【国际私法】

《通用数据保护条例》域外效力的规制逻辑、实践反思与立法启示

俞胜杰　林燕萍

【摘　要】《通用数据保护条例》(简称GDPR)在立法上扩张地域适用范围。根据“经营场所标准”,如果欧盟境外数据控制者或处理者的数据处理行为被认定与欧盟境内经营场所开展的业务存在“无法割裂的联系”,GDPR有权管辖该行为;“目标指向标准”适用于欧盟境外的数据控制者或处理者开展针对欧盟境内数据主体的个人数据处理行为。实践中,“经营场所标准”客观上引起不同法域间法律价值冲突,应当运用比例原则进行协调,与“目标指向标准”相配套的“代表制度”存在明显的适用困境。我国应该借鉴GDPR的立法经验,吸收“经营场所标准”,将“双重违反原则”引入“目标指向标准”,并以此建立双边执法合作机制,充分保护我国公民的个人信息。

【关 键 词】地域适用范围;域外效力;云计算;个人信息保护法;立法管辖权

【作者简介】俞胜杰(1992-),男,汉族,上海浦东人,华东政法大学国际法博士研究生,研究方向:国际经济法、数据保护法;林燕萍(1959-),女,汉族,上海静安人,华东政法大学国际法学院教授、博士生导师,研究方向:国际私法、欧盟法(上海 200042)。

【原文出处】《重庆社会科学》,2020.6.62~79

【基金项目】国家社会科学基金项目“数字贸易国际规则的新发展及中国法律对策研究”(17BFX216);司法部国家法治与法学理论研究项目重点课题“美国经济制裁法律的域外适用与中国对策研究”(19SFB1009);华东政法大学优秀博士论文培育项目“个人数据保护法的域外适用研究”(2019-1-013)。

一、问题的提出

21世纪以来,随着社会网络、云计算、无线射频识别、设备定位和运用定位、数据挖掘和大数据分析等现代信息技术的不断进步,互联网深度融入了人类生活和工作的方方面面,同时促进了数字经济的蓬勃发展。但是,个人信息保护的形势却不容乐观。近年来,全球性大企业的数据泄露事件频频曝出①。在“万物互联”的背景下,一项亟待解决的网络治理难题摆在世界各国政府的面前:如何在合理兼顾商业利益的同时,及时、充分和有效地保护本国公民的个人信息?②

目前我国正在研究、制定《个人信息保护法》③,国内民法学界针对个人信息权的权属性质、个人信息权与人格权的关系、个人信息权的私法保护等问题展开了热烈讨论。从另一个视角看:由于互联网的无界性、个人数据的跨境性以及数据处理活动的全球性,未来出台的《个人信息保护法》应该具备国际视野。甚至有学者认为,个人信息保护早已突破了国内法的藩篱,成为国际法上的重要议题[1]。有一个重要问题值得在国际法框架下进行讨论:如果我国境外的数据控制者或处理者处理了我国公民的个人信息,我国未来出台的《个人信息保护法》是否可以对该行为进行管辖?即《个人信息保护法》的域外效力问题。

2018年5月25日开始生效的欧盟《通用数据保护条例》是在数字经济重塑人类生活的大背景下欧

盟数据治理改革的里程碑事件，也是迄今为止全球范围内最具影响力的个人数据保护立法之一。欧盟立法机关通过制定宽泛的地域适用范围条款以赋予GDPR域外效力，旨在对作为基本权利的个人数据权提供全球范围内的充分保护，并试图通过该法扩张地域管辖，这种扩张具有全球影响力。

本文试图通过研究并分析GDPR地域范围的适用标准和规制思路，评估GDPR生效一年以来的域外实施效果，反思GDPR设定管辖边界的合理性，进而为我国正在制定中的《个人信息保护法》的域外效力规则提出合理建议。

二、GDPR域外效力的规制逻辑

法律的域外效力是指一国法律对发生在其管辖领土范围以外的某些事项具有法律拘束力[2]。

国家可以在国际法允许的范围内，通过在立法上扩张某一项法律的地域适用范围或对象适用范围以赋予该法的域外效力[3]，这本身是国家行使立法管辖权的外在表现。纵观世界各国的立法进程，包括刑法、反垄断法、证券法在内的许多部门法都曾先后出现主张法律域外效力的情形。一国可以通过巧妙地制定法律的地域适用范围条款，对发生在该国境外的行为主张管辖权。国家行使这类立法管辖权的前提条件是：该行为与管辖权之间应该存在“实质且善意”的联系，且这种管辖不能干涉他国国内管辖权或属地管辖权[4]。

欧盟虽然不是国家，但同样具备国际法主体资格，欧盟层面制定的条例对欧盟内部成员国具有直接适用性[5]。GDPR作为欧盟个人数据保护领域的立法成果，虽是欧盟立法，但该法的适用却未止于欧盟疆界。GDPR第3条系地域适用范围条款④，通过“经营场所标准”(establishment criterion)和“目标指向标准”(targeting criterion)设定了宽泛的地域管辖范围[6]。根据第3(1)条的“经营场所标准”，如果个人数据的控制者或者处理者在欧盟境内设立了经营场所(establishment)，在经营场所开展业务的场景下发生的数据处理行为受到该法管辖，无论数据处理行为的具体位置是否在欧盟境内；根据第3(2)条的“目标指向标准”，该法的地域适用范围进一步延展至在欧盟境内没有设立经营场所的数据控制者或处理者，它们直接收集、处理或者监控欧盟境内数据主体个人数据的行为也将被纳入GDPR的管辖范围。

欧盟在GDPR立法过程中主张扩张地域范围，在数据处理行为的监管思路上之所以选择单边主义的立场，在一定程度上，囿于现有国际法规则提供个人数据保护具有局限性和非充分性。从技术发展角度和欧盟自身处境看，既有应对云计算技术引发管辖困境的考虑，也充分体现了欧盟通过个人数据权以争夺全球数据竞争话语权的决心。

(一)GDPR主张域外效力的立法动因

1.现有国际合作机制无法充分保护个人数据权

无论从双边或者多边层面来看，个人数据保护的国际合作效果均比较有限。

从双边层面看，现有合作呈现出“规则碎片化”“理念差异化”和“谈判高成本”的特点。由于美国和欧盟在个人信息权利性质、隐私内涵理解、数据分享方式、执法监督路径等各方面均未能达成共识[7]，美欧仅在诸如《欧盟—美国双边司法互助协定》《旅客订座记录协定》《环球银行金融电信协会协定》等跨境数据交换协定中制定特殊的数据保护条款，条款分布呈现“碎片化”特征，且不同领域的数据保护标准各不相同。在个人数据跨境传输方面，美欧先后制定了《安全港协议》和《隐私盾协议》。因为“斯诺登事件”的曝光，《安全港协议》于2015年10月6日被欧盟法院裁定无效⑤。经过反复磋商和谈判，美欧终于在2016年7月12日达成《隐私盾协议》。由于双方在个人数据保护方式、思路、宗旨等方面存在着巨大差异，该协议从本质上看，仍然是相互妥协、让步的产物。该协议在一定程度上为欧盟和美国企业的商业活动提供了制度支持和保障，进一步强调了对欧盟公民个人数据的保护力度，但是程序性规章的宣示意义大于实质意义[8]。如果以欧盟公民的个人数据在全球范围内得到充分保护为目的，商签双边条约的谈判成本过高，效果具有明显的局限性。

