

【国际私法】

网络数据长臂管辖权

——从“最低限度联系”标准到“全球共管”模式

邵 恂

【摘要】长臂管辖权作为一种特殊的司法管辖权,其与网络数据的结合最早可以追溯到20世纪80年代中期,然而在相当长的一段时间内,数据只是进一步确定“最低限度联系”存在的连接点之一,其独立价值并未被重视。这一状况自2018年《欧盟一般数据保护条例》生效以来发生了根本性的转变,以《欧盟一般数据保护条例》为代表的部分专门性数据立法参考保护管辖原则的意涵,极端扩张了国内立法的域外适用,并通过设立具有司法职能的监督机构,为司法管辖权的单方域外行使提供了替代路径。这一架构摒弃了“最低限度联系”标准的使用,转而以“全球共管”模式来指导管辖规则的设计,赋予本国法院“对起诉时与管辖区域有联系的非居民被告的管辖权”,具备了长臂管辖的外观要件。这一长臂管辖权扩张的新模式对于我们而言既是挑战亦是机遇。挑战在于:单方司法管辖权的域外扩张会导致国家间管辖权冲突与争诉的常态化,无疑将对各国司法主权造成极大的冲击;机遇在于:不同于“最低限度联系”标准,全新司法管辖规则的适用具有“保护管辖”的意涵,其与网络主权并非天然地对立。辩证地研究美欧相关立法与司法实践能为构建网络数据长臂管辖权的中国模式提供有益的参考与经验。

【关键词】长臂管辖权;域外管辖;网络数据;最低限度联系;全球共管

【作者简介】邵恂,北京化工大学文法学院副教授。

【原文出处】《法商研究》(武汉),2021.6.73~87

【基金项目】教育部人文社会科学研究项目(19YJC820048)。

网络数据,依据2021年《中华人民共和国网络安全法》(以下简称《网络安全法》)第76条之规定,可以解读为“通过网络收集、存储、传输、处理和产生的各种电子数据”。网络数据虽然虚拟无形,但与我们的日常生活密切相关。随着大数据时代的到来,数据作为新时代的石油与黄金,其价值被日益放大,数据安全与国家安全的联系也进一步紧密。随着互联网技术的发展,尤其是云储存的出现,依托网络这一媒介,数据的跨境流动也成为常态,^①但这种常态的背后也存在两个方面的隐忧:(1)当前的数据流动并非全球范围内的均匀流动,而是呈现出一种由东向西、由发展中国家流入发达国家的整体态势;(2)常态性的数据跨境流动导致数据储存地与来源地割裂,最

为直接的后果便是数据所有权与传统意义上的管辖权分离,这一分离进一步导致数据治理规则的碎片化与数据治理主体的多元化。面对上述现状,为实现对域外数据的直接或间接管控与引流,美欧等国家和国际间组织开始寻求以全新的规范体系来规制虚拟的网络数据及其相关主体,以全新的管辖模式来应对域内外的可能风险,以单方的立法管辖将域外数据及相关主体纳入本国司法管辖之中。当前,针对域外数据,以“八国集团(G8)”为例,截至2020年,只有俄罗斯一国未针对跨国数据的管辖权行使出台相关立法,如果把观察对象放大到更具代表性的“二十国集团(G20)”,目前也只有沙特阿拉伯、俄罗斯、澳大利亚3国尚未明确本国公权力主体对域外网

络数据的管辖。不难看出,当前针对域外网络数据,扩张性的管辖权行使已经成为一种趋势。

在西方各国的相关实践中,我们最需要警惕的莫过于长臂管辖权由实体领土向网络空间的扩张。作为一种特别司法管辖权,长臂管辖权在实体领土之上通常基于最低限度联系原则来确定对于非法院地居民的管辖权,其与网络数据的结合最早可以追溯到20世纪80年代中期,但彼时的网络数据只是用以确立最低联系的一个标准,其独立价值并未得到重视,案件本身也主要涉及与网络数据相关的争议,而非网络数据本身。然而,随着《欧盟一般数据保护条例》(以下简称《条例》)的出台,针对域外网络数据,长臂管辖权的行使模式发生了根本性的转变,对于保护管辖原则的扩张性解读与借鉴取代了最低限度联系原则,数据本身也从参考的标准成为管辖的主体与所需要保护的權利。可以说,长臂管辖的全新模式对于各国司法主权与数据安全的维护带来极大的威胁,全球性的管辖冲突也将成为常态。但我们也应当认识到,针对域外数据的司法管辖并非与网络主权以及数据主权存在天然的冲突,三者间存在应然的平衡模式,而探索这一平衡并构建符合我国基本国情的长臂管辖模式,应是我国当前数据相关立法的重点所在。

一、长臂管辖权概念的解构与统一

面对无边界的网络空间以及无实体的虚拟数据,传统管辖权概念在大数据背景下,存在着适用上的困境,也存在着解读上的模糊。并且,在我国学术界现阶段的研究中,对于长臂管辖权概念的使用也存在一定的分歧,这实际上阻碍了研究成果与立法以及司法实践的衔接。因此,在具体展开本文论述之前,有必要对长臂管辖权及其相关的重点概念进行再解构,以防止出现以一个模糊概念来解释另一个模糊概念的情况。

(一)司法管辖权的域外行使

管辖权作为国际法中的一个基本概念,可被定义为“国家对特意的人、物和事进行管理或施加影响的权力”,并且其“直接派生于国家主权”。^②管辖权

是一个集合性的概念,具体可分为立法管辖、司法管辖与执法管辖。^③司法管辖权可视为“一国让特定的人或事从属于司法过程的权力”,其既包括司法机关受理和裁判案件的权力,也包括行政裁判庭受理行政复议、行政争议的权力。^④目前,长臂管辖权在我国国内学术界往往被用以代指一切形式的不合理的域外管辖权行使,也由此延伸出“长臂立法管辖权”“长臂执法管辖权”等概念。^⑤但如果回归本源,我们可以发现,长臂管辖权首先应属于一种特殊形式的司法管辖权,^⑥其最初主要针对交易行为和侵权行为,如早期美国法上的长臂管辖权仅限于民事诉讼中的对人管辖权。但经过半个世纪的衍化,长臂管辖权的内涵与外延不断丰富,适用范围逐渐扩大到美国州际诉讼以及国际诉讼,也从民事诉讼发展到刑事诉讼。^⑦但就其权利属性而言,目前依旧属于司法管辖权的范畴。参照《布莱克法律词典》对于长臂管辖权的定义,即“对起诉时与管辖区域有联系的非居民被告的管辖权”,^⑧我们亦可以明确,长臂管辖权实则为“将法律的适用范围或其司法管辖范围扩展至该国领土以外”,^⑨即司法管辖权的域外行使。

