交大法学 SJTU Law Review
No. 1 (2019)

云计算和大数据时代的国家立法管辖权

——数据本地化与数据全球化的大对抗?

王志安*

目次

摘要 欧洲一般数据保护规则为保障作为基本权利的个人数据,通过对领土原则和国籍原则在云计算和大数据背景下的再构建,赋予规则以广泛的适用范围。从国际法上的立法管辖权基础角度看,其表现出鲜明的数据本地化特征。规则不仅广泛规范域内数据处理,还严格限制数据向域外移送。欧盟数据本地化立法将产生怎样的影响,各国应如何应对,已经成为受到广泛关注的问题。作为云计算和大数据发达国家的美国,一方面通过与欧盟合作,确保数据能自由流通,同时又采取针对性立法,规定美国网络服务提供商有义务就其全球范围的数据依法保存和披露。这一立法尽管局限于执法机关对数据的管控和利用,但却基于数据全球化的现实,明确规定了域外适用。立法管辖权冲突也因此揭开了新的一幕。

关键词 GDPR 立法管辖权 数据本地化 域外适用 领土原则 数据域外移送

一、序　　论

2018年5月欧盟一般数据保护规则(GDPR)的实施,从国际法角度看,意味着对云计算和大数据时代个人数据保护的法律规制形成了一种新的范式。其最大特征就是为保护作为基本权利的个人数据,基于领土原则对欧盟域内的数据处理行为实行严格的规制,并将欧盟域内产生的所

* 日本国驹澤大学法学部教授、法学博士。

有个人数据打上欧盟烙印，或者说赋予欧盟“盟籍”，从而对数据进行本地化，〔1〕并在此基础上建构GDPR的适用范围以及欧盟或成员国管辖权。这一做法承续并细化了1995年欧盟数据保护令(DPD)的数据本地化理念，也为建构和回避云计算和大数据时代国家管辖权冲突提供了一个新思路。

然而，备受人们关注的微软传唤令案，〔2〕却让这种认识有了一个有趣的转机。以该案为契机，2018年3月23日，美国国会通过颁布《澄清合法利用海外数据法》(CLOUD Act)，修改《储存通讯法》(SCA)〔3〕，直接规定美国网络服务提供商有义务依法保存和披露其全球范围内的数据。〔4〕由于执法当局依据这一修正重新发出传唤令，受理了上诉的联邦最高法院得以避免法解释上的两难局面。〔5〕但是，案子的结审却是新事态的开始。这一法律修正，尽管主要涉及执法机关对数据的利用和管控，却包含着美国对数据实施全球化管辖的一面，能正面挑战GDPR以及各国基于数据本地化的立法，也让关注个人数据保护的许多网络服务提供商和人权学者感觉到了新的危机。〔6〕可以看到，数据全球化立法与数据本地化立法的对峙已然成型，新一轮立法管辖权冲突正在悄然升级。

本文试图从国际法上的国家管辖权原理视角阐述个人数据本地化理念的现实含义，并通过对GDPR以数据本地化为特征的立法管辖权基础的解析，评价该基础的合理性以及对回避国家管辖权冲突所具有的意义和局限，同时也鉴于美国CLOUD Act的新动向，阐明数据本地化的立法所隐含立法管辖权冲突的可能性和危险性。

二、网络空间立法管辖权的新方向

云计算和大数据背景下，人们已经敏锐地察觉到全球互联网时代可能正在过时，因为各国正在为跨越国界的信息自由流动设置新的障碍。由于对隐私、安全、监视和执法的担忧，各国开始在网络空间架设边界，分割万维网。〔7〕过去的互联网边界管制，以网络犯罪条约对管辖权的调整为代表，试图将信息滞留在某个国家，压缩信息可被接触的范围，比如限制在网络空间阅览纳粹相关

〔1〕 各国数据本地化立法的具体理由和形式并不同一，产生的后果也有许多方面。欧盟之外，俄国和中国等国家也被认为采取了数据本地化的立法措施。Tatevik Sargsyan, “Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security”, 10 International Journal of Communication 225－227 (2016).

〔2〕 该案在美国，一般被称为*Microsoft Ireland Case*。联邦地方法院有几起拒绝微软请求的判决，但联邦第二巡回法院判决支持微软请求，美国政府上诉到联邦最高法院。*United States v. Microsoft Corp.*, 138 S. Ct. 356 (2017).

〔3〕 Stored Communications Act, Pub. L. 99－508, tit. II, 100 Stat. 1848, 1860－1868 (1986) (18 U.S.C. §§ 2701－2712).

〔4〕 Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018). 新增条款规定：不管通信、记录或其他信息是处在美国国内还是国外，服务提供商必须遵守本章义务，对处于该提供商占有、保护、控制下的客户或登录者的有线或无线通信和记录或其他信息的内容加以保存、备份或披露。

〔5〕 2018年4月17日，联邦最高法院直接判定该案诉讼已失去意义。Supreme Court of the United States, UNITED STATES, *Petitioner v. Microsoft Corporation*. No. 17－2. April 17, 2018.138 S.Ct. 1186, 18 Cal. Daily Op.Serv. 3481.

〔6〕 Shelli Gimelstein, “A Location-Based Test for Jurisdiction over Data: The Consequences for Global Online Privacy”, 1 University of Illinois Journal of Law, Technology and Policy 31(Spring,2018).

〔7〕 Anupam Chander, Uyên P. Lê, “Data Nationalism”, 64 Emory Law Journal 679 (2015).

的物品或利用盗版资源。与此不同，新一代网络边界控制则是以个人数据保护为中心，试图尽可能将所有个人数据掌控在一个国家领土之内或领土管辖权范围内。过去限制的信息相对狭窄，更多的是域外与本国法律或社会理念相冲突的内容，而新一代管制，则涉及商业和社会活动中极为广泛的个人数据。数据已经成为各种网络技术试图开拓的资源宝库，域内数据也就具有了重要的社会和经济意义。

正是因为如此，数据的本地化已经开始成为一个新趋势，为网络空间的立法管辖权冲突或调整提供了一个新的平台。一些国家已经采取了数据本地化措施，并对此制定了相应法律，而同时，新一轮立法管辖权的冲突也开始刺激人们的危机意识。各国数据本地化的形式不同，采取这些措施的理由也不同。尽管各国提供了数据本地化的各种立法管辖权论据，但应该注意到，数据本地化措施不仅可能引发国家之间的管辖权冲突，也可能会在采用这种措施的国家中产生限制甚至破坏安全、隐私、经济发展和创新的影响。〔8〕毫无疑问，各国政府有权并有责任确保其管辖内居民的数据在域内和在跨越国界时的隐私和安全，也可以采取多种方式实现这些目标。〔9〕

1. 数据保护成为大数据和云计算时代的立法焦点

大数据和云计算作为网络技术尤其是它们的结合运用，使个人数据保护逐渐成为各国立法的一个焦点。这两项技术的结合，不仅使数据收集和处理大规模化和自动化，而且也使数据储存和运用具有更高且能轻易跨越国境的流动性，让人们开始窥探到数据开发、利用和控制在全球市场上的潜在价值。而且，数据具有与其原有目的分离并不断被再生利用的特性，应该怎样界定数据主体对数据的权利也自然成为人们关心的重点。因此，在数据自由流动和个人权利保护之间找到适当的均衡点，也就显得极为关键。