从多边角度来看，现有国际规则普遍缺乏法律

拘束力。无论是1980年经济合作与发展组织(OECD)制定的《隐私保护和个人数据跨境流动指南》(经2013年修订)、1990年联合国制定的《关于计算机化个人资料的处理指南》,还是2004年亚太经合组织(APEC)制定的《APEC隐私框架》,均仅有软法色彩,并不具有法律拘束力[9]。即便是于2012年正式启动的、以《APEC隐私框架》为基础构建起来的《跨境隐私规则体系》(CBPR)也仅仅约束自愿加入的成员经济体的企业,对体系外的企业没有约束力[10]。

此外,欧盟制定的国际条约提出了非常严格的数据保护标准。1981年制定的《关于个人数据自动化处理的个人保护公约》(以下简称"《108公约》")经过1999年、2001年和2012年三次补充和修订,完成了该条约的现代化改革。虽然该条约向非欧盟国家开放加入,根据第27条(非成员国或国际组织的加入)规定,该公约的加入方式并非采用"申请制",而是"邀请制"。公约委员会应该在新的缔约国加入前,充分评估该国的个人数据保护水平是否符合本公约的规定,能够确保在缔约方管辖的公共和私人领域范围内,所有个体的个人数据在被处理时均得到有效的保护,从而使个体权利(尤其是隐私权)和基本自由得到尊重。到目前为止,缔约方中欧洲理事会成员国26个,非欧洲理事会成员国仅有乌拉圭。欧盟以外的大部分国家均未加入该条约。

正是由于双边规则存在规则碎片化、理念差异化和谈判成本高的特点,多边规则呈现软法特征而缺乏法律拘束力,欧盟主导的国际条约设定了过于严苛的数据保护标准等客观事实的存在,欧盟只能寄希望于扩大GDPR的地域适用范围,将单边方法运用于在全球范围内开展的涉及欧盟个人数据的处理行为。

2.有必要对信息技术的迅猛发展作出立法回应

传统法律大多在民族国家范围内实施,国家地理疆域一般便是法律的地域适用范围[11]。但是随着信息技术的迅猛发展,互联网越来越呈现出远程化、全球化和虚拟化的特点。在大数据时代,各类互联网企业开展的数据收集和处理活动往往有赖于云计算提供技术支持⑥,全球性的互联网公司通过移动终端、应用软件收集来自世界各国数据主体的海量数据,通过云计算开展数据挖掘和大数据分析业务,以期攫取更大的商业价值;小型互联网企业同样可以通过向云计算公司购买有关个人数据的收集、分析和处理服务。

从服务方式分类来看,大致可以分为"软件服务"(Cloud Software as a Service)、"平台服务"(Cloud Patform as a Service)和"基础设施服务"(Cloud Infrastructure as a Service)三种类型⑦。以云计算平台为例,目前大致分为以数据存储为主的存储型云平台、以数据处理为主的计算型云平台以及兼具计算和数据存储处理的综合云平台[12]。云服务提供者可能兼具数据控制者和处理者的双重身份:当他控制着基础设施时,则是数据处理者;当他可以按照一定目的自由地决定个人数据处理时,则是数据控制者。更为复杂的是,在云计算环境下,个人数据存储地和处理特定个人信息的设备所在地难以精准确定,数据处理行为的发生地具有模糊性[13]。在欧盟境外,大量依托云计算技术开展的针对欧盟公民的个人数据处理行为频繁发生。

毫不夸张地说,云计算技术的迅猛发展使得互联网经济发展业态"日新月异"。欧盟立法机关在制定GDPR过程中已经充分意识到这一现象,并在GDPR序言部分的第6段指出,科技快速发展及全球化进程为个人数据保护带来了新的挑战。收集和分享个人数据的规模显著提高。因此,对信息技术迅猛发展作出有效的立法回应成为GDPR主张域外效力的立法动因之一。

3.欧盟试图将个人数据权作为参与互联网产业竞争的工具

在互联网的虚拟空间里,个人用户处于相对弱势的地位。例如,个人用户向互联网企业提交了享受线上服务所必需的个人信息之后,便成为了数据主体。"确保数据主体能够在互联网产业中得到充分保护"成为欧盟个人信息保护立法的逻辑起点。

根据《欧盟基本权利宪章》第8条⑧,欧盟公民享有个人信息权。这类权利仅仅是欧盟内部的基本权

利，仅欧盟公民才能享有。同时，《欧盟基本权利宪章》第51条(适用范围)规定："本宪章之各项规定依辅助原则适用于欧洲联盟各机构及部门并适用于各成员国实践欧盟法的过程中"。欧洲议会以充分保护个人信息权为目的研究和制定了GDPR。从更有效地实践欧盟法的角度出发，如果一项数据处理行为可能影响(或者妨碍)欧盟公民个人信息权的实现，即便该数据处理行为发生在欧盟境外，GDPR依然能够对该行为主张管辖。为保护欧盟基本权利视阈下的个人信息权，确乎可以从欧盟法法理上为GDPR主张域外效力提供正当性基础。

在"互联网女皇"玛丽·米克尔(Mary Meeker)发布的《2018互联网发展趋势报告》中⑨，全球市值最大的20个互联网领军企业中有11个来自美国，9个来自中国。作为世界主要经济体的欧盟竟然没有一家企业上榜，欧盟互联网企业在全球互联网产业中已经几乎没有竞争优势。

谷歌、脸书、支付宝等全球性互联网公司通过搜索引擎、浏览器、聊天工具、支付工具等各类应用软件收集来自欧盟境内数据主体的海量数据，利用大数据分析技术来识别包括用户兴趣爱好、工作地点、消费能力以及日常活动轨迹在内的各类个人信息，并据此开展深度数据开发，以期攫取更大的商业价值。欧盟陷入了"互联网服务输入国"和"个人数据输出国"的尴尬境地。有学者认为，欧盟只有通过"权利"这个最具正当性的工具，以强调个人信息权保护为由，以一种正义的姿态打压包括谷歌公司在内的美国互联网企业，防止其形成事实垄断[14]。互联网的无界性、个人数据天然的跨境属性决定了欧盟需要强调个人数据权，通过设定严格的数据保护标准，调整用户(数据主体)和全球范围内的互联网企业(数据控制者或者处理者)之间的力量对比。据此，欧盟才有可能成为全球互联网产业竞争中的重要组成部分。

