不受减损"。该条包含三项规范要素:(1)界定适格跨境传输的前提条件(第 1 句第 1 种情形);(2)所有后续传输亦适用上述前提条件(第 1 句第 2 种情形);(3)确立数据跨境传输的一般解释规则(第 2 句)。实质上,GDPR 第 44 条第 2 句是欧盟永久保护水平理念的具体化,保证出境数据享有的保护水平不低于 GDPR 的数据保护水平,为第三国或国际组织的数据进口方确立了数据保护的永久最低标准。②

其次,二阶审查(GDPR 第 44 条第 1 句)为数据出境建构了合法性审查框架。仅在符合 GDPR 所有其他规定(第一阶审查)并遵守第五章规定(第二阶审查)的前提下,方可实现数据出境。这意味着,数据跨境传输时,第一阶段审查仅针对传输本身的合法性,审查依据不仅包括传输本身涉及的法律依据,还涵盖 GDPR 的所有规定,但这种全面审查不涉及第三国。第二阶段审查才会考察数据传输是否满足跨境的特别要求,即数据传输的许可是否扩展到 GDPR 地域适用范围之外的领域。③ 换言之,数据出境时,仅符合 GDPR 第五章不足以构成合法依据,数据跨境传输不仅要满足数据保护的一般规定(GDPR 第 5 条至第 8 条),还要满足涉及第三国数据处理要求的特别规定(GDPR 第 13 条第 1 款第 f 项、第 14 条第 1 款第 f 项、第 15 条第 1 款第 c 项和第 2 款、第 28 条第 3 款第 a 项、第 30 条第 1 款第 d 项和第 e 项及第 2 款第 c 项)。④

(二)充分性认定:针对国家的整体适用工具

如果将数据传输的一般原则定位为欧盟管制出境数据的框架性规范,充分性认定(GDPR 第 45 条)可谓欧盟法下实现数据跨境传输的最便利的法律工具。它履行了

① Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, C.H.Beck, 2021, Art. 44 Rn. 16.

② Ibid.

③ Ibid., Art. 44 Rn. 9-10; Thomas Zerdick, in Eugen Ehmann und Martin Selmayer (Hrsg.), *Datenschutz-Grundordnung Kommentar*, C.H.Beck, 2018, Art. 44 Rn. 13.

④ Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 44 Rn. 9.

《欧盟基本权利宪章》第 8 条第 1 款的保护个人数据的义务,旨在确保出境数据能在欧盟境外继续延续欧盟的高水准保护,确保域外国家提供的数据保护水平与欧盟实质等同。① 欧委会以决定形式签发充分性认定,认定第三国、第三国特定区域或行业、国际组织能够确保提供充分数据保护水平,在获得充分性决定之后,数据出口方无须提供进一步的数据保护或任何其他授权,即可实现数据出境。

就法律工具的功能而言,充分性认定是一种整体适用、整体审查的法律形式,即对域外国家/组织进行数据保护水平的全面审查,认定特定第三国能否提供与欧盟相当的数据保护的充分水平(GDPR 第 45 条),这种充分保护水平不要求第三国法律制度与欧盟法相同,但要求第三国法律制度能在事实上确保其数据保护水平与欧盟保护水平"实质相当",整体审查的判定依据不仅包括 GDPR 第 45 条第 2 款、GDPR 序言第 102 项至第 104 项,还包括欧洲法院 Schrems I 和 Schrems II 判决确立的实质审查基准。②

就法律工具的适用而言,充分性认定主要借助实体标准(GDPR 第 45 条第 2 款)来实现整体适用。充分性认定的实体标准包括但不限于:(1)第三国存在有效数据保护体系;(2)第三国存在有效数据保护监管;(3)国际义务。③ 三项标准中,第一项标准"第三国存在有效的数据保护体系"尤其值得关注,这一标准为欧委会"变相"创设了审查域外国家法律状况的合法权限,欧委会可以依据欧盟标准和欧盟基本价值观,来整体实质评估第三国的法治和基本权利保护状况。首先,这是一项极为宽泛的标准,数据保护体系包括第三国的一般性或行业性的法律规范,有效的数据保护规则涵盖具有法律拘束力、满足透明度要求的规则,并且数据保护规则不限于数据保护领域的法律规则,也包括其他领域的规则,例如公共安全、国防、国家安全和刑法领域的法律规范,还包括不具有正式法源地位的规则,例如专业规则或安全措施。④ 其次,欧委会评估第三国数据保护法治状况与欧盟是否"等同"时,需在法治、尊重人权和基本自由(《欧洲联盟条约》第 1 条,第 2 条,第 3 条)以及保障《欧盟基本权利宪章》的背景下,对第三国的所有数据保护专门立法和其他领域立法状况进行评估。如果第三国法律规定针对侵害相应保护领域的情形,对侵害措施的范围和适用既无清晰、准确的规定,也未设置任何最低要求,或者对个人数据保护的限制不限于绝对必要程度,又或者

① European Commission, "Exchanging and Protecting Personal Data in a Globalised World," COM(2017) 7 final, 10.01.2017, p.4.

② Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 1b.

③ Ibid., Art. 45 Rn. 4.

④ Ibid., Art. 45 Rn. 4a.

侵害了基本权利的本质内容,就不满足(第三国法律与欧盟数据保护立法的)“等同”要求。① 因此,“第三国存在有效的数据保护体系”标准是一种裁量空间极大的实质审查。此外,欧盟还引入了第二项实体标准,即“有效的数据保护监管”标准,将实质审查的触角延伸到第三国的法律运行和法律救济层面。在“有效的数据保护监管”标准下,第三国仅在理论上存在数据保护监管立法远远不够,必须在实践中存在特定机构(审级)监督、执行数据保护法律的有效适用,保证遵守数据保护立法。②

就法律工具的效果而言,充分性认定是向第三国“整体适用”欧盟个人数据保护标准的一种法律方案,旨在确保在个人数据传输到第三国时继续提供高水平保护,确保欧盟对第三国采取协调一致的处置方式。③ 整体适用意味着,欧委会签发充分性认定的决定,表明欧盟官方认可该第三国具备“与欧盟兼容”的数据保护水平。④ 欧委会亦可通过签发充分性决定的机会,与第三国进行建设性对话,从而在全球范围内创建高水平的“与欧盟兼容”的数据保护标准,欧盟由此成为数据保护标准的出口方。⑤

