数据主权冲突下的跨境电子数据取证研究

廖 斌 刘敏娴

【摘 要】电子数据主权管辖的立法主要有数据控制者管辖模式和数据存储地管辖模式，这两种主权管辖模式的冲突对跨境数据电子数据取证具有较大影响。我国司法机关在数据主权存在管辖冲突的情况下进行跨境电子取证，应坚持国际礼让与互惠、安全保护等原则。为了更好地贯彻总体国家安全观，我国跨境电子数据取证的路径建构应从制度弥补与运行机制入手。一是在立法层面明确我国境内存储的跨境电子数据取证范围和程序，明确我国请求存储于他国的数据的跨境取证的方式，明确对来源不明晰的数据跨境取证的管辖范围和法律适用。二是在制度运行上，制定并增设风险评估机制、规范云服务提供者的审查义务，执行关键信息的报批义务；建立数据“白名单”制度，在国际法框架内积极推进多边协作，为跨境电子取证的数据主权问题提供“中国方案”。

【关 键 词】数据主权；跨境电子取证；跨境取证原则；取证路径；白名单制度

【作者简介】廖斌(1964-)，男，汉族，四川泸州人，广西民族大学法学院教授(广西 南宁 530006)；刘敏娴(1994-)，女，汉族，安徽芜湖人，安徽师范大学法治中国建设研究院研究员(安徽 芜湖 241002)。

【原文出处】《法学杂志》(京)，2021.8.147～161

【基金项目】本文为国家社会科学基金重大项目“大数据、人工智能背景下公安法治建设研究”(项目编号：19ZD166)的阶段性研究成果。

互联网的快捷与便利使得跨境数据流动加快，很多国家对于全球跨境数据特别是重要信息的披露，纷纷采取了相应的保护措施。而随着电子数据越来越多地存储于境外，跨境电子数据主权管辖上的分歧也日益严重，由于其涉及到主权和管辖权，极易引起争议。“不经他国数据主管部门的同意直接跨境获取他国数据，让国家主权无法得到保障，也给违反人权和自由、侵犯用户隐私权留下了空隙。”[①]可以看出，维护数据主权和有效管辖，是各国维护国家主权尊严和国家安全的一个重要问题。因此，为贯彻习近平总书记提出的总体国家安全观，笔者对数据主权下跨境电子取证的对策问题进行研究，希望引起学界更多关注。

一、电子数据主权及其相关法律范畴

(一)电子数据的含义及其类型

电子数据是指任何以电子方式对信息的记录。随着计算机网络的发展，电子数据存在于生活的方方面面。2012年我国修订《民事诉讼法》《刑事诉讼法》后，电子数据作为标准证据种类进入我国法律。电子数据通过介质传递给不同主体，主体通过跨境电子流动的方式将电子数据传递至境内外。在跨境电子数据的取证问题上，电子数据的主权及其权属问题成为了首个有待解决的问题。有学者认为，数据权有以国家为中心的国家数据主权和以个人为中心的数据权利两个维度的含义，其中数据主权包括数据管理权和数据

控制权，数据权利兼具人格权和财产权双重属性。[②]电子数据的流动性使电子数据涉及信息创造者、接受者、使用者等多个主体。在涉及数据主权时，所涉及主体必然会形成主权的重叠甚至冲突，由此也产生了诸如数据的权属、立法规制、监管治理等主权问题。由于电子数据主体关乎跨境取证的有效性问题，厘清不同数据主体是本研究的重要前提。基于数据主体不同，笔者认为跨境电子数据可分为三种类型：

一是个人数据。个人享有数据的所有权，应当包括但不限于普通理解上的个人数据，如个人基本信息、个人在私人社交媒体上发布的言论等。欧盟《通用数据保护条例》(General Data Protection Regulation，以下简称"GDPR")第4条规定"'个人数据'是指与一个确定的或可识别的自然人相关的任何信息。1.可识别的自然人指可以直接或间接识别的人，特别是通过诸如姓名、身份证号码、位置数据、在线身份识别等标识符，或参考与该自然的身体、生理、遗传、心理、经济、文化或社会身份有关的一个或多个因素可被识别的人。"[③]2017年6月1日生效的《中华人民共和国网络安全法》(以下简称《网络安全法》)也在附则第76条中规定"个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。"

二是公共数据。它存在着"公共部门信息的公共属性和私人属性双重特征引起的产权归属问题"，[④]因此这里的公共数据并不会对国家安全或公共利益产生不利影响，否则构成下文所述的关键数据。公共数据主要是指可供使用的但存储于公共空间的数据，包括企事业单位除商业秘密外的公共数据，个人在公共层面匿名化处理过的数据[⑤]等。此种类型的跨境电子数据大多可通过公开方式获取。

三是关键数据。关键数据与国家安全息息相关，涉及到国家能源、信息与通信、交通运输、卫生保健等信息。由于行业特点不同，有些部门行业的公共和个人信息也被视为关键信息。2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过的《中华人民共和国数据安全法》(以下简称《数据安全法》)增加了核心数据的概念，将其范围扩展到国家安全、经济、民生、重大公共利益等多个方面。因此，在跨境电子数据取证过程若出现以上数据类型，就要进行重点保护和管理。

(二)跨境电子数据主权及境内外相关主要立法

传统主权概念，是指一个国家在国际法上所具有的按照本国政权管理者的意志独立自主地处理对内对外事务的权力，其他国家无权以任何形式进行侵犯或干涉。数据主权的主体性问题分为狭义和广义两个派别，前者将数据主权定义为国家数据主权，后者则包含个人数据主权。电子数据主权冲突问题必然包括国家对于主权概念的厘清，具体指国家对数据管理的界限问题以及跨境数据流动中的权属问题。有国外学者将数据主权定义为数据受到其创造地和存储地国家法律约束而形成的国家执法干预和司法主权管辖。[⑥]当前数据主权的范畴问题在学术界尚未有统一结论，大体可概括为两个方面：一是数据的管理和控制权限，二是数据的管辖边界。

