数字时代跨境电子取证的现实困境与治理对策

候柔倩[1],刘梓涵[2]

1. 中南大学 法学院,湖南 长沙 410083;
2. 郑州大学 法学院,河南 郑州 450001

摘要:数字时代跨境电子取证在技术、法律和实践层面迅猛发展,并逐步演化为国际法治领域的核心议题。然而,碎片化的国际法框架、技术变革带来的颠覆性影响,以及隐私权与数据主权之间的冲突,致使当前国际刑事司法协助面临多重现实障碍。欧盟以《通用数据保护条例》为基础构建规则体系,并推出欧洲调查令等机制,但面临主权让渡难题与技术发展瓶颈;美国凭借《澄清域外合法使用数据法案》确立"数据控制者标准",在实现高效取证的同时,加剧了治理机制的碎片化。鉴于此,我国应坚持数据主权原则,积极探索制度协调的有效路径,推动技术赋能与规则创新的协同发展。同时,平衡好数据本地化与全球治理之间的关系,时刻保持对规则霸权的警觉,为推进全球数字治理贡献独有的中国智慧。

关键词:电子数据;跨境取证;数据主权;长臂管辖
中图分类号:D997 **文献标识码**:A DOI:10.12186/2026.04.009
文章编号:2096-9864(2026)04-0076-10

数字技术的迅猛发展正深刻重构全球刑事司法协助体系的底层逻辑,跨境电子取证已从技术性议题演变为牵动数字时代国际法治秩序的核心命题。区块链存证与云计算技术逐步瓦解了传统取证的物质载体依赖,欧盟委员会的一项报告显示,约85%的刑事调查需依赖电子证据,其中2/3直接涉及境外服务器数据调取,这既凸显了技术革命对犯罪治理范式的颠覆性影响,更暴露出现行国际规则体系的系统性滞后[1]。面对技术犯罪痕迹的全球化分布与数据主权壁垒的持续性增强,欧美国家率先展开制度突围。美国通过《澄清域外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act,以下简称《云法案》)构建"数据控制者标准",依托科技巨头的全球布局实施"长臂管辖";欧盟则以《通用数据保护条例》(General Data Protection Regulation,缩写为GDPR)为基石推行欧洲调查令制度,在强化数据主体权利的同时构建成员国间的快速流转机制。在"美国诉微软案"中,当第二巡回上诉法院既承认司法协助体系的低效又否定单边行动的正当性时,传统国际法上的属地管辖原则与数据空间的去领土化特性已形成难以弥合的价值悖论。当前,学界关于跨境电子取证的研究多集中在对传统刑事司法协助机制的重塑[2]、发展与反思[3]等方面,较少关注数字时代背景下跨境电子取证的

收稿日期:2025-12-02
基金项目:中南大学研究生自主探索创新项目(1053320240520)
作者简介:候柔倩(1996—),女,山西省晋城市人,中南大学博士研究生,主要研究方向:数字法学、国际法学;刘梓涵(2001—),女,河南省周口市人,郑州大学硕士研究生,主要研究方向:中国刑法理论与实践。

困境与出路。鉴于此,本文拟通过分析数字时代跨境电子取证的现实困境,解构欧美经验的内在逻辑与外部效应,提出既契合网络空间命运共同体理念又能纾解主权博弈与技术异化风险的规范路径,为全球数字治理贡献兼具理论创新性与实践可行性的治理对策。

一、数字时代跨境电子取证的现实困境

当前,大数据、人工智能、区块链和云计算等前沿数字技术的长足发展,为跨境电子取证的实现构筑了坚实的技术根基。但不可否认的是,数字化浪潮对全球司法领域的冲击和影响也日益加深,为数字时代下跨境电子取证工作的开展带来较大的现实障碍。鉴于此,国际社会敏锐地察觉到完善相关法律框架的紧迫性和必要性,逐步构建起适应数字化时代跨境电子取证需求的法律规范体系。纵观之,跨境电子取证制度的发展和完善分为三个阶段:一是基于国际礼让原则为外国执法请求提供必要帮助(19 世纪末到 20 世纪 50 年代);二是以国际刑事司法协助为主导的探索期(20 世纪 60 年代到 20 世纪末);三是跨境电子数据取证的体系化建构期(21 世纪初至今)[4]。作为当前国际社会打击跨国网络犯罪的核心环节,跨境电子取证面临着传统取证制度与技术发展的错位、主权管辖的冲突和数据权属的复杂性等难题。这些问题不仅严重制约了犯罪打击效率,更引发了国际司法协助与数据主权保障之间的深层矛盾。

