检察调研与指导

JIANCHA DIAOYAN YU ZHIDAO

2016年第6辑
（总第13辑）

最高人民检察院法律政策研究室主办

总顾问 | 柯汉民　　主　编 | 万　春

中国出版集团
研究出版社

检察调研与指导

JIANCHA DIAOYAN YU ZHIDAO

2016年第6辑
（总第13辑）

最高人民检察院法律政策研究室主办

顾问｜柯汉民　　主　编｜万　春

中国出版集团
研究出版社

图书在版编目（CIP）数据

检察调研与指导．2016年．第6辑／万春主编．—北京：研究出版社，2016. 12

ISBN 978-7-80168-985-6

Ⅰ．①检… Ⅱ．①万… Ⅲ．①检察机关－工作－中国－文集

Ⅳ．①D926.3-53

中国版本图书馆CIP数据核字（2016）第305924号

检察调研与指导（2016年第6辑）

作　　者　万春　主编

责任编辑　李鹏

出版发行　研究出版社

地　　址　北京市东城区沙滩北街2号中研楼

电　　话　（010）53390190　55602355

网　　址　www.yjcbs.com

印　　刷　北京明月印务有限责任公司

开　　本　787mm×1092mm　1/16

印　　张　8.5

版　　次　2016年12月第1版　2016年12月第1次印刷

书　　号　ISBN 978-7-80168-985-6

定　　价　30.00元

目录 CONTENTS

·司改前沿·

·实务研究·

《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

万 春 王建平 吴孟栓 高翼飞*

2016年9月9日，最高人民法院、最高人民检察院、公安部联合下发了《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《规定》），自2016年10月1日起施行。《规定》是目前国内第一部系统规定刑事诉讼中电子数据取证和认证规则的司法解释性质文件，对于解决电子数据取证难、认证难问题，提高刑事案件的办理质量和效率具有重要意义。为了便于准确理解和掌握《规定》的内容，现就《规定》的主要问题作出解读。

一、《规定》制定的背景和过程

随着计算机技术的广泛运用，社会对计算机信息系统的依赖程度越来越高，计算机和移动电子设备已经走进千家万户，广泛应用于人们的工作和生活等各个领域，利用计算机实施犯罪的问题也随之产生。自我国1986年首次发现利用计算机仿造银行存折和隐形印鉴诈骗银行巨款案以来，利用计算机实施盗窃、贪污、挪用公款、窃取国家秘密等犯罪案件时有发生，犯罪的涉案金额和造成的社会危害也越来越大。随着互联网的发展，网上银行、网上购物等网络经营活动已经普及，同时也给犯罪分子利用互联网实施犯罪提供了更大的空间。近年来，非法侵入计算机信息系统、破坏计算机信息系统、非法获取计算机信息系统数据等新型高科技犯罪案件层出不穷，各类网络犯罪“推陈出新”。绝大部分犯罪案件都涉及电子数据的收集提取问题，而电子数据又有着传统证据所不具有的新特点。为适应现代信息技术的发展，根据刑事诉讼中出现的新情况和实践需要，2012年刑事诉讼法修改时将电子数据增设为法定证据种类，进一步丰富了证据的外延，同时也对电子数据收集、移送和审查判断提出了新课题。2012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《刑事诉讼法解释》）明确了电子数据审查与认定的基本原则。2014年《最高人民法院、最高人民检察院、公安部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》）对电子数据的收集主体、方式，电子数据的移送和涉及专门性问题的鉴定与检验等问题加以明确。但是，目前在司法实践中，关于电子数据的取证和认证规则仍较

