网络犯罪治理的实务难题及其立法完善

李书静* 吴成杰**

【摘 要】我国网络犯罪治理在立法技术上未形成专门的法律规范，在内容上未能满足网络时代带来的法律难题治理需求。须正视网络犯罪行为“时空分立”、电子数据成为重要定案依据、逐一收集被害人陈述难度大等特性带来的法治范式变革。司法上在回归刑事案件“排除合理怀疑”证明标准的前提下，能动性地运用“差异化证明标准”，推动形成科学合理的证据采信规则，这一点具有现实性、紧迫性和必要性。对于涉众型网络诈骗犯罪案件的涉案财物处理，有必要进一步加强立法规范，堵塞对第三方支付机构的监管漏洞，确保能够用好用足法律手段查清被害人信息和诈骗资金流向，加快冻结诈骗资金向被害人返还进度，及时挽回被害人的财产损失，实现办理案件与追赃挽损并重的最新司法理念要求。应当结合案件审判实际，修改有违法理逻辑、内容缺漏、法意表达不准确等不协调的法律条文，力求规范合理、内容协调一致，避免法律适用过程中存在理解分歧，确保案件定性准确、量刑步骤规范及被害人损失退赔到位。

【关键词】网络犯罪；证据采信；财物处理；立法完善

引 言

近年来，随着信息技术与应用的快速发展，我国网络犯罪活动日益增多且手段不断翻新，除了公众普遍熟悉的电信网络诈骗案件[1]外，一些不法分子通过银行资金归集业务[2]的信息技术漏洞、利用黑客技术非法入侵并控制他人账户[3]、注册淘宝店铺以虚假交易方式套现他人信用卡、骗取他人使用支付宝扫描虚假二维码付款等方式实施犯罪的新类型案件日渐增多，已严重危及社会的安全和稳定。目前，我国虽然在网络犯罪治理上出台了一系列法律法规或规范性文件，如针对危害计算机信息系统安全、侵犯公民个人信息、电信网络诈骗等刑事案件出台司法解释或指导性意见，为有效打击网络犯罪提供了法律依据。但从司法实践来看，网络犯罪治理的突出难点在于证据采信标准的认定和冻结诈骗资金的返还以及条文法意表达不明确引发适用争议等方面，既关系到案件定罪量刑的打击实效问题，还关系到被害人财产损失的权益保护问题。为此，本文拟以 A 市两级法院近两年来网络诈骗案件的审理数据以及市公安局反诈骗中心的工作数据为依托，结合司法工作实际，在掌握情况、发现问题、剖析原因、总结经验的基础上，对解决相关难题提出对策建

* 厦门大学法学院博士研究生，厦门大学社会治理与软法研究中心研究员。
** 厦门市中级人民法院刑二庭法官助理，法学硕士。

[1] 电信网络诈骗案件是指不法分子利用电信、互联网等技术，通过发送短信、拨打电话、植入木马等手段，诱骗（盗取）被害人资金汇（存）入其控制的银行账户，实施的违法犯罪案件。参见中国银监会、公安部联合下发的《电信网络新型违法犯罪案件冻结资金返还若干规定》（银监发 [2016]41 号）第 2 条的规定。

[2] 银行资金归集业务是银行根据客户的约定，即时或定期将一个或多个指定账户的资金全部或部分转入另一个指定账户的业务。

[3] 恶意代码即服务（Malware-as-Service）、勒索软件即服务（Ransomware-as-Service）、DDoS 即服务等新的“黑产”形态出现，使得网络犯罪分子通过支付即可“享受”网络攻击服务，进一步降低了网络犯罪的门槛。

议，以期为新时期下网络犯罪治理提供帮助。

一、回归“排除合理怀疑”的证明标准，正确运用证据采信规则

当前，不法分子借住网络实施犯罪已然成为一大发展趋势，而利用网络实施诈骗是其中的第一大犯罪类型，即便是传统的电信网络诈骗犯罪，其犯罪手段也随着信息化时代的到来发生翻天覆地的变化，更遑论其他新型的网络犯罪案件。因此，研究如何正确运用证据采信规则，对于有效打击网络诈骗犯罪来讲意义重大。尤其是当前全面推进以审判为中心的背景下，严格证明标准、严格证据审查成为当前刑事审判工作的重点，其核心要义是据以定罪的证据不能存在合理怀疑。为此，鉴于网络诈骗犯罪在证据收集上存在电子数据多、被害人人数众多、同案犯先后到案情形多等“三多”特征，如何在坚持“排除合理怀疑”证明标准的前提下，在网络犯罪案件审理中正确适用证据采信规则，关系到打击网络诈骗犯罪的成效。

（一）关于电子数据的审查认定

电子数据作为现代网络信息社会的新兴证据种类和“证据之王”，[4] 近来备受理论和实务界关注。2016年9月，“两高一部”结合司法工作实际，制定出台了《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《电子数据规定》），对刑事诉讼中电子数据的收集、提取、审查、认定等行为予以规范，这在我国刑事证据制度发展中具有重要的里程碑意义。但正如有观点提出，传统刑事诉讼规则中调整证据收集使用、审查认定的相关制度并不能完全适用于电子数据这一新型证据种类。[5] 对于一些未完全遵守法定程序收集的电子数据，究竟是应当认定为非法证据，还是应当认定为瑕疵证据，在司法实践中仍有进一步明确的必要。在进行合法性审查的同时，如何审查电子数据的证明力也是实践中的一个难题。[6] 审查判断包括电子数据在内的所有证据均应基于证据能力和证明力规则，这也是证据裁判主义的应有之意。[7] 而从目前司法实践来看，在我国刑事诉讼过程当中，电子证据的审查还没有统一明确的标准，没有形成规范化的电子证据审查体系。[8]

从网络诈骗案件来看，层出不穷的新型互联网犯罪自身具有的网络身份难以查清、证据变动性强、证据评价标准高、取证技术要求复杂等特点，也给电子数据证据评价、采信工作带来了极大的难度。[9] 比如，电信网络诈骗囿于取证工作量大、证据种类较多且被害人众多核实工作量大，加上《电子数据规定》的立法较为前沿，有的地方的侦查机关受主客观条件限制 [10]，尚未能严格依法对网络犯罪中有关 CDR 数据查询、SKYPE 记录数据、磁盘、通讯记录等电子数据进行取证，使得实践中有的电子数据是以司法鉴定中心电子数据检验报告等形式呈现，有的电子数据是以电子截图（如支付宝转账截图、存证云合同截图、微信微博聊天截图、电子借贷合同截图）等打印件形式呈现。[11] 正如有观点提出，电子数据收集主体的理想状态就是收

