最高人民法院 最高人民检察院 公安部

关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见

为依法惩治信息网络犯罪活动，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》以及有关法律、司法解释的规定，结合侦查、起诉、审判实践，现就办理此类案件适用刑事诉讼程序问题提出以下意见。

一、关于信息网络犯罪案件的范围

1.本意见所称信息网络犯罪案件包括：

（1）危害计算机信息系统安全犯罪案件；

（2）拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动的犯罪案件；

（3）主要行为通过信息网络实施的诈骗、赌博、侵犯公民个人信息等其他犯罪案件。

二、关于信息网络犯罪案件的管辖

2.信息网络犯罪案件由犯罪地公安机关立案侦查。必要时，可以由犯罪嫌疑人居住地公安机关立案侦查。

信息网络犯罪案件的犯罪地包括用于实施犯罪行为的网络服务使用的服务器所在地，网络服务提供者所在地，被侵害的信息网络系统及其管理者所在地，犯罪过程中犯罪嫌疑人、被害人或者其他涉案人员使用的信息网络系统所在地，被害人被侵害时所在地以及被害人财产遭受损失地等。

涉及多个环节的信息网络犯罪案件，犯罪嫌疑人为信息网络犯罪提供帮助的，其犯罪地、居住地或者被帮助对象的犯罪地公安机关可以立案侦查。

3.有多个犯罪地的信息网络犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争议的，按照有利于查清犯罪事实、有利于诉讼的原则，协商解决；经协商无法达成一致的，由共同上级公安机关指定有关公安机关立案侦查。需要提请批准逮捕、移送审查起诉、提起公诉的，由立案侦查的公安机关所在地的人民检察院、人民法院受理。

4.具有下列情形之一的，公安机关、人民检察院、人民法院可以在其职责范围内并案处理：

（1）一人犯数罪的；

（2）共同犯罪的；

（3）共同犯罪的犯罪嫌疑人、被告人还实施其他犯罪的；

（4）多个犯罪嫌疑人、被告人实施的犯罪行为存在关联，并案处理有利于查明全部案件事实的。

对为信息网络犯罪提供程序开发、互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者广告推广、支付结算等帮助，涉嫌犯罪的，可以依照第一款的规定并案侦查。

有关公安机关依照前两款规定并案侦查的案件，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

5.并案侦查的共同犯罪或者关联犯罪案件，犯罪嫌疑人人数众多、案情复杂的，公安机关可以分案移送审查起诉。分案移送审查起诉的，应当对并案侦查的依据、分案移送审查起诉的理由作出说明。

对于前款规定的案件，人民检察院可以分案提起公诉，人民法院可以分案审理。

分案处理应当以有利于保障诉讼质量和效率为前提，并不得影响当事人质证权等诉讼权利的行使。

6.依照前条规定分案处理，公安机关、人民检察院、人民法院在分案前有管辖权的，分案后对相关案件的管辖权不受影响。根据具体情况，分案处理的相关案件可以由不同审级的人民法院分别审理。

7.对于共同犯罪或者已并案侦查的关联犯罪案件，部分犯罪嫌疑人未到案，但不影响对已到案共同犯罪或者关联犯罪的犯罪嫌疑人、被告人的犯罪事实认定的，可以先行追究已到案犯罪嫌疑人、被告人的刑事责任。之前未到案的犯罪嫌疑人、被告人归案后，可以由原办案机关所在地公安机关、人民检察院、人民法院管辖其所涉及的案件。

8.对于具有特殊情况，跨省（自治区、直辖市）指定异地公安机关侦查更有利于查清犯罪事实、保证案件公正处理的重大信息网络犯罪案件，以及在境外实施的信息网络犯罪案件，公安部可以商最高人民检察院和最高人民法院指定侦查管辖。

9.人民检察院对于审查起诉的案件，按照刑事诉讼法的管辖规定，认为应当由上级人民检察院或者同级其他人民检察院起诉的，应当将案件移送有管辖权的人民检察院，并通知移送起诉的公安机关。人民检察院认为需要依照刑事诉讼法的规定指定审判管辖的，应当协商同级人民法院办理指定管辖有关事宜。

