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

最高人民法院 最高人民检察院 公安部印发

《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》的通知

各省、自治区、直辖市高级人民法院、人民检察院、公安厅（局），解放军军事法院、军事检察院，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局：

为规范电子数据的收集提取和审查判断，提高刑事案件办理质量，最高人民法院、最高人民检察院、公安部制定了《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》。现印发给你们，请认真贯彻执行。执行中遇到的问题，请及时分别层报最高人民法院、最高人民检察院、公安部。

最高人民法院 最高人民检察院 公安部

2016 年 9 月 9 日

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

为规范电子数据的收集提取和审查判断，提高刑事案件办理质量，根据《中华人民共和国刑事诉讼法》等有关法律规定，结合司法实际，制定本规定。

一、一般规定

第一条 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。

电子数据包括但不限于下列信息、电子文件：

（一）网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；

（二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；

（三）用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；

（四）文档、图片、音视频、数字证书、计算机程序等电子文件。

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。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。

第二条 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。

第三条 人民法院、人民检察院和公安机关有权依法向有关单位和个人收集、调取电子数据。有关单位和个人应当如实提供。

第四条 电子数据涉及国家秘密、商业秘密、个人隐私的，应当保密。

第五条 对作为证据使用的电子数据，应当采取以下一种或者几种方法保护电子数据的完整性：

（一）扣押、封存电子数据原始存储介质；

（二）计算电子数据完整性校验值；

（三）制作、封存电子数据备份；

（四）冻结电子数据；

（五）对收集、提取电子数据的相关活动进行录像；

（六）其他保护电子数据完整性的方法。

第六条 初查过程中收集、提取的电子数据，以及通过网络在线提取的电子数据，可以作为证据使用。

二、电子数据的收集与提取

第七条 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。

第八条 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。

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。

第九条 具有下列情形之一，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：

（一）原始存储介质不便封存的；

（二）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；

（三）原始存储介质位于境外的；

（四）其他无法扣押原始存储介质的情形。

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。

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。

第十条 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。

第十一条 具有下列情形之一的，经县级以上公安机关负责人或者检察长批准，可以对电子数据进行冻结：

（一）数据量大，无法或者不便提取的；

（二）提取时间长，可能造成电子数据被篡改或者灭失的；

（三）通过网络应用可以更为直观地展示电子数据的；

（四）其他需要冻结的情形。

第十二条 冻结电子数据，应当制作协助冻结通知书，注明冻结电子数据的网络应用账号等信息，送交电子数据持有人、网络服务提供者或者有关部门协助办理。解除冻结的，应当在三日内制作协助解除冻结通知书，送交电子数据持有人、网络服务提供者或者有关部门协助办理。

冻结电子数据，应当采取以下一种或者几种方法：

（一）计算电子数据的完整性校验值；

（二）锁定网络应用账号；

（三）其他防止增加、删除、修改电子数据的措施。

第十三条 调取电子数据，应当制作调取证据通知书，注明需要调取电子数据的相关信息，通知电子数据持有人、网络服务提供者或者有关部门执行。

第十四条 收集、提取电子数据，应当制作笔录，记录案由、对象、内容、收集、提取电子数据的时间、地点、方法、过程，并附电子数据清单，注明类别、文件格式、完整性校验值等，由侦查人员、电子数据持有人（提供人）签

名或者盖章；电子数据持有人（提供人）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，应当对相关活动进行录像。

第十五条 收集、提取电子数据，应当根据刑事诉讼法的规定，由符合条件的人员担任见证人。由于客观原因无法由符合条件的人员担任见证人的，应当在笔录中注明情况，并对相关活动进行录像。

针对同一现场多个计算机信息系统收集、提取电子数据的，可以由一名见证人见证。

第十六条 对扣押的原始存储介质或者提取的电子数据，可以通过恢复、破解、统计、关联、比对等方式进行检查。必要时，可以进行侦查实验。

电子数据检查，应当对电子数据存储介质拆封过程进行录像，并将电子数据存储介质通过写保护设备接入到检查设备进行检查；有条件的，应当制作电子数据备份，对备份进行检查；无法使用写保护设备且无法制作备份的，应当注明原因，并对相关活动进行录像。

电子数据检查应当制作笔录，注明检查方法、过程和结果，由有关人员签名或者盖章。进行侦查实验的，应当制作侦查实验笔录，注明侦查实验的条件、经过和结果，由参加实验的人员签名或者盖章。

第十七条 对电子数据涉及的专门性问题难以确定的，由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。对于人民检察院直接受理的案件，也可以由最高人民检察院指定的机构出具报告。

具体办法由公安部、最高人民检察院分别制定。

三、电子数据的移送与展示

第十八条 收集、提取的原始存储介质或者电子数据，应当以封存状态随案移送，并制作电子数据的备份一并移送。

对网页、文档、图片等可以直接展示的电子数据，可以不随案移送打印件；人民法院、人民检察院因设备等条件限制无法直接展示电子数据的，侦查机关应当随案移送打印件，或者附展示工具和展示方法说明。