(二)长臂管辖权对国家主权的侵犯

长臂管辖权的实践最早可以追溯到美国1945年“国际鞋业公司诉华盛顿州案”^⑩(以下简称“国际鞋业公司案”)。在该案中,美国联邦最高法院确立了最低限度联系原则,以使扩张性的管辖权行使能够不违背传统的公平与实质正义观念。彼时的长臂管辖属于美国民事诉讼的相关概念,而“最低限度联系”主要服务于法院对被告管辖权的获取,换言之,即确保地方法院在满足特定条件时对属地管辖的优先性加以一定程度的超越,进而将管辖权延伸至域外。^⑪但当前的长臂管辖权已经不再仅仅局限于美国州际之间的诉讼,其适用也扩展至国际间的诉讼,而在国际语境中,长臂管辖权的理论基础则是管辖权的效果原则的“最低限度联系”,即当国外发生的行为在本国境内产生“效果”时,无论行为人是否具有本国国籍,或在本国拥有住所,也无论该行为在本国法律评价下是合法抑或非法,只要本国法院的管

管辖行使不因此效果而显著不合理,那么该法院便可基于此种效果而产生的诉因行使管辖权。^⑩由此,司法管辖权的域外行使常态性地面临行为人在人所在国的属地管辖与属人管辖的冲突。然而,与传统国际法理论所坚持的属地优先原则不同,长臂管辖对于“最低限度联系”的运用往往将效果原则置于更为优先的顺位,属于在他国领土之上行使国家管辖权,这一行为无疑构成对他国主权的超越乃至侵犯,也构成对包括主权平等、互不侵犯等国际法基本原则的侵犯。

(三)长臂管辖权从民事诉讼到刑事诉讼的扩张

最初的长臂管辖权主要面向民事诉讼中的对人管辖,但随着实践的发展,其也开始逐步向刑事诉讼领域扩展。然而,域外民事与刑事司法管辖权的行使存在巨大的差异,从价值层面看,刑事事项对于各国国家主权以及公共秩序的影响远高于其他事项,如果说民事诉讼侧重于解决私人之间纠纷的话,那么刑事诉讼则直接关系国家主权的行使。此外,从程序层面看,针对民事诉讼,长臂管辖权的行使一般仅需要以域外立法管辖的行使作为先决条件,而针对刑事诉讼,除了有上述先决条件之外,考虑到刑事司法管辖权的行使应以法院实际控制犯罪嫌疑人为前提,长臂管辖权的行使还应当与执法管辖权的域外行使加以结合。执法管辖权通常被定义为“国家有权通过法庭或执行行为、行政行为、警察或其他非司法行为来诱导或强迫守法与惩罚违法”,^⑪针对的是一国领土内或者领土之外但具有本国国籍的人。^⑫而长臂管辖权针对刑事争议的行使,往往需要司法或国家安全机构在域外调查取证的基础上交由相关司法主体提起诉讼,同时,也需要经由引渡程序以实现了对犯罪嫌疑人的实际控制。而包括引渡、域外调查取证等在内的权力属于执法管辖权的范畴,并且上述权力在狭义上被定义为“刑事执法管辖权”。^⑬因此,从逻辑层面我们可以确定,考虑到长臂管辖权对于国家主权的侵害,其针对刑事诉讼的适用将进一步导致执法管辖权行使的“长臂化”。

综上所述,长臂管辖权,无论是从狭义还是广义

上讲,也无论是针对民事还是针对刑事诉讼而言,都具有如下3个方面的特征:(1)长臂管辖权作为一种特别的司法管辖权,其行使需要以立法管辖权的域外行使为基础;^⑭(2)长臂管辖权的行使主要服务于将联系较弱或无直接联系的被告纳入法院的管辖之下;(3)长臂管辖权针对的争议现阶段包括民事与刑事两个方面,并且长臂管辖权对于刑事争议的解决需要以刑事执法管辖权的域外行使作为先决要件。

二、网络数据长臂管辖权行使的“最低限度联系”标准

美国是长臂管辖权的发源地,也是较早将长臂管辖权与网络数据结合的国家。然而,面对域外数据及相关主体,美国的相关司法实践最初只是立足于进一步扩张最低限度联系原则的适用,并没有对传统的司法管辖规则加以实质性的突破或改变,长臂管辖权的行使依旧需要满足以下两个方面的先决条件:(1)是否符合州内长臂管辖法规。由于美国并不存在全国性的联邦长臂管辖法规,因此相关管辖的主要合法性基础来源于《美国联邦民事诉讼规则》第4条e款的规定,即联邦地方法院可依据所在州的长臂管辖法规行使长臂管辖权。(2)是否符合《美国联邦宪法》第14修正案的“正当程序”要求。^⑮根据美国联邦最高法院于1945年在“国际鞋业公司案”中确立的“最低限度联系”标准,如果非法院地被告与法院地间存在某种最低联系,并且依据此联系进行的诉讼不会违反“平等与实质正义的传统观念”,那么法院的管辖便符合“正当程序”要求。^⑯此后,美国司法实践进一步对“正当程序”进行了完善,尤其是联邦法院在“正当程序”之外,对“最低限度联系”的适用还提出了法院在行使管辖权时需要满足“有目的利用标准”“相关性标准”“合理性标准”。^⑰另外,对于“最低限度联系”的具体确定,美国各州的规定也不尽相同,主要分为“综合式”与“列举式”两种。“综合式”即笼统地规定在一定条件下州法院可以对非法院地居民行使管辖权,如新泽西州、得克萨斯州等;“列举式”则规定了长臂管辖权适用的具体范围和特定标准,如伊利诺伊州、纽约州等。不同模式对

长臂管辖权适用的前置性考量也有所不同,“综合式”采取合二为一的路径,主要侧重于“正当程序”的探讨,而采纳“列举式”的各州虽然具体措施有所不同,但基本趋于一致,都认为长臂管辖权适用的先行条件包括在州内从事营业活动、在州内实施侵权行为和在州外实施的侵权行为对州内造成损害。

在早期,长臂管辖权与数据的结合往往服务于确认“程序正当”或者确认满足“列举式先行条件”这两个层面。以具有代表性的“加利福尼亚软件公司诉可靠研究公司案”^⑨为例,该案是公认的美国互联网第一案,也可以视为长臂管辖权与网络数据结合的第一案。该案被告于内华达州通过电子邮件和留言板系统论坛发布诽谤言论,考虑到电子邮件发往加利福尼亚州,以及论坛可以被全网观看,因此加利福尼亚州法院认为自己有权行使管辖权。在该案中,数据的作用主要是为了佐证存在“州外实施的侵权行为对州内造成损害”这一事实。另外,针对刑事案件,数据的连接点作用也得到确认。以具有代表性的《反海外腐败法案》为例,该法案在1998年修订之后,管辖范围进一步扩大,将外国企业或自然人在美国境内实施的违反法案的行为也列入该法管辖的范围,但对于何为“美国境内”,审理“证券交易委员会诉阿尔卡特·朗讯案”^⑩的法官进一步认定:“任何外国人或外国公司的雇员,只要是通过美国的邮件系统进行了通信或使用隶属于美国的国际商业工具进行了腐败支付,不论是电话、邮件还是银行转账,只要和美国发生了联系,美国都具有管辖权”。在该案中,数据虽然依旧作为确定管辖权的连接点而存在,但略有不同的是其并不发挥佐证作用,而是作用于“有目的利用标准”以及“相关性标准”的确认。^⑪

