国际法研究

数据控制者取证模式的实践抵牾、理论反思及应对策略

王　雪

内容提要:数字化技术促使数据跨境取证成为必要,数据控制者取证模式的适用范围已遍及民事诉讼与刑事诉讼。该模式以属人管辖为立法依据,并融合合法权利标准与实际能力标准界定网络服务提供者控制的数据范围。数据主权的弱属地性并未颠覆既有的国际法管辖体系,数据控制者取证模式与域外执法管辖规则之间的制度性张力依旧存在,导致数据主权冲突难以避免。数据主权通过多维度的划分与组合可实现网络空间分层架构下的场景化适用。在网络空间内容层,国家主体可通过自主让渡数据威斯特伐利亚主权与数据国内主权,以强化数据相互依赖主权。单纯"防守"数据控制者取证模式效果不佳,我国须从"攻"与"防"两方面完善方案。一方面,我国有必要区分民事诉讼与刑事诉讼的性质差异,在搭建数据出境安全评估框架时作出不同设计。另一方面,在完善配套措施的前提下,强化我国阻断法的执行。

关键词:数据控制者取证模式　数据主权　数据出境安全评估　阻断法　域外管辖

王雪,内蒙古大学法学院讲师。

一　问题的提出

大数据时代执法机关或司法机关迫切需要跨境调取数据,由此引发的实践冲突已然成为我国在跨境诉讼中面临的重要难题。长期以来,国际社会实施的数据跨境取证方式大致可划分为"数据存储地取证模式"与"数据控制者取证模式"。前者在执法机关或司法机关取证中占据主导地位,即依据数据存储的地理位置来判断一国调取数据的管辖权范围。后者则是允许执法机关或司法机关要求为本国提供服务的运营商在特定情形下提交掌握或控制的数据。

针对数据控制者取证模式引发的争议,有学者研究主权冲突下的对等回应与互

惠,[1]也有学者从多主体协同取证的角度研究应对策略,[2]或是从不同数据存储方式的角度分析跨境调取路径。[3] 2024 年 12 月,联合国大会审议通过《打击为犯罪目的使用信息和通信技术行为的全面国际公约》(*Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*,下称"《联合国打击网络犯罪公约》")。然而,数据控制者取证模式引发的对立依旧没有得到有效解决。面对他国单边数据跨境取证行为,我国执法机关与企业仍显得较为被动。鉴于此,本文在剖析数据控制者取证模式引起的核心冲突的基础上,探索缓和跨境取证摩擦的路径,并尝试从进取与防御的双重方向提出我国的应对策略。

二 数据控制者取证模式的制度嬗变与理论基础

在解决数据控制者取证模式引发的争议之前,有必要梳理这一制度的规则变化,探究其发展动向,明晰其理论基础。

(一)数据控制者取证模式的国际动向

数据控制者取证模式在民事和刑事领域均有适用空间。鉴于不同诉讼领域数据跨境取证的现行规则存在差异,有必要区分讨论。

1. 民事单边域外取证制度冲击国际协助框架

国际社会就民事案件的跨境取证曾达成多边协作框架。1970 年《关于从国外调取民事或商事证据的公约》(*Convention on the Taking of Evidence Abroad in Civil or Commercial Matters*,下称"《海牙取证公约》")作为国际民事司法协助领域最重要的多边条约之一,旨在协调各国跨境取证的法律冲突。其最核心的制度设计是制定了请求书取证模式,要求各缔约国指定中央机关,负责接收并转递来自其他缔约国司法机关的请求书。

然而,《海牙取证公约》所确立的国际民事司法协助框架已然受到单边域外取证制度的侵蚀。由于《海牙取证公约》并未回答其是否能够优先于国内法律规范得到排他性适用的疑问,1987 年美国联邦最高法院在 Societe Nationale Industrielle Aerospatiale v. United States Dist. 案中裁决《海牙取证公约》并非美国获取国外证据的唯一或强制程序。换言之,该公约相较于美国国内的取证程序不具备优先性,只是选择性补充。[4] 自该案后,美国司法实践倾向于使用《联邦民事诉讼规则》(*Federal Rules of Civil Procedure*)第 34 条与第 45 条规定的证据开示制度进行域外取证。证据开示制度可由一方当事人单方面启动,请求对象既包括案件当事人也包括案外人,请求开示的证据范围广泛且以美国法

〔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 206 页。

〔2〕 参见裴炜:《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》,《河北法学》2021 年第 4 期,第 77 页。

〔3〕 参见魏求月:《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》,《国际法研究》2023 年第 3 期,第 81-82 页。

〔4〕 See Societe Nationale Industrielle Aerospatiale v. United States Dist. Court for S. Dist., 482 U. S. 522, 107 S. Ct. 2542 (1987).

院强制执行为保障。[5] 相似地,澳大利亚联邦法院在 Joyce v Sunland Waterfront (BVI) Ltd 案[6]中,也直接以《1976 年澳大利亚联邦法院法》(*Federal Court of Australia Act 1976*)第 47A 条为依据跨境取证,而非借助请求书模式或外交渠道申请取证。综上,一国法院可绕开《海牙取证公约》确立的"公对公"取证模式,适用国内法律规范实施单边域外取证。

2. 刑事数据跨境取证制度的阵营化

国际社会为满足刑事数据跨境取证的需求所采取的合作模式出现明显的阵营化和政治化。一方面,2018 年美国颁布了《澄清合法使用境外数据法》(*Clarifying Lawful Overseas Use of Data Act*,下称"《云法案》"),成为刑事案件中数据控制者取证模式的典型代表。《云法案》所建构的跨境数据取证规则引起扩散效应,推动数据控制者取证模式在全球扩张。以欧盟国家作为主要缔约国的区域性多边条约《布达佩斯网络犯罪公约》(*Convention on Cybercrime*)[7]于 2021 年推出第二附加议定书,加强与其他缔约国境内网络服务提供者的直接合作。依据第二附加议定书第 6 条第 1 款和第 7 条第 1 款,某一缔约国的主管当局可以直接请求其他缔约国境内的网络服务提供者提供域名注册信息或用户信息。2023 年欧盟正式通过《关于刑事诉讼中的电子证据和刑事诉讼后执行监禁判决的欧洲提交令和保存令的第 2023/1543 号条例》[*Regulation (EU) 2023/1543 on European Production and Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings*,下称"《电子证据条例》"]。欧盟成员国的司法机关可通过发布数据提交令和保存令直接要求在欧盟境内提供服务的网络服务提供者出示或保全电子证据,无需考虑数据位置。