* 作者单位：最高人民检察院法律政策研究室。

为原则，侦查机关如何收集电子数据，检察机关和审判机关如何审查判断电子数据还缺乏细致的规定，比如，如何提取电子数据，如何保护电子数据的完整性，在无法封存原始存储介质和提取电子数据的情况下如何固定证据，在特定情况下能否要求网络服务提供者协助冻结电子数据以及冻结的程序要求，等等，亟待作出明确。实践中，侦查机关、检察机关和审判机关对于电子数据应当符合什么样的条件才能作为定案根据有不同认识，电子数据依然存在采信难的问题，绝大部分电子数据仍需要转化为书证、视听资料或者鉴定意见。为了进一步明确电子数据收集提取和审查判断规则，解决电子数据取证难、认证难的突出问题，着力提高刑事案件的办案质量和效率，依法惩罚犯罪和保障人权，最高人民法院、最高人民检察院和公安部共同研究起草了《规定》。《规定》初稿由公安部网络安全保卫局、公安部法制局会同上海、河北、安徽、重庆、浙江等基层公安机关网安部门联合起草，听取了奇虎360科技有限公司、腾讯公司等社会机构的意见，并征求了公安部国内安全保卫局、经济犯罪侦查局、治安局、刑侦局、技侦局、法制局、禁毒局、反恐局、情报中心和中国人民公安大学的意见。2015年7月和2016年6月，最高人民法院研究室、最高人民检察院法律政策研究室、公安部网络安全保卫局先后在重庆、厦门两次召开座谈会，广泛听取地方公检法部门和相关法学专家、技术专家的意见。会后，三家又召开会议，对《规定》中的主要问题和相关条文进行了集中研究和修改，并征求了全国人大常委会法工委的意见。各方就《规定》的相关问题达成一致意见后，于2016年9月会签印发。

二、《规定》的指导思想

《规定》在研究起草过程中始终注意坚持和贯彻以下指导思想：一是坚持同上位法和相关司法解释及司法解释性质文件保持协调一致和衔接。对于电子数据取证涉及的程序性问题，如初查的要求、技术侦查措施的适用条件等，刑事诉讼法和相关司法解释、规范性文件有详细规定的，按照有关规定执行，《规定》中不再规定；对有关规定已经作出明确规定的电子数据取证方法，在实践中执行良好的，《规定》予以保留；对虽有规定但不符合实际需要的，《规定》予以完善；对有关规定仅作出原则性规定的，《规定》予以具体化，使其更具有可操作性；对没有明确规定但在长期实践中形成的较为成熟的做法，《规定》予以明确，进一步完善了电子数据证据规则体系。二是坚持问题导向，切实进行明确和规范。从实际出发，对实践中反映出的电子数据取证难点问题作出了回应，如明确了电子数据冻结等新的证据收集、固定方式，尽可能满足办案实践的需要。同时，坚持以审判为中心，按照裁判的标准和要求，完善电子数据证据取证和审查判断规则。明确侦查机关应当遵守法定程序，遵循有关技术标准，全面、客观、及时地收集提取电子数据；人民检察院、人民法院应当围绕真实性、合法性、关联性审查判断电子数据。并且针对电子数据的特殊性，强调了对电子数据完整性的保护和审查。三是始终坚持打击犯罪与保障人权并重。在各个环节严格规范侦查机关收集固定电子数据的侦查活动，强调在电子数据取证过程中，要严格依照刑事诉讼法规定的程序收集提取电子数据，注重保护国家秘密、商业秘密、个人

隐私以及公民的通信自由和通信秘密。

三、电子数据的界定

长期以来，理论界和实践中对电子数据概念的界定不是十分清晰，有的将通过电子设备存储的资料纳入视听资料的范畴，也有的将这类资料称为“电子物证”或者将其视为书证的一种，但随着对电子数据认识的逐步深入，并且由于2010年“两个证据规定”率先将“电子证据”作为证据类型加以规定，电子数据逐渐取得了独立于视听资料等传统证据的地位。2012年刑事诉讼法修改，正式将电子数据作为法定的证据种类，但没有明确电子数据的内涵和外延。电子数据与书证、视听资料等传统证据之间存在一定交叉。

目前，有关司法解释和规范性文件对电子数据的定义主要有两种方式。一种是对常见的电子数据形式进行列举。如《刑事诉讼法解释》第九十三条列举了电子邮件、电子数据交换、网上聊天记录、博客、微博客、手机短信、电子签名、域名等电子数据。另一种是对电子数据的本质特征进行归纳概括。如《公安机关电子数据鉴定规则》规定，电子数据系“以数字化形式存储、处理、传输的数据”。

