

# 我国电子数据鉴真规则的反思和重构

## ——评公安部《公安机关办理刑事案件电子数据取证规则》

刘 芸 志

(华东政法大学 刑事法学院,上海 201620)

**摘 要:**2019 年公安部发布了《公安机关办理刑事案件电子数据取证规则》,细化了电子取证的相关程序,但仍存在数据提取与侦查的关系不清晰、原始存储介质与电子数据的鉴真相混、网络远程勘验侵犯个人隐私、审查机制倚重笔录类证据、跨境取证受阻等问题。对此,应加强电子数据取证与刑事诉讼侦查规定的衔接、划分三个层面的鉴真体系、明确远程勘验的性质、探索直接言词原则、加强国际间电子数据取证交流与合作,从而完善电子数据的鉴真规则。

**关键词:**电子数据;真实性;远程勘验;直接言词

**中图分类号:**D925.2   **文献标志码:**A   **文章编号:**1673-8039(2021)02-0080-06

随着信息技术的发展,电子数据在我国司法裁判中的地位日益提高,利用网络的新型犯罪数量不断增多。根据最高人民检察院公布的全国检察机关办案数据可知,2020 年 1 至 6 月,受新冠肺炎疫情影响,利用电信网络手段实施犯罪的数量逐渐上升<sup>①</sup>。因而如何完善电子数据取证规则,有效打击网络犯罪是当前司法工作的重点之一。

2012 年修改的《刑事诉讼法》正式将“电子数据”与视听资料并列作为一种新的证据类型之后,电子数据因其独有的高科技性、无形性、脆弱性等特点<sup>[1]102</sup>,在司法实践中陆续产生了许多新的问题。为此,司法机关一直努力通过释法、司法工作来完善电子数据规则,例如:2010 年“两高三部”发布的《关于办理死刑案件审查判断证据若干问题的规定》(以下简称“《死刑案件证据规定》”)初步构建了电子数据的鉴真规则,提出了审查电子数据来源、流转过程的要求。2013 年,最高人民法院颁行的《关于适用〈中华人民共和国刑事诉讼法〉的解释》,在《死刑案件证据规定》的基础

上,进一步强调审查电子数据的取证情况,并增加瑕疵电子数据的排除规定。2016 年,“两高一部”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》(以下简称“2016 年《电子数据规定》”),对电子数据的鉴真规则进行实质性改进,包括新增完整性审查、丰富关联性内涵、确立“独特性确认”(ready identification)<sup>②</sup>的鉴真方法、明确鉴真不能的有限排除规则<sup>[2]</sup>。2019 年公安部颁发了《公安机关办理刑事案件电子数据取证规则》(以下简称“2019 年《电子数据取证规则》”),着重强调电子取证的程序性问题,包括列举电子取证方式、完善笔录和文书规则、增设特定人员的出庭作证义务。此外,该规则还增强了私权保护意识,并与国际数据取证规则进一步衔接。尽管上述一系列规则对我国电子数据的取证规范性和证据真实性方面有了相对细化的规定,但仍存在电子数据的取证方法与刑法侦查规则衔接不善、原始存储介质的鉴真与电子数据本身的鉴真相混同、远程勘验境内计算机信息系统可能侵犯个人隐私权、笔录类证据无法达到“保管

收稿日期:2020-12-29

基金项目:国家社会科学基金重点项目“大数据侦查的程序控制与证据适用研究”(19AZD024)

作者简介:刘芸志(1997—),女,山东莱阳人,华东政法大学刑事法学院硕士研究生。

①最高检报告:受新冠肺炎疫情影响,利用电信网络手段实施犯罪的数量同比上升,起诉利用电信网络实施的犯罪 52,473 人,占起诉数的 7.8%,同比增加 3.7 个百分点。

②美国证据法上的一种鉴真方法,用于对特定物的鉴真,证人当庭陈述当初看到物证有哪些特征,并说明法庭上的该项物证与原来的物证具有相似的地方。

链条的证明”(chain of custody)标准、跨境电子数据的取证效率低等问题<sup>[3]</sup>。有鉴于此,本文拟对电子数据规则的相关理论和实践展开研究,把握鉴真实质,剖析现存问题,从而探究我国电子数据规则完善的关键。