[4] 参见刘品新：《电子证据的基础理论》，《国家检察官学院学报》2017年第1期。

[5] 参见谢登科：《论电子数据与刑事诉讼变革：以“快播案”为视角》，《东方法学》2018年第5期。

[6] 参见李睿懿、韩景慧：《电子数据的证据资格和证明力的审查与判断》，《中国检察官》2017年第8期。

[7] 参见占善刚、王超：《电子数据证据能力的审查判断》，《人民检察》2018年第8期。

[8] 参见陈思：《刑事诉讼电子数据审查探讨》，《中国检察官》2018年第3期。

[9] 参见罗文华、孙道宁、赵力：《电子数据证据评价问题研究》，《河北法学》2017年第12期。

[10] 正常来讲，公安机关内部通常由网络安全保卫部门负责收集、提取电子数据，但在越来越多类型的案件涉及电子数据的情况下，经侦、治安、刑侦、禁毒等警种甚至派出所都需要承担相应的电子数据收集、提取任务，电子数据取证呈现普及化趋势，容易造成电子数据取证过程中存在程序不规范或存在瑕疵等情形。参见周加海、喻海松：《〈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〉的理解与适用》，《人民司法》2017年第28期。

[11] 经统计A市法院的审理数据，有高达60%网络诈骗案件中的电子数据最后是以转化为检控方书面材料的形式呈现，而不能提供电子数据的原始介质或者完整备份。

集电子数据的侦查人员具有相应专业知识，但在司法实践中，经常会出现收集电子数据的侦查人员不具有相关专业技术，或者具有相关专业技术的电子数据取证人员不是侦查人员的两种情形。[12] 甚至有学者明确指出，《电子数据规定》中关于取证主体的规定，未充分反映现实情况与工作需要，亦可能与相关制度相冲突。[13]

对于以上述第一种形式体现的电子数据，辩护人主要从电子数据的证据能力角度提出辩护，如果侦查机关的收集取证程序符合电子数据规定，控辩审三方一般不持异议；对于以第二种形式呈现的电子数据，辩护人往往以证据形式不符合规则等为由，提出其不具有证据能力的辩护意见。例如，在一起诈骗案件中，由于被害人的 QQ 聊天记录已经灭失且不能恢复，侦查机关就将被害人自行整理并打印的聊天记录作为证据使用，聊天记录本是证明被告人虚构事实、隐瞒真相进行诈骗的关键性证据，但是由于侦查机关收集取证的过程不规范致使此证据的效力大大减弱。[14] 在此情况下，对于网络犯罪案件中涉及的电子数据，在司法实践中如何审查认定，关系到案件罪与非罪、犯罪数额多与少等定性和事实的认定，迫切要求司法机关需要对其证据资格作出审慎认定。不可置否，刑事案件“事实清楚，证据确实充分”的法定证明标准，任何时候都不能动摇，但这更多的是强调从证据印证规则角度来看待问题，而非针对某一单项证据是否具有证明能力，毕竟以“孤证”认定犯罪事实是证据裁判原则中最大的忌讳之一。对于电子数据来讲，其作为一种独特属性的证据种类，且往往只是网络犯罪事实认定的较多证据种类之一，其印证证明与传统证据相比较存在较大差异，如果只要以其不符合《电子数据规定》的要求，就意味着要一律认定不作为证据使用，这并不符合当前司法实践的现状和需求。事实上，我国特定历史时期及特定社会治安环境下产生的“两个基本原则”，即“基本事实清楚，基本证据确凿”，[15] 也进一步阐释了犯罪事实的认定并非仅仅依靠单一证据，更多的是审判人员运用印证证明方法进行单个证据的证明力判断和全案证据的综合判断。[16] 可见，随着网络时代带来法治范式的变革，对于涉及互联网犯罪的刑事证据证明标准的实践应用，尤其是如何运用印证证明方法对证据采信证明标准作出准确认定，已经呈现出一个不断更新和演变的态势。

不可否认的是，印证证明模式在认定案件事实，规范证据证明力审查判断标准等方面具有一定积极作用，对我国刑事司法实践产生了较为深远的影响。[17] 即它强调证实犯罪证据的充分性、体系性，也有利于分析、论证是否“排除合理怀疑”。[18] 具体到网络犯罪，司法机关要不断更新司法理念，结合网络犯罪证据的特殊属性，正确运用证据印证规则，对性质和种类不同的电子数据区分适用不同的证据采信标准。一方面，对于以司法鉴定中心电子数据检验报告等形式呈现的电子数据，如果其是认定案件犯罪事实的关键或核心证据，即便有其他建立关联的直接证据或能够形成锁链的间接证据，只要该电子数据的证据形式不符合《电子数据规定》就不能采信。以通过办理资金归集业务实施网络诈骗为例，资金归集业务可通过 U 盾在网上办理即可签约成功，资金归集业务签约后，收款方可以随时从付款方账户转款，不再需要付款方的 U 盾或密码或口令即可完成。如果行为人辩解其未通过网上办理资金归集业务且 U 盾可能存在病毒感染或登录中存在黑客非法入侵而被动办理资金归集业务，且该辩解得到一定客观证据如监控录像显示，相关资金归集业务办理成功的时点是在网吧电脑上操作完成等，那么对于起诉指控行为人通过向他人借款转入

[12] 同注 5。

[13] 参见龙宗智：《寻求有效取证与保证权利的平衡——评“两高一部”电子数据证据规定》，《法学》2016 年第 11 期。

[14] 参见陈耀武、彭辉：《电子数据类证据司法适用的困惑及应对措施》，《中国检察官》2017 年第 4 期。

[15] 其核心是要求不纠结细枝末节，从重从快惩治犯罪。只是实践中有的将其异化为“事实基本清楚、证据基本充分”，这种异化后的司法理念是要坚决杜绝的，容易把内心确认与法定证明标准混为一谈。

[16] 印证规则主要是通过两个以上不同来源的证据内容相互证实或者指向同一证明方向来实现的。参见王祺国、王晓霞、周迪：《网络犯罪中的印证证明》，《人民检察》2018 年第 3 期。

[17] 参见展中华：《“印证”刑事证明模式的实践考察与反思》，《中国检察官》2018 年第 1 期。

[18] 参见左卫民：《“印证”证明模式反思与重塑：基于中国刑事错案的反思》，《中国法学》2016 年第 1 期。

行为人银行卡的合法资金，因行为人辩解不知道该卡存在资金归集业务而被他人转走钱款并非法占有的，如何认定行为人是否以借款为名实施诈骗之实。在此情况下，对于侦查机关调取的行为人在某个时点使用其笔记本电脑访问网上银行办理资金归集业务及登陆 IP 地址等证实系行为人办理资金归集业务唯一性的电子数据，如果侦查机关取证存在不符合《电子数据规定》的情形，比如对扣押的电脑、U 盾没有进行封存或未对电子数据进行证据固定并计算出电子数据的完整校验值，无法排除在侦查过程中存在电子数据被毁坏、篡改或者伪造的可能，且侦查机关不能补正或作出合理解释等情况，即因该证据不具有适格性而不具备证据能力，那么即便有其他证人证言、监控录像等关联证据证实行为人有在那个时点上网办理过银行业务，因在案证据不能排除在行为人不知情的情况下，被他人截取信息、入侵银行账户并办理资金归集业务的合理怀疑，故相关电子数据不能作为定案依据。

