法学研究 Chinese Journal of Law
Vol.41，No.2（2019）

基于数据主权的国家刑事取证管辖模式

梁　坤*

内容提要：关于电子数据的刑事取证管辖，在国家层面形成了数据存储地模式和数据控制者模式两大方案。传统的数据存储地模式以国家疆域为基础，因其适用困难、取证效率低下而已经有所松动。数据控制者模式则依托跨境云服务提供者，实现了对数据存储地模式的部分取代。刑事数据取证管辖模式的变革，从根本上讲，乃是各国立足于自身国家利益最大化而对数据资源实施掌控所致，而数据特例主义的提出也对适用于有形实物的传统管辖模式构成了冲击。我国应当正视国际上的变革趋势，在数据主权国家战略的基础上，着力探索刑事数据取证管辖模式的中国方案。具体而言，在坚持数据存储地模式的同时，有必要设定例外情形；在把握数据控制者模式之优势的同时，亦需针对他国采取该模式给我国带来的危害予以对等回应；在程序主义数据主权的框架下，加强与其他国家的平等协商与合作，构建适用于电子数据的刑事取证管辖互惠模式。

关键词：电子数据　数据主权　取证模式　刑事管辖

一、问题的提出

无论是从国内法还是国际法的角度看，一国虽然可以依据国内刑事法律对发生在他国境内的犯罪享有立案管辖权和裁判管辖权，但是原则上并不能在程序上行使执法管辖权。〔1〕刑事执法管辖权，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〕狭义上则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，刑事取证管辖通常也不能在未经他国许可的情况下延伸至他国境内。然而，网络时代的到来导致以领土范围为标准的刑事管辖界限逐渐模糊，近年来各国在刑事侦查

* 西南政法大学刑事侦查学院（国家安全学院）副教授。
本文系2018年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）的阶段性成果。

〔1〕 See Anthony J. Colangelo, *What is Extraterritorial Jurisdiction*, 99 Cornell Law Review 1311 (2014).

〔2〕 参见张兰图、刘竹君：《国家刑事管辖权法定论》，《当代法学》2006年第5期，第107页。

中收集电子数据时跨越国家疆界的情况屡见不鲜。这里首先介绍中美两国涉及此种情况的两起典型案例。

在张某、焦某非法获取计算机信息系统数据、非法控制计算机信息系统案中，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出具的远程勘验检查工作记录载明，侦查人员对该主控服务器（IP地址为66.102.253.30）进行了远程登录，提取到主控程序“Client.exe”和“系统日志”。“主控列表”显示，该服务器共控制240个IP地址，其中包括我国境内的31个IP地址。〔3〕本案中对电子数据的取证反映了许多同类案件的类似做法，即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，进行跨境网络远程勘验。

在美国，近年来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，美国联邦调查局在查办一起贩毒案件的过程中，在取得法院签发的令状后，要求微软公司披露某邮件用户的信息。微软公司拒绝披露邮件内容数据，因为这些数据被存储在位于爱尔兰的数据中心；〔4〕微软公司主张联邦调查局应通过双边司法协助程序来收集这些数据。然而，联邦调查局坚持要求微软公司直接披露相应数据，并否认本案的侦查权出现了域外适用。〔5〕微软公司无奈之下提起诉讼，最后由检察机关上诉至联邦最高法院。2018年3月23日，《澄清合法使用境外数据法》（即“云法”）〔6〕生效。该法授权执法部门通过要求在美国境内有实体机构的服务提供者进行数据披露的方式收集境外数据。联邦调查局遂根据该法取得新的搜查令状，微软公司也对该法表示支持。4月17日，联邦最高法院终审裁决，由于本案争议的法律问题不复存在，故将案件予以驳回。〔7〕至此，“微软—爱尔兰案”尘埃落定。

在上述张某、焦某案中，我国侦查机关通过网络远程勘验直接收集存储于境外的数据。从国家刑事取证管辖的角度而言，这种跨境电子数据取证方式显然不属于常规意义上的数据存储地模式。而在“云法”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占据巨大市场优势的服务提供者间接收集境外数据，也即在刑事取证管辖模式上更多采取与数据存储地模式迥异的数据控制者模式。

两案中跨境电子数据取证的具体程序、措施尽管存在显著区别，但两案均表明，刑事取证管辖已经借助网络空间便捷地跨越了传统意义上的国家疆界。刑事取证管辖乃是国家主权行使的典型体现，因此两案所反映出的根本问题是，国家到底能否在国际法和刑事程序法理的框架下对存储于境外的数据拥有主权和刑事取证管辖权？如果答案是肯定的，那么具体到本文的论题则需要进一步回答如下问题：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时，一国应采取什么样的理论模式？本文立足于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理论分析的基础上，着力探索刑事取证管辖模式的中国方案；希冀在国际法原则和规则的框架下，为我国刑事取

〔3〕 参见湖北省武汉市中级人民法院（2016）鄂01刑终176号刑事裁定书。

〔4〕 外文文献常用“Microsoft-Ireland Case”简称此案，下文为论述方便使用“微软—爱尔兰案”的简称。

〔5〕 Microsoft Corp. v. United States, 829 F.3d 222(2d Cir.2016).

〔6〕 该法英文全称为“Clarifying Lawful Overseas Use of Data Act”，因其主要涉及跨境云数据取证从而简称为“CLOUD Act”，下文为论述方便使用“云法”的简称。

〔7〕 United States v. Microsoft Corp., No.17-2, 584 U.S._(2018).

证管辖模式的完善，提供有益参考。

二、基于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，是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。可以从四个方面来理解这一模式：其一，将数据视为与其他有形实物并无实质性差异的证据，在刑事取证管辖制度上不对数据作特殊安排；其二，将数据视为与存储介质密不可分的物品，刑事取证管辖的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，相当于是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来确定数据的刑事取证管辖边界，管辖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，一国对位于其境内的电子介质中存储的数据拥有无可争议的刑事取证管辖权。如同 A 国侦查人员不能在未经许可的情况下进入 B 国国境进行侦查取证，其原则上也不能擅自“进入”位于 B 国境内的计算机系统收集电子数据。为避免电子数据取证行为越境，许多国家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时，需要判断警方的侦查行为是否会跨越国境。如果违法从境外收集数据，法院在后续程序中可能会将该证据予以排除。〔8〕在美国，过去很长时间内的司法准则也是坚持数据存储地模式。如在 2000 年，联邦调查局在调查一起黑客案件的过程中，在未经俄罗斯官方许可的情况下，使用秘密获得的嫌疑人用户名和密码登录俄方境内的计算机系统，在线提取涉案数据。此案引发俄罗斯方面强烈的外交抗议。〔9〕美国法院认定，由于数据存储在俄罗斯，此案中的侦查行为属于跨境搜查。〔10〕在总结诸多经验和教训之后，美国司法部刑事处计算机犯罪与知识产权犯罪部在 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”。〔11〕美国的网络法专家也指出，跨境远程搜查等侦查行为会导致对他国主权的侵犯，可能面临严重的国际法后果甚至外交纷争。〔12〕

作为网络犯罪领域目前影响最大的区域性国际法文件，2004 年生效的《网络犯罪公约》（Convention on Cybercrime）中的许多条文，也遵循了数据存储地模式。例如，根据第 18 条第 1 款规定的“提供令”（Production Order）制度，各缔约方的有权机关可以命令国内

〔8〕 See Ulrich Sieber, Nicolas von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice*, Duncker & Humblot, 2016, p. 730.

〔9〕 See Russell G. Smith, Peter Grabosky & Gregor Urbas, *Cyber Criminals on Trial*, Cambridge University Press, 2004, p. 58.

〔10〕 United States v. Gorshkov, NO. CR00 – 550C, 2001 WL 1024026 (W. D. Wash. May 23, 2001).

〔11〕 See CCIPS, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, p. 58, available at http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf, visited on Nov. 1, 2018.

