主题研讨

刑事电子数据的规制路径与重点问题

喻海松

内容提要：随着现代科学技术的迅速发展，法定证据种类不断扩充完善。作为2012年《刑事诉讼法》新增的法定证据种类，电子数据在证明案件事实的过程中发挥着越来越重要的作用。针对司法实践中产生的新情况和新问题，最高人民法院、最高人民检察院、公安部等部门，通过司法解释、规范性文件等方式，对电子数据的收集与提取、移送与展示、审查与判断作了全面规定，初步构建起了我国刑事电子数据的规制体系。本文对我国刑事电子数据的规制路径进行了梳理，并在此基础上，针对电子数据收集提取、移送展示和审查判断等环节中的重点问题，特别是司法实务中存有一定争议的取证主体与取证方法要求、取证规则、冻结、检查、专门性问题的判断、备份移送与打印件以及真实性与关联性的审查判断等问题进行探讨分析。

关键词：刑事电子数据　收集提取　移送展示　审查判断

喻海松，最高人民法院研究室刑事处副处长。

作为证明案件事实的材料，法定证据种类随着现代科学技术的进步而不断扩展完善。随着网络信息技术的飞速发展，电子数据在证明案件事实的过程中发挥着日益重要的作用。2012年《刑事诉讼法》将电子数据增设为法定证据种类。针对司法实践中的新情况和新问题，最高人民法院、最高人民检察院、公安部等部门根据2012年《刑事诉讼法》的规定，通过司法解释、规范性文件等方式，对电子数据的收集提取、移送展示和审查判断相关问题作了全面规定。应该说，《刑事诉讼法》及配套司法解释和相关规范性文件的规定，初步构建起了我国刑事电子数据规制体系，对于规范电子数据的提取和运用，更好地证明案件事实，发挥了重要作用。

一 刑事电子数据的规制路径

(一)刑事电子数据的法定地位

1996 年修订的《刑事诉讼法》第 42 条第 1 款规定:“证明案件真实情况的一切事实,都是证据。”但该条第 2 款却将证据限定为七种,其中并不包括电子数据。这就导致司法实践对电子数据的运用处于两难境地:电子数据无疑可以证明案件事实,但具体应当确定为何种类型的法定证据又于法无据。应对这一局面,司法实务采取了一些变通处理的办法,主要是如下两种:

其一,将电子数据直接规定为独立的证据形式。例如,2010 年 6 月“两高三部”《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《证据审查判断规定》)第 29 条就对“电子邮件、电子数据交换、网上聊天记录、网络博客、手机短信、电子签名、域名等电子证据”的主要审查内容直接作出了规定,明显是将电子数据作为独立的证据种类加以审查与判断。

其二,将电子数据转化为其他法定证据形式,主要是转化为勘验、检查笔录予以使用。例如,2010 年 8 月“两高一部”《关于办理网络赌博犯罪案件适用法律若干问题的意见》(以下简称《网络赌博犯罪意见》)中关于电子证据的收集与保全的规定,就是将电子数据转化为勘验、检查笔录加以使用。[1]

以上两种办法都是司法实务部门囿于电子数据未被规定为法定证据种类,不得已而为之。近年来,电子数据在刑事诉讼中得到广泛应用已是不争的事实。2012 年《刑事诉讼法》第 48 条第 2 款对证据种类的规定进行了补充,将电子数据明确列为法定证据种类,进一步丰富了证据的外延。

(二)刑事电子数据的规制体系

2012 年修订的《刑事诉讼法》将电子数据规定为法定证据种类,但并未进一步细化规定电子数据的收集提取与审查判断规则。根据修改后《刑事诉讼法》的规定,有关司法解释和规范性文件确立了电子数据收集提取、移送展示、审查判断的规则。大致发展脉络如下:

1. 电子数据审查判断规则

2012 年 12 月最高人民法院发布《关于适用〈中华人民共和国刑事诉讼法〉的解释》(以下简称《解释》)。《解释》第 93 条、第 94 条吸收和完善了《证据审查判断规定》第 29 条及相关规定,对电子数据的审查判断和排除规则作了明确规定。

---

〔1〕《网络赌博犯罪意见》规定:“侦查机关对于能够证明赌博犯罪案件真实情况的网站页面、上网记录、电子邮件、电子合同、电子交易记录、电子账册等电子数据,应当作为刑事证据予以提取、复制、固定。侦查人员应当对提取、复制、固定电子数据的过程制作相关文字说明,记录案由、对象、内容以及提取、复制、固定的时间、地点、方法,电子数据的规格、类别、文件格式等,并由提取、复制、固定电子数据的制作人、电子数据的持有人签名或者盖章,附所提取、复制、固定的电子数据一并随案移送。”

2. 电子数据收集提取规则

2014 年 5 月最高人民法院、最高人民检察院、公安部联合发布《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》(以下简称《意见》)。《意见》专设“关于电子数据的取证与审查”部分,对电子数据的收集、移送和审查作了全面规定。可以说,《解释》关于电子数据的规定,主要是针对其审查判断;而按照“审什么,取什么”的原则,《意见》则侧重对电子数据的收集提取与移送展示规则作了明确规定。[2]