## 一、鉴真的性质

2016年快播公司涉嫌传播淫秽物品牟利罪一案(以下简称“快播案”)在北京市海淀区人民法院审理,该案引发了广泛的社会关注。本案中,控辩双方针对关键证据的证据能力和证明力展开激烈抗辩,即行政机关在快播公司查获的四台服务器及其中的21251个淫秽视频。但行政执法机关、侦查机关对上述两项关键证据进行提取和保管时,存在诸多违法行为,例如行政执法机关查封服务器和公安机关调取服务器时均“未对物证特征进行固定”、保管情况不明、移交手续不合法等等。这使得在取证环节上,证据来源的可靠性、与快播公司关联性存在疑问;在证据保管环节上,服务器存在被掉包、淫秽视频存在被污染的可能。因而一审法院对存储淫秽视频的服务器是否是原始扣押件、是否受快播公司实际控制和使用产生了怀疑,但受制于取证机关的程序性违法事由对脆弱的电子数据造成不可回转性毁坏,司法人员也难以再对本案电子数据的来源和流转情况进行有效审查,最终仅能通过司法鉴定意见作为补强证据来明确上述核心争议。

陈瑞华教授将上述取证、保管环节的争议审查概括为证据鉴真,主要是指在法庭上出示、宣读、播放的某一实物证据,应与举证方所声称的实物证据一致;并且法庭上出示宣读、播放的实物证据内容能反映其本来面目,是实物证据的真实记录”<sup>[4]</sup>。可见,证据鉴真主要指向证据提取和保管两个环节,快播案所反映的争议和引发的关注也正是我国电子证据鉴真规则不完善的问题。鉴真规则起源于英美证据法,美国《联邦证据规则》规定,满足鉴真的要求是实物证据具备可采性的先决条件,证据提出者需要提供充足的证据来证明所出示的实物证据与其所主张的实物证据是同一的<sup>①</sup>。在美国,所有出示到法庭上的证据首先被推定为不真实,只有符合鉴真规则的实物证据才能作为陪审团认定案件事实的依据。此时,鉴真作为一种初步筛查机制可以起到一定的证据过滤作用,需要提出主张的一方提供足以体现证据

真实性的基础性证据,否则该证据将无法成为认定案件事实和定罪量刑的依据。我国证据法学者张保生教授认为鉴真是对“物证、书证等展示性证据与案件特定事实之间联系的真实性的证明”<sup>[5]200</sup>。

## 二、鉴真规则现存问题

(一)电子数据的取证方法与刑事诉讼侦查规定的衔接不明

由于电子数据的技术性和专业性,对此类证据的取证规则除《刑事诉讼法》的规定外,还添置了许多特殊的规则,但电子数据特有的取证规则仍应遵循《刑事诉讼法》侦查和证据章节的大框架,并注意与《刑事诉讼法》侦查规定的协调。2019年《电子数据规则》加强了与《刑事诉讼法》衔接,在2016年《电子数据规定》遵守法定程序的一般性要求和使用了扣押、勘验等刑法概念及取证手段的基础上<sup>[6]</sup>,还统一了电子数据取证规范,合并了提取电子数据和逮捕、搜查、行政执法笔录。但是,在取证方式上,该规则仍未与《刑事诉讼法》侦查取证的规范体系良好协调。2019年《电子数据规则》第6条规定,收集、提取电子数据应当由2名以上侦查人员进行。《刑事诉讼法》仅要求在讯问犯罪嫌疑人时侦查人员不得少于两人。此外,2019年《电子数据规则》强调收集提取电子数据要进行拍照打印、录音录像、见证人见证、制作笔录等要求,但《刑事诉讼法》第二章所规定的侦查方法,并无上述制度要求。再次,2016年《电子数据规定》第24条中审查电子数据合法性时,并没有关于“收集、提取的电子数据是否符合《刑事诉讼法》的要求”。可见,目前电子数据的取证和审查方式相对独立于《刑事诉讼法》的侦查体系,其特殊性容易引发具体适用和执行中的争议。

(二)原始存储介质与电子数据本身的鉴真相混同

根据目前主流证据法理论,电子数据的真实性包含电子数据载体的真实性和电子数据记录信息的真实性。我国法律规范未区分电子数据本身和其载体的鉴真,而是将对数据内容的鉴真包含

<sup>①</sup>Fed. R. Evid. 901(a): In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is, 2020.