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

的个人（person）提交其持有或者控制的特定计算机数据，以及要求国内的服务提供者提供其持有或者在其控制范围内的用户数据。但无论是哪一种情况，提供令所涉及的目标数据都应“在发出提供令的缔约方国内”。〔13〕

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，即需要通过司法协助程序来执行。例如在“微软—爱尔兰案”中，爱尔兰政府的主张就明显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”意见书中，申明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。〔14〕

（二）数据存储地模式面临的困境

1．适用困难

首先，数据存储地模式适用于存储状态下的静态数据，而不适用于传输过程中的动态数据。就静态数据而言，由于存储介质的物理位置通常较为明确地位于某一司法管辖权区域内，故在确定刑事取证管辖时较易作出判断。然而，就跨境传输中的动态数据而言，在侦查开始前很难预测所要收集的数据会流向何处，这便导致无法采取数据存储地模式来确定刑事管辖归属。其次，数据存储地模式适用于位置确定的数据，而不适用于位置不确定的数据。在当今云计算的技术框架下，无论是通过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。〔15〕典型的情况是，使用云存储服务的绝大多数用户可能都不清楚其上传至“云”中的数据到底位于何处。又如，“深网”（deep web）中的多数数据通常会有加密保护，“暗网”（dark web）则无法通过常规方式访问及追踪。这些技术性的限制因素给数据存储地的确定带来了极大障碍，从而导致一国侦查机关不可能严格遵循数据存储地模式来行使刑事取证管辖权。

2．效率低下

随着跨境通讯及云计算技术的飞速发展，数据的跨境存储与流动已越发常态化。如果严格遵循数据存储地模式，数据的跨境收集原则上都要通过司法协助程序来实施。然而，这种程序耗时较长、冗繁复杂，近年来相关取证需求剧增更使得其效率低下的劣势越发凸显。由于美国在全球云数据市场占有绝对优势地位，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，按常规程序需首先将请求逐级上报该国中央主管机关，然后由后者将协助请求按美方要求的形式发送给美国司法部国际事务办公室。该办公室审查后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，警务人员方可持令状要求谷歌公司提供相应数据。统计数据表明，整个协助程序通常需耗费10个月甚至更长时间。〔16〕这对于追求

〔13〕 参见皮勇：《〈网络犯罪公约〉中的证据调查制度与我国相关刑事程序法比较》，《中国法学》2003年第4期，第152页。

〔14〕 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. 14－2985－CV (2d Cir. Dec. 23, 2014).

〔15〕 See Christopher Millard (ed.), *Cloud Computing Law*, Oxford University Press, 2013, p. 288.

〔16〕 See 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, available at https://obamawhitehouse.archives.gov/sites/default/files/docs/2013－12－12_rg_final_report.pdf, visited on Nov. 9, 2018.

效率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

为缓解上述困境并有效提升跨境电子数据取证的效率，区域性国际公约及某些国家的国内法作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出现了松动。

1．在国际共识的基础上设定数据存储地模式的特殊例外

《网络犯罪公约》第 32 条、2010 年《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的单边远程取证方式。由于后者几乎照搬前者的条文，这里仅对《网络犯罪公约》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，不论该数据位于何处。”由于这类数据在执法地便可公开获得，故国际法专家认为这种情况属于行使域内管辖权。〔17〕该条 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的合法且自愿的同意。”为避免法条适用过程中可能出现的理解偏差，网络犯罪公约委员会（T-CY）于 2014 年发布《跨境电子数据取证指引注释（第 32 条）》，强调第 32 条 b 款在性质上属于地域管辖原则的特殊例外。〔18〕而根据国际电信联盟的阐释，缔约国签署该公约实际上是放弃了部分主权，从而允许其他国家实施影响其领土完整性的调查。〔19〕

2．在数据存储于境外但无法确认所在国的情况下直接适用国内侦查程序

云计算技术有时会导致数据在境外的具体位置难以确定。2017 年发生在美国的一起欺诈案件便遇到这种情况。法院裁定谷歌公司需向联邦调查局披露存储于境外的数据，原因是连该公司也无法确定涉案数据被技术性拆分后在境外的具体存储地，因此根本不可能根据数据存储地模式开展常规的刑事司法协助。〔20〕

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

在某些案件中，在侦查取证开始之前，根本无法判断数据到底存储于国内还是国外，为此，一些国家并不绝对排斥对潜在的跨境远程侦查措施进行授权。例如，美国为解决“暗网”取证等情况下数据存储地不明的法律障碍，于 2016 年修订《联邦刑事程序规则》。其中第 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。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。〔21〕

---

〔17〕 参见［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，社会科学文献出版社 2017 年版，第 107 页。

〔18〕 See Cybercrime Convention Committee, *T-CY Guidance Note # 3: Transborder Access to Data (Article 32)*, p. 3, available at https://rm. coe. int/16802e726a, visited on Oct. 26, 2018.

〔19〕 参见国际电信联盟电信发展部门：《了解网络犯罪：现象、挑战及法律对策》，第 282 页，https://www. itu. int/en/ITU - D/Cybersecurity/Pages/Publications. aspx，2018 年 3 月 18 日最后访问。

〔20〕 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.

〔21〕 See European Commission, *Commission Staff Working Document Impact Assessment (SWD (2018) 118 final)*, p. 33, available at https://eur - lex. europa. eu/legal - content/EN/TXT/? uri = SWD%3A2018%3A118%3AFIN, visited on Oct. 29, 2018.

数据存储地模式本身存在缺陷，给刑事取证管辖造成了很多障碍，近年来也确实出现了松动。然而，这一模式并未崩塌，它仍然是国际上电子数据刑事取证管辖的基本模式。这主要有三个方面的原因：

首先，在数据的境外存储位置明确的情况下，刑事司法协助仍是常规程序。因此，除非存在国际公约的特别授权和国家间的礼让机制，一国单边开展跨境电子数据取证就与其他实物证据的跨境收集无异，原则上都不为国际法所允许。

其次，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主权的潜在侵犯程度。除了美国对可能跨境开展的侦查行为规定了远程“搜查”这样的强制性措施，上述国际公约和其他国家的国内法所授权的措施，其侵犯性明显较弱。例如，《网络犯罪公约》授权的依据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，这具有不限制相对人基本权利的“任意侦查”的特征。比利时2000年修订刑事诉讼法增加了第88条之三（Art. 88*ter*），规定可能跨境开展的电子数据取证方式仅限于“复制”。此外，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”。〔22〕

最后，在远程取证过程中确认数据存储地之后，对相关国家的告知受到重视。相应制度在比利时刑事诉讼法、荷兰2019年1月1日起施行的计算机犯罪法（三）相关条款的配套机制中均有所反映。例如，荷兰官方认为，一旦确认远程搜查跨越国境，原则上需停止侦查，并且需要基于国际礼让及时告知相应国家。〔23〕此外，欧盟于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，未来的立法应专门规定诸如应告知可能受影响的国家在内的缓解措施。〔24〕

三、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，是指在云计算的技术框架下，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，获取其控制的数据。关于这一模式，可以从三个方面进行把握：其一，数据控制者模式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在的物理空间相区隔，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，从而回避适用常规的司法协助程序。其二，数据控制者模式依托跨境云服务提供者，属于对存储在境外的数据的间接取证方式。其三，数据控制者模式下的数据范围只涉及跨境云服务提供者控制的数据，即其拥有（possession）、保管（custody）或掌控（control）的数据。

〔22〕 参见前引〔21〕，欧盟委员会报告，第71页。

〔23〕 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 117 (2017).

〔24〕 See *Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way*, available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf, visited on Sep. 15, 2018.

