跨境远程电子取证制度之重塑

梁　坤

内容提要:在网络时代,电子数据越来越多地存储于境外,从技术和法律层面均给侦查取证带来了巨大的挑战。在过去的一些年间,中国采取了赋予侦查机关以远程勘验、技术侦查等权力的单边路线来收集境外电子数据,然而这种程序法制度不仅与《网络犯罪公约》及一些国家的国内立法形成了明显的差异,而且也与我国外交部门的立场及既有的刑事司法协助机制不符。根据国家主权原则及网络环境下的权利保护和侦查权控制理念,有必要严格限制我国侦查机关采取单边路径跨境远程电子取证的权力。具体而言,可以在跨境远程电子取证的侦查程序规范中继续授权网络在线提取措施,专门设计经同意的远程勘验和搜查制度,并将采用技术手段非经同意的搜查纳入技术侦查措施并严格限制运用。在此基础上,有必要简化刑事司法协助机制抑或通过跨境数据披露的方式来回应实践取证需求,以此作为限制跨境远程电子取证的替代方案。

关键词:跨境　远程取证　电子数据　国家主权　网络犯罪公约

梁坤,西南政法大学刑事侦查学院副教授。

一　问题的提出

目前,各国侦查机关在电子数据的收集过程中面临一个同样的难题,即这类证据实际存储于境外。由于侦查权长久以来被定性为国家权力的重要组成部分,因此原则上只限于在一国境内开展活动。如果需要收集存储于境外的刑事证据,一般只能通过司法协助在双边或多边框架下开展。但是,在网络时代,这显然不是最佳的方案。司法协助请求要么得不到及时回应,要么程序复杂且耗时过长,与追求快捷、高效的电子取证理念格格不入。在此背景下,脱离司法协助框架而以跨境远程方式收集电子数据的需求越发强烈。

那么,如何从侦查程序规范甚至国际法层面看待这种取证活动?2001 年,欧洲理事会制定的《网络犯罪公约》(以下简称《公约》)对此已有规范,虽然至今仍是这一领域最主要的区域性国际规则,但条文的模糊性及对跨境远程搜查等措施的忽略导致其早已不

适应时代发展的需求。而从中国的规范层面来看,虽然相关文件对诸如跨境远程勘验这样的措施进行了规定,但是规则建构的理念不清和对侦查措施的选择性规范导致实务中采取的措施表现出多方面的乱象。此外,由于现行国内法规则与国际法原则脱节,不仅导致中国在这一领域的大量侦查实务忽略了应有的程序保障和权力控制,而且存在着潜在的国际法风险。

与跨境远程电子取证在实践中的广泛运用相比,我国学界对这一领域的关注明显不足。例如,有学者侧重从司法协助的角度对域外取得的刑事证据的可采性展开了深度分析,〔1〕但是却没有注意到大量的跨境电子取证其实已经绕开了司法协助程序;一些文献对规范和实践层面的诸多远程电子取证措施进行了研究,要么只关注到国内相关制度而缺乏跨境层面的比较分析,〔2〕要么则是在进行比较分析的时候又忽视了跨境远程取证的相应措施;〔3〕一些研究从技术层面注意到了电子取证所具有的跨区域特征,〔4〕但在法理方面进行的深刻提炼又十分欠缺。与此相对的是,跨境远程电子取证的议题从 20 世纪 90 年代中期开始便在国外受到关注,近期随着这一领域取证需求的兴盛而成为了理论研究的热点。本文首先对域外规则和中国现有规范从历史发展、主要内容及内在法理等多个角度进行综合比较,在此基础上对中国跨境远程电子取证制度的重塑提出具体建议。

二　历史维度下的域外规则及法理解析

(一)域外规则的历史发展与内容缺陷

1.《莫斯科公报》的铺垫

电子数据能够以跨越国境的方式存储,这几乎是互联网于 20 世纪 90 年代初期连通全球时同步产生的现象。正是这一时期,在意识到传统的刑事司法协助机制难以适应网络时代跨境电子取证需求的背景之下,西方多国开始关注以最快捷的方式也即通过实时远程方式收集境外电子数据的议题。在此过程中,八大工业国家高峰会(简称 G8 峰会)对这一领域达成阶段性共识起到了重要的推动作用。1999 年 10 月,莫斯科峰会发布《八国集团打击跨国有组织犯罪部长会议公报》(以下简称《莫斯科公报》),其中“附件 1”提出,成员国在符合其国内法的情况下基于以下目的开展的活动无需另一国授权:“①收集公众可以获得的数据(公开资料),而不论相应的数据位于何处;②提取、搜查、复制、扣押存储在另一方境内的计算机系统中的数据,前提是相应的行为获得了拥有法定权限而向取证方披露数据的主体的合法且自愿的同意。”

《莫斯科公报》提出的方案为后续区域性国际法框架的形成奠定了基础,具有重要的

〔1〕 参见冯俊伟:《域外取得的刑事证据之可采性》,《中国法学》2015 年第 4 期,第 247 页以下;王青、李建明:《国际侦查合作背景下的境外取证与证据的可采性》,《江苏社会科学》2017 年第 4 期,第 161 页以下。

〔2〕 参见刘品新主编:《电子取证的法律规制》,北京:中国法制出版社 2010 年版,第二、三、五、六章。

〔3〕 参见皮勇:《〈网络犯罪公约〉中的证据调查制度与中国相关刑事程序法比较》,《中国法学》2003 年第 4 期,第 148 页以下。

〔4〕 参见许兰川等:《云计算环境下的电子取证:挑战及对策》,《刑事技术》2017 年第 2 期,第 151 页以下。

历史意义。但是,由于其本身并无约束力,因此该领域真正意义上的国际法规范仍处于空白状态。在此背景下,美国联邦调查局于 2000 年在个案中以远程方式搜查位于俄罗斯境内的计算机系统,引发俄罗斯方面强烈的外交抗议。[5] 刑事诉讼中跨境远程电子取证在规则层面的缺失随着此案的助推一度引起热烈讨论,对这类取证活动进行法律规制的呼声也愈发强烈。