大数据和云计算是两个不同但同时密切相关的网络技术。虽然云计算不是一项新技术，但它是提供需求服务的一种新方法，并不断且迅速地演变为不同的业务模式。〔10〕。最近十多年云计算市场的蓬勃发展，导致了国际一级的云服务数量的增加。云计算改变了网络服务现今的管理方式，为商务和科研提供了许多优势条件。而大数据的扩展，需要云计算的能力来支撑巨量的数据处理，利用云计算服务的分散式存储设施。虽然云计算和大型数据中有许多重叠的概念和技术，但它们还是有所不同。云计算直接转换 IT 体系结构，而大数据在上层运行，影响科学和商业决策过程所必需的分析和洞察。云计算和大数据的相辅相成对现实世界产生着巨大影响。〔11〕

从我们关心的视角看，云计算有两大特征，一是它具有很强的跨境潜质，不仅技术可能而且在成本与效应判断的驱动下常常以跨境形式出现。二是它提供的多种服务常常涉及数据收集和处理，而且数据的来源不以国家领土或地理为限而是取决于客户性质。它所带来的愿景在于通过有

---

〔8〕 Anupam Chander, Uyên P. Lê, *supra* note〔7〕, at 681.

〔9〕 云计算的治理有规范、管理手段、管理机关和被管理对象等各种变数，可采取的方式也多种多样。Rolf H. Weber, Dominic Staiger, *Transatlantic Data Protection in Practice* (Springer, Verlag Berlin Heidelberg, 2017), pp.6 - 9.

〔10〕 尽管没有统一的认识，云计算服务有以下三种相对成熟的模式。第一，软件服务(SaaS)，通常称为应用程序服务提供商模型。第二，平台服务(PaaS)。作为云计算提供的服务，它为开发人员提供一个平台，包括所有系统和环境，其中包含复杂网站应用程序的端到端的开发、测试、部署和托管整个周期。第三，基础设施服务(IaaS)。它通过网络提供诸如处理、存储、网站等资源服务。Nick Antonopoulos, Lee Gillam (eds.), *Cloud Computing: Principles, Systems and Applications* (Springer International Publishing, 2017), pp.4 - 6.

〔11〕 Marcelo Corrales, Mark Fenwick, Nikolaus Forg (eds.), *New Technology, Big Data and the Law* (Springer Verlag, 2017), pp.154 - 155.

线和无线通信，创建一个设备供应商、应用程序开发商、网络运营商、电信运营商和云服务/基础设施供应商的生态系统，以创造可预见的新的商业价值链，这不仅会加速每个领域的发展，而且能带来新的创新理念和服务。〔12〕

而另一方面，数据量的增长催生了大数据技术的发展。数字通信使许多信息变成容易存储和处理的数据，并且有了流动性和持久性，随着储存技术的成熟，数据量呈指数级增长。巨大量的数据不仅使IT专业人员面临着解决数据膨胀浪潮的挑战，也给人文社会学科带来了相当多的法律问题和利益问题。“大数据是高容量、高速度和/或高多样性信息资产，需要新的处理形式，以实现增强决策、洞察发现和优化流程。”〔13〕面对收集处理数据的新潜力，人们开始确信，知道得越多，也就越能控制社会进程，引导社会进步。大数据不仅让人们看清未来，而且能够让他们根据自己的需要来塑造未来。〔14〕 大数据对法律的影响，自然也就成为人们所关心的课题。这其中最有持续力的法律挑战之一就是个人数据保护。

就欧盟数据立法应对数据自由流通与数据保护的对峙来看，有三个重要举措值得特别关注，因为它们具有引发大数据和云计算时代立法管辖权冲突的现实性和潜在可能性。

第一，将数据保护视为基本权利。2000年12月，欧洲议会、欧盟理事会和欧盟委员会在法国尼斯颁布了欧盟基本权利宪章。宪章第8条规定：1. 人人有权保护有关他或她的个人数据。2. 此类数据必须在有关人员同意或法律规定的其他合法依据的基础上公平处理。每个人都有权查阅已收集到的关于他或她的数据，并有权纠正。3. 本规则的遵守须受独立当局的管理。2009年，里斯本条约授予宪章以法律约束力，进一步巩固了欧盟法中个人数据的基本权利地位。〔15〕

欧盟将个人数据保护作为基本权利的法律运作，造成了两个重大转变。首先，一些形式上涉及计算机技术发展管制的法律概念转换成形式上不涉及任何具体技术的权利。其次，“欧盟基本权利”这一标签的确立伴随着欧盟个人数据保护的发展，立足于长期以来与国家基本权利和国际人权有密切联系的欧盟法。其结果，欧盟的数据保护法由于与欧洲人权公约的联系而具有“人权”性质。在随后的发展中，这一特性的确立使欧盟个人数据保护最终获得基本权利的地位，并且对于逐渐去除作为解释欧盟数据保护法之关键权利——隐私权的神圣光环而言，具有重要的法律意义。〔16〕

基本权利的定性是欧盟数据保护基准的立足点，也是欧盟数据立法向世界各国提出的一大挑战。大数据时代，数据有必要从传统的个人隐私观念中剥离开来，形成一种构成新型社会价值的原子要素。其中不仅有人权侧面，同时还有尚待开发的社会、经济和政治侧面。数据保护法律制度的发展，应是顺应以大数据和云计算对数据的广泛运用而强化个人权利保护的必要举措。欧盟委员会在其制定的数字单一市场战略(Digital Single Market Strategy)中强调数据信息自由流通原则的重要性，主张在此原则下，除为确保个人数据之外，所有限制数据流通的障碍都必须清除，而不涉及自然人的所有数据都必须确保自由流通。GDPR就是体现数据自由流通与个人数据保护之间最佳均衡的法律文件。〔17〕 然而，GDPR所展示的这种均衡，能否承受得了对这种均衡有着

---

〔12〕 Nick Antonopoulos, Lee Gillam, *supra* note〔10〕, at 3.

〔13〕 Marcelo Corrales, Mark Fenwick, Nikolaus Forg, *supra* note〔11〕, at 20.

〔14〕 Serge Gutwirth, Ronald Leenes, Paul de Hert (eds.), *Reforming European Data Protection Law* (Springer Netherlands, 2015), p.4.

〔15〕 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer International Publishing, 2014), pp.1－2.

〔16〕 *Ibid*.at 263－265.

〔17〕 Rolf H. Weber, Dominic Staiger, *supra* note〔9〕, at 22－23.

