财经法学 No. 2，2025
pp. 174 - 189

云取证的学理反思与制度调适

张正昌*

内容提要：云计算环境具有虚拟化、实时性、多租户、弹性伸缩、去中心分布等特征。较之常规电子数据，居于其中的云数据表现出分割离散性、动态变化性、第三方控制性等新特点，要求云取证符合更严苛的实时化、更复杂的自动化、更强效的协同化要求。既有取证措施规范仍建立在传统环境取证经验之上，秉持以扣押原始存储介质为主、提取电子数据为辅、打印拍照为例外的取证原则，折射出以物证而非数据为本位的规制进路，并试图通过增补先行冻结措施单兵突进解决云取证问题，加之原有远程勘验与在线提取数据在规范逻辑上的失洽，以及对 DFIR、蜜罐取证等新现象规制不足，导致实践困境难以化解。既有取证管辖规范偏向纯粹的数据存储地模式，其程序繁琐性难以适应云取证过程中数据实时变动所要求的高时效性。为此可根据云取证现实要求，以数据为本位，确立扣押原始存储介质与提取电子数据并重，打印拍照为例外的取证原则，构建体系化技术规制与程序制约方案，以维护国家利益为基点完善取证管辖机制，增强云取证灵活性。

关键词：云计算　云取证　自动化取证　电子数据取证　执法管辖

一、引　言

云计算是一种可提供无处不在、快捷方便、按需使用的网络连接以访问可配置的计算资源（如网络、服务器、存储、应用和服务）共享池的模式。这一资源共享池可被快速调配和释放，且只需最少化管理或服务提供商交互。〔1〕伴随犯罪形势与犯罪结构网络化，云计算环境成为世界范围内违法犯罪活动多发空间。跨境电信网络诈骗、跨境网络赌博等复杂案件均大量涉及云端环

* 张正昌，中国政法大学证据科学研究院博士研究生。

〔1〕 这是美国国家标准与技术研究院（NIST）对云计算作出的定义。See Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, p. 2, available at https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, last visited on Feb. 5, 2025.

境下的取证。云计算环境提供了极强的数据便利性，使算力得到充分发挥，但也使传统电子数据取证方式难以直接适用，对电子数据取证方式有效性与合法性构成挑战。〔2〕

域外学者较早提出云取证（cloud forensics）概念，并得到广泛呼应。〔3〕一般认为，云取证是数字取证（digital forensics）的一项重要分支，是指对云计算环境中的电子数据进行取证。与大数据侦查不同，云端是承载数据的环境，云取证还存在小数据情况，故两者并不等同。云取证针对客户端、网络端和服务器端，需要运用不同技术，搭建起系统性的取证架构，〔4〕特别是进行网络端实时取证时，传统的扣押封存措施难以适用。主流观点指出云取证包含技术、组织和法律三个层面的内容。〔5〕因此“必须看到云计算模式和传统模式的差别”〔6〕，认识到云取证不仅是一项技术问题，也是一项法律问题。〔7〕

与传统网络环境相比，云计算环境具有鲜明差异，对取证活动提出更高要求。云计算环境具有分布式、虚拟化、实时性、多租户、弹性伸缩等典型特征，〔8〕通过可能分布在不同司法辖区的服务器，虚拟化搭建云端环境供用户使用，居于其中的电子数据因此表现出去中心分布、更易灭失等新特征，仍采传统取证方式可能陷入取证不能的困境。云计算环境基于商业需求与技术特性被高度虚拟化，数据实时动态变化，经频繁回收并再分配，被释放空间中又会有新数据写入，导致旧的原始数据彻底灭失。同时，物理存储介质与电子数据之间的联系更加多变，相对稳定性不再明确，数据实时性、虚拟性和易失性等特征体现得更强烈。一旦因云计算服务到期等原因导致数据再分配，即可宣告网络端原始电子数据已难恢复，只能退而求其次，尝试通过收集云计算平台日志、客户端残留的缓存数据等进行案情分析。〔9〕并且，案发时间越久，试图从其他来源取证的难度越大，即便侥幸能够发现蛛丝马迹，也往往难以达到证明标准。

---

〔2〕 See Suleman Khan, Abdullah Gani, et al., *Network Forensics: Review, Taxonomy, and Open Challenges*, 66 Journal of Network and Computer Applications 214, 230 - 231 (2016); Bharat Manral, Gaurav Somani, Kim-Kwang Raymond Choo, Mauro Conti & Manoj Singh Gaur, *A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions*, 52 ACM Computing Surveys 1, 1 - 3 (2019). 翟晓飞指出：“对新型网络犯罪中出现的黑灰产工具、恶意程序、物联网、工业控制系统、云计算等技术的取证能力还有待提高……电子数据取证对象变为‘云＋端’的复杂系统，需要综合存储、处理、传输在不同地方的数据才能证明某项事实。”李瑾：《〈公安机关办理刑事案件电子数据取证规则〉的运行和实践——专访规则主要起草人、公安部网络安全保卫局电子数据取证鉴定工作处处长翟晓飞》，载《警察技术》2021年第3期，第6页。

〔3〕 See Keyun Ruan, Joe Carthy, Tahar Kechadi & Mark Crosbie, *Cloud Forensics*, in Advances in Digital Forensics Ⅶ, Springer, 2011, p. 36.

〔4〕 See Ameer Pichan, Mihai Lazarescu & Sie Teng Soh, *Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis*, 13 Digital investigation 38, 41 - 42 (2015).

〔5〕 云取证（cloud forensics）特指以云计算平台为主要对象的取证活动。在我国实践中，常有人称“保全网”“存证云”等取证工具为云取证方式，此类工具实际上是以云服务技术辅助传统网络取证，将所获的网页截图或录像等存放在云服务器上，形成区块链证据进行证据固定，以确保证据完整性。本文所称云计算环境中的取证，与域外所称之云取证对应，为免混淆，若无特殊说明，本文所述之云取证皆指向此义。See Ameer Pichan, Mihai Lazarescu & Sie Teng Soh, *Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis*, 13 Digital investigation 38, 41 - 42 (2015).

〔6〕 杜晓、张希臣：《大数据时代，电子取证怎样锁定“黑手”》，载《法制日报》2017年9月22日，第5版。

〔7〕 域外学者发现，传统法律规范框架可能对侦查人员在云环境展开取证产生不利作用，澳大利亚为此进行了修法调整。See Hooper, Christopher, Ben Martini & Kim-Kwang Raymond Choo, *Cloud Computing and Its Implications for Cybercrime Investigations in Australia*, 29 Computer Law & Security Review 152, 152 - 154 (2013).

〔8〕 See Bharat Manral, Gaurav Somani, Kim-Kwang Raymond Choo, Mauro Conti & Manoj Singh Gaur, *A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions*, 52 ACM Computing Surveys 1, 1 - 5 (2019).