另一方面，对于以电子截图等打印件形式呈现的电子数据，如果不是定案的关键或核心证据，且能够查明其来源合法，又能够与在案查明的其他证据能够相互印证、形成完整证据链条，那么相关电子数据可以采信。正如有学者提出，我国正步入电子数据时代，电子数据不可避免地成为主要的证据载体，其表现出的新特征需要建立完善的证据规则体系进行规范，只有法律层面的完善和制度层面的改变，方可使得电子证据合法、合理、充分地被运用，从而实现电子证据应有的功能和作用。[19] 以电信网络诈骗为例，实践中有关诈骗数额的认定并非仅仅依靠电子截图等电子数据，而是还有被害人陈述、被告人供述、银行卡转账记录等其他证据予以印证，如果侦查机关能够补正说明相关电子截图均有邮寄单据证明系由被害人直接邮寄给公安机关，取证程序合法性得以确认，且被害人陈述的内容及电子截图反映的情况均经被告人确认，电子数据检验报告证明被害人提供的电子借款合同截图与被告人使用账户的借款合同内容亦一致，从证据印证规则和全案综合判断角度来看，有关电子截图等电子数据的真实性足以确认，可以作为定案依据。正如有观点提出，办案机关违反有关规定提取的证据存在形式上的瑕疵，属于瑕疵证据，司法实践中对其排除要持慎重态度，但对电子数据取证程序的瑕疵，也要予以补正或者作出合理的解释。[20] 对于瑕疵证据可以通过情况说明或者提交其他证据予以补正，补正之后的电子数据能够与其他证据相互印证的，则可以作为定案根据，[21] 对于双方均认可的电子数据，根据自认规则，对一方当事人自认的事实，原则上法院可将其作为裁判的依据。[22] 由此，要准确适用印证这种证据分析方法或者证据审查判断方法，[23] 通过不同证据之间相互印证能够提高单个证据的可靠性，特别是可靠性较高的证据与可靠性较低的证据相互印证时，可以使可靠性较低的证据的真实性得到较大的提升。[24] 如此操作，也更加符合电子数据取证的现实合理性和打击网络犯罪的实际需要。

（二）关于涉众型网络诈骗数额的审查认定

当前，为应对互联网时代犯罪的新变化，需要刑事证据制度作出调整和完善。[25] 对于涉众型网络诈骗犯罪案件来讲，鉴于犯罪手段的特殊性，实践中被害人的分布面较广，逐一搜集被害人陈述的调查取证难度大甚至有的被害人都无法查明，加上有的被告人参与作案时间的时点不一且不易查明，辩解用于接受诈骗赃款的涉案银行卡系向他人购买或提供，不排除在其参与作案之前或使用期间存在同时被其他不法分子使用的可能，以及辩解涉案银行卡的往来款项中，有其他正当收入来源或者不承认接受的部分钱款系诈骗

[19] 参见樊崇义、李思远：《论电子证据时代的到来》，《苏州大学学报（哲学社会科学版）》2016 年第 2 期。
[20] 同注 6。
[21] 参见刘品新：《印证与概率：电子证据的客观化采信》，《环球法律评论》2017 年第 4 期。
[22] 参见娄琳莉：《论电子数据的可采性和证明力认证规则》，《广西政法管理干部学院学报》2018 年第 1 期。
[23] 参见王星译：“‘印证理论’的表象与实质——以事实认定为视角”，《环球法律评论》2018 年第 5 期。
[24] 同注 16。
[25] 参见徐庆天：《浅谈刑事案件差异化证明标准》，《犯罪研究》2016 年第 6 期。

所得等情形，使得涉案银行卡账户接受的钱款是否为诈骗钱款的认定，往往成为此类案件审理的一大难题。如何从证据采信规则角度，对该部分数额的定性作出准确认定？鉴于此，全国各地司法机关积极探索实践，有的还出台了相关指定性文件，如2007年福建省高级人民法院、省人民检察院、省公安厅三家下发的《关于办理虚假信息诈骗案件若干问题的意见》中明确规定：有证据证明行为人供认其拥有的银行账户是专门接受虚假信息诈骗钱款的，账户内款项来源虽未查到被害人或只查证到部分被害人，该账户内的金额可认定为诈骗数额。然而，该文件仅是地方性司法文件，且更多的是一种政策性导向而不具备法律层面的约束力，实践指导意义和效果相当有限。为此，2016年12月，“两高一部”《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（以下简称《电信网络诈骗意见》）第6条第1项，在参照《关于办理网络赌博犯罪案件适用法律若干问题的意见》第3条、《关于办理非法集资刑事案件适用法律若干问题的意见》第6条、《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》第20条等规范性文件的相关规定的基础上，并结合司法工作实际，进一步从规范性司法文件角度明确相关法律适用问题，即确因被害人人数众多等客观条件的限制，无法逐一收集被害人陈述的，可以结合已收集的被害人陈述，以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据，综合认定被害人人数及诈骗资金数额等犯罪事实。然而，鉴于实践中不同个案的案情有别，一些作案情节认定存在多样性，如何正确理解《电信网络诈骗意见》规定、统一法律适用认识和证据采信标准，亟待研究解决。从A市法院的审判实践来看，有的公诉机关会将案件查处涉及的银行卡都认定为是用于诈骗的银行卡，进入该账户的钱款均视为诈骗款，而不论是否有收集被害人的陈述；有的公诉机关根据传统的证据印证规则，只将银行账户明细入账钱款中能收集到被害人陈述的部分认定为诈骗金额。可见，二者指控证明标准的差异，给审判工作带来较大困扰，前者从打击犯罪分析更符合实际所需，后者从传统证据证明标准角度更具合理性。[26] 这就要求审判机关在对相关犯罪数据进行认定时，要准确理解证明标准的法律内涵和实践应用，既不人为降低证明标准，造成对当事人合法权利保障不力，又不脱离实际盲目提高证明标准，影响打击犯罪的力度和效果。

