

电子数据的取证主体:合法性与合技术性之间

谢登科

内容提要:电子数据作为现代网络信息社会的新兴证据种类,具有很高的科技含量,这就对其取证主体的技术资质提出了较高要求。在电子数据“一体收集”和“单独提取”两种取证模式下,对取证主体技术资质的要求也不完全相同。实践中多数侦查人员并不具备电子数据收集的技术知识,他们通常依靠侦查机关以外的相关技术人员收集电子数据,由此产生了取证权限合法性和技术资质合法性相互冲突的悖论。取证主体的取证权限和技术资质会对电子数据的证据能力产生不同影响。取证权限的缺失可能会侵害被调查对象的合法权利,技术资质的缺失则会减损电子数据的真实性。因此,有必要针对具体案件类型、电子数据种类等因素建立科学的电子数据取证主体制度,以防范取证主体不合法而损害电子数据证据能力。

关键词:电子数据 取证主体 证据能力 有专门知识的人

谢登科,吉林大学法学院副教授。

一 问题与路径

电子数据作为现代网络信息社会的新兴证据种类和“证据之王”,^[1]本身具有很高的科学技术含量。电子数据的技术性对其举证、质证和认证提出了较高要求,也对电子数据取证主体的技术资质提出了较高要求。如果电子数据在刑事诉讼的使用中缺乏相应的技术保障措施,则可能对其证据能力产生消极影响,侵害电子数据所承载的权利,阻碍对案件事实的正确认定。我国《刑事诉讼法》虽然将电子数据列为法定证据种类之一,但对其举证、质证和认证等诉讼活动并未做明确规定。对电子数据的取证也没有做出特殊规定,而是将其归于物证、书证等传统实物证据的提取之中。

最高人民法院2012年11月出台《关于适用〈中华人民共和国刑事诉讼法〉的解释》

[1] 参见刘品新:《电子证据的基础理论》,《国家检察官学院学报》2017年第1期,第151-159页。

(以下简称《刑诉法解释》)对电子数据的审查认定予以规定。其中第 93 条第 1 款第 1 项要求对电子数据进行审查时,需审查“提取、复制电子数据是否由二人以上进行”,但对电子数据收集主体的技术资质则未作限定。该款第 2 项要求审查电子数据的“收集程序、方式是否符合法律及有关技术规范”。电子数据收集程序和方式的合技术性,必然要求收集主体具有相应技术知识,否则很难保证其收集程序的合技术性。因此,《刑诉法解释》虽未明确对电子数据收集主体的技术资质做出要求,但对收集程序合技术性的审查规定,就已暗含了对取证主体技术资质的要求。

最高人民法院、最高人民检察院和公安部 2014 年 5 月出台《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》(以下简称《网络犯罪刑事诉讼程序意见》)第 13 条规定:“收集、提取电子数据,应当由二名以上具备相关专业知识的侦查人员进行。”该条对电子数据的收集主体做出了强制性规定:第一,电子数据的收集、提取须由两名以上侦查人员进行。当然,这里对电子数据的理解应予以适当限定,即解释为作为控方证据的电子数据。^[2] 第二,收集电子数据的侦查人员应具有相关专业知 识。该规定实际上是将电子数据收集主体的合技术性要求上升为合法性要求了。如果电子数据收集主体不具备相应专业知识,就意味着违反该条强制性规定,证据收集主体不合法,就可能对电子数据的证据能力产生消极影响。

最高人民法院、最高人民检察院和公安部 2016 年 9 月出台《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》)第 7 条规定:“收集、提取电子数据,应当由二名以上侦查人员进行。取证方法应当符合相关技术标准。”该条对电子数据收集主体合技术性要求,采取了类似于《刑诉法解释》的规定模式,即并不明确对其收集主体的技术资质进行限定。在《电子数据规定》起草中,起草者曾对电子数据取证主体采取了和《网络犯罪刑事诉讼程序意见》第 13 条完全相同的规定,但后期考虑到“具备相关专业知 识”的标准模糊、不易判断,且只要电子数据取证过程符合法定程序和相关技术规范,就能保证其真实性和完整性,故对侦查人员是否具备专业知识未做硬性要求。^[3] 然而,值得注意的是,取证主体具有相关专业知 识是取证过程符合相关技术标准的前提条件,否则就无法保证取证过程符合技术标准,因此,《电子数据规定》要求取证方法须符合相应技术标准,实际上仍然是将取证主体的技术性要求纳入取证程序或取证方法的技术性要求当中了。

有学者认为电子数据取证主体呈现出多元化特征,取证主体不局限于某些特定人员,无论是侦查人员、司法人员、行政执法人员、当事人及其律师,还是网络运营商、相关技术

[2] 证据可以分控方证据和辩方证据。由于控方证据的收集多是国家专门机关工作人员,他们有权采取各种强制性调查方式收集证据,为防止证据收集过程中的权力滥用,需要对控方证据的收集程序和方式予以限定。而辩方证据的收集主体多是被追诉人及其辩护人、法定代理人、近亲属等私人主体,其并不享有采取强制性调查方式收集证据的权力,对于辩护证据的收集程序和方式通常不做明确限定。故本文在未做明确说明的情况下所称电子数据,都是作为控方证据的电子数据。

[3] 参见万春等:《〈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〉理解与适用》,《人民检察》2017 年第 1 期,第 49-59 页。

专家等,都可在电子数据取证领域一试身手。^[4] 如果将上述观点作为对电子数据取证主体实践图景的描述,无疑具有合理性。但是,这并不意味着法律对电子数据的取证主体可不加限定。电子数据取证有可能对被调查对象的财产权、信息权、隐私权等基本权利造成侵害,若对收集主体不做限定,就可能导致电子数据收集中权利侵害的泛滥。另外,作为证明案件事实的证据材料,电子数据具有技术性强的特征,若对收集主体不做限定,也可能因缺乏相应专业知识导致对电子数据的破坏甚至毁灭。因此对电子数据取证主体不做限定,既不利于电子数据收集中的权利保障,也可能阻碍对案件事实的查明,故有必要在法律层面对电子数据的取证主体予以适当限定。电子数据收集主体的合法性通常包括两个要求:取证权限的合法性和技术资质的合法性。由于侦查权只能由公安机关、国家安全部门等国家专门机关的侦查人员行使,只有这些主体才享有搜查、扣押、查封、勘验等侦查权限,因此,电子数据的收集主体首先应是侦查人员。电子数据作为现代网络信息技术的产物,^[5]其收集过程和取证方式须遵循相应技术标准,确保电子数据免于因取证主体缺乏相应专业技术知识而遭到人为破坏。基于上述两个方面的要求,电子数据收集主体的理想状态就是收集电子数据的侦查人员具有相应专业知识,这种专业知识能有效满足电子数据收集的技术性要求。但是,在司法实践中,电子数据的收集主体经常会出现两种情况:第一,收集电子数据的侦查人员不具有相关专业技术;第二,具有相关专业技术的电子数据取证人员不是侦查人员。就前者来说,电子数据取证主体通常具有合法调查权限,但却不符合技术资质的合法性要求;就后者而言,电子数据取证主体通常具有相关专业技术,但却有悖于取证权限的合法性要求。无论是取证权限不合法,还是技术资质不合法,都会损害电子数据取证主体的合法性。不过,我国刑事诉讼法和相关司法解释均未明确电子数据收集主体不合法的法律后果,即收集主体不合法的电子数据是直接予以排除还是允许补正后使用并不明确,由此导致司法实践中存在不同的处理方法。