在《规定》的制定过程中，我们就电子数据的定义进行了认真的研究，各方一致认为，概括式规定较为抽象，缺少对电子数据常见形态的示例，实践中难以准确把握电子数据的内涵；列举式规定无法揭示电子数据的本质特征，容易出现挂一漏万的问题，难以涵括未来可能出现的新的电子数据形式。采取先定性后列举的方式对电子数据的概念作出界定，有利于司法实践中准确理解其内涵和外延。因此，《规定》第一条明确了电子数据是“案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据”。电子数据的常见形态包括但不限于下列信息、电子文件：（1）网络平台发布的信息。包括网页、博客、微博客、朋友圈、贴吧、网盘等网络平台上发布的信息，此类信息通常具有公开性，但也有不公开的情形，如通过设置浏览权限由部分人浏览。（2）网络应用服务的通信信息。包括手机短信、电子邮件、即时通信、通讯群组等的通信信息。此类信息一般以通信为目的，电子数据承载着通信内容，既可以是点对点通信，如即时通信私聊信息或者两人间的电子邮件，也可以是一点对多点通信，如即时通讯群组中发送的群聊信息、群发短信或者群发电子邮件。（3）记录类信息。这类信息的特点是以电子记录的形式存在，通常以“组”或者“条”为单位，由计算机信息系统存储、处理，并通过信息网络传输。比较典型的有：涉及公民个人信息的用户注册信息，用于确认用户在计算机信息系统上操作权限的账号、口令、密码等身份认证信息，以及各类以数字化形式存在的交易记录、通信记录、登录日志等信息。（4）电子文件。包括文档、图片、音视频、计算机程序、数据库文件、网络抓包文件、数字证书等。需要强调的是，上述分类只是便于在实践中理解和掌握。由于电子数据的表现形式复杂、种类多样，各类电子数据之间可能存在交叉，比如，数字证书本身是电子文件，当被用于确认用户在计算机信息系统上的操作权限时，又属于身份认证信息；再如，计算机信息系统日志，如果提取的是一条一条的记录，那么可以归为记录类信息，如果提取的是存储记录的数据库文件，那

么又可以归为电子文件。

为了更加准确地界定电子数据，明确与其他证据形式的界限，《规定》明确了电子数据应当是在“案件发生过程中形成”的电子数据，对此应作广义理解，不仅包括犯罪行为实行阶段形成的电子数据，还包括为实行犯罪准备工具、制造条件的犯罪预备阶段形成的电子数据以及犯罪实行终了以后行为人为掩盖犯罪事实而对电子数据进行删除、修改的过程中形成的电子数据。在《规定》制定过程中，有意见提出，讯问同步录音录像和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与电子数据是否有区别？是否应当适用本规定？我们经研究认为，电子数据通常是在案件发生过程中形成的，讯问同步录音录像则在案件发生后的侦查阶段形成，属于对言词证据的记录，不属于本规定所称的电子数据。同理，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，也不属于电子数据。但考虑到上述证据材料与电子数据一样，都是以数字化形式存储的，《规定》第一条第三款规定：“确有必要的，对相关证据的收集、提取、移送、审查，可以参照适用本规定。”