近年来，通过数据控制者模式获取位于境外的数据，在国际上已经出现两种情况：一是通过在本地无实体机构的外国服务提供者获取境外数据。例如在比利时的一起案件中，当局要求美国雅虎公司披露境外数据，遭到后者拒绝（下文简称“比利时—雅虎案”）。比利时最高法院于 2015 年判决指出，雅虎公司虽然在比利时并无分支机构，但其存在实质性的向比利时用户提供网络服务的行为，“事实上是位于”比利时的服务提供者，因而需遵守比利时刑事程序中的数据披露义务。〔25〕二是通过在本地有实体机构的外国服务提供者获取境外数据。例如，2015 年巴西一家法院指令微软公司在该国的分支机构披露其存储于美国境内的涉案数据（下文简称“巴西—微软案”），微软公司未予执行，其负责人员随后受到巴西当局的刑事起诉。〔26〕此外，根据英国 2016 年《调查权法》（Investigatory Powers Act）第 3 部分“获取通讯数据的授权”第 85 条“跨境适用”之规定，执法部门可以向其境内运营的电讯服务提供者发布指令，以获取其存储于境外的数据。

不过，比利时、巴西、英国的立法或实践更多只是对数据控制者模式作了初步探索。这一模式的系统提出主要是受了“微软—爱尔兰案”的影响，并最终在“云法”于 2018 年出台后正式成形。〔27〕“云法”开宗明义指出，其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。该法标志着美国在云数据的刑事取证管辖方面，从数据存储地模式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关系

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运行良好，各国自然无需探索新模式。在数据存储地模式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减少。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，在数据存储地模式现有的特殊例外情形之外构建新模式，从而更大程度地化解数据存储地模式所面临的困境，便成为契合时代变迁背景的选择。以美国为例，在传统的刑事司法协助机制与跨境远程提取电子数据的单边方案均存在明显缺陷的背景下，通过服务提供者获取境外云数据成为其近年来重要的战略选项。从 2016 年开始，美国便一直试图通过立法推进相关工作，〔28〕而“云法”的出台也确实有助于化解数据存储地模式所面临的困境。

其二，数据控制者模式的适用限制意味着其只是部分取代数据存储地模式。数据控制者模式完全不考虑国家疆界的限制，因此从性质上讲其并不属于数据存储地模式的特殊例外。当然，数据控制者模式与数据存储地模式不是截然对立的，不能简单地认为前者完全取代了后者。上文已经说明，数据控制者模式依托跨境云服务提供者，瞄准的只是服务提供者控制的境外数据。由此观之，数据控制者模式的适用并不具有普适性，实际上它只是部分取代了数据存储地模式。这就意味着，对于网络空间中与这类服务提供者无关的数据，

〔25〕 Belgium Supreme Court, September 4th, 2012, A. R. P. 11. 1906. N/2.

〔26〕 See Brad Smith, *In the Cloud We Trust*, http://news. microsoft. com/stories/inthecloudwetrust, visited on Jun. 11, 2018.

〔27〕 参见洪延青：《美国快速通过 CLOUD 法案，明确数据主权战略》，《中国信息安全》2018 年第 4 期，第 35 页；许可：《数据主权视野中的 CLOUD 法案》，《中国信息安全》2018 年第 4 期，第 42 页。

〔28〕 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 页以下。

数据存储地模式仍然是刑事取证管辖的基本方案。

其三，两种模式会在一定时期内以相互博弈的方式共同存在。如同下文将要着重分析的，各国对于境内及境外数据资源存在差异极大的利益诉求。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以保护境内数据，但同时又可能通过数据控制者模式力图长臂掌控境外数据。而从国际层面看，数据掌控能力较弱的国家可能会单一性地坚守数据存储地模式，一些数据强国则会倾向于同时采取两种模式。换言之，在数据控制者模式部分取代数据存储地模式之后，两种模式的共存会成为一定时期内的必然现象，相互之间的博弈也将成为常态。这是各国刑事取证管辖制度面临的全新课题。

（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

一方面，数据控制者模式导致国家间刑事取证管辖范围出现重叠并诱发国际法冲突。根据数据存储地模式，对数据的刑事取证管辖受限于国家疆域，因此，除非出现上文提到的数据存储地模式的特殊例外，否则不可能发生国家间的刑事管辖权冲突。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会将刑事取证管辖范围延伸至主张后一模式的国家境内，这会导致取证管辖范围的重叠，从而诱发国际法冲突。

另一方面，数据控制者模式将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数据存储地模式，但可以预计的是，前者在国际范围内很可能会逐渐压缩后者的适用空间。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数据市场的蓬勃发展趋势，有着广阔的应用前景。如今，无论是个人还是公司都越来越多地将数据上传至“云”中，〔29〕而不再过多地进行本地存储。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，将越来越多地出现。应当认识到，数据控制者模式相较数据存储地模式确有其优势，它有助于破解数据跨境分散存储从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。以谷歌、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统治性份额，其控制的海量境外云数据，随着“云法”的出台都将潜在地被纳入美国的刑事取证管辖范围。而从近期来看，以欧盟、加拿大为代表的美国传统“朋友圈”已经准备效仿“云法”的做法或接受该法授权的双边互惠机制，〔30〕从而将数据控制者模式在全球范围内的实际影响越发放大。

四、刑事取证管辖模式变革的影响因素分析

数据控制者模式的问世及其对数据存储地模式的部分取代，反映出国际上刑事数据取

〔29〕 据美国思科公司 2015 年 11 月的预测，到 2019 年将有 55% 的居民区网络用户会使用云存储服务，高达 86% 的工作数据将存储于云中。See Cisco, *Cisco Global Cloud Index 2014 – 2019*, available at 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, visited on Nov. 1, 2018.

〔30〕 欧盟委员会于 2018 年 4 月 17 日宣布，计划建立“欧洲数据提交令”（European Production Order）制度：成员国的执法或司法当局可直接指令欧盟境内的服务提供者提供电子数据，不论相应数据是否存储于欧盟境内。2018 年 8 月 14 日，加拿大警察局长协会、法律修正案及电子犯罪委员会发布决议，敦促加拿大政府根据美国“云法”的规定与美国政府签订数据共享协议，以应对云计算时代网络犯罪证据跨境收集所面临的挑战。

证管辖制度发生了变革。通过比较分析和理论考察可以发现，这一变革主要受到两大方面因素的影响。其中，各国立足于自身国家利益的最大化对数据资源实施掌控是核心因素。而数据特例主义的提出也对适用于有形实物的传统刑事管辖模式形成了冲击，这一因素同样不容忽视。

（一）各国立足于自身国家利益的最大化对数据资源实施掌控

数据作为一种新兴资源的巨大价值早已获得国际认可，许多国家近年来越发重视对数据资源的掌控，以实现国家利益的最大化。不过，不同国家在数据资源的实际掌控能力上存在巨大差异，因而在国家数据主权、国家数据安全以及数据权利保护等方面，各国的国家战略及法律制度均展现出显著差异，由此对国际上刑事取证管辖模式的变革产生了重要影响。

1. 国家数据主权

刑事取证管辖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，国家对数据主权的基本立场便成为刑事管辖模式塑造及变革的基础。我国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作了表述："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"。数据主权依托网络空间，因此其理应成为我国在国家安全法和网络安全法中规定的"网络空间主权"的下位概念。〔31〕而网络空间主权系国家主权在网络空间的延伸，〔32〕因此数据主权也成为国家主权不可或缺的组成部分。

然而，我国所主张的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 版"，尽管认可我国所主张的网络空间主权，但在具体内容上只涉及三个层次：（1）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；（2）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；（3）社会层，包括参与网络活动的个人和团体。〔33〕换言之，"塔林手册 2.0 版"并未涉及国家对特定数据本身行使主权。〔34〕

更为复杂的问题是，尽管以中国为代表的大多数发展中国家为抵制网络霸权对网络空间的侵害而主张网络空间主权，〔35〕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《美国国家网络战略》只字不提网络空间主权，而是再次强调其近年来力推的互联网治理的"多利益攸关方模式"。〔36〕这些国家并不支持网络空间

〔31〕 国家安全法第 25 条规定："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。"网络安全法第 1 条指出，该法的立法目的之一是"维护网络空间主权和国家安全"。

〔32〕 国家互联网信息办公室 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。"

〔33〕 参见前引〔17〕，施密特总主编书，第 58 页。

〔34〕 参见黄志雄：《网络空间国际规则制定的新趋向——基于〈塔林手册 2.0 版〉的考察》，《厦门大学学报（社会科学版）》2018 年第 1 期，第 5 页。

〔35〕 参见张新宝、许可：《网络空间主权的治理模式及其制度构建》，《中国社会科学》2016 年第 8 期，第 147 页。

〔36〕 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, visited on Nov. 15, 2018.

