

# 美欧《隐私盾协议》评析

刘碧琦\*

**摘要：**在个人数据保护领域，美欧的立法和相关实践一直走在世界前列。作为国际上首个规制跨境数据流通的国际协议，《安全港协议》曾长期为美欧跨境数据流通提供重要索引和指南，然而“斯诺登事件”的爆发，尤其是《安全港协议》无效案，直接将该协议碾为废墟。成长于该废墟之上的《隐私盾协议》，既汲取了《安全港协议》的失败教训，又在该协议的基础上有新的突破和发展。虽然肯定和质疑之声并存，《隐私盾协议》作为美欧规制跨境数据流通的新规则，不仅对美欧各自数据保护立法和配套机制的完善产生了积极的促进作用，还有可能成为国际个人数据保护领域里的新范式，并对我国个人数据保护相关机制的形成和发展提供些许启发和借鉴。

**关键词：**《隐私盾协议》 个人数据保护 《安全港协议》

长期以来，《安全港协议》较为平稳地维系着美欧之间的跨境数据流通，虽然该协议的运作存在一定的缺漏，但总是被有意无意地忽略掉。“斯诺登事件”的爆发和《安全港协议》无效案终于直击美欧跨境数据流通的要害，使《安全港协议》的缺陷一览无余。经过美欧双方紧密磋商和相互妥协，《隐私盾协议》应运而生。通过对比分析《安全港协议》和《隐私盾协议》，同时深入剖析《隐私盾协议》面临的种种质疑，有助于准确把握美欧个人数据保护机制的发展现状，有利于及时预判国际数据保护立法的发展趋向，并借此对我国个人数据保护机制的发展和完善形成有益促进。

## 一 美欧《隐私盾协议》产生背景

美国与欧盟向来高度重视彼此之间经贸合作的紧密性和交往关系的稳定性，然而，随着信息化时代的到来，个人数据流通和交换逐渐发展成为美欧在商业、法律执行领域紧密关系的核心与基石。与个人数据相关的新型社会活动，以及与之相对应的权利保障、行为规制等问题，都给美欧平稳的合作关系带来巨大的不确定性因素。在此背景下，如何能够保持个人数据跨境转移的畅通，同时维护个人数据安全和隐私权，并进而推动美欧关系平稳向前发展，自然成为美欧达成共识并加强合作的新型着力点和落脚点。为了实现美国与欧盟之间有关个人数据的跨境自由流通，2000年12月达成的美欧《安全港协议》不仅代表着信息化时代的产物，还是美欧之间互谅互

\* 武汉大学国际法研究所2016级博士研究生。

让、一致努力之下达成的一项重要共识性成果。该协议涵盖了一系列有关个人数据保护的原则和要求,例如数据主体有权反对将其个人数据传输给第三国、确保“敏感”数据的明确统一、数据主体对其个人数据有权获取并进行更正等,美国企业只要接受并顺利通过该协议项下的资格认证,即可获得来自欧盟的相关数据。由于内容相对明确、可操作性较强,该协议不仅使得美欧之间有关跨境数据流通的经贸合作和相互交往变得更加顺畅和紧密,而且填补了国际上有关跨境个人数据保护的规则空白,并进而成为该领域国际规则发展的重要引擎和风向标。

但是,2013年“斯诺登事件”的爆发和美国行政机构及其私人公司未经同意大规模擅自加工个人数据行为的曝光,引发了欧盟及其成员国的严重关切,并促使整个欧盟内部开始认真思考欧洲基本人权可能受到的影响,美欧之间的合作关系开始出现了巨大的松动和不确定性。在此情形下,“马克西米连·斯科瑞姆斯诉爱尔兰数据保护专员案”(又称“《安全港协议》无效案”)就如同一记重锤,震颤了整座美欧跨境数据流通大厦,导致美欧双方不得不重新审视《安全港协议》的有效性和可适用性,并进而为《隐私盾协议》的诞生埋下了伏笔。

《安全港协议》无效案的大致经过是,一名来自奥地利的法学专业学生马克西米连·斯科瑞姆斯,以其“脸书”数据在转移给美国“脸书”服务商时未受到充分保护为由,于2013年向爱尔兰数据保护专员提出投诉。在遭到否决后,斯科瑞姆斯又以爱尔兰数据保护专员为被告,将案件上诉至爱尔兰高等法院。案件被受理后,爱尔兰高等法院很快就将此案提交至欧盟法院,并请求后者先就某一国内数据保护机关是否受欧盟委员会调查结果的约束进行初步裁决。欧盟法院经过调查认为,欧盟委员会在通过《安全港协议》时,其对美国是否为个人数据提供了充分保护未履行应尽的调查职责,且《安全港协议》将国家安全、公共利益和法律执行需要置于隐私原则之上。综合这些判断,欧盟法院最终于2015年10月6日做出判决,认定美欧《安全港协议》无效。<sup>①</sup>该判决结果一经作出便在欧盟内外引发了强烈反响。欧盟内部人权保护机构,例如法国数据保护机关(Commission Nationale de l'Informatique et des Libertés, CNIL)和各种人权组织爆发一片欢呼之声,而欧盟其他相关机构和成员国也开始修缮与数据保护相关的立法。<sup>②</sup>然而,欧盟委员会的多项研究结果却表明,美欧数据流通受阻可能造成欧盟整体国民生产总值下降0.8%~1.3%。<sup>③</sup>这恰好印证了美国政府部门此前的担忧,因为早在案件判决作出之前,美国商务部一位发言人曾明确指出,《安全港协议》一旦被撤销很可能会给美欧数字经济增长带来负效应。<sup>④</sup>而在事实上,《安全港协议》无效判决作出之后,不仅经济下滑的恐慌一度弥漫在美欧大陆上空,而且欧盟内部有关个人数据安全、隐私权等的呼吁和质疑,还给欧盟内部团结和稳定带来不小的冲击。因此,对于重新达成有关数据转移的协定,以促进美欧双边贸易的可持续发展,同时确保欧盟内部的团结和稳定,美国与欧盟均抱有强烈的共同意愿。

① Maximilian Schrems v. Data Protection Commissioner, Judgment (6 October 2015), 2015 CURIA, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1086398> (last visited September 2, 2016).

