# 第一章

# 跨境电子取证管辖的理论模式总览

2014年1月至12月期间，张某宇雇佣了焦某（另案处理），为其上线“核对”收集可以进行分布式拒绝服务攻击（也称为DDOS攻击）的“肉鸡”[①]，以及可以被调用的网络流量。张、焦二人在网络上发布广告寻找下线，并在网上联系了罗某和黄某丙等下线。下线将木马程序植入其各自获取漏洞的计算机信息系统中，使计算机信息系统成为“肉鸡”。张、焦二人通过测试“肉鸡”的可控网络流量的大小来支付相应的费用给下线。同时，张、焦二人将“肉鸡”的控制权交给“核对”，从中赚取后者支付的用于收购流量的现金共计人民币40.11万元。

2014年12月16日，公安人员将张、焦二人抓获。焦某归案后主动向公安机关提供了一台位于美国的主控服务器的IP地址、用户名和密码。武汉市公安局网络安全保卫支队二大队出具的远程勘验检查工作记录证实，侦查人员远程登录美国主控服务器（IP地址为66.102.253.30），提取到了主控程序“Client.exe”和“系统日志”。“主控列表”显示共控制了240个IP地址，其中我国境内的IP地址为31个。[②]

上述案例中电子数据的取证反映了我国近些年的一段时间内许多同类案件的做法，侦查机关通过讯问等方式获得嫌疑人提供的账号和密码后登录服务器，进行了后文将要具体展开分析的我国刑事程序法所规定的跨境网络远程勘验。

从美国的情况来看，在同一时期，一起涉及跨境电子邮件数据收集的案件的侦查程序引发了巨大的法律争议。2013年12月，执法人员在一起贩卖毒品案件中，根据1986年的《储存通信记录法》（*Stored Communications Act*）也即《美国法典》“§2703”部分的规定，在取得纽约一家法院签发的搜查令状后，要求微软公司披露涉案邮件用户的信息。然而，由于部分数据当时并未储存于美国境内的服务器中，而是位于爱尔兰首都都柏林的欧洲云服务器的数据中心的服务器之中，

① 被非法植入了木马程序并被控制的计算机信息系统，也叫“被控端”。

② 参见湖北省武汉市中级人民法院（2016）鄂01刑终176号判决书。

微软公司因此坚持要求后者直接披露相应邮件的数据。这便是外文文献中常称的“Microsoft-Ireland Case”案件，本书为论述方便，使用“微软爱尔兰案”加以指代。

无论是从国内法还是国际法的角度来看，一国虽然可以依国内刑事法对发生在他国境内的犯罪享有立法管辖权（prescriptive jurisdiction）及裁判管辖权（adjudicative jurisdiction），但是原则上并不能在程序上行使执法管辖权（enforcement jurisdiction）。[①] 刑事执法管辖权从广义上指的是一国执法机关依照法定程序侦查、起诉和执行刑罚的权力，[②] 而狭义上仅涉及刑事侦查管辖特别是问题较为突出的刑事取证管辖。作为刑事执法管辖的下位概念，国家的刑事取证管辖通常也不能在未经许可的情况下延伸至境外。然而，在如今的网络时代，以领土范围为标准的管辖界限逐渐模糊，近年来各国在刑事侦查中收集电子数据时跨越传统国家疆界的现象已经屡见不鲜。中美两国的侦查机关在上述案例中开展的跨境电子取证，实际上就是在这样一种宏观发展背景下产生的。

从中国的上述案例来看，侦查机关通过网络远程勘验直接收集了存储于境外的数据。从本章接下来所称的国家刑事取证管辖的角度而言，这种跨境电子数据取证方案显然与常规意义上的“数据存储地模式”不符。而在美国《澄清合法使用境外数据法》（后文简称《云法案》）已经施行的背景下，美国执法部门今后必将充分依托该国在全球范围内占据巨大市场优势的网络服务提供者间接收集境外数据，也即在刑事取证管辖模式方面将更多地采用与“数据存储地模式”迥异的“数据控制者模式”。两案跨境电子数据取证的具体程序、措施尽管存在显著区别，但是均表明，刑事取证管辖已经借助网络空间而便捷地跨越了传统意义上的国家疆界。

由于刑事取证管辖乃是国家主权行使的典型反映，因此两案突显出来的根本问题即在于，国家到底是否能够在国际法及刑事程序法理的框架下对网络空间中位于境外的数据拥有主权及刑事取证管辖权？而这个问题背后更为根本性的问题则在于，不同的国家在数据主权及数据安全的战略和主张方面出现冲突时，应当

① Anthony J. Colangelo,“What Is Extraterritorial Jurisdiction”，*Cornell Law Review,* 99(2014): 1311.
② 张兰图、刘竹君：《国家刑事管辖权法定论》，载《当代法学》，2006（5）。

如何进行协调并且在国际层面作出恰当的制度安排？

如果肯定一国在一定程度上对存储于境外的数据拥有刑事取证管辖权，那么具体到本章的论题而需要进一步回答的问题即在于，针对网络空间中的数据，特别是存储于境外的数据行使刑事取证管辖权的时候，一国到底应当采取什么样的理论模式加以执行？本章将立足我国所主张的数据主权战略，在对数据存储地模式、数据控制者模式进行深入的理论分析的基础上，着力探索反映中国立场、彰显中国气派的方案，希冀在国际法原则和规则的框架下为国家刑事取证管辖模式的完善提供有益的参考。

## 第一节　基于传统国家疆域的数据存储地模式

### 一、数据存储地模式概说

所谓数据存储地模式，即以数据实际存储的物理位置来确定国家的刑事取证管辖范围。关于这一模式，可以具体从 4 个方面理解：其一，将数据视为与其他有形实物无实质差异的证据，在刑事取证管辖制度上不做特殊安排；其二，将数据视为与存储介质密不可分的物品，管辖依据实际上就是存储介质的物理位置；其三，将虚拟空间附着于物理空间，相当于将传统的适用于物理空间的地域管辖同等延伸至虚拟空间；其四，以传统意义上的属地原则（territoriality principle）来确定刑事取证管辖的疆界，其效力范围实际上等同于国家在刑事实体法上的属地管辖。

根据数据存储地模式，一国对境内的电子介质中存储的数据拥有理所当然的刑事取证管辖权。如同 A 国侦查人员不能在未经许可的情况下跨入 B 国国境开展侦查取证活动一样，其原则上也不能采取任何方式擅自“进入”后者境内的计算机系统收集电子数据。为了避免电子数据取证的侦查行为越境，许多国家的国

内法的适用及国际公约对相关制度的安排都较为谨慎。例如，英国法官在签发远程搜查令状的时候，就需要判断警方的侦查是否会跨越国境。如果违法从境外收集数据，法院在后续程序中就可能将其予以排除。[①]

而在美国，在过去很长时间的刑事侦查实践中，执法部门也曾经将数据存储地模式作为一般性的准则。1999 年至 2000 年间，两名俄罗斯黑客利用 Windows NT 系统的漏洞，从俄罗斯境内多次侵入美国的网络服务器、网上银行及在线电子商务系统，成功窃得 56000 份信用卡账户及个人金融信息（下文简称“俄罗斯黑客案”）。在此之后，这两名黑客以公布用户数据及损坏公司计算机系统相威胁，对大量的受害者进行了敲诈。此外，eBay 网站的在线拍卖、PayPal 在线支付系统也受到了他们的操控。据统计，该案造成的损失达 2500 万美元。美国联邦调查局探员经过缜密的调查之后，最终锁定其中一名嫌疑人位于俄罗斯。

于是，探员进一步开展了一次极具争议的秘密侦查。他们化身为一家名为“Invita”的网络安全公司的代表，于 2000 年与两名嫌疑人取得了联系，假装是与后者商谈在美国的预期业务。两名嫌疑人竟然信以为真，并在俄罗斯向上述“公司代表”展示了针对一个测试网站使用的黑客技术。在“公司代表”的邀请下，两名嫌疑人飞到了美国西雅图，并且就其计算机技术接受了“访问”。在此过程中，其中一名嫌疑人甚至登录了位于俄罗斯的计算机系统。然而，这些“访问”实际上就发生在配有精密装备的特定办公室当中。联邦调查局的探员使用了一款名为“探针”（sniffer）的案件记录软件，由此获取了嫌疑人的用户名和密码。此后，两名嫌疑人遭到了逮捕。

接下来就是进一步的调查取证。但是在当时，美俄两国的双边合作并未延伸到计算机犯罪的调查。在数次尝试获取俄罗斯当局的协助未果后，美国联邦调查局决定自行开展远程取证。调查人员通过上述用户名和密码登录了嫌疑人位于俄罗斯车里雅宾斯克市的目标系统，从服务器中下载了数据，并一直将数据以非读取状态进行保存。此后，联邦调查局在获得法院签发的搜查令状之后，再对这些数据进行了读取。

这起极具争议的跨境侦查取证活动最终通过司法裁判得到了盖棺定论。美

① Ulrich Sieber, Nicolas von zur Mühlen(eds.), *Access to Telecommunication Data in Criminal Justice*, Berlin: Duncker & Humblot, 2016, p.730.

国法院认定，由于数据存储于俄罗斯，因此此案的侦查行为属于跨境搜查。[①] 在总结了法律实践经验之后，美国司法部刑事处计算机犯罪与知识产权犯罪部（CCIPS）在 2009 年发布的《刑事侦查中计算机搜查扣押与电子证据收集指引》中慎重地提醒，调查人员在未经许可的情况下“进入位于他国的计算机系统”，可能触及“国家主权及礼让方面的复杂问题”。[②]

哈佛大学著名的网络法专家 Goldsmith 尽管也认为这种搜查在打击特定的计算机犯罪的成功战略中是一种关键的武器，但是其也严肃地指出，跨境远程搜查等方式（收集存储于他国境内的数据）在性质上属于侵犯他国主权，可能面临严重的国际法后果甚至外交纷争。[③]

根据数据存储地模式，跨境电子数据取证原则上应遵循适用于普通实物的程序规则，也即需要通过司法协助程序加以执行。例如在“微软爱尔兰案”中，爱尔兰政府的主张便明显地反映出对这种模式的信奉以及对司法协助程序的坚持。其在 2014 年 12 月 23 日向美国法院递交的“法庭之友意见书”（amicus brief）中申明了对涉案邮件内容数据的主权管辖，强调只有通过两国之间的双边刑事司法协助机制，才能由爱尔兰官方对相应数据进行调查。[④] 换言之，爱尔兰政府对美国政府越过司法协助程序直接要求微软公司提供其所掌握的位于前者境内的数据，是持反对态度的。

## 二、数据存储地模式面临的困境

数据存储地模式尽管是长久以来规范跨境电子数据取证的基本方案，然而随着时代的发展，其也逐渐面临难以克服的困境，而且相应的困境表现得越来越突出。

---

① United States v. Gorshkov, NO. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

② See CCIPS, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, p.58, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf, 最后访问日期：2018 年 11 月 1 日。

③ Jack L. Goldsmith, “The Internet and the Legitimacy of Remote Cross-Border Searches”, *University of Chicago Legal Forum*,2001(2001), 103.