主权，因此更谈不上赞成作为网络空间主权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，并且数据主权是否成立、是否包含于网络空间主权概念等问题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。主张数据主权的国家必然强调对网络空间中特定数据的保护和管控，特别是对于存储在其境内的数据，坚持数据存储地模式从而排他性地对抗他国的争夺，显然更符合其国家利益。然而，与此相对，反对数据主权的国家更希望松动乃至突破数据存储地模式，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的数据的长臂掌控。就此而论，数据控制者模式的问世与数据主权的国际争议不无关系。

2．国家数据安全

出于国家数据安全的考虑强化对数据的保护，这对于在网络技术、跨境通讯、云计算市场等领域处于弱势的国家尤为重要。如今，跨境云服务提供者控制的数据不仅涉及大规模的用户隐私，甚至关系到一国的国计民生，从而会潜在地影响一国的数据安全和稳定。于是，通过法律强制要求服务提供者对在其境内收集及提供服务过程中产生的数据进行本地化存储，已成为许多国家对抗数据强国、反抗数据霸权的重要选择。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的本地化存储作了明确要求。〔37〕

基于数据安全的考虑强化数据保护的另一个表现是，对数据的跨境流动或披露进行法律规制。这一方案近年来也得到许多国家的青睐，并形成以俄罗斯、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，以印度、印尼为代表的本地备份流动模式。〔38〕从便利刑事取证管辖的执行、维护数据安全从而实现国家利益最大化的角度看，数据存储地模式有显著优势。一方面，在实现数据本地化存储后，可以有效服务于本国的刑事侦查，取证活动无需经历复杂的司法协助程序、无需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，致使其他国家无法便捷地通过单边渠道收集数据，这对于维护数据安全具有重要意义。

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。这是因为，在 A 国实行数据本地化存储制度后，B 国服务提供者在 A 国从事数据业务就必须以自建服务器或本地托管的方式满足 A 国的法律要求，这必然导致 B 国的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。《美国国家网络战略》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。"〔39〕可见，美国反对其他国家的数据本地化存储制度，并主张数据跨境自由流动，这在很大程度上就是要通过维护其跨国企业的利益来实现其国家网络战略。要达到这一目标，美国必然要弱

〔37〕 See Nigel Cory, *Cross-border Data Flows: Where Are the Barriers, and What Do They Cost?*, available at https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost, visited on Oct. 28, 2018.

〔38〕 参见吴沈括：《数据跨境流动与数据主权研究》，《新疆师范大学学报（哲学社会科学版）》2016 年第 5 期，第 114 页。

〔39〕 前引〔36〕，《美国国家网络战略》报告，第 15 页。

化其他国家保护数据的力度。就刑事取证管辖而言，数据强国力主推行的数据控制者模式，可以看作是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。

3．数据权利保护

对与数据相关的特定法律权利进行保护，提升国家对数据的掌控能力，也会对刑事取证管辖模式的塑造和变革产生重要影响。2018 年 5 月 25 日，被称为“史上最严”的《通用数据保护条例》（GDPR）（下文简称“欧盟数据条例”）施行，欧盟从整体层面强化了对个人数据的保护。其中，第 48 条专门规定“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，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“欧盟数据条例”第 5 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，从而欲通过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“欧盟数据条例”相冲突。从这一角度看，该条文可被视为欧盟选择以数据存储地模式来强化个人数据保护，从而强有力地提升欧盟成员国对于存储在其境内的数据的掌控能力。这对于维护欧盟成员国的整体数据利益而言，显然具有重要意义。

但从另一角度看，“欧盟数据条例”在强化个人数据保护方面也出现了跨境适用。〔40〕根据第 3 条“地域范围”的规定，“欧盟数据条例”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”。上文已经提到，欧盟在美国“云法”出台的背景下已计划建立“欧洲数据提交令”制度，在电子数据取证方面不再考虑相应数据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“欧盟数据条例”的保护，〔41〕所以，这实际上就是通过强化个人数据保护实质性地实现欧盟成员国对境外数据的实际掌控。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予以实质性变革。这样一来，欧盟的改革方案对内强化了数据存储地模式，对外则计划推行数据控制者模式。这些实际上体现了欧盟及其成员国在信息时代尽最大可能维护自身数据利益而做出的努力。

（二）数据特例主义对适用于有形实物的传统刑事管辖模式的冲击

相较于有形实物，电子数据的出现时间较晚。由于有形实物的刑事取证管辖范围长久以来严格受限于国家疆域，所以，对于数据，要么强调其特殊性从而构建全新的刑事取证管辖模式，要么将其与有形实物予以无差别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从而需要创设新的法律规则的观点，被称为“数据特例主义”。美国学者从五个方面详细阐释了数据相对于有形实物的差异：（1）数据的迅捷流动性。以国际电子邮件为例，数据可以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。（2）数据的离散存储性。特别是在云计算

〔40〕 参见何波：《数据是否也有主权——从微软案说起》，《中国电信业》2018 年第 8 期，第 57 页。

〔41〕 See Security Union, *Commission Facilitates Access to Electronic Evidence*, available at http://europa.eu/rapid/press-release_IP-18-3343_en.htm, visited on Oct. 22, 2018.

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。（3）数据存储与获取的分离性。一方面，数据权利人所处的位置与数据的存储位置相分离；另一方面，调查人员所处的位置也与数据的存储位置相分离。（4）数据的多方牵涉性。以国际通讯为例，数据可以同时涉及境内和境外的传输和存储，通讯双方甚至多方均对数据享有权利。（5）数据的第三方掌控性。在云计算时代，用户的海量数据为跨境服务提供者所实际掌控，后者对数据存储地有着决定性的影响。〔42〕根据数据特例主义的观点，既然数据与有形实物存在诸多显著差异，因此不应基于国家疆域来确定数据的刑事取证管辖。这就意味着，数据特例主义的理论观点可以看作是对数据存储地模式的否定。

当然，与数据特例主义针锋相对的观点，并不主张因为数据具有某些特殊性就为数据构建全新的刑事取证管辖规则。例如，戈德史密斯较早提出，网络空间中的事务与现实世界中的事务并无不同，国家基于领土的管制同样适用于网络空间。〔43〕就网络空间中的数据而言，伍兹认为，它并非人们观念中所认为的那样属于新事实，其实它与有形实物并无实质不同。即使是云数据，事实上也位于特定国家领土之内的存储设备中，因此本质上也具有归属于国家疆域的基本特征。伍兹对数据具有某些不同于实物的独有特征的观点进行了批判。以所谓的“迅捷流动性”为例，实际上频繁跨境流动的资金也具有这样的特征，因此不能简单地将该特征作为构建全新法律规则的论据。〔44〕此外，斯万特森指出，更加确切地讲，数据的上述独有特征应当被称为“云数据特例主义”。〔45〕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”。根据上述观点，尽管应当承认数据的部分特殊性，但也应当采取长久以来适用于有形实物的刑事取证管辖模式，因此这类观点实质上是支持数据存储地模式的。

尽管数据特例主义在理论上遭遇了诸多批评，但由于它否定数据存储地模式，对适用于有形实物的传统刑事取证管辖模式形成了理论冲击，故其已经产生现实影响。美国“云法”所代表的数据控制者模式的问世及其对数据存储地模式的部分取代，就是这一现实影响的典型体现。就此而论，数据特例主义从程序法理和证据法理等层面，对国家刑事取证管辖模式的变革产生了深刻影响，为数据控制者模式的问世奠定了理论基础。

五、刑事数据取证管辖模式的中国立场及理论检讨

（一）我国刑事数据取证管辖的现状

对于存储在境内的数据，我国主张拥有无可争议且排他的刑事取证管辖权。2018 年 10 月 26 日起施行的国际刑事司法协助法第 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。”这一

〔42〕 See Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale Law Journal 366 – 378 (2015).

