个人数据跨境传输限制及其解决方案

张继红 *

内容摘要：商事交易的国际化使得个人数据跨境传输日趋频繁，而各国立法规则及执法体制差异性较大，以欧盟为代表的数据本地化政策严格限制个人数据的跨境传输，与数据贸易全球化趋势存在内在冲突。如何协调个人数据跨境传输与个人数据保护之间的矛盾，成为亟待解决的现实问题。随着《安全港协议》的失效，欧美开启新一轮谈判，并于2016年达成“隐私盾协议”，从内容上更多体现了欧盟数据保护法制的最新成果。在跨境数据传输领域，欧盟采用单边保护措施，推定其所信奉的数据保护价值理念，具有较强的对立性，难以实现理想效果；双边协议则可在短期内调和两国之间的矛盾；但从长远看，个人数据跨境传输本质上具有全球化属性，需要多个国家及地区共同参与并达成多边协议才能提供根本性解决方案。

关键词：跨境传输　个人数据保护　隐私盾协议　安全港协定

商事交易的国际化使得个人信息跨境传输变得愈加频繁，数以千万计的个人数据通过网络在全世界传输，以完成各种交易或管理行为。例如，美国企业 TRW Information Services（消费者信用信息收集机构）与日本信用组织签署协议，允许相互利用对方的数据库，以核查居住在本国的对方侨民的信用记录。〔1〕为了降低高昂的劳动成本、节约资源，一些企业还会把部分工作外包给其他国家的机构，将包括身份证、信用记录、税务、保险等个人数据跨国转移至一些人工成本相对较低的热门地区，如印度、菲律宾等国。这种境外安排将工作拆分为数个能够有效管理的部分，使企业能够将有限资源集中在核心领域，可大大提升其市场竞争力。〔2〕

大数据、云计算、互联网等科技手段的广泛应用，使得数据处理和传输愈加便捷，但也增加了监控和管理的难度。个人数据可能在 A 地收集、B 地处理、C 地储存、D 地使用，跨境因素的介入使得个人数据保护问题变得更加错综复杂。一些大型跨国企业的服务外包业务（特别是外包机构位于个人

* 上海对外经贸大学法学院教授，法学博士。

本文系国家社会科学基金一般项目“大数据时代金融消费者信息权保护制度研究”（项目批准号：15BFX112）阶段性研究成果；同时受上海高校智库上海对外经贸大学国际经贸治理与中国改革开放联合研究中心资助。

〔1〕See Robert M. Gellman, *Can Privacy be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 Vill.L.Rev.129, 1996.

〔2〕在美国，某金融机构将贷款申请资料委托印度公司 Wipro Spectramind 来处理，Wipro 员工通过网络连线来查阅、分析及处理申请资料。由于两地的时差，当美国公司员工休息时，印度员工可以接手工作，使得贷款所需时间大大缩短。See Jennifer Skarda-McCann, *Overseas Outsourcing of Private Information & Individual Remedies for Breach of Privacy*, 32 Rutgers Computer & Tech. L. J., 2006, p.325.

数据保护水平较差地区),使得数据安全问题愈加严峻。[3]而作为执法部门的数据监管机构却因为涉及境外个人数据控制者或处理者,其调查及制裁程序难以开展及执行。如何在大数据、云计算等新技术背景下促进个人数据的跨境流动并确保安全,有效协调各国数据保护法制的差异性,是一个亟待解决的现实问题。

一、跨境数据流动政策的矛盾与冲突:数据本地化与数据自由化

(一)跨境数据传输限制:数据本地化

针对跨境数据传输问题,为了实现对本国公民个人数据的保护,很多国家及地区都在某种程度上追求数据收集、存储和利用本地化,限制或禁止数据的跨境流动。这里,数据跨境传输的限制形式有所差异,有些要求数据输入地区达到"充分保护"标准,有些则对受益方施加特定要求如履行合同义务、取得同意或附加其他条件等。

第一类,严格限制数据跨境传输的国家及地区,以欧盟最为典型。1995年《个人数据保护指令》(以下简称《欧盟指令》)就数据跨境流动问题进行了专门规定,确立了"充分保护原则"。[4]如果查明第三国未能提供其所要求的"充分保护"时,成员国应当采取必要措施以阻止任何相同类型的数据向第三国传输。[5]受其影响,欧洲主要国家如法国、德国、瑞典、西班牙、荷兰、比利时、奥地利、冰岛、匈牙利、瑞士等都采用严格限制跨境数据传输的立法模式。2016年《通用数据保护条例》(以下简称GDPR)替代了《欧盟指令》,进一步扩大了条例的域外管辖权,明确规定GDPR对在欧盟境外处理个人数据的行为也具有适用效力。尽管欧盟指令也宣示其域外效力,但其从未明确说明拥有超欧盟区域的域外管辖效力。[6]这次对指令的修改,再次强调欧盟不允许将其公民的个人数据转移至那些不能提供充分保护的地区或国家,充分表明了欧盟希望通过立法的不断完善以保障欧盟整体数据保护水平。[7]

当然,该模式亦会提供一些例外情形,类似《欧盟指令》第26条规定,如获得数据主体的明确同意,基于当事人的利益而履行合同、采用标准合同条款、维护重大公共利益等。然而,实践中数据监管机构通常会对上述例外作狭义解释,以严格限制其适用,从而确保其本国或本区域公民的个人数据转移安全。

第二类,针对数据传输第三方施加义务和责任的国家,如加拿大、日本。相比较而言,此种模式对数据是经跨境传输、还是在国内转移至第三方并不作具体区分,而是适用统一规则。这里的"第三方",包括附属机构、关联机构以及母公司等,而不论其所处地点在哪里。简言之,上述两国立法要求

〔3〕2005年,香港及上海银行将客户记录外包给印度,大量客户数据被位于班加罗尔(印度南部城市)的三名呼叫中心的员工窃取,并将约合35万美元转移至位于普纳(印度西部城市)的假名账户中去。See Dinesh C. Sharma, Indian Police Make Arrests in Outsourcing Fraud, CNET News, Apr. 8, 2005, http://news.com.com/2100-1014_3-5660274.html?tag=n1.last visited on 12 Feb., 2017.

〔4〕《欧盟指令》第25条规定,只有在第三国提供"充分保护"时,正在处理或者将在传输后处理的个人数据才能向第三国进行传输。第三国所提供的保护水平的适当性应当根据与一次数据传输操作或一组数据传输操作相关的所有情况来评定。其中,要特别考量数据性质、将进行的数据处理操作的目的和持续时间、数据来源国及最终目的地国、第三国现行的一般性数据保护规定和部门性数据保护规定以及该国施行的专业规则和安全措施。

〔5〕被欧盟认定为达到"充分保护"的地区或国家,包括加拿大、英属马曼岛、根西岛、瑞士等。See Karin Retzer, Cynthia Rich, Morrison & Foerster, *Global Solution for Cross-border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 Geo. J. Int'l L. 449, Springs, 2007.

