发展中国家因应GDPR数据跨境传输规则的困境与启示
——以印度为例

李　菡*

内容摘要：欧盟《通用数据保护条例》利用充分性决定及适当保障措施构建了全面立体的欧盟数据跨境传输规则体系，统一了欧盟成员国向第三国传输个人数据的标准与条件。许多国家已经实施或考虑实施此类要求以促进与欧盟国家的数据依赖型贸易的发展。在数据时代，为缓解数字强国与欠发达国家间数字鸿沟的进一步扩大，关注发展中国家在数据传输方面面临的困境至关重要。印度作为发展中国家新兴经济体代表，在因应GDPR时面临着独特的挑战，其应对之策为其他发展中国家提供了数字规则谈判方面的启示。

关键词：发展中国家　GDPR　数据跨境传输　充分性决定　贸易纪律

一、问题的提出

《通用数据保护条例》（General Data Protection Regulation, GDPR）是欧盟（European Union，EU）颁布的关于欧盟和欧洲经济区（European Economic Area，EEA）个人信息隐私保护的一项法规，于2018年5月25日正式生效，取代1995年《数据保护指令》（Digital Protection Directive，DPD）成为欧盟隐私法和人权法的重要组成部分。GDPR所构建的个人隐私保护体系对域外国家的立法活动产生了显著影响，即导致了由欧盟内部数据隐私法律诱发国际范围内的立法趋同化现象。[①]GDPR的效力扩张，体现为对欧盟与欧洲经济区以外的个人数据传输的管辖扩张以及利用数据跨境传输工具进行规则的实际影响力扩张，并可能最终引发“布鲁塞尔效应”致使各国立法趋同。

作为发展中国家新兴经济体代表，印度在欧洲国际数字贸易中扮演着不可忽视的角色。2023年，欧盟成为印度第二大IT及IT相关产品的出口目的地，仅次于美国

*　英国格拉斯哥大学国际经济法博士研究生。

①　参见冯玉军、卫洪光：《GDPR的“布鲁塞尔效应”理论及批判——对立法域外影响力的分析》，《烟台大学学报（哲学社会科学版）》2023年第6期，第24页。

(占出口总额的55.5%)。[①]在印欧贸易关系中,印度向欧盟出口大量的依赖个人数据跨境传输的服务贸易,因此互联网建设和数据自由流动是促进印度服务出口日益重要的驱动力。个人隐私保护是数据跨境流动中最重要的议题之一,在印欧数据传输日益频繁的贸易交往中,GDPR作为目前全球最为全面的个人数据保护法律框架,将对印度个人数据保护法律体系产生深刻而广泛的影响。面对GDPR个人隐私保护的高要求,印度面临着对内调整国内法律制度与对外因应欧盟个人数据保护标准和条件的双重挑战。对于调整国内法律制度而言,印度《个人数据保护法案(2023)》(The Digital Personal Data Protection Bill 2023,DPDP)予以批准的迂回道路已展现出发展中国家仿效GDPR规则设计,进行法律移植所面临的巨大挑战;而在与GDPR数据跨境传输规则的对接中,充分性决定以及其他替代性机制的标准与要求可能与印度本国利益以及制度冲突。面对数字发展需求与单边立法影响力扩张的双重压力,发展中国家必须关注"如何在维护本国利益的前提下,构建国内个人数据保护法律体系以及基于本国贸易需求因应他国或区域数据传输规则"这一问题,从而确保个人信息保护与数字经济发展的相互促进。为回答这一问题,本文首先研究GDPR规则效力向他国扩张的基本原理,其次分析印度应对GDPR域外适用效力的策略及困境,最后探讨对其他发展中国家的启示。

二、扩张之势:GDPR数据跨境传输工具的使用

域外管辖的确立是GDPR效力扩张的前提条件。GDPR第3条领土范围规则(territory scope)全面规定了效力辐射的地域范围,确定了GDPR的域外适用效力。有学者将领土范围规则的逻辑形象地描述为:如果你以欧盟数据主体为目标,那么该法规就会向你伸出援手。[②]GDPR通过该规则绘制出域外管辖的蓝图,使其具备了产生全球影响的基础条件。然而,实现GDPR效力扩张的现实保障是适用于向非欧盟成员国或国际组织传输数据的一套精心设计的工具。最主要的数据跨境传输工具就是对数据目的国有关隐私保护法律体系的充分性决定(adequacy decision)[③]。在缺乏充分性决定的情况下,GDPR允许使用各种保障措施以监管欧盟作为数据出口方的数据跨境传输活动,其中包括约束性企业规则(binding corporate rules,BCRs)、标准合同条款(standard contractual clauses,SCCs)、行为准则(codes of conduct,CoC)以及认证机制(certification)。

---

① See Radhika Rao, India's Share in Global Computer Services Exports Jumps to 11% in FY23: Analysis, https://economictimes.indiatimes.com/news/economy/foreign-trade/indias-share-in-global-computer-services-exports-jumps-to-11-in-fy23-analysis/articleshow/99564838.cms, visited on 18 December 2023.

② See De Hert Paul & Michal Czerniawski, Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context, 6 International Data Privacy Law 242 (2016).

③ See GDPR, Article 45.

（一）充分性决定

充分性决定是欧盟数据跨境传输工具的主体部分。根据GDPR第45.1条的规定，充分性决定即欧盟委员会作出的、确认“第三国提供的个人数据保护水平与欧盟相当”的决定。[①]该制度是欧盟基于对个人隐私保护历史传承的战略选择，并辅之以对经济发展需求的现实考量。尽管欧盟承认隐私是国际贸易的重要组成部分，但是其将数据保护和隐私这项基本权利视为比经济激励更重要的监管依据。[②]GDPR规定了充分性保护水平的调查应当考虑的关键因素，包括法治情况[③]、第三国或国际组织所管辖的一个或多个独立监管机构的存在和有效运作情况、第三国或国际组织作出的任何国际承诺（特别是与保护个人数据有关的义务）。[④]充分性决定可以帮助欧盟有效应对数据跨境传输的安全风险。例如，GDPR增强了数据主体的权利和数据管理者的义务，并设置了对列入“白名单”国家实行定期审查的机制。充分性决定要求其他国家达到与欧盟个人数据保护“实质同等”的水平。该规定一方面弥补了数据进口国数据保护水平的不足，另一方面该数据跨境传输工具具有强制性，可实现GDPR数据立法对域外主体或行为的直接或间接适用。[⑤]具言之，数据目的国为获得欧盟的充分性决定，需要主动进行本国法制内改，使数据立法和执法达到欧盟认可的数据保护水平，以获得与欧盟进行数据传输的资格。

（二）适当保障措施

当一国未取得欧盟充分性决定时，GDPR提供了多种将个人数据传输至另一司法管辖区的机制，即有适当保障措施的转让（transfers subject to appropriate safeguards）。[⑥]这是指在没有获得充分性决定的情况下，当数据控制者或处理者提供了适当保障措施，并且具备可执行的数据主体权利和有效的法律补救措施，欧盟成员国允许将个人数据传输至第三国或国际组织。[⑦]

1.约束性企业规则

BCRs是为跨国企业量身制作的数据跨境传输工具。约束性规则必须包括所有一般数据保护原则和可强制执行的数据主体权利，以确保数据传输有适当的保障。[⑧]GDPR第47.1条规定欧盟数据保护主管机构将根据GDPR第63条规定的一致性机制

---

① See GDPR, Article 45.1.