1. 治理规则碎片化与跨境数据管辖权冲突

传统国际刑事司法协助机制以《关于从国外调取民事或商事证据的公约》(以下简称《海牙取证公约》)与《布达佩斯网络犯罪公约》(以下简称《布达佩斯公约》)为基础,着重强调属地管辖原则,要求通过司法协助请求书等程序来完成跨境数据的调取工作。例如,《布达佩斯公约》第三十二条虽允许缔约国在数据主体同意下实施远程取证,但其程序限制导致平均耗时超过 180 天,难以适应电子证据易篡改、易灭失的特性[5]。2013 年“微软爱尔兰案”的管辖权争议即暴露了这一矛盾,美国司法部依据《存储通信法》要求微软提供存储于爱尔兰都柏林服务器的用户邮件数据,而爱尔兰政府依据《布达佩斯公约》第二十七条主张需通过双边司法协助程序解决。该案的争议焦点在于美国执法机构能否依据法院搜查令获取美国网络服务提供商存储于境外的数据,进而引发公众关于数据存储地模式与数据访问地模式的论战[6]。该案历时 5 年最终由美国最高法院裁定需通过立法调整,直接催生了 2018 年《云法案》的出台。然而,《云法案》第一百零三条所确立的“数据控制者标准”,即只要企业受美国管辖,无论数据存储地为何处均需配合调取,又引发了主权冲突的进一步升级。欧盟通过 GDPR 第四十八条明确要求成员国不得承认非欧盟国家违反欧盟法律的单边数据调取令,形成与《云法案》的直接对抗[7]。这种法律框架的割裂在跨境金融犯罪取证中尤为突出。根据 Chainalysis 公司的报告数据,2021 年网络罪犯通过加密货币洗钱金额达到 86 亿美元,较 2020 年增加 30%,其中约有 17%的犯罪金额来自去中心化金融应用[8]。虚拟货币交易的去中心化特性使得犯罪行为可能涉及多个司法管辖区,各国对“主要犯罪地”的认定存在分歧,不同国家的法律体系差异、取证程序复杂导致管辖权争议频发。这无疑揭示出底层的制度困境在于:现有公约体系未能预见到云计算与分布式存储技术的普及,导致其无法解决数据物理存储地与案件实质关联性脱节的问题。在跨境电子取证的复杂情境下,各国基于法律体系与司法理念,依据多元的管辖标准主张对跨境数据行使管辖权,致使管辖权冲突在实践中屡屡出现。

2. 技术特征对跨境电子取证的颠覆性影响

电子数据所具有的跨境流动性与分布式存储特性,使得传统取证方式中基于地理位置构建的明确界限趋于模糊。在跨境流动中,数据能够在极短时间内穿越不同国家或地区的网络体系,不受物理边界限制;分布式存储则意味着数据并非集中存储于单一地点,而是分散存储于多个节点。在这种情况下,传统取证手段难以对数据进行精确的定位与有效的获取,加之云服务提供商所制定的隐私政策与数据访问规则存在显著差异,给跨境电子取证工作带来严峻挑战,极大地增加了获取相关电子证据的复杂性与不确定性。另外,为维护数据安全并保障数据主体隐私,数据加密及其匿名化技术被广泛应用。加密技术使得在未获取解密密钥的情况下,数据无法被读取与分析。而获取解密密钥既要涉及复杂的技术问题,还需严格遵循相关法律程序,通常需要投入大量的时间与资源。匿名化技术在隐匿个人身份信息、保护数据主体隐私的同时,可能导致难以准确判定数据关联性,进而削弱证据的证明效力,使取证人员在判断数据与案件的具体关联时面临较大困难。此外,在大数据背景下,电子证据的真实性与完整性验证成为一项关键且具有挑战性的任务。电子证据因其易被篡改、伪造和删除的特性,传统的验证方法在面对海量数据时难以有效发挥作用。尽管区块链等新兴技术为解决这一问题提供了新的思路与途径,但当前其应用仍受限于技术标准不统一、监管机制不完善等问题,无法构建起可靠且具有普适性的跨境电子取证解决方案,这在一定程度上影响了跨境电子取证结果的可信度及其在司法实践中的应用效果。

以电子邮件为例,一封从中国发送至美国的邮件可能经由新加坡、德国等第三国服务器中转,导致数据存储地与案件实质关联性完全脱节。更复杂的情形出现在云计算场景中,单个用户数据可能被碎片化存储于多个国家或地区的服务器。诸如,亚马逊云科技等相关云服务提供商,其标准服务协议默认将数据副本存储于至少三个不同司法管辖区的数据中心,这意味着调取单一数据集可能需向多国提交司法协助请求。跨境电子数据取证涉及多个司法辖区,需要通过国际刑事司法协助或警务合作方式完成。这一过程通常需经过多个步骤,包括请求协助、审核、处理和数据传输等,整个程序较为复杂、耗时长,需明确证据所在国。但在互联网时代,像“暗网”中的数据可能无法确定其物理存储位置、云计算技术的应用也令数据的具体位置难以确定,这些都使得基于国际法的传统国与国之间的司法协助方式难以适应时代需求[9]。技术逻辑与法律逻辑的错位,呈现出复杂的非线性关系:一方面,电子证据的即时性特征,迫切需要突破传统司法协助程序的低效瓶颈;另一方面,单边取证措施面临着严峻的主权合法性危机,此种矛盾在跨境网络犯罪与反恐领域表现得尤为显著。