针对网络数据,美国早期的相关实践可视为长臂管辖权行使的“前时代”,在虚拟的网络空间中,物理联系的进一步缺失使得数据作为确定“最低限度联系”的一个连接点而被加以关注,无论是民事还是刑事案件,其本身只是针对与网络数据相关的争议,部分情况下甚至直接将数据用作强行管辖的借口,

即以管辖权的获取这一结果反向寻找可适用的连接点,对于此类长臂管辖权的行使,考虑到数据权利的从属性以及数据功能的辅助性,学术界多将其定义为“网络案件中的长臂管辖权”,^⑫而非“网络数据的长臂管辖权”。事实上,作为司法管辖权的一种,长臂管辖权的行使并不依托于传统的管辖原则,而是依据“最低限度联系”,这一原则在实体领土之上固然可以有效地为法院管辖权的扩张开辟一条新的道路,但面对虚拟的网络空间与数据已经显得力不能及,如果盲目遵从旧例,直接将数据作为连接点加以使用,那么会导致管辖权的肆意扩张,无法对“有目的利用”加以清晰与深入的判定;也无法回应国家对数据安全以及公民对个人隐私保护的需求。基于此,面对来自虚拟网络与数据的冲击,传统长臂管辖权的行使也亟待转型。

三、网络数据长臂管辖权行使的“全球共管”模式

长臂管辖权转型的关键节点可以追溯到欧盟2018年实施的《条例》。需要明确的是,《条例》本身更多地规范了域外数据执法管辖权的行使而非司法管辖权,但《条例》对于保护管辖原则的借鉴与再解读却为此后各国的长臂管辖架构提供了新的思路。

(一)《条例》:网络数据长臂管辖权行使之“全球共管”的开端

《条例》第3条规定:“本条例适用于对欧盟内的数据主体的个人数据处理,即使控制者和处理者没有设立在欧盟内,其处理行为:发生在向欧盟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费用;或是对数据主体发生在欧盟内行为的监控。”考虑到欧盟庞大的经济体量与市场规模,上述具有保护管辖色彩的标准实际上以保障公民基本权利为表象,强行扩张了《条例》的适用范围,通过将网络的媒介属性与最低联系标准相结合的做法,数据主体无论是位于欧盟境内还是境外,只要涉及欧盟个人数据,都将受到《条例》的管辖,这在纵向上已经实现“全球适用”。^⑬此外,在“全球适用”以外,《条例》还期望达成“全产业链适

用”,具体来说,对于管辖的主体,《条例》进行了细致的横向分类,除了具有直接关联的数据控制者、处理者、接收者以外,间接或者利益相关第三方,如上下游供应商等,都被纳入《条例》的管辖之中。然而,《条例》上述管辖规则的适用存在一个关键性的问题,即管辖优先性问题。传统国际法理论认为,当犯罪人是外国人且犯罪行为发生在其国籍国领域内,而这个犯罪地国家又规定了属人和属地的管辖原则时,将与受侵害利益国的保护管辖原则发生冲突,除非行为人在受害国的实际控制之下。

为解决上述管辖优先性问题,《条例》既未针对管辖权的冲突提出一套协调或解决的方案,也没有在适用优先性上加以根本性的突破,而是采取了以下措施:首先,对数据“处理行为”的相关性加以放大,人为地将“域外”侵权“域内化”。其次,以执法管辖权的行使来代替司法管辖权,进而避免了管辖权冲突情况的发生,并规定各缔约国设立独立的监督机构,其性质为政府“公共机构”。同时,为确保《条例》能够得到有效执行,监督机构被赋予大量具有行政执法色彩的权力,包括调查权、纠正权以及授权与建议权。其中,纠正权的设立具有明显的行政执法色彩,如(对数据处理者与控制者的)警告、惩戒以及对数据处理施以临时的或终局性的)限制、撤回许可证、行政处罚款等。总的来看,监督机构虽名为“监督”,但实际上其由政府设立,同时被赋予了包括许可、处罚、强制等一系列具有行政色彩的职权,是远超“监督”实际需要的。综上所述,《条例》确立的管辖规则实际上已经具备比“最低限度联系”标准更为宽松的适用前提以及更为广泛的适用对象。

《条例》的影响是巨大的,这种影响可以从对内与对外两个维度加以论述。在欧盟之内,围绕《条例》和数据保护构建了一些全新的管辖规则,如《欧盟电子证据条例》《欧盟数字服务法》《欧盟数字市场法》等,其中最具代表性的当属2020年12月公布的《欧盟数字市场法》,其一方面继承了《条例》的管辖标准,另一方面也重点针对较大规模的“看门人”企

业,设立了更高的处罚标准与更严格的补救措施。^⑤在欧盟之外,仅仅在《条例》生效后的1个月,巴西参议院便参照《条例》的相关规定,于2018年7月10日通过了《条例》的“镜像版”^⑥即《巴西一般数据保护法》,其覆盖巴西所有的经营行业,影响全部私营和公共实体,且无论个人数据的处理是否发生在数字和物理环境中,同时,该法案还明确国家机构有权处以最高全年收入2%或者5000万雷亚尔的“行政处罚”。^⑦类似的情况还包括印度最高法院的高级别专门委员会提交的《2019年印度个人数据保护法案》。该法案基于“公共利益”与国家主权的保护,以扩张法案适用的对象,同时赋予政府以扩张性的管辖权,如处以该实体上一财政年度全球营业额的2%或5亿卢比的处罚等。^⑧但无论是保护管辖原则的扩张解读,还是基于“公共利益”的管辖扩张,其实质都是对传统管辖原则的突破,都立足于尽可能全面地将全球相关主体纳入本国规范的管辖之下,进而实现对全球数据主体的直接或间接管控。

(二)《108+公约》:网络数据长臂管辖权的欧洲模式

《条例》确立的管辖规则以及监督机构的设立,虽然在客观上服务于执法管辖权的行使,但是不可否认,对于长臂管辖权在网络空间的扩张,其也赋予了全新的可能,如《条例》第58条第5款规定:“每个成员国应当通过法律规定,其监督机构为了执行本条例的条款,有权将违反本条例的情形诉诸司法机构,在合适的情形下可以提起或参与法律诉讼”。这一规定事实上将监督机构打造成一个具有部分司法权能的行政机构,其一方面有权对数据侵权行为加以直接性的行政处罚与制裁,另一方面可就相关侵权行为提起并参与诉讼。正是监督机构的上述设定,为各缔约国的域外网络数据司法管辖权行使提供了扩张的可能。同时,考虑到监督机构的管辖权具有保护管辖的意涵,这实际上也直接成为网络数据长臂管辖权的行使由“最低限度联系”标准向“全球共管”模式转型的理论起点。