〔6〕Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) - Preparation of a General Approach, 9565/15 (June 11, 2015).

〔7〕See European Commission Memo MEMO/14/186, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014).

传输机构对于将数据传输至第三方应承担相应的个人数据保护之责，通常采用合同形式明确彼此之间的数据保护义务及责任。例如，位于加拿大的公司，如果将其所持有的个人数据转移至第三方，必须在合同中明确数据保护条款，以确保第三方机构能够提供同等水平的保护。

第三，取得“同意”或达到其他条件的国家，如韩国。在上述地区，不要求必须签署将个人数据转移至境外第三方的合同。但是，韩国要求必须得到数据主体的“选入同意”。[8]

总体而言，不论是要求数据输入方达到充分保护标准，还是通过合同、施加特殊程序性要求如取得许可等，都表明各国立法者对于跨境数据传输的基本态度，即施以一定程度的限制，防止个人数据的随意输出及滥用，从而保障国家安全并防范外国监控，以此提升对本国公民数据的保护水平。虽然数据本地化实现了对源自本国的个人数据收集、存储和利用等全过程的主动控制，但也在一定程度上失去了获得优质数据的可能，阻碍了本国数字经济的发展，进而形成非关税壁垒。

（二）跨境数据传输自由化

为了打破不同国家及地区在数据跨境传输上的壁垒和限制，推动全球数字贸易便利化，更有效的实现数据跨境流动的执法合作，满足企业间数据跨境传输的实际需要，包括经合组织（OECD）、亚太经合组织（以下简称 APEC）等国际组织制定了一系列的指南和政策，积极推动跨境数据传输自由化。

1980 年 OECD 制定的《关于隐私保护和个人数据跨境流动指南》明确指出，个人数据的跨境流动有利于经济和社会发展，应促进数据在成员国之间的自由流动，建议成员国努力消除或避免以隐私保护的名义为个人数据跨境流动制定不当障碍，建立“自由流动与合法限制原则”（第 15 条至第 18 条），包括：成员国应当采取合理和适当的措施确保个人数据的国际流通；成员国之间应去除个人数据国际流动的限制；成员国应避免借保护个人数据及个人自由之理由，在超出保护的必要程度内，创设个人数据国际流通障碍的法律与政策等。同时，OECD 于 2007 年 6 月通过“隐私保护及跨境合作执行建议”，要求成员国执行跨境合作执行隐私保护相关法律时，应采取以下适当措施：（1）改善国内隐私法规执行架构，以便于本国主管机关与外国相应机关的合作；（2）建构有利于执行跨国合作隐私保护法规的有效国际机制；（3）在执行上述法规时，应相互提供协助，包括通知、申诉、协助调查以及在适当安全保护措施基础上共享信息；（4）与利害相关方进行有利于上述法规执行的讨论及交流。[9]

此外，为了鼓励个人数据在亚太地区的跨境自由流通，APEC 于 2013 年通过了《跨境隐私规则体系》（以下简称 CBPR），其主要目的在于，确保全球组织能够收集、取得、使用或者处理 APEC 经济体的数据，在组织内制定并实施统一方法，以便全球获取和使用个人数据。同时，推动国际机制来促进和加强信息隐私权保护，并维持 APEC 经济体及其贸易伙伴间信息流动的连续性。

值得一提的是，2015 年在美国主导下达成的《跨太平洋战略经济伙伴关系协定》（以下简称 TPP）电子商务章引入“商业信息跨境自由传输条款”，以规制数据跨境传输并限制数据本地化存储，强制性要求各方允许数据跨境流动。[10]虽然 TPP 也规定了一些例外情形，如实现公共政策目标采取限制措施，但要求不得对数据传输施加超出实现合法公共政策目标所需的限制。[11]

正是由于个人数据的双重属性，一方面个人数据的人格权属性，使得以欧盟为代表的国家及地区更关注个人数据及个人自由的重要性，采取数据本地化的限制性措施；另一方面，个人数据所蕴含的巨大财产价值和经济利益，又是促使跨境数据传输自由化的关键因素。跨境数据传输本地化和自由化这一对价值矛盾与冲突，始终贯彻跨境数据传输规则始终。这里，有必要以现有国际组织如联合

〔8〕See Karin Retzer, Cynthia Rich, Morrison & Foerster, *Global Solution for Cross-border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 Geo. J. Int'l L.449, Springs, 2007.

〔9〕2006 年 9 月，同为 OECD 成员国澳大利亚及新西兰的隐私监管专员签署了“备忘录”（Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the office of the New Zealand Privacy Commissioner）。虽然时间早于“隐私保护建议”，但其于 2008 年 8 月宣布延长有效期时，被视为以双边协议方式践行该“隐私保护建议”的先例。

〔10〕TPP 协定第 14.11、14.13 条。

〔11〕参见陈咏梅、张娇：《跨境数据流动国际规制新发展：困境与前路》，《上海对外经贸大学学报》2017 年第 6 期。

国等为主导进行跨境数据传输国际规则的框架设计，积极推动各国数据监管部门之间的合作与交流，降低个人数据流动的跨境障碍，提升数据传输的便利化，增加跨境数据传输国际规则的透明度。

二、欧美跨境数据传输政策协调：从《安全港协定》到《隐私盾协议》

20 世纪 70 年代以来，美国与欧盟在隐私权保护上的巨大差异成为贸易争端的焦点。美国坚持灵活保护的策略，通过自律机制配合政府的执法保障来实现保护隐私权的目的。而欧盟却倾向于通过严苛立法对个人数据跨国流动进行保护，即“充分保护”标准。由于美国对于个人数据保护标准未能达到欧盟要求的水平，将严重限制美国企业在欧盟开展业务。为了缩小两种不同数据保护模式的差异性，并提供美国企业可以符合欧盟数据保护规则简单又高效的方法，美国商务部与欧盟委员会共同提出所谓的“安全港隐私原则”，于 2000 年 11 月 1 日达成了《安全港协定》。

（一）欧美《安全港协定》框架

“安全港”是指由美国商务部建立公共目录，在交通运输部和联邦贸易委员会管辖下的任何机构以自愿的形式加入。一旦选择加入，就要公开宣誓自己完全接受安全港原则的约束，而且每年还要向商务部提交公开隐私政策的书面报告，以此来证明自身确实遵循这些原则，否则便被视为商业欺诈行为。〔12〕自《安全港协定》生效起，有超过 2000 家美国企业或组织申请加入安全港计划。需要注意的是，美欧所签订的《安全港协定》并未涵盖金融服务业及相关行业的个人信息处理。〔13〕