跨境电子数据最先需要解决的是数据主权问题。跨境电子数据取证主要针对网络空间，数据的控制与管理权至关重要。学术界也有两种不同的观点：一种是要淡化网络主权这一概念，强调数据是共享的，形成事实意义上的数据交换平衡。美国学者理查德·N.哈斯提出数据主权不应存在，因为主权制度本身已经成为历史发展的障碍。[⑦]

另一种是要增强数据主权认识，对于信息的保护程度应该随之加大。有学者主张数据主权是特定国家最高权力在本国数据领域的外化，以独立性、自主性和排他性为根本特征。[⑧]根据以上两种观点，形成了中美不同的内部数据控制法律制度。我国学者并未针对跨境电子数据主权提出明确概念。现有文献将这一概念内化到跨境取证的环节之中，强调跨境取证正当性障碍即存在主权冲突。[⑨]笔者认为，电子数据作为法定证据的一种，理应有相对应的主体对此进行监管，将其纳入跨境取证的范围具有现实意义。一方面，电子数据本身可以广泛运用于大数据分析中，其主权所属关乎个人数据权利的适用；另一方面，电子数据所记载的内容具有信息保护价值，将其纳入主权保护范围内有利于国家安全，符合国家大安全观的要求。引用前述概念，可将其分为国家层面的国家电子数据主权以及个人层面的电子数据权利。在此基础上，了解并熟知有关国家立法是解决这一问题的关键。

美国于1967年7月6日开始实施《信息自由法案》。作为世界上最早出台的信息保护法律，《信息自由法案》体现了美国在数据控制权上的主张。该法案后经多次修正，截至2002年美国将1996年颁布的《电子信息自由法案》与1986年修正的《信息自由法案》合订，前后共经过10次修正。《信息自由法案》中的信息物理载体也演化成了“电子数据”这一概念。为适应国际竞争加剧和恐怖主义抬头的趋势，美国在该法案的修订上更加强调信息安全的重要性，也逐渐形成了美国的数据主权思想。1974年，美国颁布的《隐私权法》规定了政府机构不得未经信息当事人的书面同意披露信息，规制联邦政府对个人隐私数据的收集和使用，将内部公共数据与个人数据分开管理。随后在1986年和1987年，美国又分别出台了《电子通信隐私法》《计算机安全法》，前者赋予政府执法机构搜查用户的权利，后者引入了第三方数据机构技术局作为专门机关负责处理有关信息，这一举措也将内部交叉流动中的所有介质归为同一管理机构之下。2001年《爱国者法案》将美国领土及美国籍信息纳入信息管控范围，2013年《网络安全保护令》则对美国全境数据及网络基础设施进行控制，模糊了个人数据、公共数据与关键数据的界限。2018年3月23日，美国总统签署生效了《澄清境外数据的合法使用法案》(以下简称“云法案”)。在“云法案”下，如果客户受美国管辖，美国政府可以直接对该客户启动法律程序。该客户随后可以要求网络服务者传输相关数据给他，以便其按照法律程序及要求披露数据。该法案自2018年2月6日提出，在一个半月内即从草案转为正式法律，可见美国对境外数据保护的重视。该法案出台的诱因是美国微软公司拒绝将存储在爱尔兰都柏林云服务器中的用户信息提交给美国执法人员，理由是该数据属于境外数据，不属于美国的地域管辖范畴。“云法案”授权美国执法部门在特定案件中要求电子通讯服务提供者提供处于其控制之下的电子数据，而不论该电子数据存储于美国境内或境外。该法案的出台为美国执法者收集境外电子证据提供了有力支撑。但美国的“云法案”被普遍认为违反了国际法上的国家主权原则。通观美国数据主权制度建设的历史，可以发现美国采取的各项措施都是为其建立美国领先意义上的数据主权制度打基础，在国家、企业与个人之间寻找相互配合的机制以达到美国政府控制境内数据甚至境外数据的目的。尽管美国在国际社会中一直强调其数据自由的主张，官方不承认数据主权概念，但从其立法仍然可以看出其维护本土数据以及模糊个人、社会和重要数据提取界限的趋势。

与美国相比，我国一直强调数据主权是国家主权中网络主权的重要组成部分。早在2010年，《中国互联网白皮书》就提出“中华人民共和国境

内互联网属于中国主权管辖范围”的主张。[10]2020年9月8日外交部网站发布了“全球数据安全倡议”,明确指出各国有责任保护涉及本国国家安全、公共安全、经济安全和社会稳定的重要数据及个人数据安全。[11]从中国在国际社会上的发言可以看出,我国向来支持网络主权及数据主权。立法上,与美国相比,我国关于跨境数据的交叉性立法大多分散于各个部门法中。《民法总则》第111条首次提出“个人信息受法律保护”。[12]2017年实施的《网络安全法》第37条规定:“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储”,通过立法加强了对涉外电子数据的主权管控,一定程度上解决了跨境取证难的问题。该法的颁布也催生行政机关出台了大量相关规范性文件。2019年,国家互联网信息办公室联合公安部办公厅等部门出台了《App违法违规收集使用个人信息行为认定方法》,全国信息安全标准化技术委员会组织编辑的《信息安全技术个人信息安全规范》草案中增加了不得强迫收集个人信息等要求。但遗憾的是,对于政府出于国家安全需要收集信息或个人在公共空间内存储数据,国内并没有相关立法给出相应的解决方式,现阶段仍存在超范围、超目的使用个人信息的现象。这些信息是否传输至境外或者是否可能被黑客利用,是需要引起重视的问题。存储于企业云端的数据一旦遭到泄露,可能会给个人甚至整个国家带来不可逆转的损失。目前我国的数据控制主体在法律层面上还有发挥作用的空间,对于跨境电子数据的规范和保护起着至关重要的作用。2021年6月10日第十三届全国人大常委会审议通过的《中华人民共和国数据安全法》第六章法律责任中提出了相关组织和个人不维护数据安全的惩罚制度。2018年10月26日十三届全国大人常委会第六次会议通过的《国际刑事司法协助法》,就刑事调查取证在第4条第3款规定:“非经中华人民共和国主管机关同意,外国机构、组织和个人不得在中华人民共和国境内进行本法规定的刑事诉讼活动,中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和本法规定的协助。”相信在可预见的将来,国内关于跨境数据流动的立法将切实保护各类数据信息,更好地维护我国数据主权的主张。