② See Florida Y. Wang, Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement, 33 Harvard Journal of Law & Technology 668 (2019).

③ See GDPR, Article 45.2.

④ See GDPR, Article 45.2.

⑤ 参见文淑：《数据立法域外适用引发的法律冲突与中国解决方案》，《云南师范大学学报（哲学社会科学版）》2023年第6期，第100页。

⑥ See GDPR, Article 46.

⑦ See GDPR, Article 46.1.

⑧ See GDPR, Article 47.1.

批准《公司条例》。这说明BCRs旨在促进跨国公司自愿建立一个单一且复杂的规则体系(即合规框架),从而形成符合国际数据传输法律要求的成系统的条款和条件,确保欧盟个人数据在第三国得到充分保护。[①]依据GDPR第47.3条的规定,公司必须向欧盟数据保护主管机构提交具有约束力的公司规则,以供批准。主管机构将其草案传达给欧盟数据保护委员会(Europe Data Protection Board,EDPB),该委员会将对具有约束力的公司规则发表意见并确定《公司条例》,再由主管机构最终批准。尽管欧盟没有明确要求BCRs应当以GDPR为法律依据,但EDPB第29条数据保护工作组(WP29)发布的《关于BCRs要素和原则表格的工作文件》表明,BCRs应当说明与适用法律之间的关系,且如果当地立法(例如欧盟立法)要求对个人数据提供更高级别的保护,则该立法将优先于BCRs。[②]由此可见,BCRs也是GDPR预设的扩张其适用范围的数据跨境传输工具。

2.标准合同条款

SCCs是第46条规定的"适当保障措施"中最常用的保障措施且是全球商业跨境转移的主导机制。[③]2021年6月4日,欧盟委员会发布了GDPR下的现代化标准合同条款,取代DPD所采用的三套模版。SCCs允许将个人数据传输到欧盟境外的公司(不包括国际组织),前提是该公司接受欧盟委员会预先批准的标准合同条款。[④]欧盟委员会提供了四套模版条款(包括控制者到控制者、控制者到处理者、处理者到处理者以及处理者到控制者),前三种传输模式下的SCCs均规定,合同双方需要同意受欧盟成员国法律管辖。[⑤]SCCs可在数据进口方法律框架不足以保护数据主体权利的情形下适用,因可有效降低合规成本,其为中小型企业(small and medium enterprises,SMEs)理想的数据传输工具。[⑥]该机制可顺利施行的关键是,数据进口方应适用承认第三方收益权的欧盟成员国法律。[⑦]

---

① See Bianka Maksó, Binding Corporate Rules As a New Concept for Data Protection in Data Transfers. Personal Data in Competition, 28 MPI Studies on Intellectual Property and Competition Law 506 (2018).

② See WP29, Working Document Setting up a Table with the Elements and Principles to Be Found in Binding Corporate Rules, https://ec.europa.eu/newsroom/article29/items/614109, visited on 23 December 2023.

③ See Laura Bradford, *et al.*, Standard Contractual Clauses for Cross-border Transfers of Health Data after Schrems II, 8 Journal of Law and the Biosciences 10 (2021).

④ See GDPR, Article 46.2(d).

⑤ See Commission Implementing Decision (EU), 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, http://data.europa.eu/eli/dec_impl/2021/914/oj, visited on 23 December 2023.

⑥ See Angelica Fernandez, EDPB Opinion 14/2019 on Standard Contractual Clauses for Processors under Article 28 (8) GDPR, 5 Europe Data Protection Legal Review 527 (2019).

⑦ 有一个例外情况是,如果是采用处理者到处理者(P-P)模版,SCCs可以允许使用承认第三方收益权的非欧盟成员国的法律。

3.行为准则与认证机制

GDPR第40条鼓励代表控制者类别的协会或其他机构制定特定部门的行为准则，以帮助特定部门的机构遵守数据保护规则。[①]这些独立机构将有能力监督准则的遵守情况，甚至对不遵守准则的控制者进行罚款，或者向严格遵守准则的控制者颁发证书或印章。第40.2条规定了具体确保GDPR隐私标准实行的行为准则目录，包括个人数据的公平透明处理、控制者追求的合法利益等。但是由于缺乏相互认可机制和防止规范重复机制，各国企业代表可能会竞争起草各自的行为准则，产生规则异质性风险，为GDPR一致性审查带来了严峻挑战。[②]

GDPR第42条和第43条规定了欧盟数据保护框架中认证机制的设计与运作。GDPR最终认可认证制度是欧盟立法者在起草期间为在私人倡议和公共监督之间取得平衡而作出政治妥协的结果。[③]相关条文规定，在数据保护方面具有适当专业水平的认证机构，有权对数据控制者与处理者的数据保护水平进行认证、印章与标记，确认其充分的保护水平。[④]向控制者或处理者颁发的认证有效期最长为三年，可以在相同条件下续订，也可由认证机构撤回。[⑤]认证机制可以作为确定数据控制者或处理者具有约束力承诺的有效手段，并且为公众提供了一种问责工具，使组织能够向个人、与其合作的其他组织以及监管机构展示合规措施。目前，虽然GDPR引入了行为准则与认证机制，但相关规则尚未正式确立。[⑥]发展中国家还需在今后日益增长的实践中评估该机制的经济效应。

三、弥合之难：GDPR数据跨境传输规则对发展中国家的普遍影响

GDPR数据跨境传输规则为发展中国家带来了全方位的弥合挑战，这些挑战不仅触及法律适应层面，也深入到数据技术的实施操作以及数字贸易发展的实际需求。无论是充分性决定还是适当保障措施，其实质均是要求数据控制者或处理者对欧盟数据实行符合GDPR标准的保护措施。这不仅将全面保护模式的固有缺陷带给发展中国家，还将对隐私保护法规不健全、数字技术发展滞后的国家提出更加棘手的问题。[⑦]

---

① See GDPR, Article 40.1.

