网络犯罪中境外电子数据调查取证的三种模式*

谢登科

【摘　　要】在网络犯罪治理中，境外电子数据调查取证已经成为常态。境外电子数据取证除了受制于电子数据自身特征而产生的难题，还面临国家主权、属地管辖、数据跨境壁垒等制度障碍。境外电子数据调查取证有司法协助取证、直接取证和私人协助取证三种模式。司法协助取证模式有利于尊重国家主权，符合国际法的基本要求，但是存在条件苛刻、程序繁琐等问题，可能阻碍境外电子数据有效取证。直接取证模式契合了网络空间的弱地域性、开放性等特点，回应了网络犯罪治理中高效快速取证的社会需求，但是容易因侵犯他国主权而引发国际纠纷。私人协助取证模式通过网络服务提供者等私人主体协助收集境外电子数据，可使本国执法部门快速便捷获取境外电子数据，对他国主权干预较弱，但是可能因不同国家间的法律冲突而让网络服务提供者在跨境数据提供中面临法律风险。

【关 键 词】网络犯罪　境外数据　跨境取证　司法协助　网络服务提供者

【作者简介】谢登科，法学博士，吉林大学理论法学研究中心教授、博士生导师。

【中图分类号】D925.2　　【文献标识码】A

【文章编号】2097－1125（2025）03－0068－24

当今社会已经进入数字经济时代，人们的很多活动从线下物理空间转移至网络虚拟空间，这也包括违法犯罪分子实施的各种违法犯罪活动。网络犯

* 本文系黑龙江省哲学社会科学研究规划专题重点项目“涉俄刑事案件诉讼程序研究”（24FXH002）、吉林省教育厅社会科学研究重大项目“吉林省在线诉讼规则适用实证研究”（JJKH20231101SK）的阶段性成果。

罪已经成为当下最主要的犯罪形态，既包括传统犯罪的网络化、数字化，如网络诈骗、网络赌博、网络传销等，也包括各种新兴的信息网络犯罪，如侵犯公民个人信息罪、非法获取计算机信息系统数据罪等。[①] 在网络犯罪实施过程中，犯罪分子会在网络虚拟空间留下各种“痕迹”——电子数据，它们成为各类网络犯罪中认定案件事实的重要证据。在网络空间中，人们可以很容易地开展远程、跨境交流，由此生成的很多电子数据会自动存储于境外电脑、服务器等电子设备或存储介质之中。因此，在打击治理网络犯罪过程中，境外电子数据侦查取证就成为常态。由于电子数据具有虚拟性、系统性、技术性等特征，电子数据侦查取证问题本身就比较疑难、复杂。境外电子数据侦查取证除受制于电子数据自身特征而产生的各种取证难题，还面临国家主权、属地管辖等制度障碍，这就让境外电子数据侦查取证变得更为复杂。传统犯罪中的跨境取证主要是通过刑事司法协助和其他非正式取证措施完成的，这些侦查取证措施主要建立在物证、书证、证人证言等传统实物证据和言词证据基础之上，它们并不能完全适用于跨境电子数据取证。在网络犯罪治理中，跨境电子数据侦查取证的现有制度和实践运行主要存在司法协助取证、直接取证和私人协助取证三种模式，本文拟对境外电子数据调查取证的三种模式的形成机理、运行方式、各自利弊等问题进行探讨。

一、网络犯罪中境外电子数据取证的司法协助模式

刑事侦查权、起诉权、审判权都是国家主权的重要组成部分，对境外证据的侦查取证通常涉及他国主权，因此，跨境取证既要遵循国内法，也要符合国际法。根据国际法的基本要求，对境外证据的侦查取证，原则上应通过刑事司法协助方式来完成。刑事司法协助意味着对他国主权的尊重，只有经他国同意、协助，才能对该国境内的人或物进行侦查取证。若没有经过他国同意而直接在该国境内侦查取证，就可能违反国际法的不干涉原则，构成对他国主权的侵犯。对境外证据的侦查取证应当取得他国同意，该同意既可以表现为两国经平等协商签订双方条约，也可以是两国共同参加国际条约，还可以是两国在具体个案中做出刑事司法协助及互惠承诺。[②] 对网络犯罪案件的侦查取证若涉及境外证据收集，原则上也应当采取刑事司法协助方式，如欧盟《网络犯罪公约》第 31 条就要求通过刑事司法协助方式收集境外电子数据。联合国毒品和犯罪问题办公室的研究结果显示，70% 的网络犯罪调查

① 参见江溯主编：《网络刑法原理》，北京大学出版社 2022 年版，第 21 ~ 25 页。

② 如《国际刑事司法协助法》第 13 条第 2 款规定：“在没有刑事司法协助条约的情况下，请求国应当作出互惠的承诺。”

取证是通过国际刑事司法协助开展的。[①] 在有些国家，只有通过刑事司法协助方式收集的境外证据才具有证据能力，才能够在法庭上作为证据。通过刑事司法协助方式收集境外电子数据，既体现了对他国主权的尊重，也能够有效保障收集境外电子数据的证据能力。我国在全球犯罪治理中高度重视尊重国家主权原则，截至 2023 年 11 月，我国已经与 86 个国家签署了双边司法协助条约，年均办理国际刑事司法协助请求 300 余件。[②] 2020 年至 2022 年全国法院司法统计公报显示，我国法院系统在这三年中办理国际司法协助调查取证的案件数量分别为 87 件、[③] 94 件、[④] 60 件。[⑤] 协助调查取证包含物证、书证、电子数据、证人证言等不同证据，而不仅是电子数据。总体来看，跨境电子数据司法协助取证案件数量仍然不多，这与网络犯罪案件数量居高不下且逐步增多的发展趋势并不相符。这主要因为通过刑事司法协助收集境外电子数据存在诸多问题，其中有些是刑事司法协助制度及其实践的固有缺陷，有些则是电子数据自身特征引发的新兴问题。

（一）刑事司法协助制度的制约因素

通过刑事司法协助收集电子数据虽然有利于贯彻国家主权、平等互惠等基本原则，[⑥] 但是也意味着需要遵循刑事司法协助制度及其实践的诸多限制和要求，这可能阻碍网络犯罪跨境电子数据的有效取证。

首先，刑事司法协助通常需要遵循条约前置原则。国际法是国际政治的组成部分，是各国政治主张的正式反映和规范表达，而国际条约是各国根据自己意志和利益确立的特别法。[⑦] 刑事司法协助是国家与国家之间就刑事案件侦查、起诉、审判、执行等活动相互提供的帮助，它意味着将一国司法权延伸至该国领域之外，并通过他国司法机关完成相应刑事司法职能或者活动。[⑧] 刑事司法协助本身就意味着国家主权的必要延伸与合理让渡。此种延

① 参见 Anna-Maria Osula, Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data, *Masaryk University Journal of Law and Technology*, Vol. 43, 2015, p. 50。

② 参见赵婕：《司法部：加强法治建设　服务高质量发展和高水平对外开放》，《中国公证》2023 年第 12 期，第 9 页。

③ 参见《2020 年全国法院司法统计公报》，http://gongbao.court.gov.cn/Details/0bce90201fd48b967ac863bd29059b.html，2024 年 3 月 22 日。

④ 参见《2021 年全国法院司法统计公报》，http://gongbao.court.gov.cn/Details/a6c42e26948d3545aea5419fa2beaa.html，2024 年 3 月 22 日。

⑤ 参见《2022 年全国法院司法统计公报》，http://gongbao.court.gov.cn/Details/20587eaef248beb61ed6596018865c.html，2024 年 3 月 22 日。

⑥ 参见陈晖：《国际刑事司法协助理论与立法研究》，法律出版社 2023 年版，第 66～85 页。

⑦ 参见《国际公法学》编写组编：《国际公法学》，高等教育出版社 2022 年版，第 29～54 页。

⑧ 参见陈晖：《国际刑事司法协助理论与立法研究》，法律出版社 2023 年版，第 70 页。

伸和让渡必须建立在国家与国家之间平等协商、互惠互利的基础之上，国际条约就成为固定此种协商结果与合意内容的国际法律文件。被请求国向请求国提供刑事司法协助意味着被请求国自身国家主权的部分让渡，基于对等和公平原则，请求国在将来遇到类似情况时也应当给予必要协助或便利，这种互惠需要订立条约予以固定，由此产生了刑事司法协助中的条约前置原则，特别是英美法系国家在刑事司法协助中会严格遵循条约前置原则。但是，考虑到刑事司法协助具有促进司法公正、服务诉讼参与人的目的和功能，越来越多的国家对条约前置原则开始采取宽松态度，[①] 允许在没有订立条约的情况下，通过个案协商、互惠承诺等方式提供刑事司法协助。《中华人民共和国国际刑事司法协助法》（以下简称《国际刑事司法协助法》）没有采取绝对条约前置原则，而是采取了相对条约前置原则，这主要体现在《国际刑事司法协助法》第 13 条的规定中。[②] 依照该条规定，外国向我国提出刑事司法协助请求，应当按照条约规定书面提出。这暗含外国请求我国提供刑事司法协助，原则上应当已经与我国订立刑事司法协助条约。若没有订立刑事司法协助条约，请求国必须做出互惠承诺。若既没有订立条约，也不做出互惠承诺，我国通常会拒绝向请求国提供刑事司法协助。[③] 有学者认为互惠原则主要包括法律互惠与无条约互惠，[④] 前者是通过条约将互惠原则及其具体内容予以明确规定，后者是在无条约可循时，通过外交磋商方式承诺给予相应协助或者利益。基于条约前置原则的基本要求，在网络犯罪案件跨境取证中，若既没有订立条约，也无法通过磋商达成互惠承诺，就无法适用刑事司法协助方式来收集境外电子数据。