④ See Brief for Ireland as Amicus Curiae Supporting Appellant at 4, 7, In re Warrant To Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2 9 85-CV (2d Cir. Dec.23, 2014).

### （一）数据存储地模式适用困难

首先，数据存储地模式适用于数据于境外只有单一存储地的案件，而难以适用于有多个存储地的案件。在云计算时代，一些大型跨国企业在多个国家建立了云数据中心，相应的业务数据经常会以非常迅捷的方式在各个数据中心之间实现跨境传输。在这样的技术背景下，一国如果在进行某起案件调查的时候向多个国家同时发送协助申请，这显然是十分难以操作的。而且还不能排除这种可能性，即当接受申请的一方开始审查抑或执行取证工作时，要收集的数据可能已经恰好被传送到另一个国家了。这就导致整个司法协助程序的运行可能完全做了无用功。

此外，当一家企业的数据存储于多个国家时，其如果从技术上可以较为便捷地将位于多国的数据进行转移，这便导致其有可能在特定的情况下规避数据的初始存储国的刑事管辖，[①] 从而导致数据存储地模式在适用中遭遇困境。这显然不是采取数据存储地模式的国家所希望看到的结果。

其次，数据存储地模式适用于存储情形下的静态数据（data at rest），而难以适用于传输过程中动态数据（data in transit）。[②] 对于静态数据而言，由于存储介质的物理位置通常都较为明确地位于某一司法管辖区，因此在确定刑事取证管辖时也相对较为容易判断。然而对于跨境传输的动态数据而言，侦查取证实际开始前，却难以预测所要收集的数据会流向何处，这便导致无法适用这种模式来确定管辖。从具体的侦查实践来看，从公共政策、隐私保护等角度考虑，区别对待这两种类型的数据显然是有意义的，而且即使从境内开展电子取证的法律程序而言，也应存在较大的区别。但是对于侦查机关和网络服务提供者而言，问题在于，在技术上区分静态和动态传输中的数据是否有意义，以及在云环境中如何确定两者的界限。于是，当侦查机关要求网络服务提供者提交数据时，后者将面临法律、程序，以及操作上的不确定性。而且，当侦查机关进行调查取证时，其也会面临

---

① See Cybercrime Convention Committee (T-CY), Criminal Justice Access to Data in the Cloud: Challenges, p.11, issued on 26 May 2015, https://rm.coe.int/1680304b59, 最后访问日期：2022年1月9日。

② 需要注意的是，数据是“静止的”或是“传输的”并不表示数据的技术状态，因为云服务商所存储的数据——或称“静止的”数据——通常可能在服务商的内部资源中“传输”，例如数据因使用负载均衡技术而传输。这些词用于从法律上区分执法机关访问数据的不同权力。参见 [ 英 ] 克里斯托弗·米勒德编著：《云计算法律》，陈媛媛译，417页，北京，法律出版社，2019。

所需遵守的法律的不确定性，或者需要承担其所取得的数据被排除的风险。[①]

于是，仅仅适用于静态数据的数据存储地模式在面临信息技术特别是云计算技术的飞速发展的挑战时，在一定程度上也会面临难以适用的困境，因此难以成为跨境电子取证管辖模式设定的唯一理论依据。

再次，数据存储地模式适用于位置确定的数据，而难以适用于位置不确定的数据。数据的位置如果非常明确地位于一国境内，那么数据存储地模式对于管辖权的设定而言当然最为有利的。然而，“深网”（deep web）中的多数数据通常会有加密保护，“暗网”[②]（dark web）则无法通过常规方式访问及追踪，[③]这些技术性的限制因素都给数据存储地的确定和相应模式的适用造成了极大的障碍。在当今云计算的技术框架下，这个问题会变得更加复杂。

无论是通过网络服务提供者披露数据，还是由用户提供数据，数据的存储位置经常是不明确抑或无法确定的。[④]典型的情况在于，我们从日常经验便可以获得，使用云存储服务的绝大多数用户都不可能清楚其上传至“云”中的数据到底位于何处。实践中，当执法机关使用远程数据检索方式收集电子数据时，会更需

---

① 参见 [ 英 ] 克里斯托弗 • 米勒德编著：《云计算法律》，陈媛媛译，431 页，北京，法律出版社，2019。

② 暗网（不可见网，隐藏网）（dark net/web）乃是“深网”（deep web）的一部分，是指那些存储在网络数据库里、但不能通过超链接访问而需要通过动态网页技术访问的资源集合。它们无法通过通常的浏览器的搜索引擎检索并登录，而需要通过特殊的软件、特殊的计算机配置或授权才能够登录。

③ 基于多重加密技术的运用，游荡于暗网中的犯罪分子极难通过常规的网络定位等技术加以锁定。用户的交易完全匿名，而且位置也不会暴露。买卖双方的真实交易被掩藏在大量虚假交易当中，因此两者之间的实际联络难以辨别，侦查机关即使采用最为先进的监控软件也难以锁定。根本原因在于，现有的监控手段主要是依赖于对第三方电脑系统中留下的电子痕迹进行的“流量分析”（traffic analysis），这是一种实时进行的数据侦听机制，然而这种电子痕迹在暗网中都被掩藏了起来。如此一来，侦查机关便无法收集第三方服务器提提供的数据通信中涉及的“元数据”（metadata），也即关于通信数据的基础信息，例如来源地、目的地、数据流通量等重要的信息。例如，如果犯罪分子经由暗网以匿名方式登陆了邮件服务器，侦查机关一般会随即要求持有该邮件服务器的公司披露诸如嫌疑人 IP 地址这样的重要信息。但是该公司只会回复，嫌疑人隐藏了其 IP 地址信息。这样的结果无疑令人感到相当沮丧！在刑事案件侦查中，由于这些信息在锁定电子证据或电子设备的物理位置至关重要，因此这些重要信息的缺失导致对涉及暗网的案件的侦查就很难通过常规监控手段开展。进一步讲，由于无法确定电子证据或电子设备的物理位置，嫌疑人的身份等信息也就无法获取，当然就更谈不上对目标计算机系统进行实地勘验或搜查。

④ Christopher Millard(ed.), *Cloud Computing Law*, Oxford University Press, 2013, p.288.

要云服务商的协助。执法机关也可通过用户（无论是否为嫌疑人）访问设备来获得证据材料，而具体的方式可以表现为强制、自愿，抑或暗中进行。但是，当云上数据因调查程序而被获取时，其位置（数据所在的物理计算机）都可能是未知且不可知的，因此数据位于哪个或哪些领域也就不得而知。而这种位置的确认可能只能通过检索后进一步的法庭证据分析才可实现。换言之，对云上数据实际存储位置的确认在很多情况下会发生在证据调查之后的后续阶段，而不是启动调查的时段。[①] 于是，多重不利因素的叠加，会导致一国侦查机关不可能严格地、单一地遵循数据存储地模式来行使取证管辖权。

### （二）数据存储地模式效率低下

随着跨境通信及云计算技术的飞速发展，数据的跨境存储与流动在如今已经越发常态化。如果严格遵循数据存储地模式，数据的跨境收集原则上都需要通过司法协助程序开展。然而，传统刑事司法协助制度效率“极其复杂、缓慢和官僚化”。根据 Ian Walden 的《云中数据：长臂执法者》（*Accessing Data in the Cloud: the Long Arm of the Law Enforcement Agent*）和 George Yee 的《云计算、计算机通信和网络中的隐私和安全》（*Privacy and Security for Clouding Computing, Computer Communications and Networks*）的论述，在数据高速流动的今天，这种迟缓难以有效应对涉犯罪数据的全球高速流动，极大阻碍了犯罪的有效控制和侦查。[②] 我国也有研究者结合非法集资与非法吸收公众存款犯罪、跨境信用卡犯罪、非法经营地下钱庄等跨境金融犯罪案件指出，办案机关往往需要调取境外有关证据材料，如涉案资金流向境外的查询、境外套现的监控视频、境外服务器的勘验等。然而，境外取证常常遭遇层层审批时间长、通过审批后取证周期长、取证难度大等困难，严重影响案件侦查效率。[③]

从近年的情况来看，这类跨境取证需求的剧增进一步导致数据存储地模式在

① [英] 克里斯托弗·米勒德编著：《云计算法律》，陈媛媛译，419 页，北京，法律出版社，2019。

② 转引自裴炜：《未来犯罪治理的关键——跨境数据取证》，载《中国信息安全》，2019（5）。

③ 参见叶媛博、植才兵、江伟波：《广东跨境金融犯罪的形势分析及打防对策》，载《中国刑警学院学报》，2018（1）。

适用过程中的效率低下。由于美国在全球云数据市场占有绝对市场地位，该国当前收到的取证请求也最多。然而，一国地方侦查机关若要搜查谷歌公司存储于美国境内的邮件内容数据，按常规程序需要首先将协助请求逐级上报至该国中央主管机关，然后由后者将协助请求按美方要求的形式发送给司法部国际事务办公室。国际事务办公室审查后，再将该协助请求交由检察官处理，然后再由后者向对数据有管辖权的法院申请搜查令状。之后，警务人员才可持令状要求谷歌公司提供相应数据。美国近年来的统计数据表明，整个协助程序通常需要耗费 10 个月以及更长的时间，[①] 甚至可能长达两年或数年，[②] 这对追求快捷理念的电子数据取证而言显然是难以承受的。

## 三、数据存储地模式的松动

在数据存储地模式面临上述困境的情况下，呼吁对这种模式进行有效改造的声音近年来不绝于耳。甚至早在 1999 年举办的“第二届犯罪情报分析国际会议”（Second International Conference for Criminal Intelligence Analysts）上，英国内政部前国务大臣 Paul Boaten 就曾发表名为“未来执法的挑战”（Tomorrow’s Challenges for Law Enforcement）的演讲。其主张，“关于数据的管辖权不应仅仅取决于实际存储的位置。如果数据的所有者能够从境外远程获取，那么应当认为该所有者所在地的执法部门便对该数据拥有管辖权。”[③] 根据该观点，如果 A 国的一家公司在 B 国设立了分支机构，如果该分支机构能够有效地远程获取位于 A 国总部的计算机数据的话，则 B 国执法部门对该数据的跨境远程取证行为

① Richard A. Clarke, et. al.,“Liberty And Security In A Changing World: Report And Recommendations Of The President’s Review Group On Intelligence And Communications Technologies”(2013), p.227, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, 最后访问日期：2018 年 11 月 9 日。

② Department of Justice Office of Public Affairs,“U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online”, https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists, 最后访问日期：2022 年 1 月 23 日。

③ See Michael A. Sussmann, The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium, *Duke Journal of Comparative & Interlnational Law*, (9)1999, 472.