2. 比利时修法及《公约》的规则创制

在国际规范缺失的背景之下,比利时于 2000 年颁布《计算机犯罪法》,在《刑事诉讼法》中增加了 88*ter* 条(第 88 条之三),在全球范围内率先对跨境"计算机和网络搜查"进行了规定。具体而言,侦查法官可以在特定情形下授权搜查计算机系统,而且该搜查行为在符合法定情形时还可以延伸到与令状所注明的系统相连接的其他系统。如果搜查中发现相应的数据并不位于境内,那么只能进行"复制"。同时,侦查法官应当立即通知司法部长,并由后者及时告知相关国家。然而,比利时的修法没有引发西方各国跟风效仿,围绕国家主权、隐私权的担忧促使各国采取谨慎观望的态度。

比利时修法没有引发其他国家跟进,还有一个重要的原因在于,欧洲理事会从 20 世纪 90 年代中期开始,已经在着手制定包括跨境远程电子取证在内的程序规则。2001 年 11 月 8 日,《网络犯罪公约》及具有解释性质的《网络犯罪公约解释报告》(以下简称《公约解释报告》)在经过各国多轮激烈争论之后获得通过。《公约》通过第 32 条 a、b 两款,对缔约国单边开展的跨境远程电子取证作出了与《莫斯科公报》"附件 1"中两种情形大同小异的规定:"缔约方可不经另一方的授权许可:a. 收集公众可以获得的存储于计算机中的数据(公开资料),而不论该数据位于何处;b. 通过其境内的计算机系统提取、接收存储在另一方境内的计算机系统中的数据,前提是相应的行为获得了拥有法定权限而通过计算机系统向取证方披露数据的主体的合法且自愿的同意。"据此,跨境远程电子取证的区域性国际规则首次形成。在此基础上,缔约国根据《公约》的规定,陆续将其转化为国内法加以遵循。

3. 域外现行规则内容存在的主要问题

一是《公约》第 32 条术语不清导致适用混乱。《公约》第 32 条存在的第一个问题便是具体适用时的解释问题。例如,条文中的"法定权限""合法且自愿的同意"容易引发理解上的不一致,一些缔约国倾向于按照自己认为合法的方式开展工作。在此背景之下,《网络犯罪公约委员会关于跨境收集数据的指引注释(第 32 条)》(以下简称《公约第 32 条指引注释》)于 2014 年发布,对长久以来认识不清的许多问题进行了阐释。例如,32 条 a 款中所谓的"公众可以获得的(公开资料)"包括公众通过订阅或注册而可以获得的资料;如果相应的网络内容或服务并未向公众开放,则便不属于该条款授权的范围。此外,这份文件还对"跨境""同意"等重要术语的含义进行了说明。[6] 尽管如此,相关措词仍

〔5〕 See Russell G. Smith, Peter Grabosky, Gregor Urbas, *Cyber Criminals on Trial* (Cambridge: Cambridge University Press, 2004), p. 58.

〔6〕 See Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3 Transborder access to data (Article 32),资料来源:https://rm. coe. int/16802e726a,最近访问时间[2018 - 11 - 03]。

然存在一定的分歧。例如,《公约》并未定义“计算机数据”的范围,故涉及一国国家安全、军事利益的数据也包含在内,无形中对网络间谍行为大开绿灯。又如,为表面上满足公约所规定的“合法而自愿的同意”的条件,不能排除一些缔约国会对数据权利人采取贿赂、威胁、欺骗等非法手段。〔7〕 总之,虽然经过上述注释,但是对相关术语的理解仍然存在的不同认识导致规则条款的适用效果大打折扣。

二是现有规则体系存在法律空白。除了《公约》第 32 条规定的上述两种情形而外,缔约国是否还能通过其他方式开展跨境远程电子取证,至今没有明确答案。实际上,对于其他类型的跨境远程电子取证,《公约》既未作出合法性授权,也未明确排斥。〔8〕 这样一来,包括“远程搜查”在内的措施就处于法律的真空地带。根据法理,在没有规则的情况下只能依惯例或原则。具体而言,一国侦查机关在未经他国许可的情况下,通常不能“进入”他国领土开展侦查。据此,跨境远程搜查实际上也并不被容许。而对于数据存储地不明确的远程搜查,目前同样面临这个问题。例如,由于“暗网”多重加密等技术手段的限制,服务器所在地通常并不明确,因此以美国联邦调查局为代表的侦查机关近年来对“暗网”进行的远程搜查便很可能越境开展,这种特殊搜查行为的合法性也引发了激烈的争议。

在此背景下,《公约》已经遭遇严重的发展瓶颈。网络犯罪公约委员会在 2014 年发布的报告中承认,规范跨境电子取证的工作已经很难继续推进。〔9〕 该委员会在《公约第 32 条指引注释》的讨论稿中也无奈地认为,缔约国“可能有必要根据其国内法、相关的国际法原则或基于国际关系的考虑而评估跨境搜查或其他取证措施的合法性。”〔10〕

(二)域外规则建构的法理解析

1. 基于地缘管辖的国家主权原则设计相应程序制度

受国际法原则及国家主权的限定,侦查中远程收集存储于他国境内的电子数据,没有理由绕开司法协助机制而由一国单方开展。但是,由于这种取证发生在虚拟空间而非实体空间,侦查人员毕竟并不存在物理跨境行为。为此,哈佛大学网络法专家杰克·戈德史密斯(Jack Goldsmith)就曾提出,侦查人员开展远程搜查犹如通过卫星窥探他国领土内的活动,并不为国际法规则所禁止。〔11〕 然而,更多学者尽管也承认这类侦查活动,以领土为界限的刑事管辖权逐渐模糊起来,〔12〕但是仍然倾向于认为,如果一国执法人员未

〔7〕 参见胡生健、黄志雄:《打击网络犯罪国际法机制的困境与前景——以欧洲委员会〈网络犯罪公约〉为视角》,《国际法研究》2016 年第 6 期,第 27 页。

〔8〕 See Explanatory Report of Convention on Cybercrime, Paragraph 293, 资料来源:https://rm. coe. int/16800cce5b,最近访问时间[2018 - 11 - 13]。

〔9〕 Cybercrime Convention Committee (T-CY), Transborder access to data and jurisdiction: Options for further action by the T-CY (December 2014),资料来源:https://rm. coe. int/16802e726e,最近访问时间[2018 - 11 - 13]。

〔10〕 Cybercrime Convention Committee (T - CY), T-CY Guidance Note # 3 Transborder access to data (Article 32), Proposal prepared by the Bureau for comments by T-CY members and observers and for consideration by the 9th Plenary of the T-CY (June 2013),资料来源:https://rm. coe. int/16802e70bc,最近访问时间[2018 - 11 - 13]。

〔11〕 Jack Goldsmith, The Internet and the Legitimacy of Remote Cross-Border Searches, 2001 *University of Chicago Legal Forum* 103, 2001.