〔9〕 参见刘雪花、丁丽萍、刘文懋等：《一种基于软件定义安全和云取证趋势分析的云取证方法》，载《计算机研究与发展》2019年第10期。

面对此类实践难题，我国现有取证模式难以匹配云计算环境中电子数据取证的现实要求。传统电子数据取证模式多建立在单机取证环境办案经验之上，使用“一体收集模式”或“单独提取模式”。〔10〕两者都以现场操作为主。在云计算环境中这已难以实现，即便有所实践也可能致使整个云环境发生停滞，造成巨大损失。如波斯纳所指出：“正义的词义有时是效率，在一个资源稀缺的世界里，浪费是一种不道德的行为。”〔11〕这种手段与目的上的极端不匹配将严重影响取证合理性。因此，云计算环境中电子数据的这些结构特性和存储特性，极大增加了取证难度，使实践中常常出现取证不能，或因取证违法造成无法定案的难题。〔12〕

实践困境的形成展现出云取证规范体系上的不足与理论指引上的滞后。域外学者提出“云数据特例主义”（cloud data exceptionalism），〔13〕在不涉及云计算的情况下，数据不具备“分割离散性”（data's divisibility and data partitioning）、“动态变化性”（location independence）和“第三方控制性”（controlled by third parties）等特征，〔14〕而在涉及云计算情况下则具有此类特性，需要予以重点审视。相较而言，我国理论界对云取证相关问题的探讨仍然缺乏。〔15〕电子数据不再相对稳定地寄居于固定物理介质，而是灵活穿梭在虚拟空间之中，因此需要思考云取证为何具有差异性，如何转换取证思维应对这种差异性，从而以系统科学的取证措施和执法管辖方式处理云取证活动。有鉴于此，本文尝试全面展现云取证运行过程中所展现的新要求，检视当前法律规范在应对云取证时的局限性，以此为依据对相应规范提出完善建议。

二、云取证运行实践要求考察

云取证根植于云端环境之中，与其他网络环境下的电子数据取证活动相比，要求实现更高程度的实时化、自动化和协同化。理解并分析云端环境与其他环境的不同，是检验云取证规范适配性的基本前提。

（一）云取证要求实时化

尽管传统网络环境中的电子数据亦有易灭失性，但云计算环境采用虚拟化技术，具有伸缩弹性，居于其中的电子数据不断发生实时动态变动，因此其易灭失性表现得更为强烈，可称之为强灭失性。较之其他环境中的电子数据取证活动，云取证需满足更高的时效性要求，不能仰仗传统物理存储介质的相对稳定性来确保数据完整性和真实性，也不能依赖事后在线提取电子数据，而

〔10〕“一体收集”模式，是指在收集电子数据时连同原始存储介质一并扣押、封存、移送。在查封、扣押电子数据原始存储介质时，也实现了对其中存储电子数据的一并收集。“单独提取”模式则是指，仅从原始存储介质中提取电子数据，提取后将其存储在其他存储介质中，而并不对原始存储介质予以查封、扣押和移送。参见谢登科：《电子数据的取证主体：合法性与合技术性之间》，载《环球法律评论》2018 年第 1 期。

〔11〕〔美〕理查德·波斯纳：《法律的经济分析》（第 7 版，中文第 2 版），蒋兆康译，法律出版社 2012 年版，第 36 页。

〔12〕例如某案件中因云服务器到期造成数据永久灭失不能取得。参见最高人民法院（2023）最高法知民终 1432 号民事判决书。类似案例还可参见上海市闵行区人民法院（2023）沪 0112 民初 29410 号民事判决书等。

〔13〕See Dan Jerker B. Svantesson, *Against 'Against Data Exceptionalism'*, 10 Masaryk University Journal of Law and Technology 200, 204 (2016).

〔14〕See Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale Law Journal 326, 365 - 398 (2015).

〔15〕以“云取证、云端取证、云计算取证”等作为主题词和关键词，在中国知网进行检索，发现法学论文文献不足 10 篇，但技术类论文较多。

应以实时化提取保存为主要导向。司法实践中，大量案例均因未能实现实时取证而导致证据灭失，致使司法证明一度受阻。例如知识产权侵权案件中，若在正式立案后再申请调取云服务器中的证据，则由于民事诉讼中的当事人不能采取强制性取证措施，侵权人可能在此期间故意不再续约云服务，催化证据灭失，或篡改云服务器中的电子数据，导致原告举证受挫。另外，由于实时取证较传统事后取证要求更为严苛，若云服务商与犯罪嫌疑人相勾结，则更容易篡改毁灭证据，且更具隐蔽性和破坏力。若不予以更严密的规制，则意味着电子数据被污染或毁损的几率大幅提升，证据的完整性和真实性都难以充分保障。

云端环境瞬息万变，因此云取证过程应更加重视网络端实时取证，借此克服传统事后取证方式导致电子数据完整性与真实性缺失的风险。作为云计算服务的主要使用者，也是网络攻击的主要受害者，全球各大企业率先探索数字取证与事件响应机制（digital forensics and incident response，以下简称 DFIR），〔16〕用以保障其向云端计算与远程工作转型过程中的安全能力。这是一套自动化实时取证机制，旨在实时完成云端系统和企业内部系统有效取证和安全防御。数字取证模块聚焦于实时识别、分析、收集与固定云端系统与本地系统的数据，并将之作为证据提供给事件响应模块，用以分析事件，弥补漏洞，同时将所获证据用于诉讼。DFIR 机制将取证时点提前，从而避免数据损失造成的不利后果，并且持续不断运行，以确保云端环境下实时取证的需要。〔17〕此外，在实践中，企业或者侦查机关还通过在云端预设蜜罐陷阱〔18〕进行取证，采取了更为主动的实时化设置，将取证时点进一步提前。但是这一趋势也产生了一系列新的风险，例如蜜罐取证可能涉及诱惑侦查问题，其正当性需被进一步考察。

（二）云取证要求自动化

与传统网络环境相比，云计算环境中数据更加庞杂、隐蔽、多变，数据伪装等反取证技术更繁复。在对云计算平台进行数据提取时，取证人员不仅需要面对云计算环境中浩如烟海的巨量电子数据，还需要处理因分布式计算及多租户环境导致的电子数据混杂难题。〔19〕这种难题体现在，云计算服务通过分配分布式异构型虚拟计算资源供用户使用，导致大量半结构化、非结构化数据格式同时存在，没有统一格式标准，需要进行更为复杂的数据清洗以整合此类异构资源。〔20〕此外，在云计算环境中对日志等证据进行分析也越来越依靠自动化手段。〔21〕并且，不同类型的云计算平台数据混杂程度不同，使证据的识别与提取更加困难。在公有云、混合云中，多个租户同时租用同一云环境，若没有云服务商的协助配合，取证人员通常需在海量混杂数据中对某一特定

〔16〕 See *What is DFIR (Digital Forensics and Incident Response)?*, available at https://www.sentinelone.com/cybersecurity-101/what-is-digital-forensics-and-incident-response-dfir/, last visited on Jun. 28, 2024.

〔17〕 See Bharat Manral, Gaurav Somani, Kim-Kwang Raymond Choo, Mauro Conti & Manoj Singh Gaur, *A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions*, 52 ACM Computing Surveys 1, 5－6 (2019).

〔18〕 蜜罐陷阱（honey pot）是一种以诱骗技术为核心的网络安全技术，通过预先设置好诱骗系统，为攻击者提供一个容易攻击的目标，引诱违法犯罪者对其展开进攻并借此收集固定证据。

〔19〕 云计算取证主要问题集中于取证环境转变引发的各项挑战，但也需要注意，云端环境中的数据类型并不总是以大数据形式展现，也有小数据存在，但整体上云计算服务仍然以大数据处理作为主要形态，这也属于云计算环境的一大特点。

〔20〕 参见贾焰、方滨兴、汪祥等：《泛在网络空间大数据“雾云计算”软件体系结构》，载《中国工程科学》2019 年第 6 期。

〔21〕 See Suleman Khan, Abdullah Gani, et al., *Cloud Log Forensics: Foundations, State of the Art, and Future Directions*, 49 ACM Computing Surveys 1, 40－41 (2016).