(三)标准数据保护条款:针对商事主体的个别适用工具

如果说充分性认定是欧盟对特定第三国整体适用个人数据保护标准,那么替代性数据传输工具则是一种个别适用欧盟个人数据保护标准的法律工具。这类法律工具的适用范围虽然有限,仅适用于特定商事主体之间的特定数据传输,但更为灵活,其地理适用范围不限于特定第三国,原则上可以全球适用。⑥ GDPR 第 46 条确立了:(1)经批准的标准数据保护条款;(2)有拘束力的公司规则(BCR);(3)行为准则;(4)认证机制四类替代性数据传输工具。⑦ 当数据流向未获欧盟充分性决定的地区时,第三

① Boris P.Paal und Daniel A.Pauly(Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 4c; EuGH, “Ungültigkeit der Safe-Harbor-Entscheidung der EU betreffend die USA,” *NJW*, 2015, S.3151ff.

② Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 6; EuGH, “Ungültigkeit der Safe-Harbor-Entscheidung der EU betreffend die USA,” S.3151ff.

③ Thomas Zerdick, in Eugen Ehmann und Martin Selmayer (Hrsg.), *Datenschutz-Grundordnung Kommentar*, Art. 45 Rn. 1.

④ European Commission, “Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century,” COM(2012) 9 final, 25.01.2012; European Commission, “Exchanging and Protecting Personal Data in a Globalised World,” COM(2017) 7 final, 10.01.2017; Thomas Zerdick, in Eugen Ehmann und Martin Selmayer (Hrsg.), *Datenschutz-Grundordnung Kommentar*, Art. 45 Rn. 1.

⑤ European Commission, “Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century”; European Commission, “Exchanging and Protecting Personal Data in a Globalised World,” COM (2017) 7 final, 10.01.2017; Thomas Zerdick, in Eugen Ehmann und Martin Selmayer (Hrsg.), *Datenschutz-Grundordnung Kommentar*, Art. 45 Rn. 1; Albrecht Philipp, “Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung! - Ein Zwischenruf für einen einheitlichen Datenschutz durch die EU,” *ZD*, 2013, S.587.

⑥ Thomas Zerdick, in Eugen Ehmann und Martin Selmayer (Hrsg.), *Datenschutz-Grundordnung Kommentar*, Art. 46 Rn. 2.

⑦ European Commission, “Exchanging and Protecting Personal Data in a Globalised World,” COM(2017) 7 final, 10.01.2017, p.5.

国数据进口方可在“提供适当保障措施”的前提下,通过替代性数据传输工具实现数据国际流动。因此,标准数据保护条款是使用率最高的一种法律工具。

标准数据保护条款包括欧委会通过的标准数据保护条款(GDPR 第 46 条第 2 款第 c 项)和成员国数据保护监管机构通过的标准数据保护条款(GDPR 第 46 条第 2 款第 d 项)两种类型,欧委会通过的条款依据特定程序产生,由官方确认条款能够提供数据保护充分保障。① 在条款版本上,欧委会依据《数据保护指令》共发布三套标准合同条款,分别是《标准合同条款的决定(第一套)》(2001)、《替代性标准合同条款的决定(第二套)》(2004)和《针对第三国处理者的标准合同条款的决定(第三套)》(2010)。② 2021 年 6 月 4 日欧委会发布的最新版本条款取代了旧的三套条款,统一为一套条款四种模式,适用于欧盟或欧洲经济区内的数据控制者或处理者进行的跨境传输,旧的三套条款自 2021 年 9 月 27 日废止。③ 在名称上,标准数据保护条款(standard data protection clauses)与标准合同条款(standard contractual clauses)指代相同。

现行标准数据保护条款包含:(1)控制者到控制者;(2)控制者到处理者;(3)处理者到处理者;(4)处理者到控制者四种传输模式。现行条款合并规定四种模式,条款结构在不同模式“套叠”下迂回复杂,但事实上,四种模式是由旧的三套标准条款整合而来。旧的三套条款目标用途不同,第一套和第二套适用于数据控制者之间的数据传输,第三套条款针对第三国数据处理者。第一套和第二套条款的责任承担机制不同,第一套条款中数据出口方和进口方采取连带责任形式(第一套第 6 条第 2 款),第二套条款采取过错责任形式(第二套第 3 条第 a 款)。④ 第三套条款更契合数据处理商事实践惯例的全球化趋势,适用于在第三国的次级数据处理(sub-processing)情形,特

① Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 19.

② Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, under Directive 95/46/EC, OJ L 181, 04.07.2001, pp.19-31; Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 Amending Decisions 2001/497/EC and 2010/87/EU on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries and to Processors Established in such Countries, under Directive 95/46/EC of the European Parliament and of the Council, OJ L 344, 17.12.2016, pp.100-101; Commission Decision of 27 December 2004 Amending Decision 2001/497/EC as regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, OJ L 385, 29.12.2004, pp.74-84; Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.02.2010, pp.5-18; Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 Amending Decisions 2001/497/EC and 2010/87/EU on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries and to Processors Established in such Countries, under Directive 95/46/EC of the European Parliament and of the Council, C/2016/8471, OJ L 344, 17.12.2016, pp.100-101.

③ Commission Implementing Decision (EU) 2021/914 of 4 June 2021 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, OJ L 199, 07.06.2021, pp.31-61.

④ Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 26.

