Dispute Settlement 争议解决, 2025, 11(8), 119-127
Published Online August 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.118253

Hans汉斯

刑事诉讼电子数据取证的制度困境与法治化路径研究

宋星泽

青岛大学法学院，山东 青岛

收稿日期：2025年7月9日；录用日期：2025年8月2日；发布日期：2025年8月13日

摘　要

我国刑事诉讼中电子数据取证的现实困境与制度完善路径仍需继续深入。电子数据凭借其技术性、复合性、无形性与脆弱性等特征，已成为刑事案件证明的核心载体，但立法滞后与理论薄弱导致三大突出问题：立法体系存在部门规范冲突与公民权利保障缺位，下位法突破《刑事诉讼法》授权范围，且规则过度侧重技术真实性审查而忽视隐私权、财产权等基本权利；侦查行为性质界定模糊，以“网络远程勘验”为代表的措施兼具任意性、强制性与技术性侦查三重属性，引发程序规制失序；“以鉴代侦”现象泛化，鉴定机构实质行使侦查权，规避制度监督与当事人权利保障。对此，应作出以下对策：将电子数据收集纳入《刑事诉讼法》修订框架，以高位法统合细分规则并强化公民权利保障在宪法中的重要性；依据数据隐私层级与干预强度明确侦查行为分类体系；构建专家辅助人制度替代以鉴代侦。

关键词

电子数据，侦查，刑事诉讼法修订，权利保障

Research on Institutional Predicaments and Legal-Institutional Pathways for Electronic Data Forensics in Criminal Proceedings

Xingze Song

School of Law, Qingdao University, Qingdao Shandong

Received: Jul. 9th, 2025; accepted: Aug. 2nd, 2025; published: Aug. 13th, 2025

Abstract

The ongoing challenges and pathways for institutional refinement in electronic data forensics within

文章引用: 宋星泽. 刑事诉讼电子数据取证的制度困境与法治化路径研究[J]. 争议解决, 2025, 11(8): 119-127.
DOI: 10.12677/ds.2025.118253

China's criminal proceedings warrant deeper exploration. Characterized by its technical complexity, composite nature, intangibility, and fragility, electronic data has emerged as a pivotal evidentiary vehicle in criminal cases. Yet legislative lag and theoretical deficiencies have engendered three prominent issues: First, the legislative framework suffers from interdepartmental normative conflicts and inadequate guarantee of citizens' rights, wherein subordinate regulations exceed the authorization scope of the Criminal Procedure Law (CPL) while overemphasizing technical authenticity verification at the expense of fundamental rights such as privacy and property. Second, ambiguous characterization of investigative acts persists, exemplified by measures like "remote online inspection" that simultaneously exhibit discretionary, compulsory, and technical investigative attributes, triggering procedural regulatory disorder. Third, the pervasive phenomenon of "investigation by proxy through forensic authentication" enables forensic institutions to de facto exercise investigatory powers, circumventing accountability mechanisms and litigant rights protections. To address these, the following countermeasures should be implemented: integrate electronic data collection into the CPL revision framework, unifying sectoral rules under higher-level legislation while reinforcing constitutional mandates for rights protections; establish a clear taxonomy of investigative acts based on data privacy tiers and intervention intensity; and develop an expert assistants system to supplant proxy investigation practices.

Keywords

Electronic Data, Criminal Investigation, Criminal Procedure Law Revision, Rights Protections

1. 引言

伴随信息技术与计算机技术的迅猛发展，刑事诉讼领域也迎来众多新形态、新挑战，诉讼证明方式的变革也渐入眼前。在传统证据样态之外，电子数据作为全新的证据种类逐渐占据重要地位，在案件证明过程中起到越来越重要的作用。据学者统计，刑事案件中以电子数据证明案件事实的比例已经超过四分之一[1]。但与此重要地位并行的，却是我国电子数据研究的雏形与现存规范的不足，在实务中广泛运用的电子数据，在理论中却未能理清逻辑与价值取向，不仅未能给予规范指导，更有愈发混乱的迹象。立法的矛盾与纠葛不清为干，其中公民权利保障价值的忽视为根，而对电子数据独特性的忽视则为枝叶，电子数据取证的改革需以三者为抓手，一以贯之。

