中国数据跨境调取路径探析

——以数据相关主体和存储路径为视角

魏求月*

摘　要：特定情况下的数据跨境调取需要在传统的司法互助协定方式基础上补充其他路径。中国在坚持以双边司法互助协定和互惠原则为主要方式的基础上，应从国家安全和个人信息保护两个角度出发，探索更多灵活、便捷的数据跨境调取路径。从数据相关主体角度，当数据请求国拥有合法司法管辖权且获取数据对请求国审理司法案件具有利益时，或数据请求国对数据主体拥有属人管辖权且仅就该主体数据向中国提出请求时，中国原则上应允许调取数据。从数据存储路径角度，当仅在“完全数据本地云”模式下，中国作为数据存储地国时，才有必要结合数据请求国类型对他国数据请求进行实质审查，而在其他存储模式中，则应尊重先前的中立技术手段安排或允许在先存在的信托协议，由此排除部分不需要中国数据主管机关开展实质审查的数据调取请求，实现提高数据跨境调取效率、减轻审查压力、有效推进跨国司法审判的目的。

关键词：数据调取　个人信息保护　数据主权　数据存储　数据信托

数据跨境调取作为数据跨境流动的重要内容，在《“十四五”数字经济发展规划》中被定位为提升中国数据安全保障水平的关键环节。在行政执法和刑事司法领域，信息技术的广泛应用使得证据材料普遍以电子数据的形式存在。但不论是在行政执法还是刑事司法领域，[①] 数据跨境调取均主要由两个场景组成：一是本国执法所需的数据存储于国外；二是外国执法部门需要调取存储于本国的数据。本文立足于行政执法与刑事司法过程中的数据跨境调取路径进行探索。目前主权国家司法过程中的数据跨境调取仍旧以司法互助协定及其所涵盖的互惠原则为主，程序复杂且地域范围有限，尤其是被请求国对他国数据跨境调取请求的合理性判断标准模糊。目前，国内外

---

* 魏求月，北京理工大学法学院智能科技风险法律防控工信部重点实验室研究员。本文是司法部法治建设与法学理论研究部级科研项目“中美跨境数据流动的规则博弈及中国对策”（课题编号：21SFB4067）的研究成果。本文所用网络资源的最后访问时间均为 2022 年 12 月 25 日。

① 对于数据跨境调取的场景问题，本文有两点需要说明。第一，之所以不包含民事司法，是因为数据跨境调取要解决的是有公权力背书的数据流动和监管问题，因此，本文的研究集中于行政执法和刑事司法领域。第二，之所以不区分行政执法和刑事司法，不仅是因为现有《中华人民共和国个人信息保护法》（下文简称《个人信息保护法》）、《中华人民共和国网络安全法》（下文简称《网络安全法》）、《中华人民共和国数据安全法》（下文简称《数据安全法》）没有在法条上对二者作区分，还因为数据跨境调取解决的是，当面对国外有公权力背书的数据跨境调取请求时，被请求国监管机构如何应对的问题，此时的监管机构在不同国家主要指行政机构，其有时也需要司法机关的配合，因此没必要区分行政执法与刑事司法。

学者已经对数据跨境流动的相关问题展开了较为广泛的研究，包括数据跨境流动规制的国别/区域研究、[①] 数字贸易中的跨境数据流动规制研究、[②] 数据治理理念研究、[③] 数据出境方式研究[④]等，但对行政执法和刑事司法数据跨境调取问题的研究较少。不过，学者们仍旧对数据跨境调取形成了一定共识。一方面，数据跨境调取依然应当坚持数据主权，不放弃传统的国际公约、国家间司法互助以及互惠方式，但另一方面，学者们也普遍认为传统方式存在监管漏洞、效率低下、审查压力过大等缺陷，[⑤] 应当有条件地创设新的数据跨境调取路径。[⑥] 但是对于如何设计具体路径尚缺乏探讨，[⑦] 这是本文研究的起点。为此，笔者认为应当从与数据相关的主体和数据存储路径出发构建数据跨境调取的合理性判断标准，以此作为对上述传统数据跨境调取方式的重要补充。本文首先从数据跨境调取的肇始问题入手，澄清数据跨境调取的研究范围，并从主权国家对数据跨境调取的核心关切——国家安全和个人信息保护着眼，论证数据被请求国应如何从数据主体和存储路径两个维度判断是否准许他国的数据跨境调取请求。

一　数据跨境调取的现状及困境

2013 年 12 月 4 日，美国纽约南部地区法院发布了一项允许政府向微软调取其存储的某一用户电子邮件内容与元数据的令状。这一数据虽然被微软存储在美国服务器中，但同其他互联网公司一样，为了使用户能够就近获取信息，大部分消费者信息都存储在位于爱尔兰的数

① 参见崔静：《欧美数据流动监管的经验做法及我国的策略选择》，载《经济体制改革》2021 年第 2 期；李墨丝：《中美欧博弈背景下的中欧跨境数据流动合作》，载《欧洲研究》2021 年第 6 期；刘萧锋、刘杨钺：《东盟跨境数据流动治理的机制构建》，载《国际展望》2022 年第 2 期；冉从敬、刘瑞琪、何梦婷：《国际个人数据跨境流动治理模式及我国借鉴研究》，载《信息资源管理学报》2021 年第 3 期。See also François LeSieur, "Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy", (2012) 2 *International Data Privacy Law* 93; Joseph Liss, David Peloquin, Mark Barnes and Barbara E. Bierer, "Demystifying *Schrems II* for the Cross-Border Transfer of Clinical Research Data", (2021) 8 (2) *Journal of Law and the Biosciences* 1.

② 参见时业伟：《跨境数据流动中的国际贸易规则：规制、兼容与发展》，载《比较法研究》2020 年第 4 期；谭观福：《数字贸易中跨境数据流动的国际法规制》，载《比较法研究》2022 年第 3 期。See also Julian Rotenberg, "Privacy Before Trade: Assessing the WTO-Consistency of Privacy-Based Cross-Border Data Flow Restrictions", (2020) 28 *University of Miami International and Comparative Law Review* 91; Briseida Sofia Jimenez-Gomez, "Cross-Border Data Transfers between the EU and the U. S. : A Transatlantic Dispute", (2021) 19 (2) *Santa Clara Journal of International Law* 1; Andrew D. Mitchell and Jarrod Hepburn, "Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer", (2017) 19 *Yale Journal of Law and Technology* 182.

③ 参见黄炎：《跨境数据治理体系的多维变革及因应之策》，载《太平洋学报》2022 年第 4 期；邓崧、黄岚等：《基于数据主权的数据跨境管理比较研究》，载《情报杂志》2021 年第 6 期。See also Andrew D. Mitchell, Neha Mishra, "Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute", (2019) 22 (3) *Journal of International Economic Law* 389; Renee Berry and Matthew Reisman, "Policy Challenge of Cross-Border Cloud Computing", (2012) 4 *Journal of International Commerce & Economics* 1; M. James Daley, "Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure & Data Privacy", (2011) 12 *The Sedona Conference Journal* 121.