② See Eric Lachaud, Adhering to GDPR Codes of Conduct: A Possible Option for SMEs to GDPR Certification, 3 Journal of Data Protection & Privacy 48 (2019).

③ See Eric Lachaud, What GDPR Tells about Certification, 38 Computer Law & Security Review 2 (2020).

④ See GDPR, Article 42.1 & Article 43.1.

⑤ See GDPR, Article 42.7.

⑥ 参见李艳华：《隐私盾案后欧美数据的跨境流动监管及中国对策》，《欧洲研究》2021年第6期，第33页。

⑦ 全球普遍使用四种数据保护：全面的（comprehensive）数据保护、部门性的（sectoral）数据保护、自我监管的（self- regulatory）数据保护以及基于技术的（technology-based）数据保护。对全面的数据保护的批判主要有以下三点：（1）法规的成本可能超过收益；（2）相同程度的严格性可能不适用于所有类型数据；（3）全面的制度可能会扼杀创新。See Tiffany Curtiss, Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies, 12 Washington Journal of Law, Technology & Arts 107 (2016).

(一)法律适应

GDPR数据跨境传输规则给发展中国家带来的最主要影响是其需要构建、完善并有效执行本国数据与隐私保护相关法律,建立与GDPR同等的数据保护水平。充分性决定奠定了GDPR产生"布鲁塞尔效应"的基础,几乎形成了意与欧盟进行数字贸易的国家需要对GDPR数据跨境传输规则作出"接受或拒绝"的一刀切式抉择的局面。①

一方面,GDPR数据跨境传输规则要求发展中国家构建类GDPR数据与隐私保护框架。发展中国家需要评估现有数据与隐私保护法律是否符合GDPR要求,进行全面广泛的法律和政策审查。然而,数据与隐私保护法律框架的制定蕴含着丰富的价值考量,通常反映了一国个人隐私、数据安全、信息自由和商业利益之间平衡的价值观,需要当局考量经济因素、文化因素等多重因素而为该国量身定制。从已通过GDPR充分性决定的实践来看,尽管欧盟未要求各国在本国立法中逐字复制GDPR的条款,但欧盟等效标准要求的立法比某些国家自行起草的立法更严格。因此,欧盟通过GDPR将数据保护的做法通过特定机制向世界范围输出,具有否定各国个人数据与隐私保护立法的条件性与个性化,无视第三国与欧盟的技术能力差异、价值主张分歧与法律文化冲突的嫌疑。欧盟高质量的数字市场所产生的贸易吸引力以及GDPR所塑造的立法趋同化,使各发展中国家深陷数字贸易利益与高昂的制度成本相互拮抗的泥潭。

另一方面,欧盟在评估一个国家的数据隐私立法是否与GDPR相当时,还要评估该国是否能够有效地实施和执行该立法。对于技术、财政以及专业支持方面资源有限的发展中国家而言,这些要求向其提出了显著的经济与组织挑战。内部资源不足与经济发展的热切渴望之间的矛盾,是发展中国家在努力弥补数字贸易鸿沟的过程中面临的主要冲突。发展中国家执行类GDPR的全面数据保护法律框架将产生巨额成本,这些成本将以网络责任保证以及遵守GDPR数据跨境传输工具的形式出现。即使一个国家通过一项全面的数据保护法案,也有可能缺乏实施和执行法律规定的资源。综合而全面的数据保护方法的实施涉及安全技术与设备、合规工具与技术、合规审计、设备更新与维护以及人力资源培养等环节,需要充足的财政支持。

(二)技术应用

因应GDPR数据跨境传输规则的要求需要足够的技术保障。数字经济时代隐私

① "布鲁塞尔效应"由哥伦比亚大学教授Anu Bradford提出,描述了欧盟的全球力量如何影响其他国家采取与欧盟类似的法规。根据这一理论,欧盟的市场影响力与域外管辖的结合使欧盟能够为全球各国制定严格的监管标准,而无须诉诸国际机构或寻求其他国家的合作。See Anu Bradford, The Brussels Effect: How the European Union Rules the World 64 (Oxford University Press 2020).

保护需要符合信息安全标准(例如ISO 27001[①])的技术知识作为支撑。尽管有隐私政策等行政措施用于组织指导,但技术措施才是充分保护个人数据安全的关键因素。由于发达国家与发展中国家的划分标准并不细致,发展中国家数量庞大,面临的技术困难和现实难题并不相同。例如印度、巴西等新兴经济体具有良好的研发能力,逐步跟上发达国家的数字技术发展,但在数据要素流动机制以及数据治理体系构建等方面落后于发达国家;非洲境内的某些发展中国家可能还受困于教育相关基础设施建设以及劳动力培养,技术发展的落后通常源于当地缺乏技术教育机会,或者源于一个国家受过教育的青年熟练劳动力的迁移[②](人才流失[③])。从生产力角度看,随着互联网技术的发展以及经济全球化的不断深入,发展中国家可以拥有更多的机会接触并学习发达国家先进的科学技术。但事实上,科学技术发展不平衡极易导致发达国家凭借其技术优势,并通过规则制定,使发展中国家依附于其主导的价值产业链。[④]为应对发展中国家在数据保护方面的技术障碍,国际社会应当加强技术交流与合作,但GDPR单方面进行数据保护的强行义务要求,在没有技术支持与合作的情况下,发展中国家及其产业似乎陷入了力不从心的境地。

(三)发展需求

为满足发展中国家新兴行业的发展需求,其需要在保障国内中小型企业发展和金融创新需求的同时,抵御因过度保护而可能带来的市场竞争限制和创新活力阻碍。在全球数字经济的发展进程中,面对发达国家力争数字规则话语权的压力,发展中国家需要追求数字化贸易红利和合规成本投入之间的平衡。

1.外包业务拓展

许多发展中国家加入全球数字价值链的主要方式是为其他国家提供离岸外包服务,外包企业在被动状态下的"出口中学习"方式,是发展中国家及其新兴行业获取知识溢出、提升创新能力的重要途径。例如,近年来东南亚国家在人力资源成本、专业IT技术人才数量上具备优势,印度、越南等发展中国家逐渐处于外包软件开发排

① ISO是世界上著名的信息安全管理系统标准。它规定了信息安全管理必须满足的要求。ISO 27001标准为各行各业任何规模的公司提供了建立、实施、维护和持续改进信息安全管理系统的指导。符合ISO 27001标准意味着组织或企业已经建立了一套系统来管理与公司所拥有或处理的数据安全相关的风险,并且该系统遵守了该国际标准中规定的最佳实践和原则。See ISO, What is ISO/IEC 27001, https://www.iso.org/standard/27001, visited on 22 December 2023.