3. 电子数据规则的丰富发展

总体而言,《解释》和《意见》关于电子数据的收集提取和审查判断的规定较为原则,操作性有待增强。而随着云计算、大数据等技术的发展,收集提取电子数据的难度增加,对取证的信息网络技术要求进一步增强,因此有必要作出新的有针对性的规定。基于此,为顺利开展涉电子数据的刑事诉讼活动,2016 年 9 月最高人民法院、最高人民检察院、公安部联合发布《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《刑事电子数据规定》),对电子数据规则作了进一步细化和统一。可以说,根据《刑事诉讼法》的规定,在《解释》和《意见》相关规定的基础上,《刑事电子数据规定》针对司法实务的新情况与新问题,对电子数据收集提取和审查判断的规则作了进一步丰富发展。

二 刑事电子数据的一般问题

(一)电子数据的界定

根据现行《刑事诉讼法》的规定,电子数据是独立的证据种类。但是,电子数据实际上是传统证据种类的电子数据化。[3] 例如,过去共同犯罪人之间的共谋经常是当面或者通过电话、书信等方式进行,而现在很多共同犯罪人之间通过即时通讯工具进行共谋。信息化时代,通讯记录这种书证形式与传统的书证具有相当的差异,但如果除开具体外在形式,这种通讯记录实际上就是以电子数据形式存在的书证,因为其终究是通过内容来证明案件事实的。因此,电子数据实际上就是传统证据电子化。如果不考虑外在形式,电子数据实际上并非独立的证据种类,任何电子数据都可以还原为其他证据种类。

目前,对于电子数据的具体范围,以及电子数据与其他证据种类的界分,尚存在不同认识。根据《刑事电子数据规定》第 1 条第 1 款的规定,对于电子数据形式的实物证据属于电子数据的范畴,应当没有疑义。这实际上也反映了证据种类随着现代科学技术发展而变化的趋势。例如,视听资料本身是现代科学技术发展的产物,而科学技术、特别是信息技术的发展,又使得音像资料进一步发展:传统的音像资料主要储存在磁带、录像带、VCD、DVD 等实物中,但现在越来越多的音像资料是以电子数据的形式存在的。1996 年

〔2〕 具体而言,《意见》主要对电子数据取证人员资质与技术要求、电子数据取证原则、收集提取电子数据的笔录制作要求、电子数据的移送规则和电子数据的鉴定与检验等问题作了明确规定。

〔3〕 正如有论者指出的,“同七种传统证据形式相比,应该说电子证据来源于七种证据,是将各种传统证据部分地剥离出来而泛称的一种新证据形式。”参见何家弘、刘品新著:《证据法学》(第四版),法律出版社 2011 年版,第 185 页。

《刑事诉讼法》未将电子数据规定为独立的证据种类，故当时不少电子数据都被纳入视听资料的范畴从而证明犯罪事实。〔4〕 这种做法是法学理论和实务针对立法局限的一种变通。但是，在《刑事诉讼法》已经将电子数据作为独立证据种类的背景下，对于以电子数据的形式而存在的音像资料不能再纳入视听资料的范畴。电子数据是独立的证据种类，其与视听资料的界限不能否认，二者之间不存在交叉重合的地方。如果说在电子数据成为独立的证据种类之前，有主张将以电子数据形式存在的视听资料也纳入视听资料的范畴的话，那么在 2012 年《刑事诉讼法》施行后，这类视听资料应当被纳入电子数据的范畴。可以认为，视听资料与电子数据形式的视听资料的区别，就在于由于现代科技的发展使得视听资料先后出现了不同载体。以录音磁带、录像带、唱片、CD、光盘等实物存储介质存储的音像资料与以电子数据形式存在的音像资料，同为音像资料，但就证据种类归属而言，前者属于视听资料的范畴，后者属于电子数据的范畴。

在司法实践中，对于以电子数据形式存在的言词证据的种类归属，存在较大争议。例如，询问证人的录音录像究竟应归为“证人证言”，还是应归为“视听资料”“电子数据”，或者既是“证人证言”也是“视听资料”“电子数据”？实际上，按照《刑事电子数据规定》第 1 条第 1 款将电子数据限定为“案件发生过程中”的规定，电子数据不包括案件发生后形成的电子化的言词证据。〔5〕 本文认为，上述规定将电子数据形式的言词证据不纳入电子数据的范畴是妥当的。主要理由有两点：第一，从长期刑事诉讼实践来看，对于言词证据不宜单纯根据载体划入其他证据种类的范畴。以笔录形式记载的言词证据，并未因为其记载形式而不再纳入言词证据的范畴。同理，以数字化形式记载的言词证据，也不能因为其载体是电子数据，将其纳入电子数据的范畴，而应当仍然将其归属于言词证据。第二，将上述证据作为言词证据，更加符合人权保障的要求。不同类型的证据，依据《刑事诉讼法》规定的不同取证方法、取证程序，其审查判断的要点也不一样。例如，对于以录像形式呈现的犯罪嫌疑人口供，不仅要审查录像是否客观真实，更要审查讯问的主体、方法、程序等是否合法。因此，将电子数据形式的言词证据作为言词证据进行审查判断，可以更为充分地保护刑事诉讼相关主体的合法权益。

（二）电子数据的完整性

传统证据法认为，证据具有三性，即客观性、关联性和合法性。作为证据的种类之一，电子数据无疑也具有上述三性。在此，有必要探讨电子数据的真实性、特别是其下位概念“完整性”的有关问题。