④ 参见李仁真、罗琳娜：《欧盟数据跨境传输标准合同条款新发展及启示》，载《情报杂志》2022 年第 5 期。See also Laura Braford, Mateo Aboy and Kathleen Liddell, "Standard Contractual Clauses for Cross-Border Transfers of Health Data after *Schrems II*", (2021) 8 (1) *Journal of Law and the Biosciences* 1.

⑤ 参见洪延青：《"法律战"旋涡中的执法跨境调取数据：以美国、欧盟和中国为例》，载《环球法律评论》2021 年第 1 期。

⑥ 参见张鹏：《司法和执法数据跨境调取的国际规则发展与应对实践》，载《中国信息安全》2022 年第 3 期。

⑦ 参见王雪、石巍：《数据立法域外管辖的全球化及中国的应对》，载《知识产权》2022 年第 4 期。

据中心。[①] 因此，微软以美国《存储通信法》（Stored Communication Act）不具有域外效力为由拒绝执行法院令状。[②] 虽然法院没有采纳微软的意见，但是参与该案的许多法律顾问认为，如果法院授予美国政府在本案中强迫微软调取存储在境外数据的权力，则有侵犯他国主权的嫌疑，尤其是来自爱尔兰的法律顾问，以此为由向法院递交了法律意见。案件上诉到美国联邦第二巡回法院。联邦第二巡回法院支持了微软的请求，认为授权美国政府调取位于爱尔兰的数据的行为超出了法院的权力范围，政府不能强行调取存储在美国境外的数据。为此，美国政府出台了 2018 年《澄清海外合法使用数据法》（Clarifying Lawful Overseas Use of Cloud Data，下文简称《云法》）。该法与 2016 年通过、2018 年生效的欧盟《通用数据保护条例》（General Data Protection Regulation，下文简称 GDPR）[③] 共同成为能够代表不同数据存储模式与调取国利益的两大立法阵营。在该案中，美国法院试图绕过数据存储地主管机关，直接要求其属人管辖下的跨国公司提供存储在美国境外的数据，这与传统上美国在民刑事案件中的证据开示制度一脉相承。证据开示是美国民刑事案件中诉讼双方交换证据的司法过程，美国法院往往会以命令的形式（例如传票）支持一方当事人获取证据的要求。[④] 在刑事诉讼中，美国的判例法长久以来支持检察官通过传票的形式，要求在美国经营的公司交出处于境外的文件、记录等；[⑤] 美国司法部也明确检察官可要求外国银行美国办公室提供位于境外的文件数据，只不过要经过额外的司法部内部程序。这一美国传统上惯用的数据调取路径不仅在一定程度上侵犯了数据存储地国对存储在本地的数据的主权权利，也使跨国公司面临数据存储地国与数据调取请求国之间的法律冲突，从而增加了其经营方面的不确定性。[⑥]

站在数据主权角度，不论是本国法院想要调取存储在境外的数据，还是他国法院想要获得存储在本国境内的数据，均需要对方的同意和协助，而不能绕过他国政府有关数据管理部门自行为之。[⑦] 国际法框架内传统的行政执法和刑事司法数据调取方式主要有：第一，通过国际公约包含的部分司法协助条款；第二，通过国家之间议定的司法协助程序；[⑧] 第三，当不存在上述公约或协定时，基于互惠原则，以一事一议方式展开具体的司法协助。然而，主权国家充分参与下的数据跨境调取方式为数据跨境调取设置了“高门槛”，故而存在诸多弊端。第一，是否同意他国调取本国数据有时并非出于维护国家安全和个人信息保护的考虑，而仅是为了宏观政治和国家关

① 在该案中，被调查用户使用的是非美国代码，导致微软将数据存储到了爱尔兰，当存储完成后，大部分相同内容的信息就会在美国服务器中被删除。

② See *Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d, p. 470.

③ *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC* (*General Data Protection Regulation*) (*Text with EEA relevance*), *OJ* L 119/1, 4. 5. 2016.

④ 宋冰编：《读本：美国与德国的司法制度及司法程序》，中国政法大学出版社 1998 年版，第 274—279 页。

⑤ See *In Re Grand Jury Proceedings* (*Bank of Nova Scotia*), 740 F. 2d 817 (11th Cir), cert. denied, 469 U. S. 1106 (1985); *In Re Grand Jury Proceedings* (*Bank of Nova Scotia*), 691 F. 2d 1384 (11th Cir. 1982), cert. denied, 462 U. S. 1119 (1983); *In Re Grand Jury Subpoena Directed to Marc Rich*, 707 F. 2d 663 (2d Cir. 1983).

⑥ 洪延青：《“法律战”漩涡中的执法跨境调取数据：以美国、欧盟和中国为例》，载《环球法律评论》2021 年第 1 期，第 41—42 页。

⑦ See Maruša T. Veber and Maša Kovič Dine, *Big Data and Economic Cyber Espionage*: *An International Law Perspective* (Routledge, 2014), p. 11.

⑧ See Valsamis Mitsilega, “New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data”, (2003) 8 (4) *European Foreign Affairs Review* 515, pp. 515 – 536.

系，从而牺牲了个案效率。例如美国政府认为作为其竞争对手的俄罗斯，通常会拒绝其执法数据调取请求，即使该请求是美国司法机关通过传统双边司法协助或者互惠原则进行的。[①] 第二，传统数据调取路径受到诟病最多的是效率低下，比如外国政府向美国发出的协助请求，往往要耗时 10 个月才能得到回应，[②] 显然无法满足网络的即时性要求。第三，传统数据跨境调取路径易被罪犯利用，即本国行为人只要采用外国通信产品或服务，并使用位于境外的服务器、终端或云端，就可简单规避本国调查，而后者若只能通过司法协助程序提出获取通信内容的申请，[③] 客观上无疑会给犯罪分子提供“犯罪天堂”。第四，所有数据跨境调取请求若均采取传统方式，将会给被请求国带来巨大的审查压力，导致司法资源浪费。因此，为了提高司法证据获取效率、避免罪犯妨碍司法取证、减轻数据被请求国的审查压力，应当在传统司法协助程序的基础上，探索更具有实践价值的其他行政执法和刑事司法数据调取方式。[④]