在我国刑事诉讼法和刑事证据理论中,取证主体合法性是否会影响到有关证据的证据能力,历来存在较大争议,主要有“绝对肯定说”、“相对肯定说”和“否定说”三种观点(后文将详细分析)。对于言词证据和传统实物证据而言,影响其取证主体合法性的主要因素是取证权限。电子数据作为新兴证据种类,其所具有的科技性和相对独立性,使得取证主体合法性的问题更加复杂。电子数据的科技性特征决定了不仅取证权限会影响取证主体合法性,技术资质也会对其产生影响。与传统实物证据不同,电子数据可独立于原始载体而存在。电子数据的相对独立性决定了两种取证模式的存在:“一体收集”和“单独提取”。不同取证模式对电子数据收集主体提出了不同要求。从司法实践来看,由于我国现有法律和司法解释对电子数据取证主体合法性的规则尚不完善,理论界对取证主体合法性理论存在较大分歧,由此导致电子数据取证主体规则在司法实践中比较混乱。因此,本文拟对电子数据取证主体进行专门探讨。在研究内容上,本文主要集中于以下问题:第一,电子数据不同取证模式下的取证主体。不同取证模式对电子数据取证主体提出

[4] 参见刘品新:《电子取证的法律规制》,《法学家》2010年第3期,第73-82页。

[5] 参见何邦武:《论网络交易犯罪惩治中电子数据的保全》,《东方法学》2017年第4期,第77-83页。

了不同要求,由此决定了电子数据取证主体违法的不同表现形态。第二,取证主体对电子数据证据能力的影响,着重分析取证权限和技术资质对电子数据证据能力的不同影响及其法律后果。第三,探讨根据案件类型、电子数据种类等因素建立科学的电子数据取证主体制度以保证其证据能力,分析电子数据取证主体不同模式的适用范围和运行程序。在研究方法上,本文将结合司法实践中的典型案例对电子数据取证主体展开实证分析。对典型个案的剖析,有助于对电子数据取证主体合法性的深化研究,以期对电子数据的科学适用提供借鉴。

二 不同取证模式下的取证主体

对“电子数据收集”的界定将直接影响其收集主体的身份和范围,因此,有必要厘清电子数据收集的概念。学界关于“电子数据的收集”存在较大争议,主要有“广义说”和“狭义说”。前者认为,电子数据的收集是指对存在于计算机和相关电子设备中的电子数据进行搜查、提取、保存和归档的过程。^[6] 后者则认为,电子数据收集是指侦查机关向有关单位和个人提取能够证明案件事实的电子数据。^[7] 这两种界定既有电子数据收集方法的差异,也有电子数据收集主体的差异。总体来看,笔者更倾向于广义的电子数据收集概念,但又略有差异。其一,从取证方式来看,电子数据收集并不限于电子数据提取,广义的电子数据收集既包括单独从原始存储介质中提取电子数据,也包括对电子数据连同其原始存储介质的一并扣押。其二,从取证主体来看,电子数据取证主体既包括侦查机关办案人员,也包括相关技术人员。因此,本文所主张的电子数据收集是指,取证主体对存储于计算机、手机等电子设备中的电子数据单独进行或者连同其原始存储介质予以搜查、扣押、提取、保存和分析的过程。

电子数据与物证、书证、视听资料虽同属广义实物证据,^[8]但是,其与物证的存在形态有较大区别。物证通常是以其外部特征、存在状态或物质属性发挥证明作用,这就决定了其证明案件事实的信息蕴含于物的形态之中,其证据信息与物的形态具有一体性,这种一体性特征决定了在收集物证的实物形态时会将其自身蕴含的证据信息一并收集,因此,物证收集通常是将其证据信息连同其所依附的物质载体一并收集。电子数据则具有相对独立性,它虽然也依附于存储介质而存在,但却可以实现与其所存储介质的相互分离。这种相对独立性决定了电子数据既可以存在于原始存储介质之中,也可以存在于原始存储

[6] 参见刘品新:《电子取证的法律规制》,《法学家》2010年第3期,第73-82页。

[7] 参见王敏远、祁建建:《电子数据的收集、固定和运用程序规范问题研究》,《法律适用》2014年第3期,第27-35页。

[8] 对于电子数据是否属于实物证据,理论界也存在不同观点。有观点认为,电子数据属于言词证据还是实物证据,应当具体分析(参见陈光中主编:《刑事诉讼法》,北京大学出版社2013年版,第217页)。笔者认为,在收集言词证据过程中,通过手机、数码相机等方式记录的证人证言、被告人供述、被害人陈述等证据,电子数据本身仅仅是固定上述证据种类的方式,其在本质上仍然归属于上述言词证据。《电子数据规定》第1条第3款规定:“以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等证据,不属于电子数据。”本文的研究重点并不在于通过电子数据固定上述言词证据,因此,本文亦不将其纳入电子数据范畴。

介质之外的其他存储介质之中。电子数据的相对独立性决定了其存在两种收集模式,即“一体收集”模式和“单独提取”模式。

所谓“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。不同取证模式不仅对电子数据的收集方法和鉴真方式产生了不同影响,^[9]也对其取证主体提出了不同的要求。

(一) 电子数据“一体收集”模式下的取证主体

[案例一]: 张某伪造货币案^[10]

在张某伪造货币案中,辩护方提出电子证据收集主体不合法、不完整,不能作为定案证据使用的辩护意见。法院经审理后认为,根据《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》,对作为证据使用的电子数据,应当采取扣押、封存电子数据原始存储介质、计算电子数据完整性校验值、制作及封存电子数据备份等方法保护电子数据的完整性。本案中,侦查人员依法扣押了张某使用的手机和电脑等涉案电子数据原始存储介质,并交由徐州市公安局电子物证检验鉴定中心进行勘验检查、提取电子数据。该中心依照法定程序,采用科学方法,对涉案电子设备进行了勘验检查,制作了电子证据检验笔录,并将提取的电子数据制成光盘备份,且备份光盘有完整性校验值,能够防止数据被篡改,保证了电子数据的完整性。故本案中的电子数据证据提取程序合法,内容真实、完整,能够作为定案证据使用。