(二)地域适用范围条款的立法沿革：从《指令》到GDPR

根据GDPR序言部分的第171段，《条例》一经生效，1995年制定的《欧盟个人数据保护指令》(以下简称《指令》)同时废止。《指令》第4条(应适用的国内法)⑩为《条例》第3条(地域范围)所取代。

值得注意的是，由于《指令》不同于条例性质的欧盟法律，其并不对个人创设权利义务，一般而言，其调整的对象往往是成员国[1]。因此，第4条在很大程度上同时发挥了冲突规范的功能，主要用于缓解和消弭个人数据保护层面各国法律冲突[16]，在明确具体行为将会落入《指令》的地域范围之后，进一步解决究竟适用哪一成员国的个人数据保护实体性规则的准据法问题。

《指令》第4(1)条作为该法的地域范围条款，该条款根据"经营场所是否在欧盟境内"作为分类标准，明确了何种个人数据的处理行为将落入《指令》的地域适用范围；该条包含了是否应该适用欧盟成员国法的两项标准：其一，根据数据控制者"经营场所"的具体位置确定欧盟是否对此拥有管辖权，即"经营场所标准"(《指令》第4(1)a条)；以数据处理为目的而使用的"设备"(equipment)的具体位置确定欧盟对此是否拥有管辖权，即"设备使用标准"(《指令》第4(1)c条)。通过对比条文，可以发现两部法律地域范围条款之间存在着明显的内部继承关系：一方面，"经营场所标准"得到保留，但是GDPR第3(1)条中有"无论其处理行为是否发生在欧盟境内"的表述，该条具有主张域外效力的特点，而《指令》未明确这一点。另一方面，"目标指向标准"取代了原来的"设备使用标准"，GDPR放弃了原来依据处理数据的设备位置来确定准据法的做法，转变成为依据特定域内数据处理行为来确定法律适用的地域范围[17]。

(三)通过"经营场所标准"主张域外效力

根据"经营场所标准"，在欧盟境内设有经营场所的数据控制者或数据处理者，只要数据处理行为发生在此经营场所开展活动的场景中，即使实际的数据处理活动不在欧盟境内发生，GDPR有权管辖该数据处理行为。

1.对"经营场所"的理解

《指令》序言部分的第19段界定了"经营场所"的

基本含义:“在成员国境内设立机构意味着它可以通过稳定的安排开展真实而有效的活动;此类机构的法律形式(无论是简单的分支机构还是具有法人资格的子公司)并不是在这方面的决定性因素。”2010年12月16日,第29条工作组[11]发布意见性文件Opinion 8/2010 On applicable law。该文件提出,识别“经营场所”的关键在于判断涉案的数据控制者实施了有效而真实的活动。欧盟法院通过Weltimmo案对“经营场所”的判断标准问题予以了明确,该案的佐审官Pedro Cruz Villalón认为应该采用“两步分析法”:第一步为判断数据控制者在欧盟成员国境内是否建立了某个“经营场所”;第二步为某项特殊的数据处理行为是否是在这一经营场所开展活动的场景中发生的[12]。该案的判决意见将“经营场所”的概念延伸至通过稳定的安排进行的任何真正而有效的活动,甚至是最小体量的活动。为了确定欧盟以外的实体在成员国是否有经营场所,必须基于活动和提供服务的特定性质来判断安排的稳定性程度和在该成员国从事活动的有效性(尤其是对于那些通过互联网提供服务的企业),当数据控制者的核心活动涉及在线提供服务时,“稳定的安排”的认定标准实际上非常低。因此,在某些情形下,如果雇员和代理人的行为非常稳定,非欧盟实体的单一雇员或代理人的存在足以构成“稳定的安排”。在2019年11月12日EDPB[13]发布的《关于GDPR地域范围的第3/2018号指南》(以下简称《指南》)[14]中,EDPB确认了上述分析,并进一步指出,GDPR是否管辖某一数据处理行为,取决于数据处理行为是否是在欧盟雇员开展活动的场景中发生的。经营场所的概念较为宽泛,因此需要有所限制:如果在欧盟境内可以访问某一企业的网站,仅凭这一点,并不能够认定非欧盟实体在欧盟境内设立了经营场所。

2.对“数据处理行为发生在此经营场所开展活动的场景中”的理解

EDPB在《指南》中指出,在判断“特定的数据处理行为”是否可以被认定为“发生在此经营场所开展活动的场景中”时,应该秉承个案分析的思路,结合具体案情展开分析。一方面,为了确保对欧盟个人数据提供充分有效的保护,不应该对该问题进行限缩解释;另一方面,某些数据处理行为虽然发生在欧盟境内但是与欧盟鲜有联系(或者偶有联系),也不能对该行为的法律适用进行过度扩大解释,最终导致将GDPR错误地适用于上述行为。

在判断“特定的数据处理行为”是否可以被认定为“发生在此经营场所开展活动的场景中”时,EDPB建议围绕两大因素进行考虑:第一,欧盟境外的数据控制者或处理者与他设立在欧盟境内的经营场所之间的关系。第二,是否在欧盟境内产生盈利。

上述两项考量因素来源于Google Spain案。在该案中,欧盟法院查明:Google西班牙公司是《指令》中的“经营场所”,因为它“通过稳定的安排开展真实而有效的活动”,而数据处理行为是在Google公司美国总部(在欧盟境外)发生的,Google西班牙公司未参与相关数据处理活动。Google公司辩称,系争的个人数据处理行为并未发生在数据控制者经营场所开展活动的场景中,两项业务是相互独立的。欧盟法院并未认可Google公司的主张,并最终认定:由于Google公司的搜索引擎服务与出售广告位的活动存在着“无法割裂的联系”(inextricable link),因为《指令》适用于欧盟境外的个人数据处理行为[15]。

在属地管辖原则的视角下,可以对“经营场所标准”进行如下解读:“经营场所”构成了一个主张管辖权的连接因素(nexus),GDPR可以通过属地联系获得对境内实体的管辖权,但是在互联网环境下,这种管辖效果将收效甚微,因为真正可能对个人信息权保护产生不利影响的数据处理行为,并不一定发生在欧盟境内。欧盟便据此设计出第二个概念,即“经营场所开展活动的场景”,如果这种场景与欧盟境外的数据处理行为产生关联,并且构成了一种“无法割裂的联系”,发生在境外的数据处理行为便“顺理成章”地被纳入GDPR的地域管辖范围。

这种立法思路确乎是一种高明的制度设计,它是对信息技术迅猛发展作出的强有力的立法回应,将管辖重点放在“数据处理行为”本身,而不是数据

处理行为发生的具体位置，避免出现法律规避的情况。同时，将管辖权作为“有力武器”，强调对个人数据权的保护，以权利保护为口号，投入互联网产业竞争。由于“经营场所标准”的适用需要进行个案分析，在实践中具有一定的模糊性和不确定性，导致企业在对发生于欧盟境外的数据处理行为进行合规审查时常常担心：数据处理行为是否会被纳入GDPR的管辖范围。根据GDPR第83条有关“处以行政罚款一般条件”的规定，情节最重者可被罚款2千万欧元或全球营业额4%(以金额较高者为准)。境外企业将在“承担高昂合规成本”和“放弃欧盟市场份额”之间进行两难抉择。有趣的是，这种立法管辖权的设计确实收获了不错的宣示效果。例如，在GDPR临近生效前，QQ国际版宣布从2018年5月20日起不再为欧洲用户提供服务⑯。

