关于印发《人民检察院办理网络犯罪案件规定》的通知

各级人民检察院：

《人民检察院办理网络犯罪案件规定》已经2020年12月14日最高人民检察院第十三届检察委员会第五十七次会议通过，现印发你们，请结合实际，认真贯彻落实。

最高人民检察院

2021年1月22日

人民检察院办理网络犯罪案件规定

第一章　一般规定

第一条　为规范人民检察院办理网络犯罪案件，维护国家安全、网络安全、社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国刑事诉讼法》《人民检察院刑事诉讼规则》等规定，结合司法实践，制定本规定。

第二条　本规定所称网络犯罪是指针对信息网络实施的犯罪，利用信息网络实施的犯罪，以及其他上下游关联犯罪。

第三条　人民检察院办理网络犯罪案件应当加强全链条惩治，注重审查和发现上下游关联犯罪线索。对涉嫌犯罪，公安机关未立案侦查、应当提请批准逮捕而未提请批准逮捕或者应当移送起诉而未移送起诉的，依法进行监督。

第四条　人民检察院办理网络犯罪案件应当坚持惩治犯罪与预防犯罪并举，建立捕、诉、监、防一体的办案机制，加强以案释法，发挥检察建议的作用，促进有关部门、行业组织、企业等加强网络犯罪预防和治理，净化网络空间。

第五条　网络犯罪案件的管辖适用刑事诉讼法及其他相关规定。

有多个犯罪地的，按照有利于查清犯罪事实、有利于保护被害人合法权益、保证案件公正处理的原则确定管辖。

因跨区域犯罪、共同犯罪、关联犯罪等原因存在管辖争议的，由争议的人民检察院协商解决，协商不成的，报请共同的上级人民检察院指定管辖。

第六条　人民检察院办理网络犯罪案件应当发挥检察一体化优势，加强跨区域协作办案，强化信息互通、证据移交、技术协作，增强惩治网络犯罪的合力。

第七条　人民检察院办理网络犯罪案件应当加强对电子数据收集、提取、保全、固定等的审查，充分运用同一电子数据往往具有的多元关联证明作用，综合运用电子数据与其他证据，准确认定案件事实。

第八条　建立检察技术人员、其他有专门知识的人参与网络犯罪案件办理制度。根据案件办理需要，吸收检察技术人员加入办案组辅助案件办理。积极探索运用大数据、云计算、人工智能等信息技术辅助办案，提高网络犯罪案件办理的专业化水平。

第九条　人民检察院办理网络犯罪案件，对集团犯罪或者涉案人数众多的，根据行为人的客观行为、主观恶性、犯罪情节及地位、作用等综合判断责任轻重和刑事追究的必要性，按照区别对待原则分类处理，依法追诉。

第十条　人民检察院办理网络犯罪案件应当把追赃挽损贯穿始终，主动加强与有关机关协作，保证及时查封、扣押、冻结涉案财物，阻断涉案财物移转链条，督促涉案人员退赃退赔。

第二章　引导取证和案件审查

第十一条　人民检察院办理网络犯罪案件应当重点围绕主体身份同一性、技术手段违法性、上下游行为关联性等方面全面审查案件事实和证据，注重电子数据与其他证据之间的相互印证，构建完整的证据体系。

第十二条　经公安机关商请，根据追诉犯罪的需要，人民检察院可以派员适时介入重大、疑难、复杂网络犯罪案件的侦查活动，并对以下事项提出引导取证意见：

（一）案件的侦查方向及可能适用的罪名；

（二）证据的收集、提取、保全、固定、检验、分析等；

（三）关联犯罪线索；

（四）追赃挽损工作；

（五）其他需要提出意见的事项。

人民检察院开展引导取证活动时，涉及专业性问题的，可以指派检察技术人员共同参与。

第十三条　人民检察院可以通过以下方式了解案件办理情况：

（一）查阅案件材料；

（二）参加公安机关对案件的讨论；

（三）了解讯（询）问犯罪嫌疑人、被害人、证人的情况；

（四）了解、参与电子数据的收集、提取；

（五）其他方式。

第十四条　人民检察院介入网络犯罪案件侦查活动，发现关联犯罪或其他新的犯罪线索，应当建议公安机关依法立案或移送相关部门；对于犯罪嫌疑人不构成犯罪的，依法监督公安机关撤销案件。