② See Yann Padova, “The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?”, (2016) 6 *International Data Privacy Law* 139, pp. 139–161.

③ See Yann Padova, “The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?”, (2016) 6 *International Data Privacy Law* 139, p. 140.

④ See Mark Scott, “Data Transfer Pact between U. S and Europe is Ruled Invalid”, [http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?\\_r1/40](http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?_r1/40) (last visited September 2, 2016).

事实上,《安全港协议》被废除之后,美欧之间的数据流通并未完全陷入绝境,标准合同条款(Standard Contractual Clauses, SCCs)和有约束力的公司规则(Binding Corporate Rules, BCRs)能够作为《安全港协议》的替代规则,继续为美欧跨境数据流通提供依据。<sup>①</sup>然而,无论是标准合同条款还是有约束力的公司规则,二者在适用时都要受到欧盟成员国国内数据保护机构的监督和审查,且该监督和审查的发起只需要有一个公民的投诉即可实现,这就给美欧跨境数据流通增添了极大的不确定性和复杂性。在此之后,经过持续的对话和磋商,最终于2016年7月正式生效的美欧《隐私盾协议》就是在上述背景下诞生的。

## 二 《隐私盾协议》与《安全港协议》的关系及其受到的质疑

在制定宗旨和保护措施等方面,《隐私盾协议》与被视作其前身的《安全港协议》之间存在较为明显的沿革关系。而且,正是基于这种沿革关系,一方面使得《隐私盾协议》在美欧之间能够顺利达成并获得较快的认可和接受,另一方面也使得该协议亮点凸出,并对美欧乃至国际个人数据保护立法的发展产生了较大影响。不过,学界对《隐私盾协议》的质疑,也在一定程度上促使人们更加客观审慎地看待该协议及其影响。

### 1. 美欧《隐私盾协议》对《安全港协议》的承继

作为《安全港协议》的替代品,《隐私盾协议》在许多方面与《安全港协议》具有较大的相似性,可以说二者之间存在着明显的承继关系。首先,从宗旨上来看,《安全港协议》和《隐私盾协议》都旨在为美欧商业贸易中的个人数据转移提供便利,同时确保这些数据的安全。其次,从性质上来看,由于美国和欧盟在个人数据保护的方式、力度和利益等方面存在一定的差异和分歧,因此,这两份协议从很大程度上说都是美欧相互妥协和折中的产物。再次,从执行上来看,《隐私盾协议》的运作方式与《安全港协议》大致相同,例如美国公司对《隐私盾协议》的认证行为仍将采取自愿接受的方式,并遵守与《安全港协议》相同的七项隐私原则,<sup>②</sup>可以说,对依附在这些数据之上的个人隐私权的保护,其主动权仍掌握在美国手中。

### 2. 美欧《隐私盾协议》对《安全港协议》的变革

与《安全港协议》相比较,《隐私盾协议》在许多方面有新的发展和突破。《隐私盾协议》不仅包含美欧之间的新承诺、对美国立法和行政实践的详细阐释,更重要的是打破了《安全港协议》中个人数据交换的纯商业性质,对美欧之间包括以国家安全为目的的个人数据流通行为也进行了规定,这对于2013年“棱镜门”事件之后修复美欧相互信任关系至关重要。<sup>③</sup>《隐私盾协议》的新发展或者突出特点主要体现在以下几个方面:

首先,在数据加工主体的责任及其履行方面,《隐私盾协议》的规定较之《安全港协议》更

① See Shona McCusker, “The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?”, (2016) 37 *Business Law Review* 84, pp. 84–85.

② “安全港”七项原则,包括:(1)通知原则;(2)选择原则;(3)向外移转原则;(4)安全原则;(5)资料完整原则;(6)获取原则;(7)执行原则。

③ See Communication from the Commission to the European Parliament and the Council, “Transatlantic Data Flows: Restoring Trust through Strong Safeguards”, COM (2016) 117 final, [http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf) (last visited September 2, 2016).

加透明,标准也更加严格。例如,在对来自欧盟的个人数据进行加工以及保护相关数据主体的权利方面,美国公司不仅必须公示其入盾承诺、公开其隐私政策,还要完成定期自证审查,并接受美国联邦相关部门的监督和调查。此外,《隐私盾协议》还以严厉的惩罚措施为后盾,以确保目标公司严格遵守其所承诺的法律责任。其次,在行政权力设置方面,《隐私盾协议》首次要求美国政府向欧盟递交书面声明,并确保行政机构在法律执行、维护国家安全和保障公共利益活动中,有明确的权力范围、保障与监管机制。根据协议,美国还将任命一个独立于国家安全机构的监察员,并由其专门负责对欧盟数据主体提供救济措施。更为重要的是,该项救济措施不仅适用于《隐私盾协议》管辖范围内的被转移数据,而且适用于所有因商业目的转移到美国的个人数据,且不论转移这些数据的网络基础设施的具体情况为何。再次,在隐私权保护方面,《隐私盾协议》为欧盟境内的数据主体提供了多重救济措施。根据协议,任何一位欧盟公民,只要其认为自己的个人数据已被滥用,即可通过一些便利且低成本的途径,例如免费的替代性纠纷解决机制等获得救济。在收到投诉的情况下,《隐私盾协议》项下的目标公司需要在规定的期限内作出回应。倘若投诉始终不能获得解决,则“隐私盾”专家组将针对被投诉的公司做出裁决。而一旦上述救济措施均失效,数据主体还享有一项终极性的被救济权,即向“隐私盾”专家组求助,并由后者向美国的“隐私盾”目标公司作出有约束力和执行力的争端处理决定。最后,《隐私盾协议》的一个突出亮点还在于,其设置了一项年度联合审查机制,用以监督并确保《隐私盾协议》的正常运作,并由欧盟委员会和美国商务部共同执行。如果美国企业和政府部门未能履行其承诺,欧盟委员会就将暂停《隐私盾协议》的运作。