四、初查过程中收集的电子数据的证据资格

初查是侦查机关依据刑事诉讼法第一百一十条的规定在立案审查阶段采取的专门调查措施，初查的任务是收集必要的证据材料，确定是否有犯罪事实并需要追究刑事责任。目前在办理各类刑事案件中采取初查措施的做法已较为普遍。尤其是在网络犯罪案件中，大量的网上违法犯罪线索如不经过初查则很难确定是否达到立案标准。例如，在电信、网络诈骗案件中，犯罪嫌疑人通常诈骗众多被害人，通过聚少成多的方式谋取大量非法利益，但实践中经常是一个被害人报案，因被骗金额达不到立案标准难以立案，而不立案又无法查询银行账户，不查询银行账户也就无法发现其他诈骗案件、认定诈骗金额。因此，在立案前赋予侦查机关采取一定调查措施的权力十分必要，但为了保护公民的人身、财产权利，这种立案前的调查措施又必须受到严格的限制，应当与立案后的侦查措施有所区别。《公安机关办理刑事案件程序规定》第一百七十一条规定：“对接受的案件，或者发现的犯罪线索，公安机关应当迅速进行审查。对于在审查中发现案件事实或者线索不明的，必要时，经办案部门负责人批准，可以进行初查。初查过程中，公安机关可以依照有关法律和规定采取询问、查询、勘验、鉴定和调取证据材料等不限制被调查对象人身、财产权利的措施。”《人民检察院刑事诉讼规则（试行）》第一百六十八条规定：“侦查部门对举报中心移交的举报线索进行审查后，认为有犯罪事实需要初查的，应当报检察长或者检察委员会决定。”第一百七十二条规定：“初查一般应当秘密进行，不得擅自接触初查对象。公开进行初查或者接触初查对象，应当经检察长批准。”第一百七十三条规定：“在初查过程中，可以采取询问、查询、勘验、检查、鉴定、调取证据材料等不限制初查对象人身、财产权利的措施。不得对初查对象采取强制措施，不得查封、扣押、冻结初查对象的财产，不得采取技术侦查措施。”根据上述规定，初查过程中不得扣押电子数据原始存储设备，也不得采取技术侦查措施，只能在勘验的过程中提取电子数

据，或者通过网络在线提取电子数据，或者向有关单位和个人调取电子数据。然而，上述司法解释和规范性文件对于初查过程中收集的电子数据能否作为证据使用并没有作出明确规定。如果初查阶段收集的电子数据不能在刑事诉讼中作为证据使用，要求侦查机关在立案后重新收集，会在很大程度上增加侦查机关的负担，并且电子数据具有易丢失、易篡改、不稳定的特点，如不及时收集、提取和固定，事后很难再重新收集。经征求立法机关意见，全国人大常委会法工委认为，根据《刑事诉讼法解释》第六十五条的规定，只要依法进行初查，其间收集提取的电子数据即可在刑事诉讼中作为证据使用。即认为公安机关在立案前开展的初查活动属于行政机关的行政执法和查办案件活动，因此在初查过程中收集的物证、书证、视听资料、电子数据等证据材料，在刑事诉讼中可以作为证据使用；经法庭查证属实，且收集程序符合有关法律、行政法规规定的，可以作为定案的根据。《人民检察院刑事诉讼规则（试行）》中也规定，人民检察院初查过程中，可以调取证据材料。所以，对检察机关在初查过程中收集的电子数据也应当确认其证据资格。为此，《规定》第六条专门规定，初查过程中收集、提取的电子证据，可以作为证据使用。

需要注意的是，《规定》第十一条、第十二条规定了“冻结电子数据”，该措施属于证据保全的方法，而不是限制财产处分的强制措施，不同于对账户资金的冻结。因此，在初查阶段，为防止电子数据被篡改或者灭失，一般可以采取冻结电子数据的措施。在一些案件中，涉案电子数据可能具有虚拟财产的属性，目前我国法律尚未承认虚拟财产，对于初查阶段能否对虚拟财产进行冻结存在争议。我们认为，涉案电子数据具有虚拟财产属性的，侦查机关在初查阶段冻结电子数据应当十分慎重，严格按照有关司法解释和规范性文件关于在初查阶段不得限制初查对象财产权利的规定，及时采取其他方式固定证据或者在立案后依法采取冻结电子数据的措施。

五、电子数据的收集与提取

（一）对取证人员和取证方法的要求

关于电子数据的取证人员，《网络犯罪刑事诉讼程序意见》规定：“收集、提取电子证据，应当由二名以上具备相关专业知识的侦查人员进行。”该规定主要是考虑到电子数据取证的技术性较强，故要求取证人员具有一定的专业知识和技术水平，但该规定只是原则性规定，对于“具备相关专业知识”没有明确具体的标准。随着信息网络技术的发展，在侦查实践中，收集、提取电子数据已经成为一项基础性、普遍性的工作，例如，过去办理网络犯罪案件通常由公安机关网安部门负责收集、提取电子数据，现在越来越多的普通刑事案件需要收集、提取电子数据，经济犯罪侦查、治安、刑事侦查、禁毒等侦查部门甚至基层派出所都承担着电子数据收集、提取任务，在电子数据取证工作普遍化的情况下，认定侦查人员是否具备相关专业知识标准模糊、不易判断。在侦查人员是否具备专业知识的问题上纠缠，可能影响侦查取证工作的开展。另外，实践中的做法是，侦查人员在扣押、封存电子数据原始存储介质后，将从原始存储介质中提取电子数据的工作交给相关技术部门或者委托鉴定机构完成。刑事诉