用户的电子数据进行分层并完成“提纯萃取”，获取完整可信的证据链难度较高。

如果在云取证中采用传统人力资源手动取证为主的方式，则难以完成如此高准确度的取证目标，即便能够完成，也将造成资源严重浪费，反而得不偿失。此外，随着人工智能技术渗透到犯罪行为与侦查活动的对抗之中，深度伪造（deepfake）等手段开始被用于云端实时反取证、反侦查，仅依靠人力进行经验判别将非常困难。〔22〕为了应对这一问题，需要依靠算法来对抗算法，这就必然要求取证模式向自动化方向演进，在这一过程中，不仅需要面对当前反深度伪造技术本身在跨模态检测、实时能力、算法偏差和通用性等方面仍存在的缺陷，〔23〕还需警惕算法歧视、算法黑箱等问题。因此，在变幻莫测的云计算环境中进行取证活动需要更强的技术力支撑。单纯依靠人力资源进行取证的形态终将逐步被人机协同、机器为主的自动化取证形态所取代，云取证实践的自动化要求挑战了建立在传统人力取证经验之上的既有取证规范框架。

（三）云取证要求协同化

传统网络环境服务框架相对单一，电子数据多居于单机之中，数据原始介质所在地相对固定，能够借用物理介质的相对稳定性来保障存储其中的电子数据的真实性与完整性。在司法实践中，对物理存储介质进行扣押与传统物证扣押的方式大致相同，唯在扣押过程中如何确保电子数据的完整性与真实性等方面有不同安排。但云计算虚拟化技术的应用，或者说云数据分割离散性、动态变化性与第三方控制性的特点，使这种相对稳定性不再可靠。

云计算环境存在多种不同的复杂服务架构，为适应不同服务架构的特点，云取证需向协同化转型，主要分为两个层次，一方面要求公私合作协同，另一方面则要求跨辖区合作协同。美国国家标准与技术研究院（NIST）将云服务划分为基础架构即服务（Infrastructure as a Service，IaaS）、平台即服务（Platform as a Service，PaaS）和软件即服务（Software as a Service，SaaS）。〔24〕不同服务架构与可收集的证据紧密相关，在 PaaS 和 SaaS 云服务中，取证人员如需获得日志和配置文件等信息，基本只能依赖云服务提供商的协助配合（并且有些网络服务提供商没有存储日志的机制），IaaS 则依赖程度较低。〔25〕若缺乏稳定可靠的公私合作机制，则可能因协同不畅导致取证迟延，进而产生数据灭失的后果。或是因为云服务商与犯罪分子勾结篡改、毁损证据，从而误导侦查机关。此外，云计算环境可分为公有云、私有云、混合云（一部分数据存储在公有云中，另一部分数据存储在私有云中）等类型。在公有云和混合云架构中，不同用户的电子数据可能混杂在一起，需要进行区分处理，否则可能侵犯其他用户的数据权利。如果没有云服务提供商予以数据清洗等方面的技术配合，这一工作将非常棘手，浪费大量司法资源。

同时，云环境的去地域化特点格外鲜明，使跨境取证更加频繁。〔26〕在有组织类犯罪等复杂

---

〔22〕 See Shaik Sharmila & Ch Aparna, *Tracing Footprints of Anti-forensics and Assuring Secured Data Transmission in the Cloud Using an Effective ECCDH and Kalman Filter*, 221 Journal of Network and Computer Applications 1, 3－4 (2024).

〔23〕 See Shavez Mushtaq Qureshi, Atif Saeed, et al., *Deepfake Forensics: A Survey of Digital Forensic Methods for Multimodal Deepfake Identification on Social Media*, 10 PeerJ Computer Science 1, 31 (2024).

〔24〕 See Peter Mell & Timothy Grance, *The NIST Definition of Cloud Computing*, pp. 2－3, available at https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800－145.pdf, last visited on Feb. 5, 2025.

〔25〕 See Prasad Purnaye & Vrushali Kulkarni, *A Comprehensive Study of Cloud Forensics*, 29 Archives of Computational Methods in Engineering 33, 34－35 (2022).

〔26〕 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》，载《河北法学》2021 年第 4 期。

案件中，电子数据可能同时存放在多个处于不同辖区的云服务提供商的主机，这些云服务提供商不仅公司所在地跨多个司法辖区，其服务器物理所在地或者说数据中心所在地也往往在不同司法辖区，这意味着解决司法管辖权冲突问题面临更多挑战。传统刑事司法协助制度由于过程缓慢、程序繁琐，往往不能满足云取证的时效性要求，因此需有新的跨境协同取证框架予以支撑。

三、既有取证规范与云取证实践要求适配性匮缺

规范取证活动，最重要的价值取向在于保障取证的合法性和有效性。依此标准，解答这一问题主要涉及取证措施规范与取证管辖规范两大维度的考察。通过审视这两大维度的取证规范，能够较全面地把握既有电子数据取证制度，思考其能否与云取证实践要求相匹配相适应，以决定优化与完善的方向。

（一）既有取证措施规范的局限性

既有取证措施及其规范灵活性不足的关键原因在于，传统电子数据取证思路仍建立在物证本位基础之上，过度信赖实物证据的相对稳定性和客观性，并依思维惯性，认为栖居于具封闭外观之实物容器中的电子数据亦相对稳定和客观，但云端环境稀释了物理实物所代表的稳定性，使这一思路面临失效、失灵甚至失败的窘境。当前所推行的“扣押原始存储介质为主、提取电子数据为辅、打印拍照为例外”的取证原则，〔27〕试图通过查封扣押固定物理存储介质，以实现对此数据容器之保全，再行提取本地数据，与网络端表现相互印证，从而达到证明标准。在这其中，在线提取电子数据等只作为一种补充性、后置性方式存在。对这一原则的强调，折射出规范制定与实践运行仍以物证作为证据之王的传统思维。云端环境变化多端，以物证为本位，而非以数据为本位的规范进路和思考惯性，呈现出稳定有余而灵活不足的样态，是否能适应云取证带来的全新挑战，在理论层面颇有疑问。在此进路基础之上单独填补其他措施如先行冻结等，则使规制方案缺乏系统性，何况基本法律规范尚未将之纳入，反而表现出谨慎态度。此类问题的集聚，使既有取证措施规范体系在逻辑上和适配性上表现出一定缺陷，具体分析如下：

1. 先行冻结措施单兵突进缺乏系统性解决方案

为了应对云计算环境数据实时变动的特点，防止数据灭失，2016 年最高人民法院、最高人民检察院、公安部发布《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》），其中第 11 条、第 12 条专门规定数据先行冻结措施，将之作为云取证的重点解决方式。其后 2019 年公安部发布《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》），没有再设置新措施，对于数据先行冻结只是加入了写保护予以完善。与传统刑事诉讼法理论中的冻结不同，从性质来看，数据先行冻结措施属于一种证据保全行为，而传统刑事诉讼法理论中的冻结则是对财产性利益进行保全，因此两者在实质上有所差