与物证、书证等传统证据种类不同，电子数据本质上是以电子形式存储或者传输的数据。正是由于电子数据的特殊存在形式，即只需要敲击键盘，即可对其进行增加、删除、修

〔4〕 例如，有论者认为：“视听资料是载有能够证明有关案件事实的内容的录音带、录像带、电影胶片、电子计算机的磁盘等，以其所载的音响、活动影像和图形，以及电子计算机所存储的资料等来证明案件事实的证据。”参见陈光中主编：《刑事诉讼法》（第三版），北京大学出版社、高等教育出版社 2009 年版，第 205 页。在这一界定中，至少有一部分电子数据，即电子计算机所存储的资料，被纳入到视听资料的范畴。

〔5〕 当然，基于实践需要，对于“案件发生过程中”不应作过于狭义的把握，从而理解为必须是实行行为发生过程中。例如，性侵害犯罪发生前行为人与被害人往来的短信、网络诈骗实施前行为人设立的钓鱼网站等，只要与案件事实相关的，均可视为“案件发生过程中”形成的电子数据。

改,故一般认为其具有易变性的特征。因此,如何确保收集、提取的电子数据不被篡改、破坏,即保证电子数据的完整性,是电子数据收集提取和审查判断过程中需要特别把握的一个问题。

从《刑事电子数据规定》中不难发现,电子数据完整性是真实性的要素之一,甚至是最重要的要素。第23条规定对电子数据真实性的判断,应当着重审查电子数据的完整性是否可以保证;〔6〕第24条规定根据保护电子数据完整性的方法相应验证电子数据是否完整。〔7〕可见,电子数据的完整性是真实性的前提和基础,如果电子数据缺乏完整性,则自然无法保证其真实性,其所表达的内容或者证明的事实就可能并非客观存在的。

三　刑事电子数据的收集与提取

(一)电子数据的取证主体与取证方法

就取证方法与过程而言,电子数据与传统物证差异明显,前者对取证人员的专业知识和技术水平以及取证设备有特别要求。基于此,《意见》要求由二名以上具备相关专业知识的侦查人员收集、提取电子数据,并确保取证设备和过程符合相关技术标准。〔8〕随着时间和技术的发展,上述规定存在不适应司法实践具体情况的情形。因此,《刑事电子数据规定》对上述规定作了进一步完善,主要表现为两个方面:

其一,关于取证主体。《意见》要求由二名以上具备相关专业知识的侦查人员对电子数据进行收集、提取。目前,网络犯罪迅速蔓延且传统犯罪日益向互联网迁徙,不少刑事案件涉及电子数据的收集与提取,传统而言通常由网警负责的电子数据收集提取活动已经呈现出普及化的态势。目前,经侦、治安、刑侦、禁毒等警种甚至派出所都需要参与电子数据的收集提取工作,这就使得收集提取电子数据成为了一项基础性、普遍性侦查工作,因此要求取证人员一律必须具备相应的专业知识并不现实。在此背景之下,《刑事电子数据规定》第7条顺应当前司法实践的发展变化,取消了"收集、提取电子数据应当由具备相关专业知识的侦查人员进行"的规定,只是要求由二名以上侦查人员进行。〔9〕

其二,关于取证方法。《意见》第13条要求取证设备和过程符合相关技术标准。但从实践来看,上述规定也不符合实际情况:一方面,取证设备必须根据信息网络技术的发展不断完善,不断研发新型取证设备,这就可能使得相关技术标准很难跟得上取证设备的发展;另一方面,实践中还可能出现没有现成取证设备,不得不在现场研发取证设备的情况。无论是新型取证设备,还是侦查人员现场研发的取证设备,都极可能出现没有相应技术标准的情形,如果以取证设备没有技术标准为由,将所收集、提取的电子数据排除,显然不合适。为此,《刑事电子数据规定》第7条对取证方法符合相关技术标准作了规定,而

〔6〕 参见《刑事电子数据规定》第22条。

〔7〕 参见《刑事电子数据规定》第23条,这几项内容与第5条规定收集提取电子数据应当采取的完整性保护方法相对应。

〔8〕 参见《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》第13条。

〔9〕 当前,随着公安机关对电信诈骗等网络犯罪的办理经验愈加丰富,吸收相关网络技术人员参与案件侦查的现象日益多见。需要注意的是,此种情形下仍然是侦查人员作为取证主体,相关网络技术人员只是提供协助。

对取证设备的技术标准问题未再作规定。

(二)电子数据的取证规则

《解释》第 93 条对电子数据的审查判断作了明确要求,并确立了“以收集原始存储介质为原则,以直接提取电子数据为例外”的规则。《意见》对上述规则予以沿用。《刑事电子数据规定》第 8 条、第 9 条进一步完善了上述取证规则,正式确立了“以扣押原始存储介质为原则,以提取电子数据为例外,以打印、拍照、录像等方式固定为补充”的规则。