其次，刑事司法协助需要遵循双重犯罪原则。双重犯罪原则是刑事司法协助的重要条件，它要求刑事司法协助针对的行为在请求国与被请求国都应

① 参见黄风：《中华人民共和国国际刑事司法协助法立法建议稿及论证》，北京大学出版社 2012 年版，第 29 ~ 30 页。

② 《国际刑事司法协助法》第 13 条规定：“外国向中华人民共和国提出刑事司法协助请求的，应当依照刑事司法协助条约的规定提出请求书。没有条约或者条约没有规定的，应当在请求书中载明下列事项并附相关材料：（一）请求机关的名称；（二）案件性质、涉案人员基本信息及犯罪事实；（三）本案适用的法律规定；（四）请求的事项和目的；（五）请求的事项与案件之间的关联性；（六）希望请求得以执行的期限；（七）其他必要的信息或者附加的要求。在没有刑事司法协助条约的情况下，请求国应当作出互惠的承诺。请求书及所附材料应当附有中文译文。”

③ 参见王爱立主编：《中华人民共和国国际刑事司法协助法解读》，中国法制出版社 2019 年版，第 76 页。

④ 参见陈灿平编著：《国际刑事司法协助专题整理》，中国人民公安大学出版社 2007 年版，第 82 ~ 84 页。

当被认为是犯罪，此时才有可能给予刑事司法协助。[①] 若涉案行为在请求国不构成犯罪，通常不会启动刑事司法程序，刑事司法协助更无从启动；若涉案行为在被请求国不构成犯罪，也不能启动刑事司法协助，因为被请求国不能对依照本国法律属于无罪之人进行调查取证。之所以设置双重犯罪原则，是因为国家不能将追诉、惩罚犯罪的权力适用于无罪之人，在刑事司法协助中的调查取证行为就是国家权力运行的具体表现；另外，行为人在实施某种行为时，由于在其本国不构成犯罪，他通常无法预期其行为会被他国认定为犯罪。[②] 因此，境外电子数据刑事司法协助取证模式的有效运行，需要涉案行为在请求国与被请求国均构成犯罪。但是，不同国家对网络犯罪的界定及其范围的设置并不完全相同。在我国网络犯罪治理中，网络赌博是重要的犯罪类型之一，但是在有些国家或者地区，赌博行为不仅不构成犯罪，而且是合法产业。很多网络赌博违法犯罪分子为了规避我国的刑事司法追诉和惩罚，专门将赌博网站设置于境外服务器中。在此类网络赌博犯罪案件中，境外服务器存储的电子数据是认定案件事实的重要证据，但是受制于刑事司法协助中的双重犯罪原则，若境外服务器位于赌博行为合法化的国家或者地区，我国公安机关就无法通过刑事司法协助途径收集境外电子数据。又如利用网络传播淫秽物品犯罪，有些犯罪分子专门将“裸聊”网站、色情网站设置于境外服务器中，这一方面源于境外侦查取证难度较大、成本较高，另一方面则源于某些国家或者地区仅禁止未成年人登陆访问色情网站，而不禁止成年人登陆访问色情网站，向成年人传播色情图片、黄色视频等淫秽物品的行为不构成犯罪。此时，我国侦查机关想要通过刑事司法协助途径收集网络色情犯罪案件中的境外电子数据，通常也会受制于双重犯罪原则。刑事司法协助除了受到双重犯罪原则的限制，还受到“政治犯不协助”“军事犯不协助”等诸多条件的制约。[③] 在网络间谍、网络邪教言论、网络恐怖言论等网络犯罪治理中，也都可能涉及境外电子数据调查取证，若被请求国认为上述网络犯罪行为可能涉嫌政治犯罪、军事犯罪、死刑犯罪等，也无法通过刑事司法协助方式收集电子数据证据。

最后，刑事司法协助需要经过多重审批。为了保障刑事司法协助的合法性与安全性，请求国与协助国都会对刑事司法协助事项予以审查。刑事司法协助中的审查批准与国内调查取证中强制性侦查的审查批准存在较大区别，

① 《国际刑事司法协助法》第 14 条规定：“外国向中华人民共和国提出的刑事司法协助请求，有下列情形之一的，可以拒绝提供协助：（一）根据中华人民共和国法律，请求针对的行为不构成犯罪；……”

② 参见陈灿平编著：《国际刑事司法协助专题整理》，中国人民公安大学出版社 2007 年版，第 125 页。

③ 如《国际刑事司法协助法》第 14 条第 3 ~ 4 项之规定。

前者不仅需要对合法性进行司法审查，而且需要依据本国经济社会状况、外交政策等进行行政审查，从而保障刑事司法协助既符合国内法律和国际条约，也符合本国社会状况和外交政策。[①] 刑事司法协助的审查批准程序有助于保障其形式条件和实质条件得以有效遵守。例如，只有通过审查批准程序，才可以保障条约前置原则、双重犯罪原则等法定条件得到有效遵守。刑事司法协助的审批程序既包括请求国的审批程序，也包括被请求国的审批程序；既包括初步审查，也包括执行阶段的审查。有学者将此种境外电子数据的取证模式称为“倒 U 型”取证程序，[②] 这比较形象地阐述了刑事司法协助在请求国与被请求国中都需要经过多重审批的典型特征。从请求国角度看，我国公安机关在办理网络犯罪案件时，若需要通过刑事司法协助方式收集境外存储的电子数据，应当制作刑事司法协助请求书，将请求书与相关材料层报至公安部，经公安部审核同意之后，将其交给对外联系机关，由对外联系机关向外国提出刑事司法协助请求。[③] 从被请求国角度看，对外国提出的刑事司法协助请求，需要先由被请求国的对外联系机关进行初步审查，若符合法定条件和要求，则将其交由主管机关予以执行审查。初步审查应当是全面审查，主要侧重对刑事司法协助形式要件和内容要件的全面审查。执行审查是由具体负责执行工作的主管机关进行审查。设置执行审查的主要原因是刑事司法协助通常涉及很多具体刑事法律规则和标准，这些规则和标准需要由刑事司法主管机关进行审查和适用。另外，在刑事司法协助中相关行为的法律性质及其对国家利益的影响需要由主管机关在执行过程中进行动态化、深层化审查认定。[④] 由于刑事司法协助的审批程序较为复杂、繁琐，即便刑事司法协助取证的请求能够获得审批，通常也会耗费较长时间。实证数据显示，通过刑事司法协助方式收集境外电子数据，即便在审批程序比较顺利的情况下通常也需要 10 个月左右，在有些国家可能需要长达 2 年的时间。[⑤] 这显然无法有效回应信息网络时代及时、迅速打击网络犯罪的社会需求。

---

① 参见马进保：《国际犯罪与国际刑事司法协助》，法律出版社 1999 年版，第 44 ~ 47 页。

② 参见冯俊伟：《跨境电子取证制度的发展与反思》，《法学杂志》2019 年第 6 期，第 29 ~ 30 页。

③ 《国际刑事司法协助法》第 9 条规定：“办案机关需要向外国请求刑事司法协助的，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。”

④ 参见黄风：《中华人民共和国国际刑事司法协助法立法建议稿及论证》，北京大学出版社 2012 年版，第 111 ~ 113 页。

⑤ 参见 Halefom H. Abraha, Law Enforcement Access to Electronic Evidence Across Borders: Mapping Policy Approaches and Emerging Reform Initiatives, *International Journal of Law and Information Technology*, Vol. 29, 2021, p. 118.