3. 隐私权保护与数据主权主张的规范张力

欧盟通过 GDPR 构建的充分性保护标准,要求数据出境必须满足目的限定、最小必要等原则,而刑事取证往往涉及强制披露与宽泛的数据范围。在 2019 年美国法院审理的“Philips Medical Systems (Cleveland), Inc., et al v. Jose Buan, et al (No. 19 CV 2648/Jose Buan)案”中,法官要求中国被告提供存储在云服务器上的患者诊疗数据,被告援引《中华人民共和国保守国家秘密法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》提起抗辩,主张未经中国网信办安全评估不得向境外提供个人信息。尽管法院最终以诉讼必要性为由驳回抗辩,但该案揭示出隐私合规要求可能成为跨境取证的实质性障碍。各国数据本地化的相关立法,进一步激化了这一矛盾。例如,俄罗斯

第 242-FZ 号联邦法《就“进一步明确互联网个人数据处理规范”对俄罗斯联邦系列法律的修正案》要求,所有数据处理人在俄罗斯境内的服务器上存储和处理俄罗斯公民的个人信息,都必须将该数据存储于俄罗斯联邦境内的服务器或数据中心[10]。在这一背景下,跨国公司被迫实施数据主权嵌套策略,即在不同司法管辖区重复建设数据中心以满足本地化要求,以致企业的合规成本显著增加,严重制约了跨境协作的效率。更深层的冲突在于,这背后所蕴含的技术霸权与规则割裂。美国通过《云法案》与欧盟依据 GDPR 第四十八条形成“跨大西洋数据治理联盟”,却将中国、俄罗斯等国家列为“非合格外国政府”,导致后者在跨境取证中被迫依赖效率低下的传统司法协助渠道。这种规范对抗的根源在于电子数据的双重属性,即作为生产要素需要自由流动,作为主权载体又需受领土控制。

现行国际法试图通过“安全例外条款”调和矛盾,但国家安全概念的泛化使例外常态化。例如,美国出于对所谓“国家安全”的考量,强制要求 TikTok 将数据本地化存储,声称这是保障其本国信息安全的必要措施。然而,美国却通过《云法案》肆意获取他国数据,凭借该法案赋予的权力,美国执法机构能够要求美国境内的科技公司交出存储在国外的数据,从而实现单方面的数据主权扩张,这种双重标准严重破坏了跨境数据治理的公平性与合理性。破解这一困局尚需构建分层分类的取证机制,可考虑对普通商业数据适用简化的直接调取程序,对健康、生物识别等敏感数据维持严格的司法审查程序。国际社会在《联合国打击网络犯罪公约(草案)》中已开始探索分级制度,但其具体实施仍面临各国立法差异与技术标准互认的现实挑战。

二、数字时代跨境电子取证的欧美经验

跨境电子取证作为数字时代全球治理中兼具技术复杂性与法律敏感性的前沿议题,传统国际法框架下的属地管辖原则与司法协助机制因数据无界性、存储分散化和主权诉求冲突等现实难题而陷入系统性失效。以欧盟 GDPR 与美国《云法案》为代表的制度创新,分别通过数据主权博弈防御性立法与司法管辖权扩张性重构,试图破解跨境数据调取效率低下与权利保障不足的双重困境,但其单边化路径亦引发管辖权竞合冲突、企业合规悖论和国际规则碎片化等衍生风险。通过聚焦欧美跨境电子取证的制度演进与范式竞争,解构 2018 年“微软诉美国案”、2020 年欧盟法院“隐私盾协议”无效裁决等典型案例,厘清数据主权与司法协助的动态平衡逻辑,以期为我国构建兼具效率与正当性的治理框架提供镜鉴。