〔43〕 See Jack L. Goldsmith, *Against Cyberanarchy*, 65 The University of Chicago Law Review 1199 (1998).

〔44〕 See Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stanford Law Review 758 (2016).

〔45〕 See Dan Jerker B. Svantesson, *Against 'Against Data Exceptionalism'*, 10:2 Masaryk University Journal of Law and Technology 204 (2016).

条文显然也适用于数据的刑事取证管辖。我国通过多部法律法规强制要求数据的本地化存储以保障数据安全，如此也便于国内刑事取证的执行。例如，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”。然而，对于存储在境外或跨境流动中的数据的刑事取证管辖，侦查取证的具体情况较为复杂，须区分情形进行说明。

第一，通过刑事司法协助程序收集存储于境外的数据。国际刑事司法协助法第 25 条规定，办案机关需要外国就所列事项协助调查取证的，应当制作刑事司法协助请求书并附相关材料，经所属主管机关审核同意后，由对外联系机关及时向外国提出请求。其中第 4 项的内容是“获取并提供有关文件、记录、电子数据和物品”。由此可见，该法对电子数据与其他实物证据的跨国收集没有作任何区分，刑事司法协助是常规程序。区际刑事司法协助遵循同样的准则。例如，2009 年签署的《海峡两岸共同打击犯罪及司法互助协议》第 8 条规定的“调查取证”，虽然只列举了“书证、物证及视听资料”，但从体系解释的角度看也应包括电子数据。原因在于，协议签署时，刑事诉讼法尚未规定电子数据这一证据形式，从发展的眼光看，应当将与“书证、物证及视听资料”一样属于实物证据的电子数据纳入其中。另外，该条规定协议适用于勘验、鉴定、检查、搜索及扣押等常规的实物证据调查措施，而这些措施均可用于收集电子数据。

第二，通过单边授权的远程侦查措施收集存储于境外及跨境流动中的数据。2014 年最高人民法院、最高人民检察院、公安部《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》第 15 条，首次对跨境远程提取电子数据作了规定。具体而言，对于“原始存储介质位于境外”而无法获取介质的，可以提取电子数据。2016 年最高人民法院、最高人民检察院、公安部《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》（下文简称“电子数据证据规定”）第 9 条进一步明确：“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，我国对单边开展的三种跨境远程取证措施进行了授权。第一种称为跨境网络在线提取，一般指向境外的公开数据。第二种即跨境网络远程勘验，属于在网络在线提取措施的基础上针对远程计算机信息系统这一特定情形的取证。〔46〕第三种则是以网络监听为代表的跨境远程技术侦查，可用于收集境外或跨境流动的动态数据。〔47〕其中，跨境网络远程勘验在侦查实践中得到了更为广泛的运用，实践中主要有两种类型：其一，通过讯问等手段获取账号、密码后登录境外网站或服务器提取数据。其二，采用勘验设备或专门软件提取境外服务器中存储的数据，这在服务器架设在境外的传播淫秽物品、网络赌博、电信诈骗等案件中十分常见。

在上述三种类型之外，侦查机关是否还可以采取其他措施收集境外电子数据，目前并

〔46〕 参见 2019 年 2 月 1 日起施行的《公安机关办理刑事案件电子数据取证规则》第 27 条。

〔47〕《计算机犯罪现场勘验与电子证据检查规则》第 25 条规定了网络监听。这种技术侦查手段可以用于对跨境传输过程中的数据及境外目标系统运行过程中的数据进行实时收集。

无定论。例如，侦查机关常用的远程鉴定、远程检查、远程搜查、远程辨认等措施，〔48〕实际上都可以轻易跨越国境，实践中甚至出现了侦查中“冻结”境外电子数据的情况。〔49〕然而，这些侦查措施的跨境适用欠缺明确的法律授权。此外，对于我国侦查机关是否可以像其他国家那样采取数据控制者模式从而通过服务提供者获取境外的云数据，也无明确结论。而根据“电子数据证据规定”第13条，办案机关可以采用“调取”措施收集电子数据，并通知电子数据持有人、网络服务提供者或者有关部门执行。然而，该条既没有指明调取的电子数据是否可以涉及境外数据，也没有对网络服务提供者的跨境数据披露义务作明确要求，因此国际互联网公司在实践中往往不愿意配合。〔50〕

（二）对我国现行刑事数据取证管辖模式的检讨

1．现行刑事数据取证管辖模式的内在矛盾

一方面，我国坚持数据存储地模式，并且反对数据控制者模式。国际刑事司法协助法第25条将电子数据与其他实物证据作同类处理，实质上就是主张采取数据存储地模式。与此相应的是，我国反对外国在不符合该模式的情况下进行跨境远程取证。例如，中国代表团于2013年2月参加“联合国网络犯罪问题政府间专家组第二次会议”时指出，《网络犯罪公约》第32条b款的缺陷在于，直接跨境取证措施“与国家司法主权之间的关系值得探讨”。〔51〕出于维护数据存储地模式并保障主权和管辖权的考虑从而反对这一条款，成为我国拒绝加入该公约的主要理由之一。此外，我国通过立法对数据控制者模式表达了反对立场。国际刑事司法协助法于2017年12月一审后，有部门提出，“实践中有外国司法执法机关未经我国主管机关准许要求我境内的机构、组织和个人提供相关协助，损害我国司法主权和有关机构、组织和个人的合法权益”。由此，该法第4条增加我国“境内的机构、组织和个人不得向外国提供证据材料”的内容，其目的就是“抵制外国的‘长臂管辖’”。〔52〕

另一方面，我国的侦查程序规范及实务又时常违背数据存储地模式。严格意义上的数据存储地模式，要求跨境电子数据取证均需通过司法协助机制来加以执行。然而，“电子数据证据规定”确立的跨境远程取证措施，在很大程度上选择了单边主义。《公安机关办理刑事案件电子数据取证规则》（下文简称“电子数据取证规则”）第23条虽然强调对“境内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，但并未明确禁止网络远程勘验等侦查措施的跨境适用。具体到本文开篇提到的张某、焦某案中跨境网络远程勘验的情况，这种做法从操作上讲与《网络犯罪公约》第32条b款授权的属人主义并无实质区别，却没有像后者那样建立在多边认同的基础之上从而构成国际法所认可的数据存储地模式的特殊例外。从侦查机关使用取证设备或软件进行跨境远程勘验以及以网络监听为代表的跨境技术侦查来看，则与“未经一国的同意而‘侵入’他国境内的服务器以获取证据”的情

〔48〕 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。

〔49〕 例如，在侦查一起开设赌场案的过程中，公安机关冻结了487个涉嫌赌博的境外网站账户。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。

〔50〕 参见冯姣：《互联网电子证据的收集》，《国家检察官学院学报》2018年第5期，第37页。

〔51〕 参见《中国代表团出席“联合国网络犯罪问题政府间专家组”》，http://www.fmprc.gov.cn/ce/cgvienna/chn/drugandcrime/crime/t1018227.htm，2018年3月15日最后访问。

〔52〕 参见全国人民代表大会宪法和法律委员会：《关于〈中华人民共和国国际刑事司法协助法（草案）〉审议结果的报告》，http://www.npc.gov.cn/npc/xinwen/2018－10/26/content_2064519.htm，2018年10月31日最后访问。