讼法第一百二十六条规定："侦查人员对于与犯罪有关的场所、物品、人身、尸体应当进行勘验或者检查。在必要的时候，可以指派或者聘请具有专门知识的人，在侦查人员的主持下进行勘验、检查。"在勘验、检查现场收集、提取的电子数据可以在侦查人员的主持下指派或者聘请具有专门知识的人参与，能够在一定程度上弥补侦查人员自身专业知识不足的问题。事实上，只要取证过程符合法定程序和相关技术规范，能够保证收集、提取的电子数据的真实性、完整性即可，没有必要对侦查人员具备相关专业知识作硬性规定。有鉴于此，《规定》删去了"具备相关专业知识"的内容，规定"收集、提取电子证据，应当由二名以上侦查人员进行"。虽然《规定》对专业知识不再作硬性要求，但是，为了提高电子数据取证的质量，促进取证工作的科学化、规范化，侦查机关仍然应当加强对侦查人员在电子数据取证方面的专业培训，不断增强侦查人员的电子数据取证能力。

关于电子数据取证方法，《网络犯罪刑事诉讼程序意见》规定："取证设备和过程应当符合相关技术标准，并保证所收集、提取的电子数据的完整性、客观性。"但是，实践中发现，随着科技的进步，取证设备的更新速度很快，相关技术标准很难跟得上取证设备的发展。在一些高科技犯罪案件的侦办过程中，甚至没有现成的取证设备，侦查人员只能自行开发取证工具。如果以新式取证设备和侦查人员自己开发的工具没有相关技术标准为由，将收集、提取的电子数据予以排除，显然不合适。因此，《规定》没有再对取证设备的技术标准作出要求，仅要求取证方法应当符合相关技术标准。实践中，对相关取证设备有疑问，可以通过出具说明、侦查实验、程序功能检验或鉴定予以验证。

目前，国内关于电子数据取证的技术标准体系主要分为国家标准和行业标准，国家标准有：《GB/T 29360—2012 电子物证数据恢复检验规程》《GB/T 29361—2012 电子物证文件一致性检验规程》《GB/T 29362—2012 电子物证数据搜索检验规程》。行业标准是由司法鉴定主管部门、司法鉴定行业组织或者相关行业主管部门制定的行业标准和技术规范，主要有：《GA/T 754—2008 电子数据存储介质复制工具要求及检测方法》《GA/T 755—2008 电子数据存储介质写保护设备要求及检测方法》《GA/T 756—2008 数字化设备证据数据发现提取固定方法》《GA/T 757—2008 程序功能检验方法》《GA/T 825—2009 电子物证数据搜索检验技术规范》《GA/T 826—2009 电子物证数据恢复检验技术规范》《GA/T 827—2009 电子物证文件一致性检验技术规范》《GA/T 828—2009 电子物证软件功能检验技术规范》《GA/T 829—2009 电子物证软件一致性检验技术规范》《GA/T 976—2012 电子数据法庭科学鉴定通用方法》《GA/T 977—2012 取证与鉴定文书电子签名》《GA/T 978—2012 网络游戏私服检验技术方法》《GA/T 1170—2014 移动终端取证检验方法》《GA/T 1171—2014 芯片相似性比对检验方法》《GA/T 1172—2014 电子邮件检验技术方法》《GA/T 1173—2014 即时通讯记录检验技术方法》《GA/T 1174—2014 电子证据数据现场获取通用方法》《GA/T 1175—2014 软件相似性检验技术方法》《GA/T 1176—2014 网页浏览器历史数据检验技术方