（二）电子数据自身特征的制约因素

在数字经济时代，电子数据已经成为司法活动和诉讼程序中的“证据之王”，[①] 很多刑事案件都涉及一种或者数种电子数据。在网络犯罪治理中，境外电子数据调查取证成为现代刑事司法协助的重要内容。数据显示，每年欧盟各成员国之间关于电子数据调查取证的刑事司法协助请求约为 13000 件，欧盟各成员国与美国之间关于电子数据调查取证的刑事司法协助请求约为 1300 件。[②] 美国司法部国际事务办公室（Office of International Affairs，OIA）2017 年发布的报告显示，自 2000 年以来，外国向 OIA 请求刑事司法协助的案件数量增加了近 85%，请求电子数据调查取证的案件数量增加了 10 倍以上，OIA 的人员配置和现有资源无法适应电子数据取证刑事司法协助案件数量的快速增长。[③] 现有刑事司法协助主要针对传统实物证据和言词证据设立，不是针对在网络空间中的电子数据设立，而电子数据具有的虚拟性、流动性、系统性等特征，增加了通过刑事司法协助方式收集境外电子数据的障碍和难度。

第一，动态电子数据的流动性导致难以确定其存储地。通过刑事司法协助方式收集境外电子数据，需要确定数据存储地。网络虚拟空间中的数据需要依附电子设备、存储介质等有形物而存在。按照传统国家主权的要求，这些有形物所在国对电子设备、存储介质中的数据享有主权。[④] 但是电子数据在本质上是二进位计数制的数码 0 和 1，它们可以在网络空间中广泛传播、迅速流动，[⑤] 可以通过互联网进行快速跨境传输或者流动。有学者认为数据存储地可能与其使用地、管理地没有直接的物理空间联系，数据存储地与数据使用地可能相互分离，因此，传统的地域管辖标准无法有效适应电子数据跨境流动。[⑥] 刑事司法协助作为国家与国家之间就犯罪追诉、审判、执行展开的合作，其程序性、正式性要求都很高。在通过刑事司法协助方式收集境

① 参见刘品新：《电子证据法》，中国人民大学出版社 2021 年版，第 3 页。

② 参见 Armen Oganesean，Olga Marandici，Stefan Milicenco，et. al，Transnational Gathering of Electronic Evidences：Challenges and Perspectives in the European Union，*Revista Institutului National al Justitiei*，Vol. 62（3），2022，p. 58。

③ 参见 Miranda Rutherford，The CLOUD Act：Creating Executive Branch Monopoly over Cross-Border Data Access，*Berkeley Technology Law Journal*，Vol. 34（4），2019，p. 1182。

④ 参见吴玄：《云计算下数据跨境执法：美国云法与中国方案》，《地方立法研究》2022 年第 3 期，第 99 页。

⑤ 参见谢登科：《网络暴力犯罪自诉程序的立案证明标准反思》，《当代法学》2024 年第 3 期，第 84～94 页。

⑥ 参见 Jennifer Daskal，The Un-territoriality of Data，*Yale Law Journal*，Vol. 125（2），2015，p. 326。

外电子数据时，需要知悉电子数据存储位置及其存储介质所在国家或者地区，这样才能明确向哪国提出刑事司法协助请求。但是，动态电子数据具有流动性、分散性，其存储地可能发生变化，也可能分散存储于不同国家或地区，这就让确定电子数据存储地变得极为困难，如云存储服务的绝大多数用户都不清楚其数据存储在何处，在网络空间中的“深网”“暗网”通过常规浏览器、检索技术根本无法登陆、访问，也无法通过常规技术确定其数据存储地。[①] 在无法确定数据存储地的情况下，就无从知晓该向哪国提出刑事司法协助请求，更无法通过刑事司法协助方式收集境外电子数据。

第二，电子数据的分布式、碎片化存储，可能使在同一案件中的电子数据分散存储于不同国家或者地区。在云计算、云存储时代，既可以将数据分散存储到多个服务器中，也可以将分散、闲余的存储资源整合成虚拟存储设备，通过多台服务器分担数据存储负荷，提高数据存储能力和读取效率。[②] 云存储技术的不断兴起意味着侦查机关需要收集的境外电子数据可能并不是存储在单一服务器中，数据的访问、传输、存储等处理行为也可能不是发生于单一服务器中。[③] 从技术层面看，数据存储的分散化、碎片化有利于更好地保障数据存储的安全性，也有利于最大限度提升各种存储介质的存储效率，但是给电子数据跨境取证带来了巨大的障碍与挑战。电子数据存储的分散性、碎片化使侦查机关通过刑事司法协助方式收集境外电子数据时，即便能够确定电子数据的存储国家或地区，但是想要完整、全面收集涉案境外电子数据，就需要向数个国家或地区申请刑事司法协助取证，这不仅会导致对境外电子数据的取证程序繁琐，而且会导致在某些情况下无法成功收集境外电子数据。

第三，电子数据的系统性、海量性，可能要求在刑事司法协助中采取不同类型的调查取证措施。电子数据具有系统性特征，在电子数据侦查取证中可能涉及不同类型的数据。以电子邮件为例，在电子邮件取证中，既会涉及电子邮件的内容数据，也会涉及电子邮件的流量数据，还会涉及电子邮件的注册数据。不同类型数据承载的法益并不相同，由此决定了适用的侦查取证措施、程序保障措施并不完全相同。电子邮件的内容数据涉及公民通信秘密权、隐私权，需要对其给予严密的程序保障，通常需要采取搜查扣押方式予以收集；电子邮件的流量数据、注册数据，涉及公民个人信息权，对其程序

① 参见梁坤：《基于数据主权的国家刑事取证管辖模式》，《法学研究》2019 年第 2 期，第 191 页。

② 参见郭烁：《电信网络诈骗犯罪应对的程序性困境与完善》，《法学论坛》2023 年第 4 期，第 84 ~ 93 页。

③ 参见刘品新：《跨境电子取证的欧盟方案及启示》，《国家检察官学院学报》2022 年第 5 期，第 6 页。

保障相对宽松，通常可以采取证据调取令或者提供令方式予以收集。这些不同类型的侦查取证措施在适用于境外电子数据取证时，都有其各自不同的适用范围和运行程序。另外，从数据的完整生命周期看，电子数据在生成、传输、存储等不同环节涉及的侦查取证措施也不完全相同：在生成环节可能需要采取电子数据保护令、电子数据监控等侦查措施；在传输环节可能需要采取电子数据截取、电子数据监控等侦查措施；在存储环节可能需要采取电子数据保护令、调取令（提供令）、搜查扣押等侦查取证措施。这些不同类型的侦查取证措施，各自的运行程序、权利干预程度也并不相同。例如，跨境电子数据冻结作为新兴的证据保全措施，[①] 由于该措施本身并不会导致数据跨境传输和转移，也不会导致数据脱离既有控制和管理，它对数据主权的干预性相对较低，[②] 对其审查标准就可以适当宽松；跨境电子数据的搜查扣押作为强制性较高的侦查措施，对公民基本权利和国家主权干预程度相对较高，对其审查标准就比较严格。对境外电子数据的侦查取证可能需要综合适用不同类型的侦查取证措施，这无疑会提高境外电子数据侦查取证的复杂性，增加刑事司法协助取证的运行成本和取证难度。

第四，数据的全球化存储及其流动壁垒，提升了通过刑事司法协助方式收集境外电子数据的门槛。对信息网络公司而言，它们通常会将成本低、内存大、读取速度快、安全性高等特点作为其选择数据存储地点的重要因素，数据本地化存储在很多情况下可能不是最佳方案，数据全球化、远程化存储正逐步替代本地化存储而成为常态。随着云计算技术的兴起和发展，美国的大型信息网络企业——苹果、Google、微软等，会将其数据存储在世界各地的服务器中，而较小的公司通常会利用亚马逊网络服务（Amazon Web Services）等全球数据托管业务存储数据。[③] 从国家层面看，数据存储成本最小化、效率最大化并不是国家考虑的主要要素，国家在制定数据存储、流动制度或者政策时，需要综合考虑国家安全、社会秩序、权利保障、经济发展等因素。有不少国家为了维护本国数据安全、保护公民数据权利，可能要求数据的本地化存储，并限制数据（特别是敏感数据、重要数据）的跨境流动，对数据跨境流动设置诸多条件，[④] 如数据安全评估、个人信息保护认证等。从执法调查取证看，数据本地化存储主要具有双重功能——便利性

① 参见谢登科：《电子数据冻结：一种新兴的证据保全措施》，《东岳论丛》2023 年第 6 期，第 156～165 页。

② 参见裴炜：《论刑事跨境取证中的数据先行冻结》，《当代法学》2023 年第 2 期，第 129～130 页。

③ 参见 Miranda Rutherford, The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access, *Berkeley Technology Law Journal*, Vol. 34 (4), 2019, p. 1180。