就不应被视为侵犯 A 国主权。

为了缓解上述危机并有效提升跨境电子数据取证的效率，区域性国际公约及一些国家的国内法作出了一些有针对性的制度安排，从而导致严格意义上的数据存储地模式实际上已经松动。

### （一）数据存储地模式松动的具体表现

#### 1. 在国际共识的基础上设定数据存储地模式的特殊例外

2001 年的《布达佩斯公约》（*Budapest Convention on Cybercrime*）[①] 第 32 条和 2010 年的《阿拉伯国家联盟打击信息技术犯罪公约》（*Arab Convention on Combating Information Technology Offences*）第 40 条规定了两种无需告知数据存储地国家的单边远程取证方式。由于后者几乎照搬了前者的条文，因此这里仅对《布达佩斯公约》第 32 条进行阐释。该条 a 款规定，缔约国执法部门可以“提取公众能够获得的存储于计算机中的数据，而不论该数据位于何处。”由于这类数据可以在执法地便可以公开获得，国际法专家们认为这种情况属于域内管辖权的行使；[②] b 款则采“属人主义”，授权“通过一方境内的计算机系统提取、接收存储于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个体（person）的合法且自愿的同意。”

为了避免法条适用过程中可能产生的理解偏差，《布达佩斯公约》委员会（T-CY）于 2014 年发布《跨境电子数据取证指引注释（第 32 条）》，强调 b 款在性质上属于地域管辖原则的特殊例外。[③] 根据国际电信联盟（ITU）编纂的电子出版物的阐释，就缔约国而言，通过批准签署《布达佩斯公约》，实际上是

---

① 该公约于 2001 年 11 月由欧洲理事会的 26 个欧盟成员国以及美国、加拿大、日本和南非等 30 个国家的政府官员于匈牙利首都布达佩斯签署，并于 2004 年 7 月生效，全称应译为《布达佩斯网络犯罪公约》。出于简要表述的方便并区别于第五章将要分析的《联合国打击网络犯罪公约》，本书将《布达佩斯网络犯罪公约》统一简称为《布达佩斯公约》。

② [美] 迈克尔·施密特总主编：《网络行动国际法塔林手册 2.0 版》，黄志雄等译，107 页，北京，社会科学文献出版社，2017。

③ Cybercrime Convention Committee (T-CY), “T-CY Guidance Note # 3: Transborder access to data (Article 32)”,p.3, https://rm.coe.int/16802e726a, 最后访问日期：2018 年 10 月 26 日。

放弃了部分主权，从而允许其他国家实施影响其领土完整的调查。[①]

**2. 在数据存储于境外但无法确认所在国家的情况下直接适用国内侦查程序**

正如前文所言，云计算技术的运用有时会导致数据在境外的具体位置难以确定。原因在于，“传统刑事司法协助制度所具有的强烈的地域性与数字侦查本身的弱地域性之间存在冲突，请求国难以在作出请求之前就及时确知案件所需数据的所在地。以云计算为例，其核心在于‘以灵活性和去地域性为属性，基于用户需求对计算资源进行快速和无缝式分配’。云计算的高效能恰恰得益于计算资源与地域属性相脱离，其中又以碎片化的存储、多资源的集合、网络化的接入为典型特征。这种技术使一国的刑事司法权力机关在察觉犯罪之后，难以快速判断相关数据所在地以及适用的法律，更不用说基于该判断向相关国家提出刑事司法协助请求。”[②]

2017 年发生在美国的一起欺诈案件的调查便是云计算技术阻碍常规管辖，使得正常侦查难以施展的典型反映。该案裁决结果与“微软爱尔兰案”的案情有类似之处，因而得到了广泛的关注。联邦第二巡回法院于 2 月 3 日在裁决中指出，连谷歌公司也无法确定涉案数据被技术性地拆分后在境外的具体存储地，因此联邦调查局根本就不可能按照数据存储地模式而开展常规的刑事司法协助。据此，谷歌公司必须按照令状的要求，向当局全部转交储存在境外服务器上的该公司客户邮件数据。

法官 Thomas Rueter 在裁决书中指出：“对隐私的侵犯仅仅发生在美国境内。当联邦调查局根据令状在宾夕法尼亚州对要求谷歌披露的数据的复制件进行检验时，此职权行为仅仅发生在美国境内。据此，即使其他的行为（数据的电子传输）发生在境外，该案也是符合《储存数据记录法》的规定的。”裁决书进一步论证道，当网络服务提供者被要求从境外“取回”（retrive）数据时，这种发生在境外的对信息的复制以及将信息发回美国的行为并不构成《宪法第四修正案》中所规范的（境外）“搜查”和“扣押”。具体而言，谷歌在未经用户知晓的情况下将位于境外的服务器中的数据转移至谷歌在加利福尼亚的数据中心，并不属于调

① 《了解网络犯罪：现象、挑战及法律对策》，第 282 页，载 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx, 最后访问日期：2018 年 3 月 18 日。

② 裴炜：《未来犯罪治理的关键——跨境数据取证》，载《中国信息安全》，2019（5）。

查机关的“扣押”行为。虽然储存在境外的数据确实存在隐私被侵犯的风险，但这样做并不会对账户持有者的利益产生明显侵害。即使可能发生潜在的隐私侵权方面的问题，那也是在美国境内对谷歌公司披露的数据进行搜查的时候才会发生，而并不是发生在境外。[①]

**3. 在数据存储位置不确定的情况下不排斥电子数据取证措施的跨境适用**

有些案件的电子数据取证在开始之前，调查人员根本无法判断数据可能存储于何处。例如，在对“暗网”进行调查的时候，由于并不清楚数据实际所在的地点，因此可以说，一国侦查机关在这种状态下开展远程搜查，即使事实上出现跨境开展的情况，调查人员一般而言也并不是明知的。某些国家的法院在对这类搜查行为签发令状时，一般也并不存在明确授权调查人员跨境搜查的意图。但是问题在于，签发令状时间在前，实际执行搜查时间在后。于是，即使开展远程搜查的时候，假定搜查地点就在境内，但是搜查暗网毕竟极有可能跨越国境，从而导致一国侦查机关实际上扩大了应有的管辖范围，进而产生侵犯他国主权的结果。从这个意义上讲，对服务器实际处于境外的暗网的搜查，与只在一国境内且只在一定司法管辖区内有效的司法令状的要求构成了内在冲突，从而导致根据司法令状开展的实际调查活动很有可能在不经意间引发国际争端。

例如，美国有专家就认为，允许法官签发地点不明确的远程搜查令状，结果便是在联邦调查局的发展历史中最大限度地扩大了跨境执法的管辖权力。在此背景下，为了解决“暗网”取证等情况下无法明确数据实际存储地的问题，2016年12月1日修正施行的美国《联邦刑事程序规则》（*Federal Rules of Criminal Procedure*）“41（b）（6）”条款规定：“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权的法官，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。”换言之，新的规则授权执法部门在“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”可以对管辖区外甚至存

① In re Search Warrant No. 16-960-M-01 to Google; In re Search Warrant No. 16-1061-M to Google, 232 F. Supp. 3d 708.

储于境外的数据施以远程侦查措施。[①]

此外，另外一些国家的国内法也对可能跨境适用的远程侦查措施进行了并不绝对排斥的授权。例如，比利时于 2000 年颁布《计算机犯罪法》（*Computer Crime Act*），据此在《刑事诉讼法》中通过第 88 条之三（Art. 88*ter*），在全球范围内率先对跨越国境的远程搜查进行了规定。具体而言，警方可以在侦查法官授权后搜查计算机系统，而且这种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境外系统当中。而在欧盟，截至 2016 年 9 月，比利时、葡萄牙、西班牙、法国的国内法也对这类取证活动进行了授权。[②] 此外，荷兰于 2019 年 1 月 1 日施行《计算机犯罪法（三）》（*Computercriminaliteit III*），在“ARTIKEL II G”部分赋予了侦查机关开展技术侵入（binnendringt）并通过植入监控软件进行远程搜查的权力，在数据存储位置不确定等情况下也并不绝对排斥潜在的跨境侦查活动的开展。

### （二）数据存储地模式并未完全崩塌

不可否认，数据存储地模式本身存在着上文指出的种种缺陷，给刑事取证管辖带来了一系列的障碍，近年来也确实出现了松动。然而，这一刑事取证管辖模式并未崩塌，仍然是国际上刑事取证管辖制度运行的重要方案。这主要有 3 个方面的原因。

其一，在数据于境外的存储位置明确的情况下，刑事司法协助仍是常规程序。除非国际公约的特别授权和国家间礼让机制的存在，一国单边开展的跨境电子数据取证与其他实物证据的跨境收集并无实质差异，原则上都不为国际法所允许。以上述“俄罗斯黑客案”为例，美国联邦调查局所采取的单边跨境远程搜查