2. 电子数据理论基础

2.1. 电子数据概念界定

电子数据的概念起源于 20 世纪，1991 年第一届国际计算机调查专家会议提出“计算机证据”的概念，即通过技术手段识别、恢复、提取、保存并形成报告，在法律程序中作为证据使用的以电子形式存储的信息，此后，随着计算机技术发展及相应犯罪的增加，又出现了数字证据、网络证据、虚拟证据、多媒体证据以及电子物证诸多概念。我国学者对电子数据的系统研究起自 2000 年前后，起步较晚，2012 年《刑事诉讼法》中明确列入“电子数据”，正式将其法定化。我国现行对于电子数据的定义为：被作为证据研究的，能够证明案件相关事实的电子文件。电子文件则是指基于电子技术生成的，以数字化形式存在于磁盘等载体的，且内容可与载体分离，并可多次复制到其他载体的文件[2]。

2.2. 电子数据特征解析

电子数据的特征表现为四个方面，分别为技术性、复合性、无形性和脆弱性。

首先，技术性指电子数据的载体特征，承自电子数据的诞生原因，即计算机技术的发展。电子数据依赖于计算机系统的存储，如磁盘、光盘、服务器等，正如传统证据如书证依赖于物理实体的记载，失去载体的承托，电子数据便失去其存在价值。而其独特之处正在于，伴随技术的爆发式发展，载体的多样性也与日俱增，从以往常用而现在少见踪迹的光盘，到如今的移动式硬盘、云存储，不仅形式上承载方式的多样性正在发生量变，在证据的产生、存储、收集、处理、加工、显示等底层运转逻辑中也在发生质的变化，而在这些过程中专业技术因素的占比逐渐增大，对电子数据的处理变得离不开专业技术人员的辅助。

其次，复合性是指电子数据的表现形式多样，传统证据的表现形式多固定化，如视听资料多表现为音频、视频，书证多表现为字据合同等单一形式。而电子数据载体的发展。除了技术性的增长，还有其证据形式的多变，如聊天记录、电子邮件、博客、IP 地址等，与传统证据产生较大差异，同样对办案人员的专业水平与技术水平提出更高要求。

再次，无形性同样源于电子数据的载体固有特征，电子数据没有物理实体，只是以声、光、电等形式存储的电磁信号与二进制编码，只能通过显示设备才能切实感知到。

最后，电子数据还具有脆弱性，电子数据的存储介质决定了其脆弱性，无论是云端存储还是本地存储，电子信息极易被篡改、删除、增添内容，而操作系统的集成化，也使得数据在产生、收集、加工处理过程中极易被误操作而产生变更甚至销毁。在刑事诉讼案件证明过程中，证据的极小瑕疵都可能导致其证明力的降低，而电子数据的脆弱性自然导致其更易产生瑕疵，从而更多地被视为间接证据。

3. 电子数据取证的制度现状

3.1. 国内法律规制演进

我国对电子数据的相关研究起步较晚，自 2000 年前后始有学者对电子数据的概念、特征、取证方法等进行研究。但电子数据的相关内容在 1999 年《合同法》中已有端倪，《合同法》第十一条首次明确了数据电文的法律效力，突破了传统书面证据的限制，将电子数据引入诉讼法的视野内。至 2004 年前，我国并未有专门的电子数据规范，只在一些法律法规中零散着电子数据的相关内容，2004 年出台的《中华人民共和国电子签名法》(以下简称《电子签名法》)正式规定了电子数据规范。《合同法》与《电子签名法》标志我国从法律层面开始接受电子数据的存在，但仍未成为独立的证据类型。2005 年公安部先后发布《计算机犯罪现场勘验与电子数据检查规则》以及《公安部电子数据鉴定规则》。2009 年，最高人民检察院发布《电子数据鉴定程序规则(试行)》。2012 年，《刑事诉讼法》修订，首次将“电子数据”列为法定证据种类，使电子数据正式获得独立地位，解决了电子数据在刑事诉讼中的合法性问题，推动司法实践从“纸质优先”向“技术包容”转型。随后，最高检、最高院、公安部分别于 2014 年和 2016 年发布《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》《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》(下称《电子数据证据规定》)，其中《电子数据证据规定》是我国首个专门针对电子数据的司法解释，系统规范了电子数据的收集、提取、审查标准，明确非法取证的排除规则。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》(下称《取证规则》)，进一步细化侦查机关的取证流程，要求全程记录操作日志，确保电子数据的完整性、真实性、可检验性。2021 年，最高院发布的《关于适用〈中华人民共和国刑事诉讼法〉的解释》(下称《高法解释(2021)》)的第四章第七节专门对电子数据取证作出规定。2022 年，最高法、最高检、公安部三部门联合作出《关于办理信息网络