④ 参见何渊主编：《数据法学》，北京大学出版社 2020 年版，第 178～186 页。

（facilitative）和预防性（preventive），[①] 它既可以便利本国执法部门高效、便捷收集存储于境内的相关数据，也可以阻止外国政府直接访问、收集相关数据。例如，《中华人民共和国网络安全法》（以下简称《网络安全法》）第37条对关键信息基础设施运营者在我国境内收集和产生的个人信息、重要数据提出了本地化存储的要求。[②] 2018年2月28日，苹果公司按照我国《网络安全法》的规定，将我国内地用户的iCloud密钥等数据存储于我国境内，有利于我国侦查机关向苹果公司调取其占有、管理的我国内地用户的iCloud密钥等数据。在此之前，苹果公司收集的我国用户秘钥等数据被其存储于美国境内。2013年至2017年，中国政府曾向苹果公司发出176项数据调取要求，但是无一成功。在此期间，美国政府曾向苹果公司提出8475项数据调取要求，其中成功调取2366项，中美两国待遇形成鲜明差别。[③] 虽然数据本地化存储有利于体现和保护数据主权，但是在通过刑事司法协助方式收集境外电子数据时，会因他国禁止向境外提供本地存储数据，或者对数据境外提供设置诸多苛刻条件而面临制度障碍与门槛。

二、网络犯罪中境外电子数据的直接取证模式

境外电子数据的刑事司法协助取证模式存在诸多无法克服的缺陷和弊端，网络犯罪持续增长、高发频发的态势要求各国执法部门高效、快速收集境外电子数据。有些国家尝试在部分网络犯罪案件中规避刑事司法协助方式，直接通过木马程序、黑客程序等技术方法收集境外电子数据，这就产生了跨境电子数据的直接取证模式。有学者将电子数据直接取证模式称为“单边主义”（Unilateralist approach）的电子数据取证方式，[④] 这主要源于此种境外电子数据取证模式由一国单方决定并实施，无须取得数据存储地所在国同意、协助，它在本质上是适用本国程序收集境外电子数据的。也有学者将境外

① 参见 Halefom H. Abraha, Law Enforcement Access to Electronic Evidence Across Borders: Mapping Policy Approaches and Emerging Reform Initiatives, *International Journal of Law and Information Technology*, Vol. 29 (2), 2021, pp. 118 – 153。

② 《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。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”

③ 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154～166页。

④ 参见 Halefom H. Abraha, Law Enforcement Access to Electronic Evidence Across Borders: Mapping Policy Approaches and Emerging Reform Initiatives, *International Journal of Law and Information Technology*, Vol. 29 (2), 2021, pp. 118 – 153。

电子数据直接取证模式称为“一字型”取证程序,[①] 该概念较为形象地描述了在直接取证模式中“侦查人员—境外数据”之间的关系,即侦查人员可以直接取得境外电子数据,无须借助其他主体之手。但是,该观点在界定“一字型”取证程序的主要内涵和具体类型时可能存在偏差,将“司法/执法机关之间直接合作”“请求国执法机构与网络服务提供者直接合作”也纳入“一字型”取证程序。实际上,前者并不是某国执法机关直接取得境外电子数据,仍然是借由境外执法机关之手取得境外电子数据,在本质上仍然属于电子数据跨境取证的司法协助模式,不是“倒 U 型”刑事司法协助程序,而是“接力型”刑事司法协助程序;[②] 后者也不是某国执法机关直接取得境外电子数据,而是借助网络服务提供者之手取得境外电子数据,在本质上属于境外电子数据的私人协助取证模式,本文第三部分将详细分析和阐述。

境外电子数据的直接取证模式比较契合网络空间、电子数据的弱地域性,反映了网络空间的开放性、跨境性等特点。有观点认为,在打击治理网络犯罪的过程中,跨境电子数据单方直接取证的案件数量虽然具有不确定性,但是数量很大;由于跨境直接取证没有取得数据所在地国家的同意或批准,这些案件数量通常不会做书面记录。[③] 欧盟《网络犯罪公约》第 32 条规定了对在网络上公开发布的数据和经数据权人同意的数据可以直接实施跨境取证,因为这两类境外电子数据取证对国家主权和数据权利干预性很低。网络空间具有开放性,对在网络上公开发布的信息,处于世界上任何角落的人或者组织只要能够连线上网就可以访问、下载、复制。在很多国家或地区的个人信息保护法律中,对网络上公开发布信息数据的获取通常无须取得权利主体的“知情—同意”,[④] 这主要因为自然人公开个人信息本身就意味着他人获取该

① 参见冯俊伟:《跨境电子取证制度的发展与反思》,《法学杂志》2019 年第 6 期,第 30 ~ 32 页。

② 传统刑事司法协助取证通常也需要经过不同主体审批、执行,从这个角度看,传统刑事司法协助取证也属于“接力型”取证程序,但是此种“接力”呈现先自下而上(境内)再自上而下(境外)的“倒 U 型”结构,然后再逆向流转。在互认式刑事司法协助中,如欧盟《关于刑事案件中的欧盟调查令》规定,一国签发的搜查令等证据调查令,可以直接在他国作为该国协助调查取证的依据,此时不再是“倒 U 型”刑事司法协助取证,而是“一对一”接力型刑事司法协助取证。

③ 参见 Robert J. Currie, Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the “Next Frontier”?, *Canadian Yearbook of International Law*, Vol. 54, 2017, pp. 80 – 81。

④ 例如,《中华人民共和国个人信息保护法》第 13 条规定:“符合下列情形之一的,个人信息处理者方可处理个人信息:……(六)依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;……依照本法其他有关规定,处理个人信息应当取得个人同意,但是有前款第二项至第七项规定情形的,不需取得个人同意。”

信息，信息权人愿意承担其个人信息公开、对个人信息控制减弱而带来的相关风险。[①] 在打击治理网络犯罪中，对在网络空间公开发布的信息数据，该数据无论是存储于境内服务器还是境外服务器，侦查机关都可以直接收集、获取。对获得数据权人同意的境外数据，侦查机关通常也可以直接收集。经权利人同意后直接收集相关证据，通常是刑事司法协助的替代措施，此时无须经过数据存储地所在国家同意，也可以直接收集相关证据，这和“劝返”作为引渡的非正式替代措施具有相同的正当性基础。除了《网络犯罪公约》第 32 条规定的两类数据可以适用直接取证模式，对其他类型的境外电子数据侦查取证，原则上不能适用直接取证模式予以收集。

我国最高人民法院、最高人民检察院、公安部于 2016 年发布的《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 条第 2 款规定：“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。”公安部 2018 年发布的《公安机关办理刑事案件电子数据取证规则》（以下简称《电子数据取证规则》）第 23 条将境外公开发布的电子数据纳入网络在线提取适用范围。[②]《电子数据规定》在界定网络在线提取的适用范围时，将境外存储电子数据纳入其适用范围，没有区分“公开数据”与“非公开数据”。通过网络在线提取境外公开数据对他国主权干预低，对数据权利干预性也较低，因此，符合境外电子数据直接取证的国际惯例。但是，对“非公开数据”适用网络在线提取就意味着规避了刑事司法协助而对其直接取证，由于非公开数据的国家主权属性和个人数据利益关联度较高，这很容易侵犯他国主权而引发他国抗议或国际争端。[③] 我国司法机关显然已经注意到对境外非公开电子数据适用直接取证可能引发国际纠纷与争议。《电子数据取证规则》第 23 条对境外电子数据网络在线提取的适用范围予以限缩，将其限定为境外公开发布的电子数据。[④] 该限定既符合对公开数据可以直接取证的国际惯例，也

① 参见谢登科：《公开个人信息处理中的企业合规》，《甘肃社会科学》2023 年第 5 期，第 136 页。

② 《电子数据取证规则》第 23 条规定：“对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，可以通过网络在线提取。”

③ 参见谢登科：《电子数据网络在线提取规则反思与重构》，《东方法学》2020 年第 3 期，第 96 ~ 97 页。

④ 《电子数据取证规则》第 23 条规定没有明确表述为“境外公开发布的电子数据”，但是从网络在线提取规则的发展演变以及与境内远程计算信息系统上电子数据取证的比较关系看，该条蕴含对境外电子数据的网络在线提取仅能适用于境外公开发布的电子数据之意。这虽然有利于避免侵犯他国主权而引发国际争议，但是因对国内远程计算机信息系统上电子数据的网络在线提取，没有区分“公开数据”与“非公开数据”，容易引发境内和境外电子数据网络在线提取的差别化待遇。