10.犯罪嫌疑人被多个公安机关立案侦查的，有关公安机关一般应当协商并案处理，并依法移送案件。协商不成的，可以报请共同上级公安机关指定管辖。

人民检察院对于审查起诉的案件，发现犯罪嫌疑人还有犯罪被异地公安机关立案侦查的，应当通知移送审查起诉的公安机关。

人民法院对于提起公诉的案件，发现被告人还有其他犯罪被审查起诉、立案侦查的，可以协商人民检察院、公安机关并案处理，但可能造成审判过分迟延的除外。决定对有关犯罪并案处理，符合《中华人民共和国刑事诉讼法》第二百零四条规定的，人民检察院可以建议人民法院延期审理。

三、关于信息网络犯罪案件的调查核实

11.公安机关对接受的案件或者发现的犯罪线索，在审查中发现案件事实或者线索不明，需要经过调查才能够确认是否达到刑事立案标准的，经公安机关办案部门负责人批准，可以进行调查核实；经过调查核实达到刑事立案标准的，应当及时立案。

12.调查核实过程中，可以采取询问、查询、勘验、检查、鉴定、调取证据材料等不限制被调查对象人身、财产权利的措施，不得对被调查对象采取强制措施，不得查封、扣押、冻结被调查对象的财产，不得采取技术侦查措施。

13.公安机关在调查核实过程中依法收集的电子数据等材料，可以根据有关规定作为证据使用。

调查核实过程中收集的材料作为证据使用的，应当随案移送，并附批准调查核实的相关材料。

调查核实过程中收集的证据材料经查证属实，且收集程序符合有关要求的，可以作为定案依据。

四、关于信息网络犯罪案件的取证

14.公安机关向网络服务提供者调取电子数据的，应当制作调取证据通知书，注明需要调取的电子数据的相关信息。调取证据通知书及相关法律文书可以采用数据电文形式。跨地域调取电子数据的，可以通过公安机关信息化系统传输相关数据电文。

网络服务提供者向公安机关提供电子数据的，可以采用数据电文形式。采用数据电文形式提供电子数据的，应当保证电子数据的完整性，并制作电子证明文件，载明调证法律文书编号、单位电子公章、完整性校验值等保护电子数据完整性方法的说明等信息。

数据电文形式的法律文书和电子证明文件，应当使用电子签名、数字水印等方式保证完整性。

15.询（讯）问异地证人、被害人以及与案件有关联的犯罪嫌疑人的，可以由办案地公安机关通过远程网络视频等方式进行并制作笔录。

远程询（讯）问的，应当由协作地公安机关事先核实被询（讯）问人的身份。办案地公安机关应当将询（讯）问笔录传输至协作地公安机关。询（讯）问笔录经被询（讯）问人确认并逐页签名、捺指印后，由协作地公安机关协作人员签名或者盖章，并将原件提供给办案地公安机关。询（讯）问人员收到笔录后，应当在首页右上方写明“于某年某月某日收到”，并签名或者盖章。

远程询（讯）问的，应当对询（讯）问过程同步录音录像，并随案移送。

异地证人、被害人以及与案件有关联的犯罪嫌疑人亲笔书写证词、供词的，参照执行本条第二款规定。

16.人民检察院依法自行侦查、补充侦查，或者人民法院调查核实相关证据的，适用本意见第14条、第15条的有关规定。

17.对于依照本意见第14条的规定调取的电子数据，人民检察院、人民法院可以通过核验电子签名、数字水印、电子数据完整性校验值及调证法律文书编号是否与证明文件相一致等方式，对电子数据进行审查判断。

对调取的电子数据有疑问的，由公安机关、提供电子数据的网络服务提供者作出说明，或者由原调取机关补充收集相关证据。

五、关于信息网络犯罪案件的其他问题

18.采取技术侦查措施收集的材料作为证据使用的，应当随案移送，并附采取技术侦查措施的法律文书、证据材料清单和有关说明材料。

移送采取技术侦查措施收集的视听资料、电子数据的，应当由两名以上侦查人员制作复制件，并附制作说明，写明原始证据材料、原始存储介质的存放地点等信息，由制作人签名，并加盖单位印章。

19.采取技术侦查措施收集的证据材料，应当经过当庭出示、辨认、质证等法庭调查程序查证。

当庭调查技术侦查证据材料可能危及有关人员的人身安全，或者可能产生其他严重后果的，法庭应当采取不暴露有关人员身份和技术侦查措施使用的技术设备、技术方法等保护措施。必要时，审判人员可以在庭外对证据进行核实。

