

DOI: 10.15918/j.jbitss1009-3370.2021.9938

# 论数据保护法的域外效力

何叶华

(南京大学 法学院, 江苏 南京 210093)

**摘 要:** 受信息技术挑战、多元价值冲突与国内外规则互动关系等多方面因素的影响, 域外效力成为中国数据保护立法必须认真对待的法律问题。当前国际社会主要通过立法路径与司法路径扩张国内规则的适用范围, 其中, 司法路径一定程度填补了传统数据立法在域外效力问题上的缺失, 但具有一定局限。当本国数据保护政策具有明显扩张需求时, 立法有必要对域外效力问题作出直接宣示。直观来看, 数据立法的适用范围取决于一国主权的自主选择, 如果做全面考量, 域外效力的确定仍然需要经过国际法层面的审视。考虑到数据保护政策与参与全球数据治理的需要, 中国应在立法中确立域外效力条款, 以设立机构标准和效果原则为基础对外适用数据保护规则。在实施阶段, 应强化法院在适用域外效力规则中的作用, 支持法院综合个案事实对中国数据保护立法的效力范围进行解释, 从而与立法、行政机关之间形成良性互动, 推动中国数据治理体系的构建。

**关键词:** 数据保护; 域外效力; 国际合法性分析; 中国立场

**中图分类号:** DF9

**文献标志码:** A

**文章编号:** 1009-3307(2021)05-0161-08

近年来, 以欧盟一系列数据保护规制为代表, 国际社会兴起数据保护立法的浪潮<sup>[1]</sup>。中国数据保护起步相对较晚, 但通过颁布各项规范性文件, 数据保护立法进程在不断加快, 特别是 2019 年全国人大常委会正式将个人信息保护法纳入阶段立法规划, 一部数据保护专门立法呼之欲出。纵观世界范围内数据保护立法, 一个值得注意的立法细节是, 欧盟最新数据保护立法规定, 在一定条件下, 欧盟数据规则将适用于欧盟之外的数据处理者及行为, 以期实现本国数据保护以及数据市场开发利益的最大化。不仅欧盟如此, 其他国家数据立法也相继写入域外效力条款, 将法律规制的范围扩张到域外<sup>①</sup>。因此中国在数据立法将要出台之际需要作出抉择, 是否应当增添域外效力之规定。

一般而言, 国内法关注国内事项, 效力范围受制于一国主权领土, 适用于主权管辖权范围内的人、物和行为, 并不需要对效力范围问题作出特别规定<sup>[2]</sup>。但在国际社会实践, 已出现采纳域外效力规定的现象, 将本国领土范围之外的行为纳入本国内法规制范围, 如反垄断法、证券法等领域。可以大胆猜想, 数据保护领域是否属于这类特殊领域, 需要明确域外效力规定。回答这一问题, 不单取决于中国立法的自主选择, 还应将国际法理论与数据保护的属性一并谨慎考虑。目前中国学者更多关注国内法架构以及数据流转的国际协调等实体规则方面, 虽然也在论证中附带提出应当重视域外效力规定, 但对于国内数据保护法域外效力问题的国际法基础、中国立场选择等问题尚未形成充分讨论<sup>[3-5]</sup>。鉴于此, 本文将首先阐述数据保护法产生域外效力问题的现实基础, 再从实然层面探讨数据保护法域外效力实现的具体途径, 并论证在国际法层面的正当化基础, 最后综合分析中国在数据保护域外效力问题上的应对之策。

## 一、数据保护法域外效力问题的现实基础

自 20 世纪 90 年代以来, 互联网逐渐融入日常生活, 依托互联网科技进行信息收集、处理、转移的

收稿日期: 2020-03-08

基金项目: 国家社科基金项目“中国涉外民商事审判中选法规则的实证研究”(18BFX218)