二、跨境电子数据主权管辖冲突对跨境电子数据取证的影响

跨境电子数据取证过程中一旦发生数据主权问题争论,轻则影响惩罚犯罪的进程,重则影响两国外交关系甚至引起外交事件。从传统意义上来看,国家的刑事管辖向来以主权范围内的地域为基础,因此跨境的数据获取与取证也应当在这一范围内进行。然而电子数据极易在境内外流动,挑战了传统刑事主权边界。立法者对于网络的“境”如何定义并未给出答案,因此产生了主权冲突问题。由于国际上尚未形成统一的数据管辖规则,各国均自行制定符合其国家利益的数据主权管辖规则。在跨境数据外部交互流动中,数据主权冲突实际是由域外法律适用的不同导致的。目前,数据主权在确定标准问题上形成了全球两种主要数据管辖模式。

一是数据控制者管辖模式。该模式以美国的“云法案”为代表,无论通信、信息或其他信息是否存储在美国境内,服务提供者都有提供、披露该信息的义务,只要该信息由服务者监管或控制。[13]美国执法机构有权通过电子通讯服务或者远程计算机服务的提供者调取存储于境外的数据。这种模式实际确立了“长臂管辖”制度。“云法案”主要内容涉及的数据主权问题体现在两个方面:一是法案针对的对象为美国籍和居住在美国境内的人,因此长期生活在他国的美国公民所搜集的电子数据信息必然是“云法案”的保护对象。此举无疑增加了有损他国国家数据主权安全的可能性。二是

“适格外国政府”中“适格”一词的判断过于主观。法案明确要求外国政府在进行跨境电子数据取证时，美国执法机构应当评判该国是否在网络犯罪和电子证据方面拥有充分的实体性和程序性规定，以及该国是否加入了《网络犯罪公约》以及立法是否符合公约第1、2章[14]的规定。然而，由于《网络犯罪公约》的签署国较少，大批量的国家不足以被认定为“适格政府”，其跨境电子数据取证也无从谈起。即使“有幸”被认定为“适格政府”，其取证之路也并非一帆风顺。“云法案”对披露的数据、主体、程序等均有严格要求。“‘数据控制者标准’突破了物理空间的主权管辖范围，在数据流动可能产生的诸多管辖权关联的节点中，通过强化属人化的数据属性设定，将法律管辖权确立为数据控制者所在地。”[15]作为数据大国，美国跨国公司数量多且技术发达，在并未明确区分数据类型的情况下，“云法案”的确立实质上将其“长臂管辖”制度伸向了全球各个国家和地区，为美国执法者单边获取他国境内的电子数据证据提供了法律依据，为其“数据霸权主义”披上了合法外衣，也给我国的数据主权保护带来了挑战。

二是数据存储地管辖模式。此模式即国家通过法律强制规定对数据进行本地存储，并按照传统的刑事司法协助方式跨境收集电子数据。与数据控制者管辖模式不同，这本质上是一种应对“长臂管辖”的防守型政策，这种跨境取证的方式要求各国对数据存储模式有清晰的规范。中国和俄罗斯采用了比较严格的数据存储地管辖模式，通过数据本地化解决法律适用与执法问题。2014年，俄罗斯总统普京签署联邦242号法令，在《关于信息、信息技术和信息保护法》第16条中增加了个人信息数据提取需在俄罗斯境内的规定。[16]在《俄罗斯联邦个人数据法》中增加了运营商要保证使用俄罗斯境内的数据库的规定。[17]而我国在《网络安全法》第37条做了相关规定，对于执法取证更是出台了《中华人民共和国国际刑事司法协助法》等特别法，对取证的数据主权加以明确的相应限制。其他国家的跨境数据本地化政策虽无中国与俄罗斯严格，但也在不同程度上进行了限制。印度为促进本国经济发展，在《电子商务框架草案》中列出了大量数据本地化的豁免情形，如基于合同目的的数据传输等，但要求在跨境流动前在本国的数据中心备份。[18]2018年5月28日欧盟出台的《通用数据保护条例》(GDPR)，作为约束企业的条例，其属于事实上的本地化政策，但近年不断扩大其长臂管辖的范围，使其条例目的不再纯粹。一方面，欧盟立法者想通过GDPR制度设计强化对欧盟各国自身的网络数据控制主权，为个人数据处理主体提供国家合法性保护，降低境外国家对其运营的干涉；另一方面，欧盟又想通过提升数据治理水平在世界数字经济中谋求主导地位，将网络数据治理制度规范扩展适用于处理欧盟主体个人数据的所有外国主体，其对有关数据保护的执法力度显著加强。预计今后欧盟还会出台《网络安全法》《电子证据条例》等规范，以与其他大国在网络治理、数据治理的博弈中取得主动权。综上，作为一种防御性的政策，数据本地化实际是国家主权的直接参与模式，此种模式下数据的保密性得以提升。对于跨境电子数据取证而言，这种模式虽然会减少国家受到其他国家或集体的攻击，但由于对于数据主权采取了严格的保护措施，跨境取证的难度也相应加大。我国在跨境电子数据取证方面目前只能通过国际刑事司法协助的方式来完成。