手机、计算机中存储的相关信息是实践中较为常见的电子数据。由于手机、计算机可以较为方便地查封和扣押,故收集其中存储的电子数据证据应当将作为其原始存储介质的手机、计算机一并查封扣押。在案例一中,侦查人员就是对电子数据连同作为其原始存储介质的手机、计算机一体查封扣押的。由于电子数据具有较强的科技性且无法直接感知,参与案件处理的侦查人员可能只具有传统的实物证据收集技术,而并不掌握提取电子数据所要求的专业知识和实践经验,他们也无法仅凭视觉、嗅觉和触觉知悉原始存储介质中电子数据的具体内容,更无法知晓哪些电子数据与犯罪事实相关。^[11]因此,他们无法在案件现场直接从手机、计算机等原始存储介质中提取电子数据,而只能采取电子数据“一体收集”模式,将电子数据连同其原始存储介质一并收集。

电子数据的“一体收集”模式通常分为两个步骤:第一,在案件现场搜查、扣押、封存电子数据的原始存储介质。在案例一中,侦查人员就首先在案发现场依法扣押了张某使用的手机和电脑等涉案电子数据原始存储介质,而并未当场从手机和电脑等原始存储介质直接提取电子数据。在此环节,对电子数据原始存储介质的查封扣押也同步实现了对电子数据的一体收集。此时,对电子数据原始存储介质的收集与传统实物证据并不存在

[9] 参见谢登科:《论电子数据的鉴真问题》,《国家检察官学院学报》2017年第5期,第50-72页。

[10] 案例来源:中国裁判文书网,具体内容详见安徽省徐州市中级人民法院(2017)苏03刑终9号刑事裁定书。

[11] 参见陈永生:《电子数据搜查、扣押的法律规制》,《现代法学》2014年第5期,第111-127页。

本质区别,故对电子数据取证主体的技术资质就无需特别要求,侦查人员可将其在传统实物证据中的技术和经验应用于此环节。第二,在原始存储介质中提取电子数据。在司法实践中,多数侦查人员并不具备提取电子数据的专业知识和实践经验,他们欠缺直接从原始存储介质中提取电子数据的技术能力,需要将原始存储介质连同电子数据移送给专业技术人员,由专业技术人员从原始存储介质中提取电子数据。在案例一中,侦查人员扣押手机和电脑等涉案物品之后,并未自行从中提取电子数据,而是将其封存交由电子物证检验鉴定中心通过技术手段提取。在这一环节提取电子数据就对电子数据主体的技术资质提出了相应要求。

因此,电子数据“一体收集”模式下的不同阶段,对电子数据收集主体的技术资质存在不同要求。在第一个环节,对电子数据取证主体的技术资质并没有特别要求,而在第二个环节,则要求电子数据取证主体应具有相应技术知识和实践经验。在案例一中,辩护方提出侦查人员不具有相应技术知识、取证主体不合法进而主张该电子数据不能作为定案依据。但是,在电子数据“一体收集”模式的第一个取证环节对电子数据取证主体资质并不存在特别要求,而在第二个环节将原始存储介质交由相关的专业机构提取电子数据,就解决了对主体的技术性要求。在电子数据“一体收集”模式下,司法机关对于《网络犯罪刑事诉讼程序意见》第 13 条应予以区别适用,该条对侦查人员技术资质的要求仅能适用于“一体收集”模式的第二个环节,而对第一个环节中电子数据收集主体则不宜适用。

(二) 电子数据“单独收集”模式下的取证主体

电子数据种类繁多,并且会随着网络信息技术的不断发展而衍生出新的形态,并非所有类型的电子数据都可以采取“一体收集”模式。按照其生成所依赖技术环境的不同,可以将电子数据分为计算机类电子数据、网络类电子数据和手机类电子数据。^[12]对于计算机和手机类电子数据通常可以采取“一体收集”模式,而对于网络类电子数据则不宜采取“一体收集”模式,应当单独提取电子数据。

[案例二]:孙某非法吸收公众存款案^[13]

孙某在互联网上创办网贷平台,吸收会员注册、充值投资。该网贷平台由其委托宝智公司建设,平台数据则存放在阿里云服务器中。案发后,侦查人员找到宝智公司员工张某。张某应侦查人员要求,登录存放在阿里云服务器中的数据库,然后按公安机关要求整理汇总之后交给侦查人员。案件审理中,辩护方提出由宝智公司员工张某整理后台数据欠缺依据,电子数据提取不符合法律规定,无法确定其真伪,不能作为定案依据。法院经审理后认为,侦查机关在收集电子数据时,在两名侦查人员及相关见证人的见证下,由张某登陆阿里云服务器将后台数据下载并存盘,交由侦查机关封存保管。侦查机关在提取电子数据过程中制作了笔录和清单,并经侦查人员、数据持有人、见证人签名,足以保证电子数据提取的真实性、合法性。之后侦查人员亦将电子数据交张某比对,张某证实,其登陆阿里云服务器账号后,比对侦查人员提供的电子数据与阿里云服务器中存储数据完全

[12] 参见龙宗智等著:《司法改革与中国刑事证据制度的完善》,中国民主法制出版社 2016 年版,第 306-308 页。

[13] 案例来源:中国裁判文书网,具体内容详见山东省莱芜市钢城区人民法院(2016)鲁 1203 刑初 4 号刑事判决书。

相符,其在电子数据整理过程中没有做任何删除和更改。此外,公诉机关当庭出示的 34 名被害人陈述及被害人个人账号充值、提现等网页截图、银行记录等证据,也证实与整理汇总后的电子数据相一致,足以印证其真实性,故对该电子数据予以采信。

电子数据具有相对独立性,其可在保持内容一致的情况下与原始存储介质分离开来,即它并非与原始存储介质是一体的,可以依附于其他存储介质独立存在。将电子数据从原始存储介质复制到其他存储介质,在确保具备相应技术条件之下,复制出来的电子数据可以与原始存储介质中的电子数据完全一致。但是,物证、书证等实物证据无法同原始存储介质完全区分开来,也无法确保其复制件、复印件与原件原物完全一致。在电子数据收集过程中,在无法收集、提取原始存储介质时,就可以单独提取电子数据,将其存储在其他存储介质中。从实践运行来看,无法获取原始存储介质的情形主要包括:第一,原始存储介质不便封存。从实践来看,有些情况下难以将原始存储介质封存或者一体提取,比如网络服务器一般采取集中存储方式,其硬盘动辄上千 T 的数据,其中很多与案件无关,不必收集。在这种情况下,一般只提取与案件相关的电子数据。此外,银行、网络运营商、服务商等电子数据持有人,在配合公安机关调取注册信息、登录日志、交易流水等证据材料时,一般也不便对原始存储介质进行封存,而只提供复制出来的电子数据。第二,提取计算机内存储的数据、网络传输的数据等不是存储在存储介质中的电子数据。这些数据由于不是存储在存储介质里,自然无法封存原始存储介质。这些信息必须在开机状态下获取,一旦关机或者重新启动系统,电子数据就可能消失,难以再次获取。第三,原始存储介质位于境外。位于境外的服务器无法直接获取原始存储介质,一般只能通过远程勘验方式来提取电子数据。^[14]