进对存储介质的鉴真之中。而根据我国电子数据的规定,扣押、封存原始存储介质为原则,提取电子数据为例外。这说明电子数据具备可以与原始存储数据相分离的特性,若只对电子数据载体进行鉴真并不符合实践需要,并且电子数据的修改也并不一定会影响电子数据载体;同样,电子数据载体的真实性也无法确保电子数据的真实性。以快播案为例,如果预先没有明确四台服务器中的硬盘这一原始存储介质的真实性,而直接审查服务器内淫秽视频的真实性,则可能导致电子数据的审查缺乏依据,即便之后通过鉴定对淫秽物品进行补强,该鉴定意见仍无法确定检材的原始性,服务器中数据仍存在被污染的可能。一方面这是办案人员没有遵循取证规则所致,另一方面也与我国电子数据鉴真对象的混同有关。现行电子数据审查规则不区分存储介质和电子数据本身,未明确审查顺序,这将导致法官在审理电子数据时缺少清晰的思路和准确的判断。

(三)网络远程勘验的法律定位不明导致对私权的侵害

根据《人民检察院刑事诉讼规则》第169条的规定,“勘验”属于“任意性侦查措施”,那么以计算机系统为适用对象的网络远程勘验作为“勘验”的下位概念也应被定性为任意性侦查措施,受到较少的程序规制。但根据2016年《电子数据规定》第9条第3款可知,采取技术侦查措施的远程勘验需要经过预先的批准,不采取技术侦查措施的网络远程勘验则应遵循必要性原则,只有在其他有效侦查手段无法满足取证要求的情况下,才可进行。照此逻辑,无论是否采取技术侦查措施的远程勘验都要满足一定条件和必要的手续,与搜查、扣押等强制性措施相比,同样具有权利干涉性和侵害性,应当理解为强制性侦查措施。因此2016年《电子数据规定》与《人民检察院刑事诉讼规则》在网络远程勘验的性质界定上实则相矛盾。关于网络远程勘验与《刑事诉讼法》中的搜查和技术侦查之间的关系,缺少明确的解释。但网络远程勘验与公民个人信息密切相关,对此类问题规范的粗疏,容易导致侵犯公民个人隐私权的情况出现。因此如何在远程勘验计算机信息系统提取有关犯罪数据的同时,还保障被调查人合理隐私利益是我国在执法与司法领域上所面临的困境。

(四)直言词原则的缺少导致法官对笔录

类证据的倚重

目前,我国刑事诉讼中对电子数据的来源、收集、保管过程进行证明的方法较为单一,仅依赖一系列勘验、检查笔录和搜查笔录等书面记载来验证。有学者认为,这样的鉴真带有形式化的验证性质,难以对证据的真实性和同一性作出实质审查和确认<sup>[4]</sup>。虽然2019年《电子数据规则》增加了公安机关指定进行数据检验并出具报告人员的出庭作证义务,但仍未改变我国电子数据以笔录为中心的审理现状。这是单方面的书面化鉴真模式的先天不足所造成的。立法规定,相关电子数据的收集、提取、搜查、扣押过程中应有见证人予以见证,但电子数据的专业性和非直观性,使得即便侦查人员对该数据进行篡改,也不容易被非专业的见证人所准确识别。此外,见证人进行见证的场合仅存在于电子数据的搜查扣押过程中,在后续的保管、鉴定、出示环节,见证人不再进对电子数据的流转进行见证和监督,也就无法全程、有效的参与电子数据的收集和流转中。最后,笔录类证据系侦查人员单方制作,特别是在关键数据的收集和保管问题上,如果没有相关证人出庭作证接受盘问与对质,对证据链条的完整性上作出合理的解释,电子数据的真实性和同一性就不能得到有力的证明,同时剥夺了被告人一方的质证权,法官也同样无法对电子数据进行有效的审查。

(五)刑事跨境数据取证效率有待提高

在2016年《电子数据规定》出台后,有关我国单方面授权侦查机关对境外电子数据在线提取、远程勘验的规则在国际层面引发了较大的关注,一些国家认为该规则与国际法规则存在冲突,侵犯其国家网络空间主权<sup>①</sup>,容易引发国际争端。继而2019年《电子数据规则》将对境外电子数据在线提取、远程勘验限于“公开发布的电子数据”,对境内远程计算机信息系统上的电子数据在线提取、远程勘验则不受此限制。对此,有学者批判,这样的境内外远程勘验的差别化待遇会导致电子数据收集中权利保障不平等和制度运行失灵<sup>[7]</sup>。