第十五条　人民检察院可以根据案件侦查情况，向公安机关提出以下取证意见：

（一）能够扣押、封存原始存储介质的，及时扣押、封存；

（二）扣押可联网设备时，及时采取信号屏蔽、信号阻断或者切断电源等方式，防止电子数据被远程破坏；

（三）及时提取账户密码及相应数据，如电子设备、网络账户、应用软件等的账户密码，以及存储于其中的聊天记录、电子邮件、交易记录等；

（四）及时提取动态数据，如内存数据、缓存数据、网络连接数据等；

（五）及时提取依赖于特定网络环境的数据，如点对点网络传输数据、虚拟专线网络中的数据等；

（六）及时提取书证、物证等客观证据，注意与电子数据相互印证。

第十六条　对于批准逮捕后要求公安机关继续侦查、不批准逮捕后要求公安机关补充侦查或者审查起诉退回公安机关补充侦查的网络犯罪案件，人民检察院应当重点围绕本规定第十二条第一款规定的事项，有针对性地制作继续侦查提纲或者补充侦查提纲。对于专业性问题，应当听取检察技术人员或者其他有专门知识的人的意见。

人民检察院应当及时了解案件继续侦查或者补充侦查的情况。

第十七条　认定网络犯罪的犯罪嫌疑人，应当结合全案证据，围绕犯罪嫌疑人与原始存储介质、电子数据的关联性、犯罪嫌疑人网络身份与现实身份的同一性，注重审查以下内容：

（一）扣押、封存的原始存储介质是否为犯罪嫌疑人所有、持有或者使用；

（二）社交、支付结算、网络游戏、电子商务、物流等平台的账户信息、身份认证信息、数字签名、生物识别信息等是否与犯罪嫌疑人身份关联；

（三）通话记录、短信、聊天信息、文档、图片、语音、视频等文件内容是否能够反映犯罪嫌疑人的身份；

（四）域名、IP 地址、终端 MAC 地址、通信基站信息等是否能够反映电子设备为犯罪嫌疑人所使用；

（五）其他能够反映犯罪嫌疑人主体身份的内容。

第十八条　认定犯罪嫌疑人的客观行为，应当结合全案证据，围绕其利用的程序工具、技术手段的功能及其实现方式、犯罪行为和结果之间的关联性，注重审查以下内容：

（一）设备信息、软件程序代码等作案工具；

（二）系统日志、域名、IP 地址、WiFi 信息、地理位置信息等是否能够反映犯罪嫌疑人的行为轨迹；

（三）操作记录、网络浏览记录、物流信息、交易结算记录、即时通信信息等是否能够反映犯罪嫌疑人的行为内容；

（四）其他能够反映犯罪嫌疑人客观行为的内容。

第十九条　认定犯罪嫌疑人的主观方面，应当结合犯罪嫌疑人的认知能力、专业水平、既往经历、人员关系、行为次数、获利情况等综合认定，注重审查以下内容：

（一）反映犯罪嫌疑人主观故意的聊天记录、发布内容、浏览记录等；

（二）犯罪嫌疑人行为是否明显违背系统提示要求、正常操作流程；

（三）犯罪嫌疑人制作、使用或者向他人提供的软件程序是否主要用于违法犯罪活动；

（四）犯罪嫌疑人支付结算的对象、频次、数额等是否明显违反正常交易习惯；

（五）犯罪嫌疑人是否频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份；

（六）其他能够反映犯罪嫌疑人主观方面的内容。

第二十条　认定犯罪行为的情节和后果，应当结合网络空间、网络行为的特性，从违法所得、经济损失、信息系统的破坏、网络秩序的危害程度以及对被害人的侵害程度等综合判断，注重审查以下内容：

（一）聊天记录、交易记录、音视频文件、数据库信息等能够反映犯罪嫌疑人违法所得、获取和传播数据及文件的性质、数量的内容；

（二）账号数量、信息被点击次数、浏览次数、被转发次数等能够反映犯罪行为对网络空间秩序产生影响的内容；

（三）受影响的计算机信息系统数量、服务器日志信息等能够反映犯罪行为对信息网络运行造成影响程度的内容；

（四）被害人数量、财产损失数额、名誉侵害的影响范围等能够反映犯罪行为对被害人的人身、财产等造成侵害的内容；

（五）其他能够反映犯罪行为情节、后果的内容。

第二十一条　人民检察院办理网络犯罪案件，确因客观条件限制无法逐一收集相关言词证据的，可以根据记录被害人人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料，在审查被告人及其辩护人所提辩解、辩护意见的基础上，综合全案证据材料，对相关犯罪事实作出认定。