在案例二中,涉案的 P2P 网贷平台数据库存储于阿里云服务器中,侦查机关无法直接查封、扣押涉案电子数据的原始存储介质——阿里云服务器。云平台的共享性使得涉案虚拟服务器所挂载的虚拟硬盘等电子数据处于离散状态,虚拟服务器释放的空间会被立即分配给其他虚拟服务使用者。^[15] 由于无法直接查封、扣押涉案电子数据的原始存储介质,故只能通过技术手段从阿里云服务器中下载涉案数据库。此时,电子数据与原始存储介质就相互分离,取证主体可以直接从原始存储介质中提取电子数据。在电子数据“单独提取”模式下,电子数据很容易被修改、替换或者破坏,故对电子数据的收集提出了更高的规范性和技术性要求,这其中就包括对电子数据取证主体的要求。在案例二中,由于侦查人员并不具有直接从云服务器上提取电子数据的技术知识和实践经验,他们没有自行从云服务器上提取电子数据,而是委托宝智公司技术人员张某从云服务器中提取电子数据,这就保证了电子数据提取的合技术性要求。但是,技术人员张某并非侦查人员,其并不享有对电子数据的调查取证权。本案辩护方提出了电子数据取证主体不合法的质证意见,法院在裁判时并未对上述质证意见予以回应,没有对电子数据取证主体合法性展

[14] 参见胡云腾主编:《网络犯罪刑事诉讼程序意见暨相关司法解释理解与适用》,人民法院出版社 2014 年版,第 54-55 页。

[15] 参见杜晓、张希臣:《大数据时代,电子取证怎样锁定“黑手”》,《法制日报》2017 年 9 月 22 日第 5 版。

开审查而直接进入对其真实性的审查,这不能不说是本案裁判的瑕疵。正如前文所述,电子数据收集主体的理想状态是侦查人员具有相应的专业知识,这种专业知识能满足电子数据收集的技术性要求。但是,实践中侦查人员往往不具有从原始存储介质上提取电子数据的技术知识和实践经验,他们会委托相关技术人员收集电子数据。这种情况下就可能产生电子数据取证主体合法性的悖论:一方面,若由欠缺专业知识的侦查人员自行从原始存储介质上提取电子数据,虽满足了取证权限的合法性要求,但却无法保障取证主体技术资质的合法性要求;另一方面,若侦查人员委托相关技术人员从原始存储介质上提取电子数据,虽满足了取证主体技术资质的合法性要求,却无法保障其取证权限的合法性要求。在这种悖论之下,无论是由侦查人员取证还是由相关技术人员取证,都会存在取证主体合法性缺失的问题。

三 取证主体与电子数据的证据能力

《网络犯罪刑事诉讼程序意见》第 13 条明确规定,收集、提取电子数据应当由两名以上具备相关专业知识的侦查人员进行。这主要是考虑到电子数据的取证与传统实物证据的取证过程和收集方式存在较大差别,取证人员应具有相关专业知识和技术水平,取证设备和过程也应符合相关技术规范 and 操作流程,故有必要对电子数据取证人员的资质予以规定。^[16] 适用该条款应在电子数据“一体收集”与“单独提取”两种模式中有所区别。在“一体收集”模式之下,前期从案件现场搜查、扣押、封存电子数据的原始存储介质无需对取证人员的技术资质有特别要求,后期从原始存储介质中提取电子数据则需对取证主体的技术资质予以限定。在“单独提取”模式之下,则应要求取证主体具有相应技术资质。不过,我国刑事诉讼法和相关司法解释均未明确电子数据收集主体不合法的法律后果,实践中该问题也经常引起争议,因此,有必要分析取证主体对电子数据证据能力的影响。

(一) 取证主体合法性的三种学说梳理与评析

在我国刑事诉讼法学界和证据法学界,关于取证主体是否影响证据的证据能力历来存在争议,主要有“绝对肯定说”、“相对肯定说”和“否定说”三种观点。

“绝对肯定说”认为,取证主体合法性是影响证据能力的因素之一,取证人员应符合法定条件和资格,不资格人员所收集的证据,都不具备证据能力。^[17] 按照此种观点,只要电子数据的取证主体不具有相应取证权限或者缺乏相应技术资质,其所收集的证据都不具有证据能力,不能作为定案依据。但是,该学说将取证主体不合法作为完全否定证据能力的事由,存在过于绝对之嫌。刑事诉讼法或者证据法对证据能力进行规范,主要

[16] 参见胡云腾主编:《网络犯罪刑事诉讼程序意见暨相关司法解释理解与适用》,人民法院出版社 2014 年版,第 52 页。

[17] 参见陈瑞华著:《刑事证据法学》,北京大学出版社 2012 年版,第 87-88 页;陈光中主编:《证据法学》,法律出版社 2011 年版,第 148-149 页。

是为了促进权利保障和查明事实。^[18] 对于取证主体制度的设定,有些是为了更好地促进权利保障,有些则是为了更好地促进对案件事实的正确认定。但是,违反取证主体制度并不必然意味着权利侵害,也并不意味会阻碍对案件事实的正确认定。比如在案例二中,侦查人员在取得搜查证的情况下,将电子数据的收集工作交由相关技术人员承担,不仅不存在侵害权利问题,反而更有利于保证电子数据的规范收集,从而有利于促进对案件事实的查明。因此,“绝对肯定说”并不符合我国刑事司法的运行现状和证据能力规则的制度目的。

“否定说”则认为,取证主体并非证据合法性的构成要素,只要取证程序不违法,法定主体之外的人员所收集的证据仍然可能具有证据能力。^[19] 该说并没有将取证主体合法性作为影响证据能力的要素,而仅将取证程序合法性作为影响证据能力的要素。该观点亦存在商榷之处:一方面,它忽略了取证主体与取证程序之间的内在联系,不能完全超越主体及其权限仅仅谈论程序的合法性。^[20] 这在电子数据的收集上体现得尤为明显。如果电子数据的取证主体缺乏相应技术资质,则很难保证取证方式符合相应技术标准,也很难保证取证方式的合法性。另一方面,取证主体不合法可能影响证据能力制度目的的实现。具体而言,取证主体不合法有可能侵害当事人的权利,比如由男侦查人员检查女犯罪嫌疑人身体,就会对其人格尊严构成侵犯;也有可能阻碍对案件事实的侦查,比如在电子数据收集过程中,由缺乏技术资质的人员提取电子数据就可能破坏其真实性或者完整性,影响对案件事实的查明。因此,取证主体合法性并非完全对证据能力没有影响。

“相对肯定说”则认为,不具备法定资质人员所收集的证据,并不能完全否定其证据能力,而需结合取证的行为性质、证据的具体种类、违法的主观方面等因素综合评判其证据能力。^[21] 该学说是在批判“绝对肯定说”基础上发展起来的,并不完全否定不合法的取证主体所收集证据的证据能力,不合法主体所收集的证据是否具有证据能力需结合多方面因素权衡后确定。总体来看,“相对肯定说”比较契合我国现有法律规定和司法运行状况。一方面,该说承认取证主体会影响证据的证据能力,另一方面则要求对主体违法的不同要素予以衡量,以便确定取证主体违法性对证据能力的具体影响。“相对肯定说”的正当根基在于取证主体违法形态的多样性,不同违法形态对证据能力的影响也不相同,至于是否需要否定其证据能力,则应结合取证主体违法的具体形态予以分析。因此,“相对肯定说”亦可适用于电子数据取证主体,取证主体不合法是否损害电子数据的证据能力需根据不同情况进行分析和权衡。