不同追求以及数据技术发展所带来的压力，尚须留给实践去检验。

第二，数据的目的限制原则[GDPR 第 5 条 1(b)]。依据这一原则，在欧盟收集和处理数据需要明确界定其目的，并且这种数据不能用于与原始目的不相容的另一个目的。从基本权引申出的这一原则，对大数据应用在欧盟的发展将直接产生影响，因为可以说，大数据的根本就在于活用数据，为不同目的而进一步处理数据集，并以某种收集数据当时可能没有设想到的方式对数据进行分析利用。

目的限制原则源于欧盟理事会(CoE)(73)22 和(74)29 决议，并为后来的法律文件进一步阐述确认。1981 年欧盟理事会针对个人数据自动处理保护个人公约(108 公约)第 5 条引入了一套包括目的限制原则在内的更详细的数据保护原则，同时也规定目的限制原则允许在特定条件下的减损。第 9 条第 2 款规定，“当对本公约第 5、6 和 8 条规定的减损由缔约方的法律规定，并在民主社会中构成为以下利益所必要的措施时，这种减损应与允许：a. 保护国家安全、公共安全、国家货币利益或防止刑事犯罪；b. 保护数据主体或他人的权利和自由”。DPD 第 6 条规定了欧洲基本数据保护法原则，即公平与合法性原则、目的限制原则、数据最小化原则、数据质量原则和数据安全原则，而目的规范是该指令所确立的数据规则框架的核心内容。〔18〕

第三，限制数据向域外移送。GDPR 第 5 章对数据向第三国或国际组织的移送作了明确的限制性规定，并具体规定了允许移送的条件和管理制度。而且，遵守数据向第三国移送的法律规制，也是判断域内控制者和提供商处理数据行为合法性的一个重要指标。比如，告知数据主体数据移送[第 13 条(f)]以及移送相关的充分保护措施(第 15 条第 2 款)；数据处理者依法移送数据的义务[第 28 条第 3 款(a)]；保存移送数据记录的义务(第 30 条)。

如后所示，限制数据向域外移送是数据本地化的一个鲜明表征。在云计算背景下，其明显是一个人为的隔断数据全球性的举措，与数据可全球流动的物理特性相逆反，也与数据自由流通理念相悖逆，无论在立法管辖还是执法或司法管辖上，都可能刺激欧盟域外国家选择积极冲突和对抗。

2. 数据保护引发网络空间立法管辖权重心转移

大数据和云计算凸显了数据的重要，也将数据保护推到了各国开拓网络空间立法管辖权的前沿。立法管辖权的重心也就很自然地开始由注重域外网络行为转向域内，从而使传统的领土原则又获得了一次再生的机会。

在国际法上，管辖权问题很重要的一个方面就是如何在国家之间有效地分配管辖权，尤其是立法管辖权。〔19〕 就网络空间看，最重要一点涉及哪个国家对网络行为拥有充分且有效的立法管辖权。有了有效的立法管辖权，国家才能充分利用各种资源确保执行管辖权和司法管辖权的有效行使。由于各国法律发展之间的不平衡，时常会出现立法管辖权冲突。对这一问题，应该从消极冲突和积极冲突两个方面来理解。立法管辖权的消极冲突意味着一国依据国际法所认可的管辖权原理对网络空间实行了严格且广泛的法律管制，而其他可能受影响的国家尚未采取任何法律调整措施，实践上，它表现为一种潜在的管辖权冲突。积极冲突则是各国依据为国际法所认可的不同的管辖权原理积极地对同一网络行为实行规制所产生的冲突形态。无论是哪种冲突形态，都能造成无法有效确立立法管辖权，也即法律无法有效适用的情形。针对消极冲突，应该充分认识到其他国家有实施对抗性管辖权的权利和权力，采取自制态度；而对积极冲突，则需要在国际法上确

〔18〕 Marcelo Corrales, Mark Fenwick, Nikolaus Forg, *supra* note〔11〕, at 154 - 155.

〔19〕 Patrick Capps, Malcolm Evans and Stratos Konstadinidis (eds.), *Asserting Jurisdiction-International and European Legal Perspectives* (Hart Publishing, 2003), p.xix.

立能够调整这种冲突的法律规范和原理。因为,国家行使管辖权的权利只能由国际法决定,[20]而且,这种权利冲突也必须依据国际法来解决。[21]

以网络犯罪条约为代表的网络管辖权冲突调整,更注重域外网络行为对域内利益的侵害,管辖权冲突也就表现为各国对网络行为法律规制的不同,因此,对网络行为的规制就更需要国家之间积极的合作。具体来看,网络犯罪规制的问题意识集中在三个方面。第一,对域外网站所陈列内容的法律规制或法律适用所引起的管辖权冲突。Yahoo拍卖网站陈列德国纳粹相关物件所引发的法国与美国之间的管辖权冲突就是一个典型例子。第二,对域外网站上的行为规制而引起的管辖权冲突。如网上赌博、网络证券交易等的法律规制上的冲突。第三,对网络上交易活动的新型法律规制而产生的管辖权冲突。这包括网络交易的电子决算课税问题、网络时代知识产权保护问题等。[22]

对这些网络活动的法律规制直接导致了国家管辖权领土基础的动摇,因法律域外适用而产生的冲突也变得更加深刻。源于主权的管辖权始终以领土为基础。国际法上,领土原则可以说是原始的国家管辖权基础,除非受到明确的国际法制约,它能为国家之间的管辖权分配提供适当的法律基础。[23] 网络空间对领土原则的侵蚀是因为国家对网络空间没有确保有效主权的基础,表现为国家缺乏充分和有效的基础来对网络活动行使立法管辖权。这个问题现在依然存在,并没有因为网络犯罪条约和其他一些管辖权调整的国际合作而得到完全解决。

然而,在大数据和云计算时代,国家更注重的是以网络为中介的域内行为。有两个主要理由,一是作为个人权利的个人数据保护的国内法本质,二是数据储存处理行为技术上的全球特征,对此,国家只有立足其域内侧面才能构建有效的立法管辖权。数据本地化就成为法律规制一个重要的择优方式。当一些主要国家先行采取数据本地化的法律规制后,管辖权冲突就需要在数据本地化基础上展开新一轮的调整。把握这一新冲突和新调整的动向,不仅有益于理解主要国家数据保护措施的特征,也能有助于探索构筑有效的数据保护法律的基本策略。数据本地化的法律规制有足够充分的立法管辖权基础,因为它充分依据了最原始的国家管辖权原理,也即领土原则和国籍原则。其他国家很难依据国际法上管辖权原理来对基于本地化的数据管辖提出有效的挑战,而且,所有国家对数据本地化享有相同的利益,挑战他国基于本地化的法律规制也必然基于利益考量。不过,对具有超领土特征的网络行为采取越严格的法律规制,国家之间的立法管辖权冲突就越强烈,同理,法律规制的范围越广,冲突的可能性就越大。从数据保护的本地化方兴未艾和欧盟基于基本权利的数据保护基准的确立,可以预断,新一轮网络空间立法管辖权的竞合平台并不会毫无硝烟。

三、云计算和大数据时代的管辖权基础的本地化趋向

欧盟数据立法有很广泛的域外效力,对域外企业有很大影响,但却不是一个分析法律域外适

---

〔20〕 F. A. Mann, "The Doctrine of Jurisdiction in International Law", 111 Hague Recueil de Cours 10 - 11 (1964 - I).

〔21〕 Andrew L. Strauss, "Beyond National Law: The Neglected Role of the International Law of Personal Jurisdiction in Domestic Courts", 36 Harvard International Law Journal 415(1995).

〔22〕 对这一问题的研究,参见王志安「サイバー空間と国際法:実効性のある立法管轄権の確立を目指して」駒澤法学 1(2)2002年87 - 148页。

〔23〕 Ian Brownlie, *Principles of Public International Law* (Fifth Edition, Oxford, 1997), p.291.