《安全港协定》规定了七项隐私权保护原则，被奉为“国际安全港隐私原则”，〔14〕即：通知原则；选择原则；向前转移原则；安全原则（Security）；数据完整性原则；接入原则；执行原则。〔15〕《安全港协定》授权一套双层执行机制，原则上进行行业自律；如有必要，再由政府执法机构执行。〔16〕《安全港协定》吸引美国企业积极加入的一个主要原因：安全港实施的有关争议由美国法律而非欧盟法律确定，欧盟个人数据保护机构对于美国企业在美国的行为并无管辖权。〔17〕

《安全港协定》在信息技术方兴未艾之时发挥了积极的作用，一方面积极促进了美国企业在欧洲的发展及扩张，便利了欧美商业往来特别是中小企业的发展，降低了美欧间信息产业市场的准入门槛；另一方面，对国际跨境数据传输规范的统一起到了推动作用，体现了行业自律和强制规范两种监管体制的有机融合，在不同国家的监管体制之间开创了先例。只要符合欧盟数据保护标准的国家、地区、组织、团体皆可适用于安全港。目前，除美国安全港体系外，包括阿根廷、加拿大、瑞士等在内的 11 个国家和地区均达到了欧盟制定的“充分保护标准”，跨境数据传输规制日益统一化，极大地促进了国际网络数据传输的规范化治理。〔18〕

如前所述，对欧盟信息产业准入门槛的实质标准降低，以及进入安全港的企业可以忽略欧盟各国法律上的差异，使得美国企业合法地在两国间传输数据，大量数据被送往美国进行存储和分析。

〔12〕参见马运全：《个人金融信息管理：隐私保护与金融交易的权衡》，山东大学 2014 年博士学位论文，第 97 页。

〔13〕See Safe Harbor Workbook, available at http://www.export.gov/safeharbor/shworkbook.html. last visited on July 15, 2017.

〔14〕European Court of Justice 2000/520/EC: 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 harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) 25 August 2000, retrieved 30 October 2015.

〔15〕See Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed.Reg.45, July 24, 2000, p667—668.

〔16〕See Sammin. K.T., *Note: Any Port in a Storm: The Safe Harbor, the Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services*, Geo. Wash. Int'l L. Rev.,36, 2004, pp.653—657.

〔17〕参见［德］Chistopher Kuner：《欧洲数据保护法》，旷野、杨会永等译，法律出版社 2008 年版，第 197 页。

〔18〕参见马芳：《美欧跨境信息安全港协议的存废及影响》，《中国信息安全》2015 年第 11 期。

2013 年，前 NSA 雇员爱德华·斯诺登曝光大量来自美国情报机构的机密文件，其中不乏对欧洲领导人的监控。在这当中，像苹果、微软等大型科技公司则都有意或无意地参与了 NSA 的监控行动，直接导致欧洲民众对数据安全的担忧与日俱增，美欧之间的合作关系开始出现了阴影、裂痕以及种种的不确定性。

在此背景下，一名来自奥地利的公民 Max Schrems 向 Facebook 欧洲总部所在地爱尔兰数据保护专员投诉，指出 Facebook 向美国政府提供欧洲公民相关数据，未能达到《安全港协定》规定的充分保护要求。出于对美国情报机构入侵的担忧，欧洲法院于 2015 年 10 月 6 日最终裁定第 2000/520 号决定无效，直接导致《安全港协定》失效。该判决使得跨大西洋数据传输的合法性依据缺失，依赖该协定的 4500 多家美国企业处于法律上的不确定状态。

大数据等新兴技术的发展使得原有制度出现了裂痕，制定于 2000 年前的《安全港协定》在处理新问题时呈现出明显的滞后性，已无法有效应对新时期的问题和挑战。跨境数据泄露和滥用问题日益严峻，个人数据安全的脆弱性进一步凸显，原有的“安全港”已不再安全，技术发展成为倒逼法律制度不断更新完善的现实力量。

（二）2016 年欧美《隐私盾协议》（EU-US Privacy Shield）

虽然除了《安全港协定》，美欧之间的数据传输可以通过“标准合同条款”及“约束性公司规则”等替代性规则。然而，上述两种路径的适用都要受到欧盟成员国国内数据保护机构的监督及审查，且只要有一个数据主体提出申请，上述审查程序即可启动。这给美欧之间的数据传输带来极大的不确定性。[19]欧洲委员会指出，美欧数据流动受阻可能会造成欧盟整体国民生产总值下降 0.8%-1.3%。[20]美国商务部也担心，一旦《安全港协定》被撤销很可能对美欧经济带来不小的冲击。[21]

基于此，美国和欧盟围绕新的替代性协定积极展开对话和磋商，并于 2016 年 2 月 2 日达成一项新的框架协议，即《隐私盾协议》。[22]新协议由美国商务部和欧洲委员会共同设计，为大西洋两岸的欧洲和美国企业从欧盟向美国传输个人数据过程中提供欧盟数据保护规定的合规机制，并支持跨大西洋商业合作的发展。欧洲委员会认为，新条约足以使个人数据在现有的欧盟数据保护立法框架下进行传输，同时将给予企业一段时间对新隐私协议进行学习，并升级其内部合规机制。数据单一市场副主席 Andrus Ansip 指出：“新的欧美隐私盾框架能够确保美欧个人数据传输的安全性，并大大提升商业活动的透明度。”[23]

作为《安全港协定》的替代机制，《隐私盾协议》在内容上与《安全港协定》有着一定的相似性。其中，《隐私盾协议》也要遵守与《安全港协定》相同的七项基本原则，美国企业仍然采取自愿加入的方式接受《隐私盾协议》。但更重要的是，《隐私盾协议》弥补了先前《安全港协定》存在的种种缺陷及弊端，对美国公司施加更重的个人数据保护义务，强化了监督和执行机制，并赋予欧盟公民救济权利等，在内容上有很多新的突破。与此同时，《隐私盾协议》不仅包含美欧之间在数据传输方面的新承诺，还克服了原先《安全港协定》仅就个人数据跨境传输私人活动进行规制的局限性，对美欧之间以国家安全为目的个人数据传输行为也纳入协议调整的范围。

---

〔19〕See Shona McCusker, *The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?*, 37 Business Law Review, 2016, pp.84—85.

〔20〕See Yann Padova, *The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?* 6 International Data Privacy Law, 2016, pp.139—141.