别针对在第三国设立的数据处理者(数据进口商)将其数据处理服务分包给在第三国设立的次级处理者进行次级数据处理服务的情形。① 因此,现行标准数据保护条款的四种模式针对的情形各异,商事主体应当依据个案需求选定条款。

标准数据保护条款结构相对稳定,包括欧委会决定本身和附件两部分。欧委会决定规定了条款的目的、适用范围和意义,附件完整纳入标准合同条款和相关表格。以2021年6月修订的现行版本为例,附件中的《标准合同条款》主要包括一般条款、数据出口方义务、数据进口方义务、违约救济与争议解决等内容,为当事人设定了具体义务内容且不得规避解释。②

1. 以合同义务"补强"域外数据保护水平之不足

标准数据保护条款的价值在于合同义务的标准化。当欧盟数据流向任意第三国的公司时,位于第三国的数据进口方和位于欧盟的数据出口方通过适用标准数据保护条款,以合同义务形式确定欧盟的个人数据保护标准。合同义务标准化的意义在于,作为一种为实现第46条目的而提供的适当保障措施,标准数据保护条款必须包含在特定数据传输情形中无法满足的那些数据保护的基本要素,从而实现了对特定数据传输中所欠缺的普遍适当的数据保护水平情形的合同补足。③ 换言之,当数据控制者将数据传输到尚未获得欧盟充分性决定、保护水平尚不充分的第三国时,标准合同条款包含了在特定情形下所欠缺的数据保护的基本要素,由此起到了弥补特定第三国数据保护水平不足的功能。④

以合同义务"补强"域外国家数据保护水平之不足,亦符合数据跨境传输中欧盟个人数据保护标准的目标。若数据处理者位于欧盟境外,数据国际传输的合同构造更复杂,当合同涉及第三国数据流时,由于第三国数据接收方并不受到(欧盟的)能够提供充分数据保护水平的、可执行的数据保护规则的法律约束,就必须通过合同机制,来

① Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.02.2010, pp.5-18; Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 28.

② Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 22.

③ Thomas Zerdick, in Eugen Ehmann und Martin Selmayer (Hrsg.), *Datenschutz-Grundordnung Kommentar*, 2. Aufl., 2018, Art. 46 Rn. 11; European Commission, "Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive," DG XV D/5025/98, WP 12, 24.07.1998, p.18.

④ European Commission, "Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive," p. 16.

为数据主体提供额外的保护措施。[①] 现行条款确立了数据出口方的诸多义务,包括数据保护的保障义务(第 8 条)、次级处理者的使用(第 9 条)、数据主体权利(第 10 条)、补救措施(第 11 条)、责任(第 12 条)及监管(第 13 条)。同时,在当地法律和公共当局访问(数据时的)引入数据进口方的义务,即公共当局访问(数据时)的数据进口方的义务(第 15 条)(包括通知义务、审查义务),通过合同义务的标准化,将欧盟的个人数据保护标准以合同形式拘束当事人,并通过禁止变更规定保证欧盟个人数据保护标准的一体适用。

2. 以合同条款"固定"欧盟个人数据保护标准

标准数据保护条款实质上是一种通过标准条款"固定"欧盟个人数据保护标准的一种法律工具。在适用机制上,标准数据保护条款禁止内容变更,必须整体适用。标准数据保护条款本身是一种软法,作为示范条款,本身并无法律拘束力,仅在合同当事人采纳示范条款并将之纳入当事人缔结的数据传输合同之中时才产生拘束力。但是,根据《欧盟运行条约》第 288 条第 4 款,欧委会做出的决定在整体上具有法律约束力,可拘束成员国,成员国的国家监管机构有义务在合同中接受欧委会通过的标准条款。根据 GDPR 第 46 条第 2 款第 c 项和第 d 项,如果标准数据保护条款在内容上完整使用且未做任何更改,就无须获得数据保护监管机构的批准便可以进行数据传输。由于欧委会明确承认的标准数据保护条款是向第三国传输数据的适当保证,因此,内容完整且未更改的标准数据保护条款一般无须审批。[②] 从法律确定性的角度而言,相较于一对一的个别合同解决方案和 BCR 机制,标准数据保护条款提供了一种相对简单、合法、安全的选择,以满足将个人数据传输到境外的 GDPR 的额外法律要求,具有法律确定性的显著优势。[③] 个别的合同方案仅在获得主管监管机构授权的前提下才能使用,BCR 需要个别批准(GDPR 第 46 条第 3 款第 a 项和第 b 项)。在这两种审批程序中,主管监管机构都需要进行复杂、耗时的一致性机制(GDPR 第 46 条第 4 款、第 47 条第 1 款、第 63 条以下),而标准数据保护条款按法定程序产生,无须监管机构进一步审批。[④] 但这也意味着,欧委会通过标准合同的条款内容"固定"了欧盟个人数据保护标准,并借助禁止变更的整体适用机制,保证商事主体在个别适用中也能统一践行欧盟的个人数据保护标准。

---

① European Commission, "Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive," p. 23.

② Markus Lang, in Flemming Moos (Hrsg.), *Datenschutz und Datennutzung*, ottoschmidt, 2021, S.861.

③ Ibid.

④ Ibid.

三 司法推动:数据跨境传输工具的效力审查

单凭规则建构并不足以持续保障欧盟个人数据保护标准的贯彻,值得注意的是,欧洲法院通过司法审查制度,确立了对数据跨境传输的持续监管。欧盟司法监管的特点在于:其一,欧洲法院司法审查本属欧盟权限范畴,但司法审查的对象是域外国家的数据保护水平;其二,GDPR 法源结构的独特性为"基本权利保护"奠定了规范基础。GDPR 是一种派生性立法,应遵守欧盟基础性立法的位阶高于派生性立法的基本原则。相应地,欧洲法院在司法审查中,基础性法源主要是《欧盟基本权利宪章》中私人生活和家庭受到尊重的权利(第 7 条)和个人数据保护权利(第 8 条),派生性法源以 GDPR 为主。在双层法源结构下,但凡涉及数据跨境传输中的数据保护,就会在法律基础上与《欧盟基本权利宪章》联动,欧盟的基本权利保护价值观由此融入欧洲法院司法审查。

本文从类案和个案两个维度,观察欧洲法院对欧盟个人数据保护标准的司法推进。就类案而言,从 2003 年到 2019 年,欧洲法院确立了欧盟法扩张解释的基本立场,在 2015 年 Schrems I 案后,聚焦司法审查,使效力审查机制逐步形成。在个案上,2020 年 Schrems II 案具有突破意义,确立了欧洲法院的个案实质审查机制,司法审查"升级"为对第三国数据保护水平的实质监管,欧洲法院成为全球数据流动的"新权威"。