避免了侵犯他国主权而引发国际纠纷与争端。

境外电子数据直接取证模式能够回应对电子数据高效、快速取证的社会需求，有效因应了网络犯罪治理的治理困境。总体来看，它呈现不断扩张适用的发展态势。但是对境外电子数据的直接取证模式也容易因侵犯外国主权而引发他国抗议或国际争端，故需要对其适用范围予以严格限定，通常仅能适用于公开发布的境外电子数据或者经数据权人同意的境外电子数据。在跨国网络犯罪打击治理中，可能出现超越上述数据类型范围的直接取证，从而引发他国抗议或者国际纠纷。其中，最为经典的案例就是美国华盛顿西区联邦法院 2001 年审理的美国诉戈尔什科夫案（United States v. Gorshkov）。[①] 在该案中，美国联邦调查局在调查某黑客程序入侵美国企业计算机系统犯罪时，将俄罗斯人瓦西里·戈尔什科夫（Vasily Gorshkov）和阿列克谢·伊万诺夫（Alexey Ivanov）确定为嫌疑人。由于嫌疑人不在美国境内而是在俄罗斯，为了诱捕嫌疑人，联邦调查局在西雅图市设立 Invita 公司，并以该公司名义向嫌疑人发送招聘通知。随后戈尔什科夫与伊万诺夫来到美国，在 Invita 公司位于西雅图的办公室与联邦调查局特工见面。在此期间，戈尔什科夫应特工要求，使用联邦调查局的一台计算机演示了其黑客和计算机安全技能，通过网络远程登陆其在俄罗斯境内的计算机系统。该计算机事先被联邦调查局安装了“嗅探器”程序（一种网络监控程序），该程序自动记录了戈尔什科夫使用计算机时敲击的按键，联邦调查局由此获得了其位于俄罗斯境内的计算机系统的登陆账号和密码。美国联邦调查局使用该账号、密码远程登陆位于俄罗斯境内的该计算机系统以下载相关数据，并将数据复制、存储到光盘中。随后，美国联邦调查局向法官申请搜查令，从数据中找到涉案证据。在该案审理过程中，辩护方提出电子数据取证违反了《美国宪法第四修正案》，主张这些电子数据属于非法证据，应当予以排除。美国华盛顿西区联邦法院经审理后认为，美国联邦调查局的电子数据取证行为并不违反《美国宪法第四修正案》，故驳回了被告人申请。

在美国诉戈尔什科夫案中，美国联邦调查局无论抓捕境外犯罪嫌疑人，还是收集境外电子数据，都没有采取刑事司法协助方式，而是采取了刑事司法协助的非正式替代措施。从案件管辖权来看，由于伊万诺夫和戈尔什科夫在俄罗斯境内利用黑客程序入侵美国企业的计算机系统，美国政府根据刑事司法中的保护管辖原则，[②] 对该案拥有刑事管辖权。由于犯罪嫌疑人不在美

① 参见 United States v. Gorshkov, No. CR00 - 550C, 2001 WL 1024026。

② 保护管辖原则，指外国人在某国领域外对该国国家、公民或者组织实施的犯罪，该国刑法有权管辖。在该案中，犯罪嫌疑人通过非法手段入侵美国企业计算机系统，被害单位是美国企业，美国执法部门可以根据保护管辖原则对该案予以立案侦查。

国境内而是在俄罗斯，按照正常处理方式，美国政府应当向俄罗斯申请引渡这两名犯罪嫌疑人。但是，引渡的条件苛刻、程序复杂，它需要遵循互惠原则、条约前置主义、双重犯罪原则，并且受到死刑不引渡、政治犯不引渡、本国国民不引渡等诸多条件限制。按照上述条件和程序的限制，美国政府基本上不可能将上述两名犯罪嫌疑人引渡至美国进行追诉、审判。除了引渡，还有很多引渡的非正式替代措施实现对境外被追诉人的控制、抓捕，从而将其转移至本国追诉、审判、执行刑罚，既包括合法的引渡替代措施，如非法移民遣返、异地追诉、劝返等，也包括非法的引渡替代措施，如诱捕、绑架等。① 美国联邦调查局采取了非法的引渡替代措施——诱捕，来抓捕两名犯罪嫌疑人，这是美国政府在无法引渡情况下的惯用替代措施，美国政府也曾通过诱捕方式对中国公民袁某、宪某实施抓捕。② 即使是对其西方盟国，美国在无法成功引渡犯罪嫌疑人的情况下，通常也会采取诱捕方式将其抓获。在某贩卖毒品案件中，因无法成功引渡嫌疑人，美国缉毒局（Drug Enforcement Administration，DEA）在没有取得加拿大政府同意的情况下，在加拿大境内实施诱捕行动，由此导致加拿大和美国关系紧张。③ 诱捕作为引渡的非法替代措施，既因通过虚构事实、隐瞒真相而让犯罪嫌疑人陷入错误认识，违背了犯罪嫌疑人的自由意志，也因违反国际法中平等互惠、尊重主权原则而不具有合法性。基于国家主权原则，一国政府有权管理其境内的人和物，若未经该国政府同意就直接将其境内的人或物转移至境外，就会让其脱离该国政府管理，从而构成对该国主权的侵犯。

在境外电子数据调查取证中，存储地所在国通常对数据及其存储介质享有主权，若对境外公开数据或经数据主体同意提供的数据之外的其他数据直接进行调查取证，就很容易侵犯他国主权和他国公民数据权利。在该案中，被告人戈尔什科夫就以境外电子数据违反《美国宪法第四修正案》为由，主张该电子数据应当作为非法证据予以排除。对非法电子数据予以排除是对侦查机关违法收集电子数据的程序性制裁措施。④ 但是美国华盛顿西区联邦法院经审理后认为，《美国宪法第四修正案》不适用于对俄罗斯境内计算机

① 参见张磊：《国际刑事司法协助热点问题研究》，中国人民公安大学出版社 2012 年版，第 3～9 页。

② 参见张磊：《国际刑事司法协助热点问题研究》，中国人民公安大学出版社 2012 年版，第 39～67 页。

③ 参见 Robert J. Currie，Cross-Border Evidence Gathering in Transnational Criminal Investigation：Is the Microsoft Ireland Case the "Next Frontier"?，*Canadian Yearbook of International Law*，Vol. 54，2017，p. 73。

④ 参见谢登科：《非法电子数据排除的理论基点与制度建构：以数字权利的程序性救济为视角》，《上海政法学院学报（法治论丛）》2023 年第 3 期，第 79 页。

系统的境外访问以及对其中存储数据的下载、复制。一方面，俄罗斯境内的计算机系统不受《美国宪法第四修正案》保护，它们不是美国公民的财产，并且位于美国领土之外；另一方面，从俄罗斯境内电脑系统下载、复制数据的行为不属于《美国宪法第四修正案》规定的搜查扣押行为，因为该行为没有干预被告人或者其他人对数据的占有利益，数据完整性没有改变，被告人以及其他共享访问权限的用户仍然可以访问、使用这些数据。① 该判决承认了美国执法部门有权通过网络在线方式直接收集境外电脑系统中存储的电子数据，但是认为此种行为不属于搜查扣押，不受《美国宪法第四修正案》调整和规制。该案裁判逻辑充满“双标”，既存在对他国主权的无视与侵犯，也存在对他国涉案人员基本权利的偏见与践踏。

其一，在电子数据跨境取证中，首先应当解决执法部门是否有权对境外电子数据直接取证的问题。由于跨境取证涉及他国主权，通常需要采取刑事司法协助方式收集境外证据。一国在没有取得他国同意的情况下，直接在他国境内取证或者对他国境内物品、数据、人员等取证，通常会因侵犯他国主权而引发国际争议和纠纷。在美国诉戈尔什科夫案的判决做出后，俄罗斯向美国提出严重抗议，认为美国执法部门诱捕俄罗斯人、直接收集俄罗斯境内电脑系统中存储数据的行为，严重侵犯俄罗斯国家主权。② 刑事司法协助需要基于两国之间经平等协商签订或者共同参加的国际条约。在欠缺刑事司法协助条约的情况下，既不能由美国法官签发搜查令直接搜查扣押位于他国境内的数据，也不能由美国联邦基层法院直接确认跨境远程取证的合法性。刑事司法协助在本质上是国家司法权力在本国领土以外的必要延伸，是国家主权的具体表现形式之一，各主权国家才是刑事司法协助的适格主体，有权代表国家开展刑事司法协助的主体是经过国家授权的外交机关或者司法机关，其他组织或者个人不能以自己的名义对他国进行刑事司法协助。③ 在美国诉戈尔什科夫案中，电子数据跨境搜查扣押会干涉或者侵犯他国主权，不能由美国联邦基层法院通过签发搜查令的方式直接授权本国执法人员对境外数据进行取证，而应当通过刑事司法协助方式予以收集。在刑事司法协助中，治安法官签发搜查令仅是刑事司法协助中请求国内部开展的诉讼活动之一，治安法官无权代表美国政府向他国申请刑事司法协助。签发搜查令后，也不能由本国执法人员直接对境外数据予以搜查扣押，而需要经由请求国、被请求

① 参见 United States v. Gorshkov, No. CR00 – 550C, 2001 WL 1024026。

② 参见 Robert J. Currie, Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the “Next Frontier”?, *Canadian Yearbook of International Law*, Vol. 54, 2017, p. 77。

③ 参见陈晖：《国际刑事司法协助理论与立法研究》，法律出版社 2023 年版，第 22 页。

国各自审批之后，由数据所在地国（即被请求国）的执法部门收集。在该案中，美国执法部门直接收集存储于俄罗斯境内的电子数据，属于违法取证行为，已经构成对他国主权的严重侵犯。