通过上述分析可见,为有效规制与美国之间的跨境数据流通,欧盟除赋予数据主体更强的权利能力、同时对数据控制者施加更重的义务要求外,还强化了自身数据主权和数据治理权,而这也预示着欧盟成员国政府在管控数据流通方面的权力获得进一步强化和提升。此外,为确保双方国际贸易往来的正常发展,美国针对欧盟的新举措作出了更大的让步和妥协,而这也是《隐私盾协议》成功实施的必要前提和保障。

### 3. 学界对《隐私盾协议》的质疑

总体上看,《隐私盾协议》似乎比《安全港协议》更加具体和完善。从《安全港协议》的发展历程来看,该协议的适用和执行问题长期以来饱受诟病,但始终未能获得实质性的改变。自2009年起,针对《安全港协议》的投诉便不断增多,仅2009年一年之内就有7起投诉直指该协议的适用与执行。此外,有学者做过一次调查统计,结果显示从2000年到2015年接近16年的时间里,针对《安全港协议》的投诉案件远远超过1300件,而最终获得执行的却只有40件,且在这40件获得执行的投诉案件中,仅有两家公司最终被执行了罚款处罚。<sup>①</sup>在此背景下,《安全港协议》无效案以及《隐私盾协议》的出台,对于提升欧盟个人数据保护的执行力,无疑具有重要的积极意义。首先,该案是欧盟法院首次依据欧盟法中重要的宪法性条款,例如欧盟运作条约<sup>②</sup>和欧盟基本人权宪章,对国际数据流通的规制作出分析,这就为流通中的欧盟个人数据打开了欧盟基本法和人权法保护之窗。其次,该案确认并强化了欧盟法中的一项基本权利——数据保

① See Chris Connolly and Peter van Dijk, “Enforcement and Reform of the EU-US Safe Harbor Agreement”, in D. Wright and P. De Hert (eds.), *Enforcing Privacy, Law, Governance and Technology Series* (Springer, 2016), pp. 261–283.

② See Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), O. J. C 326/47 (2012), Article 16.

护权，同时要求进一步明确欧盟法中数据保护充分性的标准。这样一来，未来欧盟个人数据保护相关法，例如《隐私盾协议》，就应该且能够为欧盟个人数据保护权的适用提供确定的法律依据。再次，作为该案判决直接产物的《隐私盾协议》还明确规定，未来欧盟境内的数据保护机构对作为数据接收国的第三国的数据保护水平享有充分性调查权，这使得欧盟对于其境内的个人数据享有更加稳固且具有延展性的控制权，藉此也为欧盟个人数据的流通与安全增加一道安全阀。

然而，抛开上述可以预见的优势，学界对于《隐私盾协议》的规定是否切实可行，仍然提出了诸多质疑。例如，协议规定任何人只要认为其个人数据遭到了滥用，即可依照该协议寻求救济。那么公民如何知道其个人数据已经被滥用？<sup>①</sup>此外，《隐私盾协议》规定由被投诉的公司对相关投诉做出回应，那么获得成功的投诉能否就隐私权被侵犯获得赔偿？<sup>②</sup>学界对该问题的疑虑不无根据，因为既往实践表明，美国法院似乎不愿意为以隐私权为标的的案件提供赔偿救济。因为在这些法院看来，隐私权即便被侵犯，也不存在任何实际损失。然而，学界对《隐私盾协议》最大的质疑还在于，欧盟似乎并不能真正阻止美国的监听行动。因为即便《隐私盾协议》中有关隐私权的规则设计完美无缺，但在对这些规则的执行情况进行监督和追踪时，欧盟难免会陷入人力不从心的境况，毕竟欧盟不可能在美国境内直接对欧盟公民的隐私权进行保护。

此外，有学者质疑，美欧《隐私盾协议》与《安全港协议》一样，都可以作为数据转移规则现实性与虚幻性并存的证明。首先，从《安全港协议》来看，《安全港协议》无效案正反映出在规制跨境数据流通时，欧盟实际处在摇摆于现实与虚幻之间的境地。而作为该虚幻性重要载体的欧盟数据保护法和《隐私盾协议》，似乎又为人们缔造了一个美丽的幻觉，即欧盟数据保护法的效力可以拓展至全球，而欧盟仅凭合约条款就能阻却国外情报机构对欧盟公民个人数据的获取，且欧盟数据保护机构通过对互联网实施监管，似乎就能粉碎任何滥用欧盟个人数据的企图。<sup>③</sup>其次，从《隐私盾协议》的规则设计来看，该协议在增强个人权利方面似乎比《安全港协议》更加细致且更具有执行力，实则不然。该协议不仅表述啰嗦，而且其程序性规则还存在着不透明和走形式等弊病，一般民众更是难以准确理解该协议规则的内涵。<sup>④</sup>因此，有学者预测，未来《隐私盾协议》很有可能因为上述质疑的发展而被诉至欧盟法院。话音未了，这些预测就已经在现实中获得响应。“棱镜门”事件的曝光者——斯诺登把美欧《隐私盾协议》称作“说明性盾牌”<sup>⑤</sup>，而《安全港协议》无效案的发起者——斯科瑞姆斯更是直指欧盟委员会及其美国同僚的做法（缔结《隐私盾协议》）只是“换汤不换药”，同时宣称其将继续为保护欧盟个人数据不懈奋斗。<sup>⑥</sup>为了实现这一目标，斯科瑞姆斯已经在爱尔兰、德国和比利时等地，同时发起针对

① See Shona McCusker, “The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?”, (2016) 37 *Business Law Review* 84, p. 85.