(四)通过“目标指向标准”主张域外效力

1.“目标指向标准”弥补“经营场所标准”的功能缺陷

与“经营场所标准”相比，它有着完全不同的立法逻辑，能够弥补“经营场所标准”在管辖范围方面存在的不足。“经营场所标准”存在着天然缺陷：该标准的适用前提是欧盟境外数据控制者或者处理者已经在欧盟境内设立了经营场所，如果上述主体在欧盟境内未设立经营场所，该标准便无法适用。实践中，欧盟境外的数据控制者或者处理者为了实现规避“经营场所标准”的效果，完全可以选择不在欧盟设立经营场所，或者关闭该经营场所。在做出应对方案之前，他们需要考虑的重点是上述两种方法是否会导致已占有的欧盟市场份额变少或者从欧盟境内获取商业利润出现缩水的情况。如果欧盟用户对他们提供的商品和服务存在很强的“用户黏度”，或者他们提供的商品或服务是其他的数据控制者或者处理者无法替代的，他们完全可以关闭欧盟境内的经营场所。如果发生上述情况，欧盟以“保护个人数据权为口号，投入互联网产业竞争”的深层次立法目的便无法实现。

因此，欧盟立法机关在GDPR的地域范围条款中增加了“目标指向标准”。该标准适用于欧盟境外的数据控制者或者处理者开展针对欧盟境内数据主体的个人数据处理行为。具体而言，如果欧盟境外的数据控制者或者处理者实施的数据处理行为发生在向欧盟境内的数据主体提供商品或服务的过程中(无论此项商品或服务是否需要数据主体支付对价)，或者对数据主体发生在欧盟内的行为进行监控，GDPR有权管辖该行为。“目标指向标准”是欧盟个人数据保护立法改革的重大成果之一。有学者认为，根据该标准，一旦数据处理行为指向欧盟个人数据，该行为将落入欧盟法的管辖范围[18]。还有学者将该标准的确立比喻为“哥白尼式的改革”[19]。

欧盟将“效果原则”作为“目标指向标准”的理论依据。效果原则是美国法院在反托拉斯案的裁判中发展起来的管辖原则，即国家对外国人在外国所作的，对本国商业产生影响的行为享有管辖权。因为这一原则针对的是外国人而被认为是属地管辖原则的延伸，又由于它的目的是保护国家的重大利益而与保护性管辖相似[20]。将“效果原则”作为个人数据保护立法的理论依据，其合理性引起了学界质疑。有学者认为，将“效果原则”作为网络空间活动的管辖权依据过于虚无缥缈，由于经济全球化和网络全球互联，所有国家对网络行为都存在或多或少的联系，各国如果按照这一原则进行立法，管辖权冲突将非常频繁[21]。但是欧盟为了保护个人数据权主张GDPR的域外效力，从合法性角度看，制定“目标指向标准”并未违反国际法，有关该标准的讨论应该更多地在合理性视角下展开。

2.对“向欧盟境内的数据主体提供商品或服务”的理解

在判断特定的数据处理行为是否应该被GDPR纳入管辖范围时，应该重点考察向欧盟境内的数据主体提供商品或服务的“主观意图”。GDPR序言部分的第23段指出，为判断数据控制者或者处理者是否向位于欧盟境内的数据主体提供产品或服务，应确认控制者或者处理者是否明显企图向位于欧盟境内一个或数个成员国的数据主体提供服务。控制者

网站、处理者网站或其他中介网站仅可以获取邮件地址或者其他联系信息以及使用了控制者营业地所在的第三方国家的通用语言，上述行为均不足以确认其提供服务的动机和意图；一些判断因素使控制者的动机变得明显，例如使用一个或多个欧盟成员国的通用语言或货币用于订购其他语言标识的商品或服务，或者涉及欧盟境内的客户或用户。

3.对“数据主体发生在欧盟内的行为进行监控”的理解

在判断特定的数据处理行为是否应该被GDPR纳入管辖范围时，应该重点考察对数据主体发生在欧盟内的行为进行监控的“客观表现”。GDPR序言部分的第24段指出，为了判断上述处理活动是否可以被认定为是对数据主体在欧盟境内发生的行为的监控，需要确定自然人是否在互联网上被跟踪记录，或者偷偷地后续使用个人数据处理技术，包括对自然人进行数据画像特别是作出自动化决策，抑或是对其个人偏好、行为或态度作出分析或预测。由此可见，GDPR第3条的域外管辖权边界不够明确，缺乏法律的稳定性。有学者认为，GDPR第3条中的“目标指向标准”与美国宪法第一修正案、普通法以及成文法典均格格不入，缺乏可执行性[22]。

4.引入“代表制度”以增强域外效力

“目标指向标准”存在先天不足：如果一项数据处理行为符合该标准而落入GDPR的管辖范围，成员国数据监管机构一旦发现该行为未符合GDPR的实体性规定，却面临因为“鞭长莫及”而无法真正实施调查、警告、行政罚款等执法工作。

为了避免陷入尴尬的“执法困境”，欧盟立法机关引入了“代表制度”⑰。根据GDPR第27(1)条，未在欧盟设立经营场所的数据控制者或者处理者应该以书面方式指定一名在欧盟的代表。EDPB在《指南》中明确指出，代表的职能与数据保护官不同，数据控制者或者处理者根据第38条的要求在其内部设立的数据保护官应该具有独立性，而代表应该受雇于数据控制者或者处理者，按照后者的命令完成既定的任务⑱。由此可见，GDPR希望“代表制度”能够在数据控制者或处理者、数据主体以及数据监管机构三方主体之间发挥“桥梁”作用。

三、GDPR域外效力的实施效果反思

GDPR生效至今不到两年，欧盟真正实施域外管辖权的案例尚不丰富。但是，“管中窥豹，可见一斑”，通过对现有的域外管辖案例进行分析，不难发现：欧盟及其成员国在行使GDPR第3条中的域外管辖权时存在着适用困境。对于“经营场所标准”而言，以被遗忘权的执行范围为例，行使域外管辖权将引发不同法域间的法律价值冲突；对于“目标指向标准”而言，代表制度存在着明显的适用困境，由于缺乏双边执法的合作基础导致欧盟个人数据权难以在境外实现。