① 在《联邦刑事程序规则》修订之前，美国执法部门就已经在针对“暗网”犯罪的调查中采取了这类措施。通常，美国执法部门会首先利用软件漏洞，通过互联网将恶意软件部署到目标设备，获取系统的访问权限；然后，在所控设备上执行命令将其变为监视设备，将文件、照片和存储的电子邮件等秘密地上传到由执法部门控制的服务器上，从而获得并固定证据。例如，远程搜查在“丝路”等“暗网”案件的侦查中发挥了重要的作用。由于无法监控被调查对象的实际地址，通过在目标系统植入特殊软件进行证据调查，完全不用考虑目标计算机系统的实际位置到位于何处。

② European Commission,“Commission Staff Working Document Impact Assessment(SWD(2018) 118 final)”,p.33, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN, 最后访问日期：2018 年 10 月 29 日。

即使从目前来看，在国际法上也没有适用的空间，仍然受到数据存储地模式的严格限制。

其二，侵犯性较弱的远程取证措施更受青睐，以尽可能降低对数据所在地国家之主权的潜在侵犯程度。除了美国和荷兰对可能跨境开展的侦查行为规定了远程“搜查”和“技术侵入”这样的强制性措施而外，上述国际公约和其他国家的国内法所授权的措施的侵犯性明显较小。例如，《布达佩斯公约》第 32 条 b 款授权通过“属人主义”收集境外数据，需建立在相关主体“自愿”的基础上，从侦查法理上讲，一定程度上具有不限制相对人基本权利的“任意侦查”的特征。比利时于 2000 年修订的《刑事诉讼法》第 88 条之三（Art. 88ter）规定的可能跨境开展的电子数据取证方式则只限于“复制”。正如第四章的分析还将指出的那样，从欧盟委员会于 2018 年 4 月发布的规范成员国单边跨境远程取证的立法计划来看，也强调取证方式只能限于“复制”而不能进行“实时监控”。[①]

此外，我国澳门特区于 2019 年 12 月 22 日生效的《打击电脑犯罪法》规定了“不涉单方跨国取证”的境外云端数据的取证方式，以此授权执法部门提取储存于澳门以外的电脑数据资料副本作为刑事诉讼程序的证据。此次修法参考了葡萄牙、新加坡及中国内地的相关规定，采取争议不大的方式，亦即在法官批示的情况下，且在澳门地区合法扣押设备间接引申出去，例如利用相关设备登入过的云端资料进行下载。[②] 据此，澳门特区执法部门通过云端技术在线取证，需要满足两个严格的前提条件：一是司法官命令；二是已在澳门扣押电脑设备。由此，澳门特区的做法并无合法入侵、远端取证这些争议较大的行为，保安司司长黄少泽特别强调澳门“百分百不会违反国际公约”。[③]

其三，在远程取证过程中确认数据存储地后，对相关国家的告知受到重视。相应的制度在比利时《刑事诉讼法》、荷兰《计算机犯罪法（三）》上述条款的相关配套机制中均有反映。例如，荷兰官方认为，一旦确认远程搜查跨越国境，

① 同上引报告，第 71 页。

② 参见《行政会完成讨论修改第 11/2009 号法律〈打击电脑犯罪法〉法律草案》，https://www.gov.mo/zh-hans/news/256843，最后访问日期：2019 年 10 月 25 日。

③ 参见《打击电脑犯罪法一般性通过》，载《澳门日报》，2019 年 10 月 18 日，第 A14 版。

原则上需停止侦查，并且需要基于国际礼仪及时告知相应国家。[①] 此外，欧盟方面于 2017 年在其发布的非正式文件《跨境收集电子证据的改进：来自专家的意见及具体的建议》中也特别指出，对于单边跨境电子数据取证，未来的立法应当专门规定诸如应告知可能受影响的国家在内的缓解措施。[②]

由此可见，对于绕开常规刑事司法协助程序的跨境电子数据取证，国际上要么是通过区域性公约设置了特殊通道，要么是由一些国家通过国内法进行了谨慎的授权，从而导致数据存储地模式的确出现了松动。然而，无论是现有的国际公约还是国内法条款，均对单边跨境电子数据取证设置了诸多严格的限制。这充分说明，数据存储地模式的根基并未动摇，仍然是国际上刑事取证管辖制度运行的基础准则。

## 第二节　依托跨境云服务提供者的数据控制者模式

### 一、数据控制者模式概说

所谓数据控制者模式，在刑事侦查中是指在云计算的技术背景下，通过寻求跨境云服务提供者的合作或对其发出指令的方式获取其所控制的数据。关于这一刑事取证管辖模式，可以从以下方面加以理解：其一，不仅将云数据与其他有形实物相区分，而且将云数据所在的虚拟空间与有形实物所处的物理空间相区隔，在云数据的刑事取证管辖方面完全不考虑数据存储的位置，从而绕避常规的司法协助程序。其二，依托跨境云服务提供者，属于对存储于境外的数据的一种间接取证方式。其三，数据范围只涉及跨境云服务提供者控制的数据，具体而言即其

① See Anna-Maria Osula, Mark Zoetekouw,“The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives”, *Masaryk University Journal of Law and Technology,* 11:1(2017), 107.

② “Improving cross-border access to electronic evidence: Findings from the expert process and suggested way”,https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf, 最后访问日期：2018 年 9 月 15 日。

“拥有”（possession）、“保管”（custody）或“掌控”（control）的数据。[①]

通过数据控制者模式获取位于境外的数据，近年来逐渐受到一些国家的重视，并且在国际上已经展现出两种基本的表现形式。

一是通过在本地无实体机构的外籍网络服务提供者披露境外数据。例如在比利时的一起案件中（下文简称“比利时雅虎案”），嫌疑人通过雅虎的电子邮件账户针对比利时境内的目标实施了欺诈犯罪。在侦查阶段，比利时的检察官根据该国《刑事诉讼法》第“46bis § 2”条的规定[②]直接向雅虎公司在美国的办公室发出指令，要求后者披露注册用户的信息及用户的 IP 地址。然而，雅虎是在美国加利福尼亚注册的公司，在比利时并无分支机构，其拒绝向比利时执法部门披露上述数据，并认为后者是在向境外扩大适用刑事管辖权。为此，雅虎公司告知比利时的检察官，应当通过常规的双边司法协助机制，请求美国当局协助执行。不过，比利时检察官并未采取这样的方案，而是依据上述《刑事诉讼法》规定对雅虎公司提出了检控。雅虎公司在庭审中除了继续主张该案应当通过司法协助机制开展相应证据调查工作而外，也提出自身并不属于比利时境内的“电子通信的网络服务提供者”（provider of electronic communications services），因此不受比利时当局的管辖。

此案的几次审理颇为引人注目。2009 年 3 月 2 日，雅虎公司在登德尔蒙德（Dendermonde）刑事法院败诉，但是在根特（Ghent）上诉法院胜诉。经过几轮复杂的诉讼程序，比利时安特卫普上诉法院于 2013 年 11 月裁决，雅虎公司应当披露上述涉案数据。法院的理由在于，该公司通过在比利时境内提供电子通信服务，通过使用“www.yahoo.be”域名而参与到比利时的经济活动中，在该网站使用当地的语言，且网站上的弹出式广告可连接至比利时境内的商户和用户服务提供商。因此，该公司“事实上是位于”（virtually located）比利时的。于是，法院判决雅虎公司败诉。随后，雅虎公司向比利时最高法院提出上诉。2015 年 12 月 1 日，比利时最高法院拒绝了雅虎公司的上诉请求，并以未尽执法配合义务为

① “拥有、保管、控制”是《云法案》“SEC2(2)”部分所使用的术语，可见对该法所反映的数据控制者模式中的“控制”应作宽泛理解。

② 比利时《刑事诉讼法》第“46bis § 2”条规定，当执法机关要求披露用户身份信息时，电子通信网络服务提供者必须提供。

由对其罚款 44000 欧元。如果雅虎公司拒绝接受判决，则比利时最高法院会考虑将其 IP 从比利时境内移除。[①]

二是通过在本地有实体机构的外籍网络服务提供者披露境外数据。例如，2014 年 4 月 23 日施行的《巴西境内使用网络之原则、担保、权利与义务的确立》（Estabelecimento de princípios, garantias, direitos e deveres para o uso da Internet no Brasil）第 11 条第 2 段规定，只要网络服务提供者向巴西公众提供服务，即使其在国外运营，也受到该法调整。2015 年 1 月，微软分支机构受美国《存储通信记录法》约束而未按巴西一家法院的指令披露其存储于境外的嫌疑人的信息，为此被巴西当局罚款数百万美元，而且员工还遭到刑事起诉（下文简称“巴西微软案”）。[②] 此外，根据英国 2016 年施行的《调查权法》（*Investigatory Powers Act*）第 85 条即“跨境适用”（Extra-territorial application）及第 3 部分“获取通信数据的授权”（AUTHORISATIONS FOR OBTAINING COMMUNICATIONS DATA）的相关规定，执法部门可以向其境内运营的电讯网络服务提供者发送指令，以此获取其存储于境外的数据。英国政府曾对《调查权法》的前身即《数据留存与调查权法》（*Data Retention and Investigatory Powers Act*，DRIPA）草案[③] 解释道，对于“在英国为客户提供通信服务的所有运营者而言，无论其服务是从何处提供的，都应当遵守数据披露的要求。”[④] 而华盛顿大学法学院 Jennifer Daskal 女士所援引的英国官方的解读则更为具体：其主要目的就是要授权获取采用其他方法难以收集的位于美国的网络服务提供者掌控的数据。[⑤]

不过，比利时、巴西、英国的立法或实践更多的只是对数据控制者模式的问世进行了初步的探索。这一模式系统理论的提出更多地是受到了“微软爱尔兰案”

---

① Belgium Supreme Court, September 4th, 2012, A.R. P.11.1906.N/2.

② See Brad Smith，“In the Cloud We Trust”，http://news.microsoft.com/stories/inthecloudwetrust，最后访问日期：2018 年 6 月 11 日。

③ 该草案于 2016 年 12 月 31 日被废弃，在立法程序中被《调查权法》所取代。

④ UK Government, “Data Retention and Investigatory Powers Act 2014”, https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014，最后访问日期：2018 年 6 月 11 日。

⑤ Jennifer Daskal,“ Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues”,*National Security Law & Policy,* 8(2016), 473.