作者简介: 何叶华(1990—), 女, 博士研究生, E-mail: heyehuabd@126.com

① 以欧盟数据立法为代表, 俄罗斯、澳大利亚、新加坡、南非、日本等国家数据保护法中均含有域外适用的规定。

② 目前国内关于个人数据保护方面的研究主要集中在民法、宪法、行政法、刑法等领域, 部分国际法学者对国际层面有所涉及, 但主要侧重于跨境数据流转的多边机制研究。

过程随之诞生,并在科技进步、文化交流、打击犯罪等方面发挥着积极作用。发展与风险同在。随着信息技术的广泛应用以及个人生活与网络世界的密切联系,原本形式上匿名、分散的网络数据可以通过技术分析处理合成“数据人像”,借助无处不在的网络数据记录准确锁定信息主体已经成为现实,个人生活由此赤裸裸地暴露在数据使用者面前,一旦泄漏将直接危及个人隐私安全<sup>[6]</sup>;与此同时,对数据利用者而言,个人信息不再仅仅是标识符号,而是作为一种新型资源,影响着公共管理、商业活动中的具体决策,促使其通过技术手段最大化地获取数据,进而实现数据背后的社会福利抑或经济价值。由此,数据利用行为与个人信息保护之间发生不可避免的冲突。对于上述问题,国内学者从隐私权的宪法建构与私法救济视角,试图将粗线条的综合立法与细化的特别领域立法相结合,自上而下为个人信息编织一张紧密的保护网,但忽略了一个重要因素,即数据保护法的效力边界问题。在数据全球化现实面前,通过国内法对个人数据进行的规制行为并非单一国家所特有,网络的无国界特点与各国立法上的分歧必然带来数据保护法律之间的交叉与真空,而这些冲突的本源与结果都指向了个人数据保护法的域外效力问题。

具体来说,对于个人数据保护法域外效力问题的关注主要基于三方面的考虑。

其一,网络信息技术的发展对以地理为边界确定法律效力范围的传统立法模式形成挑战。一般而言,一国的法律在本国主权范围内具有拘束力,效力边界相应受制于一国的物理空间<sup>[7]</sup>。在面对网络信息技术问题时,这一原则发生了根本改变。就技术层面,大数据的运用使网络服务提供者能够在全球范围内挖掘海量个人数据,另外结合云计算技术,数据中心将计算资源虚拟化,突破本地处理模式,在云计算终端完成网络服务的跨境分配与聚合<sup>[8]</sup>。表面上这种技术操作只是呈现出技术的跨境潜质,即网络数据资源的开发与分析架构很难局限在一国地域范围。但深入分析可知,大数据与云计算技术的应用实质上是在地理界线之外创设出一个虚拟网络空间<sup>[9]</sup>。在这一空间,个人数据的交换、存储与分析等行为具有全面的空间自由与弹性,和物理空间的地域关联甚微。因此当针对个人数据的行为规制与权利保护规则由物理空间延伸到网络空间时,地理因素不再构成单一的确定性标准,法律效力与国家主权界限之间的逻辑关系随之发生改变<sup>[10]46-47</sup>,个人数据保护立法的效力范围由此成为必须重新审视的问题。

其二,个人数据保护法域外效力问题的产生并不仅仅是科技进步引发的客观现象,更深层次原因在于,个人数据具有多元价值,价值利益的冲突与制衡促使国家通过扩张本国法律适用范围的单边方法,实现对个人数据最大限度的保护。数据保护对于个人信息主体而言,一端承载着人格尊严与隐私权利,需要法律的介入来限制个人信息的跨境流动,进而实现对个人信息者的良好保护;另一端,个人信息被视为宝藏资源,借助现代网络技术可以从海量信息中识别出消费者的需求与偏好,为经营者调整规模与转型升级提供行动指引<sup>[11]</sup>。信息利用者为获取经济利益追求个人数据的自由流转,因此与个人信息主体的数据权利保护形成牵制。可以说,个人数据保护法最核心的目标就是,“权利保护”与“数据利用”二者之间的平衡。将法律规制置于全球背景下,主权国家的绝对控制权力客观丧失,价值目标的实现变得更为复杂。平衡任务不再以单一国家主权为逻辑起点,而是需要对“本国数据权利保护”“全球数据市场竞争”“国家主权利益”等多元价值目标进行综合考量<sup>[12]</sup>。此外,结合权利认知、技术能力以及信息产业发展水平等方面的现实差异,各个国家在价值目标的选择与权衡中各自得出立足本国视角的最优解,除非根据既存共同规则来协调各国法律,主权国家将本能地通过扩张本国法适用范围以保障自身绝对利益的满足,由此引发的竞争与冲突使得各国数据保护立法必须在域外效力范围问题上作出妥当安排<sup>[15]179</sup>。

其三,各国在数据保护立法方面的积极作为,不仅仅代表一种立法走向,现象背后国内法与国际法的互动关系值得重视。以欧盟立法为例,其在数据规制立法领域一直发挥引领作用,尤其通过域外效力规则的设定,欧盟规则的适用范围得以扩张到欧盟域外<sup>[13]</sup>。这种通过国内法路径来实现国际层面规则协调,不仅制约私人企业的具体行为与合规成本,也实然影响到他国规则的设定乃至国际社会数据保护标准的形成<sup>①</sup>。尤其在数据保护领域国际共同规则尚未成型之时,国内法在国际层面实际发挥补充功能,更为完备、系统的国内数据保护规则意味着国内法将为国际社会中的行为提供更为充分的国内法依据,进