(一)被遗忘权与信息自由权的有效平衡

1.案件背景与争议焦点

Google Spain案的裁决意见中并未指明“被遗忘权”的执行范围。Google Spain案以后，谷歌公司便采用基于域名的执行方案[23]，将搜索结果的调整限制在欧洲范围内。虽然某些搜索结果可能已经从google.es或google.be中删除，但只要切换到google.com或任何其他非欧洲经济区的域名扩展(例如google.ca)，用户仍然可以获得这些搜索结果。然而，法国国家信息与自由委员会(以下简称“CNIL”)对此执行方案并不满意，要求应该在其搜索引擎的所有扩展域名中删除相应链接，CNIL认为现行的执行方案可能会妨碍“被遗忘权”的充分保护，违背了《第95/46号指令》对欧盟个人数据权利提供高水平保护的立法初衷。双方遂产生争议，法国最高行政法院将该案⑲提交至欧盟法院，请求欧盟法院作出先行裁决(preliminary ruling)。

2.“经营场所标准”的适用以及判决主旨

在Google案中，欧盟法院先通过“经营场所标准”明确了GDPR的可适用性。谷歌公司在法国境内设立机构开展商业和广告活动，该活动与为了运营搜索引擎而进行的个人数据处理行为具有无法割裂的联系；其次，由于谷歌搜索引擎在不同国家版本之间存在网关，所以各国实际上是单独进行数据处

理行为。基于上述理由,法院认定:本案中的数据处理行为是在法国境内的经营场所开展活动的场景下进行的。因此,这种行为落入了《指令》与GDPR的地域适用范围。在确定准据法后,欧盟法院重点讨论了有关"被遗忘权"执行范围的问题,法院比较客观地指出,世界各国在隐私权、个人数据保护与网络用户言论自由之间的权衡可能会有很大差异,到目前为止,欧盟域外删除链接权的适用范围关于上述权利和自由尚未取得平衡。并据此最终认定:搜索引擎运营商仅应该删除其欧盟版本网站的搜索结果,谷歌公司不必在欧洲以外的全球范围内执行"被遗忘权"⑳。

3.案件的意义与启示

本案的意义有如下三点:第一,该案通过"经营场所标准"明确了GDPR的可适用性,解决了法律适用的准据法问题;第二,该案提出在处理欧盟内部各项权利时,应该"采用比例原则以动态平衡诸项基本权利"的权利协调思路;第三,该案创造性地提出:即使欧盟境外企业的数据处理行为被纳入欧盟个人数据保护法㉑的域外管辖范围,该企业运用技术手段来保护欧盟个人数据权利的实际效果(范围)原则上应该以欧盟的地域为界,只有在特殊情况下,才会要求实际效果溢出欧盟。

由此可见,在互联网环境下,"经营场所标准"仅仅解决数据处理行为的可管辖性。在Google案中,如果欧盟法院坚持要求在全球范围内执行"被遗忘权",可能会带来不同法域的法律价值冲突,尤其是隐私保护与言论自由方面的冲突。本案的裁判精神在于平衡欧盟基本权利和欧盟之外的法律价值,这是成熟运用"经营场所标准"后产生的新问题,其内在原因是:由于互联网的无界性、个人数据的跨境性以及数据处理活动的全球性,通过"经营场所标准"将欧盟境外数据控制者或者处理者的数据处理行为纳入管辖,将不可避免地导致欧盟境外的法律价值与欧盟内部的个人数据权在法院诉讼中产生了"正面交锋"。欧盟法院虽然在Google案中作出了妥协,但是这种妥协是暂时的。欧盟法院在判决第72段指出,现行欧盟法虽然并不要求在所有搜索引擎版本中删除链接,但也没有禁止该行为。因此,成员国的监管机构或者司法机关仍有权依据本国基本人权保护标准,在数据主体的隐私权、个人数据保护和信息自由权之间进行权衡,并有权在特定情形下命令搜索引擎运营商在所有搜索引擎版本中删除相关链接。

(二)个人数据保护双边执法合作机制的建立

根据管辖权的一般原理,立法管辖权越宽泛,行使执法管辖权的难度越大[24]。由于"代表制度"存在适用缺陷,"目标指向标准"在实践中像一只没有牙齿的老虎,缺乏执法的强制力保障。从目前来看,这项立法管辖权的宣示意义大于实际效果。

1.GDPR域外执法第一案

2018年7月,英国数据保护监管机构信息专员办公室(ICO)开启了GDPR域外执法第一案"AggregateIQ"案㉒的调查程序。涉案公司是加拿大公司AggregateIQ Data Services Ltd(以下简称AIQ)。

经过ICO调查,AIQ涉嫌帮助Cambridge Analytica Ltd(剑桥分析),通过处理欧盟公民的Facebook数据进行英国脱欧公投的民意分析。ICO按照"目标指向标准",对其数据处理行为主张管辖,认定AIQ对数据主体发生在欧盟境内的行为进行监控㉓。AIQ对它隶属于Cambridge Analytica的指控提出异议,并拒绝完全支持ICO的调查,并认为它不受ICO管辖。但是,根据已经收集到的证据,ICO认定AIQ违反了GDPR,该公司违法获取并处理了英国公民的个人数据,并用于未经授权的定向政治广告推送等非法目的。

ICO发布的GDRP执行通知要求AIQ在通知日期后的30天内停止处理"从英国政治组织或出于数据分析,政治竞选或任何其他广告目的而从英国政治组织获得的任何英国或欧盟公民的个人数据"。如果不遵守此类通知,可能会收到最高2000万欧元或公司年度全球收入4%的罚款(以较高者为准)。

AIQ遂向法庭上诉,称ICO对公司无管辖权,GDPR对其不适用,因为所谓的行为是在GDPR生效

之前发生的，且通知范围太广。ICO随后发布了修正的执行通知，指出适用GDPR的原因在于该数据处理行为一直延续至GDPR生效以后。该通知还阐明了AIQ为遵守通知必须采取的步骤。ICO的修订通知命令AIQ删除该公司已于2018年5月以前服务器上的所有英国个人数据。AIQ自此撤回了上诉，并表示将遵守该执法通知。

该案是适用“目的指向标准”开展域外执法的第一案，具有深远的意义。在该案中，英国和加拿大数据保护执法机构间的跨境合作之密切远超想象。一般认为，由于欧盟境外的企业，在欧盟内无实际可供各欧盟成员国数据执法机构接触、调查或限制的财产和营业场所，GDPR宽泛的域外效力将大打折扣。然而，本案中，ICO积极与加拿大隐私事务专员办公室和不列颠哥伦比亚省的信息和隐私委员会展开配合，彼此共享信息，并通过加拿大数据执法机构向AIQ施压，迫使AIQ与其合作，并最终令AIQ承认违法数据处理行为。

两国数据保护执法机构之所以密切配合，有两个原因：第一，英国和加拿大历史渊源颇深，两国有相似的法律传统和理念。第二，加拿大的《个人信息保护和电子文档法》(PIPEDA)于2018年11月1日生效，AIQ的数据处理行为同样违反了加拿大法律[24]。AIQ的不当数据处理行为构成双重违法，这可能是加拿大数据保护执法机构愿意紧密配合执法合作的深层次原因。GDPR生效仅仅一年，尚未建立起成熟、完善的双边执法框架，执法机构间长效协作机制和跨境执法活动有待进一步观察。