另一方面,发展中国家对以欧美为代表的数据控制者取证模式持反对立场。鉴于发达国家与发展中国家之间的数字鸿沟依旧明显,数据控制者取证模式致使发展中国家将长期受到数据霸权的消极影响。2019 年在中国与俄罗斯倡议下,第 74 届联合国大会决定设立政府间专家委员会负责拟订《联合国打击网络犯罪公约》。[8] 鉴于跨境向网络服务提供者直接调取数据涉及数据主权与安全的问题,数据控制者取证模式遭到俄罗斯、南非和伊朗等国的强烈反对。[9] 经过多重谈判,2024 年 12 月《联合国打击网络犯罪公约》最终通过,其中第 5 条强调保护主权为基本原则。同时第 27 条"提交令"条款允许境内网络服务提供者提交所拥有或控制的用户信息。此时数据或用户信息的地理位置位于不同的司法管辖区并不会影响这一条款的适用。[10] 可见,发展中国家与发达国家在谈判博弈后,仅就用户信息的跨境调取采取数据控制者取证模式达成共识,针对其余数据依旧采用

---

〔5〕 参见胡洋铭:《美国事证开示程序的域外效力及阻断路径探究》,《争议解决》2021 第 4 期,第 212-214 页。

〔6〕 See Joyce v Sunland Waterfront (BVI) Ltd [2011] FCAFC 95.

〔7〕 2001 年欧盟成员国与美国、日本等 30 多个国家于布达佩斯签署,该公约也成为世界上第一部专门打击网络犯罪的国际条约。

〔8〕 参见叶伟:《〈联合国打击网络犯罪公约〉:进展、前景与展望》,《北京航空航天大学学报(社会科学版)》2021 年第 5 期,第 32-33 页。

〔9〕 参见王渊洁:《联合国网络犯罪政府专家组第五次会议综述》,载中国国际法学会主办《中国国际法年刊(2019)》,法律出版社 2020 年版,第 354 页。

〔10〕 考虑到《联合国打击网络犯罪公约》第 27 条尚未有应用的现实案例,实施效果还需继续观察。

司法协助的方式予以跨境取证。

(二)数据控制者取证模式的理论支撑

数据控制者取证模式应用的关键在于管辖范围的判断,包括国家管辖的网络服务提供者的范围以及网络服务提供者所控制的数据范围。

1. 以对网络服务提供者的属人管辖权为依据

数据控制者取证模式将跨境调取数据的关键因素从数据存储的地理位置转移到对网络服务提供者的管辖权。从管辖权基础来看,无论是民事案件还是刑事案件,数据控制者取证模式的立法依据均接近属人管辖原则。

在民事案件的数据跨境取证中,法院具有合理的属人管辖权是实施证据开示的前提条件。2015 年美国纽约地区法院在 Gucci America, Inc. v. Weixing Li 案中阐明,“美国地区法院必须对非当事人具有属人管辖权,才能迫使其遵守第 45 条”。[11] 中国银行满足“最低限度联系”,因而美国纽约地区法院可对位于北京的中国银行总部行使属人管辖权并判决其提供相关的通信记录。在刑事案件的数据跨境取证中,属人管辖原则依旧是数据控制者取证模式实施的依据。其一,美国《云法案》第 102(2)条款强调管辖对象是“受美国管辖的通信服务提供者”。2019 年美国司法部发布白皮书,宣称美国司法机构对属人管辖的审判秉持“最低限度联系”的判断标准。这与 Gucci Am., Inc. v. Weixing Li 案中法院对中国银行行使属人管辖权的裁决思路一致。其二,欧盟《电子证据条例》同样以对网络服务提供者的属人管辖为核心。《电子证据条例》第 2 条与第 3 条将适用对象限定为“在欧盟境内提供服务的服务提供商”,并以网络服务提供者与其所提供服务的成员国具备实质性联系作为核心要件。这一判断标准吸收了 2015 年“雅虎案”的思路,[12] 即雅虎公司虽在比利时没有实体经营场所,但其将经济活动指向比利时的消费者,以比利时为目标,表明其自愿接受比利时法律的约束,可认定在比利时具有实际存在。

2. 合法权利标准与实际能力标准融合界定控制范畴

数据被特定的网络服务提供者所持有或控制是执法机关或法院跨境调取的前提。美国《云法案》第 103 条将披露或保存的数据范围界定为受美国管辖的网络服务提供者占有、保管或控制的所有数据。“占有”和“保管”的定义很少引起争议,因为它们均指“是或否”的二元命题,而“控制”则不那么明确。尽管《云法案》尚未界定“占有、保管或控制”,但美国法院已在判例中就《联邦民事诉讼规则》第 45(a)(1)条与《联邦刑事诉讼规则》第 16(a)(1)条中的同一术语进行了广泛论证。整体而言,美国判例法对“控制”有两种测试标准:一是合法权利标准;二是实际能力标准。前者指一方主体拥有获取文件、电子存储信息以及其他有形物品的合法权利;后者指一方主体具备获取文件、电子存储信息以及其他有形物品的实际能力。[13]

合法权利标准用于确定美国公司是否“控制”外国关联公司所持有的文件。美国法院在判断“控制权”时会考虑两项因素。第一,网络服务提供者是否拥有获得所需文件的

〔11〕 Gucci Am., Inc. v. Weixing Li, 135 F. Supp. 3d 87 (S. D. N. Y. 2015).

〔12〕 Hof van Cassatie [Court of Cassation], Dec. 1, 2015, Nr. P. 13. 2082. N (Belg.).

〔13〕 See The Sedona Conference, The Sedona Conference Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control”, 25 *The Sedona Conference Journal* 1,18 (2024).

法定权利,如总公司被强制要求交出外国分支机构持有的数据。[14] 第二,网络服务提供者是否与关联实体人格混同,法院可揭开公司面纱。[15] 例如,若母公司对子公司拥有完全控制权,则表明母公司在法律上有能力指导子公司数据的使用或转移。[16] 采用实际能力标准的执法机关或法院无需考虑网络服务提供者是否在法律上拥有合法权利获取。如果网络服务提供者有实际能力获得执法机关或司法机关要求的数据,它将必须披露。鉴于在数据跨境取证中不可能排除对网络服务提供者实际控制能力的考量,美国联邦巡回上诉法院已然将合法权利标准与实际能力标准融合使用。美国联邦第三巡回上诉法院在Gerling Int'l Ins. Co. v. Comm'r Gerling Int'l Ins. Co. 案中主张,如果子公司作为代理人,基于业务需要可以获得委托人母公司的文件,法院将不允许子公司否认控制权。[17] 判断母子公司之间业务关系实则属于对子公司实际能力的判断。此后,美国联邦第四、第八、第九、第十、第十一巡回上诉法院也前后融合使用合法权利与实际能力两种标准。[18]