如上所述,《条例》确立的管辖规则虽然可以将

更多的潜在对象纳入一国的管辖之中,但是也增加了管辖权发生冲突的可能,因此其选择以执法管辖权来对域外数据及其相关主体加以管控,对于司法管辖权的域外行使则仅强调其成立的可能,其具体的实现则交由每个成员国由国内法加以规定。然而,《条例》的谨慎并不代表上述模式不可行,事实上,2018年欧洲理事会通过的《有关个人数据自动化处理之个人保护公约》及其议定书(以下简称《108+公约》)^②继承了《条例》“全球共管”的思想与域外数据管辖模式,并在此基础之上进一步明确了网络数据长臂管辖行使的欧盟模式。

《108+公约》最初制定于1981年,其后经过3次修改,于2018年通过了现行的现代化版本。作为欧洲理事会起草的一份全球性的数据保护公约,《108+公约》解决了司法机构对域外数据管辖权行使的盲区,并得到全球55个国家和地区的签署。^③《108+公约》针对网络数据的长臂管辖进行了一次大胆且危险的创新,其继承了《条例》“全球共管”的思想,但出于避免管辖冲突的考虑,其实现路径并没有借鉴《条例》的相关规定,也没有具体阐明其管辖权行使所基于的具体原则,转而采用了依据个人请求的直接“全球共管”模式。依据《108+公约》第18条的规定,任何缔约国都有义务协助数据主体实现其权利,根据欧洲理事会的解释,此处的数据主体为不分国籍、住所等的任意个人主体,而提供协助的主体是各个缔约国依据《108+公约》第15条第4款建立的监督机构。对于缔约国司法管辖权的域外行使,《108+公约》第15条第2~3款借鉴了《条例》的相关规定:“监督机构应当参与到诉讼程序中,并将违反公约的行为提交至司法机构”。《108+公约》对监督机构的设定,相比《条例》而言,虽然范围不尽相同,但是整体职能高度相似。不过,《108+公约》架构下的监督机构的职权更为精简,主要为“调查”与“干预”两个方面,对于《条例》中具有明显行政执法色彩的纠正权则未加以规定,只概括规定了监督机构有作出包括罚款在内的行政裁定的权力。^④对于何为“参与诉讼”及其与“调查”的关系,欧洲理事会的解释表示:

缔约国有义务为监督机构参与诉讼提供相应的权力,并且这一“参与权力”是基于调查权的需要,调查能引导司法主体发现违反数据保护的行为。^⑤如果说《条例》中监督机构调查权的行使更多的是为行政执法服务的话,那么《108+公约》则明确地将监督机构的调查权作为司法管辖权行使的前置性程序加以提出,并且实际上通过赋予监督机构司法取证和起诉两项权力使其成为一个介于司法与行政之间的存在,突破了行政主体调查与司法主体诉讼之间的断层。

总的来说,对于长臂管辖权的态度,《条例》只是简单地予以了确认,而《108+公约》则确认了其具体实现的路径。毕竟,域外数据司法管辖权行使的传统模式往往需要基于国际间的司法互助与合作而展开,涉及行政、司法、外交乃至国家安全部门等多方主体,其在效率和权责划分上往往面临一定的困境,而监督机构的出现既可以直接行使一定的执法管辖权,又可突破传统的司法互助模式,即通过“全球共管”扩张司法管辖权所能够涵盖的域外对象,也通过单方调查权的行使极大地提高了刑事司法管辖的效率。此外,《108+公约》为网络数据长臂管辖权及其实现路径提供了详细的规范架构,但出于避免管辖权冲突的考虑,除了刻意回避传统管辖原则的适用以外,其在第12条也谨慎地表示:各方应采取有效的制裁与补偿措施以维护公约,但其性质由各国自行决定。这一表述实际是刻意模糊执法管辖权与司法管辖权的界限,弱化二者的区分,强调以制裁与救济是否能够符合立法预期、是否能达到保护个人数据以及隐私权的目的作为评价标准,对于其性质是司法还是非司法,则采取了开放的态度。同时,对于长臂管辖权所解决的争议性质,欧洲理事会的解释也不明确,表示对于司法制裁的性质,为“民事”“刑事”抑或“行政”,都交由缔约国自主确认。无论各缔约国最终如何对管辖权进行定性,《108+公约》无疑架构了新型的域外数据司法管辖权的行使范式,并且这一范式将长臂管辖权的行使由“最低限度联系”带入“全球共管”的新阶段。

(三)《加州法案》:网络数据长臂管辖权的美国新模式

在网络数据长臂管辖权行使的“前时代”,“最低限度联系”作为管辖权确定的标准具有显著的模糊性和软性特征。^③然而,也正是上述特征的存在,使得数据成为法院确认其管辖权的连接点之一,其本质与其他规则,如被告人住所、居所、占有等,并无区别。在《条例》通过后的一周内,美国也出台了《加利福尼亚州消费者隐私法案》(以下简称《加州法案》),该法案对《条例》的部分条款进行了借鉴,尤其是其关于保护管辖原则的扩张与《条例》具有高度的相似性,其规定本法适用于“基于商业目的处理加利福尼亚州境内消费者个人信息的企业”,即使企业没有设立在加州境内,也没有在加利福尼亚州境内从事经营活动,但当企业“存储(包括在设备上)关于消费者的个人信息”“当消费者和存储的个人信息在加利福尼亚州以外时收集该个人信息”,或当企业作为第三方“共享与购买消费者个人信息”时,其便应当接受法案的管辖。此外,对于何为“消费者”,法案给出了较为开放的定义,认为“包含了居住在加利福尼亚州的自然人,也包括因临时或暂时目的在州内居住的人,或因临时或暂时目的而在州外居住的加利福尼亚州居民”。这进一步扩展了法案潜在的适用对象。考虑到美国加利福尼亚州互联网产业的规模及其拥有的巨大经济体量,上述管辖权规则无疑会对全球的相关产业产生不可避免的影响,进而收到“全球共管”的效果。但单就管辖规则而言,《加州法案》与《条例》虽高度相似,但也存在两个显著的区别:(1)《加州法案》规定的是有限度的“全球共管”。因为其对于可能适用的企业设立了以下一个或多个阈值,即年度总收入超过2500万美元,或为了商业目的,每年单独或组合购买、收取、出售或共享5万人甚至更多的消费者、家庭或设备的个人信息,以及通过销售消费者的个人信息获得其年收入的50%甚至更多。正是由于上述阈值的提出,法案的实际管辖范围受到了较大程度的限缩,也避免了类似《条例》“全球共管”模式的出现。(2)《加州法案》并未创设诸如

监督机构的新主体,也未赋予行政机构对境外数据主体的直接执法权力,而是以司法管辖的形式,规定相关主体在总检察长以加利福尼亚州人民的名义提起的民事诉讼中承担民事处罚责任。