2.“代表制度”存在明显的适用困境

为了避免陷入尴尬的“执法困境”，GDPR第27条引入了“代表制度”。其实，代表制度早已存在于《指令》第4条的“设备使用标准”之中。由于GDPR扩大了地域适用范围，这一制度显得尤为重要，欧盟立法机关希望该制度能够促使欧盟境外的数据控制者或者处理者更好地遵守GDPR项下的各项合规义务。根据GDPR第30(1)条的要求，因此，处于欧盟境内的代表应该妥善处理好一切与数据处理有关的事情，代表应该掌握数据控制者的处理活动记录，并且密切配合监管机构的执法要求。

那么，如果任命一名代表并不妨碍对欧盟以外的控制者或者处理者提起法律诉讼，那么该代表是否可以对数据控制者或处理者的违规行为承担责任？GDPR第27条并未释明这个重要问题。但是，序言部分的第80段提到，如果数据控制者或处理者不遵守，指定的代表应接受强制执行程序。此外，EDPB在《指南》中明确指出，设立代表的根本目的在于“使执法者能够像对数据控制者或者处理者那样，对代表发起执法活动”[25]。按照上述两处措辞，代表应该承担责任以及接受行政罚款和处罚，是应有之义。

但是，GDPR内部条文之间对该问题的认识存在着矛盾。GDPR第58(2)(a)至(j)条以及第83条规定了数据保护机构的纠正权，上述规定未提及代表，GDPR第58(1)(a)条明确规定代表可以接收请求信息。在《2018年英国数据保护法》也有类似规定，信息通知可以发送给代表[26]，但执行通知的接收者予以明确[27]，处罚通知发给“某一特定个人”[28]。

笔者认为，强制执行措施的实施对象不应该包括代表，因为违反GDPR的数据处理行为是由数据控制者或者处理者实施的，代表受其雇佣，不应该成为责任承担者。但是，以此为思路，又会产生一个新问题：如果代表不承担责任，如何真正落实对“遥远的”境外数据控制者或者处理者的行政处罚？代表制度现存的适用困境，直接导致“目标指向标准”成为一项具有宣示意义的标准，缺乏执法的强制力。

对于两项标准在实践中引发的适用困境，需要运用国际法思维加以解决。在个案中应当灵活运用比例原则，根据案件具体情况协调个人数据权与信息自由权的关系，不能一味地追求个人数据权的实现。欧盟法院在判决中也承认了个人数据权不是绝对权，即使在欧盟内部亦需要与信息自由等法律价值进行动态协调。有学者认为，GDPR的地域范围条款具有很强的属地特征，根据该条主张域外管辖权时，应当恪守比例原则，避免侵犯他国主权[25]。此

外，从长远来看，GDPR已经树立起了全球个人数据保护立法的“标杆”，随着越来越多的国家立法对此进行效仿，客观上实现了全球个人数据保护立法的趋同化，使得与特定国家建立双边执法合作机制具备了一定可能性。

四、对中国的立法启示

立法机关应当改变立法上固守“属地主义”的惯性思维，充分利用目前尚未形成具有拘束力的相关国际法规则的有利条件，不自我设限，应当留有余地，在立法上设定域外管辖权。立法机关应当适度借鉴GDPR中的“经营场所标准”和“目标指向标准”，在未来的《个人信息保护法》中明确该法具有域外效力，使未来处理个案时能够游刃有余，避免在法律适用过程中陷入进退失据的尴尬境地。另一方面，增设域外管辖权规则有利于与其他国家搭建个人信息保护双边执法机制。

(一)应该在立法上赋予《个人信息保护法》域外效力

立法机关在制定《个人信息保护法》时，将面临是否应该赋予该法域外效力的立法选择。法律的域外效力一般分为属人适用范围和属地适用范围。

从中国立法实践看，凡是规定有地域适用范围条款的立法，学术界都围绕该条款开展过相关学术讨论，提出过争鸣意见[26]。我国的《刑法》《反垄断法》等实体法均有域外效力的立法表述。例如，根据我国《刑法》第6条有关空间效力的规定，犯罪行为或犯罪结果只要有一项发生在中国领域内，便认为是在中华人民共和国领域内犯罪，在立法上对发生在境外的犯罪行为主张属地管辖权。又如，根据效果原则，我国《反垄断法》第2条主张对在我国境外发生但是对境内市场竞争产生排除、限制影响的垄断行为进行管辖。有学者认为，《反垄断法》第2条应该被理解为一种行政公法的地域适用范围规范[27]。

由此可见，虽然公法体现国家和社会的公共利益，但是由于受到经济全球化的深远影响，某些公法部门也出现了放松属地主义的现象。事实上，任何一种法律是否应该赋予域外效力，取决于国家意志，而这种国家意志的产生不仅源自于国际交往中维护本国利益及相互合作的需要，还取决于所调整的现实社会关系[28]。由于互联网的无界性、个人数据的跨境性以及数据处理活动的全球性，个人信息保护形势严峻，同时，个人信息保护的国际保护标准尚未建立起来，中国立法机关应当改变立法上固守“属地主义”的惯性思维，充分利用目前尚未形成具有拘束力的相关国际法规则的有利条件，站在充分保护本国国民合法权益的角度，在立法上赋予《个人信息保护法》域外效力。

(二)确立“经营场所标准”和“双重违反标准”的管辖思路

国内法的域外管辖应该符合比例原则，不能违反国际法基本原则，不能随意地开展跨境执法。立法时不能随心所欲，应该考虑法律的适用效果，厘清个人信息保护的域外管辖边界。

中国学界曾经出现过三版有关个人信息保护法的专家建议稿[②]，在管辖权设置方面，与前两版有所不同的是，最新一版的专家建议稿(以下简称“《建议稿》”)中的第2条设置了域外管辖权条款。但是规制思路与GDPR域外效力规则的规制思路存在不同。

《建议稿》第2(1)条规定：“在中华人民共和国境内处理个人信息，以及对个人信息处理行为的监督管理，适用本法。”这一款将个人信息处理行为发生地作为确定管辖权的依据。如果个人信息处理行为发生在我国境内，则适用中国法。《建议稿》第2(2)条对发生在我国境外的个人信息处理行为的管辖权问题进行了明确：“在中华人民共和国境外处理中华人民共和国公民的个人信息，应遵守本法。”

上述两款规则，按照“处理行为是否发生在我国境内”进行分类规定，具有积极意义，但是忽略了精准锚定“处理行为发生地”的现实难度。在云计算的环境下，个人数据存储地和处理特定个人信息的设备所在地难以精准确定，数据处理行为的发生地具有模糊性。此外，按照《建议稿》第2(2)条的要求，第一个问题是如何判断数据控制者或者处理者在境外处理了中国公民的个人信息？此外，即使有证据证