1. 欧盟模式

欧盟在跨境电子取证领域的法律框架经历了从碎片化到统一化的系统性变革。以 GDPR 为核心,欧盟逐步构建起平衡隐私权与执法效率的规则体系。在新的历史时期,欧盟积极寻求制度变革,推出了由不同成员国执法机关承认和执行的欧洲调查令,并推动构建面向网络服务提供者的欧洲提交保存令[11]。2018 年 4 月,欧盟委员会推出的《关于制定欧洲刑事电子证据提交令与保存令条例的提案》和《关于制定要求委任法律代表的统一规则之指令的提案》,授权成员国执法机关发布电子证据提交令、保存令,直接要求境内外网络服务提供者提交、保全电子证据,为跨境电子取证提供了明确的法律依据和操作指引[12]。2023 年 1 月,欧盟理事会发布公告称,欧盟理事会和欧洲议会就跨境获取电子证据的相关法规和指令草案达成协议。根据新规,欧盟当局可直接向其他成员国相关数据提供方发送获取电子证据的司法指令,无论数据实际存储于何处,这一机制突破了传统数据主权的地理限制。例如,相关司法指令可涵盖各种类别的数据,并设定指令接受方

需在 10 天内进行回应;在正式确定的紧急情况下,期限可缩短至 8 小时;如果相关数据提供方不遵守指令,则可面临最高达其上一财年全球营业额 2%的罚款[13]。这一设计通过经济威慑强化了规则刚性,体现了欧盟对大型科技公司合规压力的精准把控。2023 年 7 月出台的《欧盟电子证据条例》构建起欧洲出示令与欧洲保全令机制,赋予各成员国执法与司法机构直接从其他成员国的数据控制者处获取数据的权力[14]。在跨境协作机制方面,欧盟从依赖"明示互认"转向"默示互认",前者要求接收国对请求进行实质性审查,后者则仅在服务提供商拒绝配合时触发司法介入,显著降低了程序成本。不过,与非欧盟国家的合作仍受限于法律冲突。例如,"Schrems Ⅱ案"认定美国国家安全局的数据监控不符合欧盟隐私标准,导致跨大西洋数据传输机制被迫重构,凸显了法律兼容性对跨境取证的关键影响。

技术挑战进一步加剧了欧盟跨境取证的复杂性。一方面,2018 年欧洲议会通过了《非个人数据自由流动条例》,旨在消除欧盟内的数据本地化措施,促进非个人数据的自由流动,但允许以公共安全或国家安全为由保留例外条款[15]。这种原则性禁止和例外性保留的模式虽促进数据流动,却导致执法机构难以锁定数据位置。另一方面,端到端加密技术的普及削弱了执法机构的数据访问能力。对此,"五眼联盟"拉拢印度和日本发表联合声明,要求 Signal、Telegram 等使用"端到端加密"技术的高科技公司在自身应用程序中"开后门",以便为其网络执法行动提供便利,企图将监管范围延伸至网络空间的每一个角落[16]。此举遭到了科技公司以侵犯用户隐私为由的强烈抵制。例如,Signal 首席执行官 Meredith Whittaker 威胁说,如果欧盟"在线安全法案"不允许加密,将从英国撤回其应用程序[17]。隐私权与执法效能的博弈,贯穿着欧盟跨境电子取证规则设计的始终。GDPR 第四十八条明确规定,"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、裁决或决定不会对本章规定的其他转移形式产生消极影响",严禁未经欧盟法授权的转移或披露。然而,高标准保护在实践中可能导致效率低下。如何在高标准保护体系与执法效率提升之间找到平衡点,是欧盟在数字时代治理中试图调和"权利本位"价值观与现实执法需求的关键课题。

2. 美国模式

在国际刑事司法协助的实践中,美国正加速从传统的司法互助协定(Mutual Legal Assistance Treaty,缩写为 MLAT)向双边协议转型。MLAT 的处理周期普遍较长,难以满足数字时代的执法需求,而《云法案》框架下的双边协议允许执法部门直接调取对方境内数据,双方互免事前审查。以 2022 年正式生效的英美两国之间的《关于为打击严重犯罪而获取电子数据的协议》为例,该协议允许一个国家的服务提供商迅速响应另一个国家/地区发布的合格合法电子数据命令,而不必担心违反跨境披露的限制[18]。然而,这种"俱乐部式"合作进一步加剧了规则碎片化,未被纳入协议的国家需继续通过 MLAT 申请数据,导致全球取证体系呈现"中心-边缘"分化。此外,美国执法机构与科技企业的合作模式也独具特色。例如,美国联邦调查局依据 1994 年《通信协助执法法案》要求电信企业预留监控接口,而亚马逊云与美国司法部合作开发数据镜像技术,实现跨境云存储的实时访问。这类公私合作虽提升效率,却引发巴西、印度等国以主权侵犯为由的诉讼,暴露美国单边主义的治理风险。技术革新堪称是美国跨境取证能力的核心优势,美国国家标准

与技术研究院制定的SP800系列指南文件为电子数据取证提供标准化流程,极大地确保了司法取证的合法性、真实性和关联性[19]。然而,技术进步亦伴随争议。FBI与苹果公司在加密问题上的对抗持续升级,在2016年“圣贝纳迪诺枪击案”中,FBI强制要求苹果公司协助解锁涉案手机,苹果公司以不能为了国家安全而牺牲个人隐私为由,拒绝提供任何来自用户的加密信息,此案鲜明地凸显了司法权与科技公司自主权的冲突。