用的适当素材，因为它并没有明文的域外适用的目的和条款。域内数据收集和处理行为以及域内数据保护才是它的核心所在，严格地说，对非“欧洲经济区”(European Economic Area，EEA)实体适用GDPR，不是因为其域外行为或这些行为的域内效果，而是它在域内收集和处理数据的行为或将域内数据移送到域外的行为。欧盟数据立法正是通过将法律严格适用于域内数据收集和处理行为，同时将域内数据打上鲜明的欧盟数据标签或国籍烙印，来追求对这些数据的持续且无地域限制的保护，创出了数据保护的新范式。这也是它对拥有数据保护这一基本权利的欧盟市民的承诺。这一新范式，从立法管辖权角度看，是将领土原则和国籍原则这些最为传统的基础原则加以新形态的适用，以强化对数据的实效保护，表现出很鲜明的数据本地化特征。〔24〕

1. 欧盟数据保护立法中的管辖权基础

欧盟数据保护立法的管辖权基础有两个方面，一是针对数据收集处理行为的性质，尤其是云计算时代这种行为能够跨境远程操控和自动完成的新特征，以明确的法定形式规定属于域内收集处理数据的情况，并对此根据领土原则确保法律的适用(GDPR第3条)。领土原则在这里不再只停留在源于领土主权而具有包括性，〔25〕而是表现在法律规定的域内具体行为上。二是为确保欧盟管辖下的个人数据得到持续且同等的保护，法律赋予域内数据欧盟“国籍”，在确保数据只能移送到具有法律所认可保护水准的域外或国际组织的同时，又依据国籍原则限制数据的二次移送(GDPR第44条)。

首先，我们来看一下GDPR对领土原则的精细化。在欧盟数据保护立法中，领土原则作为法律适用基础表现在其特别针对域内的数据收集和处理行为，而且，这些行为除了通过传统的域内实体或外国子公司的域内行为来确定外，还特别考虑到数据远程和自动收集处理的可能性和现实性，对区别于实体或子公司的处理数据的“营业机构”(Establishment)加以明确界定，并明确对“营业机构所在地”行使立法管辖。本来，DPD中还规定了通过域内“设备”(Equipment)处理数据的情况，并依据“设备所在地”确定法律适用范围。

针对数据处理可能涉及的多个复杂行为，DPD只关注在域内是否存在处理数据的实体、营业机构和设备，而且，数据处理行为并不要求针对一个完整的个人数据，有可能只需要涉及数据的一个或几个方面。因此，人们甚至关心，依据DPD第4条，非EEA的云计算用户或云计算提供商是否因为使用EEA数据中心或EEA的云计算提供商，或者通过在EEA居民的设备上保存cookie，而被要求遵守欧盟数据保护法。显然，这类法解释上的疑点说明，DPD管辖范围内的实体和管辖范围外实体之间的明确界定存在一定的不确定性。〔26〕也许是由于这一原因，GDPR只对营业机

---

〔24〕 实际上，作为领土原则辅助的效果理论(effects principle)是否能成为欧盟数据立法适用的基础，在WP29的意见中都尚是一个待研发的课题。WP 179 update of A29WP, “Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain”, 16/12/2015, pp.5－6. A29WP是依据DPD第29条规定组成的一个由EU成员国数据保护当局、欧盟委员会和欧洲数据保护监管机构代表构成的咨询机关。随着GDPR的实施，为欧洲数据保护局替代。A29WP公开了许多有关数据保护的法律和技术标准问题的意见。See https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinions-and-documents/, last visited 2018－11－28.

〔25〕 作为领土实体，只要国际法上没有明确的禁止规定，国家就能依据主权或领土原理行使管辖权。这也是欧洲各国所遵循的一个传统原理。Andrea Bianchi, “Comment” (on Jurisdictional Rules in Customary International Law), in Karl M. Meessen (ed.), *Extraterritorial Jurisdiction in Theory and Practice* (Kluwer Law International, 1996), p.83.

〔26〕 A29WP, Opinion 8/2010 on Applicable Law, WP179 (2010), p.6; Christopher Millard, *Cloud Computing Law* (Oxford University Press, 2013), p.220.

构作了明确界定[第4条(16)],却没有像DPD那样直接对通过设备处理数据的情况加以规定。不过,如后所述,GDPR也规定了一些域内营业机构处理数据之外的法律适用的情况。

第一,GDPR第3条第1款基本采用了DPD第4条(1)(a)的法律适用的判断标准,也即域内营业机构的数据处理或处理关联行为。它规定,"1. 本例适用于在欧盟内部设立的数据控制者或处理者的活动范围中对个人数据的处理,不论其实际数据处理行为是否在欧盟内进行"。从这个规定可以看出,域内营业机构处理权限范围的数据处理,考虑到云计算的存在,一方面不仅没有地域限制,同时,数据在同一营业机构中跨地域云计算之间的移动不作数据移送认定,而只是法定域内数据处理的一个组成部分。[27] 在这里,领土原则已经明显摆脱了地理限制,充分考虑了云计算的特征,以云计算营业机构所在地作为管辖其在网络空间的所有数据处理的立法基础。因此,这也可以看作是为适应云计算而对领土原则的一种重新建构。

DPD设想了设置在EEA以外第三国处理者的远程数据处理的情况。它的管辖权规定旨在,即使非EEA常设控制者在第三国进行数据处理,也能确保对与EEA有关的个人数据履行数据保护义务。[28] 根据第4条(1)(a)规定,如果数据处理属于在欧盟成员国领土上的控制者的营业机构上的活动范围,也即如果控制者在那里有营业机构,并在该营业机构的活动范围内处理了个人资料,那么,该成员国必须在国内对其适用DPD。如果EEA成员国的数据保护法以此营业机构为基础适用于其控制者,则无论数据处理地方在世界何处,包括通过使用云计算,法律都要求适用于在该营业机构活动范围内对所有个人数据的处理。如果法律适用基于营业机构,控制者必须就其即使发生在EEA以外的所有有关个人数据的处理,遵守有关的数据保护法。

也就是说,DPD第4(1)(a)条对适用法律规定了两阶段的判断标准,一是在欧盟成员国的领土上,控制人是否有"营业机构"? 二是否在该营业机构的活动范围内处理了个人数据? 如果两者的答案都是肯定的,那么该成员国的数据保护法适用于这种处理,无论处理发生在什么地方,也即无论是在EEA之外还是之内。针对DPD的适用,在判断营业机构的各种活动时,WP179认为应考虑到三个因素:在处理个人数据上营业机构参与活动的程度、活动的性质和数据有效保护的目标。[29]

实践中,这些判断法律适用的基准也得到了印证。德国法院处理过两起涉及社交网络服务脸书的数据保护管辖权案件。[30] Schleswig-Holstein数据保护局命令认定,脸书阻止使用虚假个人数据或虚假名字注册的用户的账户实名政策违反了规定有假名或匿名使用权利的德国数据保护法。但法院认为,脸书的德国子公司的活动仅限于广告和市场营销,德国用户的个人数据也没有被处理,因此在德国营业机构的活动范围内没有处理此类个人数据,不能适用DPD,保护当局无权下令。A29WP指出,DPD下的"营业机构"概念应遵循欧洲法院就根据《欧盟运作条约(TFEU)》第50条提供服务和营业机构设立自由所做出的判例法。在欧盟法院看来,营业机构要求至少有

---

〔27〕 Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st ed., Springer International Publishing, 2017), p.24. 此外,在分析依据设备来确定法律适用[DPD第4条1(c)]问题时,A29WP就清楚认识到,这里很难区别数据收集处理和数据移送(DPD第25和26条)。WP179 (2010), p.25.

〔28〕 对DPD中这一概念的分析,参见WP179(2010), pp.12-17。

〔29〕 WP179 (2010), p.14.