1.“原始存储介质”的概念

传统证据法坚持原始证据的优先性,要求据以定案的物证应当是原物,据以定案的书证应当是原件,从而限制物证复制品、书证复制件的证明力,以保障物证、书证的真实性,防止物证、书证在传播、复制过程中出现失真的现象,避免法官在采纳证据、认定事实方面出现错误的判断。[10] 然而,与传统证据种类不同,电子数据领域不存在“原始电子数据”的概念。其原因恰恰在于电子数据可以完全同原始存储介质相分离,而这是物证、书证等其他证据种类无法做到的。例如,就书证而言,无法确保复制件同原件的完全一致性。因此,书证的原始内容无法同原始载体完全分离开来,只能存在于原始的纸张这一载体之上。而且,不仅以物证、书证为代表的传统证据如此,就是视听资料这一新型证据亦是如此。[11] 而由于电子数据的电子性,其可以同原始存储介质分离开来,对其进行的复制可以确保与原始数据的完全一致性。例如,Word 文档等电子数据,可以同原始存储介质分开,并存储于移动存储介质之中,且可以做到复制后数据与原始数据的完全一致。基于此,“原始电子数据”概念没有实际意义,复制后的电子数据,只要与原始数据完全一致,同样可以用于证明案件事实。但是,基于保证电子数据真实性和完整性的考虑,有必要使用“电子数据原始存储介质”概念,以表明电子数据是存储在原始的介质之中,而非通过其他存储介质直接从原始介质中提取电子数据。以此为标准,可以将电子数据分为两类,即随原始存储介质移送的电子数据和在无法移送原始存储介质的情况下(如大型服务器中的电子数据)通过其他存储介质收集的电子数据。

2. 扣押、封存原始存储介质

根据《刑事电子数据规定》第 8 条第 1 款的规定,[12] 收集、提取电子数据应当优先扣押、封存原始存储介质。同时,根据《刑事电子数据规定》的规定,应当采取专门的措施对原始存储介质进行封存,以确保在不解除封存状态的情况下,无法增加、删除、修改电子数据。[13]

---

〔10〕 参见陈瑞华著:《刑事证据法学》(第二版),北京大学出版社 2014 年版,第 114 - 115 页。

〔11〕 需要注意的是,这一论断的前提是,随着电子数据成为独立的证据种类,以电子数据形式存在的视听资料是电子数据,不再属于视听资料的范畴。

〔12〕 参见《刑事电子数据规定》第 8 条第 1 款。

〔13〕 具体而言,《刑事电子数据规定》要求“封存电子数据原始存储介质,应当保证在不解除封存状态的情况下,无法增加、删除、修改电子数据。封存前后应当拍摄被封存原始存储介质的照片,清晰反映封口或者张贴封条处的状况。”“封存手机等具有无线通信功能的存储介质,应当采取信号屏蔽、信号阻断或者切断电源等措施。”当然,实践中封存原始存储介质的方法灵活多样,既可以装入物证袋封存,又可以通过对电源接口以及机箱螺钉处加贴封条达到封存目的。但是,对于手机等具有无线通信功能的存储介质,除采取普通封存方式(如装入物证袋封存)外,还应当附加其他保护措施,如拔出电池,设置为飞行模式且关闭“寻回”功能,或者直接装入屏蔽袋(盒)。

3. 提取电子数据

根据《刑事电子数据规定》第 9 条的规定，在无法扣押原始存储介质的情况下，可以提取电子数据，包括直接提取电子数据和通过网络在线提取电子数据。具体而言，提取电子数据，主要针对电子数据量过大〔14〕、电子数据存储方式〔15〕、电子数据原始存储介质存放地点〔16〕以及由于其他原因而无法扣押原始存储介质的情形。

4. 通过其他方式固定

实践中，对于有些涉案电子数据，可能出现既不便扣押原始存储介质，也无法提取电子数据的情形。〔17〕 对此，《刑事电子数据规定》第 10 条作了补充规定，允许此种情形下采用其他方式对相关电子数据加以固定，包括打印、拍照、录像等方式。可见，《刑事电子数据规定》对电子数据取证规则作了进一步完善发展，在“以扣押原始存储介质为原则，以直接提取电子数据为例外”规则的基础上，增加规定“以打印、拍照、录像等方式固定为补充”，从而使得电子数据取证规则更为周延，能够更好地适应复杂的具体情况，满足司法实践所需。

（三）电子数据的冻结

在云计算、大数据环境下，海量数据可能难以扣押、封存、提取。针对此种情形，电子数据的冻结应运而生。传统刑事诉讼领域的“冻结”，是指侦查机关根据侦查犯罪的需要，在必要时依法冻结犯罪嫌疑人在金融机构、证券公司、邮电机关或企业的存款、汇款、债券、股票、基金份额等财产的一种侦查活动。〔18〕 而在云计算、大数据环境下，越来越多的电子数据存储在云系统或者大型在线系统中，使得电子数据原始存储介质无法封存，而且难以直接提取，从而影响了侦查工作的正常开展。为适应实践需要，《刑事电子数据规定》专门规定了电子数据的冻结。

1. 电子数据冻结的适用情形

根据《刑事电子数据规定》第 11 条的规定，对于具体所列情形的，经过特定的批准程序，可以冻结电子数据。具体而言，冻结电子数据，主要针对电子数据数量大、〔19〕提取时

〔14〕 对于原始存储介质不便封存的，可以提取电子数据。从实践来看，有些情况下难以将原始存储介质封存或者全盘复制、提取，比如网络服务器一般采取集中存储的方式，其硬盘动辄成百上千 T，其中很多内容与案件无关，不必收集，在这种情况下一般只提取与案件相关的部分数据。