根据现行规则,境外电子数据取证方式分为

①网络空间主权原则是一项随着全球信息化快速发展而出现和发展起来的原则。网络空间是人们通过运用信息通讯技术模拟现实产生的数字化空间,有观点认为其属于国家主权在网络空间的自然延伸。因其虚拟性、无形性和全球性等特征,国际社会对国家主权是否同样适用于网络空间存在争议。



两类:一类是针对境外公开发布的电子数据,侦查人员将浏览服务器连接境外公开的网页,以截图、拍照、录像等方式固定和提取网页数据。第二类是针对境外非公开发布的电子数据,首先可以通过国际条约、刑事司法协助等渠道调取证据。其次可根据案件需要,在必要时对远程计算机信息系统进行网络远程勘验。通过电子数据持有人、网络服务提供者提供的账号、密码等信息获得远程计算机信息系统的访问权限,取得境外服务器数据。亦或经过严格的批准手续后,对境外电子数据采取技术侦查措施的远程勘验。但传统的司法协助具有层层审批时间长;取证周期长、难度大的弊端<sup>[8]</sup>。其他的跨境电子证据取证制度仍属于单边取证,未获得电子数据所在国的同意,可能会引发侵犯他国数据主权的国际纠纷。如何确保电子取证的合法性和提高跨境电子取证效率,是现存的难题。

### 三、电子数据鉴真规则的完善

#### (一)加强与刑诉法侦查程序规范的衔接

电子数据相关规则首先应当与《刑事诉讼法》基本规则进行衔接,在确保普通侦查人员和司法人员具备必要的技术能力基础上,再进一步强调电子数据取证、审查主体特有的素质和能力要求。关于取证主体的规范,可结合电子数据的技术性、新颖性的特点,重置侦查人员资格和数量。关于在线提取和网络勘验等高技术取证方式,非专业技术人员的操作可能会降低案件侦办效率和浪费司法资源,更甚之会造成数据证据的破坏。因而保证一定数量的专业素质水平的侦查人员参与到电子数据的收集、提取工作中,增强证据提取的专业度,保障证据合法性。此外,不再局限于“两名以上的侦查人员”,允许侦查人员与专业人员配合取证。电子数据自身的特征更强调取证人员的专业能力,但实践中的大多数侦查人员、司法审查人员不具有该技术能力,所以对电子数据取证主体人数的要求和司法审查的技术标准固然可保障取证过程合法性和证据审查的合理性,却无法适应侦查的现实需要和司法实践情况。因而可参照2019年《电子数据规则》第44条的规定,积极将专业的技术人员纳入到获取数据的司法活动中,加强证据来源的可信性和合法性<sup>[9]</sup>。最后,应当贯彻“下位法不得突破上位法”的法治原则,坚持在《刑事诉讼法》的框架内理解和执行

电子数据规定<sup>[10]</sup>,确保证据审查判断标准的集中统一,从而促进技术侦查的妥善运用。

#### (二)设立三层面的电子数据鉴真规则并明确审查判断顺序

有学者将鉴真的外延涵盖了三个方面:电子数据载体的鉴真,即针对电子数据载体的存储介质,确认其来源和流转载体的原始性、同一性、完整性;电子数据的鉴真,即针对电子数据本身,确认其来源和流转载体的原始性、同一性、完整性;电子数据内容的鉴真,即针对电子数据所包含的内容是否可以与其他证据相互印证来证明案件事实等问题。笔者认为应区分电子数据载体和电子数据本身内容的真实性,以上述三个层面来重构电子数据鉴真规则,并明确审查顺序。首先,在对电子数据载体和电子数据审查时应当关注其来源、流转载体中原始性、同一性、完整性。原始性是指诉讼过程中电子数据载体、电子数据保持原始状态;同一性是指在来源和流转各个环节,电子数据保持不变;完整性是指收集、提取的电子数据和查封、扣押的电子数据载体完整,不存在被修改、破坏的情况。同一性和完整性存在一定程度的重合,例如拍照、封存、完整性校验、数字签名和证书等方式在确保完整性的同时也可确保同一性。在对电子数据内容审查时应关注其内容的同一性,即判断证据间能否相互印证。其次,明确好三层面的审查顺序,分别审查电子数据载体真实性、电子数据真实性、电子数据内容关联性。这是因为电子数据载体的真实性是电子数据真实性的外部保障,电子数据的真实性是电子数据内容真实性的技术基础,电子数据内容的真实性则是证据能力之关联性要求<sup>[11]</sup>。由此电子数据鉴真规则成体系化、系统化运用在司法程序中。