20.办理信息网络犯罪案件，对于数量特别众多且具有同类性质、特征或者功能的物证、书证、证人证言、被害人陈述、视听资料、电子数据等证据材料，确因客观条件限制无法逐一收集的，应当按照一定比例或者数量选取证据，并对选取情况作出说明和论证。

人民检察院、人民法院应当重点审查取证方法、过程是否科学。经审查认为取证不科学的，应当由原取证机关作出补充说明或者重新取证。

人民检察院、人民法院应当结合其他证据材料，以及犯罪嫌疑人、被告人及其辩护人所提辩解、辩护意见，审查认定取得的证据。经审查，对相关事实不能排除合理怀疑的，应当作出有利于犯罪嫌疑人、被告人的认定。

21.对于涉案人数特别众多的信息网络犯罪案件，确因客观条件限制无法收集证据逐一证明、逐人核实涉案账户的资金来源，但根据银行账户、非银行支付账户等交易记录和其他证据材料，足以认定有关账户主要用于接收、流转涉案资金的，可以按照该账户接收的资金数额认定犯罪数额，但犯罪嫌疑人、被告人能够作出合理说明的除外。案外人提出异议的，应当依法审查。

22.办理信息网络犯罪案件，应当依法及时查封、扣押、冻结涉案财物，督促涉案人员退赃退赔，及时追赃挽损。

公安机关应当全面收集证明涉案财物性质、权属情况、依法应予追缴、没收或者责令退赔的证据材料，在移送审查起诉时随案移送并作出说明。其中，涉案财物需要返还被害人的，应当尽可能查明被害人损失情况。人民检察院应当对涉案财物的证据材料进行审查，在提起公诉时提出处理意见。人民法院应当依法作出判决，对涉案财物作出处理。

对应当返还被害人的合法财产，权属明确的，应当依法及时返还；权属不明的，应当在人民法院判决、裁定生效后，按比例返还被害人，但已获退赔的部分应予扣除。

23.本意见自2022年9月1日起施行。《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》（公通字〔2014〕10号）同时废止。

最高人民法院 最高人民检察院 公安部
2022年8月26日

在“依法惩治电信网络诈骗 协同推进网络诉源治理”研讨会上，专家表示——

构建多维治理电信网络诈骗体系

综述

□全链条惩治电信网络诈骗，关键是从黑灰产链条入手，由上（游）及下（游），以下（游）溯上（游），努力挤压犯罪生存空间；同时，更加重视加强对前端涉个人信息犯罪的惩治，尤其是要把批量提供个人信息、提供个人敏感信息的行为作为打击重点，坚决杜绝为电信网络诈骗犯罪“输血供粮”的现象。

□将合规科技应用到个人信息保护领域，既有个人信息违法巨额罚款甚至刑事责任的压力，也有个人信息保护与个人信息利用更好融合的动力。发展个人信息处理合规科技，是实现源头治理的关键一招。

□本报记者 刘金林

“根除电信网络诈骗，需要构建多维治理体系。”在8月26日举行的“依法惩治电信网络诈骗，协同推进网络诉源治理”研讨会上，与会专家围绕“电信网络诈骗犯罪形势发展和惩治对策”“电信网络诈骗犯罪涉案资金处置和追赃挽损”“电信网络诈骗犯罪源头预防和诉源治理”三个议题展开深层次、系统性探讨。研讨会由检察日报社、最高人民检察院第四检察厅主办，人民检察杂志社承办。

对电信网络诈骗需要全链条惩治

电信网络诈骗及其关联犯罪严重侵害群众财产安全，严重破坏社会诚信，严重影响社会和谐稳定。

公安部刑事侦查局处长张硕表示，电信网络诈骗犯罪在世界各国呈现迅猛增长态势，已成为全球性的打击治理难题。一是诈骗手法加速迭代变化。诈骗集团紧跟社会热点，诈骗类型不断翻新，话术套路不断升级，诈骗手法加速融合变化。二是技术支撑更加专业复杂。诈骗集团利用区块链、AI智能、GOIP等各种新技术新业态，不断翻新犯罪工具，技术专业性不断增强。三是跨国有组织特征日趋明显。境外诈骗集团组织严密、分工明确，其多行业支撑、产业化分布、集团化运作、精细化分工等特征日趋明显，目前电信网络诈骗境外作案占比达80%。