② See Sunita Dodani & Ronald E. LaPorte, Brain Drain from Developing Countries: How can Brain Drain be Converted into Wisdom Gain, 98 Journal of the Royal Society of Medicine 487 (2005).

③ 尽管近几十年来许多非洲国家的技术能力突飞猛进,但技术落后可能仍然是非洲企业寻求遵守GDPR的障碍。研究表明,这一潜在障碍主要源于两个因素:一是缺乏向非洲公民提供技术教育的当地学校的数量;二是熟练劳动力向其他市场的迁移——这种现象也被称为"人才流失"。See Cara Mannion, The GDPR's Disastrous Impact on Africa's E-commerce Markets, 53 Vanderbilt Journal of Transnational Law 704 (2020).

④ 参见刘洪愧:《对外开放与中国式现代化:理论分析与经验总结》,《北京师范大学学报(社会科学版)》2023年第5期,第6页。

名前列。[①]通常情况下,发达经济体主导数据产业链的上游关键环节,而将劳动力密集型的下游环节外包给发展中国家。然而与其他产业不同的是,企业提供IT行业外包服务的基础是个人数据跨境传输,外包服务提供商通常作为数据控制者,至少可以对客户信息进行最低限度的访问。严格的数据保护政策会加重外包服务企业的合规成本,甚至需要承担数据本地化所需基础设施的建设成本。

2.中小企业发展保障

类GDPR立法框架的执法成本不仅会影响一国政府,还会影响所有受监管的私主体。一方面,当一国数据与隐私安全保护立法取得充分性决定,保护标准将以"一刀切"形式满足所有市场要求,即无须区分欧盟市场与非欧盟市场,皆采用类GDPR法律框架所确定的严格数据保护标准。通常情况下,富裕国家更有能力以牺牲营利为代价来追求消费者保护。[②]而对于发展中国家而言,国内中小型企业作为贸易市场中的重要组成部分与主要经济形态,其需要在维护SMEs发展利益以追求不断增长的市场规模与数据隐私保护之间寻求平衡。GDPR数据跨境传输规则向脆弱稚嫩的数字贸易市场施压,无异于给发展中国家"雪上加霜"。另一方面,当一国政府数据保护法律框架还未取得充分性决定之前,企业若想维系欧盟市场业务,必须借助BCRs或SCCs等工具,导致数据技术保障义务需要直接由私主体承担。国内中小型企业是数字经济的受益者,互联网技术提升了其离岸能力,使其可以便捷地与目标市场建立联系,大幅度降低了运营成本。但是,面临日趋严格的GDPR保护标准,国内中小型企业需要耗费更多的成本以达到GDPR适当保障措施的数据保护要求。暂不论国内中小型企业在缺乏政府补贴等保障措施的情况下是否具备资金实力,就算其在个人数据流动过程中达到了SCCs预设的要求,经营过程中贸易营利是否可以匹配昂贵的成本,也是每一个国内中小型企业面临的现实难题。

3.行业创新需求

隐私法规可能给新兴行业带来的创新障碍是发展中国家需要考量的一个关键因素。数据隐私保护政策会在一定程度上对企业数据接入提出要求,并有可能波及企业的合理业务需求。严格的隐私监管有可能会强化大型数据平台的市场势力,限制数据市场竞争力,造成更加集中的市场结构。[③]在缺乏竞争政策的有效配合时,过度隐私保护会加剧支配平台与小型企业之间的紧张关系,进一步压缩小型企业的竞争空间,阻碍数据经济对国内中小型企业的创新激励效应。因此,发展中经济体不能盲目地执行严格数据保护措施,而扼杀新兴行业的创新发展。只有在得出隐私保

① 参见郑永年、徐兰朦:《企业如何通过开放实现技术进步》,《中国科学院院刊》2023年第11期,第1679页。

② See Anu Bradford, The Brussels Effect: How the European Union Rules the World 15 (Oxford University Press 2020).

③ See Michal S. Gal & Oshrit Aviv, The Competitive Effects of the GDPR, 16 Journal of Competition Law & Economics 349 (2020).

护监管的收益明显大于企业合规成本且不会造成不良竞争态势和严重阻碍创新的充分结论时，数据保护政策才能发挥出促进发展中国家数字行业健康有序发展的效能。

4.非欧盟市场扩张

还需注意，发展中国家的金融服务贸易并不仅限于欧盟市场，其他发展中国家和最不发达国家以及持不同数字贸易理念的发达国家，同样是重要的贸易合作伙伴。一方面，一国为履行欧盟单方面法律规定的义务而修改国内数据保护立法、提高数据保护标准和监管标准，有可能成为其他发展中国家特别是最不发达国家参与该国数字贸易市场的障碍。换句话说，欧盟将其国内数据向第三国流动的障碍巧妙地转移到发展中国家之间的合作关系中，导致这些国家之间的合作成本不知不觉地提高。另一方面，欧盟与美国两大数字贸易市场的数据保护政策异化，对发展中国家施加截然相反的压力。美国采取“二元”战略，在国内推动数据保护立法的同时，在国际上批判其他国家严格的数据保护法规具有保护主义倾向，并主张取消数据本地化要求。在缺乏统一的数据流动治理机制的情况下，发展中国家陷入发达国家间争夺数字贸易规则话语权的斗争中，难以在保证数字贸易参与度和保护个人数据安全之间寻求平衡。

四、印度因应GDPR数据跨境传输规则的策略及困境

通过对GDPR数据跨境传输工具的分析，可以看到欧盟已经建立了对第三方国家或国际组织的数据控制者或处理者传输个人数据的基本政策，并对发展中国家造成了因应困境。依照GDPR第46条的规定，一国在缺乏充分性决定的情况下，才可能以存在“适当保障措施”为由接收来自欧盟的个人数据。由于印度并不在欧盟“白名单”国家之列，因此其在致力于寻求欧盟充分性决定的同时，使用SCCs等替代性措施实现与欧盟国家的跨境数据传输。GDPR数据跨境传输工具的使用对印度政府的个人隐私保护改革以及私主体的合规工作都产生了深远影响。

（一）印度因应GDPR数据跨境传输规则的策略

目前，印度进一步促进个人隐私保护法律体系与GDPR的趋同化，正在制定全面的电子商务政策，2023年8月11日正式批准了《2023年个人数据保护法案》，这一系列措施，展现出印度追求欧盟充分性决定、维护欧盟数字贸易市场的决心。同时印度国内相关企业也在积极寻求GDPR适当保障措施的适用。