#### (三)明确网络远程勘验的法律定位保障公民合理隐私利益

2016年《电子数据规定》和2019年《电子数据规则》初步确立了网络远程勘验,但未明确对该项规则的法律定位,易造成实践中侵犯个人隐私权的情况。例如远程勘验时侵入被调查人电脑阅览其个人通话记录、商业秘密等信息。在我国,个人隐私权的含义相对难以明确,《关于加强网络信息保护的决定》将个人信息分为能够识别公民个人身份的信息和涉及个人隐私的信息,并以信息是否具有可识别性作为个人信息的认定标准,主要包括公民的姓名、年龄、身份证号、生日

期、家庭住址、财产情况、行踪轨迹、个人生物识别信息等。笔者认为隐私权应当属于个人信息权的一部分,主要表现为不愿被他人知悉的个人私密信息。根据2016年《电子数据规定》第1条第2款对电子数据的分类,除第一项所列的公开发布的信息以及第三项中能识别公民个人身份的信息,如用户注册信息、身份认证信息。其他款项所列电子数据都包含了个人合理隐私利益。因此应将电子数据的远程勘验定义为强制性侦查,比照搜查制度予以规制。初查时不允许侦查机关进行网络远程勘验,立案后的侦查则可借鉴域外电子数据取证规则,例如美国明确搜查措施的外延、限制数据搜查的范围、要求数据搜查的许可以及非法证据的排除等各方面的规定;德国明确提取数据情形、设立电子数据监督委员会的规定<sup>①</sup>,由此达到惩罚犯罪和保障公民个人隐私权的恰当平衡。

(四)扩大电子数据出庭作证人员的范围以逐步确立直接言词原则

2019年《电子数据规则》规定了不同数据取证行为的笔录和文书规则,强调了录音录像制度。但笔录类证据的丰富和相关人员签名盖章的完备,并不意味着形成了完整的证据保管链条。笔录类证据仅是相关人员侦查、见证、保管活动的记载,不足以成为有效的审查机制。要确保电子数据的真实性和构建有效的审查机制,还应在证据保管链过程中的参与者出庭作证为审查规则的保障。当一方对电子数据的真实性有疑问时,法庭应允许相关人员出庭作证,接受对方盘问和法官质询,由此法官在保障控辩双方质证权的同时,也对电子数据的真实性进行有效的审查,形成内心确认。但不可忽视的是,我国目前仍存在证人出庭作证难的问题,若大范围地适用证人证言的保管链鉴真方式,可能会影响诉讼进程,浪费必要的司法资源。因此,可初步探索在适用笔录类证据鉴真为主的基础上,选择性地适用证人证言保管链鉴真的方式,使证人证言与书面化的证据保管记录体系相配合。笔者建议,出现以下情形时应由证据保管链过程中的参与者出庭作证:第一,被告人及辩护人对电子数据的同一性和真实性提出异议,有合理依据或能初步证明电子数据保管链断裂或存有其他瑕疵的;第二,在一方对电子数据保管链提出异议后,提出证据一方无法对其进行充分地解释和说明的;第三,法官对电子数据的