二　中国数据跨境调取的基本立场与规范前提

对于在司法过程中跨境调取存储于他国的数据，中国始终坚持司法协助方式，以体现对国家主权的尊重。因此，中国并未参加旨在绕过一国权力机构审查的《网络犯罪公约》（Cyber-Crime Convention）。[⑤] 2018 年 10 月通过的《中华人民共和国国际刑事司法协助法》（下文简称《国际刑事司法协助法》）是规范中国数据境外调取的主要法律，其第 4 条规定：“非经中华人民共和国主管机关同意，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。”2021 年 9 月 1 日通过的《数据安全法》第 36 条也规定，“处理外国司法或者执法机构关于提供数据的请求”时应当遵守“我国缔结的国际条约、协定，或者按照平等互惠原则”，非经主管机关批准，不得向境外司法或执法机构提供存储于中国境内的数据。2021 年 8 月 20 日通过的《个人信息保护法》第 41 条也有类似规定，除非依据条约以及互惠原则，非经主管机关批准，个人信息处理者不得向境外司法或执法机构提供存储在中国境内的数据。由此可见，一方面，中国仍旧坚持将传统的司法互助协定方式和互惠原则作为数据跨境调取的主要方式，但另一方面，《数据安全法》以及《个人信息保护法》的生效也增添了新的数据跨境调取方式，即“经主管机关批准”，从而为数据跨境调取提供了构建新路径的契机。然而，对于主管机关依据何种标准决定是否批准，法律法规则缺乏进一步规定。从立法目的上看，中国和世界主要国家有关数据治理的立法均强调两个宗旨，即国家安全与个人信息保护。

---

① See Roderic Broadhurst, “Developments in the Global Law Enforcement of Cyber-crime”, (2006) 29 (3) *Policing: An International Journal of Police Strategies & Management* 408, pp. 408 – 433.

② See Peter Swire and Justin Hemmings, “Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program”, (2016) 71 (4) *NYU Annual Survey of American Law* 687, pp. 687 – 740.

③ See Written Testimony of Mr Paddy McGuiness United Senate, http://www.judiciary.senate.gov/download/05 – 24 – 17 – mcguinness – testimony.

④ 洪延青：《“法律战”漩涡中的执法跨境调取数据：以美国、欧盟和中国为例》，载《环球法律评论》2021 年第 1 期，第 40 页。

⑤ 该公约第 32 条规定，可以通过互联网直接获取境外电子数据，而中国认为这一方式侵犯了他国主权。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》，载《国际法研究》2016 年第 6 期，第 21—34 页。

（一）国家安全

《数据安全法》第4条规定："维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。"该法第2条规定，境外的数据处理活动不得损害中国国家安全与公共利益，由此为中国的数据治理奠定了以维护国家安全利益为核心的总基调。

美国宪法以及判例法层面一直倾向于"国家安全至上"。对于不在美国境内居住的外国公民甚至与这类公民交往的居住在美国本地的美国公民，都会在法律的授权下遭到美国政府的监视，此时为了使国家安全免受威胁，个人隐私安全只能暂时让位。尽管在"斯诺登事件"之后，美国的这一行为有所收敛，[①] 但美国政府的整体行为导向并未改变。美国宪法为美国国家安全局（National Security Agency）的数据监视及调取行为提供了宪法基础。一方面，美国宪法第四修正案（Fourth Amendment to the United States Constitution）规定，宪法给予隐私权的保护不适用于个人与"第三方"共享的信息，美国联邦最高法院依据该原则判定，宪法保护的是"合理的可预见的隐私权"，[②] 并解释道，当个人与"第三方"共享信息时，就缺乏了合理性以及可预见性基础，因为该个人应该能够预见到获得其信息的"第三方"可能将信息分享给"外国"政府。另一方面，美国联邦最高法院进一步解释道，在某些情况下，美国宪法第四修正案对隐私权的保护并不适用于美国政府对居住在美国之外的外国公民进行调查，这实际上是对美国单边域外执法的听之任之。[③]

即使是在将个人隐私提高到人权保护高度的欧盟，在国家安全问题上的立场也同美国不谋而合。首先，欧盟数据跨境调取框架特别强调为预防、调查、侦查以及起诉刑事犯罪可以降低对隐私权的保护标准。[④] 欧盟法院也通过判例承认成员国拥有为国家安全以及刑事正义采取措施的权力，[⑤] 但欧盟成员国出于国家安全考虑而实施的隐私权保护标准实际上却参差不齐。比如德国，在国家层面和联邦层面都有完善的隐私权保护体系，并能保证其严格执行；法国在2015年以前就已经通过议会以及宪法委员会为政府的监视行为扫清了立法障碍，数据隐私只能让位于国家安全。此外，欧盟有关数据保护的法律同美国一样，只适用于居住在欧盟境内的欧盟成员国公民，对于欧盟以及成员国政府的对外监视行为则没有限制，甚至采取默许态度。

---

① See J. Richard Broughton, "The Snowden Affair and the Limits of American Treason", (2015) 3 *Lincoln Memorial University Law Review* 5, p. 32.

② See *Katz v. United States*, 389 U. S. 347 (1967).

③ See *United States v. Verduto-Urquidez*, 494 U. S. 259, 259 (1990). 在该案中，美国政府同墨西哥代理人共同在一位墨西哥公民家中搜集证据，此时该墨西哥公民正在美国候审。该公民认为美国这一取证行为没有经过授权，但法庭判定宪法第四修正案并不限制美国政府在境外对外国公民调取数据的行为。

④ 根据《欧盟联盟条约》（Treaty on European Union）第4条第2款，国家安全属于成员国自己负责的事项。《欧洲议会和欧盟理事会关于在个人数据处理和自由流通过程中对个人数据进行保护的指令》（Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data，下文简称《95指令》）允许成员国出于以下原因采取法律措施限制履行本指令规定的义务：（1）国家安全；（2）自卫；（3）公共安全；（4）为预防、调查、侦查、起诉刑事犯罪；（5）成员国的重要经济或金融利益以及属于欧盟的重要事项，包括货币、预算以及税收。See *Directive 95/46/EC of the European Parliament and of Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, *OJ* L 281/31, 23. 11. 1995, art. 13.

⑤ See Joined Cases C－293/12 & C－594/12, Digital Rights Ireland, ECLI: EU: C: 2014: 238; Federico Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States", (2015) 28 *Harvard Human Rights Journal* 65, p. 81.