(一)类案形成"效力审查"机制

在集中进行效力审查之前,欧洲法院就已通过扩张解释夯实了司法监管的基本立场。欧洲法院在数据跨境传输案件的先予裁决中采取扩张解释立场,践行欧盟扩大数据保护立法实质管辖范围的立法政策。例如,在出现专门的数据跨境传输案件之前,欧洲法院就在涉及《数据保护指令》概念解释的案件中屡屡表达扩张解释欧盟数据保护法律的基本立场。在 2009 年 Rijkeboer 案和 2017 年 Nowak 案中,法院对"个人数据"概念采取扩张解释;在 2014 年 Google Spain and Google 案,法院对"处理"和"个人数据处理"概念采取扩张解释;在 2018 年 Jehovan todistajat 案和 2019 年 Buivids 案中,法院对"控制者"和"个人数据处理"仍采取扩张解释。① 扩张解释的基本立场,为后

① C-553/07-Rijkeboer, College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, Judgment of 07.05.2009; C-582/14-Breyer, Patrick Breyer v Bundesrepublik Deutschland, Judgment of 19.10.2016; C-131/12-Google Spain and Google, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgment of 13.05.2014; C-25/17-Jehovan todistajat, Judgment of 10 July 2018; C-345/17-Buivids, Judgment of 14.02.2019.

续数据传输案件的审判确立了基本思路。

在数据跨境传输案件中,欧洲法院的首要判例当属 2003 年涉及“向第三国传输数据”概念解释的 Lindqvist 案。这一判例的意义在于,GDPR 的数据跨境传输规范体系源于《数据保护指令》,因此,指令第 25 条第 6 款的“向第三国传输数据”概念,构成了 GDPR 相关概念的解释基点。该案所涉问题为,在网站上传个人数据致使第三国人员访问时,是否构成《数据保护指令》第 25 条的“向第三国传输数据”。欧洲法院认为,指令第四章未就“使用互联网”确立标准,鉴于立法时的互联网发展状况,无法假定立法者想要将“数据加载到网页”的情形纳入“向第三国传输数据”的概念之下,即便该数据会因此被具有技术手段的第三国人员访问。因此,成员国公民将个人数据上传到该成员国或另一成员国的主机服务提供商的网站,致使连接到互联网的包括第三国在内的所有人都可访问数据时,不构成“向第三国传输数据”。① 在 Lindqvist 案后的十余年间,欧洲法院在法律解释的路径上一以贯之,以扩张解释为主导,通过法律解释来明确和补充欧盟的数据保护立法。

但自 2015 年以来,数据跨境传输领域的司法裁判重心转变,以 Schrems I 案②和《航班乘客个人信息记录数据(PNR)协议》案③(《PNR 协议》案)为代表,欧盟进入司法审查时代,通过一系列“名”为法律解释、“实”为司法审查的经典判例,欧洲法院聚焦于被解释对象的法律效力,《欧盟基本权利宪章》成为司法审查的新基准。司法审查不仅成为欧盟法律文件效力审查的常用机制,而且不断产生“外溢”效应,成为欧盟跨境传输范式扩张的新工具。

例如,在 2015 年的 Schrems I 案中,成员国法院提请欧洲法院就《数据保护指令》第 25 条第 6 款的“充分性认定”概念进行解释,并提请审查美欧《安全港决定》④的效力。欧洲法院对“充分性认定”采取实质解释,判定《安全港决定》无效。欧洲法院认为,安全港原则仅适用于从欧盟接收个人数据的自我认证的美国组织,美国公共当局无须遵守安全港原则,《安全港决定》第 1 条不符合《数据保护指令》第 25 条第 6 款和《欧盟基本权利宪章》的要求,因此无效。⑤《安全港决定》第 3 条因剥夺成员国监管机构基于指令第 28 条所享有的监督权而陷于无效,并且,因第 1 条和第 3 条无效,导

① C-101/01-Lindqvist, Judgment of 06.11.2003, paras.63-64, para.68, 71.

② C-362/14-Schrems, Maximillian Schrems v Data Protection Commissioner, Judgment of 06.10.2015.

③ Avis 1/15-Accord PNR UE-Canada, Opinion of the Court of 26.07.2017.

④ Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, OJ L 215, 25.08.2000, pp.7-47.

⑤ C-362/14-Schrems, Maximillian Schrems v Data Protection Commissioner, Judgment of 06.10.2015, para.82, paras.87-89, 96-98.

致《安全港决定》整体无效。①

又如,在 2017 年的《PNR 协议》案中,案件涉及欧盟和加拿大的国际协议草案《航班乘客个人信息记录数据(PNR)共享协议》是否符合《欧盟基本权利宪章》。欧洲法院认为,协议允许将所有乘客 PNR 数据传输给加拿大当局以供其使用、保留,并可能后续传输给其他当局或第三国,无论是将 PNR 数据从欧盟传到加拿大当局,还是欧盟与加拿大就数据的保留、使用、后续传输条件达成框架协议,都构成对《欧盟基本权利宪章》第 7 条基本权利的干预,相关操作同时构成对个人数据的处理,进而构成对《欧盟基本权利宪章》第 8 条基本权利的干预,欧洲法院发布第 1/15 号意见,裁定协议若干条款不符合欧盟认可的基本权利,禁止以现行形式缔结协议。②

效力审查由此成为欧洲法院“新宠”。先予裁决的重心从解释欧盟法,转向审查被解释对象的法律效力,先予裁决的法律基础也发生转变,判决依据不再局限于GDPR或《数据保护指令》等派生性立法,而是贯穿至以《欧盟基本权利宪章》为代表的基础性立法。

(二)个案确立“实质等同”标准

欧洲法院司法审查的诡谲之处在于:针对个案的效力审查的影响远超个案本身。后 GDPR 时代,数据传输规则的解释与适用案件频出,欧洲法院通过司法审查机制,成为全球数据流动监管的“新权威”。尤其是在 2020 年的 Schrems II 案中,欧洲法院确立了跨境数据传输的个案实质审查机制,通过“升级版”的司法审查,司法审查的“长臂”“名正言顺”地触及诸如评估第三国数据保护法律水平、实质审查第三国法律是否符合欧盟基本权利保护水准等超国家事项,实质是欧洲法院对数据保护标准的司法监管。

1. 案件事实③与判决要旨

2020 年的 Schrems II 案是 2015 年 Schrems I 案的延续和升级。原告奥地利公民施雷姆斯(Maximillian Schrems)自 2008 年以来使用脸书(Facebook),脸书总公司注册于美国,欧盟用户须与脸书爱尔兰公司缔约,后者将用户的部分或全部个人数据传输到脸书的美国服务器并进行处理。2013 年,施雷姆斯向爱尔兰数据保护专员申诉称,美国法律无法充分保证存储在美国的个人数据免受当地当局的监视活动,要求禁止爱

① C-362/14-Schrems, Maximillian Schrems v Data Protection Commissioner, Judgment of 06.10.2015, paras. 105-106.