① 一方面在欧盟内部,1995年《欧盟指令》和2016年《一般数据保护条例》的核心内容大多来源于德国、法国等成员国的国内立法,另一方面在与第三国展开的跨境数据谈判协议中,也体现出欧盟规则的影响力。如2016年《欧美隐私盾框架》对美国企业规定了更为严格的数据传输与制裁规则,进一步强化对欧盟个人数据的保护与救济。

而主权国家在全球数据保护与共同规制中拥有更多话语权。反之,国内数据保护法倘若一直处于“失语”状态,也将失去与国际社会进行有效沟通与对话的机会。

综上,可以肯定,数据跨境流转趋势不可逆转,域外效力是数据保护立法必须认真对待的法律问题,继而有必要根据各国数据保护的立法与司法实践,对域外效力的实现途径进行分析。

## 二、数据保护法域外效力的实现途径

各国在数据保护具体规制方法及侧重方面存在众多分歧,但域外效力规则仍出现在多个国家立法文本与司法实践中。以欧盟、美国为代表<sup>①</sup>,数据保护法域外效力的实现主要遵循两种思路。一则对既有国内法规则进行扩张解释,从而达到对域外主体的规制效果。另一则直接通过立法明确规定数据保护法域外适用的范围。

### (一)司法路径

一般来看,各国在传统数据保护立法中根据属地原则进行空间效力的设定,即国内法效力及于一国主权领土范围之内数据主体、数据设备及数据处理行为,客观上排除数据保护法适用于域外的情况<sup>②</sup>。但伴随数据跨境特质的不断凸显与互联网公司的全球膨胀,在成文法仍然根据传统连结点成立立法管辖权,而对域外适用问题保持沉默之时,单纯对境内数据的有限规制难以充分保障数据主体的权利。司法实践于是对传统连结点进行扩张解释,借助域内规则约束域外实体的数据处理行为。

以2014年“谷歌公司案”为例<sup>③</sup>。该案源于西班牙用户针对谷歌公司及谷歌西班牙分公司提起的行政控告。在谷歌搜索引擎中输入个人姓名时,该用户发现其个人信息的债务清偿内容出现在网页搜索结果,因此以个人隐私权利受到侵犯为由,向西班牙数据保护局提出权利救济申请。随后西班牙数据保护局作出要求谷歌公司、谷歌西班牙分公司删除相关信息的行政决定。谷歌公司和谷歌西班牙公司不服该决定,遂向西班牙国家法院提起诉讼。由于该案涉及对欧盟规则的解释,西班牙国家法院随后提请欧盟法院对法律的适用作出初步裁决<sup>④</sup>。

根据欧盟95年指令第4条(1)(a)的规定,指令适用于“数据控制者在欧盟境内设立了营业机构,并在此营业机构的活动背景下所实施的个人数据处理行为”<sup>⑤</sup>。具体到本案,谷歌西班牙公司在西班牙有稳定的经营活动与安排<sup>⑥</sup>,当然满足指令第4条(1)(a)中的“营业机构所在地”标准<sup>⑦</sup>。需要进一步判断的是欧盟立法能否规范谷歌美国总公司的争议行为。若按照传统“营业机构所在地”标准,指令的效力范围限定在欧盟域内的营业机构所做出的数据处理行为,而本案中搜索引擎服务由谷歌美国公司排他完成,似乎可以规避欧盟指令的规制。对此欧盟法院指出,虽然谷歌西班牙公司并未直接承担个人数据处理,但其提供的相关商业广告与搜索结果出现在同一界面,广告位销售业务实际上是为谷歌公司搜索引擎服务获取商业利益的重要途径,二者之间具有无法摆脱的联系。因此即使个人数据处理行为不是由西班牙谷歌公司实施,也应当认定该行为是在西班牙公司的活动背景下完成,因此受到欧盟规则的约束。从以上表述可以看出,欧盟法院试图对以下概念进行扩张解释:第一,设立机构的认定从传统属地性质的注册地标准,扩张至在欧盟境内从事真实稳定数据活动的所有机构,并且不考虑该设立机构的法律外观;第二,“在该设立机构背景下”的数据处理行为,不仅包括由欧盟境内设立机构完成的数据处理

① 鉴于美国与欧盟在数据治理体系中处于主导地位并形成两大立法范式,本文重点探讨美国、欧盟的立法司法实践。

② Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12(2014)。

③ 该案适用的《欧洲议会和欧盟理事会1995年10月24日关于对与个人数据处理有关的个人保护以及此类数据自由流动的95/46/EC号指令》(Directive 95/46/EC,简称95指令)已经被2018年生效的《一般数据保护条例》(General Data Protection Regulation, GDPR)所替代,但本案涉及的条文在GDPR第3条第一款被保留,且欧盟数据保护工作组WP29针对谷歌案出具一份专门报告(Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain)用于明确95指令的适用。

④ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, 23 November 1995, No L 281/39。