其二，对外国公民在本国追究刑事责任的法律适用问题，即外国公民能否适用《美国宪法第四修正案》。该案判决认为，由于被告人戈尔什科夫是俄罗斯人，而不是美国公民，故对其不能适用《美国宪法第四修正案》。该观点主要源于美国联邦最高法院 1990 年在凡尔都戈 - 乌尔基德（Verdugo-Urquidez）案中的裁判结果。被告人凡尔都戈 - 乌尔基德是墨西哥毒枭，不是美国公民。美国执法部门在加利福尼亚州将其抓捕，并在没有取得搜查证的情况下搜查其位于墨西哥的住宅。被告人凡尔都戈 - 乌尔基德认为该搜查行为违反了《美国宪法第四修正案》，并主张在无证搜查中获取的证据属于非法证据，应当予以排除。地区法院和联邦第九巡回法院都裁定搜查行为违反《美国宪法第四修正案》。但是，美国联邦最高法院经过审理后以 5∶4 的投票结果撤销原判，认为被告人凡尔都戈 - 乌尔基德不是美国公民，也没有与美国建立充分联系，并且该搜查行为发生于美国境外，故不应受到《美国宪法第四修正案》保护。[①] 该观点显然不符合国际通行惯例。一般来说，在本国境内对外国人侦查、起诉、审判时，通常需要适用本国刑事诉讼法以及相关法律来追究其刑事责任，[②] 这是国家主权原则在刑事诉讼中的基本要求和必然体现。在本国境内追诉外国人时，若对外国人适用其所在国家的刑事诉讼法，就意味着他国法律在本国境内的适用，即他国法律适用范围延伸至本国境内，这会对本国主权构成侵犯，因此，在本国境内对外国人予以追诉、审判时，通常需要适用本国刑事诉讼法及其相关法律。在美国诉戈尔什科夫案中，美国司法机关出于保护国家主权之考虑，没有对被告人戈尔什科夫适用俄罗斯的相关法律，这体现了对美国国家主权的保护。但是，美国联邦法院在判决中同时认为被告人戈尔什科夫也不受《美国宪法第四修正案》的保护，这就意味着被告人的基本权利在电子数据跨境取证中处于“双不管”状况——他既无法受到美国法律保护，也不能受到俄罗斯法律保护，这就可能造成电子数据跨境取证的“宪法黑洞”，[③] 显然与基本权利保障的现代法治精神相背离。但是，若对被告人戈尔什科夫适用《美国宪法第四修正案》，可能就意味

① 参见 Jennifer Daskal, The Un-territoriality of Data, *Yale Law Journal*, Vol. 125 (2), 2015, pp. 337 - 344。

② 例如，《中华人民共和国刑事诉讼法》第 17 条第 1 款规定：“对于外国人犯罪应当追究刑事责任的，适用本法的规定。”

③ 参见 Halefom H. Abraha, Law Enforcement Access to Electronic Evidence Across Borders: Mapping Policy Approaches and Emerging Reform Initiatives, *International Journal of Law and Information Technology*, Vol. 29 (2), 2021, pp. 118 - 153。

着该宪法条款的域外适用，将其法律效力延伸至发生于美国境外的电子数据搜查扣押行为，这就可能构成对他国主权侵犯。此时就产生了“宪法黑洞”与宪法境外适用的选择困境，此种困境产生的重要原因就在于对境外电子数据直接进行搜查扣押，而不是通过刑事司法协助方式予以收集。

其三，对在境外电脑系统中存储数据的远程取证是否属于搜查扣押的问题。美国华盛顿西区联邦法院认为对境外电脑系统中电子数据的远程取证不属于搜查扣押，也不受《美国宪法第四修正案》调整和规制。仅从表面看，戈尔什科夫在美国境内使用的计算机并不是他本人的计算机，而是美国联邦调查局的计算机，被告人对该计算机并不享有所有权。美国执法人员通过该计算机远程登陆、获取位于俄罗斯境内的计算机系统中的电子数据，似乎没有侵犯戈尔什科夫的基本权利。但是，美国联邦最高法院于 1968 年在卡兹案（Katz v. United States）中对搜查扣押的认定就由“财产权侵害”标准转向了“隐私权侵害”标准。被告人戈尔什科夫对其在俄罗斯境内的计算机系统设置了账号、密码，这本身就体现出其中相关信息数据的私密性。美国执法人员用技术手段秘密窃取了被告人的账号、密码，并远程登陆、复制该计算机系统中的相关数据，已经侵犯或者干预了被告人戈尔什科夫的隐私权，故该行为构成搜查。美国执法部门在获取数据之后，又申请获得搜查令，这本身就可以逆向推导得出美国执法人员对俄罗斯境内计算机系统中数据的取证行为属于搜查，但是事后取得搜查证无法补救事前违法搜查的违法性。另外，将电子数据下载、复制至其他存储介质中，并对该存储介质予以“扣押”的行为，是否构成电子数据扣押？在美国诉戈尔什科夫案中，美国华盛顿西区联邦法院认为，从被告人计算机系统中远程下载、复制数据的行为，不属于《美国宪法第四修正案》规定的扣押，因为它没有干涉被告人或其他人对数据的占有利益（possessory interest），该数据的完整性并没有因为下载、复制而发生变化，被告人仍然可以访问、使用、处理这些数据，复制数据不会影响被告人的占有权利（possessory right）。因此，侦查人员下载、复制数据的行为不构成扣押。该观点主要是以传统有形物占有来认定是否构成扣押，仅从形式上分析了下载、复制数据行为不构成扣押。将扣押纳入正当程序控制之中，主要为了保障权利人对被扣押物的排他性占有利益。[①] 占有利益的核心在于排他性，数据具有可复制性，他人复制、下载数据，虽然不会影响对数据的占有、使用，但是会减损数据的排他性利益，这意味着数据主体需要和他人分享或共享数据占有利益，从而降低数据占有利益的

① 参见 Susan W. Brenner and Barbara A. Frederikse, Computer Searches and Seizures: Some Unresolved Issues, *Michigan Telecommunications and Technology Law Review*, Vol. 8, 2001, pp. 39 – 114。

排他性，也会干预或侵害数据承载的隐私利益。从这个角度看，需要将下载、复制承载个人隐私利益数据的行为纳入扣押范围。但是，美国华盛顿西区联邦法院以该行为不属于扣押为由，对该案拒绝适用《美国宪法第四修正案》，导致被告人的权利在跨境电子数据搜查扣押中无法得到正当程序保障和救济。

在德国刑事司法中，曾经发生过类似的跨境电子数据直接取证案例，但是德国司法机关做出了与美国联邦法院截然不同的裁判结果。该案申诉人是美国众达（Jones Day）律师事务所，该律师事务所在德国慕尼黑设有办事处。众达律师事务所曾为大众汽车公司提供法律服务。2017 年 3 月，德国慕尼黑第二检察院对大众汽车公司及其员工涉嫌诈骗案件进行侦查，并从治安法官处获得搜查令后，对作为第三人的众达律师事务所慕尼黑办事处进行突击搜查，该律师事务所的网站服务器及相关数据存储于布鲁塞尔。德国执法部门无视众达律师事务所的强烈抗议，通过慕尼黑办事处的计算机远程登陆、复制位于布鲁塞尔服务器中的电子数据。众达律师事务所就该搜查令及其直接跨境执行向德国慕尼黑第一地区法院提出申诉。德国慕尼黑第一地区法院于 2017 年 6 月 7 日做出裁定认为，根据欧盟《网络犯罪公约》的规定，对境外电子数据，只有在数据系公开发布或者取得数据权主体同意的情况下，才可以跨境远程直接取证，否则就需要通过刑事司法协助方式予以收集。德国执法部门在搜查前，没有向比利时政府发出欧洲调查令（European Investigation Order，EIO）或者刑事司法协助请求，就直接从德国远程登陆、访问、下载、复制位于比利时境内服务器中存储的电子数据，属于在境外非法行使管辖权，取证行为违法。故法院裁定将比利时境内服务器下载的电子数据返还给众达律师事务所，并销毁该电子数据副本。[①] 该案涉及的法律问题比较复杂，既涉及境外电子数据直接取证，也存在律师拒证权问题。[②] 德国慕尼黑第一地区法院在该案裁判中恪守欧盟《网络犯罪公约》的规定，将境外电子数据直接取证的适用范围限定于公开发布或者经取得数据权主体同意的数据，对其他类型数据则不能适用直接取证模式，而应当通过刑事司法协助方式予以收集。但是，有观点认为此种恪守传统刑事司法协助制度的裁判逻辑，不利于境外电子数据及时、迅速取证，特别是处理某些具有紧迫性的恐怖活动犯罪案件。[③] 正是因为回应高效