对冻结的电子数据，应当移送被冻结电子数据的清单，注明类别、文件格式、冻结主体、证据要点、相关网络应用账号，并附查看工具和方法的说明。

第十九条 对侵入、非法控制计算机信息系统的程序、工具以及计算机病毒等无法直接展示的电子数据，应当附电子数据属性、功能等情况的说明。

对数据统计量、数据同一性等问题，侦查机关应当出具说明。

第二十条 公安机关报请人民检察院审查批准逮捕犯罪嫌疑人，或者对侦查终结的案件移送人民检察院审查起诉的，应当将电子数据等证据一并移送人民检察院。人民检察院在审查批准逮捕和审查起诉过程中发现应当移送的电子数据没有移送或者移送的电子数据不符合相关要求的，应当通知公安机关补充移送或者进行补正。

对于提起公诉的案件，人民法院发现应当移送的电子数据没有移送或者移送的电子数据不符合相关要求的，应当通知人民检察院。

公安机关、人民检察院应当自收到通知后三日内移送电子数据或者补充有关材料。

第二十一条 控辩双方向法庭提交的电子数据需要展示的，可以根据电子数据的具体类型，借助多媒体设备出示、播放或者演示。必要时，可以聘请具有专门知识的人进行操作，并就相关技术问题作出说明。

四、电子数据的审查与判断

第二十二条 对电子数据是否真实，应当着重审查以下内容：

（一）是否移送原始存储介质；在原始存储介质无法封存、不便移动时，有无说明原因，并注明收集、提取过程及原始存储介质的存放地点或者电子数据的来源等情况；

（二）电子数据是否具有数字签名、数字证书等特殊标识；

（三）电子数据的收集、提取过程是否可以重现；

（四）电子数据如有增加、删除、修改等情形的，是否附有说明；

（五）电子数据的完整性是否可以保证。

第二十三条 对电子数据是否完整，应当根据保护电子数据完整性的相应方法进行验证：

（一）审查原始存储介质的扣押、封存状态；

（二）审查电子数据的收集、提取过程，查看录像；

（三）比对电子数据完整性校验值；

（四）与备份的电子数据进行比较；

（五）审查冻结后的访问操作日志；

（六）其他方法。

第二十四条 对收集、提取电子数据是否合法，应当着重审查以下内容：

（一）收集、提取电子数据是否由二名以上侦查人员进行，取证方法是否符合相关技术标准；

（二）收集、提取电子数据，是否附有笔录、清单，并经侦查人员、电子数据持有人（提供人）、见证人签名或者盖章；没有持有人（提供人）签名或者盖章的，是否注明原因；对电子数据的类别、文件格式等是否注明清楚；

（三）是否依照有关规定由符合条件的人员担任见证人，是否对相关活动进行录像；

（四）电子数据检查是否将电子数据存储介质通过写保护设备接入到检查设备；有条件的，是否制作电子数据备份，并对备份进行检查；无法制作备份且无法使用写保护设备的，是否附有录像。

第二十五条 认定犯罪嫌疑人、被告人的网络身份与现实身份的同一性，可以通过核查相关 IP 地址、网络活动记录、上网终端归属、相关证人证言以及犯罪嫌疑人、被告人供述和辩解等进行综合判断。

认定犯罪嫌疑人、被告人与存储介质的关联性，可以通过核查相关证人证言以及犯罪嫌疑人、被告人供述和辩解等进行综合判断。

第二十六条 公诉人、当事人或者辩护人、诉讼代理人对电子数据鉴定意见有异议，可以申请人民法院通知鉴定人出庭作证。人民法院认为鉴定人有必要出庭的，鉴定人应当出庭作证。

经人民法院通知，鉴定人拒不出庭作证的，鉴定意见不得作为定案的根据。对没有正当理由拒不出庭作证的鉴定人，人民法院应当通报司法行政机关或者有关部门。

公诉人、当事人或者辩护人、诉讼代理人可以申请法庭通知有专门知识的人出庭，就鉴定意见提出意见。

对电子数据涉及的专门性问题的报告，参照适用前三款规定。

第二十七条 电子数据的收集、提取程序有下列瑕疵，经补正或者作出合理解释的，可以采用；不能补正或者作出合理解释的，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（提供人）、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。

第二十八条 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。

五、附则

第二十九条 本规定中下列用语的含义：

（一）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。

（二）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。

（三）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，为侦查破案、刑事诉讼提供线索和证据的侦查活动。

（四）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。

（五）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。

（六）访问操作日志，是指为审查电子数据是否被增加、删除或者修改，由计算机信息系统自动生成的对电子数据访问、操作情况的详细记录。

第三十条 本规定自 2016 年 10 月 1 日起施行。之前发布的规范性文件与本规定不一致的，以本规定为准。