总之，两种数据管辖模式均会对后续跨境电子数据取证的具体路径产生影响。采用数据存储地模式的国家在跨境数据取证时需将是否属于国家数据、社会公共数据、个人数据进行厘清，因此可能产生涉及部门多、人员广等问题，不利于快速便捷地取证。数据控制者模式的国家在取证时，

需要征得数据所属国家同意，涉及数据所有者、接触者、服务者、管理者等多个主体，也可能会影响跨境电子数据取证的效率。这两者都存在一定程度的弊端，前者适用于以地域为管辖范围的传统国家，保护性的策略可能会限制跨境电子数据的流通问题；后者若适用于数据大国则其可能利用数据领先地位威胁弱势国家的数据安全。可见，数据主权管辖模式的冲突必然会给跨境电子数据取证带来程序上的限制和实际执法的影响，国际司法协助也无法解决一些“暗网”数据的取证问题，因此在跨境电子数据取证上有必要加强国内立法、完善司法适用，真正实现对跨境网络犯罪的有效打击。

三、我国跨境电子数据取证应遵循的原则

尽管各国对于数据的控制权和管辖权都有不同的定义，但面对日益增长的网络犯罪和国际恐怖主义犯罪，全球在一定范围内还是形成了有关跨境电子数据取证的一般性共识。从当今世界“和平与发展”的主题入手，根植于《联合国宪章》的基本精神，一些原则成为如今跨境电子数据取证的基本遵循，逐渐被世界各国所接受，成为全球网络空间治理的行为规范和国际法准则。

(一)主权尊重原则

联合国《刑事诉讼转移示范条约》的序言规定，“希望根据尊重国家主权和管辖权的原则以及互不干涉国家内政的原则进一步加强在刑事司法方面的国际合作与互助。”[19]根据国际法的一般原理，主权尊重是国际交流的基本准则，跨境电子数据证据取证也不例外。该原则可能会面临两方面冲突：一方面，该行为为司法取证行为，可能涉及到损害他国国家主权的问题；另一方面，其取证的数据也可能涉及到他国数据主权的问题。从全球跨国取证的形式来看，司法协助仍是取证的主流，即请求国的国家申请取证——被请求国国家接受申请的模式。在这一过程中，相关机构是否申请、是否接受申请以及如何给予材料、给予哪些材料等都由各个国家自己决定，对于主权尊重的要求也随之提高。在保护自身合法利益的前提下，双方不干涉对方内政，互相尊重司法主权和数据主权。

(二)国际礼让与互惠原则

国际礼让原则是解决国家间冲突的一项基本原则，指的是在不损害国家与人民利益的情况下，可以承认其他国家法律在本国境内的效力。国际礼让原则在于维护国家主权及数据主权关系，因此该原则有利于平衡数据主权冲突下的国家利益。比如，美国政府在“云法案”中规定的“适格外国政府”制度，实际上是国际礼让原则的重要体现。在跨境电子数据取证过程中，为了回避矛盾焦点及由此产生的数据主权问题，遵守国际礼让原则很有必要。与国际礼让有异曲同工之处的是互惠原则。我国政府为回应美国的“云法案”，颁布了与其对应的《国际刑事司法协助法》。该法规定我国应本着互惠原则开始刑事司法工作，规定了跨境取证的流程和要求，方便打击跨国网络犯罪。在跨境电子数据取证中，国际礼让与互惠原则更多体现在了国家与国家签订的条约协议中。

然而在实际操作过程中，作为“互免签证协议”思路在跨境刑事取证管辖方面的实践，“云法案”的异议程序要求服务提供者申请异议的理由须同时满足信息所涉用户非美国籍且不在美国境内和所要求的信息披露会导致服务提供者触犯某一“适格外国政府”的法律两个条件。这意味着若拒绝提供该信息的服务者并非美国所认定的“适格政府”，则这一请求可能会被法院驳回。国际礼让原则在这一点上可能被政府作为武器来利用。“长臂管辖”原则从解决州际问题不断向域外立法、司法、执法权扩张，不断限制国际礼让原则的适用。[20]国际礼让在本质上成为“少数国家的国际礼让”，即成为了美国及其盟友对于其所称的针对

犯罪的共同打击，但却不能适用于与美国利益有冲突的一部分国家。而我国按照平等互惠原则，在跨境电子数据取证中也有诸多不便。根据规定，一份电子证据的跨境调取往往需要由相对应的国家机关，如法院、检察院、公安部等进行层报，最后需要司法部对外联络机构，甚至于外交部的同意，才可以行动。外国调取我国证据也需要相同的程序。因此，适用国际礼让原则和互惠原则时存在取证程序复杂等问题，而电子证据属于极易变化的证据类型，这对证据的保全与案件的侦办都极其不利。

综上，国际礼让与互惠原则提出的本意是为了更便利地打击犯罪，但实践中复杂的操作使得其目的并不能很好地实现，有待于立法层面进一步规范与解释。

(三)安全保护原则

保护国家与公民信息安全是一个国家进行跨境电子数据取证的基本原则之一。当前国际环境复杂因素与政策不稳定因素并存，跨境电子数据取证困难重重，但各国维护其国家安全、保障公民合法权益的原则不变。根据各国规定，电子数据取证安全保护可以总结为实体安全与信息安全。实体安全保护即保证跨境电子数据取证经过相关法律法规授权，在其范围内取证，也包括数据库、人员、存储系统的安全等。实体安全的保障需要满足前文所述的数据管辖权与控制权的规定，依照主权国家进行安全保障下的取证行为。信息安全保护即保障数据本身不被随意使用、滥用或损毁。大数据时代每一条数据都可能蕴含着数以万计的价值。按照数据种类，不论是个人存储于公众空间内的数据还是企事业本身的数据库，都需要第三方介入，对主体的安全要求应当不仅为单个个体，而是在取证过程中涉及的每个主体。跨境电子数据取证的安全保护原则是各国在全球数据洪流中给自己筑牢的一道防线，都在努力构建属于其自身的安全保障机制。