犯罪案件适用刑事诉讼程序若干问题的意见》，其中第十三条、第十四条以及第十七条至第二十条则规定了办理信息网络案件过程中的电子数据取证问题。由上可见，我国关于电子数据的法律规定不可谓不多，但各部门法律各自为政、相互冲突的情况也同样不可谓不多，尤其电子数据取证主要涉及的公安侦查部门，因没有高位法统领，所以自说自话来保障本部门工作顺畅的情况也不在少数。

3.2. 域外立法经验借鉴

世界各国的刑事诉讼法体系中，无论是发达国家还是发展中国家，亦不论是海洋法国家还是大陆法国家，均将电子数据的收集问题置于重要地位，电子数据的收集已经成为刑事诉讼法中不可或缺、不可忽视的现实问题。简略外国法律建设情况，或对促进国内法律建设起到一定借鉴作用。

美国较早对电子数据的收集进行规范，其主要集中于“信息隐私权”的宪法权利，源于美国联邦宪法修正案第四条：“公民的人身、住宅、文件和财产免受无理搜查和扣押的权利不受侵犯，除非存在合理根据，并以宣誓或代誓宣言作保证，不得签发令状。”宪法修正案第四条在电子数据收集中的进一步确认与强化，由四个阶段的判例完成。首先，在 1967 年的卡兹诉美国案 [1]中被确立为隐私保障条款，凡可能侵犯公民个人隐私合理期待的侦查活动都必须事前获得法院签发的令状；其次，1995 年美国法院的判例规定，在扣押电子存储介质后，如要对电子存储介质内的电子数据进行搜查，同样需要符合特定性的要求，即明确搜查的内容、特征等，且只能包括与案件有关的数据，若在搜查中发现新罪行的证据，则需要重新申请法院签发搜查令。再次，2014 年的赖利诉加利福尼亚州案和美利坚合众国诉沃瑞案的合并判决中，美国联邦最高法院的判决明确，警察无权在逮捕犯人时搜查其手机数据，必须单独获得令状 [2]。最后，2018 年的卡朋特诉美国案中，法院认为，手机基站定位信息能够详细反映个人的行踪轨迹，具有“深刻揭示性”，足以暴露个人的生活习惯、社交关系等私密信息，构成宪法第四修正案保护的隐私利益，美联邦最高法院在此案中创设了“卡朋特标准”，被视为美国司法界对电子数据收集领域的一次革命 [3]。

德国对电子数据收集的规制集中于电讯秘密保护和公民核心隐私保护两方面。1968 年德国《刑事诉讼法典》第一百条 a、第一百条 b 规定了“监听并记录电讯内容”的侦查手段，并以比例原则、及时删除原则等进行限制[3]。2013 年德国国会修改了《电信通讯法》《刑事诉讼法典》及其他法律，其中《刑事诉讼法典》增加了众多条文，对电子数据的收集作出细致规定。2017 年，德国修订《刑事诉讼法典》第一百条的诸多内容，限制侦查权的扩张，对在线搜查等电子数据收集措施作出规定。

其他国家中，意大利《刑事诉讼法典》通过对侦查人员电子数据搜查过程的细致规定来规范侦查权，实现“搜查应严格遵循特定的程序以保障宪法所规定的自由权”这一原则[4]。俄罗斯于 2010 年对《刑事诉讼法典》进行修改，对侦查人员获取电子数据的适用条件、申请和审批程序、期限等作出详细的规定[5]。而乌克兰更是于 2001 年即对其《刑事诉讼法典》第一百八十七条进行修改，对搜查、扣押电子通讯信息作出规定[6]。

4. 电子数据取证的现实困境

4.1. 立法体系冲突与公民权利保障缺位

如上所述，我国现存电子数据的立法，无论是法律层面的规制还是部门作出的司法解释，都不可谓不多，但法律体系的完善不是条文数量的堆砌，只有法律系统的形成才是目的。我国现存冗多的法律解释内容并没有带来逻辑严谨的法律体系，关于电子数据的立法和司法解释比较多，在实践中难以把握平

[1]Katz *v.* U.S., 88 S.Ct.507 (1967).
[2]Charlie Savage, Between the Lines of the Cellphone Privacy Ruling, the New York Times, Jun.25.2014.
[3]Carpenter *v.* U.S., 138 S. Ct. 2206,2206 (2018).