〔27〕 参见田虹、翟晓飞、王艺筱：《〈公安机关办理刑事案件电子数据取证规则〉的理解与适用》，载《派出所工作》2019 年第 3 期。

异。[28] 虽然数据在一定维度亦具财产属性，但在侦查取证角度，数据更多被赋予一种证明价值，不似传统冻结一般还带有确保后续执行顺利的意图，例如查明并冻结赃款用于没收其违法所得。尽管有学者认为先行冻结电子数据属于一种技术手段，而非单设的一种侦查措施，[29] 但从文义来看，冻结一词直接选用了约定俗成的既有概念，只是冻结对象发生了变化，其本质仍是一种保全措施。在《电子数据规定》制定过程中，关于使用“冻结”还是“查封”曾发生较大争议，后请示全国人大法工委，明确查封和冻结属于性质、效果相同的侦查措施，查封多用于财物、文件，冻结多用于存款等财产，对于电子数据而言，法工委意见是两者皆可。后经权衡，确定使用“冻结”概念。[30] 结合立法过程与理论界主流观点，先行冻结电子数据应属于一种强制性侦查措施。[31] 立法者明确指出规定该措施就是“针对云计算、大数据环境下，难以将海量数据封存、扣押，以及数据难以提取的问题”[32]。但实际上，这一措施没有完全发挥预期作用，也不应承载单兵突破的重任。

首先，作为一项对公民基本权利作出强制性干预的措施，先行冻结电子数据的设定需遵行法律保留原则，应当由基本法律进行规定。《电子数据规定》和《电子数据取证规则》两项规范性文件在效力等级上过低。《中华人民共和国刑事诉讼法》（以下简称《刑事诉讼法》）没有规定数据先行冻结，2021 年《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》（以下简称《刑诉法解释》）仅在第 111 条第 5 项提及“审查冻结后的访问操作日志”，似乎认可了《电子数据规定》所提出的先行冻结措施，但观察整个《刑诉法解释》，其他条文仍然采用传统刑事诉讼理论对冻结的理解，并没有在取证措施处予以新的规定进行明确。何况《刑诉法解释》并不能超出《刑事诉讼法》进行立法创设，只能在其范围内进行法律解释。故既有规范并不足以支撑先行冻结数据作为强制性措施的合法性。

其次，当前只有部分云服务提供商在技术上建立起数据冻结服务，[33] 且未有完善的公私合作与监督配套机制予以支撑。实践中，云服务提供商基于商业利益，或是出于保护用户个人信息、隐私、商业秘密等考虑，在配合侦查机关取证时常常存在拖延或拒绝配合的情形。尽管《刑事诉讼法》第 52 条和第 54 条对私主体配合侦查工作作出明确规定，但是在跨辖区执法与司法过程中，云服务提供商基于地区保护主义等因素迟延配合冻结的例子屡见不鲜。再者，云服务提供商本身就需要对被冻结用户的身份同一性等进行核对，这也需要一定时间，如此导致冻结的实际效果并未达到预期，需要对云服务提供商的合作与监督机制进行优化。并且，冻结措施可能侵犯其他云服务用户的数据权利。云环境还具有多租户、异构性、分布式等特征，数据产权界分复

〔28〕 参见喻海松：《刑事电子数据的规制路径与重点问题》，载《环球法律评论》2019 年第 1 期。

〔29〕 参见刘浩阳等：《公安机关办理刑事案件电子数据取证规则释义与实务指南》，中国人民公安大学出版社 2020 年版，第 53 页。

〔30〕 参见刘浩阳等：《公安机关办理刑事案件电子数据取证规则释义与实务指南》，中国人民公安大学出版社 2020 年版，第 158 页。

〔31〕 参见裴炜：《论刑事跨境取证中的数据先行冻结》，载《当代法学》2023 年第 2 期；谢登科：《电子数据冻结：一种新兴的证据保全措施》，载《东岳论丛》2023 年第 6 期。

〔32〕 周加海、喻海松：《〈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〉的理解与适用》，载《人民司法·应用》2017 年第 28 期，第 35 页。

〔33〕 参见喻海松：《刑事电子数据的规制路径与重点问题》，载《环球法律评论》2019 年第 1 期。

杂。在公有云和混合云中，如果不与云服务提供商配合进行预先技术处理，则可能误将其他用户的数据冻结，对其数据权利造成严重干预。按传统理论，公民具有隐私权、财产权等基本权利，商业秘密等其他权益也受到保护。伴随数字社会来临，公民的数据权利也被广泛关注。不少学者主张建立如个人信息权、〔34〕个人数据权利、〔35〕数据财产权〔36〕等新型权利，虽侧重点不同，但均关注到数据权利的人身属性、财产属性，同时阐明其亦关涉国家主权属性。〔37〕从数据权利的这三重属性出发，除可能构成对被取证对象本身的数据权利干预以外，对其他用户的数据权利亦可能造成侵犯，因此必须建构起相应合作与监督机制，确保技术处理有效，云取证过程合法正当才能较好地解决这一问题。

最后，仅凭先行冻结电子数据单兵突进并不能一劳永逸地解决电子数据在云环境中的强灭失性。尽管冻结电子数据从理论上能够更好地保障完整性和真实性，但是在实践中还出现了诸多复杂状况，例如恶意网络服务提供商（malicious CSP）问题。〔38〕特别是在 PaaS 和 SaaS 架构中，由于这两种架构必须依靠云服务提供商秉持善意予以协助，否则即便其同意冻结数据，也不能保障在随后的在线提取过程中不被恶意干扰。因此从技术上来说，需要构建一整套配合方案，联结各项取证措施协调工作，而不应由冻结电子数据单兵突进。域外对此已有探索，分别针对云计算在客户端、网络端和服务器端运行的特点及取证实际需要，通过搭建起云取证即服务架构（包括 CFeS、〔39〕SecLaaS〔40〕等各种方案构想）予以技术层面的系统应对，在这些构想中，往往同时联结与云服务提供商的预先合作等措施，包括要求其提供虚拟机日志加密备份服务，通过依法开放数据接口等方式确保云取证的有效性。相较之下，我国现行规范仍然较为粗疏，暂未有从整体联动角度设计的技术方案，以及与之对应的控权规范机制，因此尚难做到对云取证进行精细化规制。

2. 在线提取数据与远程勘验措施规范逻辑失洽

较之传统单机环境下的电子数据取证，云取证高度依赖在线提取方式获得相关证据材料。这在《电子数据规定》与《电子数据取证规则》中得到回应，在线提取电子数据被单独规定，同现场提取电子数据形成对应，与冻结电子数据相并列，其中涵盖了远程勘验相关内容。然而，在形式层面，此方式突破了基本法律的规范，致使取证手段与措施之间产生混同。按传统刑事诉讼制度的运行逻辑，提取证据非法定侦查措施，而属侦查手段，例如提取指纹等；勘验则明确属于基本法律规定的侦查措施。然而，在处理网络在线提取和网络远程勘验之间的关系时，《电子数据规定》和《电子数据取证规则》超出传统规范逻辑，在法律性质和体系定位上更多将网络在线提

〔34〕 参见王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，载《现代法学》2013 年第 4 期。

〔35〕 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018 年第 3 期。

〔36〕 参见张新宝：《论作为新型财产权的数据财产权》，载《中国社会科学》2023 年第 4 期。

〔37〕 参见李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期。

〔38〕 See Bharat Manral, Gaurav Somani, Kim-Kwang Raymond Choo, Mauro Conti & Manoj Singh Gaur, *A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions*, 52 ACM Computing Surveys 1, 14 (2019).