② Avis 1/15-Accord PNR UE-Canada, Opinion of the Court of 26.07.2017, paras.125-126, para.165, 232.

③ C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, paras.50-68.

尔兰公司将其个人数据传至美国。申诉被驳回,理由是欧委会《安全港决定》[①]认定安全港机制能够确保美国提供充分数据保护水平。2015 年,欧洲法院在 Schrems I 判决认定《安全港决定》无效。[②] 随后,爱尔兰高等法院将施雷姆斯的申诉转回数据保护专员,脸书爱尔兰公司在数据保护专员的调查中解释称,个人数据是根据欧委会《个人数据传输的标准合同条款决定》(《标准合同条款决定》)[③]的标准条款传到美国,数据保护专员要求施雷姆斯重新申诉。2015 年,施雷姆斯申诉称,依美国法律,脸书美国公司必须将用户数据传输给国家安全局(NSA)、联邦调查局(FBI)等当局,美国当局的监控计划对施雷姆斯个人数据的处理,违反了《欧盟基本权利宪章》,《标准合同条款决定》也无法为数据传输提供正当性,施雷姆斯请求数据保护专员禁止或暂停将其个人数据传输到脸书美国公司。基于 Schrems I 判例,数据保护专员于 2016 年向爱尔兰高等法院起诉,法院于 2018 年向欧洲法院申请先予裁决。爱尔兰高等法院提供了一份 2017 年判决副本,证实美国当局依据《外国情报监控法案》第 702 条和《第 12333 号行政命令》对传输到美国的个人数据进行情报活动,允许司法部长和中情局局长对美国境外的非美国公民进行个人监视,以获取外国情报信息,尤其是为棱镜(PRISM)和上游(UPSTREAM)监视计划提供依据。在上游监视计划中,互联网服务提供商必须向 NSA 提供选定目标的所有通信,并将某些通信信息传输给联邦调查局和中情局,提供电缆、交换机、路由器等互联网骨干网的电信运营商必须允许 NSA 复制、过滤网络流量,以获取相关通信信息,NSA 可以访问相关通信的元数据和通信内容。《第 12333 号行政命令》允许 NSA 通过大西洋海底电缆访问传输到美国的数据,并在其到达美国前依据《外国情报监控法案》收集和保留数据。爱尔兰高等法院认为,美国对个人数据进行了大规模处理,却未实质上确保数据保护水平与《欧盟基本权利宪章》第 7 条和第 8 条的水平相当;美国当局处理个人数据时,欧盟公民无法享受与美国公民相同的救济措施,《美国宪法第四修正案》作为美国法对抗非法监视的最重要法律依据不适用于欧盟公民,欧盟公民起诉障碍重重;NSA 基于《第 12333 号行政命令》进行的活动不受司法管辖,美国隐私专员不属于《欧盟基本权利宪章》第 47 条意义上的

① Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, OJ L 215, 25.08.2000, pp.7-47.

② C-362/14-Schrems, Maximillian Schrems v Data Protection Commissioner, Judgment of 06.10.2015.

③ Commission Decision 2010/87/EU of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal data to Processors Established in Third Countries under Directive 95/46/EU of the European Parliament and of the Council, as Amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016, OJ L 39, 12.02.2010, pp.5-18.

法庭,美国法律未向欧盟公民提供与《欧盟基本权利宪章》实质相同的保护水平。因此,爱尔兰高等法院就案件能否适用欧盟法、标准合同条款有效性、隐私盾决定的有效性等十一项问题提请欧洲法院进行先予裁决。

在 Schrems II 案中,欧洲法院特别强调尊重私人生活的权利、保护个人数据的权利和获得有效法律救济和公平审判的权利(《欧盟基本权利宪章》第 7 条、第 8 条、第 47 条),就四项问题裁决如下。①

其一,确认 GDPR 长臂管辖。欧洲法院将 GDPR 第 2 条第 1 款和第 2 款解释为,在欧盟成员国设立的公司出于商业目的将个人数据传输到第三国设立的另一公司时,无论在数据传输之时或传输之后存在第三国当局基于公共安全、国防和国家安全目的处理个人数据的可能性,数据跨境传输应适用 GDPR。

其二,确立实质等同审查标准。欧洲法院将 GDPR 第 46 条第 1 款和第 46 条第 2 款第 c 项解释为:"适当保障"和"可执行的(数据主体)权利和有效法律救济"必须确保,基于标准合同条款传输到第三国的个人数据所获得的保护水平,应与在欧盟基于 GDPR 和《欧盟基本权利宪章》确保的保护水平实质等同(essentially equivalent)。在评估数据保护水平时,必须特别考量两类因素:(1)设立在欧盟的数据处理者、控制者与第三国的接收方之间订立的合同条款;(2)第三国当局访问个人数据的法律体系因素,尤其是 GDPR 第 45 条第 2 款非穷尽列举的因素。

其三,主管监管机关负有暂停或终止数据传输的义务。法院将 GDPR 第 58 条第 2 款第 f 项和第 j 项解释为:在不存在欧委会充分性决定时,若监管机构认为第三国无法遵守标准合同条款,并且无法通过其他手段为传输数据提供与欧盟水准相当的充分保障时;若欧盟的数据控制者或传输者未能主动暂停或终止数据传输,监管机构有义务暂停或禁止将数据依据标准合同条款传到第三国,监管机构可以通过临时性或确定性限制的方式,例如颁发数据处理禁令,暂停或禁止数据传输行为。换言之,若企业未能自行阻却数据传输,监管机构有权禁止数据传输。②

其四,判定《标准合同条款决定》有效,《隐私盾决定》无效。法院认定,《标准合同条款决定》未违反《欧盟基本权利宪章》第 7 条、第 8 条和第 47 条,有效性不受影响,

① EuGH, "Übermittlung personenbezogener Daten von Facebook Ireland in die USA - Schrems II," *NJW*, 2020, S.2613ff, Rn. 149, 199.