美国通过《云法案》重塑了跨境电子取证的法律范式,其核心突破在于确立“数据控制者标准”,要求服务提供商无论数据存储于何处均需响应美国执法机构的调取令,这一规则赋予美国事实上的“数据治外法权”。与欧盟不同,美国采取的是“内外双轨”策略,对外通过《云法案》扩展管辖权,授权与适格的外国政府签订双边协议,构建双向数据共享通道[20];对内则依托《电子通信隐私法》限制数据出境,如要求金融机构保留交易数据五年,并通过《爱国者法案》扩大联邦政府监控和调取电子数据的权力。《云法案》虽允许企业以违反外国法进行抗辩,但司法审查中重大利益权衡标准往往偏向美国政府。美国既能够继续对受美国法管辖的企业所掌握的数据保持绝对控制,也可以借机要求意欲直接调取数据的外国政府,必须遵守美国在人权和隐私保护方面的基线标准,并给予美国政府对等待遇[21]。这种进攻性法律工具和防御性数据管控机制的有机组合,有效巩固了美国在全球数据治理中的主导地位,但也引发了“数字殖民主义”质疑。

欧盟与美国分别以“权利本位”和“效率本位”为导向,形成风格迥异的跨境电子取证范式。欧盟通过GDPR构建统一规则,却在成员国主权让渡与技术瓶颈中步履维艰;美国凭借《云法案》与科技霸权实现高效取证,却因单边主义加剧全球规则碎片化。基于此,跨境电子取证需在主权、隐私与效率间寻求动态平衡,而技术标准的国际协调与多边治理框架的构建将是破局关键。对于我国而言,需在借鉴制度设计的同时警惕规则霸权,通过参与全球数据治理对话、推动技术标准互认、强化本土数据基础设施,探索符合自身利益的跨境电子取证路径。

三、数字时代我国跨境电子取证的治理对策

当下,跨境电子取证的核心锚点在于重塑数据主权、司法管辖权与技术治理之间的协同性。我国应将数据协同确立为关键驱动力,依托国内法治完善与国际规则构建的双轮驱动模式,精心擘画以技术助力高效取证、以规则维护主权安全、以协作推动全球治理的中国方案。同时,应逐步深化与“一带一路”共建国家的数据治理合作,积极推动区域性电子取证协作机制的建立,为跨境犯罪治理提供坚实有力的法治保障。

1. 我国跨境电子取证的法治立场:主权原则与制度协调的双重路径

数字时代,跨境电子取证的法治立场集中体现为主权原则的坚守与制度协调的探索之间的辩证统一。中国在此领域的法律实践,既植根于国际法基本准则,又回应了网络空间治理的特殊需求。

从国际法框架观之,数据主权可视为传统主权原则在数字空间的投射,维护数据主权安全则相应地构成中国法治立场的核心基石[22]。按照《联合国宪章》的主权平等原则,主权国家有权平等地参与网络空间国际治理,共同制定国际规则[23]。网络主权与数据主权具有高度的内在一致性,即国家独立自主地占有、处理和管辖本国范围内的数据并排除他国干预的最高权力。这一立场在2016年由最高人民法院、最高人民检察院、公安部印发的《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》中得到具体化,其第九条明确要求跨境取证需经法定程序,实质上确立了“数据主权不可侵犯”的规范原则[24]。但不可否认的是,传统主权理念现如今面临着技术解域化的挑战。电子数据的流动性特征使得物理疆界与数据控制权产生分离。对此,我国可考虑采取分层治理策略。在物理层面主张对基础设施的绝对控制权,在逻辑层面构建网络安全审查制度,在内容层面完善数据分类分级管理制度。这种分层治理既可维护国家网络安全,又可为跨境数据流动预留较大的制度空间。

尽管主权原则是跨境电子取证的重要基石,但在全球化背景下,单纯依靠主权原则难以有效解决跨境电子取证中的复杂问题,制度协调成为必然选择。制度协调路径则体现为国内法与国际规则的动态调适。一方面,我国应积极参与国际条约的制定与签署,在一些多边或区域国际条约中,与其他国家就跨境电子取证的规则、程序等进行协商与合作;另一方面,在国内法体系建设上,我国应不断完善与跨境电子取证相关的法律法规,以实现与国际通行做法的接轨。例如,我国在参与《联合国打击网络犯罪公约》的磋商谈判时,应时刻秉持主权优先、司法互助的法治立场。在具体落地上,2018 年《公安机关办理刑事案件电子数据取证规则》建立“双重审批”机制,表现为境内存储数据适用属地管辖,境外数据需通过司法协助途径获取。这种制度设计既避免了单边域外管辖的合法性争议,又符合《联合国打击网络犯罪公约》第五条关于保护主权的原则性倡议。但现有制度仍存在协调不足的问题。例如,2016 年《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》第九条允许紧急情况下的跨境远程取证,引发可能突破主权原则的质疑。为解决这一问题,可考虑引入比例原则加以审查,将取证手段的必要性与所调取数据的敏感性挂钩,实现主权保护与打击犯罪之间的平衡。