的影响，并最终在美国《云法案》于 2018 年出台之后正式成型。[①] 该法第 1 节开宗明义地指出，其立法目的就在于授权美国执法部门在云计算的背景下通过网络服务提供者获取境外数据。该法标志着美国在云数据的跨境刑事取证管辖方面，从数据存储地模式彻底转向了数据控制者模式。

## 二、数据控制者模式与数据存储地模式的相互关系

前文对数据控制者模式与数据存在地模式分别进行了介绍，但是要注意的是，两者并不是完全无关的取证模式，而是有着密切的内在关联。这可以从以下三个方面进行解读。

其一，数据存储地模式面临的困境客观上为数据控制者模式的问世提供了可能性。如果数据存储地模式本身运行良好，各国自然无需采取新的模式来执行电子数据的跨境取证。然而在数据存储地模式本身面临困境且出现松动的情况下，跨境电子数据取证的实际需求并未缩减，而且还随着网络犯罪全球化特征的越发显著而逐渐增加。特别是对于那些对境外云数据有较大掌控需求的国家而言，在数据存储地模式的现有特殊例外情形之外寻求新的取证管辖模式，从而尽可能地消解数据存储地模式的困境，便成了契合时代变迁背景的必然选择。以美国为例，正如本书第三章将要详细分析的那样，在传统的刑事司法协助机制与跨境远程收集电子数据之单边方案均存在明显缺陷的背景下，通过网络服务提供者获取境外云数据已经成为其近年来最为突出的战略选项。从 2016 年开始，该国便一直在试图通过立法的方式推进相关工作，[②] 而《云法案》的出台也确实有助于缓解数据存储地模式面临的困境。

其二，数据控制者模式的适用限制意味着其只是对数据存储地模式实现了部分取代。数据控制者模式完全不考虑传统的国家疆界的限制，因此从性质上讲并不属于数据存储地模式的特殊例外，两者的适用必然呈现出冲突状态。尽管如此，数据控制者模式与数据存储地模式实际上也并不是截然对立的，不能简单地认为

① 参见洪延青：《美国快速通过 CLOUD 法案 明确数据主权战略》，载《中国信息安全》，2018（4）；许可：《数据主权视野中的 CLOUD 法案》，载《中国信息安全》，2018（4）。

② 参见梁坤：《〈美国澄清合法使用境外数据法〉背景阐释》，载《国家检察官学院学报》，2018（5）。

前者完全取代了后者。上文已经说明，数据控制者模式依托于跨境云服务提供者，瞄准的只是其所控制的境外数据。由此观之，数据控制者模式在国家刑事取证管辖实践中的适用并不具有普适性，实际上只是对数据存储地模式进行了部分取代。在此情况下，两种模式甚至还可以构成一定的互补关系。

一方面，数据存储地模式所反映的传统双边或多边框架下的电子取证程序冗长复杂，一定程度上需要数据控制者模式所代表的快捷电子取证方案加以补充。如果数据控制者模式未来为越来越多的国家接纳并且运行顺畅，各国的主管机关就可以在很大程度上腾出精力在传统的双边和多边框架下处理其他更为紧要的刑事司法协助事项，从而减轻协助程序的负担。例如，美国之所以出台《云法案》，就有这方面的考虑。[①] 另一方面，尽管数据控制者模式已经在全球范围内成为跨境电子取证制度革新的焦点，但是跨境电子取证只能适用于网络服务提供者所掌控的位于全球各地服务器中存储的数据，因此需要数据存储地模式对于其他类型的数据的跨境取证继续发挥作用。这就意味着，对于网络空间中与这类网络服务提供者完全无涉的数据而言，数据存储地模式仍然是当今乃至未来很长一段时间内刑事取证管辖的基本方案，仍然会在跨境电子数据取证的实践中扮演极其重要的角色。

其三，两种模式将会在一定时期内以相互博弈的方式共同存在。如同本章接下来的内容将要着重分析的那样，各国对于境内及境外数据资源存在差异性极大的利益诉求。就单个国家而言，其很可能基于数据安全等核心国家利益而采取数据存储地模式来保护境内数据的同时，又会青睐于数据控制者模式的优势而力图长臂掌控境外数据。而从国际层面来看，数据掌控能力较弱的国家可能较为倾向甚至单一地选择坚守数据存储地模式，而一些数据强国则会倾向于同时采取两种模式，抑或侧重于采取数据控制者模式。换言之，数据控制者模式在部分取代数据存储地模式之后，两种模式的共存将会成为一定时期内的必然现象，相互之间的博弈以及此消彼长也将成为常态，这是各国在运行刑事取证管辖制度时必须面临的全新课题。

---

① See Department of Justice Office of Public Affairs, “Justice Department Announces Publication of White Paper on the CLOUD Act”, p.5, https://www.justice.gov/opa/press-release/file/1153446/download，最后访问日期：2021 年 12 月 31 日。

## 三、数据控制者模式在全球层面对刑事取证管辖制度的影响

### （一）导致国家间刑事取证管辖的范围出现重叠并诱发国际法冲突

根据数据存储地模式，由于对数据的刑事取证管辖受限于国家主权行使的地域范围，因此除非属于上文提到的模式松动的特例，在常规情况下并不可能产生国家间的管辖权冲突。然而，在数据控制者模式部分取代数据存储地模式之后，主张前一模式的国家便很可能经由网络空间，在个案中将刑事取证管辖的范围延伸自主张后一模式的国家的地域，这必然会导致不同国家在取证管辖范围上的重叠，从而不可避免地诱发国际法上的冲突。

实际上，这种冲突已经在“微软爱尔兰案”所反映出来的美国和爱尔兰的官方对立主张中表现得淋漓尽致。而在 2019 年于维也纳举行的“联合国网络犯罪政府专家组第五次会议”上，各国也对是否应允许一国绕过另一主权国家直接向互联网企业跨国调取电子数据展现出了较大的分歧。例如，以美国、英国、智利等《布达佩斯公约》缔约国为代表的一些国家表示，国际司法协助和执法合作等传统取证渠道效率低下，难以适应调取电子数据的需求，主张淡化国家对证据的管辖权，应授权执法机关直接向互联网企业调取存储在他国的电子数据。俄罗斯、南非、伊朗等国则强调，跨国调取电子数据应尊重证据所在国主权，保障相关主体和个人的权利。[①] 这实际上就反映出各国在数据控制者模式问世之后，对国家层面的刑事管辖权的两种截然不同的认识。

### （二）深刻改变国际上刑事取证管辖的实际运行结构

虽然数据控制者模式只是部分取代了数据存储地模式，而且上文还用了“此消彼长”一词来描绘两者的可能关系，但是理性分析未来发展趋势，笔者认为更大的可能性在于，数据控制者模式在国际范围内大概率会逐渐压缩数据存储地模式的适用空间。这主要有两方面的原因。

其一，数据控制者模式瞄准了全球云市场的蓬勃发展趋势，有着广阔的发展

① 翟晓飞、赵倩：《从国际视角看中国网络犯罪取证规则的发展》，载《中国信息安全》，2019（5）。

前景。如今，无论是个人还是公司，都越来越多地选择将生活数据、商业数据等上传至“云”中，而并不像过往那样更多的只是进行本地存储。美国思科公司在2015年11月的时候预测，到2019年就会有55%的居民区网络用户使用云存储服务，而高达86%的工作数据都将存储于云中。[①] 美国Gartner公司于2018年9月发布的数据显示，2018年全球云服务市场规模已达1758亿美元；其当时预测，到2022年这一市场规模还将增长至2062亿美元。[②] 通过这些数据足以看出，全球云数据市场在近年来经历了飞速发展，从中也表明云服务提供者对数据的掌握力度变得越来越大。

在此背景下，正如“微软爱尔兰案”那样，一份电子邮件所涉及的内容数据和非内容数据存储于不同国家的情况将在个案中越来越多地出现。应当认识到的是，数据控制者模式相较数据存储地模式的确有其优势，有助于破除个案中数据跨境分散存储而难以通过常规法律程序快捷获取的难题。

其二，数据控制者模式也因美国的技术优势和全球影响力，在刑事取证管辖方面将逐渐显现其重要性。原因在于，以GAFA（谷歌、苹果、脸书和亚马逊）为代表的美国IT巨头在全球云数据市场占据着统治性的份额，其所控制的海量的境外云数据随着《云法案》的出台都将潜在地纳入到美国刑事取证管辖的范围。而从近期来看，正如后文还将展开说明的那样，一些国家和地区已经准备效仿该法的做法或接受该法授权的双边“互惠”机制，从而使数据控制者模式在全球范围内实际发挥的效用越发增大。因此，如果以美国为代表的国家在数据控制者模式的运行方面得到持续纵深发展，那么数据存储地模式的适用空间必然会受到压制，从而令国际层面刑事取证管辖的实际运行结构出现显著转向。

---

① see Cisco,“Cisco Global Cloud Index 2014 － 2019”, https://www.cisco.com/c/dam/m/en_us/service-provider/ciscoknowledgenetwork/files/547_11_10-15-DocumentsCisco_GCI_Deck_2014-2019_for_CKN__10NOV2015_.pdf, 最后访问日期：2018年11月1日。

② “See Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019”, https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019. 最后访问日期：2019年12月15日。

## 第三节　跨境电子取证管辖模式变革的影响因素

数据控制者模式的问世以及对数据存储地模式的部分取代，反映出刑事取证管辖模式在国际层面出现了重大变革。通过深入的比较分析和理论考究可以发现，这一变革主要受到了两大方面的因素的影响。在这其中，各国立足自身国家利益的最大化而对数据资源的掌控居于核心地位；“数据特例主义”理论的提出也对适用于有形实物的传统管辖模式构成了冲击，同样不容忽视。

### 一、各国立足自身国家利益的最大化对数据资源的掌控

“数据是新的石油，是本世纪最为珍贵的财产；谁掌握了数据，谁就掌握了主动权。”[①] 数据作为一种新兴资源的巨大价值早已获得国际认可，许多国家近年来由此越发重视对数据资源的掌控，以此实现国家利益的最大化。“在数字侦查语境下，利益关系复杂化，数据本身牵涉国家关键基础资源的争夺，例如，数据安全、网络安全、个人信息保护、网络产业发展等。”[②] 从现实来看，不同的国家在数据资源的现实掌控能力方面存在巨大的差异。从近期一些国家强化其执法机关与其他法域网络服务商直接合作的取证模式来看，这势必会给互联网领域专业技术欠缺或处于弱势的发展中国家造成巨大压力，处于互联网发展初期阶段的国家或者国内网络服务提供者发展尚不具规模的国家在此种国际合作模式下将逐渐“被边缘化”并最终可能失去对数据的掌控权。[③] 因此，各国在国家数据主权、国家数据安全及数据权利保护等方面的国家战略及法律制度层面展现出了显著的差异，由此对国际上刑事取证管辖模式的变革产生了重要的影响。下面相应地从三个方面进行论证。