② See Shona McCusker, “The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?”, (2016) 37 *Business Law Review* 84, p. 85.

③ See Christopher Kuner, “Reality and Illusion in EU Data Transfer Regulation Post Schrems”, (2016) 14 *University of Cambridge Faculty of Law*, <http://ssrn.com/abstract=2732346> (last visited September 2, 2016).

④ See Stephanie Hare, “For Your Eyes only: U. S. Technology Companies, Sovereign States, and the Battle over Data Protection”, (2016) 59 *Business Horizons* 549, pp. 549–561.

⑤ See Shona McCusker, “The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?”, (2016) 37 *Business Law Review* 84, p. 85.

⑥ See Shona McCusker, “The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?”, (2016) 37 *Business Law Review* 84, p. 85.

“脸书”的新一轮更大规模的诉讼。

客观上讲,美欧《隐私盾协议》确实面临着一些问题。首先,从法律机制来看,美欧双方有关个人数据保护的立法及相关机制存在明显差异,在如何有效保护个人数据以及隐私权等问题上,二者能否真正达成并践行共识始终存在疑问和挑战。例如,有学者提出质疑称,欧盟委员会于2016年7月12号发布的“隐私盾”生效决定,仅仅符合欧盟法院于2015年10月6日所作判决的形式要求,即设定新的更高标准以保障欧盟个人数据安全和隐私。<sup>①</sup>然而,《隐私盾协议》实际上与《安全港协议》被判无效案中法庭的调查结果并不相符,因为该协议仍未能对数据主体的权利和数据传输公司的资质等提供法律上的确定性和稳定性。其次,从具体规定来看,《隐私盾协议》规定,任何对《隐私盾协议》本身及其执行不满的欧盟公民,都能够向其本国数据保护机关提出投诉,而且根据该协议的授权,这些数据保护机关都有权根据投诉,发起调查并作出中止数据流通的决定。对此,美国政府不无忧虑,因为这不仅意味着美欧之间在跨境数据流通方面的合作,其持续性和稳定性被大打折扣,还有可能导致为《隐私盾协议》所做的一切谈判努力随时被打回起点。<sup>②</sup>再次,从执行层面来看,要完全实现《隐私盾协议》所规定的权利也并非易事。该协议中的部分规定,例如限制在欧盟境内进行信息检索的被遗忘权、将违反协议的公司剔除出协议的适用范围等,相对容易实现。然而,对于《隐私盾协议》赋予欧盟公民的个人数据威胁知情权,一些学者认为该规定的理想性大于现实性。这是因为,一方面犯罪分子和情报机构不会轻易暴露自己的行踪,另一方面即便发生了个人数据被入侵的事实,公司和政府基于名誉、利益和消费者的信心等原因,也不愿将该事实对外公布。<sup>③</sup>

《隐私盾协议》从提出到生效一直备受关注,原因除了有个人数据跨境流通正逐步演变成为国际贸易的核心要素、以及欧盟和美国在国际贸易中占据举足轻重的地位外,更为重要的是,该协议所确立的个人数据保护规则在很大程度上弥补了国际个人数据保护立法的空白。可以预见的是,随着与该协议相关的国际实践不断深化和拓展,该协议所产生的影响不仅将直接作用于美欧之间,还有可能波及国际上其他国家和地区,并进而对未来国际数据保护立法产生重要的借鉴和引领作用。

### 三 美欧《隐私盾协议》的影响

#### 1. 美欧《隐私盾协议》的内部效应

作为对《安全港协议》无效案判决的及时回应,美欧《隐私盾协议》首先在美国和欧盟内部产生了较大反响,其直接体现是美欧各自立法与执行的完善和强化。

首先,从立法层面来看,欧盟在《安全港协议》无效案发生后,积极主动地完善相关立法,从而增强欧盟内部数据跨境流通的便利性和安全性;迫于来自欧盟数据保护改革的压力和落实

① See Xavier Tracol, “EU-U. S. Privacy Shield: The Saga Continues”, (2016) 32 *Computer Law & Security Review* 775, pp. 775 - 777.

② See Shona McCusker, “The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?”, (2016) 37 *Business Law Review* 84, p. 85.

③ See Shona McCusker, “The EU-US Privacy Shield: the Antidote to the Transatlantic Data Transfer Headache?”, (2016) 37 *Business Law Review* 84, p. 85.