从比较法视角切入,我国立场与欧美立场存在结构性差异。美国《云法案》采用“数据控制者标准”,允许执法机构直接调取境外数据;欧盟则通过一系列条例建立起“出示令”制度。这些机制虽有效地提升了取证效率,但存在侵蚀他国主权的风险。我国所秉持的“司法互助优先”原则更具包容性,一方面通过《中华人民共和国国际刑事司法协助法》完善双边协作框架,另一方面在“数字丝绸之路”建设中探索区域性电子取证协议。这种制度嵌套的策略既维护了主权底线,又实现了治理效能提升,为构建网络空间命运共同体提供了法理支撑。

2. 我国跨境电子取证的制度构建:技术赋能与规则创新的协同推进

我国跨境电子取证制度的现代化转型,呈现技术驱动型规则创新与规则引导型技术应用的双向互动特征。这种协同推进模式在区块链存证、人工智能审查等领域表现得尤为显著。

技术基础设施的突破重构了取证规则体系。以区块链技术为例,其不可篡改、全程留痕的特性,有效解决了电子证据的鉴真难题。2018 年杭州互联网法院审理的“全国首例区块链存证案”,确立了由存证平台资质、技术手段可靠性、电子数据完整性所构成的三重审查标准。该案例有力地推动了同年《最高人民法院关于互联网法院审理案件若干问题的规定》的出台,其第十一条明文指出,“当事人提交的电子数据,通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证,能够证明其真实性的,互联网法院应当确认”。更深远的影响在于,区块链技术的“去中心化”特征倒逼传统取证规则变革。例如,北京互联网法院建立的“天平链”电子证据平台,成功解决了电子证据的诸多难题,构建了涵盖公证处、证书授权机构的联盟链体系,实现了取证、存证、示证和质证的全流程重构。这种技术赋能的制度创新,使我

国电子证据规则从“事后审查”转向“过程控制”,形成了领先国际的预防型证据治理模式。

随着跨境电子取证技术不断迭代,从传统的网络追踪到新兴的区块链存证等先进手段,相关规则必须在取证流程、证据效力认定、数据跨境传输规范等方面进行创新,以保障电子取证在合法合规框架内高效开展,实现技术赋能与规则适配的良性互动。在国内规则创新层面,可推动制定专门的跨境电子取证操作规程,详细规定执法机关在跨境电子取证中的权限范围,明确在何种情况下可启动跨境取证程序,避免权力的滥用与越界。在取证方式上,对远程获取数据、请求境外协助等不同方式进行分类指导,释明每种方式的适用条件与操作流程。证据保管环节也至关重要,应制定严格的保管制度,从存储介质的选择到数据备份策略,都要确保电子证据在保管期间不被篡改、不丢失。同时,应明确界定在跨境电子取证过程中对个人敏感信息的收集、存储、使用和传输的限制条件。在国际规则参与层面,我国应充分发挥自身在数字技术应用和司法实践中的优势,提出符合中国国情与国际共同利益的跨境电子取证规则建议。例如,倡导各国秉持尊重主权、平等互利的原则开展跨境电子取证合作,尊重主权要求各国在跨境取证过程中不得侵犯他国司法主权与国家利益,平等互利确保合作双方在合作中都能获得实际利益,实现共赢。通过签订双边司法协助条约或谅解备忘录,明确双方在跨境电子取证中的权利义务与合作程序,可为跨境电子取证工作奠定坚实的规则基础,有效减少跨境取证过程中的法律障碍与摩擦。

协同演进还体现在司法实践与标准制定的互动中。随着技术的持续迭代更新和跨境电子取证实践的深入发展,需及时对相关规则进行评估与调整。应设立专门的技术与规则评估小组,定期收集跨境电子取证中的技术应用情况与规则实施效果反馈信息,依据评估结果对规则进行修订完善,确保规则始终能够适配技术发展的实际需求。例如,最高人民法院 2022 年发布的《关于加强区块链司法应用的意见》,明确提出区块链技术在提升司法公信力、提高司法效率、增强司法协同能力、服务经济社会治理四个方面典型场景应用方向[25],将技术参数与证据效力相挂钩,形成技术标准法律化的独特路径。这种“软法硬着陆”的规制策略,在跨境电子取证的场景中更具适应性。鉴于此,建议未来可在《中华人民共和国国际刑事司法协助法》中增设关于“技术互操作性”的条款,推动形成跨境电子取证的通用技术标准。