《布达佩斯公约》解释性报告第173段也对第18条"提交令"的"占有"或"控制"予以解读。报告阐释,网络服务提供者占有或控制的数据不仅包括其实际占有的数据,也包括在其控制下远程存储的数据。可见,《布达佩斯公约》对控制的解读不仅包括法定占有的数据,也包含对实际能力的考量。《联合国打击网络犯罪公约》第27条借鉴了《布达佩斯公约》第18条,因此,其对网络服务提供者控制权的解读也有相同的逻辑。

三 实践抵牾:数据主权冲突与合规困境

不可否认,数据控制者取证模式确实达到高效取证和成本低廉的效果,但美国与欧盟是以国内法或区域统一立法的方式试图单边跨境调取数据,极易与他国产生主权与规范层面的冲突。

(一)数据控制者取证模式引发数据主权冲突

数据主权冲突是数据控制者取证模式引发的核心矛盾,调和国家在数据领域的摩擦均绕不开对主权问题的探讨。

1. 数据主权的弱属地性不足以推翻域外管辖规则

国内学界普遍认同数据主权系传统主权在数字空间的延伸,强调国家对数据的控制权与排他性;[19] 而西方"数据例外主义"理论则主张数据的特殊性质解构了属地管辖的

〔14〕 See In re Grand Jury Proceedings Bank of Nova Scotia, 740 F. 2d 817 (11th Cir. 1984).

〔15〕 See Johnathan D. Jordan, Out of Control Federal Subpoenas: When Does a Nonparty Subsidiary Have Control of Documents Possessed by a Foreign Parent, 68 *Baylor Law Review* 189, 199 (2016).

〔16〕 See Justin Hemmings, Sreenidhi Srinivasan & Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, 10 *Journal of National Security Law and Policy* 631, 656 (2020).

〔17〕 See Gerling Int'l Ins. Co. v. Comm'r Gerling Int'l Ins. Co., 839 F. 2d 131 (3d Cir. 1988).

〔18〕 See The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control", 25 *Sedona Conference Journal* 1, 28 (2024).

〔19〕 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68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64页;朱雅妮:《数据主权及其在〈数据安全法〉的体现》,《浙江工业大学学报(社会科学版)》2021年第4期,第420-421页。

根基,需重构独立于传统国际法的数据管辖规则体系。〔20〕 这一争议实质上指向两个根本性问题:其一,当主权延伸到数据领域时是否依旧具备属地性;其二,国际法域外管辖的规则是否可以继续适用于数据领域。该双重追问不仅涉及数据主权的法理证成,更构成跨境数据取证国际合作机制建构的逻辑起点。

不可否认,数据的流动性、可复制性以及位置的独立性意味着数据流动不受领土边界的限制,〔21〕但数据主权的属地性依旧广泛存在于网络空间的物理层、逻辑层与内容层,〔22〕主权国家可借此实现管辖。其一,国家对物理层所包含基础设施的管辖具有强烈的属地特征。尽管数据在全球范围内流动,但操纵数据的设备或主体依旧受到某个国家的领土管辖。位于国家境内的网络基础设施受到法律规范的制约和保护,国家主体可采取措施行使立法、执法以及保护的权力。因而,数据主权属地性的特征在物理层较为突出,网络大国对网络基础设施行使主权也不存在原则性分歧。〔23〕 其二,数据主权在逻辑层依旧具备属地性。虽然互联网技术的 TCP/IP 协议或域名系统全球通用,但依旧会受到国家领土边界的限制。为应对地缘政治风险,俄罗斯创建本国独立域名系统并成功进行断网测试。〔24〕 该实践揭示主权国家可通过切断国际根服务器链接,在领土范围内重置网络逻辑架构,其本质是以技术自主权强化逻辑层控制能力。其三,数据本地化措施在内容层强化国家的数据控制权。我国《网络安全法》第 37 条与《数据安全法》第 31 条要求关键信息基础设施的运营者在中国境内收集的个人数据与重要数据须在中国境内存储。

综上,主权国家依旧可以通过技术治理与法律规制的交互作用维系对数据的管辖,属地性弱化不构成对既有管辖规则的体系性颠覆。“数据例外主义”理论否认数据主权的属地性,本质是为数据控制者取证模式寻求理论支持。

2. 单边域外执法挑战他国数据主权

数据控制者取证模式引发争议的核心原因在于其赋予了执法机关或司法机关域外执法的权力,侵犯了数据存储国对境内数据的执法管辖权。在习惯国际法规则中,域外执法管辖权受到一般禁止,一国在他国内部的任何执法行为均被认为侵犯了他国对其境内执法管辖权的垄断。〔25〕 尽管数据的特殊性质对国际管辖规则造成挑战,但数据的弱属地性不足以成为原有国际管辖规则的例外。数据控制者取证模式并非只是实行域外立法管辖或域外司法管辖,其根本目的是赋予一国公权力机关以数据跨境取证的域外执法权。单边主义下一国制定的法案不足以构成执法机构调取境外数据的合法性基础。无论是以证据开示制度为代表的民事域外取证,抑或是以《云法案》为标志的刑事数据单边取证,执

〔20〕 See Jennifer Daskal, The Un-territoriality of Data, 125 *Yale Law Journal* 326 (2015).

〔21〕 See Jennifer Daskal, Borders and Bits, 71 *Vanderbilt Law Review* 179, 221 (2018).

〔22〕 2006 年学者约查伊·本克勒(Yochai Benkler)运用层次表述法概括传播信息的媒介所具备的基本功能,并将媒介划分为物理层、逻辑层和内容层。See Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale University Press, 2006, p. 392.

〔23〕 参见黄志雄著:《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 71 页。

〔24〕 参见《俄罗斯举行首次国家级防“断网”演习》,http://world.people.com.cn/n1/2019/1225/c1002-31522453.html,最近访问时间[2025-04-20]。

〔25〕 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 105 页。

法机关或司法机关均是以在立法层面对网络服务提供者享有属人管辖权为依据,但却主观忽视单边调取境外数据的执法行为缺乏国际法依据这一事实。美国司法部在白皮书中宣称《云法案》并未将美国的管辖权扩展到任何新的当事方,[26]这一解释本质上混淆了习惯国际法对域外立法管辖权和域外执法管辖权的不同限制。数据控制者取证模式导致数据存储国难以控制其他国家对本国境内数据的访问和获取,而控制权作为数据主权的核心表现,数据存储国的数据安全将受到冲击。即使在看似无国界的网络空间,未经国际法赋予特定权力或外国政府有效同意的数据域外执法行为依旧可能侵犯他国主权。因此,仅仅以取证高效为由单方面强制调取存储在他国数据的行为违反国际管辖规则,极易引发数据主权冲突。