1.批准DPDP加强数据传输中的个人隐私保护

隐私权是印度宪法第21条所规定的推论基本权利。2017年8月，印度最高法院对普塔斯瓦米案（Puttaswamy Case）作出裁决，“维护隐私为印度的一项基本权利”得

以确认。[①]该案判决认为信息隐私是隐私权的一个子集,并指出隐私权包括保护个人身份的权利。[②]随着数字经济的发展,印度服务贸易对数据进出口的需求越来越高,因此印度国内迫切需要此类立法来保护数据主体的个人数据安全,且获得数据出口国对其数据保护水平的信任。为此,2017年7月,印度政府电子信息技术部成立印度数据保护框架专家委员会,由Srikrishna大法官专门领导,研究并制定数据保护法框架。该委员会于2018年7月27日提交了报告并提出了一项全面的数据保护法,经过公开征求意见等流程,DPDP于2023年8月由印度总统正式批准。[③]

DPDP深受GDPR的影响,其被认为是GDPR框架如何在欧盟以外被用做模型的最新例子之一。DPDP在2018年PDPB草案的基础上,形成了由九章共44条条款构成的完整且全面的数据保护法案。有学者已对PDPB与GDPR的关键条文作了深入的比较研究,可以看出PDPB纳入了欧盟GDPR的许多要素,其中包括传输个人数据时需要通知和事先同意的要求以及对数据用途的限制等。[④]DPDP与PDPB相比较,数据本地化条款与跨境数据流动条款发生重大革新。"数据本地化"要求的变化是DPDP中最具争议的话题之一。一直以来,印度是数据本地化政策的坚定奉行者,并且在国际谈判中一直坚持独立立场。[⑤]但DPDP并未明确提及数据本地化的要求,仅要求在印度存储"关键"个人数据;关于个人数据的跨境转移,印度政府在对必要的因素进行评估后,可以通知数据受托人按照规定的条款和条件向印度以外的国家或地区转移个人数据。[⑥]这项规定与GDPR充分性决定极为相似,此种改变展现出GDPR对DPDP的深刻影响。但DPDP面临着诸多质疑,包括该法案给印度带来的经济收益与合规成本之间的衡量,以及数据跨境传输条件及要求不明确等。

2.因应GDPR寻找数据传输途径

印度是印欧数字经济贸易关系的受益者。印度将数字商品与服务贸易联系起来,提高企业生产力,降低其参与国际贸易的成本。印度公司正在向全球客户提供各类软件服务和信息技术支持服务,涉及教育技术、健康服务和金融科技等领域。云计算服务是印度互联网服务出口的关键机遇。AdventNet位于印度钦奈的Zoho部门是

① 普塔斯瓦米案判决又称"隐私权判决",是印度最高法院具有里程碑意义的判决,该判决认为隐私权作为一项基本权利受到印度宪法第14条、第19条和第21条的保护。

② See Anirudh Burman, Will a GDPR-style Data Protection Law Work for India, 15 Policy Commons 2 (2019).

③ 该法案暂未生效。印度中央政府决定该法案的生效日期,并有权确定各项条款的不同生效日期。印度中央政府还有权制定单独的规则来实施DPDP的各项规定。只有当这些规则颁布后,才能了解这部新法律的全部范围。

④ See Harish Suryavanshi, India's Personal Data Protection Bill ("PDP Bill"), 2018: Brief Introduction, Key Provisions and Comparison with GDPR, 12 International In-House Counsel Journal 6 (2019).

⑤ 参见范婴:《印度数据本地化的范式评述及其对中国的启示》,《中国科学院院刊》2023年第8期,第1178页。

⑥ See DPDP, Article 16.

云计算服务的成功案例之一，其运营着一套流行的基于Web的应用程序，许多医院和银行使用这套程序来提供专业服务。[①]另外，IBM与Microsoft均在印度建立云计算中心，以及塔塔咨询服务有限公司（Tata Consultancy Services Limited，TCS）在国际IT行业的不俗表现，均表现出了印度数字服务的巨大潜力。印度向欧盟提供这类服务，通常需要收集欧盟公民的数据，面对GDPR对个人数据的强劲保护，印度展现出了坚守欧盟市场的决心。为增强印度公司的IT离岸能力，获得欧盟充分性决定自然而然成为印度与欧盟市场进一步合作的最主要路径。早在2009年，印度就开始寻求欧盟充分性评估，以减轻与外包有关的合规负担。[②]由于印度当时没有涵盖所有部门的全面数据保护法，其并没有获得欧盟充分性决定。为达到GDPR所要求的数据隐私保护标准，印度着手于个人数据保护法案的构建，寻求“充分”地位。由于东盟数字合作以及日本、韩国两国相继进入“白名单”的激励，印度将开启新一轮追求充分性决定的努力。[③]

由于印度尚未被欧盟视为拥有充分的数据隐私保护既定法律或监管框架，因此印度重视现有的SCCs和BCRs，确保数据从欧盟畅通无阻地流向印度。例如，上文提到的Zoho部门，明确表示其一直密切关注GDPR数据跨境传输规则的发展，并乐意接受2021年更新后的SCCs。随着SCCs可供所有人使用后，Zoho已开始通过审查转移场景、进行转移影响评估、限制转移、更新协议和公开等措施为采用新SCCs模版做充足准备。[④]2022年9月，Zoho在其官网公开了“支持Zoho的欧洲经济区客户”。可以看出，印度政府在为充分性决定做立法准备的同时，各私主体也在积极使用GDPR中的保障机制寻求数据传输路径。

（二）印度因应GDPR数据跨境传输规则的困境

发展中国家因应GDPR数据跨境传输规则并非易事。欧盟提供的各类数据跨境传输工具给各发展中国家带来了利益权衡的困扰，各国不得不进行数据传输经济收益与合规成本之间的考量。

1.类GDPR法律框架的印度本土化困境

（1）DPDP获得充分性决定的前景存疑

虽然GDPR与DPDP都提出了具有域外适用性的全面数据治理框架，但是DPDP

① See Nir Kshetri, Cloud Computing in Developing Economies, 43 Computer 51 (2010).

② See Graham Greenleaf, India's U-turns on Data Privacy, http://classic.austlii.edu.au/au/journals/UNSWLRS/2011/42.html, visited on 18 December 2023.

③ 欧盟议会官网的“议会问题”（parliamentary question）板块公开了关于印度是否符合欧盟充分性标准的问答。该问题于2023年10月6日提交，具体内容为印度最近颁布了一项全面的数据隐私法，该法将规定科技公司如何处理用户数据，但有人批评这可能会导致政府加强监控。因此，欧盟委员会评估该法律在数据保护标准方面的充分性至关重要。Reynders代表欧盟委员会于2023年12月6日作出答复，表明欧盟委员会目前尚未与印度进行充分性谈判。

④ See Andrew David, Zoho Welcomes the New SCCs, https://www.zoho.com/blog/general/zoho-welcomes-the-new-sccs.html, visited on 18 December 2023.