〔30〕 *Facebook Ireland, Facebook Inc. v Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Az 8B 60/12, Judgment of 14 February 2013 and Az B8 61/12, Judgment of 14 February 2013.

一个有一定程度的持久和稳定的工作人员的办公室，提供特定服务所需的人力和技术资源是永久性的。〔31〕

第二，相对于DPD，GDPR第3条第2款对领土原则适用作了更细致也更虚拟的限定。它规定，本条例适用于如下相关活动中的个人数据处理，即使数据控制者或处理者在欧盟内没有据点：(a) 为欧盟内的数据主体提供商品或服务——不论此项商品或服务是否要求数据主体支付对价；或(b) 对发生在欧盟范围内的数据主体的活动进行监控。该款所设定的是在欧盟域内没有营业机构而通过一定方式或手段的特定数据处理行为，也是对DPD针对通过域内“设备”处理数据而规定适用该指令的一个修正或限定。

如上所述，在域内营业机构的数据处理行为之外，DPD第4条(1)(c)还为成员国将其数据保护法适用于云服务提供了一个颇具争议的基础。也即，成员国的数据保护法，除只是为了过境通过共同体领土的情况外，如果控制者使用在该国领土上的自动或其他设备处理个人数据，就能适用于未在共同体领土内拥有营业机构的控制者，并且，这里处理的个人数据不需要与EEA的个人有关。也就是说，数据的位置或数据的物理操作不是决定性的。与数据有关个人的公民身份、住所或居住地也无关紧要。但是，一定程度上与处理地点相重叠的处理方法却十分重要。〔32〕

GDPR对DPD的修正，主要是因为处理数据的设备难以准确界定以及对数据有效保护含义的重新认识。DPD的“设备”概念有很大的争议。设备可以不需要是坚实、有形或实质性的东西，实践中甚至能有过分广义的理解。法国和德国版本的DPD使用“手段”这一更广泛的表述。根据WP179，设备概念的解释很广，它援用了手段的含义，甚至包括调查或调查表。如果控制者利用计算机、终端、服务器、存储硬件或在成员国领土内的数据中心处理个人数据，则该成员国的数据保护法将适用。对于“使用”概念，WP179认为，控制者没有必要对设备行使所有权或完全控制权。但一般认为，控制者必须对设备/手段有一定程度的控制，虽然WP179似乎采取了一个非常广泛的“使用”概念：控制者的某种活动和控制者处理个人数据的明确意图。〔33〕

针对建立在EEA以外的控制者和处理者，依据其域内设备对数据的处理来确立立法管辖权的做法，经常被批评为不透明和不可行。实践中，DPD适用范围的解释极为广泛。比如，涉及显示虐待残疾学生的视频被意大利青年上传到谷歌视频的谷歌案中，法院就确认谷歌意大利子公司本身构成位于意大利的工具或手段，无论其服务器位于美国或谷歌欧洲总部的爱尔兰。〔34〕A29WP在WP179中也承认，即使与EEA的联系有限，设备连接因素也可能触发法律适用，因此显然需要对它进行改革；并承认这个依据有不良后果，因为欧盟立法会被视为能普遍适用或域外适用，但建议保留如合法性和安全性等一些数据保护原则，以防止在欧盟有相关处理数据设备却回避欧盟数据保护法适用的情况。WP179并特别提到利用与域内的联系或以域内个人为目标的数据处理来确立对域外网站的法律适用。〔35〕

这些批评和改善意见，也就成为GDPR放弃依据通过设备处理数据来确立法律适用范围的做法，改用依据特定域内数据处理行为来确保法律适用，这一方面将法律适用范围扩大到域内营业机构的数据处理行为之外，同时又对这种扩大作了一个明确的限定，而且，即使在这种限定下，

〔31〕 WP179 (2010), p.11.

〔32〕 Christopher Millard, *supra* note〔26〕, at 220.

〔33〕 WP179 (2010), pp.20 - 21.

〔34〕 A29WP, Opinion 1/2008 on Data Protection Issues Related to Search Engines, WP 148 (2008), p.10.

〔35〕 WP179 (2010), pp.23 - 25.

GDPR也确保了十分广的适用范围。[36] 在我们看来，这一规定的立法管辖权基础虽然依旧归属于领土原则，但却明显具有将网络行为人为地隔断、强调该行为域内侧面的域内效果，也即涉及数据收集和处理的销售或服务或监控行为，显现出一定的基于效果理论的法律域外适用特征，对针对欧盟地域以及无地域限制的网络营销以及通过网站收集数据都将产生直接且巨大的影响。在今天，效果原理在国际法上也已经被广泛接受，[37]但历来重视领土原理的欧洲似乎对效果原理有一种本能的逆反心理，GDPR第3条第2款也许是这种心理的反应，其结果颇有对领土原则过度虚拟之嫌。当然，在数据保护领域之外，就针对域内具体目标的网络行为选择行使立法管辖的做法并不少见。

第三，GDPR第3条第3款继承了DPD第4条(1)(b)的规定，确保了欧盟在国际法上拥有的剩余领土管辖权。Recital 25提到了对设置在域外使领馆中的控制者适用GDPR的情况。WP179也提到了对设置在成员国使领馆中的控制者依据国际法免除适用DPD的情况。[38] 从对DPD的研究来看，这一规定还涉及确认成员国的数据保护法可根据国际法适用于在该成员国领土或在悬挂某一成员国国旗的船舶或飞机上没有营业机构的控制者。这可能主要与云计算的展开形式有关，例如，成员国领海外停泊的船舶上建立数据中心的情况。实际上，谷歌已经在美国获得了使用海水发电和制冷设备的专利。[39]

其次，欧盟数据立法在通过域内的数据收集和处理行为确立管辖权的同时，还考虑到网络空间尤其是云计算的特征，通过对国籍原则的扩张适用加强对域内数据被移送到域外时的保护，尽管这种保护不是直接依据国籍原则来适用欧盟自身的法律，而是对源于欧盟的数据打上受欧盟法律保护的烙印，通过对数据向域外移送规定具体的条件，要求接受数据移入的国家/企业和国际组织尊重欧盟对数据保护的基本理念，并将判断这种尊重是否充分的权限牢牢掌握在欧盟自己手中。不仅如此，欧盟对移送到域外的数据的二次移送也保留了制约的权限，使被赋予欧盟国籍的数据间接地受到欧盟立法的普遍性保护。其中，移送包含二次移送的规定，是GDPR对DPD的一个明文弥补和发展。在欧盟与美国之间安全港协定履行过程中，二次移送的管辖成为DPD解释的一个争议点。美国方面曾主张，个人数据一旦正式移送到安全港，此后仅受美国法律和安全港规则制约，而欧盟监管机构则认为应依然受DPD规制。[40]

GDPR第44条也没有具体定义数据移送，只是规定数据向域外的移送以及在域外的二次移送受法律制约。在A29WP看来，将个人数据传输到EEA以外的服务器就是DPD目的的受管制数据移送。因此，在考虑是否在云操作中发生数据移送时，应首先确定用于数据处理设备的地理位置，实际上也就是提供云服务的数据中心的位置。

原则上看，这种法律规制依然是针对行为，也就是数据移送行为，但在我们看来，它是对传统的国籍原则的创新利用，通过将域内数据打上受欧盟法律保护的烙印，来挑战希望接受欧盟数据移入各国(或实体的国籍国)或国际组织的数据保护的法律基准。因为对移送规制的目的在于“为

---

〔36〕 Paul Voigt, Axel von dem Bussche, *supra* note〔27〕, at 26.