衡关系[7]。如2016年最高检、最高法和公安部出台的《电子数据若干规定》，其中第二条要求人民法院应当围绕真实性、合法性、关联性审查电子数据，但最高院于2021年出台的《高法解释(2021)》却要求围绕电子数据的真实性、完整性、合法性审查电子数据。此外，《刑事诉讼法》虽将电子数据列为法定证据种类，但具体程序规则较多依赖《电子数据规定》《公安电子取证规则》等下位法，导致效力层级断裂。如一些下位法新增的“网络在线提取”“远程勘验”等措施即超出《刑事诉讼法》勘验的范畴，缺乏上位法授权，其合法性存疑。而在跨境取证方面，《国际刑事司法协助法》要求通过司法协助调取境外数据，但《电子数据规定》则允许直接远程调取境内服务器数据，造成司法实践矛盾。另外，不同法规对电子数据的定位也较为混乱，《刑事诉讼法》将电子数据列为独立证据类型，但其他法规如《人民检察院刑事诉讼规则》将其与书证、物证或视听资料等并列，如在“调取、查封、扣押、查询、冻结”章节中，即将电子邮件与传统的邮件、电报并列处理。未充分重视其独立性及特殊性，导致司法实践中标准不一。

在现存立法中，就制定机关方面看，多为侦查机关制定或参与制定，如此便导致刑事侦查中技术性规定较易转化为规范性文件，而对公民权利的保障，对公民个人信息权利的保护则保持忽视的态度[8]。刑事诉讼中，控辩双方在资源与力量上存在客观差异，多数情况下，私人力量很难与代表国家追诉力量的司法机关相抗衡，因此在刑事诉讼法中做出了诸多偏向性规则。而在电子数据收集方面，主体的力量悬殊更为严重，电子数据的收集较传统证据的收集需要更高技术性，一方面，电子数据多存于信息服务提供商的电子硬盘、服务器等介质中，侦查机关较一般个人更易获得；另一方面，虽然当下电子产品前所未有地普及，但掌握专业电子技术的人仍处少数，而侦查机关则配有专业技术人员，对电子数据的取得更为有利。现有制度对电子数据取证程序的设置主要侧重于证据真实性保障的技术规则，较少关注被调查人权利保障的程序规则[9]。如理论基础方面，《电子数据规定》以“提高刑事案件办理质量”为理论基础，而《电子数据取证规则》以“确保电子数据取证质量，提高电子数据取证效率”为理论基础，均忽视了公民权利保障的存在。在具体规则方面，《电子数据规则》第八条规定，电子数据收集原则上采取“一体式收集”模式，即将电子数据及其原始存储介质一起收集，然后运用到诉讼程序中对案件事实进行认定[10]。在第九条和第十条规定，例外情形时才使用“单独提取模式”，即将原始存储介质中的相关电子数据提取出来，转存至其他存储介质中，再以此作为刑事诉讼中认定案件事实的证据。由此可见，“一体式收集”模式在提取与本案有关的电子数据的同时，还侵犯了个人对存储介质的财产权，以及对存储介质中与本案无关的其他数据的权利。此外，关于电子取证中的隐私权保障，《电子数据规则》也仅在第三条中概括性规定了国家专门机关的保密义务，却缺乏具体操作手续，以致缺乏实际落实的可能性。

4.2. 侦查行为性界定模糊与程序规制失序

刑事诉讼诸侦查行为中，根据侦查行为的强制程度和技术特征区分，以侵犯相对人权利的程度和规制的严格程度排序，可分为技术性侦查、强制性侦查和任意性侦查。其中技术性侦查主要指利用现代科技手段获取犯罪证据，侦查对象完全不知情，侵犯性强，因此受到限制，需经严格审批方能实行；而强制性侦查与任意性侦查如其名，前者以强制力为保障，直接侵犯侦查相对人的人身权、财产权，如搜查、扣押、冻结财产等，因此同样需要经过严格审批手续，而后者则无需强制手段，依赖相对人自愿配合，侵犯性弱，因此无需严格审批，只需遵守基本程序规范。为获取同样的证据，三种侦查方式均有各自的作用方式，例如为获取犯罪组织内部情报，既可以通过询问、讯问的任意性侦查措施取得证据，又可以通过搜查、扣押行为人的电脑等强制侦查方式获知，亦可以通过监听、监控等技术侦查措施获取证据。如上所述，刑事诉讼中，按侦查措施可能侵犯公民权利的程度，划分不同的行为性质，并分别设定不同