四、我国跨境电子数据取证的路径建构

美国、欧盟等在加强本国数据保护上采取了一系列技术手段对跨境电子数据取证加以规制。我国目前对于跨境电子数据取证保护规则有一定程度的缺失，技术手段还比较薄弱，数据主权保护能力还存在可提升空间，因此构建跨境电子证据取证的路径架构符合我国保护数据主权的要求。

(一)跨境电子数据取证的制度弥补

1.立法明确我国境内存储的跨境电子数据取证的范围和程序。我国《数据安全法》第2条、第3条分别规定了境内数据的范围。虽然该法第36条对境内调取证据进行了规定，但依旧是延续了《国际刑事司法协助法》第4条的规定，未有更多具体举措，[21]规定了在中国境内的调查取证需经我国机关认可。然而，对于境外违法取证的问题，我国并未确定相应罚则，实践中也并未出现企业因为违法向国外兜售信息而受到处罚的情况。这导致在Gucci案的事件中，美国法院倾向于认为中国政府不会严厉处罚违规向美国提供数据的公司而驳回其国际礼让原则的适用。[22]同时，数据存储地模式使得境外机构在我国进行跨境取证时，需经一系列程序。前文已述，这种模式下的取证并未做到真正互惠。基于此，笔者建议参照《数据安全法》第21条的要求，对于跨境电子数据建立分级管理制度。针对数据管辖权与控制权的争议问题以及可能影响国家安全的跨境取证问题，对数据分级设置不同的保护措施与监管要求。对于实际生活中存在的数据分类不明晰、分类标准不统一等问题，从立法层面加以规制。我们应通过国内立法明确允许他国司法机关在我国取证的范围，建立对不同数据的分类取证模式。2019年，国家互联网信息办公室公布的《个人信息和重要数据出境安全评估办法》(征求意见稿)提出，要建立“主管部门评估——网络运营者自评估”的两级评估

体系，扩大数据出境的评估范围，加强数据出境安全的风险管理等。目前，我国法律仅对重要数据的出境进行了立法上的规制，[23]对于对案件有重要影响的电子数据类型能否通过其他方式调取，并未进行立法限制。数据分级管理措施可以在制度层面上保障数据流出途径的可追溯性，在前置程序上加强对数据主权的保护，减少数据不合理的流出，保护我国数据安全。对于境外机构违法取证问题，在法律层面上应对违规提供数据的境内企业和个人设置相应罚则并切实监管执行。

2.明确我国请求存储于他国的数据的跨境取证方式。除了他国从我国调取电子数据证据的跨境流动问题外，我国从境外调取数据证据也需建立更为明确化的制度规范。我国目前的单边取证方式有获取公开数据、[24]远程勘验、[25]技术侦查[26]三种。然而单边取证方式极易引起主权纠纷，为了更好地从他国取得证据，并体现我国作为一个大国应有的气度，也根据对等原则，我们可以探索跨境电子数据取证的新模式。一方面，在涉及国家安全、恐怖主义、重大社会安全的案件中，为提高办案效率，一些经评估不涉及国家安全的信息、不至于导致外交风险的信息，建议直接由有关执法机构提取使用，鼓励数据依法自由流转。另一方面，有必要通过立法对数据入境程序予以优化。立法明确电子化取证方式的有效性，可以提高他国对我国跨境电子数据取证方式的认可度。有学者提出了“探索通过协议等方式打破取证主体限制和探索视频取证”的主张。[27]电子化取证技术符合当下网络时代的特征，也在一定程度上提高了取证的效率。在满足数据管辖权和控制权的前提下，从立法层面建立有关国家通过包括电子数据取证在内的其他协助方式共同打击跨国犯罪，探索数据立法加强国际对话，可提升我国侦办跨国犯罪的效率，切实保护数据主权。

3.明确对来源不明晰的电子数据跨境取证的管辖范围和法律适用。来源不明晰的电子数据中很大一部分存在于暗网中。暗网数据不同于一般合法服务器的表层数据清晰可见，其取证需要通过专门工具或授权，甚至于专业的操作才能完成。然而此类数据又是跨境犯罪的重要源头之一。由于暗网具有空间边界模糊、动态性大、服务器地址和数据传输匿名等特点，对其数据追溯源头难度较大。2017年，世界各地的执法机构共同摧毁了当时最大的暗网市场——AlphaBay和Hansa。[28]其以区块链(blockchain)[29]为代表的去中心化特征与暗网的隐蔽性加大了执法机关的取证难度。关于暗网取证，笔者在裁判文书网上以“暗网”为关键词，查找到2020年我国法院判决的20份刑事判决书，其中有6份采用了远程勘验或在线提取的方式。[30]因此，对于一部分来源不明的电子数据，大多数国家都是根据其本国法律取证，一些国家也允许其他国家通过远程勘验的方式来共同侦查。[31]暗网数据来源不明导致其缺乏国家主权管辖归属，为各国执法和司法机构单方利用自身的先进网络技术手段远程收集创造了机会，加之这些数据难以收集和确定，一般都是由一国发现收集，通过传统刑事管辖权进行确定。有些国家执法或者司法机构对暗网采取网络攻击性技术手段收集证据，这种做法存在很大风险，易引起与暗网实际所在地国家的主权纷争。因为各国普遍将境外对其主权范围内的网络攻击行为定性为犯罪行为，使用这种技术手段取得的电子数据证据，在寻求国际司法协助过程中容易导致受攻击的国家司法机关的否定，所以对于暗网数据，可设立更为明晰的管辖方式与取证方式，先行适用发现国法律，待确定和了解后再通过其他途径进行管辖权的转移或共同侦办。