明境外的数据控制者或者处理者未能遵照中国法律来处理中国公民的个人信息，我国的执法机关可以通过何种途径开展执法活动呢?《建议稿》中未提出以上问题的解决方案。

笔者认为，我国立法机关应当在立法中充分借鉴GDPR域外效力规则中的“经营场所标准”和“目标指向标准”。

1.应当弱化对“行为发生地”的考察，而强化“数据处理行为”本身的考察。根据欧盟的“经营场所标准”，在欧盟境内设有经营场所的数据控制者或者处理者，只要数据处理行为发生在此经营场所开展活动的场景中，即使实际的数据处理活动不在欧盟境内发生，GDPR便有权管辖。未来《个人信息保护法》同样应当对信息技术迅猛发展作出强有力的立法回应，将管辖重点放在“数据处理行为”本身，而不是数据处理行为发生的具体位置，避免出现法律规避的情况。

2.借鉴欧盟经验，制定中国版的“经营场所标准”。欧盟通过作为属地因素的“经营场所”，将“经营场所开展活动的场景”与“欧盟境外的数据处理行为”的关系进行分析，如果构成了一种“无法割裂的联系”，境外的数据处理行为便“顺理成章”地被纳入GDPR的地域管辖范围。中国法也可以参考这样的立法思路。通过在《个人信息保护法》中创设一种类似“经营场所”的属地因素，按照数据处理行为与该属地因素的关联度来决定是否需要对此进行管辖。

3.将“双重违反原则”引入“目标指向标准”。GDPR中的“目标指向标准”通过考察“向欧盟公民提供商品或者服务”的主观意图以及“监控欧盟境内的数据主体行为”的客观表现来判断是否需要对该行为进行管辖。此类管辖权边界过于宽泛，在执行过程中可能会引发管辖权冲突，从国际礼让的角度来看，如果该处理行为同时违反了中国法与行为发生地国的法律，可以通过双边执法合作的方式。中国的立法机关应当以单边性质的域外效力规则为基础，将搭建具有可执行性的个人信息保护双边合作机制作为实践中不断追求的目标。

五、结语

GDPR域外效力规则的规制逻辑给中国《个人信息保护法》的立法工作提供了新的视角，为了加快推进中国法域外适用的法律体系建设[30]，立法机关应当审慎考虑该法的地域范围条款。徒法不足以自行，还应当在立法以后搭建双边合作机制，从而真正实现“试图管辖”到“有效管辖”的适用效果，最终实现商业利益与个人信息保护之间的动态平衡。

注释：

①仅2019年上半年，曾先后曝出包括云存储服务平台MEGA、服装品牌优衣库、全球顶尖求职平台LinkedIn、社交平台Facebook以及网络软件公司Citrix Systems等多家全球性企业数据泄露事件。

②“个人信息”与“个人数据”存在着一定差异，个人数据产生自互联网的虚拟环境，是个人信息的电子化表达。个人信息能够以非数据形式存在。为了防止读者在理解上产生歧义，笔者特别指出：由于欧盟习惯将“个人信息”统称为“个人数据”，本文在讨论GDPR域外效力及其实施效果时，统一采用“个人数据”的用词。由于我国目前计划立法的法律名称为《个人信息保护法》，故在第四部分讨论“对中国的启示”时，为了符合我国立法的表达，采用“个人信息”的表述。有关“个人信息”与“个人数据”的区别问题，参见王成：个人信息民法保护的模式选择[J].中国社会科学，2019(6)：124-146+207.

③2018年9月7日，《十三届全国人大常委会立法规划》公布，其中第一类项目为条件比较成熟、十三届全国人大常委会任期内拟提请审议的法律草案(共69件)，《个人信息保护法》被列入第一类项目之中。

④GDPR第3条的翻译：(1)数据控制者或处理者在欧盟境内设有经营场所，只要数据处理行为发生在此经营场所开展活动的场景中，无论数据处理行为是否发生在欧盟境内，本法对该行为有管辖权。(2)本法适用于对欧盟境内的数据主体个人数据的处理行为，该行为由在欧盟境内没有设立经营场所的数据控制者或处理者实施：(a)发生在向欧盟境内的数据主体提供商品或服务的过程中，无论此项商品或服务是否需要数据主体支付对价；或者(b)对数据主体发生在欧盟内的行为进行监控。(3)本法适用于在欧盟境内没有经营场所的控制者实施的个人数据处理行为，但该控制者的经营场所根据国际公法应适用该成员国法律。

⑤Communication from the commission to the European parliament and the council on the transfer of personal data from the EU to the United States of America under Directive 95/46/EC fol-

lowing the judgment by the Court of Justice in Case C-362/14[EB-OL].(2015-11-06) https://eur-lex.europaeu/legal-content/EN/TXT?uri=CELEX%3A52015DC0566.

⑥按照美国国家标准与技术研究院(NTSI)对云计算概念的权威定义:云计算是一种按使用量付费的模式,这种模式提供可用的、便捷的、按需的网络访问,进入可配置的计算资源共享池(资源包括网络、服务器、存储、应用软件、服务),只需要投入少量的管理工作,或者与服务供应商进行少量的交互,这些资源能够被快速提供。

⑦"云软件即服务"具有方便终端用户获得信息和收发邮件的功能,从技术上看,它是最为简单的一种服务类型,例如Google Docs;"云基础设施即服务"广泛运用于电子商务,为云消费者提供建立和管理应用的平台,例如Facebook或者Google App;"云基础设施即服务"允许云消费者使用以云服务提供商的硬件设备和计算机资源为基础建立起来的操作系统,例如存储功能和网络功能等。上述三种服务可以满足云消费者的各种使用需求。

⑧《欧盟基本权利宪章》第8条第1款规定:人人均有权享有个人数据之保护。

⑨Internet Trends 2018.[EB/OL].(2018-05-30).https://www.kleinerperkins.com/files/INTERNET_TRENDS_REPORT_2018.pdf.

⑩《指令》第4条的翻译:(1)如果出现下列情况之一,各成员国在处理个人数据时应根据本指令适用其国内法:a.数据处理行为发生在数据控制者经营场所开展活动的场景中,而该控制者的经营场所位于该成员国领域内;如果该控制者的经营场所位于若干个成员国领域内,其必须采取必要措施以确保每一经营场所都遵守所适用的法律规定的义务;b.该控制者经营场所不在该成员国境内,但其所在地根据国际公法的规定应适用该国法律;c.该控制者经营场所不在欧共体境内,并且出于处理个人数据的目的而使用了位于上述成员国境内的设备,除非使用该设备只是为了穿过欧共体全境。(2)在第(1)c条的情形下,控制者必须指派一名经营场所位于该成员国境内的代表,并且不得妨碍针对该控制者本人而提起的法律诉讼。

⑪根据《95指令》第29条的有关规定,欧盟成立的一个"在个人数据处理中保护个人的工作组",一般称之为"第29条工作组"。该工作组是一个独立的咨询机构,有成员国数据保护机构的代表组成。该工作组在欧盟数据保护法中发挥重要作用,它发布的解释性文件具有巨大影响力。

⑫参见Case C-230/14的佐审官意见第26段(该佐审官意见于2015年6月25日发布)。

⑬《通用数据保护条例》生效后,原先根据《95指令》第29条建立的个人数据保护工作组被新成立的欧洲数据保护委员会(European Data Protection Board,简称EDPB)所取代。该机构承担着欧盟个人数据保护领域的解释立法和合规咨询职能。

⑭Guidelines 3/2018 on the territorial scope of the GDPR [EB/OL]. (2019-11-12). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018territorial_scope_after_public_consultationen.pdf.