《隐私盾协议》的需要，美国也开始完善其本国相关立法，以实现其与欧盟在数据保护层面的顺利对接。具体而言，欧盟首先于2015年12月结束了两项长期且重要的谈判，并顺利达成两份政治协定兼立法动议——《网络和信息安全指令》和《数据保护改革》。2016年7月6日，欧盟议会通过了《网络和信息安全指令》，并给予欧盟成员国21个月的时间将其转化为国内法。该指令的宗旨在于对欧盟成员国设定如下义务：制定国家网络安全战略；创设一个合作组织以加强战略合作和信息交换；创设一个计算机应急小组以建立互信并加强操作上的合作等。此外，欧盟委员会还与欧洲产业界签署了一项《网络安全公私合作协定》，<sup>①</sup>并预计在2020年之前筹措到18亿欧元的投资，用以增强欧盟应对网络攻击的实力及其网络安全能力。相比之下，美国有关数据保护的立法受欧盟数据保护立法发展的影响较多，因而显得较为被动。其实在《安全港协议》被判无效之前，欧盟法院已经就有关数据保护作出过两项基本裁定。一是2014年5月13日针对谷歌与科斯特亚案，判定存在“被遗忘权”并将搜索引擎纳入欧盟数据保护法的管辖范围之内<sup>②</sup>；二是根据2014年4月8日所作的“爱尔兰数字权”裁决，以“不成比例”地干涉隐私权和数据保护权，以及独立的有权机关没有依法履行职责为由，废除欧盟有关数据留存的第2006/24/CE号指令。<sup>③</sup>有鉴于这两项基本裁定，《安全港协议》案既像是前述两项裁定的翻版，同时也是对欧盟数据保护模式的国际地位的再次确认。正如一些学者所言，欧盟善于在全球市场中采取单边规制，迫使世界其他国家或地区接受与欧盟同样的规则标准，并进而增强欧盟在国际规则制定中的主导权和影响力，欧盟的这种做法还被一些学者冠名为“布鲁塞尔效应”。<sup>④</sup>而《安全港协议》案的异曲同工之处在于，它背后似乎隐含着这样一个逻辑，即如果欧盟不允许其境内的公民个人数据流向美国，则美国就会被迫接受与欧盟相近的数据保护标准。事实上，《隐私盾协议》的达成的确离不开美国的妥协与让步，因为在该协议的谈判过程中，欧盟方面的政治人士曾提出一项前提条件，即要求美国制定一部特殊立法以约束美国国家安全局的监听行为。于是，2016年1月4日美国《司法救济法令》应运而生。<sup>⑤</sup>至少从形式上看，美国国家安全局的监听行动从此要受到明确的限制、保障和监管。紧随其后，美国又在2016年1月17日通过《第28号总统行政指令》，<sup>⑥</sup>用以改革通信情报活动，将以往大规模的数据搜集方式改为有针对性的数据收集和获取，同时还将美国境内的隐私保护扩展适用于非美国公民。此外，为了更加切实有效

① See European Commission-Press release, “Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-threats”, [http://europa.eu/rapid/press-release\\_IP-16-2321\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2321_en.htm) (last visited September 2, 2016).

② See Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD), Judgment (13 May 2014), 2014 CURIA, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=630170> (last visited September 2, 2016).

③ See Ireland digital rights (Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources Commissioner of the Garda Siochana), Judgment (8 April 2014), 2014 CURIA, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=552182> (last visited September 2, 2016).

④ See Yann Padova, “The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?”, (2016) 6 *International Data Privacy Law* 139, p. 141.

⑤ See H. R. 1428-Judicial Redress Act of 2015, <https://www.congress.gov/bill/114th-congress/house-bill/1428> (last visited September 2, 2016).

⑥ See The White House, Office of the Press Secretary, “Presidential Policy Directive 28 (PPD - 28)”, <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (last visited September 2, 2016).

地保护欧盟公民个人数据安全，美国政府在必要时还应该与欧盟数据保护机关合作。这样一来，美国的个人数据保护在立法和行政方面均实现了与欧盟的紧密绑定和对接。

其次，从执行层面来看，在《隐私盾协议》出台之后，欧盟主要通过采取形式化和本地化两种应对措施，以加强对个人数据的保护。所谓形式化是指通过实施程序性防卫措施来保障数据流通，这些措施包括由用户本人在网上点击同意按钮、数据主体和数据存储公司共同签署标准合同条款、由数据保护机构对数据转移给予正式许可、由欧盟委员会对第三国作出具有充分性的正式决定等。也正是因为这些措施的存在，《隐私盾协议》被批评者视为对国际数据流通的纯形式化回应。在这些批评者看来，协议中规定的由欧盟委员会做出充分性决定，会导致执行效率低下、决策程序不透明且受政治因素影响较大等后果。<sup>①</sup>此外，《安全港协议》案针对的主要对象之一是美国情报机构获取个人数据的行为，然而不仅欧盟法无法约束国外情报机构的行为，而且在实践中这些程序性措施也不大可能对国外情报机构获取数据的能力构成有效牵制。因此，批评人士认为上述形式化措施很难对抗国外情报机构的数据搜集行为，也不大可能给予个人数据保护权以充分保障。而所谓本地化是指鼓励或者允许将个人数据存储在欧洲境内，从而不再需要跨境转移数据的那些措施或者政策。为了实现最大程度的本地化，欧盟鼓励其境内公司将数据存储在欧洲境内的服务器上，且根据《安全港协议》案宣判后欧盟委员会及时发布的一份通讯显示，一些设立在美国的公司已陆续公布要将其保留的个人数据存储在欧洲境内。<sup>②</sup>然而，与形式化措施一样，本地化措施也遭到了批评者的多方抨击。批评者认为，首先，本地化措施只能针对个案，不具有普遍适用性。因为要将数据存储在一个特定地点，通常要考虑商业和技术因素，且并非所有的数据存储设施都安装在欧洲境内。此外，对于那些设立在欧洲境外但备受欢迎的互联网服务器，欧盟民众当然也愿意使用该服务器进行国内或者国际交流。其次，实施本地化措施会面临一些法律限制。例如，根据欧盟及其他国际人权法，在保障国家安全、维护公共秩序等特殊情形之外，个人享有不受地域限制而进行自由通信和传输数据的权利，而这也是表达自由权的应有之义，但却会给实施本地化造成巨大的法律阻碍。再次，面对国外情报机构的数据搜集行为，本地化措施只能束手无策。因为根据斯诺登的爆料，许多国家的情报机构之间长期进行着数据共享，如此一来，数据存储地与该数据能否被情报机构获得之间也许就不存在任何相关性。所以，本地化措施究竟能否有效阻止情报机构获取数据，答案几乎是不言而喻的。比较而言，美国加强个人数据保护的措施显得更加具有可操作性。因为美国主要通过技术公司为个人数据提供安全保障，且目前这些公司主要通过以下三种途径来规避政府监管，从而实现对个人数据的保护。一是采用加密技术提升公司产品和服务的独特性和安全性，但该途径一旦遇到国内法上的强制性规定，例如以立法形式要求强制信息备份时，则丧失抵御能力。二是将盟洲公民的个人数据存储在欧洲境内的服务器上，以规避美国法律规制及其政府监管。三是与存储和加工个人数据的欧盟公司合作，使数据保护变得密不透风。<sup>③</sup>

① See Yann Padova, "The Safe Harbour is Invalid: What Tools Remain for Data Transfers and What Comes Next?", (2016) 6 *International Data Privacy Law* 139, pp. 152-158.