〔21〕See Mark Scott, *Data Transfer Pact between U.S. and Europe is Ruled Invalid, Oct*, 6, 2015, http://www.charlotteobserver.com/news/nation-world/world/article37954002.html, last visited on April 23, 2016.

〔22〕European Commission Press Release IP/16/216, EU Commission and United States Agree on a New Framework for Transatlantic Data Flows: EU-US Privacy Shield 1 (Feb. 2, 2016).

〔23〕European Commission Press Release IP/16/2461, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016), http://europa.eu/rapid/press-release_IP-16-2461_en.htm, last visited on 16 Feb., 2017.

第一,《隐私盾协议》对入盾企业提出了新要求,以便更充分地保护个人数据。(1)加入企业必须在其隐私政策中公示入盾承诺及保证符合新协议,该承诺和保证可以依据美国法执行。加入企业必须通知数据主体有权访问其个人数据,以及应公共当局要求披露个人数据的规定。执法部门对入盾企业的合规情况以及将数据向第三方进行转让都具有管辖权。不仅如此,入盾企业还要完成定期自证审查,并接受美国联邦机构的监督和调查。(2)加入企业须对转移至第三方的数据负责。当加入企业将数据转移至数据控制者或处理者第三方时,其必须遵循通知数据主体及并供数据主体选择退出机制。在获取数据主体同意的前提下,须与第三方订立合同约定仅能用于有限的、明确的、特定的目的,并且第三方将会提供与收集方同等程度的个人数据保护措施。(3)加入企业必须配合美国商务部行动,即及时回应商务部有关新条约框架下提出的质询或要求。(4)在个人数据持有期间存续时,加入企业须确保按规定保护个人数据。在此基础上,加入企业嗣后退出新协议的,若其选择继续留存已经获取的个人数据,则其必须对留存的数据继续履行新协议的保护义务,或通过其他授权的方式为该等数据提供足够的保护。

第二,《隐私盾协议》为欧盟境内数据主体提供了多种救济手段及措施。(1)监察程序。欧盟公民个人有权直接对加入新协议的美国企业提起监察,该企业必须在 45 日之内回应该诉求。就欧盟公民提起的监察,入盾企业必须在不对个人造成费用负担等情况下建立独立的处置机制,保证每个欧盟公民的监察和争议都能够得到调查和快速处理。(2)若欧盟公民将投诉提交至欧盟任一数据保护当局,则美国商务部需在 90 日内回复该数据保护当局,并保证审查该纠纷并尽最大努力促使投诉得以快速解决。美国联邦贸易委员会承诺将有力的执行新协议,包括优先处理来自欧盟成员国各数据保护当局、美国商务部、隐私自律监管机构和其他独立救济机制移交的请求。(3)欧盟公民个人有权在美国州法院直接提起诉讼程序,包括误导性陈述等诉请。

第三,对于国家安全及执法的数据访问,美国政府明确作出了权力约束的保证。而这也是美国官方首次承诺对美国有关情报系统的情报活动进行实质性约束。美国情报界已经就适用于该组织的美国宪法、成文法等各层级的法律法规,以及来自美国政府立法、司法、行政三个分支的监管,形成书面文件并呈交欧洲委员会。美国司法部则提供了一份关于对美国政府基于执法、公众利益等目的访问商业数据和其他美国公司持有数据的各种限制。具体而言,美国基于国家安全实施的任何数据访问,均须有明确的限制条件和监管。美国政府承诺不对从欧盟转移至美国境内的个人数据进行无差别、规模化的监控;批量收集的公民个人数据仅能用于反恐怖主义、防止核扩散、网络安全等六个特定目的,且前提是遵守新协议保护个人数据的有关原则和规则。另外,新协议还史无前例为欧盟公民个人就信号情报活动的质询开通了一条特别通道——监察专员制度。监察专员独立于美国国家安全机关,专门负责处理欧盟公民的相关投诉。通过该制度,欧盟公民可以向该监察专员提交质询,并得到美国政府在遵守美国国家安全义务前提下给出的答复。美国副国务卿诺维利将担任首任监察专员,直接对美国国务卿负责,不受任何来自情报系统的约束。

第四,美国政府承诺将进一步强化与欧盟成员国各数据保护机构的合作。具体包括:在商务部建立联络处,专门负责与欧盟各数据保护当局进行联系,推动有关投诉的解决,协助欧盟各成员国数据保护机构寻找特定企业加入、执行新协议的情况,并向欧盟各数据保护当局提供有关新协议的材料供其在网站上发布,以增加协议在欧盟公民和企业执行的透明度。美国联邦贸易委员会亦承诺将加强与欧盟各成员国数据保护当局的合作, 包括在联邦贸易委员会内部建立联络处以及标准化的进程,供欧盟各数据保护当局转交监察;在不违反保密法律法规的前提下,就监察转交与转交机构进行信息交换;同时还将与欧盟各成员国数据保护当局进行紧密的执法合作。在此基础上,新协议还构建了一项年度联合审查机制。美国商务部、联邦贸易委员会以及其他联邦机构还将与欧盟委员会、各成员国数据保护当局及第 29 条工作组的代表们召开年度会议,共同研讨有关新协议的运作、执行、监管及执法等问题。

从《安全港协定》的发展历史来看，其执行和适用就不断受到来自各方的质疑。据统计，仅 2009 年一年之内就有七起投诉直指该协定的执行。从 2000 年至 2015 年，针对《安全港协议》的投诉远远超过 1300 件，但最终被执行的案件只有 40 个，其中仅有两家公司被执行了罚款处罚。[24]因此，与《安全港协定》相比较，《隐私盾协议》在内容及执行力上更加具体和完善。新协议为欧盟的数据主体提供了一系列强有力、可执行的保护措施，诸如企业披露如何使用个人数据的透明度要求、强有力的美国政府监管以及与欧盟数据保护机构更紧密的合作。更为重要的是，《隐私盾协议》还赋予了欧盟数据保护机构对数据接收者第三国的数据保护水平享有充分的调查权。这无疑使得欧盟对其境内的个人数据保护拥有更加稳定并具有延展性的监督权，也为欧盟数据主体的数据控制权多了一份保障和安全。