---

① 新华社评论员：《用好大数据，布局新时代——学习习总书记在中央政治局第二次集体学习时重要讲话》，载《新华每日电讯》，2017 年 12 月 11 日，第 1 版。

② 裴炜：《未来犯罪治理的关键——跨境数据取证》，载《中国信息安全》，2019（5）。

③ 方芳：《坚持在联合国框架下制定电子证据国际标准——联合国毒品犯罪办公室第五届网络犯罪政府间专家组会议研究》，载《信息安全与通信保密》，2019（5）。

### （一）国家数据主权

刑事取证管辖乃是国家主权的重要体现。由于网络空间中刑事取证管辖的对象是数据，国家对网络空间主权或数据主权的基本立场便成了具体管辖模式塑造及变革的基础。2011 年 10 月 10 日，方滨兴院士在北京“第一届网络空间国际化学术讨论会暨互联网治理与法律论坛”上，就较早地提出了“网络空间主权”的理念。[①] 这一理念此后逐渐为我国学者所接受，并且成为我国官方的主张。从此后的多份法律和文件中的表述来看，对网络空间主权或数据主权均有强调，但前者出现的频次更多。

在法律层面，2015 年施行的《中华人民共和国国家安全法》第 25 条规定：“国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。”据此，我国法律层面第一次出现了“网络空间主权”的表述。2017 年施行的《中华人民共和国网络安全法》（以下简称《网络安全法》）第 1 条则指出，该法的立法目的之一就在于“维护网络空间主权和国家安全”。[②]

除了上述法律明确规定了“网络空间主权”外，中共中央办公厅、国务院办公厅于 2016 年 7 月联合发布的《国家信息化发展战略纲要》指出：

> 树立正确的网络安全观，坚持积极防御、有效应对，增强网络安全防御能力和威慑能力，切实维护国家网络空间主权、安全、发展利益。维护网络主权和国家安全。依法管理我国主权范围内的网络活动，坚定捍卫我国网络主权。坚决防范和打击通过网络分裂国家、煽动叛乱、颠覆政权、破坏统一、窃密泄密等行为。

国家互联网信息办公室在 2016 年 12 月发布的《国家网络空间安全战略》也

① 参见方滨兴主编：《论网络空间主权》，前言部分“vi”页，北京，科学出版社，2017。

② 该条规定：“为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。”

明确指出，网络空间属于“国家主权的新领域”：

网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，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。尊重网络空间主权，维护网络安全，谋求共治，实现共赢，正在成为国际社会共识。

网络空间主权不容侵犯，尊重各国自主选择发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。各国主权范围内的网络事务由各国人民自己做主，各国有权根据本国国情，借鉴国际经验，制定有关网络空间的法律法规，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏，保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序。任何国家都不搞网络霸权、不搞双重标准，不利用网络干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。

此外，外交部和国家互联网信息办公室于 2017 年 3 月联合发布的《网络空间国际合作战略》在第三章“战略目标”的“维护主权和安全”部分也对“网络空间主权”进行了明确表述：

网络空间国防力量建设是中国国防和军队现代化建设的重要内容，遵循一贯的积极防御军事战略方针。中国将发挥军队在维护国家网络空间主权、安全和发展利益中的重要作用，加快网络空间力量建设，提高网络空间态势感知、网络防御、支援国家网络空间行动和参与国际合作的能力，遏控网络空间重大危机，保障国家网络安全，维护国家安全和社会稳定。

由于数据本身依托而不能脱离于网络空间，因此既然主张网络空间主权，数据主权就理所当然地应该成立，从而可以将其定位于网络空间主权的下位概念：

网络空间主权针对的是网络空间中的一切设施、数据及其相关活动，而数据

主权针对的客体是数据，是网络空间的一个要素。数据主权从广义上来看是将数据作为一个领域，从狭义上来看是将数据作为一种事物。数据主权所涉及的数据实际上涵盖所有信息种类，包括结构化、半结构化和非结构化的数据，几乎包括任意行为体产生的任意信息或日常行为记录。很显然，网络空间主权与数据主权属于包含关系，数据主权是网络空间主权的一个子集。[①]

我国除了主张网络空间主权外，也是数据主权的坚定主张者和支持者。2015年8月31日，国务院在其发布的《促进大数据发展行动纲要》中首次从官方层面对“数据主权”进行了表述：“充分利用我国的数据规模优势……增强网络空间数据主权保护能力，维护国家安全，有效提升国家竞争力。”

由于网络空间主权系国家主权在网络空间的延伸，因此数据主权也成为国家主权不可或缺的组成部分。尽管如此，我国所主张的数据主权仍然面临着理论和现实层面的如下困境。

一方面，数据主权在理论上并未形成一致意见，尚存在着不小的争议。有研究者认为，当前对数据主权的界定主要是从三个角度入手：第一个角度是根据国家主权的相关概念，对数据主权作出界定。第二个角度是从数据主权的内容入手，对数据主权作出界定。第三个角度是从数据主权的权责内涵进行分析而作出的界定。由于角度不同，国内外学者对数据主权的主张和界定自然差异极大，尚未出现压倒性的通说。即使只从国内学界来看，相关的争议也不绝于耳，甚至就数据主权是否成立也还有不同的声音。例如，赞成数据主权提法的观点中，有人从数据主权与国家主权的关系上分析，认为数据主权是国家主权的一部分，对网络空间中数据的保护和利用是涉及国家主权及利益的一项重要内容。有人从数据主权的来源思考，认为数据主权是伴随云计算和大数据技术的发展而来的，涉及数据的生成、收集、分析、应用等各个环节，大数据的爆发式增长很可能对国家安全和个人隐私带来潜在的危害，因此必须明确数据主权并构建相关法律制度；有人从国际视野出发，指出中国需要以“数据主权”核心诉求，推动建立“共享共治、自有安全”的全球网络新秩序。不赞成数据主权提法的观点，主要是认为

① 方滨兴主编：《论网络空间主权》，323页，北京，科学出版社，2017。

单纯强调数据主权可能会导致国与国之间形成对抗状态，不利于数字经济的发展，因此主张弱化数据主权概念，提出保障数据安全的核心是提升数据掌控和分析能力。[①]

另一方面，数据主权尚未在国际范围内得到普遍认同。例如，由“北约卓越合作网络防御中心”（CCDCOE）组织的包括中国学者在内的专家组编写的《网络空间国际法示范规则》即《塔林手册 2.0》尽管认可我国所主张的网络空间主权，但从具体内容来看只涉及 3 个层次：物理层包括物理网络组成部分，即硬件和其他基础设施，如电缆、路由器、服务器和计算机；逻辑层由网络设备之间存在的连接关系构成，包括保障数据在物理层进行交换的应用、数据和协议；社会层包括参与网络活动的个人和团体。[②] 换言之，《塔林手册 2.0》并未涉及国家对特定数据本身行使的主权。[③]

更为复杂的问题在于，尽管以中国为代表的大多数发展中国家为了抵制网络霸权对网络空间的戕害而主张网络空间主权，[④] 而且主权平等原则适用于网络空间，[⑤] 但以美英为代表的许多西方发达国家则对此予以反对。以美国为例，2018 年 9 月发布的《国家网络战略》只字不提网络空间主权，而是再次强调了其在近

---

① 张莉主编：《数据治理与数据安全》，130 ～ 132 页，北京，中国工信出版集团、人民邮电出版社，2019。

② [ 美 ] 迈克尔 • 施密特总主编：《网络行动国际法塔林手册 2.0 版》，黄志雄等译，58 页，北京，社会科学文献出版社，2017。

③ 黄志雄：《网络空间国际规则制定的新趋向——基于〈塔林手册 2.0〉的考察》，载《厦门大学学报》（社会科学版），2018（1）。

④ 参见张新宝、许可：《网络空间主权的治理模式及其制度构建》，载《中国社会科学》，2016（8）。

⑤ 外交部和国家互联网信息办公室于 2017 年 3 月 1 日发布的《网络空间国际战略》第三章“基本原则”的第二部分“主权原则”明确主张：“《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，覆盖国与国交往的各个领域，也应该适用于网络空间。国家间应该相互尊重自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。明确网络空间的主权，既能体现各国政府依法管理网络空间的责任和权利，也有助于推动各国构建政府、企业和社会团体之间良性互动的平台，为信息技术的发展以及国际交流与合作营造健康的生态环境。各国政府有权依法管网，对本国境内信息通讯基础设施和资源、信息通讯活动拥有管辖权，有权保护本国信息系统和信息资源免受威胁、干扰、攻击和破坏，保障公民在网络空间的合法权益。各国政府有权制定本国互联网公共政策和法律法规，不受任何外来干预。各国在根据主权平等原则行使自身权利的同时，也需履行相应的义务。各国不得利用信息通讯技术干涉别国内政，不得利用自身优势损害别国信息通信技术产品和服务供应链安全。”

年来所力推的互联网治理的“多利益攸关方模式”。[①] 由于这些国家并不支持网络空间主权，因此更谈不上赞成我国所主张的作为网络空间主权之下位概念的数据主权。

在对网络空间主权的认识存在明显分歧且数据主权是否成立、是否包含于网络空间主权尚未达成国际共识的背景下，不同国家基于自身利益必然会对网络空间中存储、流动的数据展开激烈的争夺。这种争夺对刑事取证管辖模式的变革产生了显而易见的影响。“在传统域外刑事取证过程中，由于目标证据材料的相对明确并显著区别于非涉案财物，对国家主权以及国家或公共利益的判断或评价相对容易。但是，在网络信息社会中，占有数据本身即可形成利益，大数据分析等技术进一步使这种占有与数据类型脱钩。从这个意义上讲，传统管辖权是划界之后的消极防守，现在则转化为各国的全面进攻，使以往偶然发生的管辖权冲突变得频繁和主动。”[②]