〔37〕 Jason Coppel, “A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law”, 6 Leiden Journal of International Law 73 (1993).

〔38〕 WP179 (2010), pp.18.

〔39〕 对这种海上数据中心在国际法上地位的分析，见 Steven R. Swanson, “Google Sets Sail: Ocean-Based Server Farms and International Law”, 43 Connecticut Law Review(2011)。文中强调，尽管执法上可能更加困难，相关国家依然能依据国际法对这种数据中心行使有效的立法管辖权(p.751)。

〔40〕 Christopher Millard, *supra* note〔26〕, at 226.

了保证本条例对于自然人的保护程度不会被削弱”〔41〕。尽管它不是一个域外适用条款，但这种挑战是深远的。一方面，它将欧盟数据保护的基本原理，作为一个国际标准要求所有接受源于欧盟的数据的国家和企业尊重，这让人仿佛看到昔日国际法上在外国人权利保护上国际标准和国内标准之争议的再现。另一方面，更为重要的是，欧盟数据保护法不是数据保护观念起步时仅仅针对行政机关对个人数据的处理，而是完全针对商业目的的数据收集和处理，因此，它对新网络技术下数据的运用可能会形成巨大的制约。尤其是，这可能使数据技术在与欧盟法律不同的国家开发的数据运用模式无法顺利在欧盟区域内实施。在某种意义上，甚至可以认为，在现行立法上欧盟是通过将数据保护定性为基本权利而对数据加以严格的保护，但这种立法的背后却隐含着大数据技术背景下对数据的开发利用新模式的法律调控。

数据域外移送的立法管辖权基础并不是表面那么简单，过于广泛的法律规制可能在实践中让规制仅仅成为一种形式，而不能起到实际作用。这必然要求数据保护立法，将重点放到数据在没有充分保护水准情况下的域外被访问利用上，因为有些移送实际上意味着数据公开。〔42〕这也是分析数据移送立法管辖权合理性和正当性的关键所在。这是因为数据域外移送定义十分复杂，需要充分考虑到网络空间以及云计算的特征，域外移送定义的具体外延呈多样性，有的涉及域外访问，有的却不涉及。DPD 限制数据域外移送的规定出台后，域外移送应该怎样规制也就成为一个争议的焦点，并在实践中逐步确认问题的本质所在，也即确保个人数据的保护标准不会因为被移送到域外而被降低削弱。可以说，从 DPD 到 GDPR，数据的域外移送也经历了一个细化立法管辖权基础的争议。

第一，由于域外云计算提供商可以不通过任何营业机构或实体设备而直接通过网站收集域内数据，并直接储存在域外数据中心；如果对这种数据处理也作为数据域外移送处理，其结果可能是，DPD 实际上阻止非 EEA 云提供商向 EEA 的用户提供远程服务。欧盟数据保护法的可执行性也会引起严重问题。尽管欧盟法能否在实践中对非 EEA 实体强制实施，是一个不同的问题，〔43〕但毫无疑问，确保有效立法管辖权却是非常重要的第一步。

欧洲法院在 Bodil Lindqvist 案中指出，将个人数据上传到网站上视为移送数据给第三国，将导致不切实际的结果。如果指令 DPD 的解释意味着每次将个人数据加载到互联网站上，都构成向第三国移送数据，并且这一转让必然是向有访问互联网所需的技术手段的所有第三国转让，那么，DPD 第 4 条规定的特别制度就因特网上的业务而言将必然成为普遍适用的制度。这样一来，如果委员会根据 DPD 第 25(4)条发现即使只有一个第三国没有确保数据得到充分保护，会员国也有义务防止将任何个人数据放在因特网上。〔44〕

第二，也正是因为如此，数据域外移送的定义中，第三方对数据的访问逐渐成为规制的焦点。在这里，值得注意的是，德国联邦数据保护法将“移送”定义为“向第三方公开个人数据，也即通过数据处理储存或获得数据，以便(a)将数据发给第三方或(b)第三方查看或访问可供查看或访问的数据”。不过在德国，也有监管机构似乎认为云计算必然涉及数据移送。

针对这种情况，有学者认为，DPD 的规则应侧重于限制未经授权的访问，而不是限制数据的输

---

〔41〕 GDPR Recital 101. GDPR 的条文和各条的 Recital 可参见 http://www.privacy-regulation.eu/en/index.htm。

〔42〕 Christopher Millard, *supra* note〔26〕, at 225.

〔43〕 *Ibid.*, at 220.

〔44〕 Case C-101/01 Bodil Lindqvist [2003] ECRI-12971.

出。换言之，最重要的不是存储信息的位置，而是谁可以阅读它，也即谁能够以可理解的形式获得对它的访问。在数据被要求加密且解密密钥管理安全的地方，数据的位置应该无关紧要。即使此类加密数据存储在第三个国家，未经授权的人员也无法以不使用密钥就可理解的形式访问数据。DPD的假设是，数据可以被第三国的人访问，仅仅是因为数据存储在那个国家，这种假设不仅因互联网更因为云计算而难以维系。〔45〕

2. 数据保护本地化与立法管辖权冲突

欧盟数据保护立法采取了数据本地化手法，整体上看，由于它立足于领土原则和国籍原则，有相对稳定和充分的立法管辖权基础，能抵御域外国家的立法管辖权挑战。反过来说，只要其他国家没有因为欧盟立法的制约而需要通过积极对抗才能保障的重大利益，通常会容忍这种立法主张，因为它们自身也需要并实际上也大都采用这种手法来确保本国管辖权下的个人数据。立法管辖权的积极冲突的背后常常是难以调和的国家之间重大利益的对峙。〔46〕 因此，对抗或排除立法仅限于个别情况。不过，由于新型的立法管辖权的展开，为回避其所带来的冲突也有必要进行一些具体的国际调整与合作。实际上，欧盟数据保护立法也注意排除管辖权冲突的危险，在现有国际合作基础上积极构筑与他国的合作措施，防止发生他国为维护重要的国家利益而不得已积极对抗欧盟数据保护立法的情况。

美国是云计算和大数据技术的发达国家，原则上选择了容忍欧盟基于数据本地化的保护立法，并积极与欧盟执法机关之间展开了必要的合作，以保障本国企业在欧盟数据市场的地位。欧盟与美国之间的安全港的构建就是一个很好的例子。但同时，美国也开始注重加强对新时代数据的掌控，甚至与数据本地化手法相反，直接在特定数据立法中明确规定域外适用，对数据实行全球索求。美国国会对SCA的最新修改就是一个十分强烈的信号。

首先，我们先来看一下美国对欧盟数据立法的认可。面对DPD，为调整与欧盟在数据保护上存在的巨大差别，1998年美国就已经与欧盟达成合意，为达到DPD第25条所规定的数据域外移送所要求的适当保护标准，设立了一个自我监管制度，允许美国企业参与“安全港”计划，确保包括云提供商在内的美国企业能从欧盟进口商业性个人数据。尽管是两国之间的合意，安全港协议对美国公司向欧盟域外移送数据规定了严格的条件。联邦贸易委员会有权力执行安全港制度，不过似乎并没有严格去处理违规案件。〔47〕

而且，2013年6月，受棱镜事件影响，欧盟委员会决定对安全港决定重新认定。而在这个过程中，针对依据脸书安全港决定进行的数据移送，Schresms以数据保护专员为被告，在爱尔兰提起诉讼，审案的爱尔兰高等法院请求欧盟法院做出先决判决。2015年10月6日，欧盟法院做出了该安全港决定无效的判决。〔48〕 法院判定，该案所涉安全港的决定相比个人隐私权更注重国家安全和公共利益，对被转移数据的主体个人的基本权利保护没有提供有效的保障。因此，不能认为，它与欧洲法律秩序下保障的基本自由的保护水平本质上相同。尽管安全港的认定标准变得更严，美国依然选择了与欧盟合作。2016年2月，美国商务部与欧盟委员会重新达成被称为“隐私权之盾”的

〔45〕 Christopher Millard, *supra* note〔26〕, at 276.