(二) 取证主体不合法对电子数据证据能力的影响

如前所述,电子数据收集主体合法性通常包括两个要求:取证权限的合法性和技术资质的合法性。其对应的违法形态也主要有两种:第一,收集电子数据的侦查人员不具有相

[18] 参见孙远:《刑事证据能力的法定与裁量》,《中国法学》2005年第5期,第161-173页。

[19] 参见万毅:《取证主体合法性理论批判》,《江苏行政学院学报》2010年第5期,第110-115页。

[20] 参见谢登科:《论行政执法证据在刑事诉讼中的使用——基于典型案例的实证分析》,《华东政法大学学报》2016年第4期,第147-159页。

[21] 参见龙宗智:《取证主体合法性若干问题》,《法学研究》2007年第3期,第133-143页。

关专业技术知识;第二,具有相关专业技术知识的电子数据取证人员不是侦查人员。前一种情况下,电子数据取证主体不符合技术资质的合法性要求;后一种情况下,电子数据取证主体有悖于取证权限的合法性要求。无论是取证权限不合法,还是技术资质不合法,都会损害电子数据取证主体的合法性。有观点认为,合法性是证据的法律属性,它要求证据的取证主体、取证方法和取证程序都须符合法律规定。无论是主体不合法、形式不合法,还是程序不合法的证据,都存在一个利益衡量的问题。对于电子数据而言,在生成、取得等任何环节存在违法,只要其违法程度足以影响真实性时,都将影响电子数据的可采性。^[22] 该观点将取证主体对电子数据真实性的影响作为确定其是否具有证据能力的因素,具有相对合理性。但亦存在可商榷之处。刑事诉讼法或者证据法对证据能力进行规范,主要是为了促进权利保障和查明案件事实。取证权限合法性和技术资质合法性对两者产生的影响并不完全相同。一般而言,前者主要涉及被调查对象的权利保障,而后者则主要会影响电子数据的真实性和相关性。

在前文案例二中,侦查人员委托宝智公司技术人员张某从云服务器中提取电子数据,这保证了电子数据提取的合技术性要求。但是,技术人员张某并非我国法律所规定的侦查人员,并不享有对电子数据的调查取证权。那么,侦查人员是否可以将其侦查权委托给技术人员张某行使。一般而言,侦查行为可以分为强制性侦查行为和任意性侦查行为。^[23] 对于任意性侦查权可以由侦查人员委托他人行使,而强制性侦查权则具有专属性,一般不能委托他人行使,只能由侦查机关自行实施。关于这一点刑事诉讼法虽未明确规定,但亦可参照其他法律基本精神。比如《行政强制法》第 17 条规定:“行政强制措施由法律、法规规定的行政机关在法定职权范围内实施。行政强制措施权不得委托。”由于行政强制措施具有即时性和强制性,它对公民、法人和其他组织的权益和自由构成极大限制,故行政强制措施只能由法定的行政机关实施,而不得委托其他组织或者个人。^[24] 这其中也包括强制性取证的禁止委托。作为刑事侦查中的调查活动,其中的很多调查措施都具有强制性,在法律并未明确规定可以委托他人行使的情况下,则只能由侦查机关自行实施。因此,在该案中张某并不能基于侦查人员的委托或者指派而享有搜查权。侦查人员委托张某从阿里云服务器中提取电子数据只能说明其满足了取证主体的技术资质合法性,而并不能说明其具有调查权限的合法性。但是,若侦查人员在已经取得搜查证的情况下,就具有了从阿里云服务器中收集电子数据的合法权限。侦查人员所具有的电子数据取证合法权限,可以弥补张某调查权限欠缺的瑕疵,因为侦查人员即使不委托张某收集证据,也可以委托或者指派其他有专门知识的人收集电子数据。技术人员张某取证合法权限的欠缺并不能否定电子数据的证据能力。因此,取证权限的欠缺在绝大多数情况下并不会影响电子数据的证据能力,但这并不意味着取证权限对电子数据的证据能力没有任何影响。

[22] 参见戴长林主编:《网络犯罪司法实务研究及相关司法解释理解与适用》,人民法院出版社 2014 年版,第 213 页。

[23] 参见[日]田口守一著:《刑事诉讼法》,张凌、于秀峰译,中国政法大学出版社 2010 年版,第 103 - 118 页。

[24] 全国人大常委会法制工作委员会行政法室编写:《〈中华人民共和国行政强制法〉释义与案例》,中国民主法制出版社 2012 年版,第 75 - 76 页。

[案例三]:侵犯商业秘密案^[25]

警方接到甲公司报案,称该公司软件被盗版。经查,该案犯罪嫌疑人丙曾与该公司签订技术开发合同,后私自将甲公司软件代码复制,并成立乙公司后在国内公开销售。警察聘请相关计算机专家制定了详细的取证方案。在到达乙公司后,为防止丙毁灭证据而切断了乙公司外部网线,同时控制了丙并让其打开电脑,按相关专家指令进行操作。在证据收集过程中,侦查人员制作了相应笔录、进行了全程录像。

在该案中,由于侦查人员自己并不具有收集电子数据的专业知识,故办案人员在收集电子数据过程中就强令犯罪嫌疑人自己操作电脑,直接在犯罪嫌疑人的计算机系统中进行操作、提取电子数据,这种做法是否可能影响其证据能力,就存在值得商榷之处。从法律角度来看,犯罪嫌疑人不仅没有收集控方证据的权限和义务,他还受到“禁止强迫自证其罪”原则的保护。禁止强迫自证其罪原则,不仅要求侦查机关禁止采取刑讯逼供等方式收集口供,也禁止侦查机关通过强制手段让犯罪嫌疑人收集证明自己有罪的证据。^[26]该案侦查人员强令犯罪嫌疑人从自己电脑提取电子数据不仅属于取证主体违法,也违反了“禁止强迫自证其罪”原则,侵害了当事人意思自治权,属于严重的程序违法。从电子数据真实性角度来看,让犯罪嫌疑人自行提取电子数据也无法保证其真实性。由于犯罪嫌疑人与案件处理结果具有直接利害关系,他可能会在提取电子数据过程中故意隐瞒或者破坏,从而无法保证电子数据的真实性。因此,对于此种主体违法情况下收集的电子数据应否定其证据能力。综合前述两个案例可以看出,取证权限违法多数情况下并不会损害被调查对象的合法权利,对电子数据的证据能力也就不存在影响。但是,若欠缺取证权限严重侵害被调查对象的合法权利时,则会减损电子数据的证据能力。