严格程度的规制机制[8]，同一侦查手段不会被分类为两种以上的侦查类型，尽可能减少对公民权利的侵犯。

在电子数据收集领域，2019 年公安部发布的《取证规则》第七条规定了五种收集、提取电子数据的方法，分别为扣押封存原始存储介质、现场提取电子数据、网络在线提取电子数据、冻结电子数据和调取电子数据。《取证规则》明确规定冻结电子数据需经县级以上公安机关负责人批准，而扣押、封存原始介质则是明显的强制性侦查措施，除此之外，剩余三者均可通过勘验、调取方式获得。其中以网络远程勘验为例，《取证规则》中将其列为一种独立的侦查措施，但在不同情形下，网络远程勘验可能呈现出不同状态，在针对网络上公开的信息进行简单收集的情况下，对个人权利的侵害不甚明显，或可默认认可其收集行为，将其纳入任意性侦查类别，而对个人公开信息的整理，则超出了个人公开其信息所期望的展示范围，亦超出一般个人的浏览范畴，对隐私权的侵犯较为突出，更甚者，如针对个人邮箱内邮件的检查、对非公开信息的搜集等，则均涉及强制性侦查措施，至于持续跟踪网络轨迹、利用技术手段远程监听等方式，则明显属于技术侦查措施。三种侦查方式集于一身，无论将其适用于何种阶段，都面临超出侦查行为必要限制之虞，而如果一律以严格批准程序规制，又对一般性的证据收集场景造成阻碍。一般认为，在立案前的调查阶段，不得使用强制侦查措施，否则会对公民个人权利造成无法约束的持续伤害，《电子数据证据规定》中却并未明确网络远程勘验是否需要批准才能实施，因此其是否能适用于立案前是未明确的，当具有强制侦查措施与技术侦查措施两方面的网络远程侦查适用于立案前时，对公民个人权利的侵害是难以想象的。

4.3. “以鉴代侦”现象泛化与制度监督虚化

随着信息网络技术发展，传统犯罪呈现出网络化的倾向，而网络犯罪也表现出多元化的趋势，使得电子数据成为刑事诉讼中取证的主要对象。此种变化给侦查机关带来两种要求，一是电子数据侦查案件数量的增加，使得以往主要由网安部门负责的电子数据收集活动，逐渐变为普遍性的侦查行为，即要求侦查主体资质一般化。2016 年出台的《电子数据证据规定》即不再要求实施或参与电子数据收集取证的侦查人员具备相关专业知识；二是电子数据收集的技术性要求极高，与传统证据收集的较固定化程式不同，电子数据的取证对象、取证方法等都在不断快速变化中，导致一般侦查人员很难胜任，且基层侦查机关配备的专业技术人员也较为匮乏。侦查主体资质的一般化与侦查行为的专业化导致了侦查机关的困境。《刑事诉讼法》第一百四十六条规定，“为查明案情，需要解决案件中某些专业性问题的时候，应当指派、聘请有专门知识的人进行鉴定”，因此在侦查中出现了两种鉴定方式，一是为解决收集提取证据中的专业性技术问题而进行的鉴定，称为“发现型鉴定”，二是为分析已收集的证据而进行的鉴定，称为“分析型鉴定”。以往，侦查机关适用的司法鉴定，一般是以分析已获取证据为主的“分析型鉴定”，在证据收集阶段，一般不存在侦查机关无法解决的专业性问题。但前述电子数据带来的变化，使得侦查机关在证据收集提取阶段即面临大量专业技术问题，因此以往传统证据收集不常见的“发现型鉴定”在如今变得更为常用。

“发现型鉴定”以鉴代侦，虽在实践中具有一定合理性，但模糊了侦查取证与司法鉴定的边界，导致诸多不利后果，如规避对取证行为的约束、弱化司法鉴定的独立性等[11]。侦查权是宪法和刑事诉讼法赋予的权利，除侦查机关及其具有侦查资格的侦查人员外，任何个人、团体都无权行使，而侦查权的国家权力属性，也要求侦查机关不得随意委托或转让权力。在“以鉴代侦”中，非行使侦查权主体的司法鉴定机关却行使着实质上的侦查权，属于主体不合法，其所收集的证据应被排除，但我国电子数据相关规定以电子数据的真实性、来源的可靠性等为重点，并没有要求排除不合法主体取得的非法证据，故此种非法证据反而会被作为定罪依据使用。此外，如前所述，电子数据收集行为的界定本就模糊，许多侦