正是由于境外作案占比极大，境外取证成为绕不开的坎。**北京市海淀区检察院第二检察部主任许丹**提出，电信网络诈骗团伙成员之间广泛使用具有端到端加密、阅后即焚、私密聊天等功能的加密通信软件，且多为远程操控、上下单线联系。囿于软件服务器往往在境外，关键电子数据如聊天记录、用户数据会出现调取不能、不复存在的情况。**最高法刑事审判第三庭审判长陈攀**也认为，目前境外执法取证受多种客观因素制约，存在境外证据特别是相关物证不移交，或者移交不全面、不及时、不规范等问题，给后期诉讼带来后遗症，影响打击效果。

随着近几年直播短视频平台的火热，网络诈骗也火速“跟进”。**快手集团法务副总裁蔡雄山**总结出典型网络诈骗五大特点：一是精准性。诈骗团伙会借助平台个性化推荐功能，更精准地传递给目标用户，这是平台治理中遇到的一大难点。二是迷惑性。三是隐蔽性。四是小额性。单个诈骗金额较小，受害者由于被诈骗金额较小，加之怕麻烦心理往往不愿意报案。五是外链性。诈骗团伙利用短视频前端吸粉，私信添加好友后引流至第三方软件或后端引至赌博网站、虚假投资网站等实施诈骗。

“魔高一尺，道高一丈。”**全国人大代表、九三学社中央委员阎建国**建议，公安机关既要始终保持严打高压态势，又要根据电信网络诈骗犯罪的特点，不断创新打击方式方法。比如，开展网络技术培训，提高经济犯罪侦查人员的网络技术素质，创新网络技术辅助侦查模式；整合涉案地区甚至全国优秀的经济犯罪侦查力量和资源，推进各地区信息共享，提高打击惩治犯罪的效果；建立情报信息库，充分利用各渠道情报资源，引导侦查方向，提高侦查效率。

面对大数据技术正在兴起的新形势，针对信息孤岛或信息不对等、不匹配等现象，**最高检检察技术信息研究中心主任刘喆**提出，从技术上看，联邦计算、隐私计算和算法共识等技术，完全可以保证数据“可用不可见，可用不可有”，确保数据安全。由此可以解决数据共享问题，让数据资源充分释放，让数据碰撞产生“化学反应”。刘喆还建议，提升电子证据取证规则法律层级，并对取证过程各环节制定更为细化的操作规则。

严惩电信网络诈骗，加强多部门合作成为共识。**检察日报社副总编辑李国明**提出，如何有效精准惩治电信网络诈骗犯罪，如何在打击犯罪的同时做好追赃挽损工作，特别是如何加强电信网络诈骗犯罪诉源治理，挖掉犯罪之“根”，既是司法实践难题，也是社会治理难题，需要各方共同努力，协同推进。**全国人大监察和司法委员会司法室处长郭海燕**也表示，全国人大常委会办公厅将“严厉打击电信网络犯罪，加强个人信息司法保护”的8件建议确定为重点督办建议，交由最高检牵头办理。最高检已经形成一套比较科学的工作机制，办出了成效，但是，还需要有关各方通力协作。

结合“反电信网络诈骗法”草案审议，**全国人大常委会法工委刑法室副主任许永安**介绍，该法注重协调惩治和防范的关系，立足综合治理、源头治理和依法治理，侧重前端防范，按照完善预防性法律制度的要求加强制度建设，变“亡羊补牢”为“未雨绸缪”，变重“打击”为“打防管控”并重。基于该法将对网络黑灰产以及电信、金融、互联网行业违反法律规定的行为给予行政处罚，**最高检第四检察厅主办检察官赵玮**提出，应加强行政执法信息在刑事司法中共享使用。行为人因类似行为受过行政处罚又实施的，往往是证明主观明知的重要证据之一。随着该法通过施行，相关行政处罚信息将实现同步移送、共享，将有力破解电信网络犯罪主观证明难题，实现对这类犯罪的全链条打击。

关于全链条惩治电信网络诈骗，**最高检第四检察厅副厅长程雷**表示，关键是从黑灰产链条入手，由上（游）及下（游），以下（游）溯上（游），努力挤压犯罪生存空间；同时，更加重视加强对前端涉个人信息犯罪的惩治，尤其是要把批量提供个人信息、提供个人敏感信息的行为作为打击重点，坚决杜绝为电信网络诈骗犯罪“输血供粮”的现象。