（二）个人信息保护

《中华人民共和国民法典》总则规定了个人信息保护的一般原则，并在“人格权编”中规定了“隐私权和个人信息保护”，确定了中国个人信息保护的基本框架。《个人信息保护法》更是在开篇即强调“保护个人信息权益、促进个人信息合理利用”，并在第 3 条明确规定某些境外的数据处理活动也要遵守个人信息保护方面的法律法规。

欧盟的个人隐私保护有着悠久历史和文化根基。早在 GDPR 生效之前，欧盟的个人数据保护立法，尤其是《95 指令》[①] 就对作为数据接收国的第三国的个人数据保护标准提出了“适当保护水平”（adequate level of protection）的要求，[②] 促使多个国家[③]为了能够满足从欧盟调取数据的要求而修改了国内法，使本国的个人信息保护标准不低于欧盟标准。GDPR 生效后，欧盟将调整重心从欧盟成员国之间数据跨境分享与调取转移到欧盟与第三国之间数据跨境分享与调取，其在第 5 章规定了个人数据获取与传输的一般规则，规定了自然人数据保护标准在传输至欧盟外的第三国时不得被减损。[④] 与此同时，为了保护以通信内容为代表的隐私数据，美国也通过阻断条款明确禁止外国政府对美国控制的通信内容进行跨境调取。《存储通信法》第 2 章明确禁止美国政府以外的任何人披露某些存储的内容，包括电子邮件。当外国政府要求为调查当地犯罪而寻求在美国控制的本国公民的数据时，即使该外国政府遵守了美国国内法要求，《存储通信法》第 2 章也禁止美国公司回应外国政府对通信内容的要求。[⑤] 虽然该章并没有关于适用范围的规定，但谷歌（Google）和脸书（Facebook）等公司将其解释为适用于其控制下的所有数据。

因此，对于司法中的数据跨境调取活动，中国除了坚持传统的国际公约、司法协助方式以及互惠原则，在立法上还构建了“经主管机关批准”这一灵活开放路径，只是目前的国内立法尚未对批准的标准作详细规定。从各国有关数据的立法来看，一国在司法程序中是否允许数据跨境调取往往会考虑国家安全与个人信息保护两个方面。换言之，如果他国在司法程序中申请调取中国数据，而该申请并不侵犯中国国家安全利益以及个人信息保护权益，则原则上应当准许，甚至当该数据与中国及境内主体联系微弱时，应当自动准许调取请求。笔者认为，在判断他国请求是否关切中国国家利益以及个人信息保护抑或是其他利益时，可以从数据主体以及数据存储路径两个角度入手。

三　以“数据相关主体”为划分标准的数据跨境调取规范

从“微软诉美国案”（*Microsoft Corp. v. United States*）[⑥] 中可知，数据跨境调取至少与数据

① *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the personal data and on the free movement of such data*, *OJ* L 281/31, 23. 11. 1995.

② 《95 指令》第 25 条第 1 款规定：向第三国转移正在处理的个人数据或者转移到第三国才开始处理的个人数据的，成员国应当规定只有该第三国对个人数据提供了适当的保护水平的条件下才可以实施。该规定不影响成员国根据本指令其他条款制定的规则的实施。

③ 比如澳大利亚、加拿大以及多个东欧国家。See Manfred Elsig, “All Politics is Global”, (2009) 8 (2) *World Trade Review* 367.

④ 该标准同时适用于数据处理者与控制者。See GDPR, art. 44.

⑤ 参见周梦迪：《美国 CLOUD 法案：全球数据管辖新“铁幕”》，载《国际经济法学刊》2021 年第 1 期。See also Jennifer Daskal, “Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues”, (2016) 8 (3) *Journal of National Security Law and Policy* 473.

⑥ See *Microsoft Corp. v. United States*, 829 F. 3d (2d Cir. 2016).

调取国、数据主体所在国、数据处理者经营所在地所属国家有关。我们将数据调取与具体的跨境案件调查相结合，会发现可能向中国申请数据调取的国家主要有以下几种。一是法院地国，比如行为地、行为结果发生地所在国等。二是数据处理者经营所在地所属国家，指经营云数据存储的公司所在地（比如微软、谷歌等的经营地）所在国；这一地点同数据实际存储地可能重合，也可能因偶然和特殊的数据安排而分离。三是数据主体所在国，也就是案件被调查对象、数据指向的主体所在国，包括该主体的住所地国、国籍国。此外，“微软诉美国案”还涉及数据实际所在地，也就是数据存储地，笔者将在下一部分从数据存储路径角度作集中探讨。

首先，法院地国原则上对案件具有管辖权，在审判过程中需要从他国调取数据，因此，来自法院地国的数据调取请求原则上是合理的。然而，各国对司法管辖权规则并无统一规定，尤其当法院地国与数据调取请求接收国的司法管辖权规则相悖时，若后者认为前者对案件并不具有合法管辖权，则拒绝其数据调取请求则是合理的。以美国“长臂管辖权”规则为例，[①] 该规则围绕“最低限度联系”判断域外行为对境内造成的影响来决定是否对域外行为人进行管辖。“最低限度联系”在美国历史上一直存有争议，更何况其他国家对其反感，这也正是“长臂管辖权”一直以来备受诟病的症结。[②] 更何况在网络领域，依靠“最低限度联系”判断管辖权的标准更加难以把握，极易出现管辖权扩张的现象，[③] 甚至最终因行为对多个法域均可能产生潜在影响，造成全球范围内的平行管辖。[④] 因此，这种影响应当限缩在一定范围内，或与其他管辖权规则相结合。换言之，如果数据调取请求来自法院地国，应首先对管辖权作出判断。即如果依据中国法律，法院地国对案件具有合法管辖权，且该数据对于案件审理具有实质影响，则原则上主管机关才应当批准此类数据调取请求，除非提供此类数据有损国家安全。

其次，有时数据调取请求也可能来自数据处理者经营所在地国。这类国家往往会在以下情况向他国提出数据调取请求：法院地国与数据存储地国不存在司法互助协定，而数据处理者所在地国与数据存储地国存在相关协定，则法院地国通过要求数据处理者提供数据，致使后者不得不通过其所在地国相关部门向数据存储地国发起数据调取请求。这种以数据处理者所在地国为桥梁调取数据存储地的数据的方式实际上属于美国证据开示制度的延续，是不可取的。第一，在诸多案件中，许多数据处理公司，比如谷歌[⑤]和脸书[⑥]均认为其经营所在地并非位于法院地境内，因此

---

① Gerlinde Berger-Walliser, “Reconciling Transnational Jurisdiction: A Comparative Approach to Personal Jurisdiction over Foreign Corporate Defendants in US Courts”, (2018) 51 *Vanderbilt Journal of Transnational Law* 1243, p. 1298.

② Mahir Al Banna, “The Long Arm of US Jurisdiction and International Law: Extraterritoriality against Sovereignty”, (2017) 60 *Journal of Law, Policy and Globalization* 59, p. 62.

③ See Henry Lowenstein and Carla F. Grabert-Lowenstein, “The Long-Arm of the Law: South Carolina's Long-Arm Statute and the Internet”, (2016) 68 *South Carolina Law Review* 47, p. 76; Adam R. Kleven, “Minimum Virtual Contacts: A Framework for Specific Jurisdiction in Cyberspace”, (2018) 116 *Michigan Law Review* 785, p. 807; Elma Delic, “Cloudy Jurisdiction: Foggy Skies in Traditional Jurisdiction Create Unclear Legal Standards for Cloud Computing and Technology”, (2017) 50 *Suffolk University Law Review* 471, p. 488.