然而，仍然有很多人对《隐私盾协议》的规定是否能够得到贯彻执行，持怀疑态度。虽然从表面上看，《隐私盾协议》更加细致且执行性强，但其程序性规则存在走过场、不透明等问题，其宣示意义更大于实质意义。“棱镜门”事件的曝光者斯诺登就将《隐私盾协议》称为“说明性盾牌”，而起诉《安全港协定》无效案的原告 Max Schrems 更是认为新协议只是“新瓶装旧酒”，美国法律依旧缺少对来自欧洲数据的充分保护。[25]第 29 条工作组也于 2016 年 4 月 13 日发布了关于“隐私盾”框架的分析意见。该分析意见指出，“隐私盾”并未排除美国知识产权机构对欧洲个人数据的大量且随意的收集行为。[26]而且，在“被处理”的标准认定上，美国及欧盟存在较大分歧，但这种认识的不一致在“隐私盾”框架中并未加以明确的解释和说明。[27]

鉴于美欧在个人数据保护方式、价值理念等方面存在着巨大差异，《隐私盾协议》从实质上看仍然是美欧相互妥协、让步的产物，从内容上更多的体现出欧盟数据保护制度最新改革成果，迫使美国接受与欧盟相近的个人数据保护标准。同时，《隐私盾协议》凸显了“棱镜门”事件后美欧重建信任合作关系的努力。“棱镜门”事件后，欧盟对美国在个人信息安全措施上表示严重怀疑，双方政府层面的网络合作几乎停滞。为了最大限度地降低“棱镜门”事件的负面影响，美国在情报收集、网络安全等方面不断进行改革和调整。2016 年 1 月 17 日通过《第 28 号总统行政指令》，将之前大规模信息收集方式改为有针对的数据获取，同时还将美国境内的隐私保护拓展适用至非美国公民。[28]2016 年 2 月 24 日，奥巴马签署了《司法救济法案》，赋予欧洲公民与美国公民同等的司法救济权，即欧洲公民有权针对美国政府不当披露个人信息的行为，依据《1974 年隐私法案》在美国法院提起诉讼。而在此之前，仅有美国公民才能向法院提起联邦机构侵害个人隐私的诉讼。[29]该法案的主要目的就是为了修补欧盟对美国个人数据保护不足的裂缝，增加彼此之间的信任。

《隐私盾协议》的签署，为欧盟及美国企业的商业活动提供了制度支持和保障，进一步提升了对欧盟公民个人数据的保护水平，标志性地宣告了政府公权力对个人权利侵犯应当受到严格限制的理念。[30]换言之，美国需要更加注重公权力对公民个人权利干涉的限制和约束。但是，随着欧洲恐怖主义抬头，欧盟严格的个人数据保护法制也开始出现动摇，以国家安全利益名义开始对个人数据保护

〔24〕See Chris Connolly and Peter van Dijk, *Enforcement and Reform of the EU-US Safe Harbor Agreement, in D. Wright, P. De Hert (eds.), Enforcing Privacy, Law, Governance and Technology Series*, Springer, 2016, p261.

〔25〕Natasha Lomas, Draft Text of EU-US Privacy Shield Deal Fails To Impress the Man Who Slayed Safe Harbor, Tech Crunch (Feb. 29, 2016), http://techcrunch.com/2016/02/29/lipstick-on-a-pig/, last visited on 12 Feb.2017.

〔26〕Article 29 Data Protection Working Party, WP238, Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision (April 13, 2016).

〔27〕美国对获取数据的解释，当数据被分析使即为“处理”；但欧盟认为从数据被收集的那一刻开始，该数据就“被处理”了。See Council Directive 95/46, art. 2(b), 1995 O.J. (L 381) 31, 38 (EC).

〔28〕参见刘碧琦：《美欧〈隐私盾协议〉评析》，《国际法研究》2016 年第 6 期。

〔29〕See H.R.1428: Judicial Redress Act of 2015.

〔30〕而在此之前，美国政府公权力可以“国家安全”为名干涉个人权利。以 2016 年 4 月发生的苹果公司事件为例，美国司法部公开表示将通过申请法院令状，要求苹果公司配合将纽约发生的某起毒品犯罪案件中缴获的苹果手机强制解锁。

设置一些适用例外。例如,法国宪法委员会通过了一项监察法案,允许政府不经过法院授权就可以监控可能是恐怖分子的电话及电子邮件。同时,还要求网络服务提供商安装所谓的“黑盒子”以监控及分析元数据,并要求网络服务商将数据提供给情报机构。〔31〕2016 年发生在德国的恐怖袭击事件也促使德国政府开始要求宽松的隐私保护法,以便政府机构能够较为便利地监控网上数据,如电子邮件、App、Skype 信息等。〔32〕而在此之前,与其他欧盟成员国相比,法国及德国都建立了相当严格的个人数据保护制度,两国近期以国家安全名义放松国内个人数据保护措施执行的表现,可能将成为未来个人数据法制在某些领域有所调整的一种信号。也就是说,国家安全利益保护在欧盟境内可能会得到更多的制度豁免,更易纳入个人数据跨境传输的例外范畴。

与之相对应,美国广被诟病的宽松的个人隐私保护模式,近期开始趋向于严格限制联邦政府机构获取个人信息。2015 年 10 月 8 日,在《安全港协定》被废止两天后,加利福尼亚州通过了《电子通讯隐私法案》。该法案禁止政府机构强制性要求商业机构提供任何“电子通讯信息或电子设备信息”,除非其持有根据特殊情形颁发的搜查令、窃听许可、电子阅读器记录许可、传票等。该法案获得网业巨头如谷歌、脸书、苹果、关系网(LinkedIn)、Dropbox 以及推特的一致支持。〔33〕应该说,欧美两大数据保护模式在跨境数据传输政策上都出现了不同程度的调整,相互汲取对方立法模式的优点,形成彼此融合、妥协的发展趋势。

三、个人数据跨境传输政策的相关检讨

随着计算机及网络技术的蓬勃发展,包括个人数据的收集、存储、使用、分享及传输在本质上即具有全球化特征,已然超越了一国或一个地区的地理界限,对传统主权理论提出了严峻挑战。〔34〕仅仅依靠个别国家或区域性组织如欧盟内部法律治理规范已经明显捉襟见肘。而各个主权国家对个人数据的保护标准及水平并不统一,个人数据可能会被传输到保护程度较低的国家或地区进行处理、编辑、利用、销售等,使得个人数据的保护效果被大打折扣。针对这一问题,以欧盟为代表的地区及国家通过创设所谓的“域外效力”,即禁止将个人数据传输至未能提供充分保护的非欧盟成员国,对个人数据的跨境传输及处理行为加以规制。虽然说这种单边的倒逼机制从某种程度上说确实可以影响相关国家的立法,迫使其提高国内个人数据的保护水平,但也形成了国际贸易往来的巨大屏障。对在全球设立多个分支机构或附属机构的跨国公司而言,其因需要遵守不同的数据保护政策所投入的精力、资源也在逐日增加,成本负担十分沉重。如何调和个人数据跨境传输自由流通与个人数据保护之间的矛盾与冲突问题,则是摆在各国立法者面前的一个难题。

(一)单边性保护措施

单边性保护措施主要存在于一些经济实力、国际影响力比较大的国家及地区性组织,如美国及欧盟,主要采取一些制裁性措施,单方推行其所信奉的法律理念及原则,迫使被制裁国能够改变其行为模式,建立与其宗旨相符的个人数据保护立法,从而达到保护其境内公民个人数据权益的目的。〔35〕

〔31〕Alyssa J. Rubin, Lawmakers in France Move To Vastly Expand Surveillance, N.Y. Times, May 5, 2015,http://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html?_r=0. last visited on Feb. 2,2017.