第二十二条　对于数量众多的同类证据材料，在证明是否具有同样的性质、特征或者功能时，因客观条件限制不能全部验证的，可以进行抽样验证。

第二十三条　对鉴定意见、电子数据等技术性证据材料，需要进行专门审查的，应当指派检察技术人员或者聘请其他有专门知识的人进行审查并提出意见。

第二十四条　人民检察院在审查起诉过程中，具有下列情形之一的，可以依法自行侦查：

（一）公安机关未能收集的证据，特别是存在灭失、增加、删除、修改风险的电子数据，需要及时收集和固定的；

（二）经退回补充侦查未达到补充侦查要求的；

（三）其他需要自行侦查的情形。

第二十五条　自行侦查由检察官组织实施，开展自行侦查的检察人员不得少于二人。需要技术支持和安全保障的，由人民检察院技术部门和警务部门派员协助。必要时，可以要求公安机关予以配合。

第二十六条　人民检察院办理网络犯罪案件的部门，发现或者收到侵害国家利益、社会公共利益的公益诉讼案件线索的，应当及时移送负责公益诉讼的部门处理。

第三章　电子数据的审查

第二十七条　电子数据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，主要包括以下形式：

（一）网页、社交平台、论坛等网络平台发布的信息；

（二）手机短信、电子邮件、即时通信、通讯群组等网络通讯信息；

（三）用户注册信息、身份认证信息、数字签名、生物识别信息等用户身份信息；

（四）电子交易记录、通信记录、浏览记录、操作记录、程序安装、运行、删除记录等用户行为信息；

（五）恶意程序、工具软件、网站源代码、运行脚本等行为工具信息；

（六）系统日志、应用程序日志、安全日志、数据库日志等系统运行信息；

（七）文档、图片、音频、视频、数字证书、数据库文件等电子文件及其创建时间、访问时间、修改时间、大小等文件附属信息。

第二十八条　电子数据取证主要包括以下方式：收集、提取电子数据；电子数据检查和侦查实验；电子数据检验和鉴定。

收集、提取电子数据可以采取以下方式：

（一）扣押、封存原始存储介质；

（二）现场提取电子数据；

（三）在线提取电子数据；

（四）冻结电子数据；

（五）调取电子数据。

第二十九条　人民检察院办理网络犯罪案件，应当围绕客观性、合法性、关联性的要求对电子数据进行全面审查。注重审查电子数据与案件事实之间的多元关联，加强综合分析，充分发挥电子数据的证明作用。