〔12〕 Mireille Hildebrandt, Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace, 63 *University of Toronto Law Journal* 196, 2013.

经许可“到位于另一国的数据库搜查计算机系统,缺乏协调和合作会引起程序法和主权问题”。[13]

在国内法层面,西方许多国家便是根据这种传统的地缘管辖而尽力避免将远程取证行为延伸到境外。例如,英国法院在签发远程搜查令状的时候,就需要判断警察的行动是否系跨境开展。如果违法从境外收集数据,则法院可能会将相应的证据予以排除。而在德国,尽管此类问题还没有得到充分的讨论,但是一旦跨境远程收集存储于境外设备中的数据,就需要考虑相应国家的主权是在什么情况下出现了妥协或让步。[14] 而从《公约》来看,相关规则也是建立在地缘管辖基础之上的。根据《公约第 32 条解释报告》的说明,《公约》第 32 条 b 款在性质上就属于国家主权原则的例外。换言之,《公约》所容许的单方开展的跨境远程取证,并不是不尊重国家主权,而是在缔约国协商一致的情况下共同商定的制度,而这恰恰是尊重国家主权的表现。

然而,《公约》的规则创制遵循的这种理念尽管为缔约国所信奉,但是具体的内容却并没有得到普遍认可。实际上,《莫斯科公报》作为《公约》的前奏,曾宣示性地提出,“如果对数据所在国进行告知为目标国国内法所许可,而且数据内容反映出对目标国刑法的违反抑或看上去系目标国利益所在,那么开展数据搜查的国家就应当考虑对目标国进行相应的告知。”不过,《公约》第 32 条明显忽略了“告知义务”。《公约第 32 条指引注释》第 3.1 部分也只是提示,基于权利保障的考虑,执行远程取证的国家“可以考虑”对电子数据存储地的相关职权部门告知。为此有人质疑,根据国家主权原则应当由数据所在国政府同意,而不应当由所谓的主体甚至是个人同意。[15] 中国也有学者认为,第 32 条 b 款很可能会对缔约国的国家主权造成冲击。[16] 一旦接受这一条款,一国就将面临他国政府部门以刑事侦查为名而收集其他情报的风险,这显然也是对国家主权的一种潜在的侵犯。[17]

这种思路成为了以中、俄为代表的国家拒绝加入《公约》的重要理由。例如在 2011 年的联合国预防犯罪和刑事司法委员会“打击网络犯罪问题政府间专家组首次会议”、2013 年的“联合国网络犯罪问题政府间专家组第二次会议”、2018 年的“联合国网络犯罪政府间专家组第四次会议”上,中国代表团均对第 32 条 b 款表达了反对意见,理由在于其实质是域外取证,因涉及到主权和管辖权,极易引起争议;[18] 研究报告草案已指出,目前大多数国家尚无此实践;[19] 应在联合国框架下通过多边协商达成共同接受的规则,避免

〔13〕 [加]唐纳德·K. 皮雷格夫:《打击网络犯罪和网络恐怖主义中的国际合作》,卢建平等译,《法学家》2003 年第 4 期,第 62 页。

〔14〕 Ulrich Sieber, Nicolas von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice*, (Berlin: Duncker & Humblot, 2016), pp. 554, 730.

〔15〕 See Nicolai Seitz, “Transborder Search: A New Perspective in Law Enforcement”, 7 *Yale Journal of Law and Technology* 23, 2004.

〔16〕 参见徐峰:《网络空间国际法体系的新发展》,《网络安全与通信保密》2017 年第 1 期,第 77 页。

〔17〕 参见胡生健、黄志雄:《打击网络犯罪国际法机制的困境与前景——以欧洲委员会〈网络犯罪公约〉为视角》,《国际法研究》2016 年第 6 期,第 28 页。

〔18〕 参见《中国代表团出席联合国网络犯罪问题专家组首次会议并做发言》,资料来源:http://www.fmprc.gov.cn/web/wjbxw_673019/t812063.shtml,最近访问时间[2018-11-13]。

〔19〕 参见《中国代表团出席“联合国网络犯罪问题政府间专家组”》,资料来源:http://www.fmprc.gov.cn/ce/cgvienna/chn/drugandcrime/crime/t1018227.htm,最近访问时间[2018-11-13]。

由单个国家或有限成员的地区采取单边立法而造成“碎片化”。[20] 俄罗斯对这一条款的态度与中国完全一致。例如,该国外交部新威胁和挑战司司长伊戈列维奇于2017年表示,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。[21]

2. 基于网络环境的特性保障权利并控制侦查权

由于跨境远程电子取证极易导致对特定权益的侵犯,于是强调对这类取证活动进行超常规的侦查权控制,成为了域外规则形成过程中重点关注的议题。例如,《莫斯科公报》第17条专门指出,“在设计跨境电子取证制度时,除了考虑国家主权,就是要关注人权保障、人民的自由和隐私”。《公约》第15条规定,权力的行使和程序的确立、实施和适用都需要遵循多份国际公约所确立的人权保障内容。《公约第32条指引注释》第3.1部分也指出,在适用这一条文的时候应当考虑个人和第三方的权利。从具体的程序设计来看,上述域外规则从两个方面体现出对权利保障的关照以及对侦查权制约的重视。

一方面,具体措施的设计反映出对强制性措施的抑制。根据《公约》32条a款,可以收集的只能是公开资料,而且必须是“存储”状态的,这实际上就否定了实时监控取证措施的运用。而从b款来看,《莫斯科公报》中列举的“提取、搜查、复制、扣押”措施在《公约》中变成了“提取、接收”,而未保留“搜查、扣押”这两种典型的强制性措施。虽然荷兰于2019年1月1日施行的《计算机犯罪法(三)》授权对可能跨境“侵入”计算机系统并进行在线监控作出强制性措施,但是立法将其限制在了贩毒、走私、恋童癖及攻击银行等起刑点4年以上的重罪。[22]