〔32〕German Officials Vow Tighter Security, Migrant Controls After Recent Attacks, Chi. Trib. (July 26,2016, 10:20 AM), http://www.chicagotribune.com/news/nationworld/ct-germany-attacks-20160726-story.html. last visited on Feb. 2,2017.

〔33〕该法案的支持者们呼吁其他各州应该效仿加州,制定类似的隐私保护法案,借以强化对政府机构获取信息权力的限制。Kim Zetter, California Now Has the Nation's Best Digital Privacy Law, WIRED (Oct. 8, 2015),http://www.wired.com/2015/10/californi-a-now-nations-best-digital-privacy-law/.last visited on Feb. 10, 2017.

〔34〕Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 Ind. L. Rev., 1999, p.173-176.

〔35〕See Peter G. Danchin, U.S. *Unilateralism and the International Protection of Religious Freedom: the Multilateral Alternative*, 41 Colum. J. Transnat'l L., 2002, p.47.

其中，以欧盟最为典型。

欧盟先后通过《个人数据保护指令》《通用数据保护条例》将个人数据保护法规直接适用于其成员国境内，并以限制个人数据的传输为制裁手段，要求非欧盟成员国提供满足其要求的“充分保护”。于是，许多非欧盟成员国担心面临来自欧盟“数据传输禁止”的制裁，会按照欧盟数据保护标准提升其国内个人数据保护水平，以投其所好。不少东欧国家如阿尔巴尼亚、玻利维亚、克罗地亚、马其顿、安道尔等国，甚至俄罗斯联邦都陆续按照欧盟指令制定或修订了其个人数据保护法律，以确保国内立法与欧盟法制相一致。〔36〕其他国家或地区，如加拿大、阿根廷、澳大利亚、新西兰等国，以及中国香港、台湾及澳门地区都制定了新的个人数据保护法律，以确保涉及个人数据传输的国际贸易不至于因不符合欧盟指令而遭到质疑。

当然，对于个人数据保护标准制定主导权的争夺，也是一国或一个地区巩固其既有经济利益的手段。但移植不可避免地会受到输入国因政治、文化、经济、历史等因素的影响，存在排斥反应。〔37〕简单、粗暴地推行单一国家或地区的法律制度及价值信仰于其他国家，容易产生抵触、敌对情绪，甚至被视为“制度帝国主义”、〔38〕霸权主义，不利于长期的合作与交流。具体到个人信息领域，某些国家或地区组织欲将使用国内或区域内的个人数据保护标准推行至全球，势必会对其他主权国家产生在价值理念等方面的冲突。〔39〕在《安全港协定》签订之前，在欧洲市场拥有营业网点的美国企业面对可能来自欧盟的数据禁运，也表现得十分焦虑。他们认为这一行为无疑相当于对企业内部的营运模式进行独裁式的指导，将引发美欧之间的贸易争端。〔40〕经济实力较强的国家尚还可与欧盟在数据保护问题上讨价还价，如美欧之间就达成了双边协议（《安全港协定》及《隐私盾协议》）。但对于其他非欧盟国家而言，欧盟数据保护标准就具有比较强的对立性和侵略性，容易导致国与国之间关系紧张。因此，在个人数据跨境传输领域，采用单边性措施很难达到理想效果。

（二）双边性保护措施

相较于单边性措施容易引发矛盾与冲突，国与国之间的双边性谈判、磋商可以较好地解决信息跨境传输的相关问题，就此引发的争议也较单边更少。与此同时，双边性协议也不像多边性谈判会牵涉多个国家，为了达成协议所耗费的时间成本也会大大降低，更容易推进合作。因此，在个人数据跨境传输方面，双边性协议在短时间内具有比较强的可操作性。

这里，比较典型的双边性协议就是前文述及的美欧《安全港协定》以及《隐私盾协议》，美欧之间通过双边协议大大缩小了在个人数据保护标准上的差异，采用美国企业自证方式加入“安全港”及之后的“隐私盾”，公开承诺遵守个人数据保护的相关规则。美国政府也无须全面修改其国内法，大大降低了其国内的立法成本。2008 年 12 月，美国与瑞士也达成了“安全港框架”，用以解决因为两国之间数据保护标准不一而影响跨境数据传输问题。

然而，双边性协议的达成本身受到协议参与国自身经济、政治力量的制约。如果两个国家实力相当，则双边性协议的内容对于参与国而言应是相互妥协让步的结果。反之，如果实力悬殊过大，这种双边性谈判必然成为利益失衡状态下对弱国主权的一种侵蚀和伤害。〔41〕另外，双边性协议仅仅解决

〔36〕See Karin Retzer, Cynthia Rich, Morrison & Foerster, *Global Solution for Cross-border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 Geo. J. Int'l L.449, Springs, 2007.

〔37〕See Mark B. Baker, *No Country Left Behind: the Exporting of U.S. Legal Norms under the Guise of Economic Integration*, 19 Emory Int'l L.Rev. 2005, p.1321.

〔38〕“制度帝国主义”，是指在国际贸易中经济及政治实力强的一方会利用其优势地位将其国家利益制度化并纳入国家贸易规则体系中去。See Anu Piilola, *Assessing Theories of Global Governance: A Case Study of International Antitrust Regulation*, 39 Stan. J. Int'l L. 207, 2003.

〔39〕Sunni Yuen, *Exporting Trust with Data: Audited Self-regulation as a Solution to Cross-border Data Transfer Protection Concerns in the Offshore Outsouring Industry*, 9 Colum. Sci.& Tech. L. Rev., 2007, p41.

〔40〕See Steven R. Salbu, *Regulation of Borderless High-technology Economies: Managing Spillover Effects*, 3 Chi.J. Int'l L., 2002, p142.

〔41〕Mark B. Baker, *No Country Left Behind: the Exporting of U.S. Legal Norms under the Guise of Economic Integration*, 19 Emory Int'l L.Rev., 2005, p.1321.