保管链条存有疑问,认为相关人员出庭作出说明有必要的其他情形。

(五)构建区域内合作的跨境电子证据取证模式

近年来,跨境网络犯罪数量不断提高,公安机关在对大量境外电子数据取证时面临着较大困难。2019年的联合国网络犯罪政府间专家组第五次会议中,参会各国的有关人士达成一致共识,未来要有效应对网络犯罪,应着重跨境数据的取证。为了解决跨境电子证据取证难的问题,我国可探索构建一定区域内电子数据取证的深度合作。有学者提出可在“一带一路”国家开展,通过签订打击网络违法犯罪的国与国间的双边协定,搭建政府间执法合作平台,来推动构建新网络犯罪公约<sup>[12]</sup>。有学者表示我国仍可以将跨境强制侦查措施保留在数据收集中,通过遵循国际法上的对等原则和履行对相对国家的及时告知义务来保障取证的合法和对他国数据主权的尊重<sup>[13]</sup>。笔者认为,我们可借鉴欧盟委员会建立的“欧洲数据提交令”和“欧洲数据保存令”制度。欧洲数据提交令和保存令赋予各成员国直接强制欧盟境内的服务提供者提供电子数据并对特定数据予以保存的权利,并不论相应数据到底是否存储于欧盟境内<sup>[14]</sup>。有鉴于此,我国同样可以构建区域间的电子证据刑事司法协作,加强电子数据信息在各国之间的频繁流动,加强各国电子取证司法的协作性,提高取证效率和案件侦办效率。此外,还应当建立跨境电子证据的监督机制,通过检察机关的介入来监督跨境电子数据的收集、提取、固定、保存等问题,由此解决了跨境取证难的问题,并有力打击了跨境网络犯罪。

## 参考文献:

- [1] 叶青. 诉讼证据法学(第二版)[M]. 北京:北京大学出版社,2013.
- [2] 刘品新. 电子证据的鉴真问题:基于快播案的反思[J]. 中外法学,2017(1).
- [3] 裴炜. 简评2019年《公安机关办理刑事案件电子

<sup>①</sup>德国《刑事诉讼法典》规定只有重大犯罪时才可以调取包含隐私内容的通话内容、短信内容以及电子邮件内容等电子数据。此外德国通过立法设立了个人信息保护委员会,允许个人信息保护委员会对收集、利用公民个人信息的行为进行全方位的监督。对于部分性质特殊的国家政府部门的内部监督,可在其部门内部设立数据保护官的职位,并赋予数据保护官监督部门内部的收集、利用公民个人信息的权利。

数据取证规则》——兼与 2016 年“两高一部”《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》比较[EB/OL]. (2019-01-10) [2020-07-29]. <https://www.secrss.com/articles/7733>.

[4] 陈瑞华. 实物证据的鉴真问题[J]. 法学研究, 2011(5).

[5] 张保生. 证据法学[M]. 北京: 中国政法大学出版社, 2009.

[6] 龙宗智. 寻求有效取证与保证权利的平衡——评“两高一部”电子数据证据规定[J]. 法学, 2016(11).

[7] 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).

[8] 叶媛博. 我国跨境电子取证制度的现实考察与完善路径[J]. 河北法学, 2019(11).

[9] 王鹤. 证据合法性的实践隐忧与规制思考——评“两高一部”电子数据证据规定[J]. 产业与科技论坛, 2019(4).

[10] 龙宗智. 寻求有效取证与保证权利的平衡——评“两高一部”电子数据证据规定[J]. 法学, 2016(11).

[11] 褚福民. 电子证据真实性的三个层面——以刑事诉讼为例的分析[J]. 法学研究, 2018(4).

[12] 辛素. “一带一路”电子取证刑事司法协作问题研究[J]. 北京警察学院学报, 2018(6).

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

[14] 梁坤. 欧盟跨境快捷电子取证制度的发展动向及其启示[J]. 中国人民公安大学学报(社会科学版), 2019(1).

## Reflection and Reconstruction of Authentication Rules for Electronic Data in China: Comment on the Ministry of Public Security's *The Rules for Electronic Data Collection of Criminal Cases of Public Security Organs*

LIU Yunzhi

(School of Criminal Law, East China University of Political Science And Law, Shanghai 201620, China)

**Abstract:** In 2019, the Ministry of Public Security issued *The Rules for Electronic Data Collection of Criminal Cases of Public Security Organs*, detailing the related procedures of electronic evidence collection. However, there are still some problems, such as unclear relationship between data extraction and investigation, confusion between original storage medium and electronic data authentication, infringement of personal privacy by network remote inspection, dependence of review mechanism on transcript evidence, and obstruction of cross-border evidence collection. Therefore, we should strengthen the connection between electronic data collection and criminal procedure investigation regulations, divide the three levels of authentication system, clarify the nature of remote inspection, explore the principle of direct speech, and strengthen the international exchange and cooperation of electronic data collection, so as to improve the rules of electronic data authentication.

**Key words:** electronic data; authenticity; remote inspection; direct speech

(责任编辑 陇 右)