可见,在《加州法案》的规范框架下,针对民事诉讼,司法管辖权的域外行使虽然没有采取模糊且软性的“最低限度联系”标准,而是采取了相对明确且硬性的有限“全球共管”模式。不可否认的是,其在客观上扩张了本国司法管辖权的域外范围,赋予了法院“对起诉时与管辖区域有联系的非居民被告的管辖权”,符合长臂管辖的外观要件。同时,阈值标准的创设也并非创新的提法,其参考了美国长臂管辖中有关“正当程序”与“有目的利用”确认的“按比例增减说”,^④该理论根据性质将当事人的活动分为3个层次:(1)当事人通过商业型网站从事商事交易,(2)当事人通过交互型网站进行信息交流,(3)当事人仅仅在网站上提供一些信息。^⑤该理论目前得到美国法院的广泛接受,其核心思想在于网络活动的交互程度和商业性质越强,法院对其行使管辖权的可能性就越大;反之,这种可能性就越小。综上,《加州法案》可视为对传统长臂管辖规则的一次扬弃:一方面,其抛弃了相对模糊的“最低限度联系”标准,既将数据视为确定管辖权的连接点,又将数据视为应加以保护的权利;另一方面,其采纳了传统长臂管辖规则中的部分标准,以限制管辖权的肆意扩张,进而降低了部分规模以下企业的相关成本。

虽然《加州法案》只规定了对民事责任的承担,但是这并不意味着当前美国网络数据长臂管辖只涵盖民事争议而不涉及刑事争议。实际上,美国于2018年通过的《域外数据澄清法案》(以下简称《云法案》)便已经将实体领土之上的单方域外数据调查取证权即刑事执法管辖权的域外行使,以立法的形式延伸到网络空间。《云法案》基于单方的属人管辖扩张解释,推动了域外数据调查与取证由“数据储存地模式”向“数据控制者模式”的转变,其规定网络运营者具有调查取证的配合义务,以确保美国政府能够获得储存于海外的美国公民的个人数据,即电子通

信服务或远程计算机服务提供者有义务披露其所拥有、监护或控制的美国公民的个人信息,包括有线或电子通信的内容、相关记录及其他相关信息,无论上述信息是否储存在美国境内。《云法案》的出现实际上赋予了属人管辖更为优先的适用顺位,其在规范中也开宗明义地表示:立法目的就是授权美国执法部门在云计算技术的背景下通过服务提供者获取境外数据。因此,虽然当前针对网络数据,域外刑事司法管辖权尚未得到美国立法的明确背书,但是考虑到美国自1922年起所确立的长臂司法管辖传统,^④加之现今单方授权的域外数据调查权的立法确认,我们有理由相信,刑事执法管辖权的“长臂化”必然会进一步带动“加州模式”由民事诉讼到刑事诉讼的覆盖。

《加州法案》并非个例,而是目前美国各州数据立法以及长臂管辖的一个代表或缩影,更是国际立法趋势的反映。在美国,除加利福尼亚州之外,华盛顿州、纽约州、新泽西州、伊利诺伊州等州也相继提出了议案。2019年华盛顿州议员提出了《华盛顿隐私法案》,成为继《加州法案》外的第二部综合性的数据隐私保护立法。在各州立法的推动以及科技巨头、民间组织的呼吁下,美国联邦层面也开始采取行动。美国参议院先后提出了《数据保障法案》《美国数据传播法案》《社交媒体隐私和消费者权益法案》《数字问责制和透明度以提升隐私保护法案》。美国众议院也提出了《加密法案》《信息透明度和个人数据控制法案》《应用程序隐私、保护和安全法案》《数据经纪人问责制和透明度法案》《数据问责和信任法案》等多项提案。虽然对联邦政府是否需要制定统一立法、是否应当纳入数据主体的范围、如何设计救济机制等问题存在诸多争议,但是自2018年《云法案》出台以来,扩张性地对管辖原则加以解释,并基于此扩张性地行使执法与司法管辖权已经成为趋势,考虑到美国作为长臂管辖的起源国,长期的司法实践侧重于发展并丰富有关属人管辖权的行使依据,^⑤并且依托自身的全球霸权地位,美国对于规则的制定、规范的执行和最后的裁判已经完成由“运动

员”向“裁判员”的转变,因此“加州模式”的“全美推进”以及“刑民全覆盖”应是必然的结果。

(四)评价与总结

《条例》开启了网络数据长臂管辖权行使的“新时代”,其主要体现在以下两点:(1)若严格以最初的定义为评判标准,则《108+公约》和《加州法案》所确立的模式都很难被定义为长臂管辖,二者都没有采取传统的“最低限度联系”标准,而是借鉴《条例》的“全球共管”模式来指导管辖规则的设计。但若以结果为导向,则《108+公约》所设立的监督机构具有司法机构的色彩,其可以代替检察官将数据争议提交至缔约国国内司法机构,而《加州法案》则直接规定以民事诉讼的形式来对相关主体加以制裁。同时,上述两类模式与传统意义上的长臂管辖都极端地扩张了本国司法管辖的域外范围,也都属于“对起诉时与管辖区域有联系的非居民被告的管辖权”。基于此,上述两种司法管辖模式从广义的角度看,无疑又是可以被归类于长臂管辖权的。(2)回溯网络数据与长臂管辖的结合伊始,我们不难发现,数据主要被视为确立管辖权所依据的连接点,其服务的依旧是数据背后的实体权益,但在《108+公约》与《加州法案》的制度架构下,数据“反客为主”,除了继续发挥其“连接点”的功能之外,其本身亦成为一项立法加以直接保护的权益,成为管辖权直接针对的对象。然而,数据的虚拟性特征以及数据的常态化跨境流动使得相关管辖权的行使很难完全因循旧例。但也正是上述特征促使长臂管辖权的网络行使走向“全球共管”这一不同以往的崭新模式。当然,我们也应注意到,上述美欧模式的兴起,体现了在互联网技术发展的大背景下,物理联系作为域外管辖权行使标准的式微,也反映出当下网络自由主义对管辖权行使的导向。从当前的实践看,美欧二者的模式都值得我们加以警惕,尤其是《108+公约》,司法管辖的单方扩张一方面将使网络经营者时时受制于其从未实际接触的区域管辖,极大地加重了网络经营者的成本与负担;另一方面,出于对数据资源的争夺以及针对恶意管辖的防御,也会进一步刺激各国的“跟风立

法”与“焦虑移植”，进而直接造成管辖权冲突的泛滥以及争讼的常态化。

四、中国网络数据长臂管辖权模式构建的若干思考

面对已成趋势的域外数据司法管辖权的单方扩张，我国一方面需要在立足维护我国数据主权的核心立场之上，寻求更有效的反制途径，以抵御来自域外的恶意管辖，进而实现国家对数据的最高控制权；另一方面，我们也有必要在结合当前国际法规范与国际关系基本准则的基础上，统筹研判数据主权和数据治理的内在逻辑联系和外在规范支撑，以构建符合我国国情与当前发展需求的网络数据长臂管辖权模式。