〔39〕 See Stavros Simou, Christos Kalloniatis, Stefanos Gritzalis & Vasilios Katos, *A Framework for Designing Cloud Forensic-enabled Services (CFeS)*, 24 Requirements Engineering 403 (2019).

〔40〕 See Shams Zawoad, Amit Kumar Dutta & Ragib Hasan, *Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service*, 13 IEEE Transactions on Dependable and Secure Computing 148 (2015).

取确立为电子数据的侦查措施，而将网络远程勘验作为其内在构成要素和实现方式，出现了倒挂现象。〔41〕并且，上述两个规范性文件还将远程勘验与技术侦查相嫁接，致使原有分野模糊化，使传统侦查措施与电子取证措施在规范表达上呈现出支离破碎的杂乱观感。〔42〕而在实质层面，无论是进行在线电子数据提取，还是实施远程勘验，均有名不符实的情况，即以勘验之名，行搜查之实，或覆盖先行冻结数据等措施。〔43〕在实践中，侦查机关为提高取证效率，应对云计算环境实时变动的特征，常常基于实用主义考量，同时概括实施多种措施。从诉讼原理出发，取得证据及证据调查程序是不同的概念，通常具有先后关系，搜查、冻结、扣押属取得证据，而勘验、鉴定等则属证据调查程序。在取得证据时，应依其强制处分层次，考量基本权干预及其合法性要件。而对于已取得证据之调查程序，则重心在于采取何种法定证据方法（如勘验或鉴定）等。〔44〕可见，两者之法律性质截然不同，对基本权利干预程度迥然有别，因此不应含混实施。

3. 缺乏对新取证实践方式的规范监督

云取证实践中企业等私主体和侦查机关采取更加积极主动的态势，广泛使用 DFIR、蜜罐取证等新式取证手段或方式，其中一些方式蕴藏风险，缺少规范控制。对于 DFIR 等提前取证时点、自动化展开证据分析与收集，并最终生成的相应证据报告是否具有证据效力，尚存理论争议。再以蜜罐取证为例，在刑事取证中，侦查机关采取此种取证方式有诱惑侦查之嫌。《刑事诉讼法》第 153 条规定了诱惑侦查，此类措施归属于技术侦查，其强制性在整个刑事侦查措施中亦属最高级别，按法律保留原则，必须由基本法律规范予以明确规定，只能在特定案件中使用，并受到包括令状主义在内的极其严格的程序限制，以此缓释对其正当性的质疑。〔45〕至于在民事案件中，私主体设置陷阱进行取证是否合法正当，尚无直接法律规定，而需依据《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第 106 条进行处置，即以严重侵害他人合法权益、违反法律禁止性规定或者严重违背公序良俗的方法形成或者获取的证据，不得作为认定案件事实的根据。

根据司法实践表现来看，现有场景中的蜜罐取证鲜少受到规制，未被纳入技术侦查措施之中。这其中涉及法律价值平衡的复杂问题，如何平衡正义与效率，实有赖于确立相应规制框架，以免肆意运行酿成风险。特别是在缺乏规制的情况下，若公权力主体与私主体相配合，通过私主体之手预先设置蜜罐陷阱，再将取得证据转交刑事侦查机关，则仍将陷入未受法律规范的诱惑侦查之正当性质疑中。

（二）既有取证管辖规范的阻滞性

由于云计算具有去中心分布和虚拟化等特征，云数据呈现分割离散性、动态变化性和第三方控制性，致使云取证大量涉及跨境取证问题，这种去地域化虚拟环境使网络空间执法管辖权问题

〔41〕 参见谢登科：《电子数据网络远程勘验规则反思与重构》，载《中国刑事法杂志》2020 年第 1 期。
〔42〕 参见裴炜：《论远程勘验：基于侦查措施体系性检视的分析》，载《政法论坛》2022 年第 4 期。
〔43〕 参见梁坤：《跨境远程电子取证制度之重塑》，载《环球法律评论》2019 年第 2 期。
〔44〕 参见林钰雄：《干预处分与刑事证据》，北京大学出版社 2010 年版，第 6 页。
〔45〕 参见程雷：《诱惑侦查的程序控制》，载《法学研究》2015 年第 1 期。

格外复杂。网络空间执法管辖权涉及网络疆界问题，本身即网络主权的重要组成部分，〔46〕在提升自身跨境取证有效性的同时，国家为维护网络主权，还需兼顾本土数据安全性，防范未经本国许可的任意跨境取证。

跨境数据取证中的执法管辖权模式主要有两种，即数据存储地模式和数据控制者模式。一般认为，数据存储地模式能更大程度上确保本土数据安全性，但面对云取证活动所要求的高时效性则有些不敷应对，可能导致取证有效性不足。这也是美国专门推出《澄清合法使用境外数据法》（又称《云法案》，Clarifying Lawful Overseas Use of Data Act，Cloud Act），转向数据控制者模式的直接动因。相比之下，数据控制者模式更趋灵活，但可能对国家司法主权构成威胁。〔47〕

纵观近年来我国逐步出台的《中华人民共和国国际刑事司法协助法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》（以下分别简称《国际刑事司法协助法》《网络安全法》《数据安全法》）《促进和规范数据跨境流动规定》等规范性文件，我国当前所采执法管辖权模式整体上属于数据存储地模式。在美国《云法案》出台后，我国颁布《国际刑事司法协助法》予以回应，该规定将数据存储物理位置作为确定执法管辖范围的基础，并要求以传统司法协助方式为主导开展跨境取证合作。该法充分体现我国高度尊重网络主权的负责任态度，但就具体取证有效性来说，客观上未能完全解决因传统司法协助程序繁琐、过程复杂带来的取证时效性不足问题。2019 年《电子数据取证规则》第 23 条限缩了网络在线提取电子数据的范围，规定只有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才可以通过网络在线提取方式取得。并且，该法所规定的冻结措施，仍是传统刑事诉讼理论中的财产性冻结，而非《电子数据规定》中的证据保全性冻结，表现出立法过程中两者之间缺乏协调，也更加突出了电子数据先行冻结仍然缺乏基本法律规定，不符合对强制性措施的法律保留原则，其合法性基础仍较为薄弱，在云取证时或将面临正当性诘问。〔48〕此外，《数据安全法》第 31 条、《网络安全法》第 37 条均设置了颇为复杂的安全评估和审查程序，以加强对跨境数据流动的管控。〔49〕综合考量跨境取证时的合法性与取证有效性问题，有学者认为纯粹的数据存储地模式已经与当前数据跨境取证的整体趋势存在一定抵牾之处，需要进行一定调整。〔50〕

目前，就跨境电子数据取证问题，各国均开始探索不同的法律框架，包括确立不同类型的云数据取证安全与执法方案。其中，美国《云法案》采用数据控制者标准，以对本国企业管辖权为依据，即便数据存储在境外，亦允许执法机关直接从本国企业获取调查犯罪所需的电子证据。为减少跨境法律冲突，美国《云法案》设计了双边协议机制，通过合作构建快捷取证通道，绕开传