〔46〕 A.D. Neale and M. L. Stephens, *International Business and National Jurisdiction* (Oxford, 1988), p.15.

〔47〕 John Schinasi, “Practicing Privacy Online: Examining Data Protection Regulations through Google's Global Expansion”, 52 Columbia Journal of Transnational Law 600 - 603 (2014).

〔48〕 *Maximillian Schrems v. Data Protection Commissioner*, CJEU, Case C - 362/14, October 6, 2015., para 73.

数据移送框架合意。[49]

GDPR 第 45 条第 1 款维持了 DPD 对数据移送的限制，确认只有当欧盟委员会做出认定，认为相关的第三国、第三国中的某区域或一个或多个特定部门或国际组织具有充足保护，才可以将个人数据转移到第三国或国际组织。而且，该条第 2 款对评估保护程度的充足性所需要考虑的因素作了明确规定，相比 DPD 的规定，更加具体明确，并侧重强调(a) 关于公共安全、国防、国家安全、刑法和公共机构访问个人数据的一般性与部门性立法；(b) 要求设立独立监管机构，保证数据保护规则的实施；(c) 明确要求接受数据二次转移的国家或机关具有充分的数据保护水准。其中(a)的规定，就考虑了 Schrems 判决，进一步加强了对安全港的认定管理。而对二次转移的规定是对 DPD 的完善，弥补了 DPD 规定下审查标准的缺陷。

美国对 DPD 和 GDPR 的容忍，显然与欧盟数据立法的坚实且正当的立法管辖权直接相关。但这却并不意味欧盟数据立法没有引起管辖权冲突的潜在危险性。Schrems 案的判决表明，欧盟数据保护标准的向外扩展很有些“数据帝国主义”的味道。[50] 更重要的是，云计算和大数据技术对数据的开发利用还刚刚起步，而追求数据利益的新的开发模式完全有可能会要求变更欧盟的保护原则和基准，到那时，国家之间围绕数据立法的冲突就将显现出来。事实上，欧盟数据立法的管辖权基础虽然坚实，但却远远达不到具有排他性的程度。而且，还应该注意到，在与国家主权真正相冲突的事项上，对各种管辖权原理作优劣排位的做法在理论上都不可能行得通。[51]

其次，来看一下美国在应对欧盟数据立法时所显示的对数据未来掌控的决心。从上述对欧盟立法的容忍可以看出，美国没选择直接用对抗立法来消除欧盟立法的域外影响。然而，针对欧盟数据立法可能制约美国执法机关对美国企业储存在欧盟域内数据的利用，美国决然地选择了要求美国云计算运营商承担依法储存和披露全球范围数据的义务，并至少具体明确了犯罪取证执法命令的域外适用。尽管 SCA 只是美国相对分散的数据立法中的一个并不占据主要地位的法律，[52] 然而，对美国云计算运营商数据储存和披露的全球化要求，暗含着美国选择与欧盟数据立法全面积极冲突的危险。

数据全球化在美国成为立法现实的一个重要契机就是微软传唤令案。微软传唤令案中，美国执法机关怀疑微软客户的电子邮件中有贩毒证据，依据 SCA 授权传唤微软，下令要求提交电子邮件内容。微软提供了一些无内容的记录，但提起诉讼要求撤销传唤令，理由是该内容存储在 SCA 的领土适用范围以外的服务器上，也即在爱尔兰。第二巡回法院根据数据存储位置对请求进行分析，认定问题的关键取决于使用 SCA 传唤令检索海外储存的记录是否违反了该法否定域外适用的

---

〔49〕 European Commission, “EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU - US Privacy Shield”, February 2, 2016, available at http://europa.eu/rapid/press-release_IP-16-216_en.htm.

〔50〕 将数据保护标准强加给美国，被认为是侵害了美国国家主权，因此，EU 实质上也就在推行具有帝国主义伪装的数据保护立法。Liane Colonna, “Prism and the European Union's Data Protection Directive”, 30 John Marshall Journal of Information Technology & Privacy Law 50(Fall/Winter 2013).

〔51〕 M. Koskenniemi, “The Politics of International Law”, 1 European Journal of International Law 14 (1990).

〔52〕 美国数据保护立法与欧盟的不同点及其分散式立法的概述，参见 Paul Lambert, *Understanding the New European Data Protection Rules*(Auerbach Publications CRC Press, 2018), pp.12-15。

推定。这一推定源于联邦法规除非有明显的相反意图只适用于美国域内的判例法原则。〔53〕法院在判决中认定,存储在国外的数据超出SCA传唤令的范围,该法没有规定SCA传唤令的域外适用,而且使用传唤令迫使微软将储存在爱尔兰的记录带进美国以作为执法证据构成授权条款的域外适用。〔54〕

微软的暂时胜诉,引起了很大的震动,也将联邦最高法院逼进了两难局面。因为人们清楚地看到,最高法院必须在两个具有深远影响的立场之间进行选择。一方面,微软胜诉的判决可能会过度限制合法的执法调查,甚至会迫使官员向外国政府请愿要求提供有关美国公民的记录。另一方面,政府胜诉的判决将向世界宣告,美国执法人员可以访问任何地方的其国内企业持有的数据。〔55〕尽管声援微软的立场不少,也提供了相对充分的主张依据,但政府方面对第二巡回法院的判决采取了强烈批判的态度。因为判决挫败执法机关为获取证据所作的努力,特别是调查中的受害者、嫌疑人和账户持有者都在美国。联邦政府反复强调了SCA所规定的向政府披露信息的义务,以及在微软案之前对该义务基本遵守的事实。〔56〕不过,司法部官员和学者也建议修改SCA,以便该法能维持或明确域外适用。〔57〕应当注意到,代表欧盟的欧盟委员会作为法院之友对欧盟数据立法在该案背景下的意义作了明确陈述。陈述主要有两个方面,一是微软受命将要提供的数据,属于欧盟数据立法保护的范围。二是,美国执法机关仅凭单方面的权限不能合法地命令从欧盟域内移送数据,必须经合理程序与欧盟展开新的合作,因而其实际上要求美国联邦最高法院在解释美国数据立法域外适用时也采取其一贯的自制态度。〔58〕而且,从GDPR第48条的具体规定以及对该条的理解来看,依据修改后的SCA所发的传唤令依然需要与欧盟之间达成新的合意。〔59〕

最终,美国国会为联邦最高法院解了围,基本上采纳了司法部的建议,制定CLOUD Act,直接规定了SCA的域外适用。如上所述,该法针对美国的数据企业,规定了数据全球化原则,要求这些企业依法储存和披露其全球范围的数据。这一方面解决了眼下域外取证中的法律域外适用问题,同时,也为将来具体挑战数据本地化的各国立法搭建了一个法律平台,也即针对国内企业行使依据国籍原则的立法管辖权,将以云计算为基础的数据全球化直接纳入国内法规制范围。

从围绕微软传唤令案所展开的美国对域外取证的思考和应对,我们可以清楚地看到美国开始针对云计算的特征有意识地将国内立法的适用范围扩大到域外,甚至是积极制定对抗其他国家基于数据本地化政策的数据保护立法。用法律明确规定数据保存和披露义务的域外适用的做法,是

---

〔53〕美国判例法认定法律域外适用的判定分两步走。第一阶段,法院确定法律规定是否明确允许域外适用。如果规定在这方面不明确,法院仍必须确定法律规定的"适用"是否构成域外适用。第二阶段,根据构成有关法定条文的焦点"领土事项或领土关联"审查请求。*Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010) and *RJR Nabisco, Inc. v. European Community*, 150 F. Supp.2d 456 (E.D.N.Y. 2001).