似乎具有保护主义的倾向。例如,印度中央政府以国家安全、国家主权和公共秩序为由,规定政府机构免受该法案的约束。[①]虽然GDPR包含类似条款,但它们受到不同欧盟指令和司法监督的严格监管。DPDP没有类似的监管措施,可能会赋予中央政府超越现有GDPR框架访问个人数据的权力。加之,某些模糊性条款加剧了数据跨境传输过程中的不确定性,可能引起欧盟对此类问题的担忧。例如,DPDP中央政府可以要求委员会和任何数据信托机构或中介机构提供其可能要求的信息。[②]虽然这一规定表面上是为了改善政府服务的提供,但并未提及如何使用数据、是否可以与其他私营企业共享数据,或者是否会为数据提供补偿。由于欧盟对第三国数据监控的担忧,目前DPDP可能无法满足GDPR充分性要求。

(2)DPDP对印度经济的影响不明晰

印度有学者批评,印度数据保护框架专家委员会虽然于2018年7月27日提交了评估报告,并初步构建了一项全面的数据保护法,但它未能权衡在印度实施GDPR式法律的经济成本和收益。[③]该专家委员会报告对全球范围内使用的法律框架进行广泛调查,但它没有对拟议法案可能产生的经济影响进行任何评估。[④]如今,数据隐私保护法律新版本DPDP似乎也面临着相同的问题。依照GDPR标准制定个人数据保护法律无疑将大幅度提高印度的数据保护水平,但是印度经济水平、法制发展水平以及文化传统背景是否可以与之契合,需要专业委员会进行深入调研与评估。

值得关注的是,就国家充分性调查结果而言,隐私标准不是可分离的,即必须满足向所有市场销售的要求,而不是像合同范本那样可以按数据目的地进行分离。如果DPDP被认为是具备足够数据保护能力的法律制度,那么个体企业或公司无须承担与BCRs和SCCs相关的任何其他合规成本。由此,DPDP将要求所有公司遵守严格的相同隐私标准,无论其业务规模的大小以及数据技术能力的高低,也无论其服务于欧盟市场或是其他市场。国内中小型企业(以及初创企业)依然是印度经济的中坚力量。鉴于SMEs的特殊需求与有限资源,其既受益于互联网与数据分析带来的成本收益,又缺乏处理复杂数据的技术和资金。DPDP如何在确保消费者隐私保护和国内中小型企业利益之间取得平衡,成为应当深入思考的问题。一部分总部位于印度的美国公司已表现出对DPDP的担忧,它们表示公司应监控DPDP实施进展,考虑如何利用现有的GDPR和加州消费者隐私法(California Consumer Privacy Act, CCPA)合规机制,为DPDP正式取代2011年信息(合理的安全实践和程序以及敏感个人数据或信

① See DPDP, Article 17(2)(a).

② See DPDP, Article 36.

③ See Anirudh Burman, Will a GDPR-style Data Protection Law Work for India, 15 Policy Commons 1 (2019).

④ See Anirudh Burman, Will a GDPR-style Data Protection Law Work for India, 15 Policy Commons 1 (2019).

息)技术规则做好准备。[①]美国是印度服务出口的第一大国,印度政府无法忽视与美国(以及其他贸易进口大国)的服务贸易关系维持。另外,由于欧盟成员国之间的数据保护法律差异化程度高,GDPR对欧盟而言最主要的经济收益就是隐私标准的统一。但印度在数据保护方面没有遇到先前存在的、分散的监管框架问题,因此DPDP能为其带来何等程度的经济利益,印度政府需要有更为清晰的评估与认识。

2.企业适用保障措施的合规压力

目前,印度个人数据保护法还未获得欧盟GDPR充分性决定,印度数据管理者或控制者将被要求通过BCRs或SCCs确保对欧盟公民的个人隐私保护。相比使用充分性决定这一数据跨境传输工具,印度公司将保留在非欧洲市场运营时遵守不同隐私标准的灵活性。印度正在努力巩固其作为首选全球外包中心的地位,越来越多的欧洲经济区实体与印度公司合作进行数据处理。外包业务是印度数据经济的支柱产业,并且印度公司大多在欧盟没有商业存在,其对欧盟个人数据跨境传输有巨大需求。目前从欧盟接收数据的印度公司通常依赖SCCs和BCRs满足GDPR的合规要求。其中BCRs尚未在市场中形成依赖型影响力,根据欧盟委员会2022年的统计,全球共有134家公司寻求BCRs批准。[②]部分原因是特定BCRs获得批准需要耗费大量的时间、费用和精力。[③]然而,SCCs因其"现成性"特征成为最为流行的数据跨境传输工具。受Schrems II案的影响,欧盟对SCCs的要求更加严格。新SCCs虽仍未提出数据本地化要求,但却要求数据进口方的数据保护水平应与欧盟标准相当,并可以对数据采取额外的保护措施。这无疑会加重企业的合规成本并会对数据跨境流向其他国家造成阻碍。在此情况下,许多企业被迫选择数据本地化这一方法,将数据存储于欧盟境内,最大程度减少其对数据安全的后顾之忧。如前所述,印度信息服务出口大多是外包或合同的形式,并越来越多地直接向欧盟消费者提供服务,在欧盟并未设立办事机构。这也是对于技术与资金薄弱的国内中小型企业而言利益最大化的贸易方式。如果新SCCs的严格标准导致国内中小型企业消耗大量的成本因应欧盟要求(甚至是数据本地化),将会减损SCCs机制在数据跨境流动中的替代性作用,并且可能造成印度企业商业机会的重大损失。

五、印度因应GDPR困境对发展中国家的启示

GDPR严格的数据传输标准,给发展中国家的数字服务出口造成了威胁。印度实

① See Lothar Determann, India: India's Digital Personal Data Protection Act - What should United States Companies Do Now, https://insightplus.bakermckenzie.com/bm/data-technology/india-indias-digital-personal-data-protection-act-what-should-united-states-companies-do-now, visited on 19 December 2023.

② See European Data Protection Board, Pre-GDPR BCRs Overview List, https://edpb.europa.eu/sites/default/files/files/file1/edpb_information_20201218_pre-gdpr_bcrs_overview.pdf, visited on 22 December 2023.

③ See Phillip Rees, *et al.*, Transferring Personal Data Outside the EEA: The Least Worst Solution, 13 Computer and Telecommunications Law Review 66 (2007).