④ See Paul Schiff Berman, “Legal Jurisdiction and the Deterritorialization of Data”, (2018) 71 *En Banc-Vanderbilt Law Review* 11, p. 27.

⑤ 有关谷歌的典型案件为：Case C - 131/12, *Google Spain SL v. Agencia Espanõla de Protección de Datos* (*AEPD*), 2014 E. C. R。在该案中，谷歌认为欧洲法院对谷歌具有管辖权，依据《95 指令》，谷歌在西班牙建立了分支机构，并在西班牙进行广告宣传，其服务也针对的是西班牙居民。

⑥ 有关脸书的典型案件为：*Douez v. Facebook, Inc.*, 2017 SCC 33 (CanLII), [2017] 1 SCR 751。Facebook 认为其针对的是加利福尼亚州居民，而其服务条款中也载明所有的与数据相关的纠纷都应在加利福尼亚州法院解决。

没有必要服从法院地的指令，此时，法院地国往往依靠对数据处理者或其高管的属人管辖，直接要求数据处理者提供数据。[①] 第二，数据处理者经营所在地具有随机性。一方面，公司经营所在地同云技术下的数据存储地一样，具有任意性。与一国毫无关系的个人可以很容易地在该国设立公司，并宣称受该国法律管辖，而实际上其经营项目以及由此而产生的纠纷与该国关系微弱甚至毫无关系。另一方面，公司可以出于避税的需要轻易在外国设立分支机构，即使其大部分税收收入来源于内国。除此之外，数据处理者只是提供数据的存储、分析等服务，在不涉及更改数据内容的情况下，对数据的具体内容及其所牵连的案件都无从知晓。正因如此，某些国家以数据处理公司在其境内设立为由，强行要求其雇员提供公司所控制信息的行为缺乏法律基础。因此，当数据请求来源于数据处理者经营所在地时，由于上述原因，中国可以考虑拒绝该请求，除非存储于中国的数据有其他特殊的存储安排，这也是对美国证据开示制度以及美国强制个人或企业披露存储于他国的数据的做法的回应。

最后，数据调取请求还可能来自数据主体所在地国，包括被调查对象的住所地国或国籍国。从对案件的管辖权以及对处理案件是否有实质影响的角度，除了法院地国，作为被调查对象的数据主体是与案件存在实质联系的一方。被调查对象与他人的谈话内容、电子邮箱地址、银行账户等信息构成了数据的主要内容。一方面，数据主体住所地国或国籍国基于属人管辖权，对居住在本地的居民或拥有其国籍但并不居住在本地的公民，出于公共管理的需要具有调取数据的合理利益；另一方面，数据构成数据主体隐私权的重要客体，出于隐私权保护的需要，数据主体所在地或国籍国在控制、审查数据流动方面也应享有权力，并且这种隐私权保护利益与法院地国调查、起诉案件所彰显的国家安全利益一致，都是数据跨境调取过程中需要关注的核心诉求。[②] 因此，如果中国主管机关收到的数据调取请求来自于数据主体住所地国或国籍国，且请求所涉及的数据主体并非中国公民，则原则上应当予以准许。

四　以“存储方式”为划分标准的数据跨境调取规范

自美国第二巡回法院在“微软诉美国案”赋予数据存储地以数据跨境调取权并支持微软拒绝美国政府的数据请求以来，[③] 对数据存储地国与数据之间的关系、数据存储地国与数据调取国之间关系的讨论便不绝于耳。[④] 相关讨论围绕数据存储地国是否能够仅因数据在其境内存储这一

① 比如 2015 年 1 月，微软雇员就因为不肯违背美国《存储通信法》而被巴西政府逮捕，这是数据调取国威胁本地外籍雇员的典型例子。

② See Paul Schiff Berman, “Legal Jurisdiction and the Deterritorialization of Data”, (2018) 71 *En Banc-Vanderbilt Law Review* 11, pp. 24 – 35; Andrew Keane Woods, “Against Data Exceptionalism”, (2016) 68 *Stanford Law Review* 729, p. 768.

③ *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.*, 829 F. 3d 197 (2d Cir. 2016).

④ See Secil Bilgic, “Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act”, (2018) 32 *Harvard Journal of Law & Technology* 321; Jennifer Daskal, “Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues”, (2016) 8 *Journal of National Security Law & Policy* 473; Paul Schiff Berman, “Legal Jurisdiction and the Deterritorialization of Data”, (2018) 71 *En Banc-Vanderbilt Law Review* 11; Paul M. Schwartz, “Legal Access to the Global Cloud”, (2018) 118 *Columbia Law Review* 1681; Jordan A. Klumpp, “International Impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations”, (2020) 48 *Georgia Journal of International & Comparative Law* 613.

单一联系就拒绝他国调取数据，以及数据存储地国是否有必要对其境内存储的所有数据的调取请求进行审查展开。一方面，数据存储地有其优点，比如相比数据主体所在地更易被确定；从支持数据具有地域性的观点出发，数据与票据、股票没有本质区别，其所在地与数据本身具有密切的联系。但另一方面，如果数据存储地只因数据存储在本地就可以自然地拒绝或妨碍他国的数据请求，那么将至少产生4种负面影响。一是基于目前大部分数据都存储在美国，这一规则将赋予美国广泛的数据调取利益，使其掌握全球数据话语权。① 二是如果肯定了数据存储地国可以只因数据存储在本地就拒绝他国的数据调取请求，将会引发各国数据本地化立法泛滥，不利于数据自由流动。② 三是方便数据处理者通过变更存储地绕过某一政府对数据的调取请求。四是如果中国作为数据存储地，对任何数据的跨境调取请求都需要进行批准审查，无疑会增加工作量。因此，虽然原则上数据存储地与数据之间具有一定联系，且其有权审查来自他国的数据调取请求，但也不能忽略从科技角度探究“云存储”的具体模式，因为不同的科技手段将对法律规制产生差异化影响。因此，为解决科技给法律造成的难题，也应从科技这一源头思考应对之策。

（一）“数据本地云”路径

不论是“微软诉美国案”中两级法院是否支持微软拒绝向美国政府提供数据的决定，还是目前很多国家采用的“数据本地存储”立法要求，其科技基础都是针对“数据本地云”这一存储模式而言的。也就是说，公司将云中的信息只存储在一个国家或区域内。③ 许多经营云存储服务的科技公司，包括著名的微软以及亚马逊网络服务公司（Amazon Web Services，下文简称AWS）均采用这种模式。AWS在全球范围内拥有55个“可访问域”，最新开放的可访问域位于法国。德国通信公司同样也只将信息存储在德国。因此，“数据本地云”存储模式采用了科技手段，依靠科技将数据存储在本地，并只允许特定的来自一个或多个地点的访问，排除了非授信地的访问申请和权限。这一存储模式是“微软诉美国案”的核心。该案涉及的电子邮件存储在爱尔兰的都柏林，该云存储服务器是由微软的爱尔兰分支机构独立运营的，美国纽约南区联邦地区法院想通过域外执行法律获得该数据，但联邦第二巡回法院在上诉中否定了美国法（《存储通信法》）在该领域的域外效力，支持了微软的拒绝提供行为。