〔54〕In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, (2d Cir. 2016), pp.221 - 222.

〔55〕Andrew Kirschenbaum, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", 86 Fordham Law Review 1947 - 1949 (March, 2018).

〔56〕Reply Brief for the United States, Microsoft Ireland, No. 17 - 2, Feb. 13, 2018. 2018 WL_835269.

〔57〕Andrew Kirschenbaum, *supra* note〔55〕, at 1953 - 1954.

〔58〕Brief of the European Commission on Behalf of the European Union as *Amicus Curiae* in Support of Neither Part, Microsoft Ireland, No. 17 - 2, pp.5 - 6. 2017 WL 6383224.

〔59〕Jennifer Daskal, "Microsoft Ireland, the Cloud Act, and International Lawmaking 2.0", 71 Stanford Law Review Online 11 (May 2018).

否会引发与欧盟数据保护规则的直接冲突，尚需要进一步考察分析。但至少，包括网络犯罪条约在内的现行域外犯罪取证的国际合作并没完全消除 GDPR 对数据域外移送限制所带来的制约。不仅如此，对数据保存和披露义务的全球性规定，说明美国实际上与欧盟异曲同工，不是通过国际法，而是通过国内法，凭依并充分利用云计算技术全球展开的特征开始抢占数据规制的制高点。因为，依据该法，美国还限制其提供商向外国政府提供数据，并且，为加强对数据的管控和利用，允许在司法协助协定之外，与其选定的政府之间达成有严格限制条件的数据移送协定，其中包含对隐私和个人自由提供充分的实体法和程序法的保障。〔60〕

四、结　　语

领土管辖权或领土原则在 17 世纪与领土国家一起出现。技术进步减弱了领土原则的重要性。到今天，领土原则不再是一个分配管辖权的可靠指南，不仅是因为很难确定事件和行为的领土边界，而且还因为管辖权意义上的领土本身是一个法律上易于操纵且不断变化的概念。其结果，具有很强建构性或虚拟性的领土原则从来没有解决管辖权冲突，而只重新表述这种冲突。很显然，欧盟数据立法对个人数据的本地化，很重要一方面就是对领土原则的一种新型虚拟，因为它隔断了收集处理数据的地理范围，仅将其域内侧面作为规制的焦点。同时，它也是对国籍原则的一种新型虚拟，让数据带上国籍印记，要求其他国家认可数据保护标准。

可以说，虚拟性或构建性的领土化本身就属于严格的领土原则传统的一部分。即使 70 年代由美国司法和立法开拓的效果理论，也可以看作是虚拟的领土管辖权，尽管它不是依赖地理位置唯一性，而是依赖颇为分散的域内效果。而新型的国籍原理的虚拟，强调的是“联系”或“关联”，这一方面是为回避领土原则的制约，将数据保护标准扩张到域外的一种做法，同时又与领土原则保持一种特定的联系。归根结底，管辖权原理的多样性和多面性表明了国家管辖权之“迈达斯接触（迈达斯的点金术）”的特征，也就是说，无论国家做什么，国家采取何种行动，它这么做是因为它有责任维护其基本价值。〔61〕 追求这种基本价值是扩张适用范围的各种新立法的根本动机，也是国家之间立法管辖权表现为积极冲突的内在原因。然而，我们应该铭记，对应管辖权冲突单纯回归到传统的国家利益分析形式并不一定是最好的方法。〔62〕 美国在容忍和应对欧盟数据立法上所作的具体努力，值得认真评价。

数据本地化，从国际法角度看，并没有触及为法所明确禁止的管辖权行使方式，而且，因为是依赖于对领土原则和国籍原则的建构，有充分且正当的管辖权基础。然而，这种管辖权，相对他国的立法管辖权来讲，具有明显的重叠性和非排他性，欧盟域外国家不仅在物理上能对其管辖之下企业的欧盟域内数据处理行为行使管辖权，而且也具有充分合法和正当理由去行使管辖权。同时，不可否认的是，数据本地化是抗拒云计算和大数据时代数据能够全球化这一技术物理特征而展开的一种法律建构。并且，也已经出现了像美国这样顺应云计算特征，依据国籍原则对数据保存和披露设定全球性义务的做法。在这样的背景下，国家利益容易合理调整的领域，比如对网络

〔60〕 Jennifer Daskal, *supra* note〔59〕, at 12－13.

〔61〕 Peter D. Szigeti, “The Illusion of Territorial Jurisdiction”, 52(3) Texas International Law Journal 380－385 (2017).

〔62〕 Harold G. Maier, “Extraterritorial Jurisdiction at a Crossroads: An Intersection between Public and Private International Law”, 76 American Journal of International Law 317 (1982).

犯罪追诉的合作，管辖权的重叠性和非排他性并不会产生什么具体影响，但随着数据利用价值和方式的变更，重叠的管辖权就更可能成为积极对抗的焦点。此外，将数据保护视为个人基本权的思路在大数据和云计算时代是否真的有效可行，尚须时日来定。毫无疑问，数据本地化和数据全球化的立法管辖权竞合平台上已经升起狼烟。

Abstract Looking from the perspective of prescriptive jurisdiction in international law, it is quite clear that the EU General Data Protection Regulation holds an obvious characteristic of data localization. For the purpose of protecting the personal data as a fundamental right in European Economic Area, the GDPR defines very broad territorial scope for its application based upon the territorial principle of jurisdiction newly reconstructed to response to the era of Cloud Computing and Big Data. At the same time, it regulates strictly the transfer of data to the area outside the European Economic Area by using quite fictitiously the principle of nationality as its base for prescriptive jurisdiction. What would be the impacts of data protection laws based upon the idea of data localization and how to react to them have become new issues with broad concerns in international society. The United States of America, as a state with developed technologies in Cloud Computing and Big Data, has shown its great concerns with the EU data protection legislation. On one hand, for protecting the proper status of American companies in the world data market, it has engaged very cooperatively with EU to avoid the impact of EU data localization laws. On the other hand, when the impact of EU data protection laws restricting its law enforcement agencies has been felt, a new law with a clear extraterritorial application for American companies' global data preservation and disclosure has become its first and quick choice. As a result, the conflict of prescriptive jurisdiction in the era of Cloud Computing and Big Data has gradually become a real issue.

Keywords GDPR, Legislative Jurisdiction, Data Localization, Extraterritorial Application, Territorial Principle, Extraterritorial Transfer of Data

（责任编辑：黄韬）