(二)数据控制者取证模式下的合规困境

数据控制者取证模式忽视了他国在个人数据保护、数据安全以及为抵制数据控制者取证模式等方面颁布的立法规范,导致网络服提供可能被迫承担行政或刑事责任。

1. 礼让弱化下民事数据跨境取证的法律冲突

美国法院通过消解、规避或美国主权利益优先的方式,否认中国《个人信息保护法》《数据安全法》以及阻断法对数据跨境取证的限制,拒绝承认存在法律冲突,限缩国际礼让分析框架的适用范围。[27]

第一,美国法院借助解释论证消解数据跨境取证命令与我国《个人信息保护法》的分歧,否认存在真实法律冲突,拒绝适用国际礼让。2022 年,在 Design Systems, Inc. v. SyntronicAB 案中,美国首席治安法官斯佩罗(Joseph C. Spero)将“外国法院的命令”解读为符合我国《个人信息保护法》第 13 条第 3 款“为履行法定职责或者法定义务所必需”这一例外情形。其主张美国法院发布的跨境调取数据的命令属于中国企业应当遵守的法定义务,所以无须取得我国数据主体的同意。[28] 因此,法院裁决,中国法律与美国法院的命令之间不存在真实的法律冲突,不满足适用国际礼让分析的前提,驳回了申请。

第二,美国法院借助“话术包装”规避我国阻断法。为防止美国不当域外管辖,我国在刑事、民事以及行政立法中已经构建了多重阻断条款。如 2018 年《国际刑事司法协助法》第 4 条、2021 年《数据安全法》第 36 条、《个人信息保护法》第 41 条以及 2024 年《民事诉讼法》第 294 条。但现实中我国企业面临数据跨境取证时,上述阻断法难以起到实际效果。2022 年,在 Philips Med. Sys. (Cleveland), Inc. v. Buan 案中,美国伊利诺伊州北区地区法院运用“话术包装”的技巧,借助美国普通法体系的诉讼特点,将“证据开示”包装成仅在当事人之间进行的程序,否定司法机关参与所披露数据的管理或使用。换言之,其仅通过文字的表层含义将对数据披露请求的回应有意识地解读为当事人之间的交易,而非向美国法院履行义务,从而规避中国《数据安全法》第 36 条,主张无须进行礼让分析。[29]

---

〔26〕 See Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act White Paper, https://www.justice.gov/opa/press-release/file/1153446/dl, 最近访问时间[2025-04-20]。

〔27〕 参见李贤森:《民事域外取证与数据出境监管的冲突及应对》,《比较法研究》2025 年第 1 期,第 218 页。

〔28〕 See Cadence Design Sys. v. Syntronic AB, 21-cv-03610-SI (JCS) (N. D. Cal. June 24, 2022).

〔29〕 See Philips Med, Sys, (Cleveland), Inc. v. Buan, 19 CV 2648 (N. D. Ill. Mar. 1, 2022).

相似地,在 Intex Rec. Corp. v. Bestway (USA), Inc. 案中,美国加利福尼亚州中区地区法院也以同样理由规避了中国《数据安全法》第 36 条与《民事诉讼法》原第 284 条,[30]要求厦门某公司继续披露数据。[31]

第三,即便美国法院承认证据开示命令与我国阻断法之间存在真实冲突并运用国际礼让予以分析,但在考量国家利益要素时,却以我国阻断法不具有执行性为由强调美国国家利益优先。在 Concepts Nrec, LLC v. Xuwen Qiu 案中,美国佛蒙特州区地区法院认可需要对法律冲突进行礼让分析。但在分析国家主权利益时,法院主张被告没有举出因披露数据而遭到中国阻断法处罚的案例,"美国在保护自己的商业秘密和知识产权方面具有重大利益……中国执行其法律的总体目标并不比美国的利益更重要"。[32]

2. 平衡测试下刑事数据跨境取证的规则对抗

鉴于刑事立法的公法属性,刑事数据跨境取证相较于涉外民事诉讼更加强调司法主权与国家意志,单边调取行为更具有侵入性。美国《云法案》与欧盟《电子证据条例》为缓解刑事数据跨境调取中的规则对抗设置平衡测试。

第一,美国《云法案》在平衡网络服务提供者的义务时,依旧运用了国际礼让的分析框架,但却设置了极为苛刻的前提条件。只有当用户并非美国人且不在美国居住,且披露将会使网络服务提供者面临违反"适格外国政府"法律的实质性风险时,美国法院才会酌情考虑进行礼让分析。但评估"适格外国政府"的因素众多、程序繁琐,《云法案》颁布后只有英国、澳大利亚两国被美国认定为"适格外国政府"。是故,《云法案》礼让分析的适用范围极为狭窄,展现了美国立法的"双重标准"。虽然在执法机关通过行政传票调取用户信息与交易数据时,美国法院也可开展国际礼让分析,但我国阻断法难以得到执行成为美国法院驳回抗辩的常用理由。以 2019 年"中资银行案"为例,美国华盛顿特区联邦上诉法院认为我国银行无法提供因违反阻断法而遭到行政机关处罚的案例,因而银行对违反阻断法的担忧只是猜测。[33] 这意味着我国银行将长期面临外国刑事数据跨境取证的命令与我国阻断法相冲突的局面。

第二,欧盟平衡测试的立法态度发生转变。依据《电子证据条例》第 17 条,当主管法院审查确定第三国法律禁止披露有关数据,应评估是维持还是取消提交令。与美国不同的是,欧盟在平衡测试中对评估考量因素的比重予以赋权,着重考虑受第三国相关法律保护的利益以及刑事案件与两个司法管辖区之间的关联程度这两项要素。前者包括第三国法律保护的基本权利和阻止披露数据的基本利益,特别是第三国的国家安全利益;后者着重分析数据主体或刑事犯罪受害者的所在地、国籍和居住地以及刑事犯罪的发生地。尤其强调,仅凭数据存储地点不足以确定实质性联系程度。然而相比于初稿,《电子证据条例》最终不再要求主管法院咨询第三国中央当局的意见,而是根据上述因素由法院自由衡量。但刑事数据跨境取证冲突的背后是国家主权意志的碰撞,一国法院也难以真正理

〔30〕 在 2024 年新修订的《民事诉讼法》中,该条款的编号改为第 294 条。

〔31〕 Intex Rec. Corp. v. Bestway (USA), Inc., CV 19-8596-JAK(Ex) (C. D. Cal. Oct. 30, 2023).

〔32〕 Concepts Nrec, LLC v. Xuwen Qiu, 662 F. Supp. 3d 496 (D. Vt. 2023).