具体到不同的国家而言，主张网络空间主权特别是数据主权的国家必然会强调对网络空间中特定数据的保护和管控。特别是对于存储于其境内的数据而言，坚持数据存储地模式从而排他性地抗衡其他国家的争夺，显然更符合其国家利益。然而与此相对的是，反对数据主权的国家则更希望松动、突破数据存储地模式的僵硬枷锁，从而在云计算的时代背景下凭借其技术优势实现对存储于他国境内的数据的长臂掌控。就此而论，数据控制者模式的应运而生与网络空间主权或数据主权的国际争议不无关系。

### （二）国家数据安全

基于国家数据安全而强有力地保护数据，这对网络技术及在跨境通信、云计算市场处于弱势的国家尤其重要。如今，跨境云服务提供者所控制的大数据不仅涉及大范围的用户隐私，甚至还关系到一国的国计民生，从而潜在影响国家数据安全和稳定。于是，通过法律强制要求网络服务提供者对境内所收集及服务供给

① “see National Cyber Strategy of the United States of America”, p.25, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 最后访问日期：2018 年 11 月 15 日。

② 参见裴炜：《未来犯罪治理的关键——跨境数据取证》，载《中国信息安全》，2019（5）。

过程中产生的数据进行本地化存储也即“数据本地化”（data localization）[①]，已经成为许多发展中国家对抗数据强国试图依托这类网络服务提供者实现数据霸权的重要选择。特别是在美国“棱镜门”计划曝光之后，数据本地化存储法律制度更是得到了越来越多国家特别是发展中国家的重视。2017 年的一份研究报告显示，全球范围内已经有包括中国在内的 36 个国家和地区通过立法等方式对数据本地化存储进行了明确要求，但形式并不相同。例如，全球互联网治理委员会（Global Commission on Internet Governance）在其 2015 年的发布报告《数据本地化规则对金融服务的影响》（*Addressing the Impact of Data Location Regulation in Financial Services*）中，将数据本地化概括为四种类型：一是数据出境的地域限制，即要求数据必须于某一国家或区域境内存储和处理；[②] 二是数据位置的地域限制，即允许数据副本出境处理，但在本国或本区域内必须存有副本；三是基于许可制的数据出境限制，即要求数据出境需经主管当局许可；四是基于标准体系的数据出境限制，即要求数据出境必须采取标准化的步骤以确保数据安全和隐私保护。其中，前两种类型会直接限制数据跨境流动，是当前世界数据本地化立法的主要类型。[③]

也有学者比较了多个国家的数据本地化措施，从不同的宽严程度出发，将其进行了类型化归纳：（1）仅要求在当地有数据备份，而并不对跨境提供作出过多限制；（2）数据留存在当地，且对跨境提供有限制；（3）要求特定类型的数

① 有学者认为，“数据本地化”是指出于本国公民隐私保护、国家数据安全或执法便利等目的，在国家内部收集、处理和存储有关公民或居民的数据。参见王融：《数据跨境流动政策认知与建议——从美欧政策比较及反思视角》，载《信息安全与通信保密》，2017（2）。从一国作为对抗他国跨境取证方案的“数据本地化”而言，主要强调的是数据的本土化存储，本书也主要是从这个层面来探讨“数据本地化”的。当然，本书分析的本地化存储的数据也并不限于公民或居民的数据，而是包括一切数据。

② 例如，俄罗斯于 2014 年 5 月通过的《〈关于信息、信息技术和信息保护法修改案〉及个别互联网信息交流规范的修正案》，在“互联网信息传播组织者的义务”中增加了数据境内留存的要求，规定“自网民接受、传递、发送和（或）处理语音信息、书面文字、图像、声音或者其他电子信息 6 个月内，互联网信息传播组织者必须在俄罗斯境内对上述信息及网民个人信息进行保存。参见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）》，第 408 页，北京，中国法制出版社，2015。

③ 参见裴炜：《全球互联背景下数据要地化发展趋势与展望》，载《中国信息安全》，2021（5）。

据留存在境内；（4）数据留存在境内的自有设施上，等等。[①]

还有学者同样将宽严程度作为划分标准，从不同的角度，对数据本地化进行了不同类型的划分：（1）最严格的数据本地化形态为“完全禁止本国数据出境”。也就是说，本国的数据必须保存在本国境内的存储设备上，他国跨国公民要想进入本国市场，就必须在本国境内建立数据中心以存储本国公民数据，例如印度的数据本地化便呈现出这种样态。（2）稍微宽松一些的是俄罗斯、澳大利亚等国家采取的策略——“禁止本国特定数据出境。”（3）欧盟和韩国的数据本地化措施更为开放，只要数据满足了法律规定的条件，就可以自由出境。（4）“境内数据中心备份出境”当属最宽松的数据本地化形态。[②]

基于数据安全而保护数据的另一个表现在于对数据的跨境流动或披露进行法律规制。这实际上属于上述《数据本地化规则对金融服务的影响》报告中的第三种类型，属于一种特殊的数据本地化举措。这一方案近年来也得到了许多国家的青睐，并形成了以俄罗斯、澳大利亚为代表的刚性禁止流动模式，以欧盟、韩国为代表的柔性禁止流动模式以及以印度、印尼为代表的本地备份流动模式。[③]

综上，无论是对数据进行本地化存储还是对数据的跨境流动或披露进行法律规制，实际上都反映了不同国家基于数据安全而进行的战略选择。以数据本地化制度为例，虽然部分发达国家的数据保护立法中也有相应的规定，但是综合来看，这类立法在发展中国家更为多见。有学者提出，“整体上，发达国家反对宽泛的数据本地化要求，而发展中国家则更多地倾向于宽泛的数据本地化。发展中国家的数据本地化要求多出于国家安全、网络安全、数据安全，以及监管执法、国家战略、地缘政治等宽泛性考量，而发达国家的相关规则目的往往更加具体，多是对特殊数据、敏感数据的强化保护，以保护公民基本权利和尊严。”[④] 也有学者

① 参见王融：《数据跨境流动政策认知与建议——从美欧政策比较及反思视角》，载《信息安全与通信保密》，2017（2）。

② 张莉主编：《数据治理与数据安全》，138～139页，北京，中国工信出版集团、人民邮电出版社，2019。

③ 参见吴沈括：《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（5）。

④ 龙卫球主编：《〈中华人民共和国数据安全法〉释义》，35页，北京，中国法制出版社，2021。

类似地提出，“从各国的数据立法来看，严格追求数据本地化政策的国家大多是互联网和数据技术不发达的国家，数据本地化政策是一种防守性政策，可以作为这些国家与其他国家和互联网公司谈判的筹码。”①

从便利刑事取证管辖的执行及维护数据安全从而实现这些国家的利益最大化的角度而言，数据存储地模式有着显著优势。一方面，从法律层面要求对数据本地化存储，显然有助于有效服务本国的刑事侦查，电子取证活动无需再经历司法协助的复杂程序并受制于他国的取证标准；另一方面，限制或禁止数据跨境流动或披露，致使其他国家无法在侦查中便捷地通过单边渠道收集数据，这对于数据安全的维护具有重要的意义，而且实际上也有利于本国刑事侦查中电子取证的顺利开展。

反对数据本地化存储并主张数据跨境自由流动，则更符合在云数据市场占绝对优势且试图推行数据霸权的国家的利益。原因在于，严格的数据本地化政策确实不利于全球层面云计算和大数据的产业发展，这是必须要正视的。于是，在 A 国实行数据本地化制度后，B 国网络服务提供者在 A 国从事数据业务时就必须以自建服务器或本地托管的方式满足后者的法律要求。这必然导致 B 国的网络服务提供者大大增加在境外的成本投入，削弱其在云计算方面的技术优势。② 2018 年 9 月，由时任美国总统签署发布的《美利坚合众国国家网络战略》便指出：“数据本地化规则对美国企业的竞争力产生了负面影响，美国将继续抵制阻碍数据和数字贸易自由流动的壁垒，促进全球数据自由流动。”③ 美国作为数据产业的第一大国，显然不愿意看到这样的局面持续下去。

由此可见，美国反对其他国家对数据的本地化存储并主张数据跨境自由流动，很大程度上就是要通过维护其跨国企业利益的方式实现其国家网络战略。而要达

① 翟志勇：《数据主权的兴起及其双重属性》，载《中国法律评论》，2018（6）。

② 许多发达国家开展跨境云计算业务的网络服务提供者往往也反对“数据本地化”。一个不容忽视的原因在于，“不断扩大本地化存储对象的范围，加之严格限制相关数据外流，必将导致电子数据的‘孤岛化’现象，会对数字经济发展产生不利影响。”参见冯俊伟：《跨境电子取证制度的发展与反思》，载《法学杂志》，2019（6）。

③ see “National Cyber Strategy of the United States of America”, p.25, https://www.dni.gov/files/NCSC/documents/supplychain/20190328-National-Cyber-Strategy-Sep2018.pdf, 最后访问日期： 2022 年 1 月 19 日。

到这一目标，美国必然会选择弱化其他国家对数据的保护力度，令后者的数据安全保障大打折扣。从刑事取证管辖的角度而言，数据强国所力主推行的全新的数据控制者模式，从根本上讲也就可以视为对其他国家在数据本地化存储、跨境数据流动管制的背景下维护数据安全并坚守数据存储地模式的战略回击。

### （三）数据权利保护

对与数据相关的特定法律权利进行保护，以此提升国家对数据的掌控能力，也会对跨境电子取证管辖模式的塑造产生重要的影响。除了下文还将分析的美国《储存通信记录法》（SCA）对本地存储的通信内容数据进行强有力的保护外，历来强调个人隐私保护的欧盟近期的改革动向也非常值得关注。

2018 年 5 月 25 日，被称为“史上最严”的《通用数据保护条例》（GDPR）施行，欧盟于是从整体层面强化了对个人数据的保护。在这其中，第 48 条专门规定了“未经欧盟法授权的转移或披露”——任何法庭判决、仲裁裁决或第三国行政机构的决定若要求控制者或处理者对个人数据进行转移或披露，应同时满足以下条件时方能得到认可或执行：一是该判决、裁决或决定必须基于提出请求的第三国与欧盟或其成员国之间订立的法律互助协议等国际条约；二是该判决、裁决或决定不会对本章规定的其他转移形式产生消极影响。根据该规定，如果外国执法机构单方采取数据控制者模式而欲通过网络服务提供者转移或披露存储于欧盟成员国境内的数据，在不满足上述两个条件的情况下便与《通用数据保护条例》相冲突。从这个角度而言，这一条文可以视为欧盟选择了数据存储地模式来强化个人数据保护，从而强有力地提升了成员国对存储于其境内的数据的掌控能力，这对维护成员国的整体数据利益而言显然具有重要的意义。