涉案财物处置与定罪量刑并重

众所周知，作为电信网络诈骗案件后端的资金处置、追赃挽损一直是办案难题。

如何比犯罪分子的手更快？围绕涉诈银行账户和资金处置问题，**公安部国家反诈中心专家杨琛**介绍了公安机关会同中国人民银行等部门推进资金链治理的“组合拳”：紧急止付；即时查询；快速冻结，尤其是对前期紧急止付工作中拦截的涉案资金，第一时间进行冻结，以便开展后期资金返还工作；资金预警；加强对涉案银行账户管控；等等。

对于资金流转链条中的虚拟货币问题，许丹分享了办案经验：尝试由公安机关生成并提供比特币地址，犯罪嫌疑人将其账户内的比特币转移至该地址，最终账户的公钥私钥由公安机关唯一控制掌握，这样可以避免涉案比特币被转移。但目前，虚拟货币如何变“实”，尚无法定程序，急需顶层设计支持。

就电信网络诈骗犯罪案件涉案财物处置问题，**最高法研究室处长喻海松**认为，公检法机关要落实好涉案财物处置的各自职责，从公安机关收集证据、检察机关提出处理意见、法院裁判处理等环节，真正做到涉案财物处置与定罪量刑并重。对应当返还被害人的合法财产，依法及时返还。

中国银行保险监督管理委员会法规部处长周兰领表示，银保监会将积极配合公安机关继续做好涉案账户查询、止付、冻结等工作，持续推进涉案账户资金网络查控平台建设。进一步研究完善相关技术规范，推动尽早实现资金查控数据证据转化工作目标；继续配合公安机关、检察机关等做好涉案账户资金处置等工作，督促指导银行业金融机构严格落实好各项工作要求。

构建个人信息“多维保护”立体化框架

保护好个人信息，才能对电信网络诈骗实现源头治理。**全国人大代表、辽宁安行律师事务所创始合伙人李宗胜**建议，各部门执法、司法过程中，破获一起案件都要尽可能从中梳理出违法犯罪的脉络和关键节点，梳理出哪个环节出现了疏漏，从而发现个人敏感信息泄露来源，防范“视而不见”“放任自流”现象，在电信网络诈骗的信息传输源头上构建立体化治理框架。

反电信网络诈骗的经验教训证明，防止“一老一幼”被骗和防止因关切“一老一幼”被骗，既是“打防管控”重点，也是“群防群治”难点。**最高检第八检察厅二级高级检察官邱景辉**认为，对老年人、儿童、妇女、残疾人等特定群体的个人信息，特别是生物识别、金融账号、行踪轨迹等敏感个人信息要进行特别保护，检察机关精准针对买卖、泄露、滥用上述特定群体个人信息的违法犯罪行为开展公益诉讼，斩断个人信息侵权与电信网络诈骗之间的利益链条。

开展个人信息保护，互联网平台企业如何作为？**蚂蚁集团首席隐私官聂正军**提出，应坚持三项原则：一是公开透明原则。隐私政策简明易懂，充分保障用户知情权。二是“三同时”原则。产品设计时，同时制定隐私保护和数据安全的管理方案；产品方案开发时，同时实施隐私保护和数据安全管理措施；产品上线运行时，同时上线运行隐私保护和数据安全管理功能。三是“三要三不要”原则。要给用户安全感，要用数据给用户创造价值，要确保安全与合规；不要替用户做主，不要滥用数据，不要采集来历不明的数据。

清华大学法学院教授劳东燕对于“三同时”原则深表赞同，并认为法律应该及时跟上。个人信息保护的法律基本归责机制的构建应受到重视，劳东燕建议考虑四个因素：一是相应的风险是谁创设。制造这种风险的人应该对风险及其结果负责。二是谁是利益的最大获得者。获得利益最大的，承担的风险应该最高。三是谁预防能力比较高。在技术社会中，能力越高，责任越大。四是法律惩罚哪个主体最能起到预防效果。比如让银行承担部分过错，表面上看对银行不利，但这会倒逼银行提高技术安全保障，从而从根源上防止信息泄露。

技术赋能，必不可少。**中国社会科学院法学研究所网络与信息法研究室副主任周辉**表示，应通过以合规技术反制电信网络诈骗技术，赋能加强个人信息保护，避免个人信息被不法分子非法利用，不断增强实现电信网络诈骗的源头治理效能。将合规科技应用到个人信息保护领域，既有个人信息违法巨额罚款甚至刑事责任的压力，也有个人信息保护与个人信息利用更好融合的动力。发展个人信息处理合规科技，是实现源头治理的关键一招。