另一方面,争议较大的强制搜查以司法令状的特别程序设计为前提。根据令状原则,侦查机关在采取可能会侵犯公民基本权利的强制性措施之前,原则上需要取得司法授权。例如,美国联邦调查局对境外“暗网”的搜查,虽然很可能并不清楚数据存储介质的实际物理位置,但是基于搜查的措施属性,来自于法官的授权必不可少。而在法律允许跨境远程搜查的一些国家,法律还设置了特殊的程序机制来强化对侦查权的控制。例如,比利时刑事诉讼法中尽管允许有条件的跨境远程搜查,但除了强调只能采用“复制”措施,还特别要求侦查法官发现侦查行为跨越国境后应当立即通知司法部长,并由后者及时告知相关国家。

总之,就跨境电子取证的域外规则而言,无论是区域性国际法规则还是一些国家的国内法规则,并非尽善尽美,而且至今不乏争议。但不可忽视的是,基于对国家主权原则的尊重、对网络环境下的个人权利保障及对侦查权制约的重视是规则背后的精髓所在,这应当成为分析、检讨中国当前相应制度的重要参考。

---

〔20〕 参见《中国代表团在联合国网络犯罪政府专家组第四次会议各项议题下的发言以及提交的书面建议》,资料来源:外交部条约法律司微信公众号“中国国际法前沿”(2018年4月10日刊发),最近访问时间[2018-04-11]。

〔21〕 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》,《人民日报》2018年1月12日第23版。

〔22〕 See Janene Pieters, New Law Allows Dutch Police To Hack Suspects, 资料来源:https://nltimes.nl/2018/06/27/new-law-allows-dutch-police-hack-suspects,最近访问时间[2018-11-04]。

三 中国现行制度检视及理论反思

(一)程序法依据与实务类型

中国对跨境远程电子取证的程序规定,与域外以《公约》为主线的规范状况并无关联。在《刑事诉讼法》没有对相应措施进行规范的情况下,公安部为了回应实践需求,在 2005 年发布的《计算机犯罪现场勘验与电子证据检查规则》第 3 条中对“远程勘验”进行了规定。虽然规则并未指明这一条款是否适用于跨境形态下对电子数据的勘验,但无疑为此后相关规则的形成奠定了基础。2014 年,最高人民法院、最高人民检察院、公安部在其发布的《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》(以下简称《网络犯罪意见》)第 15 条中首次规定,对于“原始存储介质位于境外”而无法获取的,可以提取电子数据。但是对于到底该如何跨境提取这类电子数据,具体措施有哪些类型,该意见并未明确。2016 年,最高人民法院、最高人民检察院、公安部联合发布的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》(以下简称《电子数据规定》)第 9 条在承继《网络犯罪意见》第 15 条规定的基础上进一步明确,“对于原始存储介质位于境外或者远程计算机信息系统上的电子数据,可以通过网络在线提取。为进一步查明有关情况,必要时,可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验,需要采取技术侦查措施的,应当依法经过严格的批准手续”。

据此,在《电子数据规定》出台之后,中国侦查机关跨境远程电子取证的制度体系已经成型。当出现原始存储介质位于境外的情况时,虽然无法像常规的电子取证那样扣押原始存储介质,但是也可以采用“网络在线提取”措施加以收集。这里需要注意的是,2019 年 2 月 1 日施行的《公安机关办理刑事案件电子数据取证规则》(以下简称《公安机关规则》)第 23 条将“网络在线提取”的数据限定为“公开发布的电子数据、境内远程计算机信息系统上的电子数据”。在此基础上为了进一步查明有关情况且在必要时,侦查机关可以采用“网络远程勘验”措施。在进行网络远程勘验而需要采取“技术侦查”措施的,再按相应程序执行。除此之外,虽然侦查机关远程开展的鉴定、检查、搜查、辨认等方式[23]实际上都可以轻易地跨越国境,而且实践中甚至还出现了“冻结”境外电子数据的案例,[24]但是由于这些措施并未在规范层面得到明确,因此本文的规范分析将主要以《电子数据规定》为依据。

(二)规范与实务的理论反思

1. 中外侦查措施的横向比较

从上述域外规则及以《电子数据规定》为主的中国程序规则的比较来看,尽管所采取措施的称谓存在差异,但也存在交集。具体情况见表 1。

〔23〕 参见高峰、田学群:《五方面细化规范“远程取证”工作》,《检察日报》2013 年 12 月 15 日第 3 版。

〔24〕 例如在一起开设网上赌场案件的侦查过程中,公安机关冻结涉嫌赌博的境外网站账户达 487 个。参见雷强、张发平:《境外注册境内狂拉下线,在线赌博网站涉赌 9.8 亿》,《市场星报》2015 年 10 月 9 日第 5 版。

表 1　跨境远程电子取证的侦查措施对比

	域外侦查措施	域外规则	中国侦查措施	中国规则
完全相同的措施	提取公开数据	《公约》第 32 条 a 款	网络在线提取	《电子数据规定》第 9 条第 2 款、《公安机关规则》第 23 条
	经同意的提取或接收	《公约》第 32 条 b 款	远程勘验（经同意的提取）	《电子数据规定》第 9 条第 3 款
部分相同的措施	远程搜查（复制数据）	比利时《刑事诉讼法》88*ter* 条（第 88 条之三）	远程勘验（非经同意的提取）	《电子数据规定》第 9 条第 3 款
形似而实异的措施	远程搜查（技术破解或侵入、实时监控）	美国《联邦刑事程序规则》第 41（b）（6）条；荷兰《计算机犯罪法（三）》第 IIG 条	技术侦查	《电子数据规定》第 9 条第 3 款

第一，部分措施完全相同。从中国侦查机关对境外电子数据进行的“网络在线提取”来看，尽管实务中经常将其与“远程勘验”混同，[25] 但这其实是一种单独的侦查措施。根据最高人民检察院的解读，这种措施一般就是通过网络公共空间对网页、网上视频、网盘文件上的电子数据进行提取，可以理解为从网上下载文件。[26] 实际上，这种情况下跨境对电子数据的远程提取，与普通网民浏览境外网站并下载图片、音视频并无区别。换言之，采用这些方法所提取的电子数据应当都是属于表面信息、公开信息、浅层信息，或者简单地说就是普通网民都可以接触、使用的信息，因此侦查机关在提取数据时无需采用特别的侦查措施。《公安机关规则》第 23 条所谓的“公开发布的电子数据”实际上就包括境外的公开数据。由此可见，“网络在线提取”应当等同于《公约》32 条 a 款中规定的“提取公开数据”。