② See Stephanie Hare, "For Your Eyes only: U. S. Technology Companies, Sovereign States, and the Battle over Data Protection", (2016) 59 *Business Horizons* 549, pp. 549-561.

③ See Stephanie Hare, "For Your Eyes only: U. S. Technology Companies, Sovereign States, and the Battle over Data Protection", (2016) 59 *Business Horizons* 549, p. 552.



除此之外，为了增强法律执行的力度和效果，并为跨大西洋数据传输提供高水平的数据安全保障，美国与欧盟还将签署一份《欧美保护伞协定》。从公布的草案来看，该协定最大的特色在于，其针对的对象是为预防、调查、侦查和起诉包括恐怖主义在内的刑事犯罪而进行的个人信息交换行为，但该协定本身不能作为交换个人信息的法律依据，而必须以美欧之间既存的或者未来达成的协定为根据。<sup>①</sup> 总之，从内部效应来看，美欧《隐私盾协议》旨在重建美国与欧盟在跨境数据流通领域里的相互信任关系，为了实现这一目标，《隐私盾协议》提供了更高的数据保护标准和更强有力的执行保障。而该协议的谈判、签署和适用，也会在一定程度上促进欧盟和美国各自数据保护相关规则的完善和发展。

## 2. 美欧《隐私盾协议》的溢出效应

与此同时，该协议已经呈现出一定的溢出效应，并对世界其他国家和地区的数据保护立法和国际合作产生了直接或者间接影响。具体而言：

首先，从立法来看，美欧较为完善和先进的个人数据保护立法给世界其他国家和地区完善相关立法提供了可资借鉴的模型，而这对于互联网产业发展迅猛而个人数据保护立法却亟待填补或完善的国家而言，显得尤为重要。<sup>②</sup> 此外，在被学习和借鉴的过程中，欧盟个人数据保护立法浓厚的人权导向（尤其对隐私权的维护）和人权保护价值理念也会对其他国家法治的发展形成潜移默化的影响。由此可见，《隐私盾协议》的达成和适用，能够在一定程度上影响其他国家和地区个人数据保护立法的形成和发展，并进而为国际个人数据保护法的形成和发展铺设道路。<sup>③</sup> 此外，《隐私盾协议》还表明在个人数据保护领域，国家在司法主权与人权之间需要而且能够达成一定的平衡，且维护和落实国家司法主权是保障和实现个人人权的前提和必要条件。

其次，从执行来看，国际数据保护规则的发展存在复边化和碎片化趋势，这就给不同国家和地区之间的相互认可和执法合作增添不少困难。在此情形下，美国与欧盟为缔结《隐私盾协议》而进行相互妥协和让步的做法，为今后隶属于不同法律体系的国家之间实现相互谅解并进行与数据保护相关的合作，提供了可资借鉴的成功经验。此外，《隐私盾协议》的谈判过程及文本内容还暴露出美欧双方在数据保护立法与执行合作中的既有缺陷，例如谈判程序不透明、无力应对情报机构的监听行为等。虽然这些缺陷本身并不具有严格的国家或者地域属性，但却有可能对现有国际秩序产生相当大的冲击。从这个意义上讲，《隐私盾协议》还预示着未来个人数据保护国际合作的发展方向，同时也是互联网时代国际法面临新挑战，从而需要在网络空间确立并发展新规则证明。

再次，从国际经贸往来和国际合作来看，随着《隐私盾协议》中个人数据保护高标准的落实，美欧个人数据保护法的发展对来自其他国家或地区企业的制约性影响将更加显著。例如，2016年7月6日欧盟议会通过的《网络和信息安全指令》一旦被成员国转化完毕，则欧盟在与

① See Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal, [http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf) (last visited September 2, 2016).

② See Seth P. Hobby, "The EU Data Protection Directive: Implementing a Worldwide Data Protection Regime and How the U. S. Position Has Progressed", (2005) 1 *International Law & Management Review* 155, pp. 155 - 190.

③ See Michael D. Birnhack, "The EU Data Protection Directive: an Engine of a Global Regime", (2008) 24 *Computer Law & Security Report* 508, pp. 508 - 520.

信息安全相关的问题上将采取更加统一的高标准和数据保护行动。由此,在国际贸易领域,凡是不符合欧盟个人数据保护标准的境外企业将面临被欧盟拒之门外的风险。<sup>①</sup>而在国际经济法上,《隐私盾协议》是否有助于推动与数据保护相关规则的新发展,是否会改变相应的人权保护标准,答案也是不言而喻的。

除此之外,由于美欧在个人数据保护领域里的领先地位及其在国际贸易中的巨大影响力,《隐私盾协议》一方面印证了前述学者提出的“布鲁塞尔效应”主张,另一方面还可能引发“多米诺骨牌效应”,即除了对与数据保护相关的国际贸易产生较为直接的影响外,《隐私盾协议》还可能对反恐行动中的资金追踪、航空运输业务中的乘客登记等诸多与数据相关的活动产生间接性影响。<sup>②</sup>因此,在数据日益发展成为现代社会重要基础设施之一的互联网时代,随着与数据保护相关的国际实践不断拓展和完善,数据保护问题会否影响国际法的发展路径,会否不断纵深成为国际法领域里的基础性问题,都值得关注和探讨。