从当前理论界和实务界对证明标准的前沿研究情况来看，已经有专家结合时代背景和现实意义，提出构建刑事案件差异化证明标准的建议。[27] 孟建柱同志在2016年中央政法工作会议上指出，要研究对被告人认罪与否、罪行轻重、案情难易等不同类型案件，实行差异化证明标准。实际上，差异化证明标准已经具有一定的理论基础且在司法实践中业已得到实际应用。如在审理死刑案件中，应当坚持最严格的证据标准和办案程序，[28] 除需要排除合理怀疑以外，还需要排除其他可能性，体现了立法机关对死刑案件和普通刑事案件在证明标准适用上有所差异的态度。[29] 而在适用认罪认罚从宽制度尤其是适用速裁程序审理的案件中，有观点指出刑事司法实践中证明标准已经降低的事实，[30] 如A市政法各部门联合制定司法程序及证据标准化意见，比照被告人认罪案件中“适当降低证明标准”的程度进行适用，自2016年11月至2018年10月，两级法院点适用认罪认罚从宽制度审理一、二审案件（包括一审涉外案件）共计5636件6040人，无抗诉案件，统筹兼顾了案件质量和效率问题，进一步体现了特定范围内的案件在刑事证明标准适用上的针对

[26] 参见吴成杰、陈雯：《电信网络诈骗案件中的疑难问题探讨》，《法律适用》2017年第21期。

[27] 即有的认为差异化证明标准的设定应该以类案划分，不同类别的案件划定不同的证明标准；有的认为刑事案件的判定要求事实清楚、证据确实充分，但在不同犯罪案件中，达到证据确实、充分必然存在不同的标准，因此差异化证明标准也是刑事诉讼的规律之一，有助于避免错误地认定犯罪和放纵犯罪，使每一个案件能准确地体现公平正义；有的认为实施差异化证明标准，必须严格遵守刑事诉讼的基本原则，如排除合理怀疑等，以确保法律的统一正确实施。参见林中明：《应构建刑事案件差异化证明标准》，载《检察日报》2016年4月7日第3版。

[28] 2010年“两高三部”《关于办理死刑案件审查判断证据若干问题的规定》不仅全面规定了死刑案件的刑事诉讼证据基本原则，细化了证明标准，还进一步具体规定了对各类证据的收集、固定、审查、判断和运用。

[29] 参见陈思：《论刑事案件差异化证明标准的证成》，《中国检察官》2017年第6期。

[30] 参见闵丰锦：《多维度与差异化：认罪认罚案件的证明标准探析》，《证据科学》2017年第4期。

性与差异性。

具体到网络犯罪案件的审理上，如果采取与死刑案件同样的证据证明标准，显然不切实际，毕竟网络犯罪与死刑案件的作案方式、定案的重要证据种类等方面存在较大差异，达到证据确实、充分必然存在不同的标准。实践中，相关司法文件规定亦体现该种精神。比如，正如前文所述，《电信网络诈骗意见》第6条第1项对有关证据收集和审查判断作出规定，明确了特定情形下的有关犯罪数额可予推定。[31] 即在电信网络诈骗犯罪案件中“犯罪数额”采用推定的证明标准，而推定在证明标准上，不要求达到“确实、充分”，不仅有效防止了实践中因证明不能而放纵犯罪，也节约了司法资源，降低了诉讼成本。[32] 那么，对于前文所述关于涉案银行卡账户接受钱款的性质认定，面对被告人及其辩护人提出的辩解辩护意见，且在无法逐一收集涉案银行卡转入方即“潜在被害人”陈述的情况下，如何根据有关规定对犯罪数额予以推定，且达到“排除合理怀疑”的证明标准，是当下网络犯罪案件审理的一大证据采信规则运用问题。对此，在适用《电信网络诈骗意见》第6条第1项规定的特殊证明规则时，需要重点把握以下两点：首先，有关记录被害人数、涉案资金数额等犯罪事实已经在案书证、电子证据等证据查证属实。换言之，相应的客观性证据已经足以证明基本犯罪事实，如通过网络服务运营商、第三方支付机构、商业银行等提供的帮助，从诈骗网站后台技术分析数据得出被害人情况，通过银行资金流水计算涉案金额等。即在电信诈骗类案件中，缺少被害人陈述，并非意味着数额认定可以没有印证，数额认定仍需遵循事实推定的印证模式才是符合我国最低证明标准的。[33] 然而，由于受资金层层分转进入“资金池”流转、资金流中有第三方机构加入等客观条件的限制无法查明被害人信息，导致逐一收集相关言词证据的难度大。如果部分证人证言因客观原因而无法收集到，但综合分析全案证据能够锁定基本犯罪事实，能够排除合理怀疑，则没有必要过分追求证据数量上的充分性。[34] 需要明确的是，对于有条件取得的被害人陈述，还是应当尽量取证，特别是对一些具有典型性、代表性的被害人陈述，一般应当取证。[35] 其次，对于被告人及其辩护人提出的辩解、辩护意见要认真审查，在坚持“排除合理怀疑”证据证明标准的前提下，结合全案证据材料，对相关犯罪数额做出认定。例如，对于涉案银行卡接收钱款性质的认定，要结合银行卡是否实际缴获到案、是为该被告人完全控制还是无法排除同时被其他诈骗人员用于接受诈骗钱款等可能性、所接受款项是否发生在其实施诈骗行为期间、被告人是否从事其他正常商业活动等情形综合认定。[36] 在适用证据采信规则时，有观点提出必须要有证据证明账户是用于诈骗犯罪，必须确定被告人对账户内资金的合法性无法做出合理解释。[37] 可见，对于经查证有关银行卡专门用于接受诈骗钱款，但被告人辩解部分钱款有正当来源的，此时可参照“非法证据排除”的适用规则，适用差异化证明标准，即由被告人负责提供线索供进一步核实，若经查证属实或不能排除其他合理怀疑的，则不能认定该笔诈骗事实，否则可认定所涉银行卡里面的钱款均系诈骗款项。可见，差异化证明标准是司法体制改革中刑事证据制度调整的需要，也是解决案多人少矛盾、实行案件繁简分流的需要，[38] 符合当前刑事诉讼的实际；不承认证明标准的差异化，就不是“实事求是”的态度。[39]

[31] 参见李艳：《宽严相济刑事政策在惩治电信网络诈骗犯罪中的科学运用》，《法律适用》2017年第9期。

[32] 同注29。

[33] 参见胡云飞、朱国斌：《电信诈骗案犯罪数额的认定应适用事实推定而非刑事推定》，《上海公安高等专科学校学报》2018年第2期。

[34] 参见姚志强：《刑事案件可实行差异化证明标准——“刑事案件差异化证明标准”研讨会观点综述》，《人民检察》2016年第10期。

[35] 参见李睿懿、王珂：《惩治电信网络诈骗犯罪的主要法律适用疑难问题》，《法律适用》2017年第9期。

[36] 同注26。

[37] 同注35。

[38] 同注34。

[39] 参见李勇：《证明标准的差异化问题研究——从认罪认罚从宽制度说起》，《法治现代化研究》2017年第3期。

二、坚持“办案与挽损并重”原则，规范涉案财物处理司法机制

党的十八届三中、四中全会决定明确提出，要进一步规范查封、扣押、冻结、处理涉案财物的司法程序。党的十九大报告指出，要依法打击和惩治黄赌毒黑拐骗等违法犯罪活动，保护人民人身权、财产权、人格权。从涉众型电信网络诈骗案件来看，囿于理念和制度等原因，我国刑事司法活动长期以来更多关注的是对诈骗分子打击成效的问题，而在冻结诈骗资金返还等涉案财物的处理上未能给予足够的重视。随着我国经济社会的不断发展，被害人对财产权益的重视度不断提高，迫切要求我国在电信网络诈骗治理时，要高度重视对被害人经济损失的追赃挽损工作，这既符合现代刑事诉讼文明的要求，也关系到让人民群众在每一个司法案件中感受到公平正义目标的实现。