而在合法取得嫌疑人自愿配合获取帐号密码并远程登陆境外邮箱系统或服务器取证的情况下，在中国被称为跨境远程勘验，[27] 实际上也就是《公约》第 32 条 b 款所规定的“经同意的提取或接收”的具体表现。这个观点可以从《公约解释报告》第 294 段落中找到根据：当某人的电子邮件的内容信息存储于境外邮件系统中的服务器时，便可以认为其拥有合法权限将该邮件信息披露；如果其同意向一国侦查机关披露，便属于“经同意的披露”的典型情况。此外，《公约第 32 条指引注释》第 3 部分关于条文解释的内容也对此进行了重申。

第二，有些措施部分相同。中国的远程勘验并非完全属于“经同意的提取或者接

〔25〕 例如在某寻衅滋事案中，侦查机关对境外网站登载的文章、照片进行“勘验”获得了相应电子数据。参见《云南省楚雄彝族自治州中级人民法院刑事判决书》（2016）云 23 刑终字第 82 号。

〔26〕 参见万春等：《〈关于办理刑事案件收集提取和审查判断电子数据若干问题的规定〉理解与适用》，《人民检察》2017 年第 1 期，第 53 页。

〔27〕 例如在某非法猎取、控制计算机信息系统数据案中，嫌疑人焦某归案后主动向公安机关提供了位于美国的另一台主控服务器的 IP 地址、用户名和密码。公安人员在经过“远程勘验”在该服务器上提取了相应的“主控程序”以及“登录日志”和“主控列表”等电子数据。参见《湖北省武汉市中级人民法院刑事判决书》（2016）鄂 01 刑终字第 176 号。

收”,除了使用勘验软件开展工作而外,实践中还存在通过“技术侦查”获取帐号密码后登陆取证的情况。[28] 下文还将论证,如果针对嫌疑人控制的计算机服务器进行取证,从措施的性质上讲并不属于勘验而是搜查,因此实际上属于比利时《刑事诉讼法》规定的远程搜查。但需要注意的是,尽管都属于搜查,取证的限度却存在差异。具体而言,比利时规定的跨境远程搜查只能对电子数据进行“复制”。而就中国实践中这类名为跨境远程勘验而实属远程搜查的措施而言,取证过程并不限于“复制”,甚至还包括后文所述的“冻结”。

第三,部分措施形似而实异。从中国目前规定的跨境技术侦查措施来看,实务中包括实时监控取证。然而从本文搜集到的资料来看,无论是国际法还是他国的国内法规则,笔者均未查阅到域外直接授权侦查机关对境外计算机系统进行实时监控取证的明确规定。当然这里需要指出的是,美国和荷兰的规定与中国虽有类似之处,但是实际上也存在着实质区别。

根据 2016 年修订的《联邦刑事程序规则》第 41(b)(6)条[29]的规定,美国执法部门可以对存储位置不确定的网络空间中的电子数据进行“远程搜查”。这种措施从实践来看往往就是通过植入技术软件进行在线搜查,尽管称谓不同,但是与中国的远程“技术侦查”的一些做法并无区别。不过,中美两国在运用这类措施的法律程序方面却存在显著差异。这是因为,《电子数据规定》第 9 条第 3 款可谓是明确授权侦查机关可以直接对境外目标进行“技术侦查”。与此不同的是,因技术原因的限制,美国执法部门在个案中对“暗网”进行的远程搜查,至少在申请法院令状的时候通常并不清楚数据的实际存储位置,因此法官签发的令状并不是直接授权侦查机关对境外目标进行远程搜查。[30] 与美国的情况类似的是,荷兰《计算机犯罪法(三)》赋予了侦查机关开展技术侵入并通过植入监控软件进行远程搜查的权力。[31] 虽然在数据存储位置不确定等情况下并不排斥跨境侦查活动的开展,但是官方的态度却是一旦确认远程搜查跨越了国境,原则上将停止这种侦查活动,并告知相关国家。[32] 换言之,荷兰的立法也不属于对侦查机关远程搜查境外目标的直接授权。

2. 中国相关侦查措施的再认识

在对中国和域外关于跨境远程电子取证的规范与实务进行了横向对比之后,结合中

〔28〕 例如在某开设赌场案中,公安机关通过技术侦查手段掌握余某提供的涉案网站的两个代理商账户 chh98、chj9 及密码,登陆后进行了远程勘验,并对取证过程及结果进行了鉴定。参见《湖南省郴州市中级人民法院刑事判决书》(2016)湘 10 刑终字第 69 号。

〔29〕 该条的内容是:“在因技术原因而导致媒介或信息的储存地点被隐藏的情况下,对可能已发生的犯罪存在关联的所有地方有管辖区的法官,均有权针对管辖区内或管辖区外签发令状以开展对电子储存媒介的远程搜查,并且授权扣押或复制电子存储信息。”

〔30〕 See Ahmed Ghappour, “Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web”, 69 *Stanford Law Review* 1075, 2016.

〔31〕 具体的监控方式将包括按键记录、自动截屏、秘密打开麦克风或摄像头及 GPS 定位等。See JJ. Oerlemans, “De Wet computercriminaliteit III meer handhaving op internet”, 15 *Strafblad* 356, 2017.

〔32〕 但是这种告知仅仅是基于国际礼仪,而非法律义务。See Anna-Maria Osula, Mark Zoetekouw, “The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives”, 11:1 *Masaryk University Journal of Law and Technology* 107, 2017.