形更为类似,〔53〕而这与数据存储地模式背后的国家主权理念是背道而驰的。

2．现行刑事取证管辖模式欠缺数据主权国家战略的统领设计

刑事取证管辖直接体现国家主权的行使，刑事数据取证管辖也就体现了国家数据主权的行使。根据《布莱克法律词典》的界定，国家主权既包括内部主权即国家在其境内享有的最高权力，也包括外部主权即对外处理其国家利益的权力。〔54〕与此相应，我国学者也多主张应从对内、对外两个维度来认识数据主权。〔55〕然而，学界对数据主权的范围划定却存在分歧。一种观点认为，数据主权只涉及对本国网络、数据中心、信息系统中的数据行使所有权、控制权、管辖权和使用权;〔56〕另一种观点则认同属人主义，主张对境外的部分数据也拥有主权。〔57〕在数据主权的概念和范围没有得到清晰界定的情况下，我国目前对于刑事数据取证管辖模式，自然无法在数据主权国家战略的统领下进行良好设计，内在的矛盾和冲突难以避免。

六、基于数据主权的刑事取证管辖模式之完善

（一）基于数据主权国家战略完善刑事取证管辖模式的基本主张

1．坚持数据主权，刑事取证管辖应纳入数据主权的战略部署

在大数据和云计算的时代背景下，数据已成为国家核心资源。我国应当坚定不移地主张和行使数据主权，并使其成为网络空间主权的有机组成部分。数据的刑事取证管辖直接体现国家数据主权的行使，因此，从国家战略层面应当意识到，刑事取证管辖模式的完善应成为数据主权建设的重要组成部分。

2．维护数据主权，刑事取证管辖模式的建构应与国家数据安全保障整体协调

维护数据主权的重要前提是保障数据安全，而刑事取证管辖模式的良好设计与数据安全保障密切相关。考虑到控制海量数据的服务提供者在刑事取证管辖方面扮演着越发重要的角色，对其实际执行的跨境数据披露进行有效的法律规制，对于保障数据安全、维护数据主权具有重大意义。

3．尊重数据主权，对外行使刑事取证管辖不得侵犯他国对内的数据主权

“互相尊重主权和领土完整”是我国长期坚持的和平共处五项原则中的第一位原则。对于数据主权，各国应当遵循同样的原则，旗帜鲜明地反对数据霸权。我国在主张数据主

〔53〕 参与制定“塔林手册 2.0 版”的专家一致认为，“未经一国的同意，另一国的执法机关不可侵入该国境内的服务器以获取证据。”参见前引〔17〕，施密特总主编书，第 106 页。

〔54〕 See Black's Law Dictionary (9th ed.), Thomson West, 2009, p. 1610.

〔55〕 参见齐爱民、盘佳：《数据权、数据主权的确立与大数据保护的基本原则》，《苏州大学学报（哲学社会科学版）》2015 年第 1 期，第 67 页；孙南翔、张晓君：《论数据主权——基于虚拟空间博弈与合作的考察》，《太平洋学报》2015 年第 2 期，第 65 页；孙伟、朱启超：《正确区分网络主权与数据主权》，《中国社会科学报》2016 年 7 月 5 日第 5 版。

〔56〕 参见冯伟、梅越：《大数据时代，数据主权主沉浮》，《通信安全与保密》2015 年第 6 期，第 49 页；沈国麟：《大数据时代的数据主权和国家数据战略》，《南京社会科学》2014 年第 6 期，第 115 页。

〔57〕 例如，有学者认为，“数据主权也意味着数据即使被传输到云端或远距离服务器上，仍然应受其主体控制，而不会被第三方所操纵”（蔡翠红：《云时代数据主权概念及其运用前景》，《现代国际关系》2013 年第 12 期，第 59 页）。也有学者认为，“一国公民在境外形成的数据也属于该国管辖的范围”（杜雁芸：《大数据时代国家数据主权问题研究》，《国际观察》2016 年第 3 期，第 6 页）。

权的同时，也应相应地基于国际礼让承认并尊重他国同等享有的数据主权，而无论他国是否对此作出明确主张。对于各国基于自身国家利益和网络空间战略而发生的刑事取证管辖范围的重叠，有必要在国际法的框架下通过平等互利的协商来加以解决。

（二）基于数据主权完善刑事取证管辖模式的具体构想

1．数据存储地模式的坚持与调整

基于数据主权战略，原则上应当坚持数据存储地模式，并尊重他国同样以国界划定的数据主权。鉴于此，应当根据这一模式并在国际法的框架下，对现有刑事取证管辖制度进行三个方面的调整：

首先，根据数据存储地模式的内在要求，严格限制国内法单边授权的跨境远程取证。基于数据主权的立场，我国在坚决反对他国以远程搜查等方式收集存储于我国境内的数据的同时，也应有效清理我国现有侦查程序中有可能侵犯他国数据主权的制度和规范。如上文所述，一国在数据存储地模式下以单边途径收集存储于他国的非公开数据，只能在国际公约、国际礼让及他国法律允许的情况下进行。然而，“电子数据证据规定”单边授权实施的某些跨境远程取证措施却不符合数据存储地模式的内在要求。最高人民法院权威人士解读相关司法解释时提出，“对位于境外的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”。〔58〕这种单边主义思路过度放大电子数据相对于常规实物证据的特殊性，针对电子数据打造了回避适用刑事司法协助程序的快捷跨境取证制度，这明显违背数据存储地模式的内在要求。而且，这种做法也与我国所主张的数据主权战略相冲突，忽视了对他国数据主权的尊重。因此，除了下文提出的三种特殊例外，其他类型的跨境远程取证应在程序法上受到严格限制。

其次，根据数据存储地模式的特殊例外，允许开展特定的单边跨境远程取证。

第一，在国际认同的情况下依据属人主义获取境外数据。如上文所述，《网络犯罪公约》第 32 条 b 款是属人主义的典型表现。我国也有学者明确支持通过这种方式对境外数据行使管辖权。〔59〕从本文开篇提到的张某、焦某案进行跨境远程勘验的情况来看，属人主义实际上已经在我国的侦查实践中得到广泛接受。虽然外交部门就《网络犯罪公约》第 32 条 b 款对国家主权的潜在侵犯提出了反对意见，但根据学者的解读，对该条款的质疑除了国家主权方面的考虑外，主要是担忧该条款可能会被滥用，例如被用于非刑事侦查程序的情报收集。〔60〕然而，本着互相尊重数据主权的原则，我国没有理由在采取属人主义对境外数据单方行使刑事取证管辖权的同时，却认为他国采取同样方式取证会侵犯我国（数据）主权。这也意味着，我国在没有与其他国家签署有关条约的情况下，依属人主义采取远程勘验等侦查措施，有违反数据存储地模式从而侵犯他国数据主权之嫌。因此，我国可以考虑在平等互利的基础上达成国际认同，对这类跨境远程取证的具体要求进行限定，从而在国际法上形成数据存储地模式的特殊例外。由于这种国际认同的实现有赖于下文要提出的互惠模

〔58〕 胡云腾主编：《网络犯罪刑事诉讼程序意见暨相关司法解释理解与适用》，人民法院出版社 2014 年版，第 55 页；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。

〔59〕 参见前引〔57〕，蔡翠红文；前引〔57〕，杜雁芸文。

〔60〕 参见胡健生、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。

式的构建，因此这里不作展开。

第二，收集无需特别侦查措施即可访问的境外公开数据。这主要是指《网络犯罪公约》第 32 条 a 款涉及的数据类型，即普通公众能够获得的数据。“电子数据取证规则”第 23 条、[61]“电子数据证据规定”第 9 条第 2 项规定的网络在线提取的数据，实际上就包括这类境外数据。根据最高人民检察院权威人士对后一条款的解读，这种措施的实际操作“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”。[62] 具体而言，这类数据主要分为两种情况：一种是普通搜索引擎能够检索并且普通用户能够直接访问的数据；另一种则是常规搜索引擎无法爬取的“深网”中的部分数据，例如境外封闭在线论坛、聊天频道或者私人主机服务器中的数据。这类数据尽管受到登录凭证或其他方式的保护，但从性质上讲也属于公开数据。2014 年由网络犯罪公约委员会发布的《跨境电子数据取证指引注释（第 32 条）》便将这类数据界定为“公众可以获得的公开资料”，包括公众通过订阅或注册可以获得的资料。[63]“塔林手册 2.0 版”更是阐明，在使用登录凭证收集境外数据的情况下，一国行使的是“域内管辖权，而不是域外管辖权”。[64]