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

〔47〕 参见梁坤：《基于数据主权的国家刑事取证管辖模式》，载《法学研究》2019 年第 2 期。

〔48〕《欧盟通用数据保护条例》第 48 条明确规定，第三国法院裁判以及行政机关决定，要求数据控制者或处理者传输或披露个人数据，只有基于第三国与欧盟或欧盟成员国之间的有效国际协议，且不影响该条例第五章规定其他法律规定，才可获承认或执行。第五章第 45 条等确立了保护水平充分性评估机制，要求重点进行权利保护等因素的审查。

〔49〕 参见裴炜：《论刑事跨境取证中的数据先行冻结》，载《当代法学》2023 年第 2 期。

〔50〕 参见梁坤：《基于数据主权的国家刑事取证管辖模式》，载《法学研究》2019 年第 2 期。

统刑事司法协助渠道，直接从对方企业调取境外电子数据。〔51〕此外，美国还意图以其《云法案》为基础建构数据取得的全球标准，以链接全球云数据；〔52〕欧盟虽未全面转向数据控制者模式，但亦改变纯粹的数据存储地模式，而是对其进行适度变通。欧盟强调欧洲云战略（European Commission Cloud Strategy），〔53〕以《欧盟通用数据保护条例》《欧盟数据治理法案》等规范性文件为基础，维护技术主权，进行可信化监管。欧盟通过欧洲云联盟（European Cloud Alliance）等组织引领产业发展，〔54〕不断强调云数据基础设施安全，〔55〕并提升欧盟域内的数据调取协同化，在成员国互认原则基础上，建立欧洲调查令、提交保存令等制度简化欧盟内部的数据跨境取证问题，其中数据所在位置对指令签发等事项不再重要，网络服务提供者是否“在联盟中提供服务”则变得尤为重要，这意味着纯粹的数据存储地模式已然松动。〔56〕欧盟数据保护委员会（EDPB）还通过批准《欧盟云行为准则》（The EU Cloud Code of Conduct）〔57〕等措施，引导企业遵守《欧盟通用数据保护条例》等法律法规，接受定期评估和监督，以建立统一行为规范，为云取证等执法活动提供便利。欧美均基于其自身特点和利益，欲推动其云规范成为全球标准，以取得全球治理的主动权。此外，欧美还寻求达成新的跨境电子数据取证相关协议，〔58〕并格外重视与云服务提供商之间的公私协作，探索各种新型合作机制。若我国不加以系统应对，可能难以针对欧美云服务商进行高效取证，而我国在欧美开展商业活动的云服务提供商则需要服从其规则协助取证，如此不对等或将对我国国家利益有所不利。〔59〕

对此，我国除加强域内法律规范供给外，还积极参与《联合国打击网络犯罪公约》谈判进程，力争以联合国为中心确立相应国际规范，维护我国涉外活动中的国家利益。我国认为应平衡尊重国家司法主权与打击犯罪的需求，明确主张现阶段各国宜主要通过优化司法合作机制的方式提高取证效率，并共同推动在联合国框架下确立普遍接受的跨境调取电子数据规则。〔60〕整个谈

---

〔51〕 参见张路遥、龚雯聪：《联合国打击网络犯罪公约相关法律问题的各国立场》，载《中国信息安全》2020 年第 9 期；梁坤：《美国〈澄清合法使用境外数据法〉背景阐释》，载《国家检察官学院学报》2018 年第 5 期。英国与美国已签署相关协议。See *US and UK Sign Bilateral E-Evidence Agreement*, available at https://eucrim.eu/news/us-and-uk-sign-bilateral-e-evidence-agreement/, last visited on Jun. 8, 2024; Marcin Rojszczak, *CLOUD Act Agreements from an EU Perspective*, 38 Computer Law & Security Review 1, 1-4 (2020).

〔52〕 See Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 Columbia Law Review 1681 (2018).

〔53〕 See *The European Commission Cloud Strategy*, available at https://commission.europa.eu/system/files/2019-05/ec_cloud_strategy.pdf, last visited on Jun. 8, 2024.

〔54〕 See *European Alliance for Industrial Data, Edge and Cloud*, available at https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance, last visited on Jun. 8, 2024.

〔55〕 典型代表为 GAIA-X-European Federation of Data and Cloud Infrastructure，其网站为 https://gaia-x.eu/about/，最后访问时间：2024 年 6 月 8 日。

〔56〕 参见刘品新：《跨境电子取证的欧盟方案及启示》，载《国家检察官学院学报》2022 年第 5 期；Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings, Art. 3 (1), Art. 3 (2).

〔57〕 See *What is the EU Cloud Code of Conduct?*, available at https://eucoc.cloud/en/about/about-eu-cloud-coc, last visited on Jun. 8, 2024.

〔58〕 See *E-Evidence: Commission Obtains Mandates for EU-US Agreement and Negotiations in Council of Europe*, available at https://eucrim.eu/news/e-evidence-commission-obtains-mandates-eu-us-agreement/, last visited on Jun. 8, 2024.

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

〔60〕 参见张路遥、龚雯聪：《联合国打击网络犯罪公约相关法律问题的各国立场》，载《中国信息安全》2020 年第 9 期。

判过程中，我国反对滥用数据控制者模式，主张尊重各国主权，建立具有广泛包容性与可接受性的跨境电子数据取证规则。在各国充分博弈后，《联合国打击网络犯罪公约》规范文本未采用数据控制者模式，但是确立了一部分更符合电子数据取证要求的取证措施，并建立了更多国际合作快速反应机制。其中第四章自第 25 条至第 30 条，要求各缔约国授权建立提交令、快速保全、实时收集电子数据等机制。第五章则着力确立国际合作机制，但就其中内容各国不同观点激烈交锋，最终较为稳妥地确立了司法协助一般原则与程序。

《联合国打击网络犯罪公约》中文规范文本在确立取证措施时，明确采用了“快速保全存储的电子数据”“快速保全和部分披露流量数据”“搜查和扣押存储的电子数据”“实时收集流量数据”“拦截内容数据”“冻结、扣押和没收犯罪所得”等表达。通过区分电子数据、流量数据、内容数据等概念，对数据予以适当类型化处理，设置更具有针对性的取证措施，既保障取证合法性，又提升取证有效性。同时，公约仍然明确冻结应作为一种针对违法所得的财产性保全措施予以使用。根据公约内容，对电子数据的证据性保全，需以搜查、扣押以及提交令等作为主要强制性措施。整体而言，《联合国打击网络犯罪公约》所确立的框架，能够被更广泛地接受，更符合我国实践要求。但当前我国域内法律尚未完全与之协调，以此为标杆，我国或将进一步完善域内法律规范，适应公约要求，并对数据存储地模式予以适度调整，并建立与云服务提供商等私主体更为紧密的新式公私合作机制，赋予执法管辖机制更多灵活性，以确保跨境取证合作更加顺利。

四、云取证制度调适方案

云取证的实际运行状况表明，既有取证规范与相应制度难以完全适应其实际需求，应当予以适当调整。可转换取证思维，从取证措施规范与执法管辖规范两方面着手，寻求更加系统化、科学化的调适方案。