② C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, para.113.

《欧委会关于美欧隐私盾的充分性决定》(《隐私盾决定》)①无效。

2. 实质审查第三国数据保护水平

Schrems II 案判决《隐私盾决定》无效,释放出欧洲法院审查第三国数据保护水平的全面实质审查信号。事实上,在美欧 2015 年《安全港决定》因 Schrems I 案陷于非法后,美欧就数据保护达成了新的《隐私盾决定》,欧委会在《隐私盾决定》第 1 条第 1 款评估得出,美国能够确保通过隐私盾协议传输到美国的欧盟个人数据达到充分保护水平,允许企业基于特定保护措施将个人数据从欧盟传输到美国。② 在性质上,隐私盾是欧委会针对特定行业的数据传输对相应美国企业做出的一种"充分性认定",但实践中存在主权国家干预、访问欧盟个人数据的可能风险,经由 Schremes II 案,欧洲法院再次将之上升为政治问题。③

首先,《隐私盾决定》无效的原因在于其未能提供有效数据保护。欧洲法院判定《隐私盾决定》违反比例原则、违反《欧盟基本权利宪章》和缺乏有效法律救济。具体而言,其一,违反比例原则。欧洲法院认为,对欧盟公民基本权利的干预不都会违反《欧盟基本权利宪章》,但美国法律规定未能充分准确地规定美国当局采取措施的前提和范围,法律规则具有一般性和模糊性,不符合欧盟法的比例原则,对基本权利的干预并无充分限制。④ 其二,违反《欧盟基本权利宪章》。欧洲法院认为,若将《欧盟基本权利宪章》视为 GDPR 国际适用的标准,那么美国法律在隐私领域全然不符合欧盟保护标准,如果美国企业侵犯欧盟公民隐私,受害人应有权起诉,欧盟公民缺乏有效的法律保护工具来就美国当局的监控措施采取行动并行使权利,尤其缺乏独立的法院审判,构成对《欧盟基本权利宪章》第 7 条、第 8 条和第 47 条的违反。⑤ 其三,缺乏"可强制执行的(数据主体)权利和有效法律救济"(GDPR 第 45 条第 2 款)。欧洲法院对美国数据保护专员有无足够权限来有效维护欧盟公民合法权益提出质疑,尽管《隐私盾决定》试图通过在美国设立数据保护专员为欧洲数据提供有效保障,但美国监视法律影响过大,隐私盾的保护对于欧盟公民而言不够充分,监控程序不能确保监控仅限于

① Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, OJ L 207, 01.08.2016, pp.1-112.

② EuGH, "EU-US-Datenschutzschild ungültig - Schrems II," *MMR*, 2020, S.597.

③ Alexander Golland, "Datenschutzrechtliche Anforderungen an internationale Datentransfers," *NJW*, 2020, S. 2593.

④ EuGH, "EU-US-Datenschutzschild ungültig - Schrems II," S.597.

⑤ C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, paras.176-178, para.199; Alexander Golland, "Datenschutzrechtliche Anforderungen an internationale Datentransfers," S.2593; EuGH, "EU-US-Datenschutzschild ungültig - Schrems II," S. 597.

选定目标,对个人数据的收集缺乏适当限制。①

其次,《标准合同条款决定》的有效性需以实践中始终保持“适当数据保护水平”为前提,欧盟公司和接收数据的第三国公司应审查个案中是否维持了充分的数据保护水平。② 而“适当数据保护水平”之存续,须以(1)存在诸如标准合同条款的适当保障措施,和(2)在实践中保障“可执行的(数据主体)权利和有效法律救济”为前提。③ 因此,数据进出口方仅订立标准合同条款仍不充分,数据出口方的义务更在于审查个案中依据标准条款是否切实充分保障数据保护。④ 因此,欧洲法院立场明确,数据国际传输原则上允许使用标准数据保护条款,但若数据出口方未做个案研判或未能保证提供与欧盟同等的数据保护水平,数据传输仍可能无效。

Schrems II 案可能引发产生蝴蝶效应。以瑞士和英国为例,瑞士和美国之间的隐私盾在很大程度上与美欧隐私盾相似,Schrems II 案是否会导致瑞士和美国之间的隐私盾无效?若瑞士维持隐私盾决定,又会对瑞士数据保护法的充分性评估有何影响?英国能否创设与隐私盾功能类似的数据传输工具?⑤ 由此看来,所涉国家现有数据跨境传输法律安排的不确定性大幅增加。

(三)穿透式监管

欧洲法院对欧委会《隐私盾决定》和《标准合同条款决定》的司法审查,要求域外法律必须在实质上符合欧盟的基本权利保护标准,是一种穿透式监管。穿透式监管意味着,商事主体在适用标准数据保护条款之后,仍受欧盟法院监管,条款仍可能被判无效。欧盟通过对欧委会《标准数据保护条款决定》的司法审查,实现了对标准数据条款的效力控制。尽管标准数据保护条款仅约束缔约当事人,对第三国政府当局并无拘束力,但条款以欧委会通过《标准数据保护条款决定》的形式发布,而这种欧委会决定的效力,取决于合同条款是否包含有效机制,在实践中能否确保缔约方遵守欧盟法要

① EuGH, “EU-US-Datenschutzschild ungültig - Schrems II,” S.597.

② C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, paras.126, 149; EuGH, “Datenschutzrecht: Übermittlung personenbezogener Daten von Facebook Ireland in die USA - Privacy Shield,” S.941; Alexander Golland, “Datenschutzrechtliche Anforderungen an internationale Datentransfers,” S.2593.

③ C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, para.91; Alexander Golland, “Datenschutzrechtliche Anforderungen an internationale Datentransfers,” S.2593.

④ C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, para.134; Alexander Golland, “Datenschutzrechtliche Anforderungen an internationale Datentransfers,” S.2593.

⑤ EuGH, “EU-US-Datenschutzschild ungültig - Schrems II,” S.597.