⑤ Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14(2015)。

⑥ 欧盟法院在2015年Weltimmo案中进一步明确欧盟境内设立机构是一个宽泛的概念,不限于分公司、子公司等具体形式,只要数据控制者或处理者在欧盟境内通过稳定的活动安排实施了真实有效的数据处理,均应认定为在欧盟境内成立设立机构。



行为,也包括当境外数据处理机构与境内设立机构存在“无法摆脱的联系”时,发生在欧盟境外的数据处理行为<sup>①</sup>。由此法院突破以客观属地连接点为基础的传统标准,进一步将欧盟指令的效力范围从欧盟境内延伸至欧盟境外。

与欧盟法院针对属地规则的扩张阐释不同,美国法院在微软案中重点探讨以属人连接点为基础的国内法规则的域外适用<sup>②</sup>。在微软案中,美国缉毒局根据1986年《存储通信法》(Stored Communications Act, SCA)向纽约南区联邦地方法院申请搜查令,要求微软公司提供涉嫌走私毒品的犯罪嫌疑人的电子邮件账户及相关信息。由于数据信息存储在位于爱尔兰的服务器内,微软公司认为按照“数据存储地标准”,存储在国外的数据超出SCA搜查令的效力范围,因此拒绝向执法部门提供相关信息。初审法院则采纳“数据控制者标准”,认为微软是美国公司,且作为数据的控制者有能力调取,因此即使数据内容存储在美国境外,也应当适用SCA规则披露相关数据。不难看出,尽管立法并未对域外效力问题作出明确规定,初审法院以数据控制者为连接点,要求美国数据企业对其所掌控的全球数据承担披露义务,进一步认可了美国国内法的域外效力<sup>③</sup>。

## (二)立法路径

在全球信息自由流动的冲击下,数据保护逐渐成为各个国家所关注的焦点。而效力范围的界定直接影响着国内数据保护政策的实现,因此可以发现,除却对原有规则的扩张解释,立法机关根据本国政策考量直接明确域外效力问题已经成为一种普遍现象。

考察多国立法实践,包含域外效力问题的立法规定具体表现为:

第一,以利用境内数据处理设备为标准,确立本国法对境外个人数据控制者相关行为的约束。例如英国1998年《数据保护法案》(Data Protection Act 1998)、欧盟95年《指令》均有规定,当数据控制者在境内没有设立营业机构时,除传输目的之外,如果利用了境内的数据处理设备,那么数据处理行为也将受到法律约束<sup>④</sup>。该规则主要考虑到网络数据具有虚拟属性,境外数据控制者无需在境内设立营业机构就可以远程完成数据处理行为。为了避免出现数据控制者故意将经营地设立在域外并利用国内数据设备逃避欧盟法律规制的情况<sup>⑤</sup>,立法因此通过域内设备与相关数据处理行为之间的关联,将境外信息控制者纳入数据保护法的规制范围<sup>⑥</sup>。

第二,通过效果原则设定域外效力规则。以数据保护立法一直领先的欧盟立法为例,在保留95指令对于域内设立营业机构的规定之外,2016年通过的GDPR新增第3条第2款规定:“该条例也适用于在欧盟域内不存在经营机构情况下,数据控制者对欧盟境内数据主体进行的相关个人数据处理行为,如果数据处理行为:(a)是为欧盟境内数据主体提供商品或服务,无论该项商品或服务是有偿或无偿;或者(b)对欧盟境内数据主体的活动进行监控”<sup>⑦</sup>。该条款专门针对欧盟境外的数据控制者或处理者,其中对于“为欧盟境内数据主体提供商品或服务”的情形,GDPR绪言第23条补充说明,应从数据处理者或控制者视角,判断其是否明显具备向欧盟数据主体提供商品或服务的目的。这一规定体现出对传统属地原则的突破,或者说引入“效果原则”,即无论数据处理者是否为欧盟主体,数据主体是否为欧盟公民,处理行为发生在何地,一旦行为对欧盟实际产生或意图造成影响,都将受到欧盟规则约束<sup>⑧</sup>。类似的规定也出现

① 对于何种情况构成无法摆脱的联系,欧盟法院认为应当进行个案判断,并不局限于谷歌案中所体现的商业广告与免费引擎服务这种特定业务模式。

② Microsoft Corporation v. United States of America, 829 F.3d 197(2016)。

③ 值得注意的是,微软公司后上诉至联邦第二巡回法院,上诉法院以SCA并未明确规定域外适用为由,推翻初审判决,判定搜查令只能限制存储在美国境内的数据资料。但在联邦最高法院审理阶段,美国国会又通过直接修法重新肯定初审法院立场,明确了SCA的域外适用。