（一）构建体系化技术规制与程序制约方案

既有取证措施规范“以扣押原始存储介质为主、提取电子数据为辅、打印拍照为例外”的电子数据取证原则，已难以适应云取证的现实需求，不能确保云取证的时效性，使电子数据的完整性和真实性存在缺损风险。应当重视电子数据本体，而非全盘贯彻既往以处理实物证据方式对待数据的思路，需关注云数据的分割离散性、动态变化性和第三方控制性，不再单纯拘泥于以扣押原始存储介质为主、提取电子数据为辅的思路，在云取证中将在线提取电子数据作为主要取证手段。可考虑在线提取电子数据与扣押原始存储介质并重，打印拍照为例外的取证进路，以增强云取证有效性，同时需加强程序性保障，使之合法性与正当性得到保障。

此外，我国当前的规制思路仍以规范冻结、远程勘验、在线提取数据等手段方式作为导向，但当前因应云取证的现实需求，域外所探索的云取证即服务框架越来越多见（如 SecLaaS）。这些框架分别针对客户端、网络端、服务器端作出系统性处理，客户端与服务器端主要运用传统网络取证方式并予以技术升级迭代，网络端则格外侧重静态分析与动态实时分析并重的方式，以此适应云环境的实时变动。在这三端通过一整套框架同时采取多项手段，结合区块链存证等最新技术，实现以技术规制技术的进路。基于此路线，我国可进一步完善技术性程序规制，借鉴引入区

块链存证的经验，吸收较为成熟稳定的云取证即服务框架作为主要技术应用方案，实现以云治云的策略，并基于此构建具体规则，改变过往冻结措施单兵突进的思维模式。配合这一方案，需要建立技术能力审查机制和伦理审查机制，可通过设置相应委员会对云取证即服务框架进行评测，建立白名单机制，将成熟可靠的云取证技术方案纳入白名单之中并用于云取证实践。

同时，应当厘清既有取证措施之间的逻辑关系。在规范表达层面，明确在线提取电子数据等方式属于一种取证方式或方法，在基本法律未予以明确规定的情况下，不应与冻结电子数据等强制性侦查措施在逻辑上并列，亦不应与勘验甚至技术侦查混同。应重新梳理并更新《电子数据规定》《电子数据取证规则》等规范性文件的相关内容，清楚界分在线提取方式方法与侦查措施的区别，形成逻辑自洽的规范体系。从长远来看，则需明确先行冻结电子数据应否纳入《刑事诉讼法》之中，并考虑其与《联合国打击网络犯罪公约》的协调性。

再者，应当将刑事案件中的蜜罐取证等自动化实时取证活动纳入技术侦查体系予以严密控制。从行为本质上看，蜜罐取证与诱惑侦查、控制下交付等有性质相近之处，因此应以更高要求予以限制。基于当前涉网犯罪案件不断攀升的实际情况，以及全链条打击的现实需求，可以考虑限定蜜罐取证等自动化实时取证的陷阱设置所适用的案件范围，例如传统危害国家安全类犯罪、黑社会性质组织类犯罪、网络毒品与金融类犯罪，以及跨境电信诈骗等特定复杂犯罪，并以获取相关令状作为自动化实时取证的前提条件，或设计相应备案报告制度，要求公权力机关将自动化实时取证设置备案以供审查，以此平衡程序正义与诉讼效率。

此外，DFIR 等自动化电子数据取证机制已然成为一种新的趋势，对其中人工智能加持下自动生成证据报告的审查判断机制也需予以因应，特别是需明确其证据效力与归责问题。可考虑先将此类报告定义为《刑诉法解释》第 100 条所规定的专门性报告。当前其定义为“有专门知识的人就案件的专门性问题出具的报告”，其生成主体仍为人类。若依严格的文义解释，人工智能加持下机器自动生成的分析报告能否归入《刑诉法解释》第 100 条所确定的专门性报告有所疑问。但可考虑对专门性报告予以扩大解释，将云取证中应用的自动算法定位为有专门知识的人进行科学活动时运用的工具，其责任主体仍可归于有专门知识的人本身，以缓释该问题。就长期发展而言，则需根据奇点〔61〕能否突破，决定自动生成证据报告的归责问题如何解决。

最后，在补足云取证灵活性的同时，应以权利束理念强化数据权利保障，加强对云取证过程中公权力的控制约束。针对公有云、混合云等特殊环境的特性，应当进行公私合作，厘清数据产权。数据上的权能分割从一开始就是常态，数据自产生伊始就具有复杂的利益共生和相互依存关系，因此有观点主张以权利束理念应对其带来的权利保障难题。〔62〕通过区分数据来源主体的法定在先权利和数据处理主体的数据财产权利，进一步厘清数据一般财产权模块、子财产权利模块进行标准化处理。〔63〕此类安排意味着云取证等活动应更加精细化，并且需要符合比例原则，〔64〕

〔61〕 奇点即人工智能具备主体性的临界点。参见赵汀阳：《人工智能提出了什么哲学问题?》，载《文化纵横》2020 年第 1 期。

〔62〕 参见熊丙万：《论数据权利的标准化》，载《中外法学》2023 年第 5 期。

〔63〕 参见熊丙万：《论数据权利的标准化》，载《中外法学》2023 年第 5 期。

〔64〕 参见林钰雄：《刑事诉讼法》（第 11 版，上册），新学林出版股份有限公司 2022 年版，第 320－326 页。

避免对新兴数据权利产生过度干预。

各类取证主体亦需要加强与云计算服务企业等数据处理主体的协调与合作，进行更细致的数据分级处理，依据数据产权的基本结构，判别数据产权的权利归属。在一些利益关涉重大的情形中，侦查机关可要求云服务企业必须建立一定技术机制，便于在取证时对庞杂的数据进行一定区隔，以防止在取证过程中侵犯公有云或混合云中其他用户的数据权利。从更宏观的视野来说，这也是当前数据治理提出的必然要求。〔65〕当然，在这一过程中，对新兴权利的证成应当更加谨慎，否则新兴权利的泛化将危及权利概念本身的重要性。因此，在数据确权得到进一步完善前，亦不能忽视传统的隐私权、财产权、通信自由等典型基本权利的保障，结合数据确权的理论思考，指引取证主体相关活动。在上述规范基础之上，还应当注重为当事人提供相应救济途径，赋予其程序性权利，使其能够对技术决策提出异议。可以考虑从增强当事人知情权入手，增加技术应用说明机制。当事人可要求公开技术应用过程与细节，或者引入相对客观中立的第三方审核机制，辅助当事人检验技术应用场景是否匹配，技术是否具有足够的有效性和可靠性，审查技术运行的具体效果，以此增强司法可接受性。

（二）以维护国家利益为基点完善取证管辖机制

云数据所具有的分割离散性、动态变化性与第三方控制性对跨境执法管辖提出新挑战。我国当前执法管辖权规范仍较保守，为回应美国《云法案》等形成的挑战，可考虑以维护我国国家利益为基点，适当调整完善既有执法管辖权模式，在尊重各国主权的前提下，以《联合国打击网络犯罪公约》的谈判和订立为契机，依据我国国家利益的现实需要，逐步确立更高效率的程序，并通过积极参与谈判，掌握规则制定的主导权，提出云取证国际合作的中国方案。