在取证主体不具有相应技术资质的情况下,取证主体违法就可能造成电子数据的破坏、遗漏、毁灭等情形发生,从而影响对案件事实的正确认定。此种情况下若不能保证电子数据真实性,就会减损或者否定其证据能力,比如下面的案例。

[案例四]:曾某开设赌场案^[27]

在曾某开设赌场案中,辩护方提出公安机关不能自行提取电子数据,应当由专业的技术人员提取数据。故公安机关根据其在赌博机中收集的电子数据,不能作为赌博机的实际盈利数额,其制作的盈利表不真实、不客观,不能作为定案依据。法院经审理后认为,该盈利表是公安机关根据被查扣的赌博机上显示的数据制作而成,是公安机关自行提取并统计的,该表对赌博机的最初显示数据和最终显示数据进行了记载,通过二者相减得出了盈利数,但是最高人民法院、最高人民检察院、公安部《关于办理利用赌博机开设赌场案件适用法律若干问题的意见》中规定,赌资是包括当场查获的用于赌博的款物,还有代币、有价证券、赌博积分等实际代表的金额,以及在赌博机上投注或赢取的点数实际代表

[25] 参见戴长林主编:《网络犯罪司法实务研究及相关司法解释理解与适用》,人民法院出版社2014年版,第218-221页。

[26] 参见董坤:《不得强迫自证其罪原则在我国的确立与完善》,《国家检察官学院学报》2012年第2期,第114-122页。

[27] 案例来源:聚法案例网,具体内容参见湖南省娄底市娄星区人民法院(2016)湘1302刑初93号刑事判决书。

的金额。该盈利表统计的数据是赌博积分实际代表的金额,应当以该盈利表最终的数据 278935 元认定为赌资,不能认定为二被告人的违法所得。而二被告人违法所得的数据应当结合本案其他证据予以综合认定。被告人记载的原始记账凭证就是笔记本电脑,通过该电脑上统计的数据显示,被告人颜某乙每天最后统计的数据是纯盈利数,该数据已经扣除了游戏厅所有的开支,被告人颜某乙就该事实于 2015 年 10 月 20 日在公安机关讯问中予以了供述,且根据其结合笔记本电脑统计的数据为 34217 元,该数据是二被告人开设赌场的纯盈利数。

在该案中,收集电子数据的侦查人员具有合法调查权限,但不具有相应专业技术知识和实践经验,由此导致电子数据的真实性无法得到保证,法院最终否定了该电子数据的证据能力,没有将其作为认定案件事实的根据。取证主体若不具有相应技术资质,其在取证过程中就可能造成电子数据的破坏、遗漏、毁灭,从而损害电子数据的真实性,进而导致其因不具有证据能力而不能作为依据。《电子数据规定》第 28 条规定了电子数据不得作为定案依据的三种情形,^[28] 主要都是因为电子数据的真实性无法得到保证而否定其证据能力的。其中该条第 3 项规定属于兜底性条款,可以将取证主体不具备相应技术资质而无法保证电子数据真实性纳入其中。

(三) 瑕疵电子数据的补正与修复

取证主体不具备相应技术资质,其在电子数据收集过程中就可能造成电子数据的破坏、遗漏、毁灭,从而损害电子数据的真实性,就会减损或者否定其证据能力。对于完全丧失证据能力的电子数据,则不能作为定案依据;对于部分丧失证据能力的电子数据,则应当给予补正和修复的机会。在后一种情况下,则不应完全否定电子数据的证据能力,而应将其作为瑕疵证据予以补正或者修复,比如下文案例五。

[案例五]: 吴某猥亵儿童案^[29]

在吴某猥亵儿童案中,辩护方提出本案电子数据收集程序严重违法,不应认定其证据效力。法院经审理后认为,南京市公安局玄武分局于 2014 年 9 月 7 日出具调取证据通知书,向证据持有人孙某调取本案案发现场的监控录像,在调取证据清单上仅有一名办案人员签名。一审审理中,因辩护人对监控录像调取程序提出异议,后南京市公安局玄武分局板仓派出所出具情况说明,该说明显示了由公安局四名侦查、技术人员调取案发现场周边“小孙米行”录像的过程,同时将证人孙某的询问笔录提交给公安机关,笔录记载,孙某陈述有三四个警察到其店里拷走录像。根据最高人民法院《关于适用〈中华人民共和国刑事诉讼法〉的解释》第 94 条规定,视听资料、电子数据具有下列情形之一的,不得作为定案的根据:(一)经审查无法确定真伪的;(二)制作、取得的时间、地点、方式等有疑问,不能提供必要证明或者做出合理解释的。本案中,公安机关调取证据清单上虽仅有一人签名,确有瑕疵,但其后出具的情况说明对此可以做出合理解释,且证人孙某的证言能与公

[28] 《电子数据规定》第 28 条规定:“电子数据具有下列情形之一的,不得作为定案的根据:(一)电子数据系篡改、伪造或者无法确定真伪的;(二)电子数据有增加、删除、修改等情形,影响电子数据真实性的;(三)其他无法保证电子数据真实性的情形。”

[29] 案例来源:聚法案例网,具体内容参见江苏省南京市中级人民法院(2015)宁少刑终字第 7 号刑事裁定书。

安机关的情况说明相印证,该电子数据可以作为定案根据。

在该案中,监控录像属于电子数据而不是视听资料。视听资料和电子证据的主要区别在于,前者是以模拟信号在介质上进行存储的声音、影像及其组合等资料,而电子数据是以数字信号在存储介质上进行存储的数据。监控录像中虽然也含有声音、活动影像等资料,但其存储方式并不是以磁带、胶卷等模拟信号为载体的资料,因此,其属于电子数据而不是视听资料。辩护方提出电子数据收集笔录上仅有一人签字,实际上是想通过主张取证主体和程序违法而排除该电子数据。但是,控诉方却通过补正和说明情况的方式恢复了该电子数据的证据能力,并最终被法官所采信。程序补正也被称为违法诉讼行为的治愈,是指对于情节较轻的程序违法行为,在被宣告无效之前,允许侦查人员、检察人员及下级法院重新实施特定诉讼行为,以纠正原有违法程序,重新做出相应诉讼决定。^[30]我国现行法律和司法解释对瑕疵实物证据规定了两类补正方式:一是进行必要补正,二是做出合理解释或说明。这些传统实物证据的瑕疵补正方式亦适用于电子数据。对于电子数据取证主体违法但不存在导致其真实性丧失的情况下,应当给予补正或者修复的机会。《电子数据规定》第27条第2项和第4项可以为取证主体轻微违法的瑕疵补正提供法律依据。^[31]对于该瑕疵证据可以通过情况说明或者提交其他证据予以补正,补正之后的电子数据能够与其它证据相互印证的,则可以作为定案根据,^[32]否则就应当予以排除、不能作为定案根据。