④ Data Protection Act 1998 c.29。

⑤ The Article 29 Working Party 5035/01/EN/Final WP 56, p.7。

⑥ 但由于数据处理设备的外延模糊,以及数据处理设备使用的不确定与偶然性,很可能出现国内规则适用于全球的极端情况,因此欧盟在最新数据立法中并未采纳该标准。

⑦ Regulation 2016 /679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95 /46 / EC (General Data Protection Regulation), 4 May 2016, L 119/33。

⑧ Guidelines 3/2018 on the territorial scope of GDPR(Article 3) version 2.0 (2019)。

在日本、美国等国数据保护立法条文之中<sup>①</sup>。

第三,依据数据处理器标准规定本国数据法的域外适用。在美国联邦最高法院审理微软案阶段,美国国会通过《澄清合法利用海外数据法》(Clarifying Lawful Overseas Use of Data Act, CLOUD)<sup>②</sup>,明确规定无论该通信、记录等信息是位于美国境内还是国外,美国数据服务提供商必须对其占有、保护、控制下的客户通信及记录等信息的内容加以保存、备份或披露。虽然法案仅适用于执法机关域外取证过程,但是考虑到美国数据企业的领先优势以及在世界范围内的跨境发展,实际效果是以属人连接点为基础确立域外效力规则,将美国企业掌握的全球数据均纳入管辖范围。

### (三)小结

综上所述,以美国、欧洲为代表,个人数据保护法的效力范围呈现出扩张趋势,无论是通过对原有域内适用规则的扩张解释抑或是经由立法直接予以肯定,均可以实现数据保护法的域外适用。但深入分析,两种路径的选择实则对应着不同的历史背景与现实需求。传统数据保护立法一般根据属地连结点行使立法管辖权,具体规制本国领域内的数据主体、数据处理器及数据资料。但面对网络技术革新与数据价值的膨胀,立法尚未作出及时调整,需要更多交由法官在个案中判断将国内法适用于域外的数据处理行为和主体的具体条件。这一定程度放松了传统立法对严格属地原则的坚持,但也填补了立法在域外效力问题上的缺失。同时应当注意,司法权力天然处于被动地位,法院并不能突破既有的立法框架,并根据新的连结点进行扩张解释。尤其在需要通过创设新的连结点实现本国数据政策时,司法机关只能发挥间接作用,因此有必要通过立法对本国数据保护法的域外效力作出直接宣示。如欧盟综合以往司法实践,通过最新立法 GDPR,在原有“设立机构标准”之外,针对欧盟外数据控制者、处理者又引入以效果原则为基础的“意图标准”。其目的,一则为了贯彻数据权利背后所承载的欧盟人权理念,二则是为了迎合欧盟数据产业的发展要求,通过效果原则将指向欧盟市场的域外数据处理行为均纳入立法管辖范围,最大程度地维护欧盟内部市场的利益。对比来看,美国以微软案为契机推出 CLOUD 法案,以属人连结点架构域外效力规则,实则也是立足本国数据产业的全球优势,服务于依托本国数据企业来实现控制全球数据的目的。

## 三、数据保护法域外效力的国际合法性分析

国内立法将在何种限度发挥作用取决于一国主权的自主选择,但是如果做全面考量,国内法效力边界的确定本质上需要经过国际层面的审视,即除却国内法赋予其“自内向外”效力扩张之外,应当考虑国内立法在域外适用是否符合国际法的一般要求,如果域外效力的规定与国际法相冲突,那么将必然受到质疑,反之亦然。因此,数据保护法的域外效力问题也必须接受外部评价,以获得国际法层面的正当性支撑。

### (一)国际判例的默示承认

早在 1973 年,欧盟成员国德国的黑森州颁布第一部个人信息保护法,然而时至今日,在数据保护法领域各国尚未达成一部多边公约,用于协调各国数据保护法的效力边界问题<sup>[15]</sup>。有学者试图从《公民权利和政治权利国际公约》中寻找数据保护法域外效力的正当化依据,但并未论证成功<sup>[16]</sup>。除国际公约之外,对于主权国家国内法效力范围问题最为经典的解释,可以追溯至 1927 年的“荷花号案”。在该案中,国际常设法院一方面肯定:“除非根据国际条约或国际习惯,一国不应当在他国领土上直接行使权力。”同时又指出:“在国际法中尚未衍生出一项普遍规则,即禁止主权国家将国内法的适用范围和司法管辖权延伸到域外的人、事物及行为。这一问题可以交由各国自由裁量决定。在一般情形中,主权国家可以自主决定并采取本国认为最适合的管辖权原则”<sup>③</sup>。