法》等等。[①] 相关技术标准还在不断发展和完善之中。

（二）扣押电子数据原始存储介质

电子数据依赖于存储介质而存在。所谓存储介质，是指具备数据信息存储功能的电子设备、硬盘、光盘、优盘、记忆棒、存储卡、存储芯片等载体。在侦查过程中是否获取原始存储介质，对于审查判断收集、提取的电子数据是否全面、真实、完整，具有重要意义。这是因为，侦查机关可以在扣押原始存储之后提取其中存储的电子数据，只要原始存储介质未被损坏，提取的过程可以重复操作。因此，在侦查过程中，为保证电子数据的完整性，在收集电子数据时应尽量获取电子数据的原始存储介质。根据《刑事诉讼法解释》第九十三条的规定，对电子数据，应当审查以下内容：是否随原始存储介质移送；在原始存储介质无法封存、不便移送或者依法应当由有关部门保管、处理、返还时，提取、复制电子数据是否由二人以上进行，是否足以保证电子数据的完整性，有无提取、复制过程及原始存储介质存放地点的文字说明和签名。《刑事诉讼法解释》将电子数据区分为两种情形：一种是随原始存储介质移送的；一种是从原始存储介质中提取、复制的。《网络犯罪刑事诉讼程序意见》则明确了“以扣押原始存储介质为原则，以直接提取电子数据为例外”的取证规则，规定：“收集、提取电子数据，能够获取原始存储介质的，应当封存原始存储介质，并制作笔录，记录原始存储介质的封存状态，由侦查人员、原始存储介质持有人签名或者盖章；持有人无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章。有条件的，侦查人员应当对相关活动进行录像。”《规定》第八条基本上沿袭了这一规定。有意见提出，“能够获取”的表述有歧义，例如，侦查机关能够找到并接触到原始存储介质，但是该原始存储介质无法封存或者不便移送，是否属于能够获取原始存储介质？实际上，这里的“能够获取”表述为“能够扣押”更准确。因此，《规定》第八条的表述作出了相应的调整，规定：“收集、提取电子数据，能够扣押电子数据原始存储介质的，应当扣押、封存原始存储介质，并制作笔录，记录原始存储介质的封存状态。”

实践中，办案机关对电子数据原始存储介质的封存存在不规范的问题，如有的没有以封存的状态移送；有的虽然已经封存，但封存的方式不能保证计算机内部的硬盘不被更换；有的手机在封存状态下仍然开机并可以接收信号，难以保证电子数据不会灭失或者发生改变。针对上述问题，《规定》对原始存储介质的封存作出了规范，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。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

① 刘浩阳、李锦、刘晓宇主编：《电子数据取证》，清华大学出版社2015年版。

可以通过对电源接口以及机箱螺钉处加贴封条封存。对于手机等具有无线通信功能的存储介质，可以将手机装入屏蔽袋（盒），也可以拔出手机电池或者通过设置为“飞行模式”并关闭“寻回”功能等方式进行附加保护。实践中需要特别注意，对已扣押的原始存储介质应当按照涉案财物管理的有关规定予以妥善保管，采取必要措施防止原始存储介质发生损坏，以避免电子数据灭失或者发生改变。

（三）直接提取电子数据和通过网络在线提取电子数据

《规定》第九条第一款规定，无法扣押原始存储介质的，可以提取电子数据，但应当在笔录中注明不能扣押原始存储介质的原因、原始存储介质的存放地点或者电子数据的来源等情况，并计算电子数据的完整性校验值。所谓完整性校验值，是指为防止电子数据被篡改或者破坏，使用散列算法（又称哈希算法，英文为“Hash”）等特定算法对电子数据进行计算，得出的用于校验数据完整性的数据值。无法扣押原始存储介质的情形主要有：（1）原始存储介质不便封存的；（2）提取计算机内存数据、网络传输数据等不是存储在存储介质上的电子数据的，比如，分布式拒绝服务（DDoS：Distributed Denial of Service）攻击案件中从网络截取的攻击数据包就属于典型的网络传输数据，此类数据并非存储于存储介质上，又称为易丢失数据；（3）原始存储介质位于境外的；（4）其他无法扣押原始存储介质的情形。