具体到我国而言,美欧个人数据保护法的发展也可能产生一定的鞭策作用。例如,有助于促进我国发展和完善有关个人数据保护的立法,有助于将个人数据保护权融入到我国法治体系之中,促进我国调整与美欧之间有关跨境数据流通的贸易安排和司法合作。虽然在现实层面,我国个人数据保护仍然存在一定的缺陷和不足,但厘清我国个人数据保护现状,有助于我们准确发现症结所在并有针对性地提出完善建议。

## 四 《隐私盾协议》对我国完善个人数据保护的启示

### (一) 我国个人数据保护现状

较之于美欧起步早且已成体系化的个人数据保护制度,我国个人数据保护相关制度的发展则起步较晚,虽然近年来相关立法发展较为迅速,但仍存在较大的完善空间。具体而言,在立法上,我国目前与个人数据保护直接相关的法律法规有《关于加强网络信息保护的决定》《互联网信息服务管理办法》《刑法》《侵权责任法》等,与之间接相关的法律法规有《宪法》《民法通则》《民事诉讼法》《刑事诉讼法》等。此外,针对特殊群体和特殊领域,我国还制定了诸如《未成年人保护法》《妇女权益保护法》《医疗机构病历管理规定》《执业医师法》等法律法规。此外,2016年11月7日刚刚通过的《中华人民共和国网络安全法》,还在很大程度上弥补了我国有关个人数据保护专门立法的空缺,且其在立法层级、全面性和可操作性等方面均获得了显著的提升。但对比而言,我国个人数据保护机制建设仍较滞后于社会发展实践;有关个人数据保护的专门性法律法规数量仍然有限;而对数据主体的权利(例如起诉权),以及对数据控制者的义务(例如删除或更正个人信息的期限、数据分类的标准)等内容规定仍存在模糊地带和缺失。此外,在《中华人民共和国网络安全法》出台之后,如何协调该法与其他部门法之间的关系,

① See Jane Reichel and Anna-Sara Lind, “The New General Data Protection Regulation—Where Are We Are and Where Might We Be Heading?”, in Deborah Mascalzoni (eds.), *Ethics, Law and Governance of Biobanking*, (Springer, 2015), pp. 95 – 101.

② See Yann Padova, “The Safe Harbour is Invalid : What Tools Remain for Data Transfers and What Comes Next?”, (2016) 6 *International Data Privacy Law* 139, pp. 139 – 161.

并使这些立法中有关个人数据保护的规定形成有效衔接和紧密配合，仍待进一步论证和解决。而与个人数据保护立法相对应，我国在配套机构设置方面也还存在一定的不足。例如，针对《中华人民共和国网络安全法》中有关行政监管的规定，行政监督检查主体的范围、职责权限等还有待进一步明示。

或许正是源于上述不足的存在，许多从事国际贸易的中国企业在“走出去”时常常会面临来自东道国的种种限制和阻碍。此外，由于个人数据保护被大多数西方国家视为人权问题，而我国在个人数据保护立法上的缺漏，很可能成为一些居心叵测的国家批评指责中国人权状况的又一口实。

## （二）我国个人数据保护完善建议

由上述分析可见，完善我国个人数据保护机制，提升我国数据保护水平，不仅必要而且紧迫。通过对比分析欧盟和美国较为完善的个人数据保护制度，并结合我国个人数据保护现状，笔者认为当务之急可以从以下几个方面着手，努力完善我国个人数据保护制度，从而使我国能够有效应对来自国内外有关个人数据保护方面的压力和挑战。

1. 完善立法和机构配置。首先，在立法上，增加预防性立法，同时在有关个人数据保护的新法出台时，单独或者附加规定该法与其他部门法之间的关系。此外，可以把个人数据保护权确立为一项重要人权，明确该权利的内涵，并将其明示于立法文本之中，使我国个人数据保护法能够呈现出数据监管和人权保障之间的价值平衡。此外，修正和完善其他部门法中有关个人数据保护的规定，使新的个人数据保护专门法与原有部门法，例如新旧特殊规则与一般规则、行业规范等，在个人数据保护规定方面能够形成有效衔接和密切配合，并最终建构起稳固而又坚实的个人数据保护规则大厦。其次，在机构设置上，依照相关法律规定并结合不同地区的实际情况，形成权责清晰、分工明确且各层级有效衔接的行政监管体系。

2. 提升立法和政策透明度并加强宣传。《隐私盾协议》在修正《安全港协议》方面所体现的突出特点之一是，极大地提高了协议本身的透明度。《隐私盾协议》从谈判开始便向公众透露出协议的目标，以及该协议较之《安全港协议》的优越性。在2016年年初，欧盟还将拟通过的协议文本及相关解释向全社会公布，并广泛征集欧洲民众的意见。该做法获得了欧洲民众积极的认可和支持，在破解欧洲“民主赤字”的同时，《隐私盾协议》得以在2016年7月顺利生效。有鉴于此，在制定新的个人数据保护立法时，可以借鉴《隐私盾协议》的有益经验，提高立法程序和监管政策的透明度，并在新法中或者新法出台后，及时对重要术语和相关规定作出解释说明。此外，有必要加强对立法和政策的宣传教育力度，以便相关主体提前预知行为后果并及时调整行为，进而保障立法和政策宗旨的顺利实现。

3. 增强司法和执法力度。欧美个人数据保护立法之所以能够获得长足发展并具有强大的国际影响力，很大原因在于美国与欧盟不仅有较为完善的立法指引，更有配套的司法和执法机制保障这些立法宗旨的顺利实现；不仅在各自内部不断完善其司法和执法机制，还重视在执法领域加强国际合作，例如《隐私盾协议》还规定欧盟委员会要联合美国商务部对该协议的实施情况进行年度联合审查，这将有利于实现美欧在个人数据保护领域国内外政策和执行的统一，从而对个人数据形成有效保护。然而，针对我国而言，当务之急是要在完善我国个人数据保护立法的同时，加快建立配套的司法和执法机制。例如在司法和执法机构中，设立专业部门负责与个人数据