〔33〕 In re Grand Jury Investigation, 381 F. Supp. 3d 37 (D. D. C. 2019).

解对外国阻断法的立法理念,更不会让自身成为外国主权意志的代理人,因而平衡测试反而可能成为域外管辖权扩张的工具。

四　理论反思:数据主权的场景化适用

数据控制者取证模式引发的矛盾折射出国家主体之间数据主权的激烈竞争。2015年我国国务院在《促进大数据发展行动纲要》中强调"增强网络空间数据主权保护能力",这一表述表明我国坚定维护数据主权的独立自主并排斥他国干涉的理念。随着我国深入参与全球数据治理,这一理念从"防守"他国干涉向动态灵活地维护数据主权转变。例如2024年我国《促进和规范数据跨境流动规定》第3条、第4条及第5条规定国际贸易等特定活动免于申报出境安全评估。可见,我国在维护数据主权的独立权、平等权、自卫权与管辖权等核心权能不受侵犯的同时,也包容数据流动对开放性的需求。同样,在数据跨境取证中,数据主权的适用并非是在自由与安全的价值选择之间"一刀切"。网络空间分层架构下数据主权的场景化适用可以为调和数据跨境取证冲突提供核心理念。

(一)数据主权的多维度划分

鉴于传统的主权理论无法适应新的国际形势,学者们对主权概念的理解不再是静态单一的,而是逐步划分为多维度。学者克拉斯纳(Stephen D. Krasner)将主权内涵横向划分为四种不同的维度:[34]国内主权(domestic sovereignty)、相互依赖主权(interdependence sovereignty)、国际法律主权(international legal sovereignty)以及威斯特伐利亚主权(Westphalian sovereignty)。不同维度的主权不一定是共存的。以此为参照,数据主权的内涵也可以划分为不同维度:第一,数据国内主权,即国家对境内数据的控制力度;第二,数据威斯特伐利亚主权,即排斥他国干涉本国境内数据;第三,数据相互依赖主权,即国家公权力机构对跨境数据的控制力;第四,数据国际法律主权,即国家以独立法律主体的身份同其他国家签订数据相关的协议或加入国际组织。

主权涵义的多维度划分为数据主权的场景化适用提供了实现路径。[35] 鉴于在物理层数据主权的属地性最为明显,国家依据属地管辖原则对物理基础设施可直接行使排他性管辖权。当场域延伸至逻辑层时,主权国家需通过技术手段对数据传输路径实施监管,实施成本较物理层显著提升。及至内容层,数据本地化的政策虽能强化管控数据流动的能力,但同时减损跨境数据流动效率,形成负外部性效应。由此可见,从物理层上升到内容层,数据主权的属地性减弱,主权国家实施数据规制的边际成本呈攀升态势。这也折射出数据主权的规制效力在网络空间呈现显著的梯度性特征。基于此,数据主权的四项维度在网络空间的不同分层将呈现差异化运行。从物理层向内容层的延伸过程中,数据威斯特伐利亚主权的排他性与数据国内主权的控制力呈现衰减态势;而数据相互依赖主权则因国际社会对数据跨境流动的需求上升而呈现增长倾向;作为基础的数据国际法律主

〔34〕 See Stephen D. Krasner, *Sovereignty: Organized Hypocrisy*, Princeton University Press, 1999, p. 4.

〔35〕 参见许可:《自由与安全:数据跨境流动的中国方案》,《环球法律评论》2021年第1期,第36页。

权因涉及国家主体的国际法律资格则保持恒定(见图 1)。这意味着数据主权的适用需结合网络空间的分层架构和多维度划分设置不同范式。

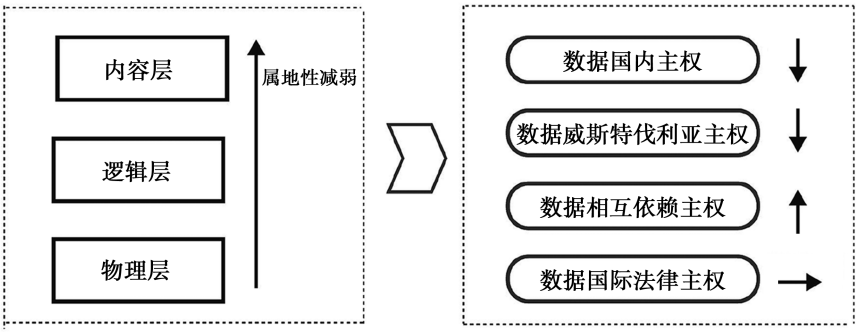

图 1 数据主权多维度划分与差异化运行

(二)数据主权的多维度组合

在国际关系中,国家作为国际法律主体,为获得合理的对价(如互惠)让渡自身部分主权权能,同时保留随时恢复让渡权能的方式。为不损伤主权的根本属性,主权的让渡是自主且有限的。[36] 基于数据主权的多维度划分与差异化运行特征,在保障数据国际法律主权不受损的前提下,数据主权的其余三项维度可依据国家利益的需求予以组合。

第一,当数据跨境取证涉及调取位于被请求国领土范围内的电子设备时,遵循“公对公”架构的民事或刑事司法协助程序是不侵犯被请求国数据主权的唯一合法措施。物理层明显的属地性意味着被请求国具备有力的数据控制权并强烈排斥他国干涉。当请求国执法或司法机关单边要求被请求国的网络服务提供者提供电子设备以获取特定数据时,被请求国的数据主权无疑遭到严重侵犯。在 Juul Labs, Inc. v. Chou 案中,美国加利福尼亚中区地区法院承认调取电子设备的取证方式具有较强的侵入性且将给被告带来的沉重负担,支持被告以我国《数据安全法》第 36 条为依据提出的抗辩。[37] 可见,美国法院对于跨境调取电子设备的态度较为审慎。所以,在物理层,只有依据司法协助条约或者互惠开展的司法协助程序是尊重数据主权的合法路径。

第二,当数据跨境取证涉及内容层时,数据主权不同维度的相互组合须依赖程序主义与数据分类分级的配合。[38] 一方面,程序主义意味着当数据的单边监管影响到他国利益时,所有受到影响的国家主体均有发言权,并通过国际谈判和协议来实现其立场。[39] 内容层是数据本体所在的主要空间分层,数据威斯特伐利亚主权与数据国内主权本身会呈现衰减态势,而数据跨境流动的效益追求促使国家主体急需强化数据相互依赖主权。但值得警惕的是,在数据控制者取证模式弱化了被请求国前两项数据主权维度的同时,数据

〔36〕 参见刘凯著:《国家主权自主有限让渡问题研究》,中国政法大学出版社 2013 年版,第 82-89 页。

〔37〕 Juul Labs, Inc. v. Chou, 2:21-cv-03056-DSF-PDx (C. D. Cal. Apr. 19, 2022).

