浅析《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》

朱君韬　实习律师

2016-09-26

## 法规解读：

近日，最高人民法院、最高人民检察院和公安部联名印发了《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》”），《规定》的发布对于电子数据这类新型证据在收集、提取、审查判断方面提供了依据，使得我国刑事案件办理过程中对于电子证据的使用有了可操作性的规范。联想到年初“快播案”庭审中公诉人对于电子数据类证据极不专业的背景知识和糟糕的庭审表现，《规定》对于电子数据类的证据的采用提供了可操作性的指导。下面简单梳理一下《规定》的亮点。

**第一**、《规定》明确了电子数据类证据的范围，其最大的特点是以数字化形式存储、处理、传输的，能够证明案件事实的数据。其本质是数据，这是与其他类型证据最主要的区别。《规定》以列举的方式，列出了一些常见的电子数据，包括网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；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；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；文档、图片、音视频、数字证书、计算机程序等电子文件。同时，对于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言词证据作出了排除性规定，究其原因是该类证据须经过庭审质证，更适于使用言词证据的证明力规则。

**第二**、《规定》确立了收集、提取、审查判断电子证据的基本原则。**以电子数据的原始性、完整性、真实性为最高标准。**原则上应当扣押封存原始存储介质；在对电子数据进行操作时应当采用写保护装置（使用“只读锁”）；对电子数据的提取、解读等操作应当在备份数据上进行，而不是原始数据；对于向法庭出示的相关电子数据，应当出示其计算的电子数据完整性校验值与原始数据完整性校验值一致。对于无法封存原始介质、不便提取的数据，可以要求数据的存储方对数据进行冻结等措施。《规定》第 8 条、第 9 条规定，“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。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。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。”

我国对于电子数据类证据的确认始于 2012 年《刑事诉讼法》的修订，相关配套的制度还有待完善，实务中相关的操作方法和标准也没有完全统一。同时，我国在电子数据证据这方面的经验，相对国外发达国家和地区还有一定的差距。本次《规定》的出台，标志着电子证据类证据相关配套制度的创立，使我国证据学、法庭科学、鉴定科学等相关学科的研究有了新的区域，也使得律师业务的领域有所拓展。

## 法规全文：

### 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。