国外交部门的立场以及中国相关侦查措施的实际运用，可以形成以下三个结论。

第一，相关规范及实务与外交部门的立场存在冲突。如上文所述，外交部门近年来在多个多边场合提出了对《公约》第 32 条 b 款的反对意见，并以此作为拒绝加入《公约》的一个重要理由。然而对中国相关规范的分析和典型案例的介绍却表明，侦查机关在实践中开展的跨境“远程勘验”中有一部分实际上就属于该条款中所谓的“经同意的提取或接收”。

第二，跨境远程勘验掩盖部分强制处分措施。一般认为，勘验属于任意侦查措施。然而，实践中的跨境远程勘验实际上夹杂了部分强制处分措施。如上文所示，在某网络赌博案件中，针对境外网站帐号所进行的“冻结”也被纳入到“远程勘验”之中。又如，规范层面并未明确的“远程搜查”也大量以“远程勘验”的名义得到适用。之所以强调远程勘验的实践做法包含了远程搜查，是基于同实体空间中开展的搜查的对比。例如，侦查机关若要进入嫌疑人的住处查扣计算机设备，只能按照搜查程序进行；然而在虚拟空间，侦查机关使用“勘验”设备远程“进入”嫌疑人设置在境外的计算机系统并提取其中的电子数据，目前却是按照远程勘验程序开展的。又如，侦查机关若要对嫌疑人持有的书信进行调查，一般只能通过搜查程序要求或强制其提交，然而，侦查机关通过讯问获得了嫌疑人提供的邮件帐号和密码后，远程登陆境外邮件系统提取相应数据，在实践中亦是按照远程勘验程序进行的。

虽然勘验和搜查的对象从表面来看有所重合，[33] 但针对嫌疑人的物品、住处及其他有关地方进行的查证因可能侵犯《宪法》《刑事诉讼法》保护的公民合法私有财产、住宅而涉及到基本人权方面的特别保护，故只能按照搜查程序开展。特别是就虚拟空间中远程收集嫌疑人计算机系统中的电子数据而言，除了涉及到财产权而外，还可能侵犯《宪法》第 40 条保护的通信自由和通信秘密，理应定性为搜查。

第三，域外争议重重的实时监控措施实际上得到了授权。如上所言，《公约》第 32 条的 a、b 两个条款均指明，一国单边开展的跨境远程电子取证的措施应当是着眼于“存储”状态的数据，从而将实时监控这样的措施排除在外。比利时《刑事诉讼法》授权的跨境远程取证也只能对电子数据进行“复制”而不能实时监控。虽然《公约》对未予规定的措施模糊性地“既未授权又未反对”，但国际社会对跨境开展的实时监控类取证相较一般性的远程搜查而言更为警惕。而根据《公安机关办理刑事案件程序规定》第 225 条，中国的技术侦查包括“记录监控、行踪监控、通信监控、场所监控”等措施。根据最高人民检察院的解读，在网络环境下，侦查人员采取侵入或者控制他人计算机信息系统的手段，对他人的记录、行踪、通信等进行监控的，应当认定为技术侦查措施。[34] 通过比较就可以看出，国际社会所普遍不能接受的跨境实时监控型技术侦查措施在中国的《电子数据规定》中实际上得到了授权。

〔33〕《刑事诉讼法》第 128 条规定的勘验针对的是“与犯罪有关的场所、物品、人身、尸体”，第 136 条规定的搜查针对的是“犯罪嫌疑人以及可能隐藏罪犯或者犯罪证据的人的身体、物品、住处和其他有关的地方”。

〔34〕参见万春等：《〈关于办理刑事案件收集提取和审查判断电子数据若干问题的规定〉理解与适用》，《人民检察》2017 年第 1 期，第 53 页。

3. 法理基础的深层次反思

一方面是规则理念欠缺对国家主权原则的关照。我国对传统意义上的国家主权原则的尊重自不待言。在此基础上,作为国家主权原则在网络空间中的自然延伸,中国可以说是许多欧美国家并不承认的网络空间主权的坚定支持者。例如国家互联网信息办公室在 2016 年发布的《国家网络空间安全战略》明确指出,“国家主权拓展延伸到网络空间,网络空间主权成为国家主权的重要组成部分”。于是,无论是基于地缘管辖的国家主权原则还是网络空间主权原则,中国都有必要尽力对存储于我国境内的网络设施、设备中的电子数据进行保护,从而排斥他国未经许可的单边远程收集。实际上,这恰恰就是上文提到的外交部门在国际场合的官方态度的理论基础。然而,国家主权原则不可能是孤立的,要维护好本国的主权就必须同时强调尊重他国的国家主权,对于网络空间主权而言也是同样的道理。

不过,在设计跨境电子取证的程序制度时,由于与域外规则发展的大背景脱节,相关规则的内容很大程度上忽视了对国家主权这一基础要素的考虑。根据最高人民法院的解释,对位于境外服务器无法直接获取原始存储介质的,一般只能通过远程方式提取电子数据。[35] 这种理念明显侧重于回应侦查机关便利、高效取证的需要,忽视了潜在的国际法甚至外交风险。实际上,中国与数十个国家签署的刑事司法协助条约多规定了侦查取证方面的内容。2018 年 10 月施行的《国际刑事司法协助法》第 25 条也将“电子数据”与“有关文件、记录和物品”并列,均规定为办案机关需要外国进行协助调查取证的内容。虽然这种程序较为复杂且耗费时间,但无疑是双方在相互尊重主权前提下共同缔造的法律机制。因此,中国在与他国存在刑事司法协助机制的情况下,单方授权侦查机关进行跨境远程勘验或技术侦查,与既定的司法协助框架存在着冲突。

另一方面是具体侦查措施的开展缺乏强有力的权利保障及侦查权制约的考量。其一,中国侦查机关针对境外计算机系统进行的远程勘验和技术侦查在许多情况下都属于秘密侦查,缺乏事前或事后告知的制度设计。《刑事诉讼法》第 130 条规定,侦查人员执行勘验,必须“持有”证明文件;而第 138 条规定,进行搜查,必须向被搜查人“出示”搜查证。由于未明确规定远程搜查,进行“远程勘验”时就无需嫌疑人知晓,而只需“持有”证明文件便可进行,这对嫌疑人权利的保障显然不利。其二,授权开展的侦查措施一定程度上表现出强制侦查的一面,欠缺监督制约机制。具体而言,非经同意状态下使用技术设备对目标系统内存储的数据进行的远程勘验、实时监控等技术侦查均具有强制侦查的属性。而从技术层面来看,跨境远程勘验已经可以做到对目标系统的后台数据进行全盘镜像复制或深度获取。[36] 此外,就经嫌疑人同意而进行的跨境远程勘验而言,虽然应当属于“经同意的搜查”而被纳入任意侦查的措施体系,但实践中也常表现出强制侦查的样态。原

〔35〕 参见喻海松:《〈关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见〉的理解与适用》,《人民司法(应用)》2014 年第 17 期,第 21 页。