第三十条　对电子数据是否客观、真实，注重审查以下内容：

（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，是否说明原因，并注明相关情况；

（二）电子数据是否有数字签名、数字证书等特殊标识；

（三）电子数据的收集、提取过程及结果是否可以重现；

（四）电子数据有增加、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。

第三十一条　对电子数据是否完整，注重审查以下内容：

（一）原始存储介质的扣押、封存状态是否完好；

（二）比对电子数据完整性校验值是否发生变化；

（三）电子数据的原件与备份是否相同；

（四）冻结后的电子数据是否生成新的操作日志。

第三十二条　对电子数据的合法性，注重审查以下内容：

（一）电子数据的收集、提取、保管的方法和过程是否规范；

（二）查询、勘验、扣押、调取、冻结等的法律手续是否齐全；

（三）勘验笔录、搜查笔录、提取笔录等取证记录是否完备；

（四）是否由符合法律规定的取证人员、见证人、持有人（提供人）等参与，因客观原因没有见证人、持有人（提供人）签名或者盖章的，是否说明原因；

（五）是否按照有关规定进行同步录音录像；

（六）对于收集、提取的境外电子数据是否符合国（区）际司法协作及相关法律规定的要求。

第三十三条　对电子数据的关联性，注重审查以下内容：

（一）电子数据与案件事实之间的关联性；

（二）电子数据及其存储介质与案件当事人之间的关联性。

第三十四条　原始存储介质被扣押封存的，注重从以下方面审查扣押封存过程是否规范：

（一）是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否与实物一一对应；

（二）是否封存或者计算完整性校验值，封存前后是否拍摄被封存原始存储介质的照片，照片是否清晰反映封口或者张贴封条处的状况；

（三）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

第三十五条　对原始存储介质制作数据镜像予以提取固定的，注重审查以下内容：

（一）是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否记录原始存储介质的存放位置、使用人、保管人；

（二）是否附有制作数据镜像的工具、方法、过程等必要信息；

（三）是否计算完整性校验值；

（四）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

第三十六条　提取原始存储介质中的数据内容并予以固定的，注重审查以下内容：

（一）是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否记录原始存储介质的存放位置、使用人、保管人；

（二）所提取数据内容的原始存储路径，提取的工具、方法、过程等信息，是否一并提取相关的附属信息、关联痕迹、系统环境等信息；

（三）是否计算完整性校验值；

（四）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

第三十七条　对于在线提取的电子数据，注重审查以下内容：

（一）是否记录反映电子数据来源的网络地址、存储路径或者数据提取时的进入步骤等；

（二）是否记录远程计算机信息系统的访问方式、电子数据的提取日期和时间、提取的工具、方法等信息，是否一并提取相关的附属信息、关联痕迹、系统环境等信息；

（三）是否计算完整性校验值；

（四）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

对可能无法重复提取或者可能出现变化的电子数据，是否随案移送反映提取过程的拍照、录像、截屏等材料。

第三十八条　对冻结的电子数据，注重审查以下内容：

（一）冻结手续是否符合规定；

（二）冻结的电子数据是否与案件事实相关；

（三）冻结期限是否即将到期、有无必要继续冻结或者解除；

（四）冻结期间电子数据是否被增加、删除、修改等。

第三十九条　对调取的电子数据，注重审查以下内容：

（一）调取证据通知书是否注明所调取的电子数据的相关信息；

（二）被调取单位、个人是否在通知书回执上签名或者盖章；

（三）被调取单位、个人拒绝签名、盖章的，是否予以说明；

（四）是否计算完整性校验值或者以其他方法保证电子数据的完整性。

第四十条　对电子数据进行检查、侦查实验，注重审查以下内容：

（一）是否记录检查过程、检查结果和其他需要记录的内容，并由检查人员签名或者盖章；

（二）是否记录侦查实验的条件、过程和结果，并由参加侦查实验的人员签名或者盖章；

（三）检查、侦查实验使用的电子设备、网络环境等是否与发案现场一致或者基本一致；

（四）是否使用拍照、录像、录音、通信数据采集等一种或者多种方式客观记录检查、侦查实验过程。

第四十一条　对电子数据进行检验、鉴定，注重审查以下内容：

（一）鉴定主体的合法性。包括审查司法鉴定机构、司法鉴定人员的资质，委托鉴定事项是否符合司法鉴定机构的业务范围，鉴定人员是否存在回避等情形；

（二）鉴定材料的客观性。包括鉴定材料是否真实、完整、充分，取得方式是否合法，是否与原始电子数据一致；

（三）鉴定方法的科学性。包括鉴定方法是否符合国家标准、行业标准，方法标准的选用是否符合相关规定；

（四）鉴定意见的完整性。是否包含委托人、委托时间、检材信息、鉴定或者分析论证过程、鉴定结果以及鉴定人签名、日期等内容；

（五）鉴定意见与其他在案证据能否相互印证。

对于鉴定机构以外的机构出具的检验、检测报告，可以参照本条规定进行审查。

第四十二条　行政机关在行政执法和查办案件过程中依法收集、提取的电子数据，人民检察院经审查符合法定要求的，可以作为刑事案件的证据使用。

第四十三条　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取证人员、见证人、持有人（提供人）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。

第四十四条　电子数据系篡改、伪造、无法确定真伪的，或者有其他无法保证电子数据客观、真实情形的，不得作为定案的根据。

电子数据有增加、删除、修改等情形，但经司法鉴定、当事人确认等方式确定与案件相关的重要数据未发生变化，或者能够还原电子数据原始状态、查清变化过程的，可以作为定案的根据。

第四十五条　对于无法直接展示的电子数据，人民检察院可以要求公安机关提供电子数据的内容、存储位置、附属信息、功能作用等情况的说明，随案移送人民法院。

第四章　出庭支持公诉

第四十六条　人民检察院依法提起公诉的网络犯罪案件，具有下列情形之一的，可以建议人民法院召开庭前会议：

（一）案情疑难复杂的；

（二）跨国（边）境、跨区域案件社会影响重大的；

（三）犯罪嫌疑人、被害人等人数众多、证据材料较多的；

（四）控辩双方对电子数据合法性存在较大争议的；

（五）案件涉及技术手段专业性强，需要控辩双方提前交换意见的；

（六）其他有必要召开庭前会议的情形。

必要时，人民检察院可以向法庭申请指派检察技术人员或者聘请其他有专门知识的人参加庭前会议。

第四十七条　人民法院开庭审理网络犯罪案件，公诉人出示证据可以借助多媒体示证、动态演示等方式进行。必要时，可以向法庭申请指派检察技术人员或者聘请其他有专门知识的人进行相关技术操作，并就专门性问题发表意见。