① 日本《个人信息保护法》第 75 条规定:对于在向国内的数据主体提供商品或服务的过程中获取该数据主体个人信息的个人信息处理业者,并在国外处理该个人信息或者利用以该个人信息为基础制作而成的匿名加工信息,第 15、第 16、第 18 条(第二款除外)、第 19~第 25 条、第 27~第 36 条、第 41 条、第 42 条第一款、第 43 条及后一条的规定也适用。個人情報の保護に関する法律(2003 年 5 月 30 日法律第 57 号)。

② Clarifying Lawful Overseas Use of Data Act 18 U.S.C.A. §2703 (2018)。

③ S.S. Lotus (Fr. v. Turk.)1927 P.C.I.J.Series.A, No.10, p.19。

从其表述可以看出,一般推定,主权国家只在其领土范围之内享有立法管辖权,即自内向外肯定一国立法对其境内一切人、事物及行为的法律约束力。但是反向来看,国际公约或判例对于主权国家法律的效力范围并没有划定任何外部限制,尤其是在具有正当依据的前提下,允许主权国家超越本国领土范围赋予其本国法律以域外效力的作法。因此回到数据保护法领域,对于域外效力问题的判断亦是做出内部视角与外部视角两种解读。从内部视角分析,国际法以是否允许为逻辑起点,数据保护法的效力范围应当与本国主权范围保持一致。就外部限制而言,由于数据保护领域国际公约及判例尚未形成任何禁止性规则,因而不能排除国内法效力扩张的可能空间,这种国际法层面的默示态度也就构成数据保护法域外效力的正当化基础。应当承认,“荷花号案”判决的释明意义有限,但站在更为宏观的视角可以做出倾向于后者的决断,这是因为,虽然国际法的主要功能是调整国家之间的关系,但作为约束国家的国际法规则始终源于国家意志,国家始终是国际法的主要立法者。因此,除非国际公约或判例明确禁止,国家有权基于自身利益考量对法律效力范围进行扩张。

## (二) 支撑数据保护法域外效力的国际习惯法原则

在国际法框架下,如果无国际公约约束,主权国家一般依据自身与管辖客体之间的真实联系确立立法管辖权,进而适用本国法律。基于真实联系上的具体差异,国际社会逐渐沉淀出属地管辖、属人管辖、保护性管辖及普遍性管辖原则,作为国内法效力范围设定的正当化基础<sup>①</sup>。具体来看,属地原则是指国内法的效力止于一国领土边界。属人管辖则指国家根据国籍、住所等属人连结点行使立法管辖权。保护性管辖强调对危害本国国家利益的行为成立立法管辖权。最后普遍管辖权专门针对损失国际社会利益以及严重侵犯人权的行为,如对海盗行为,各国均有权行使管辖权<sup>[17]460-461</sup>。目前这四种管辖权基础已经得到国际社会的普遍认可,因此对于数据保护立法而言,也只有基于上述管辖权主张域外效力,才符合国际法上的合法性要求。

欧盟 GDPR 以效果原则为基础设定域外适用规则。效果原则最初应用在美国反垄断法领域,曾饱受争议。但在当前实践中,效果原则在反垄断法、证券法等市场法领域得到广泛采纳,并衍生成为一项相对独立的立法管辖权依据。效果原则本身是对属地管辖的拓展,仍指向国内,但是一种特殊的属地原则。因为其关注法律规制行为对本国造成的影响,而非行为实际发生地,换言之,该原则淡化行为的客观地理因素,对属地原则的适用作出高度弹性的设计,进而将发生在领土范围之外的行为一并纳入本国法律的适用范围。同时应当注意,效果原则作为域外效力的判断标准大多出现在市场法领域<sup>[18]</sup>。这主要因为在经济全球化背景下,即使行为发生在域外,也会对国内市场产生不利影响,立法因而具有强烈的域外适用需求<sup>[19]</sup>。实际上,这与 GDPR 引入效果原则具有相似之处。信息技术进步使信息处理行为脱离属地原则的束缚,导致数据处理行为发生地与损害结果地相分离,为了保障欧盟数据主体的权利以及应对数据霸权国家对本国数据产业的威胁,欧盟立法因而在设定最高数据保护标准的同时,也通过效果原则最大限度地这一国内标准扩张至域外。

此外属人原则也可以为数据保护法的域外效力提供正当化依据。欧盟 95 指令和 GDPR 中皆根据属人连结点提出“设立机构标准”。该标准对属人连结点进行扩张,放宽对企业注册地的限制,要求数据处理者或控制者在欧盟存在稳定的安排和活动,因此有效确立了域外适用规则。此外,美国的 CLOUD 法案明确授权行政机关可以获取美国公司在全球存储的数据信息。以属人连结点为基础的设定本身并不违背国际法原则,但是由于美国数据公司向世界范围提供服务,并在全球数据治理中占据领先地位,数据控制者标准的适用意味着美国可以对全球数据资源提出披露要求<sup>②</sup>。这无疑将打破数据保护的主权壁垒,极大威胁各国对本国数据资源的控制以及国家安全<sup>[20]</sup>。

## 四、数据保护法域外效力问题的中国立场

在信息技术、数据多元价值等因素的推动下,数据保护规则的域外效力问题由此产生。实然层面,

① Restatement (Fourth) of Foreign Relations Law, §407.