两国之间的跨境数据传输问题，相比多边性措施其适用范围过窄。若要尽可能多的获得其他国家或地区的跨境数据传输认可，就需要逐一与不同国家进行谈判、磋商，而国际谈判过程通常复杂、冗长，直接导致时间及资源成本不断攀升，形成巨大的交易成本。

由此可见，虽然双边性协议在短期内对于调和不同国家之间的数据保护标准不一问题，属于比较可行的解决路径。但从长远看，个人数据跨境传输本质上具有全球化性质，需要多个国家及地区的共同参与并达成多边性协议或机制，才能使问题得以根本性解决。

（三）多边性保护措施

大数据时代，个人数据的收集、使用、处理、传输及分享主要通过网络或电脑等科技手段进行，个人数据被滥用的现象屡禁不止。单靠某个国家或地区，或者几个国家几乎不可能有效地实施及执行国内的个人数据保护制度。个人数据处理的国际化，使得切实落实个人数据保护措施需要国际社会、各个国家的共同努力和积极参与。

1.区域性多边保护措施

各个国家或地区个人信息保护法制差异性极大，而其本身又有独特的政治、经济、文化、历史背景，这也势必造成多边性谈判的阻力巨大，要想达成初步共识难度相当大。作为过渡性手段，区域性多边机制的建议应该说是很好的尝试。但是，即便是建立了单一市场的欧盟，推行统一的数据保护标准的谈判过程也并非一帆风顺，受到来自各国及各个行业利益集团的影响。以 1995 年欧盟《个人数据保护指令》为例，在五年的磋商过程中，就形成了南北方两大阵营。英国、爱尔兰、丹麦、芬兰、挪威及瑞典组成所谓“北方阵营”，反对将信息隐私视为基本人权，认为新闻自由亦应得到保护。在最后表决时，英国投了弃权票，以示对指令的反对态度。法国、意大利、西班牙及卢森堡则为另一阵营。因为分歧较大，指令的最终版本具有相当程度的开放性，还有诸多例外条款，是各方利益妥协、让步的结果。2016 年《通用数据保护条例》弥补了《欧盟指令》的不足之外，具有自动执行效果，能够直接适用于欧盟各成员国，不再需要进行国内法的转化。但是近期，随着英国的正式脱欧，反全球化的思潮开始不断涌现。

相比欧盟具有刚性约束力的特点，亚太经合组织及经合组织采用了柔性规范的思路。如前所述，OECD 通过的《有关隐私保护及个人数据跨境流动指南》及《隐私保护及有关跨境合作执行建议》仅具有劝告、指导作用，不具有强制约束力，只能提供成员国及其他国家有关个人信息保护立法或跨境合作的执行参考。但是，对于经济欠发达、较贫穷的非工业化国家来说，OECD 往往被描述为“富人俱乐部”，其成员大都是经济实力强的工业化国家，其主要弊端在于该组织缺乏开放性和透明性。亚太经合组织既不像欧盟基于条约或宪法产生，也不类似 OECD 设立准入门槛要求，其组织结构更加松散，由各种大小会议维持，成员 APEC 所为的承诺也并无强制执行力。虽然 APEC 在隐私保护领域的纲领、政策并无约束力，但是确立了该领域最低而非最高的数据保护标准，允许会员采取更严格的立法，或多或少的影响着会员关于个人数据保护法制的建设。APEC 成员国个人数据保护相关法制分歧性非常大，既有保护程度较高、采用综合性统一立法的日本、韩国、澳大利亚、加拿大以及中国台湾地区，也有采用部门立法、行业自律的美国，还有没有建立个人数据保护法的印尼、菲律宾等国家和中国大陆地区。数据产品可为一种“奢侈品”，经济发达的成员需求更为强烈，而各成员国保护水平及状态不一，也被视为亚太经合组织之间限制个人数据流通的潜在障碍。相对于欧盟、OECD，亚太经合组织成员的经济、文化、政治及社会发展程度差异性更大，想要建立并推行具有强制执行力的统一多边性个人信息保护规则更是难上加难。

应该说，区域性多边保护措施充分发挥了某一区域地缘化优势，将该地区诸多国家联合起来形成合力，更有利于在跨境数据传输方面达成一致意见。但是，区域性保护措施其影响力毕竟有限，要想建立长期、制度性的合作方式，唯有大多数国家达成共识，形成具有普遍性的行为规范，才能真正解决个人数据跨境传输问题。加之，网络科技又缔造出一种新形态的社会交往模式，单靠地方、国家

或某个区域组织的传统管理方式难以应对全球化、网络化带来的风险及挑战，唯有采取新的策略以及全球性规范才能寻求根本性的解决之道。

2.全球性多边保护措施

全球性多边保护措施，虽然能够统筹协调世界范围内不同背景的国家在数据保护方面的差异性，但因为参与国家众多且缺乏国际性法律框架，将面临信息不对称、不确定性大等诸多问题，妥协程度相比区域性措施及双边协定更大，且谈判成本更高。尽管多边性谈判面临重重困难，但由更多国家合作和参与下制定的跨境数据传输规则不仅更具有实效性，能够大幅降低重要的信息收集、监督与执行协议的成本，还能通过建立清晰明确的法律机制及程序性规则，使得各国在个人数据保护领域的决策及执行更加透明化，[42] 对于参与数据处理的企业及其他机构而言亦能形成稳定的预期，有针对性地制定其隐私政策。

事实上，很多国际组织如联合国、经合组织、亚太经合组织等都制定了个人数据流通的指南、政策等，应该说在多边合作领域作了非常好的尝试。欧洲各国为了遵循 1995 年欧盟《个人数据保护指令》的规定，纷纷设立了专门的数据保护机构。自 1979 年开始，各国数据保护机构每年召开“数据保护与隐私专员国际会议”。[43]2005 年 9 月在瑞士举办的第 27 届数据保护与隐私专员国际会议，通过了“蒙特勒宣言”，认识到各国数据保护法律规范的分歧性，而造成个人数据全球化流动所应有的保护措施缺失，呼吁各国在尊重法律、政治、经济及文化背景多样性的同时，应强化先前的国际组织如经合组织、联合国、欧盟及亚太经合组织提出的关于个人数据保护的基本原则，使其获得世界性的普遍认可。各国政府、国际组织及超国家的组织应加强合作，发展个人数据保护的普遍性公约。同时，呼吁联合国应该通过具有约束力的法律规范，将个人数据保护及相关权利列为具有执行力的人权。[44] 这里，为了促使个人数据的自由流动及全球性个人数据保护标准的建立，可以借助一些全球性政府间国际组织如联合国等，积极探索多边性保护措施。