实践中，鉴于涉众型电信网络诈骗存在诈骗得逞后资金转移快、被害人报警较为及时、嫌疑人归案较慢等特点，因此被骗资金需要由公安机关快速冻结并开展资金返还工作，甚至大量案件在侦查启动后，因嫌疑人未归案而无法进入刑事诉讼程序，导致相当一部分被骗钱款无法通过刑事判决处理，这是此类案件有别于其他经济犯罪案件的一大特点。因此，对于诸如电信网络诈骗的涉案财物处理来讲，如何对被骗资金进行快速止付冻结并依法返还，是此类案件财物处理需要重点关注的一大问题。为此，2016年9月，公安部、银监会联合下发《电信网络新型违法犯罪案件冻结资金返还若干规定》（以下简称《资金返还规定》），为公安机关开展冻结资金返还工作提供了执法依据，但由于第三方支付机构的迅速发展和监管不到位，使得其不断沦为诈骗分子转移资金的新工具，造成诸如涉案资金层层分转进入第三方支付机构的“资金池”流转、POS机消费转移赃款致使部分在第三方支付机构登记的冻结账户的真实性难以甄别、第三方支付机构线上支付转移账款造成部分冻结资金的交易路径不易查清，进而导致冻结资金权属难以查明的法律后果，导致资金返还受阻甚至影响到案件审判阶段对查封、扣押、冻结财物的依法处理。

（一）关于冻结诈骗资金返还的法律规制

随着我国信息化技术的发展，金融领域中第三方支付平台[40]快速发展，因使用便捷、作案隐蔽等特点，一些第三方支付平台就像一个庞大的“资金池”，已成为电信网络诈骗团伙套取、漂白非法资金的“绿色通道”，即诈骗分子先通过银行卡转到第三方支付平台，再从此平台分转至多张银行卡取现。从A市反诈骗中心的工作开展情况看，由于第三方支付机构存在监管上的漏洞，如存在查询手续烦琐、各地配合协调能力不足、无法直接通过转入银行卡号进行查询、查询反馈周期长等问题，给公安机关及时冻结被骗资金和侦破案件造成障碍。从资金权属审查认定规则来讲：首先，由于涉案资金层层分转进入“资金池”流转，转入及转出资金金额和转账时间无法形成一一对应关系，使得钱款属性难以界定。实践中，被冻结账户的开户人往往辩称账户内钱款为正常贸易、汇兑外币、购买比特比、赌博网站获利等资金，而办案机关又无法准确界定钱款属性为诈骗资金，使得资金返还工作难以开展。其次，有的诈骗分子通过POS机消费转移赃款，因第三方支付机构已将资金结算给POS机商户，商户认为被冻结在结算账户内的资金是“善意第三人所得”，由于钱款的权属性质难以甄别，资金返还工作受阻。再次，诈骗分子通过第三方支付机构线上支付转移赃款，

[40] 是指非银行的第三方机构在消费者、商家和银行之间建立连接，提供网上支付结算和资金转移服务的互联网机构。目前，拥有中国人民银行发放牌照的第三方支付平台多达200多家，此外还有大量非正规的机构从事此类业务。参见周科、方问禹、李丽静、毛伟豪：《第三方支付变脸诈骗“洗钱池”》，经济参考网 http://www.jjckb.cn/2018-01/23/c_136916366.htm，最后访问时间为2018年11月21日。

流转后再转入银行账户，由于资金流中有第三方机构加入，资金的属性不清，无法开展资金返还工作。[41] 可见，这种赃款转移方式与以往从银行卡到银行卡的转账方式相比，明显不利于办案机关查清冻结资金的权属性质。实践中，办案机关若想查清冻结在第三方支付机构及其 POS 机结算账户和“资金池”中的钱款属性，往往需要逐一查找每一个诈骗账户的开户人，且有些人头账户根本无法找到实际使用人，查找难度高，工作量巨大。此外，因《资金返还规定》未就涉及从第三方支付机构冻结资金的返还提出指导意见，使得相关操作行为无法可依，即冻结资金是指公安机关依照法律规定对特定银行账户实施冻结措施，并由银行业金融机构协助执行的资金，[42] 并不包括由第三方支付机构协助执行的资金。

可见，在当前我国对第三方支付机构的法律监管立法不足，主要规定在 2014 年 4 月由中国银监会、中国人民银行联合下发的《关于加强商业银行与第三方支付机构合作业务管理的通知》，且该通知并未对第三方支付机构的监管做出明确规定的情况下，中国人民银行、中国银行保险监督管理委员会有必要进一步出台文件加强监管。如有业内人士认为，第三方支付平台为抢占市场实现快速到账，常被诈骗分子和套现人员非法利用，建议从完善相关法律法规加大惩罚力度，加强平台自律和审核义务、将第三方支付平台纳入止付和冻结范围、整合系统资源打通地区、部门设置的查询门槛等方面加强规制。[43] 具体来讲，可结合金融市场发展实际，参照银行个人账户实名制的管控措施，及时就第三方支付平台的账户实名认证、改进后台系统建设提高查询效率、简化司法查询冻结手续等方面做出部门规章规定，同时及时修订《资金返还规定》的内容，明确第三方支付机构负有与商业银行履行同等协助资金返还的法律责任。

（二）关于被害人权利救济机制的完善

根据中办、国办《关于进一步规范刑事诉讼涉案财物处置工作的意见》文件中第 6 点的规定，即“完善涉案财物审前返还程序。对权属明确的被害人合法财产，凡返还不损害其他被害人或者利害关系人的利益、不影响诉讼正常进行的，公安机关、国家安全机关、人民检察院、人民法院都应当及时返还。权属有争议的，应当在人民法院判决时一并处理”。然而，正如前文所述，实践中很多电信网络诈骗案件中被冻结账户的资金权属难以查清且嫌疑人又未到案，在此情形下，涉案财物难以通过刑事诉讼途径交由人民法院审查判断并作出处理，甚至由公安机关开展资金返还工作都受阻。对此，被害人是否有权通过民事诉讼途径主张资金返还，是一个值得研究的法律难题。