① 参见 Den Beschluss des Landgerichts München I vom 6. Juni 2017 – 6 Qs 5/17, 6 Qs 6/17。

② 《德国刑事诉讼法》第 53 条赋予被告人辩护人、律师、法律顾问等特定职业人员拒证权下，主要是为了保护特定职业人员与其客户之间的信赖关系，在违反拒证权制度的情况，可能会导致证据被认定为非法证据而予以排除。参见林钰雄、王士帆、连孟琦：《德国刑事诉讼法注释书》，台湾新学林出版股份有限公司 2023 年版，第 217 页。

③ 参见 Nathalie A. Smuha, Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights and Consistency, *European Criminal Law Review*, Vol. 8, 2018, pp. 95 – 96。

打击治理网络犯罪的社会需求，有些执法人员可能会在实践中突破刑事司法协助制度框架，通过远程搜查、远程勘验、网络在线提取等方式直接收集境外电子数据。但是，需要对境外电子数据直接取证模式的适用范围予以适当限定，否则就会侵犯他国主权而引发国际纠纷，也可能违法取证导致相应电子数据被认定为非法证据。

三、网络犯罪中境外电子数据取证的私人协助模式

在数字经济时代，网络服务提供者等第三方主体的科技研发和经营活动大幅降低了人们利用信息网络实施各种行为的技术成本和准入门槛，他们在为人们提供信息网络服务时，也占有、控制了人们在网络空间实施相关活动的海量“痕迹”数据。向网络服务提供者等第三方主体收集、获取电子数据，成为数字经济时代常见的侦查取证措施，包括数据提供令、第三人搜查、数据调取令等侦查措施。正如美国科尔教授所言：“绝大多数网络犯罪的侦查取证，都始于从网络服务提供者处调取其存储数据。”① 欧盟《网络犯罪公约》第 18 条规定了数据提供令制度。联合国《打击网络犯罪公约(草案)》第 27 条也规定了数据提供令制度。《中华人民共和国刑事诉讼法》虽然没有规定电子数据提供令制度，但是规定了证据调取制度。② 证据调取在本质上属于双方行为：侦查机关在知悉有关组织或者个人占有、控制相关证据时，通知该组织或者个人交出证据；该组织或者个人在收到证据调取通知后，将其占有、控制的证据提交给侦查机关。③ 电子数据调取的概念主要着眼于电子数据的取证方，而不是电子数据调取的相对方——网络服务提供者等第三方主体，但是完成电子数据调取需要第三方主体的配合。电子数据提供令主要着眼于电子数据取证相对方——第三人，数据提供仅是手段或方法，其最终目的是让侦查人员获取相关电子数据。因此，电子数据调取在本质上是“中国式电子数据提供令”。

境外电子数据的刑事司法协助取证模式是建立在国家与国家经协商并同意基础之上的、由数据所在国协助收集电子数据的取证模式。境外电子数据的直接取证模式则是由一国执法人员通过网络远程操作直接收集位于境外的

① Orin S. Kerr, Digital Evidence and the New Criminal Procedure, *Columbia Law Review*, Vol. 105, 2005, p. 309.

② 《中华人民共和国刑事诉讼法》第 54 条第 1 款规定：“人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。”

③ 参见谢登科：《论侦查机关电子数据调取权及其程序控制——以〈数据安全法（草案）〉第 32 条为视角》，《环球法律评论》2021 年第 1 期，第 55～56 页。

电子数据，在取证过程中通常没有他国或第三方协助。向网络服务提供者调取电子数据，与刑事司法协助取证、直接取证两种模式存在本质差别，它是对境外电子数据的第三种取证模式，在本质上是借助私人主体协助来收集境外电子数据。与刑事司法协助取证相比，境外数据调取通常也需要第三方主体的协助与配合，但是这里的配合并不是国家与国家之间开展的刑事司法协助与配合，而是国家与私人之间的协助与配合，网络服务提供者等第三方私主体的协助、配合，通常体现为国内立法的相关法定义务，即第三方主体应当按照法律规定或者令状要求提供其占有、控制的境外相关数据。向网络服务提供者直接调取电子数据，通常也无须他国政府提供协助。从这个角度看，也可以将向网络服务提供者调取境外电子数据归为境外电子数据直接取证模式。但是，此种取证模式与严格意义上的境外电子数据直接取证也存在差别，境外电子数据调取不是由侦查机关直接采取相关措施取得境外数据，而是借助网络服务提供者等第三方主体的提交行为来取得电子数据。无论是执法部门自行直接收集境外电子数据，还是向网络服务提供商调取境外电子数据，二者都可以让本国执法部门快速、便捷地获取相关涉案数据，但是前者主要是执法部门自己直接实施证据收集行为，后者是借助网络服务提供者等第三方主体的证据提供行为。由于境外电子数据直接取证模式是由本国执法部门直接收集位于境外的电子数据，本国执法部门在没有取得他国同意的情况下直接获得位于他国境内的电子数据，在直接收集数据的过程中将本国主权延伸至他国境内，很容易侵犯他国主权而引发国际纠纷与争议。向网络服务提供者等第三方主体调取境外电子数据，并不是本国执法部门直接采取相关措施来收集境外数据，而是由网络服务提供商将其占有、控制的境外数据提供给本国执法部门。提供令的法律效力通常限于本国境内的网络服务提供者，在此过程中，直接获取境外数据的行为并不是本国执法部门实施的，而是由对境外数据享有登陆、访问、管理、处理等权限的网络服务提供者等第三方主体实施的。因此，相较境外电子数据的直接取证模式，向网络服务提供者调取境外数据对他国主权的干预或侵犯相对较弱。

虽然向网络服务提供者等第三方主体调取境外电子数据对他国主权的干预或者侵犯相对较低，但是并不意味着完全不会侵犯他国主权。很多国家在对待境外电子数据调取问题上，通常处于言行不一、相互矛盾的状态。各国通常一方面对他国执法部门向网络服务提供者调取存储于本国的数据持保守态度，另一方面对本国执法部门向网络服务提供者调取位于他国境内的数据持开放态度。[①] 从数据调取制度

① 参见 Robert J. Currie, Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?, *Canadian Yearbook of International Law*, Vol. 54, 2017, pp. 78 – 79。

的发展历程看，数据提供令或者调取令制度适用于本国境内存储电子数据通常并无争议，但是能否适用于境外存储数据的收集取证，则存在较大争议。例如，美国联邦最高法院审理的微软案（Microsoft Corp. v. United States）就存在该争议。2013 年，美国纽约州执法人员在调查某毒品犯罪案件时，根据美国《通信存储法》（the Stored Communications Act，SCA）之规定，[①] 向联邦地区法院申请搜查令，要求微软公司提供一名用户的电子邮件相关数据。但是，微软公司仅提供了存储于美国境内的部分数据，对其他数据则以数据存储于爱尔兰、不属于搜查令效力范围之内为由拒绝提供。随后，微软公司向法院申请撤销搜查令，但是治安法官、地方法院都驳回了微软公司的撤销申请，主要理由是虽然数据存储于爱尔兰，但是该数据处于微软公司控制、管理之下，微软公司注册地在美国境内，搜查令对微软公司具有法律约束力，它应按照搜查令将涉案数据提交给执法人员。微软公司不服，提出上诉。美国联邦第二巡回法院经审理后认为，美国《通信存储法》没有将其法律效力延伸至境外存储的数据，治安法官签发的搜查令不具有域外效力，要想获得境外存储数据就需要通过刑事司法协助途径予以收集。该案改判的重要因素之一就是包括爱尔兰政府在内的诸多组织出具“法庭之友”意见书支持微软公司，爱尔兰政府强调不接受他国司法程序对本国主权的侵害或减损，对相关电子数据的调取应当通过刑事司法协助方式完成。[②] 美国政府对该判决结果不服，提出上诉。在美国联邦最高法院审理过程中，美国国会于 2018 年 3 月通过《澄清合法使用境外数据法》（The Clarifying Lawful Overseas Use of Data Act，CLOUD Act，以下简称“云法”），规定网络服务商有义务提供其境外存储的相关数据，这就解决了微软案的相关法律问题。在“云法”通过后，美国联邦最高法院认为该案审理已无实际意义，故终止了该案审判程序。[③]

在境外存储数据的调取或提供问题上，美国“云法”并没有将其法律效力局限于境内存储的数据，其效力已经延伸至境外存储数据。根据“云

① SCA 是由美国国会 1986 年制定通过的，该法赋予电信服务商对其用户注册信息、通信流量信息、通信内容信息等数据的存储义务，并有义务向执法部门提供其存储的上述信息。但是，SCA 根据不同信息类型及其私密程度差异，要求执法部门履行不同程序。对流量信息数据需要通过提供令方式予以收集，对内容信息数据需要通过搜查令方式予以收集。但是，SCA 仅规定了美国境内存储通信数据的取证，没有规定境外存储数据的调取。随着云存储、云计算等信息网络技术的不断兴起，电信服务提供商、网络服务提供商将上述数据存储于境外成为常态。