但从另一角度来看，《通用数据保护条例》在强化个人数据保护方面也出现了跨境适用。[①] 根据其中第 3 条“地域范围”之规定，《通用数据保护条例》“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在欧盟境内设立机构”。具体而言，《通用数据保护条例》中“数据管辖权的扩张主要是通过弱化数据所在地对于管辖范围的限制，以动态的数据管理和处理行为为管辖权

① 参见何波：《数据是否也有主权——从微软案说起》，载《中国电信业》，2018（8）。

核心关注点，从而使欧盟在个人信息保护方面的管辖权不仅大幅扩张，并且为主管机关建构起较大的自由裁量空间。”[①]

正如本书第四章将要展开细致分析的那样，欧盟在美国《云法案》施行的背景下已计划出台“欧洲数据提交令”（European Production Order）制度，在电子数据取证方面并不考虑相应数据到底是否存储于欧盟的地域范围内。由于欧盟强调这一改革提议所涉及的个人数据受到《通知数据保护条例》的保护，[②] 这实际上就是通过强化个人数据保护的方式，实质性地实现成员国对境外数据的现实掌控能力。如果“欧洲数据提交令”制度未来能够落地，欧盟必将在刑事取证管辖方面对数据存储地模式施以实质性的变革。这样一来，欧盟的改革方案一方面对内强化了数据存储地模式，而对外则计划推行数据控制者模式，这样的变革实际上都反映了欧盟及其成员国在数字化时代尽最大可能维护其自身数据利益而开展的努力。

在此背景下，由于数据控制者模式强化了一些国家通过网络服务提供者对外掌控其他国家境内存储之数据的能力，这必然导致与数据本身直接相关的某些权利的保护受到直接威胁。除了国家层面的主权与安全因素而外，相关威胁主要表现为两个方面。

第一，给网络服务提供者带来合规困境。鉴于全球范围内对网络犯罪的定义和范围尚无统一界定，加之各国在跨境取证程序方面的单边性立法及部分多边条约的复杂性，当他国执法或司法机关向另一国的网络服务提供者发布跨境电子取证的披露指令时，后者在大量案件中便会面临难以预测的合规困境。原因在于，如果单方面接受他国执法或司法机关的跨境电子取证执法协助指令，虽然有助于维系网络服务提供者的相应国家的合规运营，但却很有可能，与此同时违背数据存储国关于数据本地化及数据流动或出境管制的法律禁令。在某些国家滥用跨境电子取证侦查权力的情况下，跨国运营的网络服务提供者所面临的这种合规困境必定会更加突出。

---

① 裴炜：《欧盟 GDPR：数据跨境流通国际攻防战》，载《中国信息安全》，2018（7）。

② Security Union, “Commission facilitates access to electronic evidence”, http://europa.eu/rapid/press-release_IP-18-3343_en.htm, 最后访问日期：2018 年 1 月 22 日。

第二，对保护公民的个人隐私等基本权利可能造成较大损害。[①] 网络服务提供者掌握的数据除了部分自身开展业务的运营数据外，还包括用户的注册信息、交易数据、财务数据、通信内容数据等多种类型的数据。在数据控制者模式问世之后，采取这种模式对待跨境电子取证行为的国家在向网络服务提供者发布数据披露指令时，通常只是要求后者配合执法，而不要求对所涉用户进行事前或事后的告知。这对数据存储国境内的公民个人隐私等基本权利的保护而言显然是非常不利的。

综上，数据控制者模式的出现在很大程度上反映了开展跨境执法的国家对数据相关权利进行强化保护的趋势，但同时也导致跨境运营的网络服务提供者的数据合规、公民的个人隐私等基本权利受到直接冲击。各国在近年来就此展开激烈博弈，也就不足为奇了。

## 二、“数据特例主义”对适用于有形实物的管辖模式的冲击

相较于有形实物而言，电子数据的出现时间较晚。由于有形实物的刑事取证管辖的范围长久以来都严格受限于国家疆域，因此对于数据而言，要么是强调其所具有的特殊性而需要建构全新的刑事取证管辖模式，要么是将其与有形实物予以无差别化地对待从而适用传统模式。

强调数据在刑事取证管辖方面不同于有形实物的特殊性而创设新的法律规则的观点被称为“数据特例主义”（Data Exceptionalism）。对此，美国华盛顿大学的 Daskal 于 2015 年提出的理论观点在学界受到了较大的关注，因而颇值一提。她从 5 个方面详细地阐释了数据相对于有形实物的差异。

一是数据的迅捷流动性（mobility）。以国际电子邮件为例，数据可能迅速且频繁地穿行于他国的云服务器，而有形实物的越境流动则受到严格限制。二是数据的离散存储性（divisibility）。特别是在云计算的技术背景下，基于数据运营安全及效率的考虑，离散式跨境存储已呈常态。三是数据存储与获取的分

① 参见方芳：《坚持在联合国框架下制定电子证据国际标准——联合国毒品犯罪办公室第五届网络犯罪政府间专家组会议研究》，载《信息安全与通信保密》，2019（5）。

离性（location independence）。一方面，数据权利人的位置与数据存储位置相分离；另一方面，调查人员的位置也与数据存储位置相分离。[①] 四是数据的多方牵涉性（intermingling）。以国际通信为例，数据可能同时涉及境内和境外的传输和存储，通信双方甚至多方均对数据享有权利。五是第三方掌控性（third-party control）。[②] 在云计算时代，用户的海量数据为跨境网络服务提供者所实际掌控，后者对数据存储地的确定有着决定性的影响。[③] 这种特性导致在刑事诉讼活动中，侦查机关越来越多地依赖于向第三方数据平台取证，而不是采取传统的方式对嫌疑人的设备直接进行搜查。[④] 根据“数据特例主义”的观点，既然数据在这么多方面都与有形实物存在显著差异，因此不应基于传统意义上的国家疆域而确定刑事取证管辖的范围。这就意味着，“数据特例主义”的理论观点实际上可以视作对数据存储地模式的否定。

当然，“数据特例主义”在理论界也面临较大的争议。针锋相对的观点并不主张基于数据的某些特殊性而建构全新的刑事取证管辖的法律规则。从理论脉络来看，这种观点起源于对“网络自身主权论”的反对。例如，Goldsmith 较早地提出，网络空间中的事务与现实世界的事务并没有什么不同，因此主张国家基于领土的管制同样适用于网络空间。[⑤] 就网络空间中的数据而言，Woods 相应地认为，它并非人们观念中所认为的那样属于新事实，其实与有形实物并无实质不同。即使

---

① 这种“分离”的特性所导致的一个潜在的后果是，执法机构很可能因被请求方不具备相关电子数据取证能力，而导致其无法通过常规的刑事司法协助程序获取到理想的证据。原因在于，“传统刑事司法协助制度以被请求国确有能力和权力获取该证据为前提。在数据取证的语境下，数据的物质载体无法有效限定和区分其中的数据类型、体量和相关性，执法机关面临着数据存储与数据控制相分离的现实状况，被请求国即便是数据载体的所在地，也并不意味着其具有获取载体所有数据的能力和权力。在保护个人数据的价值导向下，这种分离有可能被进一步强化。”参见裴炜：《未来犯罪治理的关键——跨境数据取证》，载《中国信息安全》，2019（5）。

② 也有学者将此特征称为“聚集性”。具体而言，“传统形式的证据很少具有聚集性，不同种类的证据可能分散在不同地方，但电子数据在多数情形下具有集中性、聚集性，即很多电子信息或者通话信息都处于一定的主体（如网络服务提供者）控制之下，被集中存储和管理。”参见冯俊伟：《跨境电子取证制度的发展与反思》，载《法学杂志》，2019（6）。

③ Jennifer Daskal, “The Un-Territoriality of Data”,*Yale Law Journal,* 125(2015), 365.

④ See Jennifer Daskal, “Privacy and Security Across Borders”,*Yale Law Journal Forum,* 128 (2019), 1029.

⑤ Jack L. Goldsmith, “Against Cyberanarchy”,*The University of Chicago Law Review*, 65(1998), 1199.

是云数据，其也事实上位于特定国家领土之内的存储设备之中，因此本质上也具有归属于国家疆域之基本特征。Woods 也对 Daskal 所论证的数据的某些不同于实物的独有特征进行了批判。以数据所谓的“迅捷流动性”为例，实际上跨境流动早已十分频繁的资金也具有这样的特征，因此不能简单地将该特征作为建构全新法律规则的论据。[①] 此外，Svantesson 认为，“数据特例主义”还存在概念逻辑上的论证错误，并指出 Daskal 所提到的数据的上述特征更为确切地讲应当称为“云数据特例主义”。[②] 例如，在不涉及云计算的情况下，数据完全不具备“离散存储性”和“第三方掌控性”。根据这种观点，尽管需要承认数据有一些特殊性，但是也应当采用长久以来适用于有形实物的刑事取证管辖模式，因此该观点实质上是支持数据存储地模式的。

尽管如此，“数据特例主义”理论的提出毕竟指出了数据不同于有形实物的一些特殊性，特别是对于云数据而言更是如此。在此背景下，“数据特例主义”的理论观点由于否定数据存储地模式，因而对适用于有形实物的刑事取证管辖模式确实构成了冲击。就美国《云法案》条款所代表的数据控制者模式而言，其对数据控制者模式的部分取代实质上也反映出“数据特例主义”理论观点已经产生了无可否认的现实影响。就此而论，“数据特例主义”从程序法理和证据法理的层面对国家刑事取证管辖模式的变革构成了深刻的影响，为数据控制者模式的登台亮相奠定了理论基础。

① See Andrew Keane Woods, “Against Data Exceptionalism”, *Stanford Law Review*, 68(2016), 729.

② Dan Jerker B. Svantesson, “Against ‘Against Data Exceptionalism’”, M*asaryk University Journal of Law and Technology,* 10(2016), 204.