从相关民事法律规定来看，《侵权责任法》第 4 条规定：“侵权人因同一行为应当承担行政责任或者刑事责任的，不影响依法承担侵权责任。”《最高人民法院关于银行储蓄卡密码被泄露导致存款被他人骗取引起的储蓄合同纠纷应否作为民事案件受理问题的批复》（法释〔2005〕7 号）规定：“因银行储蓄卡密码被泄露，他人伪造银行储蓄卡骗取存款人银行存款，存款人依其与银行订立的储蓄合同提起民事诉讼的，人民法院应当依法受理。”从上述法律规定来看，结合相关法理精神和逻辑，被害人因被诈骗分子实施电信网络诈骗而产生经济损失的，其同样可以侵权之诉提起民事诉讼，民事诉讼的审理并不需以刑事诉讼的裁判为依据，毕竟民事起诉对象是账户所有人或发卡银行、第三方支付平台机构，这与受骗事实不属于同一法律关系，且二者的诉讼程序、证据证明标准等方面有别，刑民之间完全可以分开处理。由此，既能有利于及时保护被害人的合法权益，又能充分发挥侵权法的救济功能。具体来讲，如果账户所有人如 POS 机商户认为第三方支付机构已结算给其的资金属于善意第三人所得，或者银行卡持卡人认为冻结资金系其合法收入，人

[41] 截至 2017 年 12 月 31 日，A 市反诈骗中心共冻结 2099 个嫌疑账户，涉及款项达 1·3 亿余元，目前已累计返还群众被骗资金 1044 万元，仅占冻结总金额 10·43%。从公安部主管的《中国防伪报道》杂志 2018 年部分期刊内容看，天津、湖南等地普遍存在止冻金额巨大，而实际返还的资金占比较少的情形。

[42] 参见《公安部出台规定电信诈骗诈骗资金分三种情况返还》，《中国防伪报道》2017 年第 4 期。

[43] 参见周科、方问禹、李丽静、毛伟豪：《杜绝第三方支付安全隐患需强化源头管理》，经济参考网 http://www·jjckb·cn/2018-01/23/c_136916367·htm，最后访问时间为 2018 年 11 月 21 日。

民法院在认真审查 POS 机商户在第三方支付机构的登记手续是否齐全、第三方支付机构是否存在监管疏漏、持卡人提交资金来源的合法收入证据材料是否真实有效等情况下，对冻结资金的权属性质依法作出认定，并可根据过错原则判定冻结账户所有人、商业银行、第三方支付机构需要承担的责任比例[44]，倒逼第三方支付机构、商业银行、经营商户严格履行相关审核义务和经营规则，既有助于进一步堵塞赃款转移的漏洞，又能最大限度给被害人提供权利救济途径。

（三）关于未查明被害人部分的财物处理

实践中，鉴于涉众型电信网络诈骗犯罪的被害人众多，且犯罪分子通过第三方支付机构等方式转移赃款，使得赃款转移路径极其复杂，部分冻结款项的被害人无法查明。与此同时，根据网络犯罪的证据采信规则和证明标准，审判实践中认定的诈骗数额又往往高于查明被害人被骗部分的数额，如果查扣或退缴在案的赃款高出查明被害人部分的数额，那么对于高出部分的款项或者需要继续追缴到案的款项应当如何处理，这是当前此类案件涉案财物处置难以解决的一个客观实际难题，是判令作为违法所得予以没收上缴国库，还是判令用于责令退赔其他未查明的被害人，法律争议较大。此外，对于扣押在案的作案工具，是一律予以没收还是对于有一定拍卖价值的可判令用于拍卖退赔被害人的经济损失，实践中判决处置方式不一。

经研究认为，对于扣押在案的诈骗所得赃款数额高出经查证的被害人被骗金额的数额，或者尚未追缴到案需要继续追缴的违法所得财物，建议在判决主文中笼统表述判决予以追缴，[45] 但不明确是用于返还被害人还是没收上缴国库，而是将该部分财物的处理留到执行阶段进行处置，即人民法院执行部门可以采取限期公示制度，公示期届满，若“潜在被害人”仍未查明或前来领取的款项，人民法院执行部门有权对查扣高出部分的数额或继续追缴到案的赃款做出没收、上缴国库的处理。[46] 此外，对于扣押在案的作案工具，应当本着退赔被害人经济损失为原则、没收上缴国库为例外的基本法理进行处置。但一定要正确理解作案工具的价值属性，确有拍卖价值的如汽车等财物，可以判令用于退赔被害人经济损失，对于手机、笔记本电脑等作案工具，随着经济社会的发展，基本上已经不再具有拍卖的价值意义，不宜再判令用于退赔被害人经济损失，否则容易造成实际无法执行的法律难题。

三、遵循“逻辑严密”的立法要求，修改法意表达不准确的条文

法条是法的表达方式，是权利义务的载体。法条如何设置，如何表达，事关立法的质量，至关重要。法条的设置与表达应能满足三项基本的要求，一是条款完备而无疏漏，二是法意表达准确而不生误解，三是法条之间协调而不相抵触。[47] 依照上述三项标准，网络犯罪的一些规范性文件的条文设置与表达还存在着一些不足之处，如法意表达不准确、定性方面的规定存在疏漏、有违法理的规定需要修改等，亟待调整。

（一）关于诈骗既未遂方面的条文规定

结合网络诈骗的实际，根据当前有关规范性法律文件规定[48]，实施电信网络诈骗犯罪，被告人实际骗得财物的，以诈骗罪（既遂）定罪处罚；诈骗数额难以查证，但发生诈骗信息或拨打诈骗电话、在互联网上发

[44] 《电信网络诈骗意见》规定：金融机构、网络服务提供者、电信业务经营者等在经营活动中，违反国家有关规定，被电信网络诈骗犯罪分子利用，使他人遭受财产损失的，依法承担相应责任。

[45] 参见黄应生：《〈关于适用刑法第六十四条有关问题的批复〉的解读》，《人民司法》2014 年第 5 期。

[46] “两高”发布《关于适用犯罪嫌疑人、被告人逃匿、死亡案件违法所得没收程序若干问题的规定》中明确，电信诈骗、网络诈骗案件适用违法所得没收程序。

[47] 参见柳经纬：《论我国民法典形成之时总则编之调整》，《政治与法律》第 2018 年第 6 期。

[48] 详见《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》第 5 条、第 6 条和“两高一部”《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》第 2 条第 4 款、第 5 款的规定。