〔15〕 对于计算机内存数据、网络传输数据等不是存储在存储介质上的电子数据，自然无法封存原始存储介质。而且，这些信息必须在开机运行的状态下获取，一旦关机或者重新启动系统，电子数据就会消失，难以再次获取。当然，此处的“存储介质”以稳定存储为前提，如果不作此限定，则传输电子数据的网线也可能瞬间存储电子数据，可以成为存储介质。这有悖于一般人的认知，明显不妥。

〔16〕 对位于境外的服务器无法直接获取原始存储介质，一般只能通过网络在线提取电子数据。对于远程计算机信息系统上的电子数据，也可以通过网络在线提取。

〔17〕 例如，实践中数额较小的网络侵财类案件不仅数量大、而且涉及老百姓切身利益，社会广泛关注。这类案件大部分由派出所管辖，往往没有专业取证设备，无法提取电子数据，而受害人即使报案也不愿将手机交给公安机关。又如，目前市场上出现了一种“阅后即焚”的通信模式，越来越多的即时通信软件具备了“阅后即焚”功能（比如“支付宝”和“钉钉”的即时通信软件）。信息接收者收到信息后，点击阅读信息数秒后自动删除，无法及时提取数据，并且难以恢复，即使扣押封存了也毫无意义。再如，船舶的导航系统等部分工控系统，只有操作界面，无接口可以导出数据，也无法把整个船舶或者大型系统扣押。

〔18〕 参见陈光中主编：《刑事诉讼法》（第六版），北京大学出版社、高等教育出版社 2016 年版，第 303 页。

〔19〕 数据量大，无法或者不便提取的，可以冻结电子数据。例如，在一起传播淫秽物品牟利案中，涉案 70 个网络云盘涉及淫秽视频 150 余万部，共 1000T，按照传统固定证据方式，需要 2T 硬盘 500 块，是该市电子数据取证过去十年消耗硬盘的总和。

间长、[20]直接展示困难[21]以及由于其他原因需要冻结电子数据的情形。

2. 电子数据冻结的具体程序

《刑事电子数据规定》对冻结电子数据的文书要求、协助部门以及解除冻结相关问题作了明确规定。[22] 从实践操作来看,部分网络服务提供商已经在开展数据冻结服务,从技术操作的层面来看完全可行。根据实践情况和相关技术原理,《刑事电子数据规定》进一步规定了具体冻结措施,[23]以确保冻结状态下的电子数据不被增加、删除、修改,确保完整性。当然,上述规定只是原则性规定,从具体操作的角度,有关侦查主管部门宜进一步评估现行电子数据冻结操作实践,对相关问题作进一步研究,进而就电子数据冻结的具体技术问题制定相应行业标准,以切实增强可操作性。

(四)电子数据的检查

就传统证据而言,无论是书证还是物证,侦查过程通常只涉及现场侦查和鉴定两个阶段,主要侦查工作通过前一阶段的勘验、搜查、提取、扣押等可以完成,对于专门性问题的判断通过后一阶段可以解决。然而,对于电子数据而言,上述两个阶段可能尚难以完成全部侦查任务。例如,对现场提取的加密电子数据无法直接移送的,应当进一步解密;对现场制作的存储介质镜像文件由于数据删除也无法直接移送的,应当进一步恢复提取被删除的数据。实践中,无论是电子数据的解密,还是电子数据的恢复,通常都难以在现场完成,但也不宜都作为专门性问题通过鉴定作出判断。基于此,在电子数据现场取证和专门性问题判断的鉴定程序之间亟须增加一个阶段,即电子数据的检查环节,以作为现场取证工作的自然延续,但也不属于对专门性问题作出判断的鉴定程序。按照上述思路,《刑事电子数据规定》第 16 条对电子数据检查的有关问题作了明确。[24]

上述规定施行以来,司法实践中存在较大争议的问题是,对于电子数据的检查是否需要见证人。见证人制度是我国刑事诉讼制度的重要组成部分。在刑事诉讼中,一些活动需要见证,以确保公安司法人员进行刑事诉讼活动的合法性,以及对相关笔录和清单记载的真实性,保证刑事司法公正。《刑事电子数据规定》明确了收集、提取电子数据的见证人,要求除客观原因外应当依照刑事诉讼法的规定由符合条件的人员担任见证人。[25] 需要注意的是,应当依据《刑事诉讼法》的规定判断相关电子数据取证活动是否需要由见证

〔20〕 提取时间长,可能造成电子数据被篡改或者灭失的,可以冻结电子数据。例如,在一起网络贩卖、传播淫秽视频案中,共查扣涉案网盘近千个,按照一条 100 兆光纤(属较高级别带宽)下载速度及运行商能够提供的最高限速,在全程无中断情况下,预计时间为 15 至 16 个月。又如,四川绵阳“12·21”云盘传播淫秽物品案也反映了云盘案件中对电子数据采用传统方式提取存在的困难。据介绍,涉案的一个“母盘”账号就是 5T 内容,电脑工作 24 小时也需要下载整整五天时间。参见《四川破坏网络云盘传播淫秽视频案》,《法制日报》2016 年 4 月 12 日第 8 版。

〔21〕 通过网络应用可以更为直观地展示电子数据的,可以冻结电子数据。例如,在一起非法集资案中,大量电子数据是从云系统提取的,这些数据只有在云环境下才能方便查看、筛选,为提取后查看、筛选这些数据,侦查机关不得已耗费了大量人力物力又搭建了一个相同的云环境,增加了不必要的办案成本。