〔38〕 除却物理层与内容层,逻辑层的核心功能在于通过协议规则与算法系统实现数据的结构化传输,控制对象不包括数据本体。因此逻辑层并不涉及本文所述的跨境调取数据的争议。

〔39〕 See Adeno Addis, The Thin State in Thick Globalism: Sovereignty in the Information Age, 37 *Vanderbilt Journal Transnational Law* 1, 60 (2004).

相互依赖主权并不必然得到提升。因为数据控制者取证模式具有单边性,美国《云法案》甚至实施“双重标准”。可见,在内容层数据主权至关重要的并非不受外部干扰,而是国家有机会参与国际社会数据治理。因而,在内容层数据主权的多维度组合以国家平等协商或政府的授权同意为前提,实现自主有限的让渡数据威斯特伐利亚主权与数据国内主权,并强化数据相互依赖主权。《联合国打击网络犯罪公约》第 27 条“提交令”就“用户信息”实行数据控制者取证模式达成共识,是国际社会应用程序主义场景化适用数据主权的典型代表。另一方面,数据主权多维度的组合需要配合数据分类分级。我国《数据安全法》根据数据的重要程度以及非法滥用后的危害程度,将数据划分为一般数据、重要数据和核心数据。与我国立法从安全视角的划分不同,现有涉及数据跨境取证的国际条约中倾向于将网络服务提供者掌握的数据划分为“用户信息”“流量数据”以及“内容数据”,不同类型数据跨境调取的条件也由弱趋强。〔40〕 数据分类分级的本质均是为了区分不同数据背后的主权属性。若数据泄露引发的风险波及国家安全或公共利益,须国家主动保护,则数据具有较强的主权属性;相反,若风险或损害局限于私域,且主体享有救济方式,则数据所附有的主权属性较弱。〔41〕《联合国打击网络犯罪公约》第 27 条“提交令”之所以将范围局限于“用户信息”,便是因为用户信息主权属性较弱,被强制调取在多数场景下不涉及国家安全或公共利益,风险限于私域范围。而针对其他数据,国家主体须在平等协商中依据国家利益考量让渡数据主权的限度,以满足自身对数据跨境取证的个性化需求,在不影响国家安全与公共利益的前提下,国家主体可就境内特定类型的数据降低控制力度,同时强化数据相互依赖主权,从而满足自身对数据跨境取证的个性化需求(见图 2)。

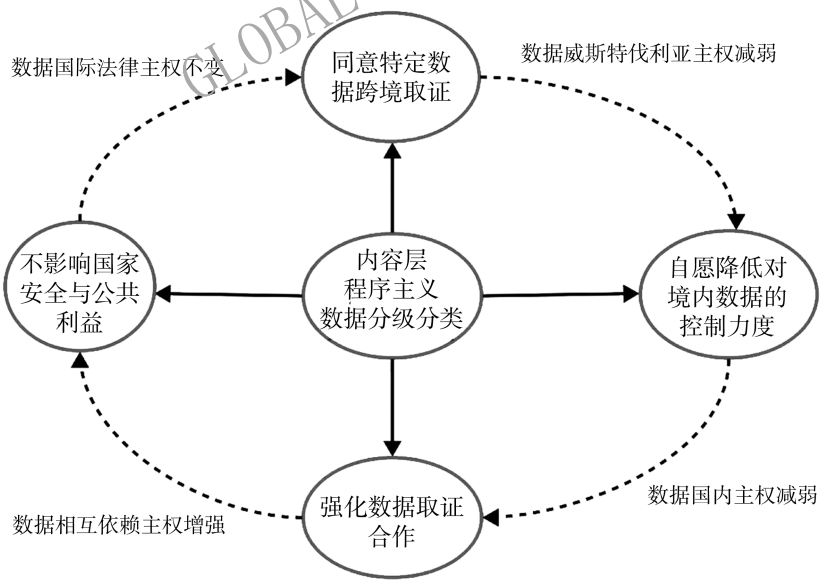

图 2　数据主权在内容层的多维度组合

〔40〕 参见梁坤:《网络犯罪国际公约中的跨境调取数据条款》,《当代法学》2024 年第 2 期,第 128 页。

〔41〕 参见吴玄:《数据主权视野下个人信息跨境规则的建构》,《清华法学》2021 年第 3 期,第 84 页。

五 数据控制者取证模式下的中国方案

虽然我国适用数据主权的理念有所转变,但数据立法整体倾向依旧着重防御而“进取”不足,所以可从“攻”与“守”两个方面优化数据跨境取证方案。

(一)搭建数据出境安全评估框架

鉴于民事诉讼是解决平等主体之间权益争议的程序,更多关注个体权益的平衡与保护,而刑事诉讼本质上是国家惩罚权的实现过程,司法职权理念较强。因此,设置数据出境安全评估框架须区分民事与刑事案件的性质差异。

1. 设立民事案件数据出境安全评估通道

我国民事案件数据跨境取证的立法范式出现转变,但立法态度却呈现“内外不一”。《民事诉讼法》第 284 条第 2 款规定,若所在国法律不禁止且双方当事人同意,我国法院可以采用即时通讯工具取证或双方当事人同意的其他方式取证。这意味着无需借助民事司法协助,我国法院可以直接跨境取证。虽然《民事诉讼法》并未将数据跨境取证的对象延伸到第三方网络服务提供者,但不可否认,此条款彰显我国域外民事证据取证制度出现转型。然而,《民事诉讼法》第 294 条阻断条款与 2023 年司法部发布的《国际民商事司法协助常见问题解答》第二部分“关于调查取证”的回答依旧强调外国司法机关调取我国境内的数据须通过民事司法协助程序,[42] 立法价值取向的“内外不一”可能引发主权信用危机。鉴于《海牙取证公约》确未规定公约相较于国内法具有排他性与优先性,是故,我国可在民事司法协助体系之外建立常态化民事案件数据出境安全评估通道。

第一,明确民事案件数据出境安全评估的方式及审查内容。一方面,鉴于我国司法协助中心已建立线上系统处理境外机构通过司法协助递交的申请,数据出境安全评估通道也可通过电子化方式为网络服务提供者或外国司法机关提供便利,同时为司法协助交流中心的受理设置时限以保障司法效率。另一方面,明确审查内容。《数据出境安全评估办法》第 5 条已规定网络服务提供者自评估的考量因素。我国可以参考上述条款细化民事案件数据出境安全评估的审查内容。例如审查网络服务提供者与请求国的联系程度、被调取数据的类型与范围、数据出境的合法性与必要性以及出境对国家安全、公共利益、个人或者组织合法权益带来的风险等。