3. 我国跨境电子取证的国际合作:数据本地化与全球治理的再平衡

我国实施数据本地化政策,能强化国家对关键数据的管控,防止数据被不当获取与利用,为国内企业与公民的数据权益筑牢屏障。然而,过度的数据本地化限制则可能给数据跨境流动造成阻碍。从全球治理视角看,构建统一、高效的跨境电子取证机制,对打击跨国犯罪、维护网络空间秩序至关重要。我国在国际合作中,采取防御性数据本地化与建设性全球治理相结合的平衡策略,既能够捍卫核心数据主权,又可积极参与规则塑造。

数据本地化政策是构筑安全防线的基石。《中华人民共和国网络安全法》第三十七条规定,“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”,这一规定在跨境电子取证场景中具有双重功能:其一,通过数据物理驻留确保司法管辖权的有效行使,避免出现数据在境外、案件在境内的管辖困境;其二,为司法协助提供谈判筹码,即以数据本地化为前提换取取证程序简化。另外,我国在 2020 年《全球数据安全倡议》中提出“各国如因打击犯罪等执法需要跨境调取数据,应通过司法协助渠道或其他相关多双边协议解决。国家间缔结

跨境调取数据双边协议,不得侵犯第三国司法主权和数据安全”[26],允许成员国在国家安全受威胁时暂停数据跨境,这为电子取证中的主权保留提供了国际法依据。但过度本地化可能引发数据割据效应的发生,对此我国探索出动态分级机制。2022 年《数据资源体系构建白皮书》提出“负面清单+审慎清单”制度,对低风险数据放宽流动限制。这种精准化的本地化策略,既避免了欧盟 GDPR 的刚性约束缺陷,又为跨境电子取证合作保留了制度弹性。

为达成数据本地化与全球治理的再平衡,我国可施行一系列协调策略。在国际合作框架下,中国应积极参与多边跨境电子取证规则的制定。通过与各国开展全面而深入的磋商,明确数据跨境流动的条件、规范程序和严格的保护标准,在满足数据本地化要求的基础上,为跨境电子取证开辟合法、便捷且高效的路径[27]。例如,在区域性国际组织中,我国可发挥影响力,推动建立数据共享协议。该协议规定,在跨国网络诈骗、恐怖主义融资等特定类型犯罪案件中,成员国在遵循严格的隐私保护原则的前提下,能够迅速且精准地提供相关电子证据,显著提升跨境电子取证的时效性与准确性。我国亦可大力强化与其他国家的数据保护合作,通过积极签署双边或多边数据保护协定,梳理并协调各国数据本地化政策差异[28]。协定对数据存储、使用、传输等环节进行详细规范,消除因政策理解不同引发的误解与冲突,在此过程中,逐步构建稳固的互信机制。基于此互信机制,各国能够在跨境电子取证中更放心地共享数据,大幅减少因政策冲突导致的合作阻碍,促进跨境电子取证合作的顺利开展。

四、结语

当前,跨境电子取证深陷数据主权与司法管辖的结构性张力之中,其困境源于法律竞合、技术失范和协作低效的三重桎梏。以美国《云法案》为代表的“数据控制者标准”与欧盟 GDPR 所倡导的“数据存储地标准”形成冲突,促使全球其他国家为对标其标准而修改国内立法。在国际协作机制中,欧盟《布达佩斯公约》框架下跨境电子取证请求响应缓慢、耗时较长,暴露出传统程序与网络犯罪时效性需求的根本性矛盾。美欧实践暴露了治理逻辑的深层分歧,美国通过《云法案》构建公私协作和双边协议的制度体系,使微软、谷歌等科技公司承接大量的跨境取证请求;欧盟则依托 GDPR 强化双重犯罪和司法审查的标准体系,屡遭效率瓶颈,再次印证了效率与主权让渡的不可调和性。基于此,中国路径需在技术赋能与制度创新中寻求突破。在立法层面,应完善《中华人民共和国国际刑事司法协助法》所确立的刑事司法协助响应机制,对涉国家安全数据执行强制本地化存储标准,普通案件探索“白名单”企业直接响应;在技术层面,可推广浙江检察机关区块链存证实践,依托“数字丝绸之路”建设分布式取证节点;在制度层面,需采取分层协作的策略,在反恐、洗钱领域与上合组织共建电子证据平台,在普通刑事案件中细化《中华人民共和国刑事诉讼法》第五章对于电子数据的权利救济程序。通过跨境电子取证相关立法的完善、国家级电子证据区块链平台的搭建,以及数字司法协作倡议的发起等路径,以期为保障数据主权,推进全球数字治理,破解现行跨境电子取证困境提供独具中国特色的治理方案。

参考文献:

[1] Christakis T, Terpan F. EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options [J]. International Data Privacy Law, 2021, 11 (2): 85.