② 法案同时规定数据服务商仅在两种情况下可以提出抗辩:其一,用户不是美国人且不住在美国;其二,信息的披露将实质违背由美国认可的适格外国政府的法律。



无论是通过明确规定还是做更为宽泛的解释,域外效力问题在立法与司法实践中都已经有所体现。司法与立法两种路径既相互关联又各有侧重。司法路径相对被动,需要法院对传统数据立法进行扩张解释,在个案分析中积累域外适用的经验。立法路径更为直接,在需要通过创设新的连结点实现本国数据政策时,国家有必要通过立法方式对本国数据保护法的域外效力作出直接宣示。事实上,各国数据保护法在域外效力问题上的选择是由国家意志决定,但是域外效力问题仍然需要放置在国际法框架下进行审视。考察国际公约、判例以及习惯法原则,国际法并不禁止本国数据保护法中域外效力规定,但各国在数据立法实践中一般以国际社会广泛接受的习惯法原则为正当性基础,根据本国的数据政策选择不同连结点来设定域外规则的范围。

对于中国而言,数据保护法域外效力问题的讨论具有更多意义。当前中国网络用户人数已位居世界首位,数字经济规模位列全球第二,数字背后既反映出数据产业的强大实力,又对数据的保护与立法规制提出更高要求。除此之外,国际社会在数据保护法领域尚未形成共同规则,从单边思路为本土数据保护规则的适用开通域外适用路径,将有利于中国在积累本国数据立法经验的同时,与全球数据治理建立内外联动模式,推动数据保护国际规则的形成。但总体来看,中国数据法律体系仍存在问题:由国家互联网信息办公室主导已陆续制定《网络安全审查办法》《互联网个人信息安全保护指南》《儿童个人信息网络保护规定》等法律文件,但是尚未出台一部统一的个人数据保护法,立法相对碎片化,规制目标不明确,对于个人数据保护问题的评价也主要停留在国家安全视角,难以兼顾数据权利保护与数据市场的需求<sup>[4][50]</sup>。具体在数据保护立法的适用范围问题上,缺少对域外效力条款的专门规定,中国难以在跨境数据规制中发挥积极作用。

中国在未来个人数据保护立法中,为直接弥补在域外适用规则方面的不足,应通过立法方式确立域外效力条款。对于域外效力条款的具体设定可以借鉴国外经验,在不违反国际法规则的同时,更多考虑中国数据产业发展现状与政策的规制目标。以美国 CLOUD 法的域外适用为例,数据控制者标准的选择与美国跨国数据企业在全世界市场的霸权地位密切相关,包括欧盟在内的任何国家实体显然不能按照此种方式构建数据立法的域外效力条款。相形之下,以欧盟立法为代表,根据设立机构标准和效果原则设定域外效力的做法更符合中国需要。首先,根据设立机构标准,可以克服数据处理行为地认定的技术难题,将在本国范围内从事稳定数据活动的企业均纳入规制范围。其次,对于设立机构标准之外的情况,以效果原则为连接点,对于中国这种拥有巨型数据市场的大国来说尤为重要。一方面,可以尽量避免外国数据处理企业借助数据业务的特定模式利用中国数据市场,同时逃避中国数据立法约束;另一方面,这样做可能加重中国数据企业“走出去”的合规成本,但从长远角度看,可以更全面地保障中国企业和个人数据权益,提高企业核心竞争力。此外,在域外效力规则的实施过程中,应建立统一监督机构,为中国数据权利主体提供行政控告以及司法诉讼多种救济途径。在司法层面,应强化法院在适用域外效力规则中所起的作用,支持法院综合个案事实对中国数据保护立法的效力范围进行解释,与立法、行政机关之间形成良性互动,推动中国数据治理体系的构建。

有学者担忧,一旦世界各国普遍对其法律赋予域外效力,是否将激化国家之间的法律冲突,为商业发展与权利保护带来更多不确定性,阻碍个人数据的全球流通。对此假设应当理性看待,数据保护天然具有“跨境”特质,借助网络在全球范围内的流通势必会动摇原本以主权为界限的国内立法,在此领域的域外效力规定是应有之义。更重要的,数据保护领域域外效力的立法实际上并不是可以任意为之,其实际效果根本取决于一国的国家实力。以中国强大的国家实力作为后盾,中国有需求同时有条件认可数据保护法的域外效力。与此同时,中国作为负责任有担当的大国,一直以来致力于国际社会的和平稳定发展,数据保护法域外效力的规定只是为中国参与国际数据市场的良性竞争、充分保护个人数据与维护国家安全等多重目标的平衡过程提供多一重法律路径,并不排除中国参与国际协商以及自我约束机制的保留,这种立法上的探索不仅具有本土意义,也可以为国际社会的数据规制贡献出中国智慧。

#### 参考文献:

- [1] BIRNHACK M. The EU data protection directive: an engine of a global regime[J]. Computer Law & Security Report, 2008, 24 (6):

508-520.