数据跨境流动和取证在内涵上并不等同，但外延上有重合之处，均关乎数据安全与数据效益。云取证的执法管辖完善机制必须依托数据法律基本规范框架，此为根本前提。依据2022年发布的《中共中央国务院关于构建数据基础制度 更好发挥数据要素作用的意见》（又称“数据二十条”）所传达的精神，需激活数据要素潜能，“积极参与数据跨境流动国际规则制定，探索加入区域性国际数据跨境流动制度安排。推动数据跨境流动双边多边协商，推进建立互利互惠的规则等制度安排。鼓励探索数据跨境流动与合作的新途径新模式”〔66〕。按此规划，我国可逐步探索更加灵活、符合我国国家利益的新型执法管辖模式，进一步思考云计算网络时代管辖与主权之间的关系，基于共同体管辖理论探索弹性管辖机制，通过协调商定国际规则，加强信息交流，提升裁判与执行兼容性，并尊重私主体自治，推动普遍国际规范的确立。〔67〕我国在遵行国际礼让原则的同时，亦需反击其他国家未经允许对我国境内数据进行的远程取证活动。我国可先考虑以近期中德双方共同签署的《关于中德数据跨境流动合作的谅解备忘录》为范本，通过更多的双边合作与接触，初步建立互谅互让的包容性框架，为后续加强云取证等方面的跨境合作奠定良好基础。同时，应进一步细化数据等级分类，根据不同等级的数据选择具体执法管辖模式。

〔65〕 参见沈岿：《数据治理与软法》，载《财经法学》2020年第1期。

〔66〕《中共中央国务院关于构建数据基础制度 更好发挥数据要素作用的意见》，载《人民日报》2022年12月20日，第1版。

〔67〕 参见屈文生：《从治外法权到域外规治——以管辖理论为视角》，载《中国社会科学》2021年第4期。

另一方面，我国可通过建立更完善的协作与监督机制，在此框架内与云服务提供商进行公私合作。这不仅因为云服务提供商是云取证过程中执法管辖权的关键连接节点，还因为缺乏云服务商本身的善意配合，云取证将格外困难，其数据完整性和真实性难以得到保障。尽管我国已通过《网络安全法》第 28 条、《数据安全法》第 35 条规定，结合《刑事诉讼法》第 52 条、第 54 条规定要求网络服务提供商为侦查活动提供技术支持和协助，但是这些规范仍然较为粗疏。当前的云取证实践中，更多由技术工程师等协助调查人员进行实质操作，而侦查人员则越发向监督者的角色转型。实际上，在云计算环境中使用自动化实时取证技术时，整个取证过程对侦查人员而言如同一个技术黑箱，工程师等专业人员才是取证的实质操作者和主导者。如果调查人员故意毁损证据，但却借故程序错误等原因，往往很难予以认定。我国应当防范恶意网络服务提供商等问题，除了通过传统的帮助毁灭、伪造证据罪等进行威慑以外，还可考虑建立黑名单制度，对于在我国境内运营的恶意干扰侦查机关云取证过程的云服务商，可以进行行政或刑事处罚，对于未在我国境内运营的云服务商，则可实施市场禁入等制裁措施。为防范云服务提供商与个别公权力行使人员相勾结，确保取证的有效性和合法性，可考虑建立类似法庭技术调查官取证监督机制，这一机制可由人民检察院负责。通过该机制，由肩负法律监督职责的检察机关对侦查机关的取证活动进行引导和监督，此举也符合检察引导侦查的改革趋势。〔68〕

五、结　语

人创造环境，同样，环境也创造人。〔69〕云计算平台的推广运用，与网络治理空间与治理环境的转型相伴生。从环境整体变化的视角，理解栖居其中的云数据所表现的新特征，并对电子数据取证司法实践展开进一步观察，可拓展认识技术应用与法律活动间互动关系的新视野，而不局限于过往纯粹以技术手段或数据类型发生的变化作为考察视角的方法。云计算平台作为关键数据基础设施，通过大规模应用不断扩容，创立了一种更具开放性的多元化云环境。这一环境同时容纳大数据、区块链、人工智能等多种技术，驱动着取证模式转型，使既有规范体系表现出捉襟见肘的窘态，难以与云取证实际需求相匹配，致使云取证合法性与正当性面临挑战。针对云取证，需予以全流程精细化规范，改变过往以物证而非数据为本位的思维惯性，尝试构建系统性机制进行包容性规制。〔70〕当前，欧美各国正意图推动各自实施的云计算法律规范成为全球标准，〔71〕争夺全球网络治理的话语权。在此背景之下，我国可提出本国云计算环境治理主张，打造云计算法律规范的中国方案。

凡益之道，与时偕行。在科学时代，革新是一种常态，因此必须不断更新思维方式适应新的环境，面对新的科技范式。〔72〕只有顺应时代发展的趋势，适度调整对新技术的治理框架，才能

〔68〕 参见周新：《检察引导侦查的双重检视与改革进路》，载《法律科学（西北政法大学学报）》2020 年第 2 期。

〔69〕 参见〔德〕卡尔·马克思、弗里德里希·恩格斯，中共中央马克思恩格斯列宁斯大林著作编译局编：《马克思恩格斯文集》（第一卷），人民出版社 2009 年版，第 545 页。

〔70〕 参见李训虎：《刑事司法人工智能的包容性规制》，载《中国社会科学》2021 年第 2 期。

〔71〕 See Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 Columbia Law Review 1681 (2018).

〔72〕 参见〔美〕托马斯·库恩：《科学革命的结构》，张卜天译，北京大学出版社 2022 年版，第 58－59 页。

在工具理性与价值理性之间尝试寻得平衡。通过完善法律规范体系以因应技术风险，仍是保障社会进步，并使人类之尊严不至失落的有益之道。

Abstract: The cloud computing environment is characterized by virtualization, real-time, multi-tenancy, elasticity and scalability, and decentralized distribution. Compared with conventional electronic data, the cloud data residing therein exhibits new features such as discrete division, dynamic change, third-party control, etc., which requires cloud forensics to meet the requirements of more stringent real-time, more complex automation, and more effective synergistic requirements. The established norms of forensic measures are still built on top of the traditional environmental forensic experience, upholding the forensic principle of seizing the original storage media as the main focus, extracting electronic data as a supplement, and printing and photographing as the exception, which reflects the regulatory approach based on the physical evidence rather than the data, and attempts to solve the problem of cloud forensics through the addition of the first freezing measures in a single move, coupled with the loss of harmony between the original remote survey and online data extraction in the normative logic, and insufficient regulation of new phenomena such as DFIR and honeypot forensics, leading to practical difficulties. Existing forensic jurisdiction norms favor pure data storage mode, and its cumbersome procedures are difficult to adapt to the high timeliness required by real-time data changes in the process of cloud forensics. In this regard, according to the reality of cloud forensics requirements, and basing on data, should establish the seizure of the original storage media and the extraction of electronic data, printing and photographing as an exception to the forensic principles, to build a systematic technical regulation and procedural constraints program, to safeguard the interests of the state as the basis for improving the forensic jurisdiction mechanism, and to enhance the flexibility of cloud forensics.

Key Words: cloud computing, cloud forensics, automated forensics, electronic data forensics, law enforcement jurisdiction

（责任编辑：李　伟）