[2] 梁坤. 跨境远程电子取证制度之重塑[J]. 环球法律评论, 2019, 41(2): 132-146.

[3] 冯俊伟. 跨境电子取证制度的发展与反思[J].

法学杂志,2019,40(6):25-36.
[4] 冯俊伟.数字时代跨境刑事取证制度的转型[J].地方立法研究,2022,7(4):18-31.
[5] Mishra B, Mishra S. Adaptiveness of traditional judicial systems to digital forms of evidence[J]. International Journal of Engineering and Advanced Technology,2020,10(2):268-275.
[6] 吴玄.云计算下数据跨境执法:美国云法与中国方案[J].地方立法研究,2022,7(3):96-110.
[7] Shurson J. Data protection and law enforcement access to digital evidence:resolving the reciprocal conflicts between EU and US law[J]. International Journal of Law and Information Technology,2020,28(2):167-184.
[8] Crypto money laundering rises 30%,report finds[EB/OL].(2022-01-27)[2025-12-01]. https://www.bbc.com/news/technology-60072195.
[9] 陈冉.加强跨境电子数据协作与分层取证[N].检察日报,2024-09-07(3).
[10] 孙祁,哈里托诺娃.数据主权背景下俄罗斯数据跨境流动的立法特点及趋势[J].俄罗斯研究,2022(2):89-107.
[11] 刘品新.跨境电子取证的欧盟方案及启示[J].国家检察官学院学报,2022,30(5):3-23.
[12] 魏光禧,刘想树.跨境数据取证中公私合作的具体路径[J].中国人民公安大学学报(社会科学版),2024,40(1):63-74.
[13] 欧盟通过跨境获取电子证据法规和指令草案[EB/OL].(2023-01-25)[2025-12-01]. https://content-static.cctvnews.cctv.com/snow-book/index.html? item_id=4696990511894894785&track_id=5A462C11-B615-4408-9D73-7F824C89F8D0_696339438620.
[14] 陈爱飞."数据控制者标准"取证模式及中国因应[J].法商研究,2024,41(3):60-74.
[15] 谭观福.数字贸易中跨境数据流动的国际法规制[J].比较法研究,2022(3):169-185.
[16] 季澄."五眼联盟"拉拢日印,升级网络监控举措不得人心[EB/OL].(2020-10-20)[2025-12-01]. https://j.eastday.com/p/1603158505021591.
[17] CLABURN T. EU attempt to sneak through new encryption-eroding law slammed by signal,politicians[EB/OL].(2024-06-18)[2024-12-01]. https://www.theregister.com/2024/06/18/signal_eu_upload_moderation/.
[18] Landmark U S-UK data access agreement enters into force,by U S department of justice[EB/OL].(2022-10-03)[2025-12-01]. https://www.justice.gov/archives/opa/pr/landmark-us-uk-data-access-agreement-enters-force.
[19] 张涛.美国受控非密信息制度及其启示[J].情报理论与实践,2023,46(1):197-204.
[20] 赵海乐.论美国跨境电子取证与我国数据安全立法的冲突与对策[J].安徽大学学报(哲学社会科学版),2024,48(1):100-108.
[21] 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[J].环球法律评论,2021,43(1):38-51.
[22] 万广军,马小蕊.我国数据跨境流动法律规制的问题检视与完善路径[J].郑州轻工业大学学报(社会科学版),2025,26(1):59-68.
[23] 网络主权:理论与实践(2.0版)[EB/OL].(2020-11-25)[2025-12-01]. https://www.cac.gov.cn/2020-11/25/c_1607869924931855.htm.
[24] 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[N].检察日报,2016-09-21(3).
[25] 最高人民法院.关于加强区块链司法应用的意见[EB/OL].(2022-05-25)[2025-12-01]. https://www.court.gov.cn/zixun/xiangqing/360281.html.
[26] 全球数据安全倡议[N].人民日报,2020-09-09(16).
[27] 陈丽.跨境电子取证的中国应对[J].国家检察官学院学报,2022,30(5):24-40.
[28] 元轶,纪钊洋.大数据时代跨境电子取证的治理困境与应对[J].中国政法大学学报,2024(4):180-191.

[责任编辑:毛丽娜 吴永辉]

引用格式:候柔倩,刘梓涵.数字时代跨境电子取证的现实困境与治理对策[J].郑州轻工业大学学报(社会科学版),2026,27(4):76-85.