第二,为我国网络服务提供者设置豁免情形。鉴于 2024 年《促进和规范数据跨境流动规定》已然就特定场景下的数据出境作出豁免规定,在民事案件数据跨境取证中我国立法也有必要允许网络服务提供者在特定情形下向外国执法机关或法院提供相关数据,无需因阻断条款的存在担责。豁免应当符合以下要件:其一,我国网络服务提供者与请求国存在紧密联系,如在申请国设立分公司或是控股子公司,这意味着其将长期在请求国开展业务且有权干预外国业务的数据流动。其二,请求国调取的数据不涉及网络服务提供

〔42〕 参见《国际民商事司法协助常见问题解答》,https://www.moj.gov.cn/pub/sfbgw/jgsz/jgszzsdw/zsdwsfxzjlzx/sfxzjlzxxwdt/202503/t20250324_516204.html,最近访问时间[2025-5-20]。

者在我国境内的业务且不涉及我国境内人员的数据,即与我国境内开展的经济活动或数据主体无关。其三,不包括重要数据与核心数据。

2. 调整刑事案件数据出境安全评估机制

2024 年《关于实施〈中华人民共和国国际刑事司法协助法〉若干问题的规定(试行)》(下称"《规定》")第 12 条设立"刑事证据出境审查工作机制",办公室归属司法部统筹。值得注意的是,《规定》第 14 条允许我国境内的个人或机构经审查后向外国主动提供证据,这表明我国刑事案件数据出境的刚性防御态势有所松动。但《规定》尚未区分依刑事司法协助程序开展的数据出境安全评估与依数据控制者取证模式提出的数据出境安全评估。前者是基于主权让渡形成的条约义务体系,无论数据处于物理层抑或是内容层,均不会有损数据主权,但后者则不同。而相较于民事案件,刑事诉讼更强调司法安全,因此有必要区分两种模式下的数据出境安全评估机制。

第一,简化依据刑事司法协助程序开展的数据出境安全评估。刑事司法协助条约或互惠的许诺均代表外国与我国彼此间经风险评估后达成的合意,蕴含着国家主体间的政治互信。倘若被申请的数据出境并不危害国家安全与公共利益,且请求国提交的材料满足形式要件,原则上数据应被允许出境。我国可借鉴《联合国打击网络犯罪公约》第 45 条"实时收集流量数据方面的司法协助"规定的要件,简化司法协助申请书的审查要素。此外,刑事司法协助下调取的数据范围可由双方基于政治互信或协商谈判予以确定,不拘泥于特定类型。例如,《中华人民共和国和肯尼亚共和国关于刑事司法协助的条约》(*Treaty on Judicial Assistance in Criminal Matters between the People's Republic of China and the Republic of Kenya*)第 19 条允许我国与肯尼亚相互请求提供与犯罪行为有关的银行信息。尽管依据数据分类分级,金融数据出境的风险程度不低,但我国与肯尼亚通过国际谈判让渡了金融数据所蕴含的数据威斯特伐利亚主权与数据国内主权,相互强化对跨境金融数据流动的控制力,即数据相互依赖主权。

第二,面对数据控制者取证模式,我国刑事证据出境审查工作机制须与国际条约对接,明确数据出境遵守必要性与目的限制原则,且以设置安全保护措施为前提。首先,《联合国打击网络犯罪公约》已对"用户信息"采用数据控制者取证模式达成共识,因而有必要针对用户信息单独简化《规定》第 14 条设计的审核因素。例如,"相关主管部门的意见"这一审核要素带有强烈的行政许可色彩,构成了用户信息出境的前置性条件,与国际条约对接后可以省略。其次,司法部工作机制办公室须结合数据分类分级,尽快细化各行业重要数据与核心数据的具体目录。〔43〕 若被调取的数据属于重要数据或核心数据,则应直接拒绝数据出境申请。倘若不在具体目录范畴,司法部须强化对数据出境的必要性审核,来确保数据出境的最小化;同时要求其严格遵守目的限制原则,数据出境后只限用于刑事诉讼。〔44〕 最后,对用户信息以外的其他类型数据,出境的安全保障措施应当以请求国执法机关或司法机关设置的安全保障措施为前提。在 Anywhere Commerce, Inc. v. In-

〔43〕 参见梁坤:《网络犯罪国际公约中的跨境调取数据条款》,《当代法学》2024 年第 2 期,第 132 页。

〔44〕 参见郑曦:《刑事数据出境规则研究》,《法律科学》2022 年第 2 期,第 142-143 页。

genico, Inc. 案中,美国马萨诸塞州地区法院批准对法国公司提供的文件实施保护令,将其标记为“仅限高度机密的律师查看”,并在诉讼结束后归还或销毁文件。[45]

(二)阻断法的优化

阻断法表明了我国对数据控制者取证模式的立场,是敦促他国与我国开展国际谈判的筹码,考虑到其实施效果还不够理想,需要进一步的优化。

1. 强化阻断法的执行

比较我国法律文件中各阻断条款的内容,可以发现我国阻断法架构设计相似,均是以“主管机关批准”作为数据出境的前提。《数据安全法》第 36 条与《个人信息保护法》第 41 条在民事诉讼与刑事案件中均可适用。美国法院面对我国网络服务提供者以阻断法为由的抗辩,判决思路一致,均是以可执行性衡量中美国家利益的轻重。因此,面对数据跨境取证,阻断法的立法架设并不需要区分诉讼性质的差异,而是应强化条款的可执行程度。

阻断法的执行性会直接影响他国司法机关的评价。美国联邦法院在面临数据控制者取证模式与阻断法冲突时,63%的概率会明确考虑阻断法的执行历史,而在国际礼让分析中,国家实际执行阻断法的程度是判断国家利益强度的有力指标。[46] 在前文“中资银行案”与 Concepts Nrec, LLC v. Xuwen Qiu 案中,美国法院均以我国阻断条款不具备执行先例驳回抗辩。而在 Motorola Credit Corp. v. Uzan 案中,美国纽约南区地区法院基于瑞士宝盛银行的前雇员因协助德国税务机关被判处三年监禁的执法案例,将银行保密视为瑞士积极的社会利益,驳回了涉及瑞士文件的传票。[47] 是故,我国须强化阻断法的执行强度以优化防御策略。