公诉人在出示电子数据时，应当从以下方面进行说明：

（一）电子数据的来源、形成过程；

（二）电子数据所反映的犯罪手段、人员关系、资金流向、行为轨迹等案件事实；

（三）电子数据与被告人供述、被害人陈述、证人证言、物证、书证等的相互印证情况；

（四）其他应当说明的内容。

第四十八条　在法庭审理过程中，被告人及其辩护人针对电子数据的客观性、合法性、关联性提出辩解或者辩护意见的，公诉人可以围绕争议点从证据来源是否合法，提取、复制、制作过程是否规范，内容是否真实完整，与案件事实有无关联等方面，有针对性地予以答辩。

第四十九条　支持、推动人民法院开庭审判网络犯罪案件全程录音录像。对庭审全程录音录像资料，必要时人民检察院可以商请人民法院复制，并将存储介质附检察卷宗保存。

第五章　跨区域协作办案

第五十条　对跨区域网络犯罪案件，上级人民检察院应当加强统一指挥和统筹协调，相关人民检察院应当加强办案协作。

第五十一条　上级人民检察院根据办案需要，可以统一调用辖区内的检察人员参与办理网络犯罪案件。

第五十二条　办理关联网络犯罪案件的人民检察院可以相互申请查阅卷宗材料、法律文书，了解案件情况，被申请的人民检察院应当予以协助。

第五十三条　承办案件的人民检察院需要向办理关联网络犯罪案件的人民检察院调取证据材料的，可以持相关法律文书和证明文件申请调取在案证据材料，被申请的人民检察院应当配合。

第五十四条　承办案件的人民检察院需要异地调查取证的，可以将相关法律文书及证明文件传输至证据所在地的人民检察院，请其代为调查取证。相关法律文书应当注明具体的取证对象、方式、内容和期限等。

被请求协助的人民检察院应当予以协助，及时将取证结果送达承办案件的人民检察院；无法及时调取的，应当作出说明。被请求协助的人民检察院有异议的，可以与承办案件的人民检察院进行协商；无法解决的，由承办案件的人民检察院报请共同的上级人民检察院决定。

第五十五条　承办案件的人民检察院需要询问异地证人、被害人的，可以通过远程视频系统进行询问，证人、被害人所在地的人民检察院应当予以协助。远程询问的，应当对询问过程进行同步录音录像。

第六章　跨国（边）境司法协作

第五十六条　办理跨国网络犯罪案件应当依照《中华人民共和国国际刑事司法协助法》及我国批准加入的有关刑事司法协助条约，加强国际司法协作，维护我国主权、安全和社会公共利益，尊重协作国司法主权、坚持平等互惠原则，提升跨国司法协作质效。

第五十七条　地方人民检察院在案件办理中需要向外国请求刑事司法协助的，应当制作刑事司法协助请求书并附相关材料，经报最高人民检察院批准后，由我国与被请求国间司法协助条约规定的对外联系机关向外国提出申请。没有刑事司法协助条约的，通过外交途径联系。

第五十八条　人民检察院参加现场移交境外证据的检察人员不少于二人，外方有特殊要求的除外。

移交、开箱、封存、登记的情况应当制作笔录，由最高人民检察院或者承办案件的人民检察院代表、外方移交人员签名或者盖章，一般应当全程录音录像。有其他见证人的，在笔录中注明。

第五十九条　人民检察院对境外收集的证据，应当审查证据来源是否合法、手续是否齐备以及证据的移交、保管、转换等程序是否连续、规范。

第六十条　人民检察院办理涉香港特别行政区、澳门特别行政区、台湾地区的网络犯罪案件，需要当地有关部门协助的，可以参照本规定及其他相关规定执行。

第七章　附则

第六十一条　人民检察院办理网络犯罪案件适用本规定，本规定没有规定的，适用其他相关规定。

第六十二条　本规定中下列用语的含义：

（一）信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及局域网络；

（二）存储介质，是指具备数据存储功能的电子设备、硬盘、光盘、优盘、记忆棒、存储芯片等载体；

（三）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；

（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）生物识别信息，是指计算机利用人体所固有的生理特征（包括人脸、指纹、声纹、虹膜、DNA 等）或者行为特征（步态、击键习惯等）来进行个人身份识别的信息；

（七）运行脚本，是指使用一种特定的计算机编程语言，依据符合语法要求编写的执行指定操作的可执行文件；

（八）数据镜像，是指二进制（0101 排序的数据码流）相同的数据复制件，与原件的内容无差别；

（九）MAC 地址，是指计算机设备中网卡的唯一标识，每个网卡有且只有一个 MAC 地址。

第六十三条　人民检察院办理国家安全机关、海警机关、监狱等移送的网络犯罪案件，适用本规定和其他相关规定。

第六十四条　本规定由最高人民检察院负责解释。

第六十五条　本规定自发布之日起施行。