(二)跨境电子数据取证运行机制的完善

1.完善他方请求我方取证的运行机制。此种运行机制重点在于保护我国数据，构建完善的跨

境数据流动管辖与信任体系。对于存储在我国境内的数据，我国主张拥有刑事管辖权。在数据存储地模式下反对他国的“长臂管辖”。本着主权尊重的原则，结合我国倡导的网络主权，在他方请求我方取证的情况下应坚持对等原则。有学者认为这种管辖权是“域内管辖权”而不是“域外管辖权”，[32]即应当遵循我方的取证规则，保护我国电子数据的取证安全。他方请求我方取证时，我国执法机关应关注所要调取的数据类型，具体做好以下三个方面的工作：首先，对个人数据进行风险评估。对于个人存储于网络公共空间内的电子数据，在境外机构取证时，我国云服务提供者应有相应的风险评估机制，设立安全等级，数据服务应具有针对性，如评估电子数据的类型及可能境外流动的对象或范围等。由于这种数据由个人发布，通过普通网络搜索方式可以直观了解，经过风险评估机制评估后属于安全的信息就可以在两国刑事管辖框架内进行调取，无需经外交途径，这也符合我国倡导的互惠原则。其次，设立云服务提供者的先行审查义务，在个人涉及的关键信息可能流出时，云服务提供者应当进行审查，审查传输信息的取证相关性或取证目的或取证的使用频率等。如果存在危害国家安全或者数据主权的风险，应及时向国家网络数据安全监管机关报告。这种审查机制属于事前的民间自我审查机制，可将国家数据主权意识直接内化于云服务提供者的运行机制中，对互联网服务提供者起到一个普遍预防的作用，防止其存储的相关数据信息不当流出。由于我国《国际刑事司法协助法》第4条的限制，云服务提供者在一般情况下禁止提供数据，上述情况只能依赖“国际礼让原则”发挥作用。笔者建议规定除了涉及多数人等可能影响国家安全的数据，云服务提供者可以在其与信息使用者的协议框架内对数据进行审查后提供。为了保障云服务提供者在我国境内获取的公共数据或者个人数据、关键数据不被外国政府或者境外机构或个人恶意利用，我国可以按照数据存储地模式，立法明确要求云服务提供者将云服务器建立在我国境内并建立本地数据库，以保护我国各类主体的数据安全。在境外机构或人员申请调取云服务者收集的我国公共数据或者个人数据时，我方可通过行使数据主权管辖而加以有效管控。再次，立法加强对云服务提供者的监管。一是强化履行存储使用关键数据信息的报批义务。涉及到存储使用和流转关键信息，不论数据主体是谁，云服务提供者应严格坚持我国数据存储地的管辖模式，严格履行申请报批义务。二是加强对云服务提供者履行审查义务的监管，即检查云服务提供者对境内外第三方调取云空间的公共数据或个人数据是否做到了自我审查、是否向网络安全监管部门报批等情况。最后，完善境外机构调取我国政府数据的机制。政府数据是重要的关键信息，我国应当健全完善政府数据开放的程序机制，界定政府数据开放的标准，[33]以便在对等原则下依法向对方提供相应的政府开放数据，这有利于国际交流合作。

2. 主动确立我方请求他方取证的运行机制。我国坚持数据存储地模式，但也实行单边管辖模式，可能会侵犯到他国的数据主权安全。为尽量避免出现这一情况，我国司法机关请求他方国家提供电子数据时，不仅要判断数据类型，还要判断数据管辖类型。如果他方是数据控制者模式的国家，基于数据主权的原则，可在该国法律规定框架内进行取证活动。比如美国《加州法案》规定，企业从可验证的消费者处接收到访问个人信息的请求后，应立即采取措施向消费者免费披露和提供所要求的个人信息。我国执法者同样可以利用此渠道和方式获取相应的个人信息电子证据。对采用数据存储地模式的国家，则需要按照数据类型进行进一步判断。在两种数据模式存在冲突的情况下，我国应坚持数据存储地模式，但在具体措施

上可进行调整。

首先，建立数据“白名单”制度。对于境外主权国家法律不禁止提取和使用的境外网络上的各种电子数据，我们可根据国家总体安全的工作需要，依照国内法由执法机关直接在境外网络服务器上调取。建立提取电子数据证据“白名单”制度可以使我国在调取一些境外数据时不受繁琐程序的限制，更快更有效进行电子数据的取证活动。我们的“白名单”制度是以维护我国主权与国家总体安全利益为根本出发点而建立的，不以境外国家法律的限制而转移。对于不能单方解决的电子数据主权冲突，甚至是其他国家反向利用我国确定的“白名单”制度来对我国电子数据的提取加以限制的情况，可以用其他程序方式予以调取或采取相对应的反制措施。具体而言，“白名单”信息及取证规范可涵盖以下内容：第一，我方通过对方网络公开信息查询到的数据，包括境外网站、境外服务器可直接在线提取的电子数据如境外裁判文书、照片，通过犯罪嫌疑人提供的账号密码查阅收集到的银行流水信息、其他犯罪嫌疑人团伙成员的个人信息和授权其使用的信息，境外服务器虽已删除但我国执法机关通过科学技术手段使该文件得以恢复而提取的电子数据等；若是已经有国家间对应的司法协助协议，则可以直接调取对方电子数据。第二，需要输入账户密码等储存在公共范围但对于案件进程有重大影响的电子数据，应列入“白名单”中，同时简化提取程序。我国对于这类电子数据以远程勘验方式取证，也采取了司法协助方式进行。在单边取证环节中，明确“白名单”中的数据提取范围及目的，将进一步提高取证效率。第三，采用司法协助方式获取的对于案件有直接影响且符合双方安全利益的、无需通过技术侦查方式获得的境外数据，可列入“白名单”中直接作为证据使用。在未来的“白名单”制度规定中可以列明以哪些方式和途径获取的数据可以直接作为电子证据使用，笔者在此列举也仅起抛砖引玉作用。