求的保护水平,以及在违反合同条款或无法履行合同条款时能否暂停或禁止数据传输。① 在 Schrems II 判决中,欧洲法院强调,欧委会通过的标准数据保护条款应仅发挥合同保障功能,其唯一宗旨是为欧盟的数据控制者和处理者提供统一适用于在第三国的合同保障,原则上使各缔约方能在此基础上保证各方之间的数据保护水平,但条款与第三国本身的数据保护水平无关,审查或确保(条款涉及的)第三国的数据保护水平的充分性问题,恰恰不是欧委会的任务所在。② 换言之,只要未被欧洲法院判定无效,《标准数据保护条款决定》就能够拘束监管机构,当第三国无法遵守标准合同条款或无法保障对数据的充分保护时,监管机构必须暂停或终止基于标准合同条款向第三国传输个人数据(GDPR 第 58 条第 2 款第 f 项和第 j 项)。③ 不仅如此,根据Schrems II 判决,数据接收方负有采取补充措施的义务,以达到与欧盟实质等同的数据保护水平。在 Schrems II 判决后,如果商事主体选择以标准数据保护条款的形式传输数据,就需进行个案审查,例如通过向数据接收者发送调查问卷的形式来审查,了解是否存在第三国当局干预的可能性。④ 2021 年 6 月 18 日,欧盟数据保护委员会发布《数据跨境传输的补充措施建议》⑤,为数据跨境传输提供了实践参考标准,例如,以问责制的方式应用于数据跨境传输,包括了解传输对象、核实采用的传输工具、根据 GDPR 第 46 条评估传输工具、确定并采取补充措施等六个步骤。在欧洲法院 Schrems II 案判决前,标准数据保护条款的价值在于效率性和安定性,但 Schrems II 判决后,在欧洲法院"实质等同"的司法审查之下,通过标准数据保护条款把个人数据传输到无法提供充分数据保护水平的第三国时,标准条款仍可能被判无效。

穿透式监管的风险也体现在其他的替代性传输工具上。例如,BCR 也基于合同产生,不拘束政府机构,如果商事主体使用 BCR 机制,也需个案审查,根据欧洲法院判决,BCR 的有效性判断和标准数据保护条款类似,需要进行实质审查,这意味着,如果

① Kristina Schreiber, "EU-U.S.-Privacy Shield ungültig, Standardvertragsklauseln zu prüfen," S.379; Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 12c; C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, paras.136-137.

② Boris P. Paal und Daniel A. Pauly (Hrsg.), *Datenschutz-Grundordnung*, Art. 45 Rn. 12c; C-311/18-Facebook Ireland and Schrems, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Judgment of 16.07.2020, para.133.

③ Kristina Schreiber, "EU-U.S.-Privacy Shield ungültig, Standardvertragsklauseln zu prüfen," S.379.

④ Ibid.

⑤ European Data Protection Board, Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU level of Protection of Personal Data, Version 2.0, 18.06.2021.

标准数据保护条款无效,那么此种情形下也不应考虑 BCR 机制。① 欧洲法院对第三国数据保护水平的“实质等同”司法审查,使欧盟数据跨境传输规则的法律效力的安定性受到较大挑战。

穿透式监管的真正危险在于:欧洲法院在有关标准合同条款的论证中表明,只有数据出口方在个案中确保第三国法律状况具备充分数据保护水平时,GDPR 所要求的“适当保障”方得满足,否则就需补充标准合同条款内容。换言之,即便欧盟标准合同条款原则有效,数据进出口方仍需审查个案中是否维持了适当的数据保护水平。② 这意味着,如果数据进口方所在国家无法提供充分数据保护水平,也无法通过标准合同条款提供充分保障,企业就无法将数据传输到第三国。无论是《隐私盾决定》还是《标准合同条款决定》,只要不符合欧盟个人数据保护的基本权利保护要求,都可能陷入无效,这意味着全球企业始终处于欧盟司法审查的达摩克利斯之剑下。③

四 范式扩张:欧盟个人数据保护标准的风险与展望

谁制定了标准,谁就掌控了市场。数据保护标准的立法竞争,实质是数字市场的全球竞争。然而,欧盟在全球数字经济中的市场份额与其在数据立法领域的“欧洲中心主义”毫不匹配。联合国《2019 年数字经济报告》显示,中美引领全球数字经济,占据全球七十个最大数字平台市值的 90%,欧洲份额仅为 4%。④ 虽然欧盟的数字经济规模滞后,但其通过法律领域的传统优势,以立法影响数字市场发展,一跃成为全球数字立法的引领者。欧盟通过 GDPR 和《非个人数据欧盟境内自由流动条例》完成了个人数据和非个人数据的全类型数据流动立法。在将 GDPR 模式成功推向全球后,欧盟数据立法全面开花:从 2018 年《网络安全条例(草案)》到 2020 年《数字服务法案(草案)》和《数字市场法案(草案)》,直至 2021 年《数据库条例(草案)》和《人工智能条例(草案)》,欧盟通过统一的条例立法(regulation),涵盖数字服务、数字市场、人工智能、网络安全等众多主题,全领域、多类型的欧盟数据法律体系初现轮廓,数据立法的欧洲

① Kristina Schreiber, “EU-U.S.-Privacy Shield ungültig, Standardvertragsklauseln zu prüfen,” S.379; European Data Protection Board, FAQ on the Judgment of the ECJ in Case C-311/18, p.3; Datenschutzkonferenz, Pressemitteilung, 28.07.2020, 1f.

② EuGH, “Datenschutzrecht: Übermittlung personenbezogener Daten von Facebook Ireland in die USA - Privacy Shield,” S.941.

③ Alexander Golland, “Datenschutzrechtliche Anforderungen an internationale Datentransfers,” S. 2596.

④ https://unctad.org/system/files/official-document/der2019_en.pdf.