随着互联网的发展，电子数据与网络的关系越来越密切，收集、提取电子数据可以不受时空限制，并且能够保证电子数据的真实性和完整性，司法实践中，通过网络在线提取电子数据已经成为重要的侦查取证方式，被各级公安、检察机关越来越多的使用。在《规定》征求意见过程中，基层侦查实务部门强烈建议明确通过网络在线提取的电子数据的证据效力。经征求全国人大常委会法工委的意见，其也认为，对于通过网络在线提取的电子数据，只要取证过程能够保证电子数据的真实性、完整性，即可以作为证据使用。为此，《规定》第六条明确了通过网络在线提取的电子数据，可以作为证据使用。《规定》第九条第二款明确，对于原始存储介质位于境外或者远程计算机信息系统上的电子数据，可以通过网络在线提取。我们认为，对于原始存储介质位于异地，或者原始存储介质虽然位于本地，但案件尚在初查过程中，侦查人员不便进入现场，不及时提取电子数据可能造成证据灭失，且相关电子数据能够通过网络在线提取的，属于该款规定的“远程计算机信息系统上的电子数据”，可以通过网络在线提取。实践中，通过网络在线提取电子数据主要适用于下列案件：一是危害计算机信息系统安全犯罪案件；二是利用计算机实施的盗窃、诈骗、敲诈勒索等犯罪案件；三是在网络上发布违法信息的犯罪案件，如网络诽谤案件；四是设立主要用于实施犯罪活动的网站、通讯群组，针对不特定多数人实施犯罪或者组织、教唆、帮助不特定多数人实施犯罪的案件，如设立赌博网站，或者在网上组织传销活动；五是主要犯罪行为在网络上实施的其他案件。

需要说明的是，《规定》第九条第一款规定的直接提取电子数据和第九条第二款规定的通过网络在线提取电子数据可能使人产生误解，认为直接提取电子数据一般是在进行现场勘验、

检查过程中通过犯罪现场的计算机设备直接提取，而通过网络在线提取电子数据则是通过任意一台计算机设备连接互联网在线提取电子数据。但实际上，在“原始存储介质位于境外”的情况下，无论从哪一台计算机设备上提取，都不是从原始存储介质上提取，而是通过网络进行操作，但从保证电子数据的真实性、完整性的效果上看，通过网络在线提取电子数据和从原始存储介质上直接提取电子数据又没有实质性差别。因此，直接提取电子数据和通过网络在线提取电子数据并不是并列关系，而是包含与被包含的关系，直接提取电子数据包括通过网络在线直接提取电子数据。在研究起草《规定》的过程中，有意见提出，通过网络在线提取电子数据应表述为“网络远程提取”，经研究认为，“远程提取”的概念不准确，网络空间是虚拟空间而非现实空间，根据物理距离划分“远程”和“非远程”没有意义，且容易引发歧义。因此，《规定》使用了“网络在线提取”的表述方式。

（四）网络远程勘验和技术侦查措施

《规定》第九条第三款规定：“为进一步查明有关情况，必要时，可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验，需要采取技术侦查措施的，应当依法经过严格的批准手续。”在这里，有必要对网络在线提取和网络远程勘验的概念作出区分。二者都是通过网络进行操作，最终目的也都是提取电子数据，以往在司法实践中对二者并没有进行过明确区分，一般统称为远程勘验。例如，2005 年公安部《计算机犯罪现场勘验与电子证据检查规则》第三条规定，远程勘验，是指通过网络对远程目标系统实施勘验，以提取、固定远程目标系统的状态和存留的电子数据。但事实上，二者有明显的区别。所谓网络远程勘验，是指通过网络对远程计算机信息系统实施勘验，发现、提取与犯罪有关的电子数据，记录计算机信息系统状态，判断案件性质，分析犯罪过程，确定侦查方向和范围，为侦破案件、刑事诉讼提供线索和证据的侦查活动。网络在线提取，只是通过网络对网页、网上视频、网盘文件上的电子数据等进行提取，可以理解为从网络下载文件。实际上，网络远程勘验类似于对犯罪现场的勘验。在传统犯罪中，犯罪嫌疑人会在犯罪现场留下指纹、足迹、DNA、凶器等痕迹和物证。而在网络犯罪等高科技犯罪中，犯罪嫌疑人使用计算机、网络、手机等智能终端设备时，在虚拟空间中也会留下相关的犯罪痕迹和侦查线索，与传统犯罪现场不同，遗留的线索和证据材料多以电子数据的形式存在。网络犯罪现场可能是一台计算机、一部手机、一个局域网甚至是一个大型网络，可能涉及多个地域。犯罪嫌疑人的物理活动范围和涉案电子设备的物理地址有可能是分离的，如犯罪嫌疑人在国内，赌博网站、淫秽色情网站的服务器托管地却在国外。网络远程勘验的目的就是进入虚拟空间去寻找与犯罪相关的证据，判断案件性质，分析犯罪过程。可见，网络远程勘验是一个相对复杂的过程，网络在线提取则相对简单得多。