⑮由于文章篇幅有限,Google Spain案的基本案情不再展开,详情请参见杨开湘."被遗忘权"的司法确立——重探谷歌数据隐私案[J].经济法论丛,2018(1):359-386.

⑯欧盟隐私保护新规实施在即,QQ国际版将停止欧洲服务 [EB/OL]. (2018-04-13). https://baijiahao.baidu.com/s?id=1597638078853539586&wf=spider&for=pc.

⑰参见GDPR第27条。

⑱Guidelines 3/2018 on the territorial scope of the GDPR [EB/OL]. (2019-11-12). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018territorial_scope_after_public_consultation_en.pdf.

⑲该案全称为Google ILC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés(CNIL),案号:C-507/17,判决发布时间:2019年9月24日。

⑳参见欧盟法院案例Case C 507/17判决书的第60-61段以及第73段。

㉑此处的"欧盟个人数据保护法"是指《第95/46号指令》和GDPR。在Google案中,欧盟法院以"上述两部法律均赋予数据主体要求搜索引擎运营商删除链接的权利"为由,肯定了上述两部法律在本案中的可适用性。

㉒Extraterritorial Application of The GDPR: Lessons from Recent Developments[EB/OL].(2018-11-08).https://thetmca.com/extraterritorial-application-of-the-gdpr-lessons-from-recent-developments/.

㉓First GDPR Enforcement Action Is Against A Canadian Data Controller[EB/OL].(2019-03-18). https://wwwstevensbolton.com/site/insights/articles/first-gdpr-enforcement-action-against-canadian-data-controller.

㉔Extraterritorial Application of The GDPR-Lessons from Recent Developments, at https://thetmca.com/extraterritorial-application-of-the-gdpr-lessons-from-recent-developments/,Nov. 20, 2019.

㉕Guidelines 3/2018 on the territorial scope of the GDPR [EB/OL]. (2019-11-12). https://edpb.europa.eu/sites/edpb/files/files/filel/edpb_guidelines_3_2018territorial_scope_after_public_consultation_en.pdf.

㉖《2018年英国数据保护法》第142(1)条与第142(9)条。

㉗《2018年英国数据保护法》第149条。

㉘《2018年英国数据保护法》第155(1)条。

㉙3份建议稿分别为中国社科院周汉华研究员牵头负责

的个人数据保护法研究课题组所起草的《中华人民共和国个人信息保护法(专家建议稿)》、重庆大学齐爱民教授拟定的《中华人民共和国个人信息保护法示范法草案学者建议稿》以及中国人民大学张新宝教授《个人信息保护法(专家建议稿)》。

㉚2019年11月5日,《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》发布,该文件中提出"加快中国法域外适用的法律体系建设"。

参考文献:

[1]张新宝.我国个人信息保护法立法主要矛盾研讨[J].吉林大学社会科学学报,2018(5):45-56+204-205.

[2]石佳友.我国证券法的域外效力研究[J].法律科学(西北政法大学学报),2014(5):129-137.

[3]江国青.国际法中的立法管辖权与司法管辖权[J].比较法研究,1989(1):34-36.

[4]伊恩·布朗利.国际公法原理[M].曾令良,余敏友,等,译.北京:法律出版社,2007:271.

[5]蔡高强,刘健.论欧盟法在成员国的适用[J].河北法学,2004(4):116-119.

[6]金晶.欧盟《一般数据保护条例》:演进、要点与疑义[J].欧洲研究,2018(4):1-26.

[7]伍艺.大数据时代执法合作中个人数据跨境保护问题研究[J].重庆邮电大学学报(社会科学版),2018(3):52-59.

[8]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.

[9]冯硕.网络个人信息保护国际合作的障碍与选择——以软法为路径[J].网络法律评论,2016(2):123-136.

[10]弓永钦,王健.APEC跨境隐私规则体系与我国的对策[J].国际商务,2014(3):30-35.

[11]夏燕."被遗忘权"之争——基于欧盟个人数据保护立法改革的考察[J].北京理工大学学报(社会科学版),2015(3):129-135.

[12]齐爱明,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.

[13]Faye Fangfei Wang. Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction[J]. European Business Law Review, 2013(24): 589-616.

[14]刘泽刚.欧盟个人数据保护的"后隐私权"变革[J].华东政法大学学报,2018(4):54-64.

[15]邵景春.欧洲联盟的法律与制度[M].北京:人民法院出版社,1999:60.

[16]杜涛.国际私法国际前沿年度报告(2015-2016)[J].国际法研究,2017(2):89-128.

[17]王志安.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?[J].交大法学,2019(1):5-20.

[18]Paul de Hert and Michal Czerniawski. Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context[J]. International Data Privacy Law, 2016(3): 230-243.

[19]Christopher Kuner. The European Commission´s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law[R]. Bloomberg BNA Privacy and Security Law Report, 2012: 1-15.

[20]王虎华.国际公法学[M].北京:北京大学出版社,2015:85.

[21]Lilian Mitrou. The General Data Protection Regulation: A Law for the Digital Age?[G]//Tatiana Eleni Synodinou, Philippe Jougleux, Christiana Markou, Tbalia Prastitou. EU Internet Law: Regulation and Enforcement, Springer, 2017: 32.

[22]Kurt Wimmer. Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?[J]. Syracuse Law Review, 2018(3): 545-576.

[23]Brendan Van Alsenoy and Marieke Koekkoek. Internet and Jurisdiction after Google Spain: the Extraterritorial Reach of the "Right to Be Delisted"[J]. International Data Privacy Law, 2015(2): 105-120.

[24]Christopher Kuner. Data Protection Law and International Jurisdiction on the Internet(Part 2)[J].International Journal of Law and Information Technology, 2010(3): 227-247.

[25]Stefano Saluzzo. The Principle of Territoriality in EU Data Protection Law[G]//Marise Cremona, Joanne Scott. EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law, Oxford University Press, 2019: 55.

[26]袁发强.国家管辖海域与司法管辖权的行使[J].国际法研究,2017(3):102-114.

[27]杜涛.论反垄断跨国民事诉讼中域外管辖权和域外适用问题的区分——以中美新近案例为视角[J].国际经济法学刊,2019(1):72-84.

[28]吕岩峰.刑法的域外效力辨析——来自国际私法学的观照[J].法制与社会发展,1998(4):49-53.