查行为如网络远程侦查兼具任意性侦查、强制性侦查和技术性侦查的性质，公安机关及其侦查人员常以任意侦查的形式，行使强制侦查的实质[12]。在相关权利保障本就弱化的现状下，“以鉴代侦”则更是彻底规避掉对侦查主体的限制，侦查对象的权利保障完全被架空。“发现型鉴定”规避掉的不止是侦查对象的权利，更有对侦查机关的制约，将监督对象由侦查机关的侦查人员转到司法鉴定机关的鉴定人员，而鉴定意见属于法定证据种类，通常被推定具有证明力，即使当事人意图推翻鉴定意见，启动补充鉴定，难度也较大[13]。同样，侦查机关的侦查行为要求具有一定开放性，如现场提取证据时要求有见证人在场，而若鉴定人行使实质上的侦查权时，则完全规避掉此种限制。

5. 电子数据取证的法治化路径

5.1. 以《刑事诉讼法》作出引导

如上所述，我国现存关于电子数据的法律及法律解释不可谓不多，各部门均给予高度重视，但总体呈现两个方面特点，即立法矛盾冲突与缺乏公民权利保障。立法矛盾集中于各机关的法律解释等文件之间，尤其体现在侦查机关与审判机关之间的差异，前者实际施行侦查行为，更侧重侦查的便捷、有效，而后者处于中立地位，更注重侦查的合法、合规。业务的差异带来了立场的不同，而若意欲纠正这种差异，必须以高位法统一领导，即在《刑事诉讼法》中对电子数据的收集作出专门、系统性的规范。而后者，即缺乏公民权利保障，同样需由《刑事诉讼法》进行矫治，《刑事诉讼法》又称“小宪法”，公民权利保障是刑事诉讼法的应有之义，有学者认为，自 2012 年我国将“尊重和保障人权”写入刑事诉讼法后，保障公民权利即成为我国《刑事诉讼法》的根本任务[14]，而在各机关制定的关于刑事诉讼法的规范性文件中，较少涉及公民权利保障的问题，其中原因，一是因为在《刑事诉讼法》没有明确规定的情况下，各机关不愿自我设限，同时也无法超出《刑事诉讼法》的范围自行设定侦查权力范围与公民权利范围；二是“基本权利”只能由全国人大及其常委会制定的法律加以限制，其保障同样围绕该层级的法律进行，这是“法律保留原则”的必然要求[15]。因此综上所述，现存法律体系中诸多弊病，只能寄希望于《刑事诉讼法》中作出解决。

将电子数据收集纳入《刑事诉讼法》修改已有较为坚实的基础。在理论层面，理论界对电子数据的收集诸问题，如电子数据证据、电子数据取证程序和电子数据取证中当事人权利保护等问题已进行了较为充分的讨论。在电子数据证据方面，早在 2012 年电子数据成为法定证据种类之前，即有学者对其证据属性作出讨论，更有学者提出“电子数据”这一概念[16]，此后其研究逐渐形成体系，诸多学者对其特征与审查判断规则作出研究，并对现有规则作出反思，认为电子数据法定是理论与实践发展的重要方向。在电子数据取证方面，随着信息电子技术的发展，传统的取证方式已不足以适应现状，因此学者要求《刑事诉讼法》应当对取证制度作出改革，以适应时代要求[17]。而在电子数据个人信息的保护方面，无论是个人信息权的权利性质界定，还是在此之后将《个人信息保护法》的精神融入《刑事诉讼法》之中，都有诸多学者进行了探讨。而在实践领域，电子数据的立法也取得了诸多经验，如 2012 年将电子数据作为证据写入《刑事诉讼法》中，此后诸多法律文件都将其作为法定证据之一予以认可；而收集、提取电子数据方面，虽公民权利保障尚未完善，但具体技术规范已然成熟；至于电子数据的取证规则，其真实性审查规则已经建立起来。综上所述，无论是理论层面还是实践层面，电子数据已经做好了基础铺垫，现如今迫切需要的，便是将其统一整合，纳入《刑事诉讼法》中，做到电子数据取证的法治化。

5.2. 重构侦查行为分类体系

如前所述，侦查行为的性质关系重大，其直接决定采取何种严格的规制措施，并直接影响着相对人的权利在国家强制力前的暴露程度。而电子数据收集中诸多行为的性质模糊，如上文所述的网络远程勘