〔22〕 参见《刑事电子数据规定》第 12 条第 1 款。

〔23〕 参见《刑事电子数据规定》第 12 条第 2 款。

〔24〕 参见《刑事电子数据规定》第 16 条第 1 款。

〔25〕 参见《刑事电子数据规定》第 15 条。

人进行见证。[26] 目前，并无规定明确要求见证人对电子数据检查进行见证，故不能以电子数据的检查环节没有见证人为由而认为其所获取的电子数据不具有完整性、真实性。从实践来看，要求电子数据的检查环节由见证人进行见证不符合现实情况，且国外电子数据的检查环节也并无此类规定和要求。但是，《刑事电子数据规定》对检查过程中电子数据的真实性、完整性的保护问题作了专门规定。根据《刑事电子数据规定》第16条第2款的规定，对于电子数据检查，首先要求对存储介质的拆封过程进行录像；[27] 而且，此后对存储介质的检查，应当优先通过写保护设备或者制作备份的方式进行检查，即使由于客观原因无法使用写保护设备且无法制作备份的，作为补充，也要求对相关活动进行录像。实际上，上述规定严于见证人制度的要求，只要落到实处，完全可以确保电子数据的完整性。

（五）电子数据专门性问题的判断

办理网络犯罪案件，就电子数据而言，经常会涉及计算机病毒、计算机程序功能、数据同一性认定等专门性问题。根据实践所需，《刑事电子数据规定》对电子数据专门性问题的判断确立了鉴定意见与报告“两条腿走路”的原则。

1. 鉴定意见与报告“两条腿走路”

自2005年10月1日起施行的由全国人民代表大会常务委员会制定的《关于司法鉴定管理问题的决定》对司法鉴定工作进行统一规范管理。根据该规定，国家对从事法医类鉴定、物证类鉴定、声像资料鉴定以及根据诉讼需要由司法部与“两高”协商确定的其他应当对鉴定人和鉴定机构实行登记管理的鉴定事项[28]的鉴定人和鉴定机构实行登记管理制度。需要注意的是，法律对上述事项的鉴定人和鉴定机构的管理另有规定的，从其规定。

根据《刑事诉讼法》第50条的规定，鉴定意见是证据的种类之一。鉴定意见和其他证据种类一样，必须经过审查判断，确定属实的，才能作为定案的根据。由于鉴定要求对刑事诉讼中的专门性问题作出判断，为确保鉴定意见的可靠性，必须要求鉴定机构和鉴定人具有相应的资质。因此，根据《刑事诉讼法》和有关规定，对鉴定机构和鉴定人法定资质的审查是重要内容。

当前，我国司法鉴定体制处于改革转型的过程，客观上出现了司法鉴定机构和鉴定人一定程序欠缺的问题。[29] 作为应对措施之一，一些司法解释规定可以委托司法鉴定机构

---

〔26〕《刑事诉讼法》对于见证人对侦查活动进行见证的规定，主要有第133条、第139条第1款、第140条以及第142条。

〔27〕与之相呼应的是，如前所述，《刑事电子数据规定》第8条第2款针对电子数据的存储介质作出了“封存前后应当拍摄被封存原始存储介质的照片，清晰反映封口或者张贴封条处的状况”的规定。

〔28〕2016年1月，最高人民法院、最高人民检察院、司法部和环境保护部就环境损害司法鉴定实行统一登记管理和规范环境损害司法鉴定工作作出明确规定。这是《关于司法鉴定管理问题的决定》施行以来，就“其他应当对鉴定人和鉴定机构实行登记管理的鉴定事项”作出的唯一具体规定。

〔29〕对于法医类鉴定、物证类鉴定、声像资料鉴定“三大类鉴定”以外的鉴定事项，部分地方司法行政机关赋予了其司法鉴定资质，实际上也有违《关于司法鉴定管理问题的决定》的规定。因为对于三大类鉴定以外的鉴定事项，系“由国务院司法行政部门商最高人民法院、最高人民检察院确定的其他应当对鉴定人和鉴定机构实行登记管理的鉴定事项”，并不应当由司法行政机关直接予以确定。

以外的相关机构就专门性问题出具报告。[30] 这些部门所出具的报告，可以作为定罪量刑的参考，这是解决这一问题的妥善办法。相应而言，司法机关结合案件情况对出具的报告进行审查，并根据具体情况可以作为证明案件事实的参考。对此，《解释》第 87 条第 1 款作了专门规定，进一步规范了报告的相关问题。[31]

2. 电子数据专门性问题的鉴定意见与报告

目前，具有电子数据鉴定资质的机构[32]偏少，难以满足办案需求。为确保相关案件的及时、顺利办理，经综合有关方面意见，《意见》规定对网络犯罪案件中相关电子数据涉及的专门性问题，既可以由司法鉴定机构出具鉴定意见，也可以由公安部指定的机构出具报告，即鉴定意见与报告“两条腿走路”。在此基础上，《刑事电子数据规定》第 17 条作了进一步完善，将上述规则扩展到所有刑事案件相关电子数据涉及的专门性问题难以确定的情形。