（一）中国模式的应然架构

当前，无论是国际法规范还是国内法规范，对于传统的“最低限度联系”标准都持负面态度，该标准从一开始就受到各国的普遍谴责，被认为是对国际法基本原则的违反。^⑧美欧全新管辖规则的构建已经摒弃“最低限度联系”标准，转而借鉴并参照保护管辖原则的法理内涵，虽然这种“全球共管”模式依旧存在一定的单边主义色彩，但是上述实践也同样表明，域外数据管辖权的行使与网络主权以及数据主权并非存在天然的冲突，网络数据长臂管辖权的行使与国际法规范也并非存在无解的僵局。应然的协调是存在的，并且这种协调也是我国在构建网络数据长臂管辖权模式中应当明确的基本架构。要构建上述架构，我们应从程序与价值两个方面来加以设计。首先，就程序方面而言，主要应包含3个要求：（1）针对网络数据，长臂管辖权应建立在立法管辖权域外行使这一前提条件之上，即通过立法的形式确定我国司法机构域外管辖权的享有以及我国国内法域外适用的可能；（2）长臂管辖权针对民事诉讼，应当赋予公民对域外相关主体提起数据侵权之诉的可能与路径；（3）长臂管辖权针对刑事诉讼，也应当确立全新的刑事执法管辖权域外行使模式，以便利我国的域外取证、调查等权力的行使。其次，就价值方面而言，中国模式的架构要求我们必须对两个方面的平

衡加以维持，即承认并尊重他国网络主权、数据主权与管辖权域外行使的平衡，以及管辖权域外行使与网络数据跨境流动的平衡。为达致上述平衡，我们一方面应严格限制扩张性管辖规则的适用，坚持以利害关系为导向，对于直接主体加以优先管辖，对于上下游的间接主体，非基于国家安全或公共利益，则不予以管辖；另一方面也应当寻求多元化的数据管辖合作模式，在有法可依的前提之下，寻求法外合作，构建“法中法”与“法外法”，以减少管辖冲突产生的可能性。

（二）中国模式构建的现实困境

实际上，考察相关国内立法，我国已经开始初步寻求建立符合自身需求的长臂管辖权模式。2016年《中华人民共和国网络安全法》（以下简称《网络安全法》）第5条明确规定：“监测、防御、处置来源于中华人民共和国境内外的数据安全风险和威胁”；2021年《中华人民共和国数据安全法》（以下简称《数据安全法》）第2条明确规定：“中华人民共和国境外的组织、个人开展数据活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任”。同时，《网络安全法》第74条规定：“违反本法规定，给他人造成损害的，依法承担民事责任。违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任”；《数据安全法》也在第6章规定了多样化的行政与刑事处罚措施。从规范层面分析，这两部法律无疑是具有域外效力的，并且管辖权域外行使所依据的主要是保护管辖原则。从具体的制裁类型看，上述相关规定结合了执法管辖与司法管辖两类权力的行使，覆盖了民事与刑事两种类型的争议解决。上述规范可以说为我国域外数据司法管辖权的行使提供了良好的法律依据。

虽然《网络安全法》和《数据安全法》为我国域外数据司法管辖权的行使提供了可能，但是面对网络这一特殊环境，为确保上述权力实际行使的可能性，就程序方面而言，我国当前立法还存在如下两个方面的主要问题：（1）从民事责任追究的角度看，对于数

据侵权,虽然这两部法律都明确行为人承担民事责任的可能性,但是以《数据安全法》为例,其仅仅赋予组织或个人投诉与举报的权利,对于私人主体是否可以就域外主体的数据侵权行为提起诉讼则未作出规定。同时,《中华人民共和国涉外民事法律关系适用法》第44条规定:“侵权责任,适用侵权行为地法律,但当事人有共同经常居所地的,适用共同经常居所地法律”。而侵权行为地,依照《中华人民共和国民事诉讼法》的规定,包括行为地和结果地两处。上述规范结合《数据安全法》《网络安全法》的相关规定,共同确定我国法院对相关域外数据争议享有管辖权,但如果参考1986年《中华人民共和国民事诉讼法通则》第12条关于我国民法地域适用的规定,并考虑到2020年《中华人民共和国民法典》并未纳入法律适用的前提下,^⑨那么就会发现《网络安全法》和《数据安全法》仅仅确立了针对域外数据及其相关主体的民事司法管辖权的存在,由于其依旧强调司法管辖对于相关法律法规的“依据”或者仅仅以“依法承担民事责任”这一概括性的表述来代替,因而在具体管辖过程中会不可避免地出现缺乏民事法律规范支持的情况,简言之,即会出现“有权无法”的困境,同时,这种确权也可能进一步由于“属地优先”而让诉于外。

(2)从刑事争议解决的角度看,虽然《网络安全法》和《数据安全法》都赋予了司法机构对域外数据相关主体加以刑事管辖的可能性,但是《数据安全法》仅在第36条明确了境外执法机构对储存于我国境内数据的调查取证程序,对于我国执法机构的相关权力则未涉及,因此参照部门法的相关规定,针对域外数据,我国刑事司法管辖权的行使仍需基于司法互助与合作而展开。^⑩参考《布鲁塞尔民商事案件管辖权和判决的承认与执行规则》《关于在民事或商业事务中向国外提供证据的海牙公约》等国际性立法则会发现,司法互助程序本身是高代价以及耗时的,^⑪对于结果也缺乏可预测性,因此当前各国实际上也在积极地构建新型的司法互助机制,如《云法案》在确定本国对于域外数据单方获取的同时,对于域外主体相应地获取在美数据,也规定了严苛的标准,其规

定司法执行协议订立的基础是请求国属于“适格外国政府”,对于何为“适格”,则参考美国司法部长的相关表述,判断的核心在于外国政府的国内立法是否“提供了对隐私和公民权利强健的实质和程序上的保护”,同时也应考虑国内立法完备与否、人权的尊重与否以及互联网开放与数据的自由流动程度等方面的因素。^⑫类似的条款与要求也出现在《条例》和《亚太经济合作组织隐私框架》下的“跨境隐私规则体系”之中。可以说,上述门槛的存在对于我国参与国际数据司法协作与合作而言,无疑是一个巨大的障碍。基于此,如果严格遵从《中华人民共和国民事诉讼法》有关司法互助的相关规定,那么面对新形势与新技术的发展,则刑事执法管辖权的域外行使无法突破,我国刑事司法管辖权也将由于缺少前期程序,包括调查、取证等,而陷入“形式可能”而“实质不可能”的僵局。

(三)中国模式当前的应然突破

为了解决我国当前司法管辖权域外行使存在的“有权无法”困境以及破解“形式可能”而“实质不可能”的僵局,针对网络数据,现阶段的立法工作无疑需要对如下关键方面加以重点突破。