---

① 从目前来看，在全球范围内提供云存储服务的公司主要是美国科技公司。比如，在印度、巴西、英国以及德国排名前十的提供云存储服务的网络科技公司，美国公司就分别占了9个、7个、9个和7个。See Top Sites in India, ALEXA, http://www.alexa.com/topsites/countries/IN; Top Sites in Brazil, ALEXA, http://www.alexa.com/topsites/countries/BR; Top Sites in United Kingdom, ALEXA, http://www.alexa.com/topsites/countries/GB; Top Sites in Germany, ALEXA, http://www.alexa.com/topsites/countries/DE.

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。”印度也直接要求在印度境内与金融交易相关的信息必须存储在境内。See Notifications, Storage of Payment System Data, RESERVE BANK OF INDIA, Reserve Bank of India-Notifications. 印度还在2018年通过了针对所有在印度境内收集、分享、获取的数据必须物理性地存储在印度境内的立法，即《电子商务政策草案》（Draft National E-Commerce Policy – India's Data for India's Development）。《越南网络安全法》也在越南第十四届国会第五次会议上通过，并于2019年元旦生效。依据该法，在越南境内提供网络服务的所有外国和本国公司，以及所有从越南网络用户中收集、分析、获取的个人数据都要受制于数据本地化要求。参见《国际：欧盟—美国跨境数据传输》，http://www.raysync.cn/news/post-id-613。

③ See Patrick Spaulding Ryan *et al.*, “When the Cloud Goes Local: The Global Problem with Data Localization”, (2013) 46 *Computer* 12, pp. 54, 57.

但是，“数据本地云”又有两种模式：“完全数据本地云”与“不完全数据本地云”。该案中微软采用的“数据本地云”存储具有特殊性，这是一种“不完全的”或者说“部分化的”数据本地云存储。虽然该案中的电子邮件仅存储在爱尔兰，但其授信的“访问域”则有两个——都柏林和微软总部雷德蒙德。因此，美国主张获取该数据也并非没有道理。而 AWS 以及微软在欧盟的分支机构则采用的是“完全”数据本地云存储，从而排除了数据存储地以外的法域对数据的请求权，数据跨境调取权也就当然归数据存储地所有。

因此，在“不完全数据存储”模式下，虽然数据存储在中国，但如果通过数据处理者的特殊技术安排，中国并非其开放的“访问域”，而只是数据处理者利用了中国的数据存储中心或设备，则除非有证据证明提供数据将有损国家安全和个人信息保护权益，否则中国不应当拒绝来自“访问域”国家的数据调取请求。当然，这种数据调取安排需要以中国允许数据中心经营“不完全数据本地存储”服务为前提。

（二）“数据共享云”路径

与“数据本地云”相反，“数据共享云”运营者将数据存储在全球范围内的多个位置，分别由国内以及国外服务器同时管理数据。[①] 通过这种方式存储的文件会被智能系统拆分成几部分并自动决定分配到某一服务器存储，而分配标准主要由效率决定。通过这种方式形成的数据存储地与国家物理边界的关联甚微，并且出于效率以及存储方便的考虑，数据会不断在云端流动，即使是数据碎片也不会固定存储在某一地，除非公司通过法律手段限制这一流动。谷歌公司是采取这一存储方式的典型代表，因此并不能因为数据存储在谷歌经营的服务器中就强制谷歌提供数据，而应当依据行为发生在美国并给美国造成影响从而支持美国的数据调取请求权。[②] 虽然在“数据共享云”模式下数据碎片化地存储在多国，但这并不意味着凡是数据存储国都应当对其存储的数据进行审查，否则将浪费大量的行政或司法资源。比如谷歌就仅开放美国为可访问域，当其他国家申请调取数据时也并不向数据的实际存储地国申请，而是向美国提出请求。在数据共享云模式下，数据公司只是为了技术方便而存储数据，并非有意将数据实际存储地与数据本身或数据主体之间建立联系。因此，如果中国允许数据控制者或数据处理者采取“数据共享云”的模式在中国存储数据，且数据调取请求国能够在“数据共享云”模式下访问存储在中国的数据，则除非有证据证明提供数据将有损国家安全和个人信息保护权益，则中国不应当拒绝其他国家的数据调取请求。

（三）“数据信托云”路径

“数据信托云”是一种特殊的数据存储安排，[③] 是目前为止数据流动领域受主权国家政府支配最弱的数据存储模式。苹果公司与中国云上贵州公司之间的合作即采取了类似方式，但与“数据信托云”不完全相同。同“数据本地云”一样，在“数据信托云”模式中数据本身不会被分割，但数据的管理权却是分离的。数据公司通过信托协议切断了数据存储地与数据之间的必然联系，但以“管理权分配”建立了可访问权限拥有者与数据之间的联系。以“微软云德国”为

① See Sikha Bagui & Loi Tang Nguyen, “Database Sharding: To Provide Fault Tolerance and Scalability of Big Data on the Cloud”, (2015) 5 *International Journal of Cloud Applications and Computing* 36.

② *In re Search Warrant NO. 16 – 960 – M – 01 to Google*, 232 F. Supp. 3d, p. 721.

③ See Microsoft, Microsoft Cloud Germany Datasheet 1 – 2 (2016), https://go.microsoft.com/fwlink/? LinkId = 839380&clcid = 0x409.

例，数据存储所需的网络硬件以及软件设施由“微软数据信托”提供并运营，其将消费者信息存储在位于法兰克福以及马格德堡的数据中心，但数据的保密以及访问则被委托给独立的德国公司——德国电信的子公司 T-Systems，只有该公司有权访问存储数据的网络。微软与 T-Systems 的信托安排依据德国法，由 T-Systems 排他地负责数据的加密与访问权限，就连微软也不能违背信托安排任意访问数据。如此一来，包括德国政府在内的任何政府或公司想要调取数据，只能向 T-Systems 提出请求，而不能通过法律强制微软提供数据。特别是，依据德国信托法以及微软与 T-Systems 的信托安排，微软也被安排在禁止访问之列，T-Systems 对消费者数据拥有排他的、唯一的访问权与监督权。微软既在德国法上被禁止访问消费者数据，也在技术上无法获取数据访问密码。由此可知，此时的数据存储地——法兰克福与马格德堡仅因其特定技术安排而存在，与数据本身并不具有法律上的联系，在国家安全以及个人信息保护方面均不存在利益。相反，在数据调取层面，数据受托公司，即作为真正的数据处理者的 T-Systems，其对数据能够进行实际访问、使用、处置而使其经营所在地国在国家安全或个人数据保护方面具有利益。此外，T-Systems 作为受托公司，通过依据德国法签订的信托协议，一方面相对于美国、德国及其他可能具有数据跨境调取权的政府，获得了独家设置访问权限与加密的权利，使政府无法直接通过数据处理者（微软）达到获取数据的目的，另一方面相对于微软获得了完整的数据密钥和数据控制权，使数据的开放不需要经过微软及美国的再次审查。而在苹果公司与云上贵州的合作模式中，能够见到明显的数据信托云的影子，但相比 T-Systems，云上贵州相对于苹果、美国以及中国政府仅具有相对独立性，数据信托云或可成为云上贵州未来的发展方向，并为中国数据跨境调取规则的构建提供启发。