验，即兼具任意性侦查、强制性侦查与技术性侦查三者于一身，在相关性质未界定的前提下，使得公民权利虚置。有学者认为，网络远程勘验类似于进入被调查者的住宅，应直接划分为强制性侦查措施[18]。也有学者认为，不应简单划分为某一类，而应“以强制性侦查为原则，任意性侦查为例外”[12]。在相关国家已有相关立法的情况下或可以借鉴，如俄罗斯立法认为，勘验对象多数承载着对象合法权益，只有少数未承载个人权益，因此应将勘验作为强制性侦查，并明确作为任意性侦查处理的例外情形[19]。同样，我国《电子数据规定》第一条第二款列举了四种电子数据类型，除第一种外，其余几种均“承载着对象合法权益”，因此或可对国外相关立法进行借鉴，将大部分情形下的网络远程勘验规定为强制性侦查措施，如对相对人的邮件、聊天记录、浏览记录等进行收集，而对少部分的特定情形单独规定为任意性侦查措施，如针对相对人自愿公布的、不涉及隐私的信息进行一般性收集等。扩展到一般性的电子数据收集措施中，同样可以类比网络远程勘验，区分数据的不同隐私层级与干预强度，分别定性，针对公开的数据提取此类低干预强度的行为，如一般性收集社交媒体的公开信息等，可定性为任意性侦查，因其对私权利侵犯相对较弱，无需额外审批程序，以保证侦查行为的顺畅，而针对非公开数据的调取或对公开信息进行进一步技术处理等中等干预强度的行为，如提取加密通信或云端存储等，则定性为强制性侦查更为恰当，最后，若涉及深层数据挖掘、实时监控等高干预强度行为，则必须设置为技术侦查措施，由市级以上公安机关批准实施并限定应用范围。

此外，仅在立法层面作出规定是不够的，还需强化法院对侦查行为性质的实质性审查，有学者认为应改变我国现行强制性侦查仅由县级以上侦查机关批准的现状，改为由具有中立性的司法机关审查批准[20]。但在现行制度未作出改变的前提下，应着重以事后司法审查弥补事前的缺位，即对电子数据的侦查行为性质进行实质审查，以前文所述“网络远程勘验”为例，不仅要明确认定侦查行为属于“网络远程勘验”，更要根据涉及数据的隐私等级和干预强度，清楚认定其属于网络远程勘验中的强制性侦查措施还是任意性侦查措施，而对于违反规定，将具有强制性侦查性质的网络远程勘验作为任意性侦查行为实施的，则应认定其收集的电子数据为非法证据予以排除，实现对电子数据取证的程序性制裁，确保电子数据取证行为性质的明确界定。

5.3. 完善专家辅助人制度

如上所述，电子数据取证因其普遍性、技术性与侦查机关资源的不足，导致电子数据取证中广泛存在“以鉴代侦”现象。但侦查权属于宪法赋予的专属性权力，司法鉴定同样应超然独立于司法机关，基于此，应对此现象作出回应。

基于电子数据收集中现存困境，代替以往“以鉴代侦”中鉴定单位的角色应同时具备两个条件，即形式合法与实质合理，前者指代替者应为侦查机关的人员，具备侦查权背书，后者则指代替者应具备专业技术，能够解决电子数据收集中的技术难题。因此结合两点，可采取专家辅助人制度予以改进，在这一模式中，侦查主体仍为相关侦查人员，专家辅助人只作为辅助性主体，同时专家辅助人的专业技术也能在电子数据取证中起到重要作用。

《电子数据取证规则》第六条和第四十四条规定，公安机关可以指派或聘请专业技术人员或者有专门知识的人，在侦查人员主持下参与电子数据的收集提取或检查。其中所述“专业技术人员”或“有专门知识的人”即此处所称专家辅助人。但现存制度对专家辅助模式的供给不足，或可通过以下几点予以改进：首先，明确专家辅助人在侦查阶段的角色定位。现有侦查程序中，公安机关往往直接与具有电子数据取证能力的第三方公司签订协议，再由其指派专业技术人员参与辅助取证。而第三方公司与其专业技术人员的诉讼角色定位如何却并未明确，或可参照司法鉴定，其同样采取类似的间接委托形式，先委托鉴定机构，再由鉴定机构指派具体的鉴定人，而鉴定人才是真正的鉴定主体。那么在指派专家辅助人

的情况下，也应认定实际指派的专业技术人员，而非第三方公司，才是实质上的诉讼参与人。其次，应明确专家辅助人资格条件，因其主要目的为辅助侦查人员对电子数据取证中的疑难问题做出解决，所以其应具备实质上的电子数据取证专业知识与技术，从而为规范行业运行，降低侦查机关的选择成本，同样应要求其具备形式要件，如颁发的资格证书，或着手建立专家辅助人名册等。最后，应完善专家辅助人参与侦查的程序和实体制度，程序制度如专家辅助人的启用条件、内部审批程序、对专家辅助人的监督指导等，实体制度如专家辅助人的薪酬待遇、人身安全权利等。