首先,在不与现有部门法相冲突的情况下,最为直接且有效的措施便是对网络空间的“域外”与“域内”加以再解读,力求将域外管辖“域内化”。具体来说,当前,以民法为代表的我国部门法虽然推崇属地优先主义,^⑬但是对于何为“域内”却没有结合跨境数据流动这一现象加以再解读。数据跨境流动在概念层面于20世纪70年代首先由经济合作与发展组织采用,指的是点到点的跨越国家政治疆界的数字化数据传递。^⑭“域内”与“域外”的区分主要服务于执法调查权的行使,^⑮而当前得到较多接受的观点是储存地模式,即对于一国而言,其依据属地管辖无法获取的数据都可以视为“域外数据”。^⑯同时,对于“域内”包含的具体场景,美欧的司法实践普遍认为一国在以下3种情况下可以依据属地管辖原则对其领土内的信息进行管辖:(1)信息的接受点在该国领土内;(2)信息的发出点在该国领土内;(3)当信息在一国领

土内的线路或网络中传播时,该国可以对此信息享有管辖权。^④实际上,我国可以参考上述观点,将接受点与发出点在我国国内的数据,以及在我国领土内的线路或网络中传播的数据纳入属地管辖的范围。这是为我国当前立法所忽视的。如果参考上述观点,考虑到数据侵权可以视为一个连续性的行为,那么当信息接收点位于我国,必然意味着其经由我国线路或网络传播,因而对其行使司法管辖权就可视为域内而非域外管辖,相应的,便不存在域外法律适用的问题,“有权无法”的困境也能够得到一定程度的缓解。

其次,确立我国法院基于国家安全及公共利益优先行使管辖的可能性。属地优先原则长期以来都是国际公认的管辖权冲突解决原则,但构建网络数据长臂管辖权的中国模式,有力保障我国司法主权及数据安全,面对物理联系式微的网络空间,一味地推崇属地优先原则与当前的国际实践以及我国的现实需求不相符合。当前,《网络安全法》和《数据安全法》都包含“国家安全”及“社会公共利益”保障的相关条款,基于此,对于关键领域及核心利益,面对域外违法行为,我们应当在管辖原则的适用上摒弃“绝对属地主义”思想,从立法层面将保护主义原则的适用优先性加以提升,以便利我国司法机构对关键利益的维护以及参与全球治理。可以说,上述构思的落实一方面将有利于打破我国长臂管辖权刑事适用所面临的“实质不可行”的僵局,另一方面也符合中国模式在价值层面的主张,即在坚持以实害结果为导向的基础上严格限制管辖权的扩张适用。

最后,确立基于“对等原则”的事前阻断与事后反制。在实体领土之上,司法管辖权的域外行使需要基于司法互助与合作而展开,无论是调查权的行使还是文书的送达,缺少协作的单方行为不但难以操作,而且有可能被视为对主权的威胁或侵犯。但在无边际的网络空间中,上述阻碍则并非难以逾越,基于云计算的发展,考虑到数据的常态性跨境流动与“离散型储存”,司法协助及合作的价值也被互联网技术所削弱,以《云法案》为代表的美欧网络数据

长臂管辖权的行使,往往建立在单方域外调查权的基础之上,即基于“数据控制者模式”,单边授权收集储存于境外服务器或处于跨境流动中的数据。然而,对我国而言,完全借鉴或移植美国模式也会造成侵害他国司法主权及数据主权的后果,但如果完全因循传统司法互助模式,那么将不利于我国司法管辖权的域外行使,同时在面对域外恶意管辖时,也将失去“战略上的对冲”。^⑤面对这一两难处境,我国应当在充分利用数据流动性的基础上,确立我国刑事执法管辖权的域外效力,保留基于“数据控制者模式”行使域外数据调查的权力:一方面,确定对于“发出点”与“接收点”为我国的数据,以及在我国领土内线路或网络传播的数据的属地管辖,无论其控制者是域内还是域外主体;另一方面,对于我国数据控制者存储于域外的数据,依照“对等原则”给予单方的保留或管辖。上述措施可以视为一种事前的阻断机制,而《数据安全法》在第26条亦赋予我国相关部门针对他国或者地区的“歧视性的禁止、限制或者其他类似措施”加以对等反制的权力,这可视为一种事后的对等反制机制,主要涉及“数据和数据开发利用技术等有关的投资、贸易方面”。此外,我们还可以参考2021年1月商务部出台的《阻断外国法律与措施不当域外适用办法》第8条和第9条的规定,对等反制的具体内容在上述规则中有相对详尽的说明,主要包括(受侵害的)国内主体申请“豁免遵守禁令”或通过诉讼要求“对等赔偿损失”两种手段。参考上述规制方法,我们不难发现,基于“对等原则”的反制与阻断已经得到我国当前立法的重视,并且我国在投资与贸易等重点领域也已经初步建立一套相应的事后处罚机制,但对于事前机制的构建,尤其是对域外恶意执法管辖权的阻断,还有待加强。毕竟,如果从效果与效率方面看,对于前置性司法程序的事前阻断要显著优于对域外恶意司法管辖的事后反制。

此外,基于中国模式在价值层面的应然内涵,我们也应积极地寻求国际间合作的可能,为司法管辖权域外的行使提供更多新模式与新可能。例如,与他国点对点地建立包括“安全港”协议在内的更为高

效便捷的双边网络数据协作机制;或者有条件地加入如亚太经合组织跨境隐私规则这一类体系,并将规则的认证标准与模式向潜在缔约方推广;亦可将域外数据管辖相关内容纳入自由贸易协定等谈判之中,进而将跨境数据流动规则纳入具有法律约束力的协议中,使得跨境数据流动规则融入全球经贸规则体系。

五、结语

基于保护管辖原则的单方扩张解读,网络数据长臂管辖权经历了由“前时代”向“新时代”的转变,也由“最低限度联系”标准迈向了“全球共管”模式。2021年《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》明确提出,“健全国家网络安全法律法规和制度标准,加强重要领域数据资源、重要网络和信息系统安全保障”以及推动“制定数字和网络空间国际规则”。在当前长臂管辖权扩张已渐成趋势的大背景下,我国作为网络强国,面对外部威胁,要实现上述愿景:一方面应缓和长臂管辖权行使与网络主权以及数据主权天然存在的冲突,正视欧美模式的有益价值并加以跟进,探究构建符合我国国情及社会需求的司法管辖权域外行使新模式;另一方面,作为数据大国,在完善立法的同时,也应当积极寻求网络治理与数据管辖的多边合作,在有法可依的基础上,构建国际合作的“法中法”与“法外法”,实现由国际规则参与者向国际规则制定者的转变。可以说,构建网络数据长臂管辖权的中国模式应是我国当前数据立法的重点所在,其既是有效维护我国司法主权、国家安全以及公民隐私权的应然需求,也是加强我国在参与国际数据合作体系过程中的竞争力以及话语权,进一步构建网络空间命运共同体,维护和平安全、促进开放合作、构建良好秩序的重要法律保障。

注释:

① See Neil Robinson, Review of the European Data Protection Directive, 2 *Rand Europe*, 23(2009).

② 参见曾令良、江国青、周忠海主编:《国际公法学》,高等

教育出版社2018年版,第118~121页。

③ See Harold G Maier, Extraterritorial Jurisdiction at a Crossroads: An Intersection Between Public and Private International Law, 76 *American Journal of International Law*, 280(1982); Anthony J. Colangelo, What is Extraterritorial Jurisdiction, 99 *Cornell Law Review*, 1310(2013).