2018 年 1 月，苹果公司正式对外宣布在中国的 iCloud 云服务将转由中国贵州的云上贵州公司负责运营，[①] 这是苹果为了中国市场，面对中国有关云服务业务外资准入监管要求所作出的世界范围内的妥协，是中国数据监管领域的一次标志性事件。[②] 依据《iCloud（由云上贵州运营）条款与条件》，[③] 云上贵州应当被视为中国用户数据的控制者，或者至少和苹果公司一道被视为中国用户数据的共同控制者，同时苹果公司决定将中国区用户的 iCloud 密钥也在中国境内存储，但继续独家管理 iCloud 密钥，并处理来自中国的行政执法和司法数据跨境调取事宜。而在其他国家，苹果会将用户文件的元数据（metadata）和用于加密用户数据内容的密钥存储在 iCloud 账户中，第三方云存储提供者则是数据处理者，而苹果是唯一的数据控制者。可见，云上贵州取得了类似于 T-Systems 的法律地位，但不同的是，云上贵州相对于苹果公司并没有取得对数据的完整控制权。中国司法部门调取用户数据的法律文件仍由苹果公司（而非云上贵州）单独接收，而且苹果公司还会将其接收到的数据调取请求反映在其透明度报告中，且苹果不会对来自中国司法

① 《致中国内地 iCloud 用户的重要通知》规定：“自 2018 年 2 月 28 日起，与您的 Apple ID 相关联的 iCloud 服务将转由‘云上贵州’运营。使用这些服务及您通过 iCloud 存储的所有数据（包括照片、视频、文稿和备份等）都将受到 iCloud（由云上贵州运营）条款与条件的约束。”参见 http：//www. sohu. com/a/215771365_ 114877。

② 工信部 2016 年《关于规范云服务市场经营行为的通知（征求意见稿）》明确要求：“云服务经营者与有关单位开展技术合作，应向电信管理机构书面报告云服务合作事项。合作过程中不得存在以下行为：（1）以任何形式向合作者变相租借、转让电信业务经营许可证，以及为合作者非法运营提供资源、场地、设施等条件；（2）由合作者直接与用户签订合同；（3）仅使用合作者的商标和品牌向用户提供服务；（4）违法向合作者提供用户个人信息和网络数据；（5）违反法律法规规定的其他行为。”

③ 《iCloud（由云上贵州运营）条款与条件》规定：“凡提及云上贵州之处，在苹果公司提供支持的范围内，应视为提及云上贵州和苹果公司。”参见 https：//www. apple. com/legal/internet - services/icloud/cn_ si/gcbd - terms. html。

部门的“批量数据调取请求”作出响应。但即便如此，相比苹果与云上贵州合作之前，由于密钥仅存储于美国，世界上其他国家想要调取 iCloud 用户账户内容均只能向美国寻求司法协助的境况，目前由云上贵州与苹果公司共同掌握数据控制权要好得多。

可见，在“数据信托云”路径下，数据跨境调取权限由信托协议安排。在德国电信模式中，只能依据德国法调整下的信托协议向德国电信申请调取数据；而在云上贵州模式下，虽然中国争取到了将数据存储在境内的权利，但独家密钥仍旧由苹果公司掌控，中国执法部门调取数据仍旧需要向苹果公司提出申请，受制于苹果公司的审核。笔者认为，如果一国允许其境内数据控制者采取“数据信托云”路径存储数据，在申请调取数据时就应当服从信托协议的安排。

五　中国数据跨境调取规则的构建

自《网络安全法》颁布以来，立法者又从个人信息以及数据两方面着手，开启了《个人信息保护法》以及《数据安全法》的立法程序，使这 3 部法律成为治理网络世界的三驾马车。直接调整数据跨境调取权的条款为《网络安全法》第 37 条、《数据安全法》第 31 条、《个人信息保护法》第 38 条，以及《数据出境安全评估办法》。从国际条约层面上看，当数据作为证据使用时，中国与他国之间的刑事司法协助条约以及《国际刑事司法协助法》也能够为数据跨境调取提供法律依据。然而，总体来看，与美欧相比，中国跨境数据传输规则的制定起步较晚，尚未形成一套清晰、完整的规则体系，各项规范仍在探索中。

（一）基本立场：数据主权与安全

《网络安全法》第 37 条、《数据安全法》第 31 条均强调在中国境内收集和产生的重要数据只有在例外情况下履行一定手续才能够出境，即使专门规定数据出境的《数据出境安全评估办法》也在强调数据跨境时特别将“安全”置于“自由流动”之前。作为数据跨境流动重要内容的数据跨境调取，也需要平衡好数据安全与数据自由流动之间的关系。

一方面，数据跨境调取规则应始终以数据安全为准绳，并从基本立场、内部逻辑与产业生态 3 个方面进行完善。从规则的基本立场讲，必须明确数据跨境调取的必然性与需求性，应当在一定范围内（比如“一带一路”倡议）尝试建立以数据管辖为基础的数据调取方案，同时强调数据跨境调取中数据安全的重要性。从规则的内部逻辑讲，应当将数据跨境调取与网络空间的一般治理规则适当分离，将数据按照数据主体与存储路径详细分类，为数据调取权留下足够的探讨空间。此外，中国应从“国家权力—公民权利”的二元互动视角出发，[①] 建构网络治理法律体系内部的数据跨境调取规则。从规则与网络产业生态的角度看，在网络信息产业发展方面，中国既是数据提供者也是数据需求者，应首先积极主导建立数据跨境调取规则，尽快在实体法上确定数据跨境调取的本国模式，并在尊重主权的基础上与他国就数据跨境调取规则的核心关切——国家安全与个人信息保护——进行协调，缓解规则冲突。同时，中国在强调网络安全时，还应特别从人权保障出发，以保障公民基本权利为基础，在国际数据攻防关系中有效制衡他国数据跨境调取行为。[②]