〔36〕 例如,北京市公安局在 2015 年发布的《关于办理电信诈骗案件指导意见》的“取证要点及规格”部分,强调远程勘验除了调取涉案网站的前台数据,还要收集“后台数据”,具体而言需重点调取“域名、IP、伪造文书信息、木马等恶意程序和登录维护日志”。

因在于,在中国的讯问程序中,采取非法方法进行的讯问没有根除。在此背景下,侦查人员通过非法讯问获得境外计算机系统的帐号、密码并登陆其中进行所谓的远程勘验,与《公约》有意排斥强制侦查的理念形成了鲜明对照。[37] 然而,对于这些潜在侵权性较强的取证措施,目前尚不存在任何来自于外部的监督或审批程序。而根据《公安机关办理刑事案件程序规定》第255条,技术侦查由设区的市一级以上公安机关负责技术侦查的部门实施,这实际上只是相对其他的侦查措施而言提高了开展技术侦查的侦查机关的级别。与此相对,域外主要国家一方面普遍未明确授权跨境技术侦查,另一方面即使是非跨境开展的这类侦查措施也需要由中立的司法机关进行严格的事前审查。

四　制度重塑的具体建议

从上述比较研究来看,中国以《电子数据规定》为代表的跨境远程电子取证条款与国际发展状况存在着较大程度的脱节。当然,这并不是说中国必须盲从《公约》的内容以及美、比、荷这样具有代表性的国家的法律规定,但是对国家主权原则的遵循以及网络环境下的权利保障和侦查权的控制有必要成为完善中国相应制度的指导理念,这也是未来加强国际合作的基础。

(一)继续单列网络在线提取措施

《电子数据规定》没有将“网络在线提取”纳入“网络远程勘验”当中,而是强调在进行网络在线提取工作的情况下“必要时”可以进行网络远程勘验。虽然《公安机关规则》第28－32条将“网络远程勘验”编排在了第四节“网络在线提取电子数据”的内容体系当中,但是根据第33条的表述,两种措施并非包容而是并列关系。[38] 由于网络在线提取相当于《公约》第32条a款授权的措施因而通常只是提取对境外网站或网络公开信息,实际上对《宪法》和《刑事诉讼法》所保护的重要权利并无任何干预性,因此基于侦查自由原则而开展的这类侦查取证没有必要纳入勘验措施中。

继续单列网络在线提取措施,可以同国际社会普遍接受的类似侦查措施相对接,不仅不会产生国家主权方面的争议,而且信息发布者显然也对相关内容并不持有相应的隐私、数据保密方面的权利期待,因此无需设置特别的监督机制。例如,《刑事诉讼法》第133条规定,勘验过程应当有见证人在场,但是由于网络在线提取措施并不可能导致对目标网站或系统的破坏,因此没有必要要求有见证人在场。

(二)专门设计经同意的勘验和搜查制度

实际上,跨境远程勘验从规范层面来看确实有存在的空间。例如,侦查人员通过合法途径获得受害人或证人的同意,登陆帐户远程提取境外服务器中的用户数据,就不属于搜

〔37〕 根据《公约第32条指引注释》第3.4部分的说明,《公约》第32条b款的适用必须建立在合法且自愿的基础之上,这就意味着提供登陆方式或同意披露数据的人没有受到强迫或者欺骗。

〔38〕 该条规定:“网络在线提取或者网络远程勘验时,应当使用电子数据持有人、网络服务提供者提供的用户名、密码等远程计算机信息系统访问权限。”

查程序,仍应按照勘验程序来开展相应工作。从比较的视角来看,这种经同意的跨境远程勘验属于《公约》第 32 条 b 款所规定的“经同意的提取或接收”的具体表现。

而从中国侦查机关开展跨境远程勘验的另外一些工作来看,要么是直接提取嫌疑人在境外设置的服务器中的电子数据,要么是登陆跨境网络服务提供者的系统提取嫌疑人帐户数据,〔39〕因此都应归入搜查程序。换言之,实践中按照勘验程序跨境远程提取这类电子数据属于侦查措施的定性错误。在法律性质上对跨境远程搜查进行界定之后,就可以按照搜查程序的基本法理来搭建相应的制度框架。从理论上讲,搜查既可以是任意侦查,也可以是强制侦查,前者指经过权利人同意后的搜查,无需证件;后者则指侦查机关经过批准或依职权强行搜查,原则上需要搜查证,但在紧急情况下,也可以进行无证搜查。〔40〕

搜查的第一种类型即经同意的搜查,实际上属于《公约》第 32 条 b 款所规定的“经同意的提取或接收”的一种表现形式。由于这一条款建立在相应主体“合法同意”的基础上,如果根据正当法律程序开展相应侦查工作,其潜在的侵权性较弱,因此得到了多国认可。然而,中国外交部门多次对这一条款提出了反对意见。根据外交部条法司胡生健先生和武汉大学黄志雄教授的解读,反对意见主要体现在两个方面:其一,担忧该条款可能会被滥用,例如可能被用于非刑事侦查程序的情报收集;其二,更为重要的是,担忧国家主权无法得到有效尊重。〔41〕 于是,如果能够在双边或多边平台与相关国家达成共识,在国家主权原则的框架下细化规则从而在法律层面明确排斥情报收集等活动,上述两方面的问题完全可能得到解决。换言之,经同意的远程搜查在跨境提取电子数据的制度中仍然有存在的必要,而且有存在的现实可能性。

(三)将采用技术手段非经同意的搜查纳入技术侦查措施并严格限制运用

跨境远程搜查的另外一种形式是非经同意进行的,属于秘密侦查的一种表现形态。需要注意的是,这种搜查一般都需要采用技术手段进入目标系统后方能提取电子数据。从比较分析来看,这类并未进行实时监控的措施在国外无疑属于搜查,但是在中国现行的侦查措施体系中应纳入到技术侦查措施当中。〔42〕 因此,实践中采用技术手段进行“系统重构”的跨境远程勘验,严重降低了侦查措施的适用标准,应定性为程序误用。

与多数国家没有直接授权相比,这种掩藏于跨境远程勘验之下而实际上应纳入远程技术侦查的远程搜查在中国的侦查实践中已得到一定程度的运用。而从实时监控型远程技术侦查来看,虽然中国将其作为与远程勘验并列的独立的侦查措施,但是国外通常是将