④ 参见李庆明:《论美国域外管辖:概念、实践及中国因应》,《国际法研究》2019年第3期。

⑤ 参见肖永平:《“长臂管辖权”的法理分析与对策研究》,《中国法学》2019年第6期。

⑥ 参见[美]理查德·弗里尔:《美国民事诉讼法》(上),张利民译,商务印书馆2013版,第47页。

⑦ 参见肖永平:《“长臂管辖权”的法理分析与对策研究》,《中国法学》2019年第6期。

⑧ See Bryan A. Garner, *Black's Law Dictionary*, West Group, 8th ed., 2004, p.2758.

⑨ See Anthony J Colangelo, What is Extraterritorial Jurisdiction, 99 *Cornell Law Review*, 1303(2013).

⑩ See *International Shoe Co. v. Washington*, 326 U.S. 310 (1945).

⑪ 参见郭玉军、向再胜:《网络案件中美国法院的长臂管辖权》,《中国法学》2002年第6期。

⑫ 参见李庆明:《论美国域外管辖:概念、实践及中国因应》,《国际法研究》2019年第3期。

⑬ See Herdegan & Matthias, *Restatement Third, Restatement of the Foreign Relations Law of the United States*, 39 *The American Journal of Comparative Law*, 207(1987).

⑭ See John H Currie, *Public International Law*, Irwin Law Press, 2008, p.301.

⑮ 参见梁坤:《基于数据主权的国家刑事取证管辖模式》,《法学研究》2019年第2期。

⑯ See Derek W Bowett, *Jurisdiction: Changing Patterns of Authority over Activities and Resources*, 53 *British Yearbook of International Law*, 567(1983).

⑰ 参见郭玉军、向再胜:《网络案件中美国法院的长臂管辖权》,《中国法学》2002年第6期。

⑱ See *International Shoe Co. v. Washington*, 326 U.S.310 (1945).

⑲ See *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297(1980); *Burger King v. Rudzewicz*, 471 U.S. 462, 475 (1985); *Asahi Metal Indus. Corp., Ltd. v. Superior Court of Cal.*, 480 U.S.102(1987).

⑳ See *California Software Inc. v. Reliability Research*, 631 F. Supp. 1356(C.D. Cal. 1986).

㉑ See *Complaint of Securities and Exchange Commission*

(SEC) of Case "SEC v. Alcatel-Lucent", S.A., 10-cv-24620, 2010, <http://fcpa.stanford.edu/fcpac/documents/2000/000654.pdf>, 2021-07-01.

② See Annalisa Leibold, Extraterritorial Application of the FCPA Under International Law, 51 Willamette Law Review, 228 (2014); Heidi L. Hansberry, In Spite of Its Good Intentions, The Dodd-Frank Act Has Created a FCPA Monster, 102 Journal of Criminal Law and Criminology, 200(2012).

③ 参见郭明磊、刘朝晖：《美国法院长臂管辖权在 Internet 案件中的扩张》，《河北法学》2001 年第 1 期。

④ See Beata A. Safari, Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, 47 Seton Hall Law Review, 812(2016).

⑤ 《欧盟一般数据保护条例》第 83 条规定了两种处罚标准：(1) 上限 1000 万欧元，或全球年营业额的 2%，取较大者；(2) 上限 2000 万欧元，或全球年营业额的 4%，取较大者。但《欧盟数字市场法》的处罚标准是：企业全球年收入 10% 的罚款或最高可达企业全球日收入 5% 的定期罚款。后者的处罚标准显然是要高于前者的处罚标准。

⑥ See Kavita M Berger & Phyllis A Schneck, National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data, 7 Frontiers in Bioengineering and Biotechnology, 23(2019).

⑦ See Brazilian General Data Protection Law, 2018, <https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-Data-Protection-Law.pdf>, 2021-07-01.

⑧ See The Personal Data Protection Bill, 2019, https://iapp.org/media/pdf/resource_center/India_Draft_Personal_Data_Protection_Bill.pdf, 2021-07-01.

⑨ 该公约在欧洲理事会《欧洲条约集》中的编号为 108，通常被习惯性地称为《108 号公约》，该公约被公认为最重要的关于个人信息保护的国际公约性法律文件。由于 2018 年在修订之后加入了新的补充议定书，因而被赋予了具有互联网特色的简称，即“108+Convention”，本文便参照此简称，将该公约翻译为《108+公约》。

⑩ 最新签署《108+公约》国家的数目已有媒体进行了报道。See <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures>, 2020-05-01.

⑪ See Council of Europe, Explanatory Report Regard to the Protocol Amending Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Personal Data, Para 119, <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>, 2021-07-01.

⑫ See Council of Europe, Explanatory Report Regard to the Protocol Amending Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Personal Data, Para 123, <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>, 2021-07-01.

⑬ 参见韦燕：《“最低限度联系”与网络管辖权——美国有关网络管辖权的判例及其发展》，《河北法学》2001 年第 1 期。

⑭ 参见郭玉军、向再胜：《网络案件中美国法院的长臂管辖权》，《中国法学》2002 年第 6 期。

⑮ See Bensusan Restaurant Corp. v. King, 937 F.Supp.295 (S.D.N.Y.1996) affd 126 F.3d 25(2d Cir.1997).

⑯ 参见肖永平：《“长臂管辖权”的法理分析与对策研究》，《中国法学》2019 年第 6 期。

⑰ 参见郭玉军、向再胜：《网络案件中美国法院的长臂管辖权》，《中国法学》2002 年第 6 期。

⑱ 参见郭明磊、刘朝晖：《美国法院长臂管辖权在 Internet 案件中的扩张》，《河北法学》2001 年第 1 期。

⑲ 参见肖永平：《“长臂管辖权”的法理分析与对策研究》，《中国法学》2019 年第 6 期。

⑳ 参见谢望原：《域外刑事管辖权及其实现》，《法学论坛》2000 年第 1 期。

㉑ See Secil Bilgic, Something Old, Something New, and Something Moot: The Privacy Crisis under the Cloud Act, 32 Harvard Journal of Law & Technology, 332(2018).

㉒ See Executive Agreements on Access to Data by Foreign Governments, 18 U.S. Code §2523.(b)(1)(B).

㉓ 参见杜涛、肖永平：《全球化时代的中国民法典：属地主义之超越》，《法制与社会发展》2017 年第 3 期。

㉔ 参见程卫东：《跨境数据流动的法律监管》，《政治与法律》1998 年第 3 期。

㉕ See Kathleen Hixson, Extraterritorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States, 12 Fordham International Law Journal, 127(1988).

㉖ See Jennifer Daskal, Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, 8 Journal of National Security Law & Policy, 473(2015); Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review, 729(2016).

㉗ See Scan Kanuck, Sovereign Discourse on Cyber Conflict Under International Law, 88 Texas Law Review, 1573(2010).

㉘ 参见梁坤：《基于数据主权的国家刑事取证管辖模式》，《法学研究》2019 年第 2 期。