第三，运用国内法授权的措施收集存储地不明的数据。对于一国在数据存储地不明确的情况下，是否可以潜在地行使域外刑事取证管辖权，国际法上目前并无确定的解决方案。在此背景下，美国、比利时、葡萄牙、西班牙、法国的法律已经对这类刑事取证活动进行了授权。我国在侦查实务中也已经出现类似的“暗网”取证，[65] 这种潜在的跨境电子数据取证应当在侦查程序中得到明确认可。

最后，根据电子数据取证的快捷理念，着力推动司法协助高效开展。单边跨境远程取证的扩张与传统司法协助程序无法满足时代发展的需要不无关系。然而，在上文主张根据数据存储地模式的内在要求严格限制单边方案的背景下，侦查实务的取证需求并未萎缩甚至还在持续增长，这就需要为跨境电子数据取证另寻出路。对此，国外已经出现的双边和多边快捷司法协助方案，给我国提供了富有价值的参考。

从双边方案来看，特事特办的“司法协助函”（letters rogatory）近年来在某些重大犯罪的跨境电子数据取证方面，发挥了重要作用。例如，法国于 2015 年 1 月 7 日发生《查理周刊》总部恐怖袭击案之后，便向美国递交了这种函件，请求在调查过程中及时共享相关数据，最后得到了美国的支持。又如，美国近年来在查办“丝路”（Silk Road）暗网黑市交易案的过程中，在与冰岛没有签署司法协助条约的情况下，也向后者发送了这种函件，在获得准许后对位于冰岛的服务器进行了在线实时监控取证。[66]

---

〔61〕 该条规定：“对公开发布的电子数据……可以通过网络在线提取。”

〔62〕 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。

〔63〕 参见前引〔18〕，网络犯罪公约委员会报告，第 4 页。

〔64〕 参见前引〔17〕，施密特总主编书，第 107 页。

〔65〕 例如，在我国网警办理的“暗网”取证第一案中，警方根据美国方面提供的一个虚拟身份，在境外隐秘网络中采取“蹲守”“勘验”等措施进行取证。参见刘子珩等：《境外隐秘网络第一案背后的暗黑世界》，《新京报》2016 年 11 月 25 日第 13 版。

〔66〕 See Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 Nyu Annual Survey Of American Law 702 (2017).

从多边方案来看，欧盟于2018年系统提出并计划于2019年底立法的方案，将可能极大程度地推动跨境电子数据取证的快捷执行。具体而言，欧盟准备对目前适用于所有证据类型的“欧洲调查令”进行改良，〔67〕专门针对电子数据的特点，打造取证协助的在线加密通讯平台。预期方案拟要求一国执法机关在发布“欧洲调查令”的同时，需提供接受请求的一方便于开展工作的电子调查令版本，并附上操作者在无需接受专门培训的情况下便可快捷执行的明确指引。〔68〕

然而，“司法协助函”尽管高效快捷，却不可能大范围推广；欧盟的多边跨境快捷电子数据取证方案需要成员国的集体认同，真正落地难度也不小。尽管如此，我国可以吸取其有益经验，相应地在双边、多边框架下着力打通快捷刑事司法协助渠道，使之能够产生替代部分单边跨境电子数据取证措施的效果。

2．数据控制者模式的运用与对等回应

首先，数据控制者模式的有效运用。主张数据主权且在刑事取证管辖方面坚持数据存储地模式，并不意味着数据控制者模式就没有任何的适用空间。如上文已述，数据控制者模式适应了云计算技术发展的时代背景，在某些方面确有其优势。虽然这一模式目前是由试图扩张数据霸权、占据技术优势的国家所竭力主张，但是，在一定程度上，它也可以为包括我国在内的欠发达和发展中国家所有效运用。

具体而言，在外国法允许的框架下开展与服务提供者的合作，是依托数据控制者模式有效开展跨境快捷电子数据取证的重要方式。如果数据存储地国的法律不禁止，甚至明确允许外国执法部门采取数据控制者模式收集其境内数据，相应措施当然可以为我国所用。例如，欧盟国家近年来便广泛开展与美国服务提供者的合作，在后者自愿且不违反美国法律的情况下，通过数据披露机制快捷获取存储于美国境内的部分数据。根据美国《储存通讯记录法》的规定，外国政府若要通过这种方式获取存储于美国的内容数据，会受到严格的程序限制。〔69〕但是，该法也规定了两种无需启动司法协助程序的情形。第一种可以称为“一般例外”。例如，服务提供者在自愿的情况下，可以向他国执法部门直接披露用户名称、网络地址、通讯时长等非内容数据。〔70〕第二种可以称为“特殊例外”。例如，服务提供者基于善意且有理由相信，当出现涉及生命或严重身体伤害的威胁时，甚至可以立即披露内容数据。〔71〕又如，外国执法部门在获得服务订阅者或客户的同意后，可以直接要求服务提供者披露内容数据。〔72〕

我国可以在符合外国法规定的情况下，寻求与跨境服务提供者合作，在一定范围内有效实现对部分境外数据的便捷收集，从而改变目前实务中向外国服务提供者调取境外数据时普遍遭到拒绝的境况。为此，我国侦查实务应当加强对外国法中相关授权性或非禁止性

〔67〕“欧洲调查令”制度于2017年5月22日起施行。收到请求的成员国，最多有30天时间来决定是否接受该请求。如果接受该请求，具体的取证执行期限只有90天。

〔68〕参见前引〔21〕，欧盟委员会报告，第46页。

〔69〕外国政府的此类取证请求必须经过司法协助程序，并由美国相应辖区的法官进行审查，以满足美国宪法第四修正案所规定的启动搜查、扣押措施的“合理根据”标准。18 U.S.C. § 2703 (a).

〔70〕18 U.S.C. § 2703 (c) (2).

〔71〕18 U.S.C. § 2702 (b) (8).

〔72〕18 U.S.C. § 2703 (c) (1) (C).

规定的把握，争取服务提供者在保护客户信息的前提下自愿合作，最大程度地发挥数据控制者模式的优势。但是，这种主张在未来可能面临较大的障碍。这是因为，国际刑事司法协助法第 4 条原则上禁止我国境内的机构、组织和个人向外国提供包括电子数据在内的证据材料。所以，在此背景下我国如欲实现对数据控制者模式的有效运用，在政策层面就存在矛盾之处。于是，一些国家在无法通过服务提供者获取存储于我国的数据的情况下，也极易对我国采取对等举措。其国内法在授权其他国家通过数据控制者模式获取其境内的部分数据的同时，可能会单方面对我国施加限制。因此，数据控制者模式的有效运用，实际上需要在国际礼让的基础上才能实现。

其次，数据控制者模式的对等回应。为确保数据控制者模式发挥最大效用，一些国家对服务提供者施加了强制性法律义务，并且在其违反该义务时施加处罚。这在“比利时—雅虎案”“巴西—微软案”当中都有体现。由于美国“云法”集中体现了数据控制者模式的运作方式，这里重点分析该法对我国可能产生的影响，并提出应对策略。

根据国际刑事司法协助法第 4 条，在我国运营的服务提供者将不得向外国披露存储于我国境内的数据。然而，如果相关服务提供者同时在美国运营，则在未来的个案中，将面临该国执法部门依据“云法”要求其提供我国境内数据的问题。这样一来，包括中国互联网公司在内的服务提供者将受到两国法律冲突的挤压，并可能因无法向美国提供数据而受到处罚。实际上，“云法”也提供了一定的权利救济机制，允许跨境服务提供者在可能违反“适格外国政府”法律禁令之重大风险的情况下，向美国法院提出申请撤销或更改数据披露指令的动议。然而，该法对所谓“适格外国政府”设置了大量限制条件，除了要求其必须与美国签署有专门的行政性协议，还需要审查其是否为《网络犯罪公约》的缔约国抑或其国内法是否与该公约第 1 章、第 2 章的界定和要求相符。综合来看，我国目前并不是美国“云法”所谓的“适格外国政府”。〔73〕于是，在中美两国均运营的服务提供者，无法适用该法提供的所谓救济机制。