其次，加强与主权国家的协作机制。数据存储地模式虽然保护了数据安全，但由于其防御性的本质，在电子证据的取证上效果并不令人满意。有学者就认为“传统电子取证因数据本地化存储和‘倒U型’取证结构而效率不高。”[39]尽管我国属于数据大国，但是我国执法机构向境外网络数据服务者或者网络数据主权行使机关申请调取证据却常常碰壁。在现有西方国家掌握网络服务器主权的国际体系下，其制定的互联网规则成为世界电子数据流动的主要制度依据。无论美国“云法案”还是欧盟GDPR确立的规则，中国数据主权均不在受益范围之内，例如，远程勘验需要与境外的数据服务机构进行合作，但在国际上我国并未享有数据主动权。因此，我国在坚持数据存储地模式的前提下，应当积极寻求电子数据取证的便利性，在制定国内有关网络数据电子取证的规则时，除了制定适应国内执法需要的一般性规则外，还要对一些影响国家安全和主权形象的政治性、敏感性、战略性数据进行有差别的规范，从而提升和强化我国对网络数据的管辖力度，传递出我国在数据主权领域制定规则的声音。以此为基础，我国要主动倡导多边合作协议，以具有针对性的网络数据管理规范和技术标准，尽可能与多数国家达成跨境电子数据取证的双边或多边协议，提高我国办理跨境电子数据取证的效率。

最后，严格限制技术侦查措施的范围。对于只有采用跨境技术侦查的方式才能进行的取证，由于涉及到对方数据主权与国家安全，我们应当谨慎。在提取电子数据时除了需考虑对方管辖模式问题，还应考虑此种方式的提取是否会造成外交风险。提取对案件有重大意义且只能通过技术侦查方式获取的电子数据，应当符合我国诉讼程序规则要求。

3.扩充来源不明晰的数据取证的运行机制。尽管公众无法访问暗网数据，但这不意味着暗网数据来源无法查明。首先，可以从技术手段上提升取证方式。比特币的适用与区块链技术联系密切，我们可以充分利用区块链技术积极寻找暗网数据来源，进行大数据分析，寻找侦查线索，提高对主权国不清的暗网存储数据的破解能力。其次，加强国际合作。暗网数据往往分处各个国家，同时蕴含着暴力杀戮等内容，无形中加大了跨国犯罪的可能性，因此各国应通力合作，共同参与打击暗网犯罪的行动。2014年欧盟成立的网络犯罪中心就旨在联合打击网络犯罪，维护欧盟的数据网络安全。最后，对于我国执法机关首先发现的暗网数据，可以在体现国家主权和维护国家总体安全观的理念下，优先适用我国取证规则。我国一方面应对暗网数据中可能涉及的犯罪进行侦查，在不引起跨境国家数据主权争议的情况下，运用先进的科学技术手段多渠道获取有利于认定犯罪嫌疑人的优势证据；另一方面要“更加善于在网络空间国际博弈中灵活运用和有效引导一些国际互联网行为规范的制定，使之最大限度地服务于我国的利益和诉求”，[55]尽力使我国的有关政策主张在国际刑事法律合作中得到充分体现，积极寻求更多的国家达成合作协议，加强与国际刑警组织的合作，通过国际刑警组织将中国制订的电子数据取证规则在世界各国加以传播并推广。通过国际司法协助及其他形式的合作，推动形成电子数据取证管辖共识，共同打击跨国犯罪。

五、结论

在目前全球不同国家的数据主权管辖模式下，任何国家都不可能独立完成对电子数据的取证。我国应以维护电子数据主权利益为出发点，完善跨境电子取证的法治架构，从立法、执法、司法等层面严格规范电子数据取证，通过多种途径获取境外数据来源。随着我国坚定不移地走对外开放和多边主义道路，我国在全球互联网数据领域也必将发挥越来越重要的作用。通过积极推动国际合作实现共同打击跨境犯罪，我国与他国在维护数据主权和打击犯罪的合作中将求同存异，实现双赢格局；通过立法完善电子数据取证制度，我们将中国声音和中国网络治理与网络数据电子证据运用方案介绍到世界，并在世界各国电子数据主权确立与管辖博弈中获得应有的地位和尊重。在实践中，就数据主权的确立与保护问题，我国立法者还需要结合我国境内外网络数据平台经营者的实际运行情况、我国网络数字经济的对外开放发展情况以及电子数据对国家安全、公民个人信息权利的影响，制定既符合网络数字经济市场发展规律，又能维护国家利益、保护公民个人信息的法律规范，构建在权利保障、责任追究、管辖程序等方面符合国际法基本原则的数据主权司法管辖制度体系。

注释：

①参见[俄]罗加乔夫·伊利亚·伊戈列维奇：《网络犯罪国际立法需与时俱进》，载《人民日报》2018年1月12日第23版。

②参见肖冬梅、文禹衡：《数据权谱系论纲》，载《湘潭大学学报(哲学社会科学版)》2015年第6期，第70页。

③国家金融IC卡安全检测中心信息安全实验室、北京交通大学金融信息安全研究所、上海交通大学网络安全学院：《一般数据保护法(General Data Protection Regulation)全文译文》，高志民、张大伟等译，2018年3月30日。

④付熙雯、郑磊：《政府数据开放国内研究综述》，载《电子政务》2013年第6期，第11页。

⑤个人匿名化的数据是指个人在公共空间发表的没有身份特色的电子数据，由于其经过拆分处理，原个人主体与数据本身没有指向性，这里将其认定为公共数据。参见王融：《关于大数据交易核心法律问题——数据所有权的探讨》，载《大数据》2015年第2期，第53页。

⑥Irion, Kristina, Government Cloud Computing and National Data Sovereignty, Policy & Internet, 2015, pp. 40-71.