践清晰地展现出发展中国家因应GDPR的两难困境:一方面,如果发展中国家寻求欧盟充分性决定,则本质上需要颁布与欧盟隐私法基本相同的隐私保护法,且需要撇清保护主义或国家监控之嫌疑,同时,不仅国内的所有企业需要依据这一隐私保护法进行改革,而且在非欧盟市场的贸易活动也需要遵守此法。这可能造成整个经济管辖区内经营成本的整体提高。另一方面,当未获得充分性决定时,数据目的国公司被要求使用SCCs、BCRs等数据跨境传输工具获得欧盟数据的入境资格。这两个传输工具依然要求数据管理者或控制者提供欧盟水平的保护、监督与准入措施,这对于发展中国家最主要的企业规模形态而言,无疑需要耗费昂贵的时间成本和资金成本。面对此种困境,可能的解决方式是在GDPR充分性决定的激励下构建和完善符合本国国情的数据保护法律框架,同时寻求更具合作性和对称性的数据跨境传输合作方式。

(一)构建符合本国国情的数据保护法律框架

GDPR数据保护标准是否应该成为非欧盟国家(特别是没有建立或健全隐私制度的发展中国家)的行为准则。[①]究其本质,数据跨境传输面临的障碍是跨司法管辖区数据保护及其传输的政策异化。GDPR旨在通过精心设计的数据传输工具以及独特的"布鲁塞尔效应",促使各数据目的国政府(或私主体)采用与欧盟标准趋同的数据保护体系,解决政策异质性的问题。然而,各个国家经济发展、法制建设以及文化传统等各不相同,数据隐私议题受历史因素影响较大,且对数据基础设施的要求较高,此类法律移植并非易事。数据隐私保护法律框架具备个性化特征,受到经济因素、社会因素及文化因素等多重限制,一套保护政策难以具备普适价值。发展中国家应当以本国国情为基准,参考GDPR、CCPR等的优秀实践,衡量法律移植的成本与经济利益之间的关系,制定符合经济数字发展水平以及与文化传统相适应的数据保护法律框架。

(二)寻求更具合作性的数据传输方式

目前,国际上大致存在三种数据传输合作治理机制:一是单边制定国家或地区法规,通过数据跨境传输工具对他国提出合规要求;二是进行贸易纪律的国际谈判,利用贸易协定平台进行数据传输规则的协商;三是涉及监管机构的隐私合作。后两者是比GDPR这类单边立法行动更具有合作性的数据跨境传输方式。

1.数据跨境传输的国际治理法规

(1)单边制定国家或地区法规

GDPR就是单边立法行动最为典型的例子。如前所述,数据跨境传输的主要障碍来源于管辖权限制,从GDPR的管辖规则及数据传输规则可以看出,欧盟意图规避或

① See Tiffany Curtiss, Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies, 12 Washington Journal of Law, Technology & Arts 106 (2016).

模糊数据本地化这一饱受诟病的措施，利用单方立法行动冲破管辖权限制，最终达到数据目的国使用欧盟标准保护欧盟个人数据的目的。但是，此种方式是不对称的，极易迫使发展中国家及其企业消耗大量成本，以追求与欧盟数字贸易产生的经济利益，忽视二者的平衡。有学者以经济学中的DID方法研究了东道国保护是否会抑制中国电商跨境并购这一问题，得出实施GDPR会从提高成本和降低收益两个方面显著抑制跨境并购的结论。[①]因此，数据跨境传输的双方寻求可以实现隐私保护可互操作的、对称的合作平台至关重要。

（2）进行贸易纪律的国际谈判

自《美韩自由贸易协定》第一次在自由贸易协定（free trade agreement，FTA）中纳入数据传输规则后，美国在此后的FTA中加以推广。由于高水平的自由贸易协定具有溢出效应以及FTA得天独厚的优势，各双边或区域贸易协定（regional trade agreement，RTA）纷纷效仿，使在FTA中进行数据传输谈判这一方式在国际社会流行。以RTA为例，其具有以下优势：第一，RTA是一个可以实现充分协商的平台。RTA成员因为共同的区域经济利益走向合作，为达成互利共赢的贸易局面，各国可以进行讨价还价，而避免对某一特定国家或地区法律制度的机械性应对。第二，RTA是一个具有包容性的治理机制。一方面，例外条款（exception clauses）是贸易协定的独特设置，为数据源国提供了监管空间。另一方面，RTA可以对数据保护的标准问题进行灵活处理，为发展中国家和最不发达国家提供特殊与差别待遇，充分考虑数据弱国的利益。[②]第三，RTA的区域模式有利于寻求各国利益最大公因数。在多边谈判滞缓的背景下，区域主义逐渐发展并盛行，形成了USMCA、CPTPP、RCEP等一系列区域贸易协定，这是世界各国在贸易领域的“抱团”现象。各成员“抱团”，旨在通过充分协商寻求各方利益的最大公因数，建立统一市场的自由贸易协定。超大型区域贸易协定RCEP的成员包括发达国家和发展中国家，若能在数据传输议题上提出可行方案，势必有助于推动更广泛多边规则的形成，并帮助发展中国家和最不发达国家融入全球数据价值链。第四，开放性区域经济的发展为地方利益提供保障。《关税及贸易总协定》（General Agreement on Tarrifs and Trade，GATT）第24条明确将RTA作为最惠国待遇原则的例外。欧盟进口香蕉案引发了世界各国对区域一体化例外的质疑，开放性区域主义[③]得以发展。在此理念下，各RTA应当给予第三方经济体足够的机会来谈判类似的安排。例如RCEP可以向其他外部经济体开放，比如中亚、南亚及大洋洲其

① 参见马述忠、吴鹏、房超：《东道国数据保护是否会抑制中国电商跨境并购》，《中国工业经济》2023年第2期，第108页。

② 特殊与差别待遇允许发展中成员作出的减让承诺比发达国家少，是世界贸易组织各协定给发展中成员的优惠待遇，指在一定范围和条件下，发展中成员可以背离各协定所规定的一般权利和义务，享有较优惠和特殊的待遇。其是国际贸易协定的重要基石。

③ 开放性区域主义是指区域内逐步消除壁垒的同时，依然遵守最惠国待遇原则，相应地降低对非成员的壁垒。

他经济体。但是,从现行实践来看,其缺点已展现出来,FTA仅通过限制数据外流的方式来规制数据跨境传输,各成员高度依赖例外规则规避数据传输义务。造成这一局面的原因有二,一是例外条款中"公共目的""审慎例外"[①]等关键概念规定模糊,造成了条款过度使用;二是各成员未充分利用平台进行各方利益的讨价还价。