模式初具规模。①

不容否认的是,在全球层面,欧盟数据立法模式呈现出扩张态势。无论是巴西《通用数据保护法》,还是印度《2019 年个人数据保护法案(草案)》,乃至《东盟跨境数据流动示范合同条款》,都不同程度地借鉴了 GDPR 模式及其数据跨境传输规则。②但正如美国学者纽曼(Abraham Newman)所言,欧盟的"政策出口"成功地向其他国家输出欧盟规则,欧盟的"充分性认定"成为其他国家政治参与者推动国内立法改革的重要工具,推动了其他国家的隐私保护立法,但是,当各国法律传统和民族价值观差异巨大时,欧盟不能强迫其他国家改变立法。③

欧盟数据立法模式的潜在风险在于:其个人数据保护标准以基本权利保护作为价值根基,以欧洲法院的"宪法审查"式司法审查作为终极监管工具。这对于法律移植而言,是一个颇值思量的问题。近年来,中国学者对于数据立法借鉴 GDPR 模式多有反思,但对法律移植的风险尚未达成共识。《个人信息保护法》与 GDPR 在一定程度上存在趋同。④ 例如,《个人信息保护法》专章规定个人信息跨境提供规则,引入具有

---

① European Commission, "Proposal for a Regulation of the European Parliament and of the Council Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' Meeting in Salzburg on 19-20 September 2018," COM(2018) 630 final, 12.09.2018; European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC," COM(2020) 825 final, 15.12.2020; European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), COM(2020) 842 final, 15.12.2020; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-including-the-review-of-the-Directive-96-9-EC-on-the-legal-protection-of-databases-/public-consultation_en, last accessed on 07.08.2021; 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," COM(2021) 206 final, 21.04.2021.

② 例如,巴西《通用数据保护法》第五章规定数据跨境传输,确立了与 GDPR 类似的数据传输规则,第 33 条区分"第三国或国际组织的个人数据保护水平充分性程度下的传输""具体合同条款""标准合同条款""全球性公司规则"等传输机制。印度《2019 年个人数据保护法案(草案)》第七章规定"个人数据跨境传输的限制",设置了与充分性认定类似的"向某一国家或某一国家内的某一实体或某一类别的实体或国际组织传输",引入与标准数据保护条款和 BCR 机制类似的"根据保护局批准的标准合同"和"集团内部计划"等数据跨境传输形式。《东盟跨境数据流动示范合同条款》区分(1)控制者到处理者和(2)控制者到控制者两种传输模式,规定了数据出口方义务和数据进口方义务。

③ 自 1999 年起,借助欧盟扩张过程中的结对程序(Twinning),欧盟的国家数据保护专员向中欧国家提供立法改革建议,例如捷克、西班牙、拉脱维亚、立陶宛和马耳他,旨在通过不同国家间数据保护机构的联系以改进其监管能力。参见 Abraham Newman, "European Data Privacy Regulation on a Global Stage: Export or Experimentalism?" in Jonathan Zeitlin, ed., *Extending Experimentalist Governance? The European Union and Transnational Regulation*, Oxford University Press, 2015, pp.227-246。

④ 例如,《个人信息保护法》第 1 条受到 GDPR 第 1 条个人数据处理定义的影响,将"规范个人信息处理活动"作为立法目标,未能全面反映中国规范个人信息处理活动的立法意图。《个人信息保护法》第 4 条的个人信息处理概念遵循 GDPR 第 4 条对个人数据处理的宽泛界定,但宽泛界定和欧洲法院的扩张解释立场可能导致规范对象和适用范围的泛化,导致法律对社会干预过度。相关学理反思,参见高富平:《个人信息处理:我国个人信息保护法的规范对象》,载《法商研究》,2021 年第 2 期,第 73 页;高富平:《论个人信息保护的目的——以个人信息保护法益区分为核心》,载《法商研究》,2019 年第 1 期,第 93 页;许可:《数字经济视野中的欧盟〈一般数据保护条例〉》,载《财经法学》,2018 年第 6 期,第 71 页。

欧盟特色的“标准合同”规则(第 38 条第 1 款第 3 项),要求“境外接收方处理个人信息的活动达到中国的个人信息保护标准”(第 38 条第 3 款),确立了特定数据跨境传输的安全评估制度(第 40 条)。《个人信息保护法》第 55 条和相应的国家标准(例如《信息安全技术个人信息安全影响评估指南》GB/T 39335-2020;《信息安全技术 个人信息安全规范》GB/T 35273-2020)不同程度地借鉴了 GDPR 的风险规制模式,个人信息保护影响评估受到 GDPR 模式的风险规制影响。但若将个人信息保护标准作为衡量出境数据的核心基准,或将落入欧洲法院实质审查中国数据保护水平的“长臂管辖”陷阱,开启欧盟司法审查基本权利保护的“潘多拉魔盒”。更深层的问题在于,GDPR 所代表的欧盟数据立法模式将基本权利保护视为个人数据流动的价值根基,欧盟层面的司法审查更趋近于基本权利保护的“宪法审查”。欧盟在充分性认定和标准数据保护条款中嵌入欧洲法院“宪法审查”机制,这对于无宪法审查传统或者违宪审查制度不发达的国家而言,若与欧盟达成充分性认定或适用其标准数据保护条款,就可能存在法律趋同的制度障碍。中国的法律传统、法律体系和司法结构与欧盟不同,数据立法仍处于部门法、单行法逐步完善的建构阶段。无论是《数据安全法》《网络安全法》和《个人信息保护法》,还是未来个人信息保护的具体规则和标准合同制定,数据立法都存在借鉴欧盟制度的可能性,但若依循法律移植欧陆成文法的历史惯性,有意识或不自觉地盲目接受、移植欧洲规则,就可能存在风险。类似欧洲法院式的司法审查并不契合中国法律体系和法律传统。

中国是数据资源超级大国,绝非数据保护“洼地”,寻找本土规则,确立中国模式,应为数据立法的题中之义。立法者宜审慎评估和研判欧盟数据保护立法模式的潜在风险,谨慎对待充分性决定、标准数据保护条款、个人数据保护标准等富有欧盟特色的复杂法律工具。GDPR 代表的欧洲模式并非最佳立法方案,具有域外扩张和基本权利评价功能的欧盟个人数据保护标准并非中国数据流动的最优基准。中国数据流动立法应关注本土数据的流出控制,既要全盘统筹,在聚焦个人信息保护的同时关注非个人数据的流动方案,又要避免陷入个人数据保护的标准竞争,防止出现个人数据保护标准的竞次现象,还应积极探索并建构价值中立、适宜法律趋同的法律工具。建构数据流动法律的中国方案,任重而道远。

(**作者简介**:金晶,中国政法大学民商经济法学院民法研究所副教授;**责任编辑**:张海洋)