因此，为制衡“云法”所代表的数据控制者模式的长臂管辖，特别是为了应对在两国运营的中国服务提供者在个案中可能违反该法从而受到美国处罚的情况，我国应当对等保留采取数据控制者模式收集美国境内云数据的权利，通过对美国服务提供者施加跨境数据披露义务的方式，形成“战略上的对冲”。〔74〕如此一来，对于数据存储地模式的突破，就完全是国际法上对等原则的体现，而不能视为我国对这种模式的放弃。

3．“程序主义数据主权”概念下的互惠模式

上文的论述充分说明，在各国对数据采取不同刑事取证管辖模式的背景下，国家主权及国际法上的冲突不可避免。这种现象的出现，从根本上讲是因为各国采取单边视角，从自身国家利益和网络空间战略出发，单方面设计刑事取证管辖制度的结果。尽管本文主张在一定程度上可以采取对等回应方式抵御外来跨境刑事取证管辖并维护我国的数据主权与安全，但是冲突和对抗毕竟不是长久之计。因此，要从根本上解决各国在刑事取证管辖方面的冲突，就有必要摒弃界定数据主权的单边视角，而应当从网络空间治理的角度尽最大

〔73〕 参见前引〔28〕，梁坤文，第 155 页。
〔74〕 参见前引〔27〕，洪延青文，第 35 页。

可能寻求国际共识。

就此而论，美国学者阿迪斯的研究提供了重要启发。阿迪斯将主权的行使划分为极权主义模式、自由主义模式和程序主义模式。〔75〕前两种模式属于单边视角的界定，而程序主义主权模式将主权理解为一个关系概念，只有在相互交往的过程中才能被定义。根据这种阐释，主权概念的核心不是免于外来干涉，而是参与国际关系。〔76〕

将程序主义主权模式引申到数据主权的界定中，便可以生成“程序主义数据主权”概念。根据这一概念，一国不能采取单边视角自行界定数据主权，而应当在平等参与国际关系的基础上，与他国就数据主权是否存在、范围划定及冲突解决方案等问题，进行有效沟通和协调。在这一概念框架下，我国主张的数据主权在国际上才有可能得到更好的理解和尊重。实际上，外交部门的立场也符合程序主义数据主权的意旨。2011 年 1 月，中国代表团在参加联合国“打击网络犯罪问题政府间专家组首次会议”时提出：“从国际合作的实践看，为打击跨国性日益突出的犯罪，国内法的域外适用一方面是必要的，但因涉及主权和管辖权，也是极易引起争议的，需要各国在此方面加强协调。”〔77〕

从有效推动国际上对程序主义数据主权达成共识，并协调各国刑事取证管辖模式的立场出发，理想的方案是缔结全球性公约，对国家、侦查机关、服务提供者及相关主体的权利义务进行明确规定。然而，这一方案目前看来几无实现的可能。欧美强国极力主张将《网络犯罪公约》扩展为全球性公约，而我国对于缔结或参加这类公约所坚持的底线是，应以联合国为唯一的国际合作平台和主体。〔78〕因此，在联合国的多边平台之外，更为灵活地寻找程序主义数据主权的沟通渠道，目前看来是更为符合实际的方案。

国家间通过外交上的平等沟通，可以在就数据主权达成共识的基础上，构建刑事取证管辖的互惠模式。这种模式是对数据存储地模式和数据控制者模式的有机结合。一方面，国家间彼此认同数据存储地模式，尊重对方基于领土范围而享有对数据的原则性、排他性刑事取证管辖权。另一方面，国家间彼此让渡一部分对内数据主权，有条件地容许对方采取数据控制者模式或根据数据存储地模式的特殊例外，直接收集己方境内的数据。

实际上，刑事取证管辖的互惠模式在国际上已现雏形。有学者提出，可以效仿国家间的互免签证协议为跨境电子数据取证寻找新思路，通过双边条约的形式有条件地消除刑事司法协助程序所造成的障碍。〔79〕作为“互免签证协议”思路在跨境刑事取证管辖方面的实践，美英两国曾于 2016 年初计划签署条约，授权彼此的执法部门在严重犯罪的调查中直接要求对方境内的服务提供者披露电子数据。不过，随着“微软—爱尔兰案”法律争议的出现，美国调整了自身方案，最终呈现的是“云法”的条款安排。该法虽然宣称秉持互惠理念，但实际上是通过国内法对国际性刑事取证管辖进行规定，考虑到其对“适格外国政府”及其数据披露指令施加了非常严苛的双重限制，因此根本谈不上真正意义上的互惠。

---

〔75〕 See Adeno Addis, *The Thin State in Thick Globalism: Sovereignty in the Information Age*, 37 Vanderbilt Journal of Transnational Law 1 (2004).

〔76〕 参见刘连泰：《信息技术与主权概念》，《中外法学》2015 年第 2 期，第 517 页。

〔77〕 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》，http://www.fmprc.gov.cn/web/wjbxw_673019/t812063.shtml，2018 年 3 月 15 日最后访问。

〔78〕 参见于志刚：《缔结和参加网络犯罪公约的中国立场》，《政法论坛》2015 年第 5 期，第 98 页。

〔79〕 参见前引〔66〕，Swire 等文，第 732 页。

我国若基于程序主义数据主权构建刑事取证管辖的互惠模式，可以以“云法”规定的双向机制为参考，但绝不能照搬其实质不平等的所谓“互惠”机制，而应当与其他国家通过双边或多边平台在彼此平等、尊重的基础上实现真正意义上的互惠。当然，这就意味着我国有必要在坚持数据存储地模式并切实维护数据主权与安全的基础上，正视各国刑事取证管辖存在一定程度交织的现状，从而适度放开对内数据主权的绝对管控。为了在数据安全保障与数据适度对外共享、开放之间达成平衡，可以考虑保留适用严格的数据存储地模式以行使“关键数据主权”的权利。例如，网络安全法第 37 条强制要求关键信息基础设施的运营者在我国境内运营中收集和产生的个人信息和重要数据应当在我国境内存储。这就是通过数据的本地化存储，对特定数据进行特殊保护。即使在程序主义数据主权的框架下可以开放或让渡部分数据主权，但对于这类需要特别保护的数据，在刑事取证管辖方面，也应原则上适用数据存储地模式，坚持通过刑事司法协助程序来解决相关问题。当然，对于这类关键数据的范围，还需要我国相关法律法规作进一步的明确。

Abstract: With respect to the criminal jurisdiction over the access to data, two basic models have already been developed at the national level, i. e., the data location mode and the data controller mode. The data location mode, which is constructed on the basis of the traditional national territory, has been weakened in the field of cross-border access to data as a result of the difficulties and low efficiency in its application. In contrast, the data controller mode relies on cross-border cloud service providers, thus partially replacing the data location mode. Fundamentally speaking, the change of the mode of jurisdiction over criminal evidence collection at the international level is caused by the attempt by various states to control the domestic as well as overseas data resources for the maximization of their own national interests. Meanwhile, it should be noted that the theory of data exceptionalism has also made an important impact on the traditional mode of jurisdiction over evidence collection that applies to tangible objects. China should face up to this international trend and strive to explore the Chinese mode of jurisdiction over criminal evidence collection on the basis of national data sovereignty strategy. More specifically, firstly, we should adhere to the data location model, while at the same time making some exceptions to this mode; secondly, we should make reciprocal responses to the harms to our own interest caused by the adoption of the data controller mode by other countries while sharing the bonus of this mode to a certain extent; and thirdly, we should strengthen the equal consultation and collaboration with other countries under the conceptual framework of “procedural data sovereignty”, so as to construct a reciprocal mode of jurisdiction over criminal evidence collection applicable to data.

Key Words: electronic data, data sovereignty, evidence collection, criminal jurisdiction