(3)涉及监管机构的隐私合作

涉及监管机构的隐私合作,包括经合组织隐私准则、APEC跨境隐私规则以及美欧数据隐私框架等。以美欧数据隐私框架(EU-US Digital Privacy Framework,DPF)为例,2023年7月10日,欧盟委员会通过了欧盟—美国数据隐私框架的充分性决定。美欧通过DPF达成数据传输共识的基本逻辑是相互约束,即美国承诺按照欧盟标准保护欧洲公民的隐私,以换取不受限制的数据传输。《美欧安全港协议》与《美欧隐私盾协议》的两次失败,暴露出美欧之间关于"美国情报局应承担的监管责任"这一问题的严重分歧。因此,在作出此次充分性决定之前,美国签署了一项行政命令,该命令引入了新的具有约束力的保障措施,以解决欧盟法院在2020年7月Schrems II案裁决中提出的问题。值得注意的是,新义务旨在确保美国情报机构只能在必要和适当的范围内获取数据,并建立独立和公正的补救机制来处理来自欧洲公民的有关用于国家安全目的而收集数据的投诉。[②]但是,该框架对美国情报机构信息收集活动的"必要性"与"相称性"定义仍模糊。[③]因此,新数据隐私框架前景具有不确定性,仍有待进一步观察。由此可见,两国之间以进行涉及监管机构的隐私合作、实现两大法域法律规制的兼容十分困难。因为数据隐私问题具有丰富的价值体系(包括国家安全、网络安全、权利问题等),各国监管机关基于主权考量很难在此问题上作出妥协,另外,欧美具有相对势均力敌的市场地位,双方可以基于基本对称的角色进行谈判协商。如果谈判双方地位不对称,监管合作的谈判路径很容易沦为另一种单方立法的输出形式。

2.贸易纪律谈判方式的先进性

贸易协定可能是有利于发展中国家维护本国数据利益的最佳平台。FTA为实现数据跨境传输与隐私保护法规的互操作性提供了多层次的方式构建,依次包括明确业务需要的数据跨境传输义务、例外条款以及数据本地化的选择性要求。但是如前所述,FTA需要弥补其缺陷以发挥出应有效能,关键一步即是降低各国基于数据来源国的立场对例外条款的依赖。一方面,应当阐明例外条款的关键性概念。在缺乏趋同的隐私保护标准的情况下,FTA各成员将严重依赖例外条款限制个人数据的传输,架空第一层次中的"明确数据自由流动义务"。为防止例外条款的滥用,释明"公共目

① "审慎例外"是特殊适用于金融服务贸易的例外条款。

② See Christian Wigand, European Commission - Questions & Answers: EU-US Data Privacy Framework, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752, visited on 20 December 2023.

③ 参见程海烨、王健:《美欧跨大西洋数据流动的重启及其前景》,《现代国际关系》2023年第10期,第123页。

的”“审慎例外”“隐私安全”等概念的内涵和外延是关键一步。另一方面，为充分利用FTA这一协商平台，可以引入美欧数据隐私框架的基本逻辑，即相互约束，规定数据目的国的义务。以CPTPP为例，第14.7.2条要求各成员应制定或维持消费者保护法以禁止欺诈和欺骗性商业活动；第14.8.2条要求各成员应采用或维持一个法律框架保护电子商务用户的个人信息；第14.8.3条规定各成员应当致力于采取非歧视做法保护电子商务用户免受其管辖范围内发生的个人信息违法行为的侵害。此类义务实现的关键是数据目的国与数据源国的相互承诺与约束，即数据目的国承诺可与数据源国合作完成以上义务，数据源国亦将履行数据传输义务。如此便可有效降低数据源国根据例外条款采取单方面行动的需要。虽然CPTPP上述条款中许多具体操作细节有待进一步讨论，但其提供的此种相互约束的合作方式可供借鉴，各成员可以对内设置符合本国国情的隐私保护标准，对外制定数据出口条件，以小范围形式自主选择具体安排并逐步落实深化，最终形成更加广泛的个人隐私保护共识。由此可见，FTA可以为发展中国家充分参与数字规则谈判提供平台，为突破欧美等发达国家制定的数据跨境传输规则的桎梏创造条件。

六、结语

国家间数据隐私保护法律框架的差异不能也不应完全消除。尽管欧盟继续在世界范围内推广欧洲模式，并愿意与拥有相同隐私保护标准和值得信赖的伙伴合作，但许多国家尚未具备采用GDPR的经济基础与技术条件。尤其对于发展中国家来说，在进行GDPR模式的立法以及使用GDPR数据跨境传输工具寻求合作时，将会面临昂贵的合规成本，加重初创企业与中小企业的监管负担。由此可见，在全球范围内推行一套通用的隐私保护标准并非易事，而各国通过对话和协商寻求更加灵活和可持续的解决方案更具可行性。本文认为目前最佳的国际治理机制可能是贸易纪律的国际谈判，其有利于不同国家以更加平等和对称的地位进行协商，在尊重各自法律框架差异的同时，促进数据跨境传输合作。当前欧盟如火如荼地进行着利用GDPR数据跨境传输工具输出其单方立法的行动，发展中国家抛出的以FTA寻求数据传输合作的橄榄枝可能并不受欧盟青睐。但贸易纪律谈判似乎可以成为发展中国家在面临GDPR合规压力和开拓维持欧盟市场的缓兵之计，其可以利用FTA建立与欧盟数据市场平等对话的平台，也可以在加入RTA的过程中寻找与世界各国隐私保护法律的互操作性，充实本国维护数字发展权的谈判筹码。贸易是双向行为，是各国追求利益最大公因数、追求互利共赢的活动。发展中国家应当抓住数字经济的机会，不断提升数字技术与隐私保护水平，积极参与国际对话与合作，以更为自信的姿态在国际平台上表达自己的利益诉求。

Dilemmas and Enlightenments for Developing Countries in Responding to the GDPR's Cross-Border Data Transfer Rules – The Case of India

Abstract: EU General Data Protection Regulation (GDPR) has constructed a comprehensive and three-dimensional system of cross-border data transfer rules by using adequacy decision and appropriate safeguards and harmonized standards and conditions for personal data transfers to third countries in all EU member states. Many countries have already implemented or are considering implementing such requirements to pursue the development of data-dependent trade with EU. In the data age, it is crucial to focus on the dilemmas faced by developing countries in data transfers in order to mitigate the further widening of the digital divide between digital powerhouses and less developed countries. As a representative of an emerging economy in developing countries, India faces unique challenges in responding to the GDPR rules, and its responses provide insights for other developing countries in the aspect of negotiating digital rules.

Key words: developing countries; GDPR; cross-border transfer of data; adequacy decision; trade disciplines

(责任编辑:肖军)