⑦[美]理查德·N.哈斯：《新干涉主义》，殷雄、徐静译，新华

出版社2000年版，第88页。

⑧吴沈括：《数据跨境流动与数据主权研究》，载《新疆师范大学学报(哲学社会科学版)》2016年第5期，第115页。

⑨裴炜：《向网络信息业者取证：跨境数据侦查新模式的源起、障碍与建构》，载《河北法学》2021年第4期，第65页。

⑩参见国务院新闻办公室：《中国互联网状况白皮书(2010年版)》，http://www.scio.gov.cn/tt/Document/1011194/1011194.htm，访问日期：2021年3月22日。

⑪参见《全球数据安全倡议(全文)》，http://www.gov.cn/xinwen/2020-09/08/content_5541579.htm，访问日期：2021年4月11日。

⑫“个人信息”受法律保护并不等于“个人信息权”，至于“个人信息”上究竟体现了哪些具体民事权利，有待于今后进一步作出立法解释。

⑬See Callaway D, Determann L. The New US Cloud Act-History, Rules, and Effects, Computer & Internet Lawyer, 2018, p. 3.

⑭《网络犯罪公约》第1、2章主要内容包括网络犯罪基本术语的介绍，对于非法进入、非法截取、资料干扰、系统干扰、设备滥用、伪造电脑资料、电脑诈骗、儿童色情的犯罪、儿童色情的犯罪行为的解释及处罚措施。

⑮夏燕、沈天月：《美国CLOUD法案的实践及其启示》，载《中国社会科学院研究生院学报》2019年第5期，第110页。

⑯Federal Law of the Russian Federation: On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Processing of Personal Data in Information and Telecommunication Networks, ROSSIISKAIA GAZETA, 2014, p. 242.

⑰《就“进一步明确互联网个人数据处理规范”对俄罗斯联邦系列法律的修正案》第1条、第2条。中央网络安全和信息化领导小组办公室、国家互联网信息办公室政策法规局：《外国网络法选编(第一辑)》，中国法制出版社2015年版，第418页。

⑱胡文华、孔华锋：《印度数据本地化与跨境流动立法实践研究》，载《计算机应用与软件》2019年第8期，第307页。

⑲United Nations: General Assembly Resolution on A Model Treaty on the Transfer of Proceedings in Criminal Matters, International Legal Materials, 1991.

⑳肖永平：《“长臂管辖权”的法理分析与对策研究》，载《中国法学》2019年第6期，第51页。

㉑该法第2条、第3条强调其活动单位在中华人民共和国境内且数据为任何电子或者其他方式对信息的记录；第36条强调对数据进行出口管制，取消了个人和组织向境外提供数据的权限，但实际还是《国际刑事司法协助法》第4条要求的体现，要求有主管机关的同意，并未对此有明确的出口管制措施要求。

㉒See Gucci Am., Inc. v. Weixing Li, 135 F. Supp. 3d 87(S. D. N. Y. 2015).

㉓具体如《商业银行法》第29条，《涉及恐怖活动资产冻结管理办法》第15条。

㉔对境外公开发布的电子数据，可以通过网络在线提取。

㉕根据案情需要，在必要的时候对远程计算机信息系统进行网络远程勘验。境外数据的网络远程勘验，是指使用电子数据持有人、网络服务提供者提供的用户名、密码等进行远程计算机信息系统访问。

㉖办理批准手续后，可以对境外电子数据采取技术侦查措施进行远程勘验。

㉗黄伟：《跨境资金犯罪的域外取证》，载《检察风云》2018年第10期，第18-19页。

㉘AlphaBay被称为暗网Amazon，此前允许用户以匿名的方式用比特币交易毒品、武器、黑客工具和其他非法商品。Hansa黑市则是全球第三非法商品的网上集市，主要以违禁药品为主。

㉙中国电子技术标准化研究院联合数十家单位于2017年5月16日发布的《中国区块链技术和产业发展论坛标准CBD-Forum-001-2017》，将区块链(blockchain)定义为“一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式(注：事务处理包括但不限于可信数据的产生、存取和使用等)”。

㉚参见《中国裁判文书网》，文书截止查询日为2020年10月7日。6份判决书分别为(2020)苏01刑初25号、(2019)浙0703刑初407号、(2020)浙0213刑初430号、(2020)苏0206刑初427号、(2019)沪0151刑初399号、(2019)浙0303刑初1217号。

㉛如美国2016年修订《联邦刑事程序规则》第41条b款第6项，授权执法部门可以在“因技术原因导致媒介或信息的储存地点被隐藏的情况下”，对管辖区外(含境外)的数据进行远程侦查。

㉜参见梁坤：《基于数据主权的国家刑事取证管辖模式》，载《法学研究》2019年第2期，第204页。

㉝宋华琳：《中国政府数据开放法制的发展与建构》，载《行政法学研究》2018年第2期，第39页。

㉞王立梅：《论跨境电子证据司法协助简易程序的构建》，载《法学杂志》2020年第3期，第86页。

㉟黄志雄：《网络空间负责任国家行为规范“起源、影响和对策”》，载《当代法学》2019年第1期，第69页。