四 电子数据取证主体制度的建构与前瞻

取证主体违法会损害或者降低电子数据的证据能力,取证主体不适格可能导致电子数据不被法官所采信,即使经过补正或修复后能够作为定案依据,也会增加电子数据认定和采信中的诉讼成本。因此,有必要根据具体案件类型、电子数据种类等因素建立科学的电子数据取证主体制度,以防范取证主体不适格对电子数据证据能力的损害。如果仅从取证主体角度来看,电子数据的取证存在“独立取证”、“联合取证”和“委托取证”三种模式,它们存在各自不同的适用范围和运行程序。

(一) 独立取证模式下的电子数据取证主体

侦查机关在刑事诉讼中享有法定的调查取证权,其内部享有办案权限的侦查人员在法律上是适格的取证主体,其中就包括对电子数据的取证权限。但是,这仅仅是从法定权限的角度保证了取证主体的合法性,却并不能从技术资质角度保证取证主体的合法性。正如前文所述,电子数据具有技术含量高的特征,侦查人员若缺乏相应专业知识作支撑,

[30] 参见陈瑞华著:《刑事证据法学》,北京大学出版社2012年版,第315页。

[31] 《电子数据规定》第27条规定:“电子数据的收集、提取程序有下列瑕疵,经补正或者做出合理解释的,可以采用;不能补正或者做出合理解释的,不得作为定案的根据:(一)未以封存状态移送的;(二)笔录或者清单上没有侦查人员、电子数据持有人(提供者)、见证人签名或者盖章的;(三)对电子数据的名称、类别、格式等注明不清的;(四)有其他瑕疵的。”

[32] 参见刘品新:《印证与概率:电子证据的客观化采信》,《环球法律评论》2017年第4期,第109-127页。

很可能无法有效收集电子数据,甚至会损坏电子数据的真实性。因此,有必要在侦查机关内部建立具有电子数据取证资质的专门人才队伍。侦查人员具有电子数据取证资质和经验,既能保证取证主体权限的合法性,也能保证取证主体技术资质的合法性,这是电子数据取证主体发展的最佳模式。从世界范围来看,很多发达国家为打击计算机犯罪、网络犯罪,很早就成立了收集电子数据的专门组织,比如美国成立的“计算机紧急反应小组”,英国成立的“高科技犯罪调查组”,德国、法国、日本等国亦有类似电子数据取证专门机构。^[33] 目前,我国公安、国家安全等侦查机关也在逐步建立电子数据取证专业队伍,比如公安机关内部所属网络安全保卫部门中的侦查人员,即网络警察。他们一方面对现有侦查人员队伍进行电子数据取证的相关培养和教育;另一方面则在高校、科研院所招聘相关专门人才,设立专门的电子数据取证实验室,专门负责对电子数据的收集。前一种路径相对快捷,但仅适用于比较简单的电子数据取证,比如无需解码的电子数据收集取证,对于比较复杂的电子数据取证则并不具有可行性;后一种路径周期较长,但既可适用于简单的电子数据取证,也可适用于较为复杂的电子数据取证。

从实践来看,我国侦查机关电子数据取证队伍建设存在上下发展不平衡的问题。基层侦查机关承担了大量刑事案件的处理,但是,由于受制于经费、人员、技术等因素,基层侦查机关自身并不具有独立的电子数据取证能力,电子数据取证队伍建设亦无法有效满足实际办案需要。电子数据取证实验室多数建立在市级或者省级侦查机关,基层侦查机关在现有取证力量不足的情况下,只能向省、市级侦查机关请示,但是由于侦查机关内部审批程序和手续较为繁琐,可能会因无法及时收集到有价值的电子数据而贻误案件侦查。另外,在基层侦查机关将电子数据连同其原始存储介质移送上级侦查机关进行提取、鉴定时,往返过程可能会导致电子数据提取和分析的延误,增加了电子数据保管链条鉴真中的安全风险。消除上述风险的有效途径就是强化基层侦查机关电子数据取证队伍建设。在侦查机关内部,加强侦查部门和技术部门的有效联动与配合,探索建立电子数据取证技术侦查一体化发展模式,从而真正兼顾电子数据取证主体取证权限的合法性和技术资质的合法性。

(二) 联合取证模式下的电子数据取证主体

在网络信息技术飞速发展背景下,侦查机关自身技术取证力量建设相对电子数据技术发展而言,总会存在滞后性。侦查机关除了需要发展自身电子数据取证专业队伍建设之外,也必然需要依赖其自身之外的专业技术取证力量。这种专业技术取证力量一方面存在于同为公权力主体的其他行政机关之中,另一方面则涉及具有相关专业技术力量的社会组织和个人。侦查机关在借助于其他行政机关的专业技术力量时有两种路径:一是与其他行政机关联合办案时,可以联合其专业技术人员收集相关电子数据;二是自身独立办理相关刑事案件时,将其中的电子数据收集工作委托给相关行政机关的专业技术人员承担。行政机关和司法机关的职能分工,决定前者无权处理刑事犯罪行为而仅能对一般违法行为进行行政执法,而后者则只处理刑事犯罪行为。但是,由于行政机关对特定行业

[33] 参见裴兆斌:《论刑事诉讼中电子数据取证模式》,《东方法学》2014年第5期,第87-95页。

或领域负有日常性的行政监管职责和执法权限,这使得它能够在日常监管和执法活动中先行发现、处理特定违法行为。^[34]这也决定了行政机关对其监管领域的违法行为和犯罪行为进行调查取证,具有更大的便利性和专长性。侦查机关在联合执法中与行政机关的专业技术力量联合收集电子数据,一方面可以解决行政机关单独执法中取证权限缺失所导致的取证不合法问题,另一方面则可以解决侦查机关自身技术力量不足所导致的技术资质不合法问题。

从适用范围来看,并非所有刑事案件都可以适用联合取证模式,其主要适用于行刑交叉案件,比如环境污染犯罪、涉税犯罪、金融犯罪、知识产权犯罪等。而对于那些比较传统的犯罪,比如杀人、盗窃、抢劫等犯罪则并不能适用,因为只有行刑交叉案件中才有可能涉及到联合管辖执法问题。在联合取证模式下需要解决由谁来主导或者指挥电子数据的收集工作,这就必然涉及取证主体的取证权限和技术资质问题。从取证权限来看,行政机关在行政执法案件中享有调查取证权,而对于刑事案件则没有侦查权;侦查机关在行政案件中没有调查取证权,只对刑事案件享有侦查权。因此,在涉及行政执法的案件中,电子数据应由行政机关主导收集。如果随着调查取证的深入,发现案件社会危害性较大、已经涉嫌刑事犯罪时,则应将案件移交由侦查机关主导侦查,电子数据的收集亦应交由侦查机关主导。由侦查机关主导电子数据收集工作,可能会存在电子数据收集中的“外行指导内行”的困境。为避免上述困扰,对于侦查机关主导的范围应予以适当限定,其主要应承担电子数据收集的组织和指挥工作,在程序和法律上予以把关,而对于电子数据收集中的技术性工作则仍然需由行政机关的技术人员自行完成。由于联合执法中收集的电子数据后期会进入刑事诉讼程序,对电子数据合法性的审查需要按照刑事诉讼法规定的取证程序进行,故由侦查机关主导电子数据收集中的程序和法律问题更有利于保证电子数据的合法性。