布诈骗信息达到一定数量的，以诈骗罪（未遂）定罪处罚。诈骗既有既遂，又有未遂，分别达到不同量刑幅度的，依照处罚较重的规定处罚；达到同一量刑幅度的，以诈骗罪既遂处罚。不可否认，网络诈骗犯罪这种独具的入罪标准和量刑机制，是对传统刑法观点的一种变革和创新。对于这种新型的定罪量刑规则，实践中司法机关往往存在不同见解和做法，尤其在条文规定的理解适用上存在较大争议。一方面，经网络技术分析，行为人拨打诈骗电话或发送诈骗短信的条次可以通过电子数据等证据予以查实，但难以或无法区分既遂、未遂部分各自对应的数量，此时如何认定未遂部分的数量，是否可以将包含既遂部分在内的所有条次全部认定为犯罪未遂，并依法从轻或减轻处罚，尤其是在仅根据未遂部分的条次不能构罪而只有加上既遂部分的条次才能符合入罪标准的情况下，如何认定诈骗未遂的数量关系到案件定性，即罪与非罪的问题。另一方面，在诈骗既有既遂又有未遂的量刑适用规则上，如何确定各自的量刑幅度，关系到最终对行为人量刑评价的问题，尤其是对于未遂部分如何确定对应的量刑幅度，是否先行考虑未遂等量刑情节再确定相应的量刑幅度，实践中做法不一。尤其是以诈骗未遂定罪处罚的适用前提是“诈骗数额难以查证”，若查明既遂数额对应的法定刑在“有期徒刑 3 年以下”，而未遂部分对应的法定刑在“有期徒刑 10 年以上”，该选择何种量刑幅度并达到罪责刑相适应的目的，有时难以抉择。[49] 实践中，检察机关往往简单地以未遂部分对应的法定刑提出指控，审判机关则更多在考虑案件量刑情节的基础上，经对法定刑与宣告刑进行对比后，再择重选择量刑，比较而言，公诉机关与审判机关的分歧较大。

为此，对于上述两方面法律适用存在的争议，有必要在进一步剖析取舍的基础上，通过条文修订明确法意，确保在司法实践中能够规范适用。首先，关于发送诈骗短信或拨打诈骗电话条次的法律规范。对于既未遂情形并存的网络诈骗犯罪，若最终确定以诈骗未遂部分定罪处罚，那么在拨打诈骗电话或发送诈骗短信条次的认定上，应当将既遂部分的条次一并纳入计算并据此确定量刑档次，如此处理显然更加符合立法的本意。其次，关于“分别达到不同量刑幅度的，依照处罚较重的规定处罚”的理解适用。有必要在司法解释文件中进一步明确，在犯罪未遂对应的量刑幅度认定上，应当先评价未遂等量刑情节，然后根据调整后确定的量刑幅度为基准，与犯罪既遂对应的量刑幅度进行比较，再从中选择较重的处罚进行量刑，确保案件处理不失均衡。主要理由如下：一方面，《电信网络诈骗意见》区分诈骗既未遂情形的入罪条件，是基于电信网络诈骗犯罪手段特殊性的一种政策性举措，目的在于克服取证难、提高打击实效，但从网络诈骗造成的社会危害程度看，传统观点还是认为诈骗既遂对于被害人造成的危害程度一般是高于诈骗未遂，所以在诈骗既未遂并存时对应量刑幅度进行择重处罚时，诈骗未遂对应量刑幅度的确定应当是根据未遂等情节作出相应调整后的量刑幅度。另一方面，现行司法解释文件并未就诈骗未遂部分如何确定对应的量刑幅度作出规定，从相关解读精神看，负责起草《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》的最高法院研究室的观点认为：对此类案件，首先要分别根据行为人的既遂数额和未遂数额判定其各自对应的法定量刑幅度，未遂部分还需同时考虑可以从轻或减轻处罚；之后，根据比较结果，如果既遂部分对应的量刑幅度较重，或者既遂、未遂所对应的量刑幅度相同的，以既遂部分所对应的量刑幅度为基础酌情从重处罚；反之，如果未遂部分对应的量刑幅度较重，则以该量刑幅度为基础，酌情从重处罚。[50] 实际上，有关案例如《刑事审判参考》第 1020 号《王新明合同诈骗案》，在对诈骗既未遂情形并存时的司法认定也采用了该种量刑原则、步骤和方法。

（二）关于罪名定性方面的条文规定

目前，《电信网络诈骗意见》对全面惩处关联犯罪方面作出比较全面系统的规定，但对于其他一些新

[49] 同注 26。

[50] 参见胡云腾、周加海、刘涛：《〈关于办理诈骗刑事案件具体应用法律若干问题的解释〉的理解与适用》，《人民司法》2011 年第 9 期。

类型网络犯罪案件的定性处理，缺乏相应法律条文的明确规定，造成实践中出现是定一罪还是数罪、此罪还是彼罪的法律适用争议，亟待通过立法加以规范调整。例如，被告人利用“钓鱼网站”链接、“木马”程序链接、网络渗透等隐蔽技术手段获取被害人信息并实施财物窃取或占有的行为，在罪名选择适用上，是要定诈骗罪、盗窃罪还是妨害信用卡管理犯罪，同时是否要以构成侵犯公民个人信息罪进行数罪并罚，实践中争议较大。首先，如果被告人通过网络侵入方式获取被害人的网络账户资金账户和密码等信息后，采用更改密码或更改被害人账户的捆绑手机号码、邮箱等方式，伺机盗取被害人账号内的资金，这种行为符合秘密窃取他人财物的构成要件，应当以盗窃罪定罪量刑，被告人非法入侵他人信息的行为，属于实施盗窃的犯罪手段，不宜再以侵犯公民个人信息罪进行数罪并罚。其次，如果被告人入侵他人的管理员邮箱，获悉第三人欲购买入侵对象的商业交易信息，后被告人冒用入侵对象管理员与第三人联系并取得信任和诈骗得逞，对于被告人骗取第三人财物的行为，应当以第三人信以为真是在和被入侵对象进行商业交易、自愿支付相应交易款项的角度，认定被告人的行为构成诈骗罪，同时被告人使用非法获取的公民个人信息实施网络诈骗犯罪行为，如果构成侵犯公民个人信息罪的，应当依法予以并罚。最后，如果被告人发布虚假信息植入木马等手段获取被害人的银行卡及密码等信息，再与下家共谋，利用非法方式获取的被害人的信用卡信息资料，通过下家注册的淘宝店铺进行虚假交易，冒用被害人名下的信用卡非法套现，骗取被害人的财物，这种情形的作案方式因存在“刷卡套现”的行为，从犯罪构成要件上来看，更加符合妨害信用卡管理罪法定构成要件的特别规定，即冒用他人信用卡进行非法套现和占有，应当以妨害信用卡管理犯罪的定罪处罚，而不宜以盗窃罪对其定罪处罚，同时被告人使用非法获取的公民个人信息实施网络犯罪行为，如果构成侵犯公民个人信息罪的，应当依法予以并罚。