根据刑事诉讼法第一百四十八条的规定，公安机关在立案后，对于危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、重大毒品犯罪或者其他严重危害社会的犯罪案件，人民检察院在立案后，对于重大的贪污、贿赂犯罪案件以及利用职权实施的严重侵犯公民人

身权利的重大犯罪案件，根据侦查犯罪的需要，经过严格的批准手续，可以采取技术侦查措施。根据《公安机关办理刑事案件程序规定》第二百五十五条的规定，技术侦查措施是指由设区的市一级以上公安机关负责技术侦查的部门实施的记录监控、行踪监控、通信监控、场所监控等措施。由于一些技术侦查措施也能够通过网络完成，因此，技术侦查措施和网络远程勘验、网络在线提取容易发生混淆。实际上，它们之间有着本质的区别。网络远程勘验和网络在线提取属于一般性的侦查活动，侦查机关均可以执行。而采取技术侦查措施应当依法经过严格的批准手续，通常只能由特定的部门如公安机关技术侦查部门来执行。实践中，确有多种侦查手段配合使用的情况，但只要涉及技术侦查措施，就必须符合刑事诉讼法规定的条件，并依法经过严格的批准手续。

（五）采取打印、拍照或者录像等方式固定证据

《网络犯罪刑事诉讼程序意见》明确了收集、提取电子数据应当以扣押原始存储介质为原则，以直接提取电子数据为例外。《规定》第八条、第九条重申了这一原则。但是，我们注意到，实践中还存在这样的情况，侦查人员既无法扣押、封存原始存储介质，又不能提取电子数据。例如，目前市场上流行的一些即时通信软件（如“支付宝”“钉钉”等）开发了“阅后即焚”功能，开启这种通信模式后，用户在点击阅读信息后5秒左右该信息即被自动删除，并且常常采用覆盖删除的方式，难以恢复，这就需要在极短的时间内迅速将电子数据固定下来，否则相关证据将灭失，即使扣押、封存手机也无法恢复数据。又如，船舶的导航系统等部分工控系统只有操作界面，没有接口可以导出数据，侦查机关不可能将整个船舶或者大型系统扣押，因此，既有的取证规则明显不能适应现实需要。此外，在实践中，大量的轻微刑事案件由基层公安机关派出所侦办，但派出所往往没有专业取证设备，或者受技术条件的限制无法直接提取电子数据，甚至有的被害人报案后不愿将手机交给侦查人员，为防止证据灭失，需要及时采取必要措施固定证据。基于以上考虑，《规定》对电子数据取证规则作出进一步完善，确立了“以扣押电子数据原始存储介质为原则，以直接提取或者通过网络在线提取电子数据为补充，以其他方式固定证据为例外”的取证规则。《规定》第十条规定：“由于客观原因无法或者不宜依据第八条、第九条的规定收集、提取电子数据的，可以采取打印、拍照或者录像等方式固定相关证据，并在笔录中说明原因。”需要注意的是，这种固定证据的方式只能在无法扣押、封存原始存储介质，又不能提取电子数据的情况下使用，并在笔录中注明原因。

（六）冻结电子数据

随着云计算等信息技术的发展，越来越多的电子数据存储在云系统中，有的电子数据存储于境外服务器或者大型在线系统中，这些情况下，无法扣押电子数据的原始存储介质，直接提取电子数据也有困难，给侦查办案带来很大困扰。为了解决云计算、大数据环境下难以将海量数据原始存储介质扣押、封存，以及难以提取海量数据的问题，《规定》第十一条、第十二条创设性地规定了冻结电子数据的证据保