② 参见裴炜：《数字正当程序：网络时代的刑事诉讼》，中国法制出版社 2021 年版，第 67～68 页。

③ 参见 Miranda Rutherford，The CLOUD Act：Creating Executive Branch Monopoly over Cross-Border Data Access，*Berkeley Technology Law Journal*，Vol. 34（4），2019，pp. 1177－1180。

法”的规定，网络服务提供商有义务存储、备份、披露其占有或者管理的用户注册身份信息、流量信息、通信内容信息等数据，无论这些数据存储于美国境内还是境外。对境内存储的数据，美国执法部门在处理刑事案件时固然可以通过提供令、搜查令来向网络服务提供者进行调取；对境外存储的数据，若网络服务提供者位于美国境内，或者向美国境内组织、个人提供了通信服务，根据“云法”的规定，美国执法部门也可以通过提供令、搜查令向网络服务提供者调取相关数据。美国“云法”的颁布实施扩张了提供令、搜查令的法律效力，实现了从数据存储地标准向数据控制者标准的变革，改变了对境外存储数据的调查取证模式。数据控制者标准将数据控制者作为确立法律管辖权的重要依据，扩张了物理空间的主权管辖范围，突出了在数据流动中产生的诸多管辖权关联点，强化了数据的属人管辖因素。[①] 美国“云法”的出台主要为了解决在网络犯罪案件中通过刑事司法协助途径收集境外电子数据效率低下、程序繁琐的问题。当然，美国“云法”并不能完全替代刑事司法协助取证，后者在境外电子数据收集中仍然可以适用，但是“云法”可以大幅降低在境外电子数据取证中刑事司法协助请求的数量。“云法”不仅允许美国执法部门直接向位于美国境内的通信服务商调取涉案数据，而且允许其他国家直接向位于美国境内的通信服务商调取涉案数据，前提是其他国家已经与美国政府签订执行协议，这就要求其他国家建立完善的隐私保护、公民自由和基本权利保护制度。仅从表面看，“云法”似乎体现了国际法中的平等互惠原则，它既允许美国执法部门向通信服务者调取存储于他国境内的数据，也允许他国执法部门向通信服务者调取存储于美国境内的数据。但是这种“互惠”是相对的，[②]“云法”对他国执法部门获取美国境内数据设置了诸多不对等条件，由此体现了在跨境电子数据取证中的美国利益优先。

按照数据控制者标准，若通信服务提供者受某国法律管辖，该国执法部门在调查取证中，不仅可以调取其存储于境内的数据，而且可以调取其存储于境外的数据。但是，这可能让网络服务者在不同国家之间的法律冲突中面临两难选择困境。例如，按照美国“云法”的规定，苹果公司应当向美国执法部门提供其存储于欧盟境内的个人信息数据，但是根据欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）第 48 条之规定，[③]

① 参见夏燕、沈天月：《美国 CLOUD 法案的实践及其启示》，《中国社会科学院研究生院学报》2019 年第 5 期，第 110 页。

② 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 154～156 页。

③ 参见京东法律研究院：《欧盟数据宪章：〈一般数据保护条例〉GDPR 评述及实务指引》，法律出版社 2018 年版，第 30 页。

此时仍然需要以达成的刑事司法协助条约为基础。若按照美国“云法”确立的数据控制者标准，通信服务商有义务将其存储于欧盟境内的相关数据直接提供给美国执法部门。但是，从数据存储地国看，该数据提供行为属于典型的数据境外流动（将境内数据提供给境外组织或人员），这就涉及数据所在地国主权和数据权利保障问题。未经他国允许，直接将存储于该国境内的相关数据提供给美国执法部门，虽然便利了美国执法部门调查取证，但是会侵犯他国主权，也不利于他国公民的数据权利保障，因为数据跨境流动对自然人权益产生重大影响，它会导致对个人数据的监管场域、法律适用、维权成本等方面的巨大变化，造成自然人对个人数据控制弱化、维权难度和成本上升等不利后果。[①] 在微软案中，美国联邦第二巡回法院改判支持微软公司的重要原因就是爱尔兰政府主张直接调取数据会侵害或减损其国家主权。但是，按照“云法”的规定，美国境内网络服务提供者需要将其在境外存储的数据按照提供令或搜查令要求向执法部门提交涉案数据。这虽然有利于美国执法部门高效、快速收集境外电子数据，但是容易引发国际纠纷与争议，也会让企业在数据跨境流动中面临合规困境。

从世界范围看，为了有效打击治理网络犯罪，越来越多的国家允许通过提供令、搜查令制度向通信服务提供者收集其境外存储数据，如英国、比利时、葡萄牙、塞尔维亚、新加坡等国家。[②] 在 2007 年的 eBay Canada Ltd. v. Canada（National Revenue）案中，加拿大税务执法部门根据其税收法规，在取得法官签发的提供令后，要求 eBay 公司提交与税务评估相关的电子数据，这些数据并没有存储于加拿大，而是存储在美国加利福尼亚州的服务器中。eBay 公司向法院申请撤销提供令，主要理由是数据并非存储于加拿大，该提供令对境外存储数据不具有管辖权。但是，加拿大两级法院都没有采纳 eBay 公司的观点，认为提供令对拥有或者控制数据的人具有管辖权，而 eBay 公司在加拿大境内的员工是管理这些数据的主体，能够很迅速地获取境外存储数据。2015 年，比利时最高法院在比利时诉雅虎（Belgium v. Yahoo）案中做出了类似裁判结果。比利时刑事执法部门在侦查某网络诈骗案件时，在取得法官签发的提供令后，要求雅虎（Yahoo）公司提供与某电子邮件账户相关的 IP 地址。但是，雅虎公司拒绝提供，主要理由是雅虎公司在比利时没有开展业务，该公司在比利时没有网络基础设施，相关数据

① 参见谢登科：《个人信息跨境提供中的企业合规》，《法学论坛》2023 年第 1 期，第 85 ~ 94 页。

② 参见 Robert J. Currie, Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the “Next Frontier”?, *Canadian Yearbook of International Law*, Vol. 54, 2017, pp. 81 – 82。

不是存储于比利时境内，若要收集相关数据，应通过刑事司法协助方式向数据存储地所在国提出请求。比利时最高法院经审理后没有采纳雅虎公司的观点，主要理由是雅虎公司为比利时公民提供了电子邮件服务，比利时执法部门可以根据属地原则享有管辖权，雅虎公司应当向比利时执法部门提供其掌握的相关数据。[①] 但是也有很多国家仍然将数据调取范围限定为境内存储的数据。例如，根据《网络犯罪公约》第31条之规定，对网络服务提供者存储于境外的数据，仅能通过刑事司法协助方式获得。有学者将无法通过提供令从网络服务提供者处收集境外存储数据视为《网络犯罪公约》的立法漏洞，[②] 该观点不无可商榷之处。对境外存储电子数据的调查取证本身就涉及他国主权，数据提供令属于干预程度较高的强制性侦查，即便网络服务提供者在技术层面能够管理、控制境外存储的数据，侦查机关也不能通过提供令来要求网络服务提供者提交其占有、管理的各种不同类型数据，否则就意味着将数据提供令的法律效力延伸至境外，此时就很容易因侵犯他国主权而引发国际纠纷或者争议。

四、结语

跨境电子数据取证是世界各国在网络犯罪治理中面临的共同难题，在实践中主要有司法协助取证、直接取证和私人协助取证三种模式，它们各具优长，也各存短板。我国现有的制度规则和司法实践也有这三种模式。在网络犯罪打击治理中，对跨境电子数据的调查取证需要根据具体情况适用不同取证模式。跨境电子数据取证的三种模式也有需要发展完善之处。对刑事司法协助取证模式，需要适当放宽适用条件、简化审批程序，利用信息技术建立不同国家或者地区间的刑事司法协助调查取证网络平台，提高刑事司法协助取证模式的运行效率。对直接取证模式，需要严格限定其适用条件和范围，其适用应当以不侵犯他国主权为前提条件，这就要求对其适用对象和范围予以限定，通常仅能适用于网络空间中公开发布的电子数据或者经数据权利主体自愿同意提供的电子数据，对其他类型的境外电子数据，则不宜适用直接取证模式。对私人协助取证模式，需要不同国家或者地区展开协商，消除不同国家或者地区间数据跨境流动的制度差异和壁垒，降低网络服务提供者在数据跨境提供中的合规风险。

（责任编辑：方　军）

① 参见 Robert J. Currie, Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?, *Canadian Yearbook of International Law*, Vol. 54, 2017, pp. 85 – 87。

② 参见李彦：《打击跨国网络犯罪国际法问题研究》，中国法制出版社2021年版，第150页。