又如，电信网络诈骗犯罪往往伴生妨害信用卡管理犯罪，尤其体现在“取款组”团伙的行为定性上，这个层级的行为人在参与诈骗或者为他人取款提供帮助时，往往非法收购、持有大量信用卡。从审判实践遇到的案件实际来看，部分信用卡经查证属实是用于接受诈骗钱款，但仍有相当部分信用卡缺乏证据证明行为人系用于实施诈骗犯罪，或者无法查证具体用途，在可能同时构成诈骗罪和妨害信用卡管理罪的情况下，是构成两罪还是择一重罪论处，亟待通过立法或出台司法解释方式予以明确。具体来讲，应当区分不同情形予以规范：一是对于行为人明知他人实施诈骗犯罪行为而提供信用卡帮助的，一般应以诈骗共犯定罪处罚；无法认定明知的，以妨害信用卡管理犯罪定罪处罚。二是对于行为人为实施诈骗或为他人实施诈骗提供取款、信用卡帮助而非法购入、持有信用卡，同时构成诈骗罪和妨害信用卡管理罪的，建议区分以下情形追究刑事责任：（1）所犯诈骗罪的法定量刑档次高于或等于所犯妨害信用卡管理罪的法定量刑档次的，以诈骗罪定罪处罚，但应将非法购入、持有信用卡的事实作为酌情从重处罚情节。（2）所犯诈骗罪的法定量刑档次低于所犯妨害信用卡管理罪的法定量刑档次的，为有力打击犯罪，应以二罪数罪并罚。三是对于行为人实施诈骗或为他人实施诈骗提供取款帮助，还非法购入、持有信用卡，但缺乏证据证明其非法购入、持有信用卡系为了实施诈骗犯罪的，在同时构成诈骗罪和妨害信用卡管理罪的情况下，一般以二罪数罪并罚。[51]

（三）关于收集被害人陈述方面的条文规定

电信网络诈骗的一个突出特点就是被害人众多且分布广，受此等客观条件限制，逐一收集被害人陈述的难度大。在此情况下，根据《意见》第6条第1项的规定，可以结合已收集的被害人陈述，以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据，综合认定被害人人数及诈骗资金数额等犯罪事实。从立法本意来讲，如前所述，如果存在第三方支付机构监管不到位等客观原因无法核实被害人的，司法机关可以结合在案其他证据对诈骗金额作出认定，这种特殊的证明规则在一定

[51] 同注26。

程度上有助于打击犯罪。然而，从司法实践来看，该条文规定出台后，一些办案机关误读了其立法本意，在侦查中全面弱化向被害人取证，即有的被害人陈述虽可以取证但侦查机关却未依法取证，或者收集的被害人陈述越来越少，甚至有的案件出现“零被害人陈述”的情形。换言之，该条文规定存在过于注重打击犯罪成效，而忽视被害人财产权益保护的立法逻辑，实质上并不符合现代刑事诉讼文明的要求，也不符合基本法理精神的要求。在此情况下，容易造成两种法律后果：一是被告人及其辩护人经常提出，对于“没有被害人的陈述”或“只有被害人的报案信但没有制作询问笔录”部分的诈骗数额不能认定的辩护意见。二是因可查明但未查明的相关被害人，审判机关在对涉案财物作出处理时，包括对扣押赃款判令退赔或尚未到位的赃款继续追缴退赔时，因为被害人没有查明而退赔无门，最终导致相关被害人的财产权益得不到保障。为此，建议在立法上进一步明确，对于有条件取得的被害人陈述，侦查机关应当尽量取证，特别是对一些具有典型性、代表性的被害人陈述一般应当取证，否则对该部分诈骗数额的认定不能参照《电信网络诈骗意见》相关规定的特殊证明规则予以推定。由此，进一步倒逼侦查机关依法查明被害人信息，既有助于诈骗数额能够准确认定，又能保障应当查明但未查明的被害人的退赔权益得到法律保护。同时，检察机关和审判机关要加强对被害人信息的审查，对于有线索表明可以查明的被害人信息或者发现被害人的新线索，应要求侦查机关补充侦查，进一步补充完善案件被害人信息，确保相关被害人陈述取证充分和全面。从信息化技术角度，建议建立健全网络诈骗报案信息平台的建设，对于电信网络诈骗这种被害人众多且各地分散报案的案件，建议公安部统一建立类似“DNA”“打拐”数据库模式的电信网络诈骗信息平台，要求各地公安机关在录入被害人报案信息时，要在信息平台中强化“转出银行账户”“转入银行账户”等户名、卡号信息的录入和检索功能，实现相关信息的办案资源共享，通过信息化手段最大限度查明被害人信息，既有助于取证被害人陈述补强案件证据印证力，又有助于实现对相关被害人经济损失的及时退赔。

结　语

网络犯罪治理是一项系统而复杂的重大工程，实践中，司法机关根据打击犯罪和保护被害人财产权益的客观现状，结合网络犯罪的发展实际，及时出台相关解释规定、指导性文件，虽有助于在一段时期内解决一些打击犯罪难题，但也容易造成证据采信证明标准不一、条文规定跟不上网络时代发展、法条意思不够明确引发适用争议等难题。当前，在一系列规范性法律文件已经出台并实施一段时期的情况下，有必要重新对网络犯罪的条文规定进行梳理分析和专项调研，在掌握情况、发现问题、剖析原因、总结经验的基础上，及时对一些好的经验做法和需要修订的条文规定进行整合调整，通过立法或出台司法解释的方式固定下来，为进一步规范此类案件处理提供法律依据，确保网络犯罪治理取得政治效果、法律效果和社会效果的高度统一。

The Practical Problems and Legislative Improvements of Cybercrime Governance

Li Shujing, Wu Chengjie

Abstract: China’s cybercrime governance has not formed a special legal norm on legislative technology, and it has failed to meet the legal problems brought by the network era. It is necessary to face up to the paradigm

changes brought by “the space-time separation” of cybercrime behavior, the fact that electronic data has become the basis for important judgments, as well as the difficulty in collecting victims’ statements. As for the judicature, under the premise of returning to the “exclusion of reasonable doubt” standards in criminal cases, it is realistic, urgent and necessary to apply actively the “differentiated proof standard” to promote the formation of scientific and reasonable evidence-acquisition rules. For the handling of the properties related to mass involved cyber fraud cases, it is necessary to further strengthen the legislative norms to block the regulatory loopholes of third-party payment institutions, and to ensure that legal means can be used to find out the victims’ information and the flow of fraud funds in order to accelerate the freezing as well as the returning of the funds, so that the victims’ loss can be recovered in time, and the up-to-date judicial concept of paying equal attention to the handling cases and the recovering of damage will be realized. In accordance with the reality of the trials of cases, it is necessary to revise the uncoordinated legal provisions that violate the logic of law, lack essential contents, or express inaccurately the meaning of law, in order to guarantee the reasonableness of legal norms and the coherence of legal contents and to avoid the divergence in applying them, ensuring the accurate determination of cases, the standardization of penalty and the completion of the restitution of victims’ loss.

Keywords: cybercrime; evidence collection; property handling; legislative improvement

（责任编辑：吕英杰）