〔39〕 除了最为典型的提取境外邮件系统中的内容数据而外,实践中还包括对提供其他网络服务的平台的注册用户信息进行远程提取的案例。例如,在某走私珍贵动物、珍贵动物制品案中,公安机关使用嫌疑人在 EBAY 网站的用户名 tracywang-xm,远程提取了发帖记录、交易记录等信息的情况。参见《江苏省苏州市中级人民法院刑事判决书》(2015)苏中刑二初字第 00005 号。

〔40〕 参见孙长永著:《侦查程序与人权——比较法考察》,中国方正出版社 2000 年版,第 93 页。

〔41〕 参见胡生健、黄志雄:《打击网络犯罪国际法机制的困境与前景——以欧洲委员会〈网络犯罪公约〉为视角》,《国际法研究》2016 年第 6 期,第 27 页。

〔42〕 实体空间向网络空间转换后,理论上仍应存在非经同意的搜查。但是由于网络空间中进行的非经同意的搜查一般需要采用技术手段破解、侵入系统后远程提取数据,因此在中国的侦查程序规范中与远程技术侦查呈现程序上的交织状态。考虑到远程技术侦查在程序规范力度方面更强,因此无需在规范层面单独规定非经同意的远程搜查。

其作为远程搜查的一个组成部分。作为潜在侵权性最为严重的一种搜查,国外对其跨境运用极为警惕。因此,无论是基于未来加强国际合作还是获得国际认同的考虑,这两类采用技术手段未经同意且秘密开展的跨境技术侦查都不宜得到明确授权,抑或不应将现有的两类措施纳入合法开展的跨境侦查措施体系当中。实际上,《公安机关规则》第 23 条将远程提取"计算机信息系统上的电子数据"限制在了"境内",明显出于这方面的考虑。然而,由于该条是对"网络在线提取电子数据"的规定,其他条文则并未明确禁止针对境外目标系统的远程搜查或技术侦查,因而这两类跨境强制侦查措施在实践中仍可能得到运用,为此应当在未来的规则中进一步作出限制。不过,参考国外立法及国际法原则,中国可以从两方面保留跨境技术侦查措施的运用。其一,参考美国和荷兰的立法,如果确因技术加密等原因而无法确认数据存储位置,允许进行可能跨越国境的技术侦查,但一经确认数据存储地则应及时对相关国家进行告知。其二,基于国际法上的对等原则,如果确认他国有对中国开展同类技术侦查的行为,中国也应对等保留对该国境内的数据使用同种侦查措施进行远程取证的权利。

当然,即使在特定情形下保留对等适用这些跨境强制侦查措施,考虑到跨境远程技术侦查在国际上存在的巨大争议,中国也有必要强化其监督和制约。一方面,必须从横向加强外部监督。就跨境技术侦查的运用而言,国外普遍需要由法官令状授权。考虑到当前的国情,有学者建议由性质上同属司法机关的检察机关来行使电子数据搜查的审批权比较适当。[43] 笔者同意此观点,将这类强制处分措施的审批权从侦查机关剥离出来确有必要,考虑到相应取证措施所涉及的法律问题的复杂性,由检察机关行使审批权更加合适。特别是对于实时监控型跨境技术侦查的适用而言,应强制要求司法机关进行事前审查以进行最为谨慎的风险评估。另一方面,必须从纵向加强内部监督。例如,通过最高层级的侦查机关对跨境技术侦查进行把关,一来可以避免基层侦查机关滥用这类侦查措施,二来在出现国家主权争议或外交纠纷的时候能够保证相关部门更好地与他国进行沟通和交涉。从公安机关开展的跨境技术侦查来看,即使无法做到所有案件都由公安部进行纵向审批,但是也有必要通过系统内部的专门平台向公安部主管机构备案。此外,公安部与外交部有必要建立与此相关的定期联络与沟通机制。

五 结 语

本文在对以《公约》为主的域外跨境电子取证制度进行分析的基础上,结合中国的规范和实务作出了理论评析,提出了重塑相应制度的具体方案。这种重塑意味着对侦查中跨境远程电子取证的严格限制。这样一来,很可能导致大量侦查实务无从快捷开展。为了平衡理论方案和侦查实务的需求,有必要从更为宏观的国际发展背景来寻找出路。实际上,各国在侦查中采取的跨境远程电子取证的系列措施不是孤立的。具体而言,跨境电子取证除了单边的远程收集而外,还包括刑事司法协助及针对跨境服务提供者的数据披

〔43〕 参见陈永生:《电子数据搜查、扣押的法律规制》,《现代法学》2014 年第 5 期,第 122 页。

露这两种基本形式。[44] 三种方式是互动发展的,如果刑事司法协助及数据披露制度运转良好,一国侦查机关自然没有必要在可能触犯他国主权的情况下选择单边路径;反之,如果前两种制度在运行时出现障碍,单边路径的需求就会上升。就此而言,在未来的规范层面限制跨境远程电子取证,有必要通过简化刑事司法协助机制或者通过跨境数据披露的方式来回应实践需求。

[本文为作者主持的 2019 年度教育部人文社会科学研究青年基金项目“网络空间主权视域下的跨境电子取证制度研究”(19YJC820033)的研究成果。]

[**Abstract**] In the Internet era, more and more electronic data is stored overseas, thus posing a great challenge to criminal evidence collection both at the technical level and at the legal level. Over the past several years, China has taken the unilateral route of empowering investigative organs to have access to overseas data by such means as remote network inspection, technical investigation and so on. However, this procedural system is inconsistent not only with the Convention on Cybercrime and the domestic legislation of some other countries, but also with the position taken by China's foreign affairs departments and its current criminal judicial assistance mechanism. According to the principle of state sovereignty and ideas of protection of rights and control of investigative power in the network environment, it's necessary to strictly limit investigative organs' power of cross-border access to electronic data by unilateral means. More specifically, the norms on investigative procedure with respect to cross-border remote access to data can continue to authorize online taking measures. Consent-based remote network inspection and search measures should be specially designed, and search without consent by technical means should be incorporated into technical investigation measures and their application should be strictly limited. On this basis, it is necessary for China to simplify the criminal judicial assistance mechanism or respond to the practical evidence collection demands with cross-border data disclosure, and take it as an alternative way of restricting cross-border remote access to data.

(责任编辑:郑 佳)

〔44〕 参见梁坤:《〈美国澄清合法使用境外数据法〉背景阐释》,《国家检察官学院学报》2018 年第 5 期,第 159 – 165 页。