2007 年，经合组织采纳了的“隐私保护建议”就明确指出，成员国应当促成一个非正式隐私执行框架的建立，隐私执行当局及其他利益相关方应当就隐私制度的执行合作进行讨论，分享跨境数据传输领域执行的实践经验。隐私保护执行机构之间应加强合作，遵守国内法及建议要求。正是基于该建议，并考虑到诸如联合国、经合组织、亚太经合组织都关注到数据保护的执行问题。2010 年 3 月，11 个国家及地区的隐私执行当局联合起来建立了 “全球隐私执行网络”（The Global Privacy Enforcement Network, GPEN），并提出了行动计划。之后，16 个国家的隐私执行当局也加入了该计划。[45]GPEN 设立的目的，就是为了联合全世界的隐私执行机构以促成隐私保护法制在跨境领域的合作，具体包括：交换有关跨境执行方面的经验、问题，分享执行技巧及好的实践措施，加强与隐私执行相关组织的对话，建立双边、多边合作机制等。为了吸引更多的隐私保护执行机构加入，GPEN 作为一个开放性网络，只要向 GPEN 委员会提出申请并签署行动计划，就可以加入。为了发挥在隐私执行机制建设上的作用，GPEN 采取以下行动：定期召开会议讨论执行问题；展示不同监管机制下有效的调查技巧及执行策略；探讨程序、实体以及证据规则方面的相似性及差异性；涉及多方执行机构的调查合作；与其

〔42〕See Peter K. Yu, *Currents and Crosscurents in the international intellectual Property Regime*, 38 Loy.L.A. L. Rev.323, 2004.

〔43〕参与该国际会议的国家，除了欧洲的德国、法国、英国数据保护专员外，还包括加拿大、拉丁美洲国家，以及亚太地区的澳大利亚、纽西兰、日本以及中国香港、澳门特区的数据保护机构官员。

〔44〕See Montreux Declaration（16.09.2005）, http://www.edsb.ch/e/aktuell/konferenz/declaration-e.pdf, last visited on Feb.2, 2017.

〔45〕到目前，已经有五十多个国家及地区的数据保护机构加入该行动计划，除了欧盟数据保护监督员、美国联邦贸易委员会、澳大利亚信息专员办公室、加拿大隐私专员办公室，还包括欧洲国家如英国信息专员、比利时数据保护委员会、保加利亚个人数据保护委员会、西班牙数据保护机构、捷克个人数据保护办公室、法国 CNIL、德国联邦数据保护委员会、柏林数据保护及信息自由专员，以及荷兰、波兰、瑞士、新西兰等国的数据保护机构，还吸引了中国澳门及香港特区、韩国、日本等亚洲国家及地区和摩洛哥等非洲国家的数据保护机构加入。相关信息可以登录 GPEN 官网，see www.privacyenforcement.net，2017 年 5 月 10 日。

他相关组织的合作；向跨司法管辖区的有关消费者或者商业隐私及数据安全的教育项目提供支持；保持与其他国际组织的合作；对参与执行机构进行人员的调配。就像 GPEN 在行动计划中特别强调的那样，“行动计划并不具有强制性，也不会要求加入机构提供机密或敏感信息”，也无意于干涉有关国家主权、民事及刑事法律执行、国家安全等的政府行为。〔46〕虽然没有约束力，但从目前运行情形看，已经有 50 多个国家及地区的数据保护机构加入 GPEN，具有相当的广泛性和代表性，有助于发现并促成数据保护规则的统一框架，是关于跨境数据传输领域执行机构之间进行紧密合作的一个非常有益的尝试。在将来，GPEN 可在综合各国数据保护实践及跨境执行合作的基础上，提出有关跨境数据传输的国际规则草案，并提交联合国审议，能够更快的促进多边性保护机制的形成。

有学者提出，可以在世界贸易组织框架下，推动“信息隐私总协定”的达成。毕竟，不论各个利益集团或国家的意愿如何，跨境个人数据传输必然涉及与服务相关的贸易问题，WTO 难以置身事外。并由此提出，可以藉由涉及知识产权的 TRIPS 协定所建立的知识产权保护标准，将其纳入缔约国国内法制之中。〔47〕该建议看似具有相当的合理性，但缺乏一定的可操作性。个人数据是否属于知识产权的范畴，本身存在极大的争议，将其纳入 TRIPS 协定的难度极大。再加之，WTO 本身的谈判时间及成本巨大，参与国家情况差别极大，协商更是费时费力。例如，乌拉圭回合谈判时，有 120 个国家参与，谈判时间更是长达 9 年，2001 年开始的多哈谈判也是如此。

随着大数据时代的到来，个人数据的收集、存储、使用、传输等行为已经遍及全球，早就超越国家及地域界限，这也使得数据跨境流通问题已非一国或一个地区的内部力量就能彻底解决。即便区域性多边保护措施如欧盟，虽然排除了其成员国内部的数据流动障碍，但当个人数据传输至非欧盟成员国时，会因“数据禁运”而形成较高的贸易壁垒。只有通过更多国家参与全球多边性组织如联合国建立数据跨境流通的适用规则，才能真正实现既保护个人数据，又促使其跨境合理流动的目标。

结　语

大数据时代个人数据已经成为各方争夺的宝贵资源，数字经济亦逐渐成为国际贸易发展的重要力量。跨境数据传输自由化与数据本地化这一对相互冲突的价值目标一致贯穿跨境数据传输的全过程。闭关自守、完全禁止数据跨境流通会严重阻碍数字经济的发展，在保障个人数据安全性的前提下允许数据跨境传输才符合未来的发展趋势。反观我国，个人数据保护起步较晚，虽然目前尚未出台专门的个人数据保护法，但《刑法》《网络安全法》《民法总则》《消费者权益保护法》等都有针对个人信息保护的一般性规定。2017 年 4 月，国家网信办发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》，确立了跨境数据传输安全评估的基本原则和程序。应该说，我国个人信息法律保护体系正在逐步完善，但与欧美等国相比仍存在较大差距。作为亚太经合组织的重要一员，我国应积极参与跨境数据传输国际规则的制定，并在此框架下最大限度地发挥我国互联网企业的优势，实现国内信息保护法律制度与国际规则的对接与协调，在数字经济全球化过程中扮演更加重要的角色。

〔46〕See Action Plan for the Global Privacy Enforcement Network, https://www.privacyenforcement.net/public/activities.last visited on 2 Feb., 2017.

〔47〕参见翁清坤：《论个人资料保护标准之全球化》，台湾《东吴法律学报》2009 年第 1 期。