(三)委托取证模式下的电子数据取证主体

将专业问题交由专业人员处理是任何证据收集过程中应遵循的基本准则。电子数据收集集中涉及到相关专业问题亦应交由专业技术人员处理。从法律关系上看,侦查人员将证据集中的专业技术工作交由专业技术人员处理,二者之间是委托关系。《刑事诉讼法》第126条和第144条分别规定侦查人员可以指派、聘请有专门知识的人进行勘验、检查和鉴定。在电子数据收集过程中,也可以指派有专门知识的人进行相关勘验、检查和鉴定工作。有专门知识的人员接受侦查人员委托并在其主持下,从事电子数据的勘验、检查和鉴定工作,解决了侦查人员单独收集电子数据时技术资质欠缺的问题。但这里需要解决的仍然是取证权限能否委托的问题。由于《刑事诉讼法》第126条和第144条已经明确了勘验、检查和鉴定可以指派、聘请有专门知识的人进行,故将电子数据集中的勘验、检查和鉴定工作委托给有专门知识的人是具有合法性的。而对于通过勘验、检查和鉴定之外的其他侦查措施包括收集电子数据是否允许委托,笔者认为,在委托有专门知识的人收

[34] 参见谢登科:《论行政执法证据在刑事诉讼中的使用——基于典型案例的实证分析》,《华东政法大学学报》2016年第4期,第147-159页。

集电子数据时,需要考虑以下两个方面的问题:

第一,关于委托范围。除了勘验、检查和鉴定之外,侦查人员是否可以委托有专门知识的人从事电子数据的其他侦查行为,比如搜查、扣押。正如前文所述,电子数据收集是对电子数据的搜查、扣押、提取、保存和分析的过程,它不仅包括电子数据的勘验、检查和鉴定,还包括对电子数据的搜查、扣押、查封等侦查行为。由于现有法律并未规定搜查、扣押、查封等侦查行为可以委托有专门知识的人进行,但是电子数据搜查中可能涉及到相关的专门性问题,此时是否允许委托有专门知识的人处理,就值得探讨。有学者认为,搜查、扣押、提取电子数据载体的获得性取证行为,应当要求有两名以上侦查人员行使;而对可能需要具备必要技术能力的取证行为,则实行侦查人员与专业技术人员相配合的取证方法。^[35] 该观点认为,搜查、扣押只能由侦查人员进行,理由是搜查的技术含量较低,无须委托有专门知识的人处理。这一观点无疑具有相对合理性。相对于勘验、检查和鉴定而言,搜查的技术含量确实较低,但是,技术含量高低不仅仅取决侦查行为类型本身,也取决于侦查对象。电子数据自身具有技术性强的特征,由此在搜查中可能存在某些专门性问题令侦查人员无法解决,而必须委托有专门知识的人来处理。因此,对于电子数据的搜查、扣押、查封中的专门性问题,侦查人员自身无法解决时,应当允许委托有专门知识的人在其指挥下参与相关搜查、扣押、查封工作。需要注意的是,强制性侦查措施一般不宜委托给他人行使,这里需要做适当区分。强制性侦查措施适用中通常包括两项权力,即强制措施的审查决定权和执行权。审查决定权是通过了对申请事由和相关证据材料的审查决定是否同意采取强制性侦查措施,它直接决定了强制性侦查措施的正当性与合法性。强制性侦查措施不宜委托给他人行使应理解为其审查决定权不宜委托给他人行使。而适用强制性侦查措施的决定一旦做出,侦查人员就享有对电子数据取证的合法权限。对于搜查或者扣押决定的执行,本身就是为了收集证据和查明事实。如果在取得合法权限之后,将强制性侦查措施的执行委托给有专门知识的人行使能够更好地实现上述目的,则自然是应当允许的。故对电子数据搜查、扣押、查封中的审查决定工作不能委托有专门知识的人承担,但对于具体执行工作则可以委托。

第二,关于委托对象。《刑事诉讼法》第 126 条和第 144 条将委托代为勘验、检查和鉴定的对象限定为“有专门知识的人”,这其中也包括电子数据收集中委托“有专门知识的人”从事上述工作。从司法实践来看,有的司法机关是委托相关鉴定机构的鉴定人进行电子数据收集;有的则是委托相关软件开发单位或者运营单位的工作人员收集电子数据(比如前文案例二)。这些人员是否都属于“有专门知识的人”,值得探讨。现行法律和相关法律解释并未对何为“有专门知识的人”给出明确界定。由于有专门知识的人参与刑事诉讼活动并不具有固定性、长期性和职业性,故没有必要将他们纳入到司法行政管理体系,要求他们必须取得相关专业技术证书。^[36] 但是,这并不意味着对委托“有专门知识的

[35] 参见龙宗智:《寻求有效取证与取证权利的平衡——评“两高一部”电子数据证据规定》,《法学》2016 年第 11 期,第 7-14 页。

[36] 参见陈邦达:《论“有专门知识的人”参与刑事诉讼——兼论〈刑事诉讼法〉第 192 条》,《大连理工大学学报(社会科学版)》2014 年第 3 期,第 85-90 页。

人”收集电子数据没有任何限制。从规范电子数据的收集、审查和认定角度来看,对于“有专门知识的人”应予适当限定:(1)“专门知识”应限定于与电子数据收集相关的专业技术知识,包括计算机技术、网络信息技术、云存储与计算技术、软件开发技术等。(2)法官在采信所收集的电子数据之前,应对参与电子数据收集的“有专门知识的人”是否具有与电子数据收集相关的专业技术知识进行审查,可从学历、职称、专业背景和职业经历等方面进行考量。(3)电子数据的举证方应提供相关证据证明参与电子数据收集的“有专门知识的人”具备相关领域的专业知识,法庭应给予控辩双方就电子数据收集主体是否适格予以辩论和质证的机会。

[本文为中央高校基本科研经费项目“电子数据收集与认定实证研究”的研究成果。]

[**Abstract**] Electronic evidence, as a new type of evidence emerged in the modern network information society, is the product of high technology. As such, it imposes strict requirements on the technical qualification of electronic evidence collectors. There are two models of collection of electronic evidence: integrated collection and separate collection. Those two models have different requirements on the technical qualification of collectors. In practice, most investigators do not have enough technological capacity for collecting electronic evidence and have to rely on specialists to complete the collection. However, this would lead to the conflict of legitimacy between collectors' investigation power and their technical qualification, which have different influences on the admissibility of electronic evidence. The lack of technical qualification would infringe upon the lawful rights of the targets of investigation whereas the lack of investigation power will impair the reliability of electronic evidence. Therefore, it's necessary to establish reasonable rules on competent collectors of electronic evidence, so as to prevent the impairment to the admissibility of electronic evidence.

(责任编辑:王雪梅)