2. 完善阻断法实施的配套措施

仅仅依靠阻断法并不能达到防御效果,一味加强执行亦可能导致网络服务提供者陷入两难,所以阻断法的执行须完善配套措施。首先,当我国企业被国外机构要求提供相关数据时,应先判断是否属于豁免情形。倘若不属于豁免情形,且我国司法部评估发现数据出境给国家安全、公共利益带来的风险较大,则应遵守阻断法。其次,明确企业遵守阻断法可获取的支持。鉴于网络服务提供者可能因遵守我国阻断法受到外国法院的处罚,其可根据我国《阻断外国法律与措施不当域外适用办法》第 11 条规定获取支持,但该条并未详细解释支持的内容。因此须细化网络服务提供者可获得的支持范围,以缓解其面临的压力。最后,对等反制与阻断法相互配合促使实施数据控制者取证模式的国家与我国谈判,更有效地防御单边跨境取证对我国的侵害。基于国际法对等原则,我国《个人信息保护法》第 43 条与《数据安全法》第 26 条分别规定我国针对其他国家在个人数据保护或数据开发利用技术领域采取的歧视性的禁止、限制或者其他类似措施可采取“对等反制措施”。虽然此类措施并不专门针对数据跨境取证,但我国可以明确将“对等反制”引入

〔45〕 Anywhere Commerce, Inc. v. Ingenico, Inc., 19-cv-11457-IT (D. Mass. June 3, 2021).

〔46〕 M. J. Hoda, The Aérospatiale Dilemma: Why U. S. Courts Ignore Blocking Statutes and What Foreign States Can Do about It, 106 *California Law Review* 231, 246 (2018).

〔47〕 Motorola Credit Corp. v. Uzan, 73 F. Supp. 3d 397 (S. D. N. Y. 2014).

数据跨境取证领域。针对不在我国阻断法豁免范围内且违反我国司法案件数据出境安全评估流程的单边取证行为,我国可设置“黑名单”。如面对外国单边在侦查案件中对存储于我国的数据远程取证,我国保留使用同种侦查措施远程调取数据的权利。〔48〕

六 结 语

美国单边实施数据跨境取证的案件频繁出现,司法审判暴露了数据控制者取证模式引发的数据主权冲突与合规困境。我国颁布的一系列阻断条款在涉外案件中难以得到美国司法机关的承认与适用。面对外国执法机关或司法机关的单边数据跨境取证行为,我国企业被迫承担双重合规的负担。现有各国对数据主权的认知差异以及数据跨境流通的不同策略导致数据控制者模式引发的问题难以得到有效解决。数据主权理论急需得到进一步深化以调和数据跨境取证的现实矛盾。“数据例外主义”作为支持数据控制者取证模式的主流理论,有意忽视数据主权在网络空间物理层、逻辑层与内容层的属地性,一味强调数据介质的特殊性。证实数据主权在网络空间各个层次的属地性是驳斥这一理论并在数据跨境取证领域打破西方话语垄断的重要一步。但也需认识到,数据主权的属地性在网络空间存在梯度差异,数据主权的四项维度在网络空间不同层次的运行也存在区别。在尊重主权属地性的同时,数据主权可进行多维度划分与组合,实现场景化适用,从而调和数据跨境取证的冲突。物理层发生的数据跨境取证必须经国际司法协助程序开展,而网络空间内容层上数据主权可配合程序主义与数据分类分级,在自主让渡数据威斯特伐利亚主权与数据国内主权的同时,强化数据相互依赖主权。

面对数据控制者取证模式的压力,完善“攻防兼备”的中国方案是当务之急。就进取方案而言,应结合民事诉讼与刑事诉讼的差异,设立民事案件数据出境安全评估通道,保持立法态度的内外一致;调整刑事案件数据出境安全评估机制,区分依据刑事司法协助提出的申请与依据数据控制者取证模式提出的请求。就防御方案而言,我国须有效运用阻断法这一工具,配合豁免情形的规定以强化阻断法的执行性。进一步明晰我国企业遵守阻断法可以获得的支持范畴,并可以考虑将对等反制引入数据跨境取证。总之,面对数据跨境取证冲突,我国不仅须积极参与全球数据跨境取证规则的制定,更应有针对性地优化数据防御战略,探索兼具安全性与开放性的中国路径。

[本文为作者主持的2024年度内蒙古自治区社会科学规划项目“中蒙俄数字经济合作的法律挑战与应对研究”(2024NDC168)的研究成果。]

〔48〕 参见梁坤著:《数据主权与安全:跨境电子取证》,清华大学出版社2023年版,第209页。

The Data Controller Forensic Model: Practice Contradictions, Theoretical Reflections and Coping

[**Abstract**] In the era of big data, state authorities increasingly rely on the data controller forensic model to achieve rapid data acquisition. Data sovereignty demonstrates varying degrees of territoriality at the physical, logical, and content layers of cyberspace, and the theory of "data exceptionalism" is insufficient to overturn the rules of extraterritorial enforcement jurisdiction. The unilateral enforcement of the data controller forensic model continues to infringe upon the data sovereignty of countries in which data is stored. Furthermore, blocking statutes in most scenarios fail to receive judicial recognition in both civil and criminal cases. This places internet service providers in a compliance dilemma when confronted with the data controller forensic model. Under the layered architecture of cyberspace, data sovereignty can be achieved through multidimensional division and functional combination to enable scenario-based applicability. The conceptual framework of data sovereignty can be delineated into Westphalian data sovereignty, domestic data sovereignty, interdependent data sovereignty, and international legal data sovereignty. Given the pronounced territoriality of physical layer of cyberspace, application of data sovereignty does not differ from traditional sovereignty, and cross-border digital evidence acquisition must comply with mutual legal assistance procedures. However, within the content layer of cyberspace, in conjunction with proceduralism and data classification hierarchies, states may voluntarily cede aspects of Westphalian and domestic data sovereignty to strengthen interdependent data sovereignty. China's purely defensive posture toward the data controller forensic model has proven ineffective, necessitating urgent development of a comprehensive Chinese approach that incorporates both defensive and proactive elements. On the one hand, given fundamental distinctions between civil and criminal proceedings, security assessments for outbound data transfer should be calibrated accordingly. China must establish a dedicated security assessment protocol for outbound data transfer of civil cases, with potential exemptions for internet service providers under defined conditions. In criminal matters, China could simplify review criteria for security assessments based on formal criminal judicial assistance requests. Regarding applications predicated on the data controller forensic model, Chinese legislation must align itself with international treaties while adhering to principles of necessity and purpose limitation, contingent upon requesting nations implementing adequate security measures. On the other hand, to mitigate pressures faced by internet service providers, Chinese legislation must articulate more explicitly the support mechanisms available to them, and supplement such mechanisms with exemptions and countermeasures to promote the implementation of blocking statutes.

(责任编辑:贾 元)