- [2] 廖诗评. 中国法域外适用法律体系: 现状、问题与完善[J]. 中国法学, 2019(6): 20-38.
- [3] 许多奇. 个人数据跨境流动规制的国际格局及中国应对[J]. 法学论坛, 2018(3): 130-137.
- [4] 张金平. 跨境数据转移的国际规制及中国法律的应对: 兼评中国《网络安全法》上的跨境数据转移限制规则[J]. 政治与法律, 2016(12): 136-154.
- [5] 黄宁, 李杨. “三难选择”下跨境数据流动规制的演进与成因[J]. 清华大学学报(哲学社会科学版), 2017(5): 172-182.
- [6] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.
- [7] 廖诗评. 国内法域外适用及其应对: 以美国法域外适用措施为例[J]. 环球法律评论, 2019(3): 166-178.
- [8] 孟小峰, 慈祥. 大数据管理: 概念、技术与挑战[J]. 计算机研究与发展, 2013(1): 146-169.
- [9] 马长山. 智能互联网时代的法律变革[J]. 法学研究, 2018(4): 20-38.
- [10] 齐爱民. 大数据时代个人信息保护法国际比较研究[M]. 北京: 法律出版社, 2015.
- [11] 王志安. 云计算和大数据时代的国际立法管辖权: 数据本地化与数据全球化的大对抗[J]. 交大法学, 2019(1): 5-20.
- [12] JENNIFER D. Boarder and bits[J]. Vanderbilt Law Review, 2018, 71(1): 179-240.
- [13] BRADFORD A. The brussels effect[J]. Northwestern University Law Review, 2012, 107(1): 1-68.
- [14] 齐爱民, 王基岩. 大数据时代个人信息保护法的适用与域外效力[J]. 社会科学家, 2015(11): 101-104.
- [15] KUNER C. Data protection law and international jurisdiction on the internet: part I[J]. International Journal of Law & Information Technology, 2010, 18(2): 176-193.
- [16] SVANTESSON D B. The extraterritoriality of EU data privacy law—its theoretical justification and its practical effect on U.S. businesses[J]. Stanford Journal of International Law, 2014, 50(1): 53-102.
- [17] CRAWFORD J. Brownie's principles of public international law[M]. London: Oxford, 2012.
- [18] TURLEY J. When in Rome: multinational misconduct and the presumption against extraterritoriality[J]. Northwestern University Law Review, 1989, 84(2): 598-664.
- [19] 霍政欣. 国内法的域外效力: 美国机制、学理解构与中国路径[J]. 政法论坛, 2020(2): 173-191.
- [20] 叶开儒. 数据跨境流动规制中的“长臂管辖”: 对欧盟 GDPR 的原旨主义考察[J]. 法学评论, 2020(1): 106-117.

## The Extraterritoriality of Data Protection Law

HE Yehua

(Law School, Nanjing University, Nanjing Jiangsu 210093, China)

**Abstract:** Affected by many factors such as information technology challenges, multiple value conflicts, and the interaction between domestic and foreign rules, extraterritoriality of data protection law has become a legal issue that China must take seriously. At present, the international community mainly expands the scope of application of domestic data rules through legislative and judicial approaches. Among them, the judicial path fills in to a certain extent the lack of traditional data legislation on the issue of extraterritorial effectiveness, but it has certain limitations. Especially when the domestic data protection policy has obvious expansion needs, it is necessary for legislation to directly declare the issue of extraterritorial effectiveness. Intuitively, although the scope of application of data legislation depends on the independent choice of a country's sovereignty, the determination of extraterritoriality of data protection law still needs to be reviewed at the level of international law if all considerations are made. Taking into account China's data protection policy and the need to participate in global data governance, China should establish extra-territorial effectiveness clauses in legislation, and set the scope of application of the data protection law by utilizing established institution standards and effect criterion. In the implementation stage, the role of the court in applying the extraterritorial effectiveness rules should be strengthened, and the court should be supported to explain the scope of the effectiveness of China's data protection legislation based on the facts of individual cases, so as to form a benign interaction with the legislative and administrative authorities and promote the data governance system Construct.

**Keywords:** data protection; extraterritoriality; international legitimacy; China's position

[责任编辑: 箫姚]