鉴定意见系《刑事诉讼法》规定的法定证据种类，而报告系《解释》在总结司法实务经验基础上作出的专门规定，前者可以作为定罪量刑的根据，而后者可以作为定罪量刑的参考。因此，在规定对电子数据专门性问题的鉴定意见与报告“两条腿走路”后，司法实践中面临的问题是如何取舍鉴定意见与报告。对于相关电子数据专门性问题鉴定意见与报告并存的情况下，特别是对于鉴定意见与报告提出的意见不同时，如何处理，存在不同认识。本文认为，在电子数据鉴定意见与报告“两条腿走路”原则的基础上，不能仅凭形式而当然地采纳鉴定意见，适宜的做法是作实质审查判断。实际上，证据的外延较为宽泛，可以用于证明案件事实的材料都属于证据的范畴。特别是，电子数据的判断较为复杂，在存在不同认定意见的情况下，对鉴定意见和报告不能仅凭形式作出取舍，而应进一步审查，有利于对专门性问题作出准确判断，确保案件的公正处理。

四 刑事电子数据的移送与展示

（一）电子数据的备份移送

为防止电子数据移送后出现被增删改的情形，在可能的情况下，后续环节的审查判断通常都是针对电子数据的备份进行。基于此，《刑事电子数据规定》要求随同移送电子数据的备份。需要注意的是，一律要求对全部电子数据制作备份，既无必要，也不便利。故而，对于此处规定的备份的具体范围，通常应当理解为与案件事实相关的电子数据。

（二）电子数据的打印件

以电子数据是否可以直接展示作为标准，电子数据可以分为可以直接展示的电子数

〔30〕 参见最高人民法院、最高人民检察院《关于办理盗窃刑事案件适用法律若干问题的解释》第 4 条第 1 款第 1 项。此处的“委托估价机构估价”，实际上就是由价格认证机构对价格进行认证，而这也不是司法鉴定，所出具的价格认证报告也不是鉴定意见而是报告。

〔31〕 参见《解释》第 87 条第 1 款。

〔32〕 司法实践中，对于电子数据鉴定是否属于《关于司法鉴定管理问题的决定》规定的三大类鉴定事项，也存在不同认识。

据和无法直接展示的电子数据，前者如电子文档、图片等，后者如计算机病毒、木马程序等。对于前者，特别是在电子文档等特别大，导致打印件的数量繁多的情况下，宜直接展示电子数据进行查看，没有必要移送打印件；而后者根本没有打印件，自然不存在打印件的移送问题。

基于上述考虑，《解释》未规定移送电子数据的打印件。然而，司法实践中，受制于技术设备的原因，不少庭审仍主要通过打印件对电子数据进行审查判断。基于此，《意见》专门规定，在检察部门和法院受技术条件限制的情况下，公安机关应当随案移送打印件。《刑事电子数据规定》在上述规定的基础上，进一步对可以直接展示的电子数据的打印件问题区分情况作出规定。[33]

对于计算机病毒、木马程序等无法直接展示的电子数据，自然无法随案移送打印件。鉴于此类电子数据的审查判断专业性较强，为便于后续审查判断，《意见》要求作出相关说明并随案移送。《刑事电子数据规定》重申了上述原则。[34]

五　刑事电子数据的审查与判断

（一）电子数据真实性的审查与判断

电子数据本身是现代科技、特别是信息网络技术发展的产物，故对电子数据的审查判断、特别是真实性的审查判断，不可避免地具有技术性色彩。因此，《刑事电子数据规定》第22条在充分考虑电子数据技术性的基础上，根据实践反映的情况，规定了如下几个方面对电子数据的真实性作出审查判断：（1）对是否优先封存原始存储介质以及对原始存储介质的相关问题进行审查。（2）对数字签名[35]、数字证书[36]等特殊标识进行审查。对于具有数字签名、数字证书等特殊标识的电子数据，可以通过数字签名或者数字证书以判断相关电子数据是否真实。实践中，对数字签名、数字证书的验证，可以通过审判人员自行验证、技术人员验证和侦查人员验证等多种方式进行，实践中可以自行掌握。[37]（3）对电子数据收集、提取过程是否可以重现进行审查。例如，在判断电子数据检查过程中从扣押的原始存储介质中恢复的电子数据是否真实时，就可以对数据进行再次恢复，并比较两次数据恢复的内容是否相同，从而对电子数据是否真实作出准确判断。[38]（4）对电子数据是否存在增删改的情形进行审查。电子数据发生增加、删除、修改的，并不必然

〔33〕 参见《刑事电子数据规定》第18条第2款。

〔34〕 参见《刑事电子数据规定》第19条第1款。

〔35〕 数字签名是指利用特定算法对电子数据进行计算，得出的用于验证电子数据来源和完整性的数据值。

〔36〕 数字证书是指包含数字签名并对电子数据来源、完整性进行认证的电子文件。

〔37〕 并非所有的电子数据都有数字签名或者数字证书，自然不能因为相关电子数据没有数字签名或者数字证书就认为其不真实。

〔38〕 实践中并非所有的电子数据收集、提取过程都可以复现。例如，拒绝服务攻击案件中从网络截取的攻击数据包，或者从计算机内存中提取的电子数据，这些数据在拒绝服务攻击结束或者计算机关机后就会消失，收集、提取过程无法复现。因此，不能因收集、提取过程不能重现就否定电子数据的真实性。