6. 结语

电子数据的兴起是信息技术嵌入司法实践的必然结果，其在提升犯罪追诉效能的同时，也对传统刑事诉讼规则与公民权利保障框架提出严峻挑战。当前我国电子数据取证面临立法体系冗杂、侦查行为失范、制度监督虚化等问题，根源在于未理顺技术特性与权利保障的关系。未来改革需要以《刑事诉讼法》修订为统领，通过高位阶立法引领细分规则，明确电子数据收集的程序边界；另以数据隐私层级和干预强度作为标准明确侦查分类，建立梯度化审查机制；以专家辅助人制度破解技术与权力困境，在保障侦查效能的同时坚守权力法定原则。只有将技术理性纳入法治轨道，在追诉犯罪与保障公民权利间寻求动态平衡，才能实现电子数据取证从“技术主导”向“权利本位”的范式转型，回应数字时代司法公正的核心诉求。

参考文献

[1] 邢永杰, 张杨杨. 刑事诉讼中电子数据真实性审查“三步法则” [J]. 中国人民公安大学学报(社会科学版), 2019, 35(4): 75-83.

[2] 蔡武. “电子数据”相关问题研究[EB/OL]. http://www.law-lib.com/lw/lw_view.asp?no=20825, 2025-05-18.

[3] (德)特马斯·魏根特. 德国刑事程序法原理[M]. 江溯, 等, 译. 北京: 中国法制出版社, 2021: 75-78.

[4] 施鹏鹏, 褚侨. 德国刑事诉讼与证据制度专论(第一卷) [M]. 北京: 法律出版社, 2023: 372-373.

[5] 俄罗斯《刑事诉讼法典》第 186-1 条(赵路, 译) [M]//《世界各国刑事诉讼法》编辑委员会, 编译. 世界各国刑事诉讼法·欧洲卷(上). 北京: 检察出版社, 2016: 447.

[6] 乌克兰《刑事诉讼法典》第 187 条、第 187-1 条(张璐, 译) [M]//《世界各国刑事诉讼法》编辑委员会, 编译. 世界各国刑事诉讼法·欧洲卷(中). 北京: 检察出版社, 2016: 1496-1497.

[7] 李春薇. 破除电子数据在司法实践中的运用壁垒[N]. 检察日报, 2019-04-13(3).

[8] 陈永生, 张睿. 电子数据收集应当被纳入本次《刑事诉讼法》修改[J]. 法治研究, 2024(5): 106-118.

[9] 谢登科. 论电子数据收集中的权利保障[J]. 兰州学刊, 2020(12): 33-45.

[10] 刘品新, 谢登科, 裴炜, 等. 电子数据的法治化路径[J]. 数字法治, 2024(4): 6-27.

[11] 陈如超. 以鉴代侦: 电子数据司法鉴定的扩张趋势及其制度回应[J]. 法学研究, 2024, 46(3): 174-190.

[12] 谢登科. 电子数据网络远程勘验规则反思与重构[J]. 中国刑事法杂志, 2020(1): 58-68.

[13] 陈如超. 当事人启动重新鉴定的行动策略——兼论刑事重新鉴定启动机制的合理化改革[J]. 中国司法鉴定, 2013(6): 1-10.

[14] 易延友. 刑事诉讼法规则原理应用[M]. 北京: 法律出版社, 2019: 82-83.

[15] 张翔. 基本权利限制法律保留的中国方案[J]. 法律科学(西北政法大学学报), 2023, 41(6): 80-90.

[16] 周晓燕. 电子数据检察实务研究[J]. 中国刑事法杂志, 2011(1): 58-65.

[17] 冯俊伟. 数字时代背景下刑事取证制度的困境与回应[J]. 北方法学, 2024, 18(1): 20-32.

[18] 奚玮. 我国电子数据证据制度的若干反思[J]. 中国刑事法杂志, 2020(6): 135-154.

[19] (俄)K·Φ·古岑科, 主编. 俄罗斯刑事诉讼教程[M]. 黄道秀, 等, 译. 北京: 中国人民公安大学出版社, 2007: 221.

[20] 龙宗智. 强制侦查司法审查制度的完善[J]. 中国法学, 2011(6): 43-50.