① 参见裴炜：《个人信息大数据与刑事正当程序的冲突及其调和》，载《法学研究》2018 年第 2 期。

② 裴炜：《向网络信息业者取证：跨境数据侦查新模式的源起、障碍与建构》，载《河北法学》2021 年第 4 期，第 77—80 页。

另一方面，数据跨境调取规则应始终以数据主权为宗旨，并随着数字技术发展适当拓展数据主权的概念与范围。“数据主权论”认为全球数据治理依然应当围绕主权展开，对数据治理的关注是网络发展与治理的高级形态，因此，数据主权理论是网络主权理论的自然延伸，是物理主权在网络空间的逻辑映射。[①] 为此，数据跨境调取规则应当从内外两个方面坚守数据主权：“对内”始终坚持主权国家对信息通信技术、信息通信平台、信息通信系统及其承载的数据具有最高的、排他的管辖权与支配力；[②] “对外”始终坚持主权国家治理本国网络空间不受他国干涉，各国在《联合国宪章》原则下坚持网络空间与现实空间在国际制度上的一致性。[③] 此外，主权国家对数据调取请求的审查应当既包括对数据处理者及其行为——收集、使用、传播或披露个人信息——的审查，也包括对数据本身的审查。

（二）中国数据跨境调取的具体规范

中国的数据跨境调取规则应进一步细化。首先，目前以司法互助协定方式和互惠原则为主的数据跨境调取路径适用门槛过高，效率低下，而国际公约中的部分司法协助条款覆盖面有限，无法适应网络即时性与全球性的特点，不利于在全球范围内实现高效的司法取证，也难以有力打击网络犯罪。其次，多种形式的数据存储路径目前已经客观存在于不同国家，随着中国数据存储模式的逐渐丰富，如果对所有数据请求都逐一甄别、审查，势必会造成司法资源与行政资源的浪费，而降低对某些数据跨境调取请求的审查门槛，也可以吸引更多数据存储在中国。再次，随着中国数据出境方式的不断丰富，中国在数据跨境调取领域逐步探索更加便捷的规范路径也是顺应全球数据治理的表现。最后，对与中国国家安全与个人信息保护无关的数据跨境调取请求采取较为宽松和开放的态度，也可以体现出数据主权与数据自由之间的平衡。为此，在不同场景中，笔者认为应当对数据请求采取不同的态度。

一方面，从数据相关主体的角度，中国在面对不同的数据主体所在国发出的数据调取请求时，应当采取不同态度。第一，当数据调取请求国依据中国法律对数据所涉案件具有合法管辖权时，应当肯定其出于司法审判需求原则上具有数据调取权，但应当限缩在一定范围内，即该数据调取对司法案件处理具有实质性影响。第二，如果数据请求国仅以其为数据处理者所在地国为由，要求调取存储于中国的数据，而该国既不对案件拥有管辖权，也不对数据的获取存在实质利益，则中国原则上可以予以拒绝。第三，出于个人信息保护要求，数据主体的国籍国或住所地国对调取本国公民数据具有利益，也就是说，当这类国家向中国申请的数据仅涉及其属人或属地管辖下的国民，且该数据出境不影响中国国家安全，则应当予以准许。

另一方面，从数据存储路径的角度，虽然数据存储在中国，但根据不同的数据存储安排，中国对他国的数据调取请求应当采取不同态度。第一，如果数据采取“完全数据本地云”路径，则应当肯定数据与存储地之间的紧密联系以及国家建立此种联系的正当性和必要性，从而肯定数据在中国存储是出于相关方的主动安排，则中国在这种模式下应当继续结合数据请求国类别对数据调取请求进行实质审查，即在不妨碍国家安全和个人隐私保护的情形下，原则上同意具有合法

① 支振锋：《网络主权根植于现代法理》，载《光明日报》2015 年 12 月 17 日，第 4 版。

② 方滨兴主编：《论网络空间主权》，科学出版社 2017 年版，第 82 页。

③ 黄志雄主编：《网络主权论——法理、政策与实践》，社会科学文献出版社 2017 年版，第 70 页。

司法管辖权的法院地国的数据调取请求；当个人数据不属于中国公民时，原则上同意数据主体所在地国的数据调取请求；同时，严格把控来自数据处理者所在地国的数据调取请求，原则上对其不予准许。第二，如果数据以“不完全数据本地云”路径存储在中国，且中国允许这种存储方式存在，那么中国实际上与被存储数据之间由于数据处理者设置的“可访问域”而缺乏实质联系，则应当通知请求国向属于“可访问域”的国家提出请求。第三，在“数据共享云”路径下，数据仅因技术安排偶然存储在中国境内，中国对该数据并不具有相关利益，除非有证据证明数据出境将有碍中国国家安全或个人信息保护，则应该进行形式审查后直接允许调取。第四，在“数据信托云”路径下，数据调取权应当以意思自治原则为基础遵守信托协议的安排。如果中国允许数据信托协议存在，即肯定了由协议双方通过意思自治将数据的控制与处理权限与某一方建立密切联系，则后期也应当肯定该方所在国的数据调取权，即直接根据信托协议安排决定是否允许调取数据。

总之，在跨境调取数据方面，中国在制度上已经表现出与普通数据跨境流动相似的立法倾向，即一方面基于整体国际形势和维护中国整体主权、安全和发展利益的需要，坚持数据主权理论，以司法互助协定和互惠方式作为数据跨境调取的主要方式；同时，考虑到促进数字经济发展、推动数据跨境流动、助力高效处理司法案件等目的，探索更加快捷的数据跨境调取路径，将灵活性与原则性相结合，动态地维护中国数据主权。

Exploring the Path of Cross-Border Data Access in China: Perspective on Data-Related Subjects and Storage Paths

Wei Qiuyue

Abstract: Under specific circumstances, cross-border data access needs to be supplemented with other paths based on traditional mutual legal assistance agreements. On the basis of bilateral mutual legal assistance agreements or the principle of reciprocity, China should explore more flexible and convenient paths for cross-border data access from the perspectives of both national security and personal information protection. From the perspective of data-related subjects, China should, in principle, allow access to data when the data requesting country has proper jurisdiction and access to data is of interest to the requesting country in hearing judicial cases, or when the data requesting country has personal jurisdiction over the data subject and the request only for the subject's data. From the perspective of data storage path, when China is only the data storage country in the "full storage mode", it is necessary to conduct substantive review of data requests from other countries in conjunction with the type of data requesting country, while in other storage modes, prior neutral technical means arrangements or preexisting trust agreements should be respected, thereby excluding some data access requests that do not require substantive review by the Chinese data authorities, so as to improve the efficiency of cross-border data access, reduce the pressure of review and advance transnational justice effectively.

Keywords: Data Access, Personal Information Protection, Data Sovereignty, Data Storage, Data Trust

（责任编辑：谭观福）