导致其不真实,例如基于正常使用的目的对电子数据进行修复的情况。[39] 因此,审查发现电子数据存在增删改的情形时,应当进一步查明原因和具体情节,以判断是否出于善意,从而区别对待。如果是基于善意的目的,为了顺利展示或者分析电子数据而作上述操作,对电子数据证明的事实没有影响,可以认为其是真实的;如果是基于非善意的目的,特别是故意篡改电子数据的,则应当认定其是不真实的。(5)对电子数据的完整性进行审查。《刑事电子数据规定》仍然从真实性、合法性、关联性的角度对电子数据提出审查要点,但要求在审查真实性的同时对完整性作出判断。

(二)电子数据关联性的审查与判断

随着电子数据取证的逐步规范,司法实践中对电子数据的真实性和合法性的争论逐渐减少。但是,对于电子数据与待证事实是否存在关联,则可能是未来审查判断刑事电子数据的关键与重点。只有与案件事实存在关联的电子数据,才能作为证据使用;不存在关联的,不应当作为证据使用。考虑到关于电子数据关联性的理论研究和实践经验相对薄弱,《刑事电子数据规定》仅对电子数据的关联性审查与判断作出原则性规定,留待将来进一步丰富完善。

根据《刑事电子数据规定》,电子数据关联性涉及虚实对应和人机关联两个方面。[40] 针对司法实践中经常遇到的虚拟身份与真实身份对应的判断难题,《刑事电子数据规定》要求综合各种证据材料进行判断,以确定网络身份与现实身份的同一性。[41] 针对行为人与存储介质关联判断的难题,《刑事电子数据规定》强调通过相关证人证言和口供辩解等证据材料综合作出判断。[42] 需要强调的是,司法实践中还应当重视提取包括指纹、DNA 等在内的痕迹物证,以综合判断存储介质是否与行为人存在关联。此外,由于技术原因,电子数据的形式多种多样、涉及面较宽,因而涉及案件事实的电子数据的范围也相应较宽。因此,在司法实践中,要注意全面收集与案件事实有关联的电子数据、包括外围数据,避免有所遗漏。特别是对于犯罪嫌疑人删除或者由于其他原因被删除的电子数据,应当借助一定的技术手段予以恢复,以更为全面地证明案件事实。通过全面综合审查,审查电子数据之间以及电子数据与其他证据之间的关系,从而确认电子数据与待证事实之间的关系。

六 结 语

无论是收集提取,还是移送展示,抑或审查判断,作为证明案件事实的证据种类之一的电子数据,相关证据规则必须符合刑事诉讼法对证据的一般要求,必须符合现代法治的

〔39〕 例如,为了使部分损坏的视频文件能够正常播放,在视频文件的文件头增加某些信息;为了查看乱码电子文档,修改文档文件头的某些字节;或者为了打开部分损坏的电子图片,对文件错误的字节进行修改。

〔40〕 这实际上也是有论者所概括的电子数据的“双联性”,即内容关联性与载体关联性。前者是指“电子证据的数据信息同案件事实之间的关联性”,后者是指“电子证据的信息载体同当事人或其他诉讼参与人之间的关联性”。参见刘品新:《电子证据的关联性》,《法学研究》2016 年第 6 期,第 175 页。

〔41〕 参见《刑事电子数据规定》第 25 条第 1 款。

〔42〕 参见《刑事电子数据规定》第 25 条第 2 款。

基本要求。但是,电子数据是现代科学技术、特别是信息技术发展的产物,故对其规制必须考虑相关技术特性,遵循相关技术标准。因此,电子数据证据规则的建构,必须基于法律和技术两个维度,才能规范电子数据的提取和运用,确保电子数据的真实性、合法性和关联性,促进电子数据更好地发挥证明案件事实的作用。

在我国刑事电子数据规制体系已经初步构建的背景下,对于电子数据的研究和关注重点应当从宏观转向微观,从理论转向实务,从应然转向实然。特别是,《刑事电子数据规定》的相关条文在具体运用中仍存在一些争议问题。这需要电子数据理论研究加以关注,更需要有关部门在深入调研的基础上作出进一步细化规定,[43]以统一司法适用。

[**Abstract**] With the rapid development of modern science and technology, the types of legal evidence have been continuously expanded and improved. As a new type of legal evidence in the 2012 Criminal Procedure Law, electronic data plays an increasingly important role in ascertaining the facts of the case. In light of the new situation of and new problems in judicial practice, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security and other government departments have adopted a series of judicial interpretations and other normative documents that contain comprehensive provisions on the collection, extraction, transfer, display, review and determination of electronic data, thereby establishing a preliminary criminal electronic data regulation system. This paper reviews different approaches to the regulation of criminal electronic data in China and, based on the discussion of such general issues as the definition and integrity of electronic data, analyzes the key issues of collection, extraction, transfer, display, review and determination of electronic data, as well as the controversies in judicial practice over subjects of evidence taking, requirements of forensic methods, rules on the collection, freezing, and inspection of evidence, determination of special issues, backup transfer and printing, and the review and determination of authenticity and relevance.

(责任编辑:郑　佳)

〔43〕 2018 年 12 月,公安部印发《公安机关办理刑事案件电子数据取证规则》(公通字〔2018〕41 号),自 2019 年 2 月 1 日起施行。该规则实际上就是根据《刑事电子数据规定》的相关要求,对公安机关办理刑事案件收集、提取涉案电子数据作出的进一步细化规定。