相关业务,并及时完善相关程序性规定,以便在落实我国个人数据保护立法的同时,还能够为深化国际司法和执法合作提供便利的规则指引和保障。

4. 深化国际交流与合作。作为网络技术发展的后起之秀,我国在互联网技术、法律法规和人才培养等诸多方面需要进一步完善和提升,加强国际交流与合作也因此显得十分必要和迫切。在具体做法上,我们一方面需要加强与美欧在个人数据保护立法、技术和人才培养等方面的交流与合作,学习后者先进的管理经验,另一方面可以参照美欧《隐私盾协议》模式,及时制定与他国进行跨境数据流通的合作政策和执行规则。但在有关数据保护的标准设定上,我们要坚持从本国国情出发,坚定维护本国数据主权和国家利益,并在数据监管与人权保护、国家利益与国际合作之间达成适度平衡。

## 五 结语

与《安全港协议》被废除相比,《隐私盾协议》的谈判和生效受到了同等关注。这一方面源于两份协议在功能、内容等方面存在明显的沿革关系,对其中任意一份协议的轻视都无助于认清当前美欧个人数据保护机制的发展现状和未来走向,另一方面由于《隐私盾协议》较之《安全港协议》具有显著的进步性和更加鲜明的特色,全面把握对《隐私盾协议》的积极认可和种种质疑,有助于对该协议形成更加客观且深入的认识,进而对国际数据保护法的发展作出有效预判。具体到《隐私盾协议》的内容设计上来,强劲有效的执行机制无疑是该协议最显著的特色,而为数据主体提供的较为完善的权利救济措施,还体现出美欧在个人数据保护方面所做的努力及其新发展。然而,围绕《隐私盾协议》的具体实施和现实效果,各种批评和质疑不曾消失。的确,从现实层面来看,欧盟只能被动地接受美国企业对《隐私盾协议》的自主认证,而对于违反《隐私盾协议》的主体及相关行为,欧盟也无法在美国领土上进行直接管辖和规制。另外,对于欧盟民众而言,要准确理解《隐私盾协议》中的每一项规定也会存在不小的困难。但是,根据该协议的规定,任何欧盟公民都有可能引发对协议本身以及相关活动的审查和起诉机制,这至少会在心理层面对美欧双方具体落实协议规定产生警醒作用。而欧盟看似无为或者被束缚的背后,实则是对美欧跨境数据流通国际协定的信任和遵守,以及对他国主权的尊重和维护,而这也将是未来国际数据保护法发展和实现相关国际合作的必要前提。因此,对《隐私盾协议》效力虚幻性的部分质疑,其本身是否存在虚幻性也值得商榷。

作为互联网技术的后起之秀和网民数量位居世界前列的网络大国,中国在个人数据保护方面也需要紧跟国际发展步伐,而美欧《隐私盾协议》的谈判和生效恰好为我国提供了现实参照。在国内个人数据保护立法、司法和执行方面,《隐私盾协议》生效前后美欧对各自国内数据保护立法的完善可以为我国发展相关机制提供一定的启发,更为重要的是,《隐私盾协议》对美欧之间的合作安排,例如对数据主体的权利救济、双方数据保护机构之间的国际合作等规定,可以成为我国未来制定跨境数据流通政策和开展相关国际合作的经验指南。然而,不可忽视的是,《隐私盾协议》并非尽善尽美。例如,在如何协调不同法律体系、不同国情和不同发展需求的国家之间的利益,如何保证已生效的国际协定在这些国家得到有效实施等方面,《隐私盾协议》并没有给出程式化的方法和路径,且该协议本身也还面临着种种质疑。此外,美欧《隐私盾协议》

规定的对个人数据保护的高标准，不仅代表和引领着国际个人数据保护立法的新趋向，还体现出欧盟个人数据保护立法的外溢效应，以及欧盟对国际个人数据保护法发展主导权的渴望和争夺。因此，在国际个人数据保护立法的初始阶段，结合我国国情制定和完善有关个人数据保护的国内立法，同时积极发出中国声音，有针对性地提出符合包括我国在内的广大新兴国家利益的国际个人数据保护规则建设性主张，这既是现实所需，也是有效应对国际个人数据保护立法发展的权宜之策。最后，针对欧盟不断强化对数据主权的维护、强调政府对数据的监管职能的做法，我国应该有更加充分的底气和自信主张数据主权、同时强化行政主体的监管职能，为维护和不断提升我国个人数据安全提供坚实的立法和行政保障。

## Comment on “Privacy Shield Agreement” between the US and the EU

*Liu Biqi*

**Abstract:** In the field of personal data protection, legislation and related practices in the US and the EU have been at the forefront of the world. As the first international agreement to regulate the flow of data across borders, the Safe Harbor Agreement has provided important indexes and guidelines for cross-border data flows between the US and the EU for a long time. However, the outbreak of the Snowden incident, especially the case of the invalid Safe Harbor Agreement, crushed the agreement directly into ruins. The “Privacy Shield Agreement”, which came out of the ruins, not only draws lessons from the “Safe Harbor Agreement”, but also makes new breakthroughs and developments on the basis of the agreement. Although the voices of affirmation and questioning coexist, “Privacy Shield Agreement”, as a new rule for regulating the cross-border data flow between the US and the EU, not only has played a positive role in promoting the improvement of the legislation and supporting mechanism on data protection of the US and the EU, but may also become a new paradigm for the international personal data protection and provide us with certain inspirations and references in the way of forming and developing relevant personal data protection mechanisms.

**Keywords:** Privacy Shield Agreement, Personal Data Protection, Safe Harbor Agreement

(责任编辑: 李西霞)