Open Journal of Legal Science 法学, 2023, 11(5), 4151-4157
Published Online September 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.115589

Hans汉斯

电信网络诈骗案件的证据侦查困境与应对策略

陈荣礼

贵州大学法学院，贵州 贵阳

收稿日期：2023年6月29日；录用日期：2023年7月17日；发布日期：2023年9月13日

摘　要

电信网络诈骗案件的取证难度往往比传统犯罪更大，因此需要采取有别于传统诈骗犯罪的应对策略。从电信网络诈骗案件的证据困境出发，探讨其主要原因，包括诈骗技术手段的高度隐蔽、证据来源的不确定性、案件证据的跨境性等。同时，从现有取证技术和案件侦查实践中总结出一些有效的证据应对策略：一是数据挖掘技术的应用，提高证据的准确性和可靠性；二是建立协作协同联动机制，提高侦查效率和质量；三是提升调查人员的专业素养，提高调查人员的取证技能和判断能力，不断积累侦查实践经验；四是完善电信网络诈骗电子证据的取证制度，确保电子证据的真实性和完整性。

关键词

电信网络诈骗，证据侦查，困境，应对策略

Difficulties in Evidence Investigation of Telecommunication Network Fraud Cases and Countermeasures

Rongli Chen

Law School of Guizhou University, Guiyang Guizhou

Received: Jun. 29th, 2023; accepted: Jul. 17th, 2023; published: Sep. 13th, 2023

Abstract

The difficulty of obtaining evidence in telecom Internet fraud cases is often greater than that in traditional crimes, so it is necessary to take countermeasures different from traditional fraud crimes. Starting from the evidence dilemma of telecom Internet fraud cases, this paper discusses the main reasons, including the high concealment of fraud technical means, the uncertainty of evidence sources, and the cross-border nature of case evidence. At the same time, some effective

文章引用: 陈荣礼. 电信网络诈骗案件的证据侦查困境与应对策略[J]. 法学, 2023, 11(5): 4151-4157.
DOI: 10.12677/ojls.2023.115589

evidence response strategies have been summarized from existing evidence collection techniques and case investigation practices: firstly, the application of data mining technology to improve the accuracy and reliability of evidence; Secondly, establishing a collaborative and collaborative mechanism to improve the efficiency and quality of investigation; The third is to enhance the professional literacy of investigators, enhance their forensic skills and judgment abilities, and continuously accumulate practical experience in investigation; Fourthly, improving the evidence collection system of electronic evidence of telecommunications Internet fraud to ensure the authenticity and integrity of electronic evidence.

Keywords

Telecommunication Internet Fraud, Evidence Investigation, Difficulties, Coping Strategies

1. 引言

网络安全既是稳定社会和保障公民正常生活的基本要求，也是国家安全的重要组成部分，切实加强网络安全法律保护，对防范和打击电信网络诈骗违法犯罪，促进社会的和谐发展具有重要意义。近年来，中国成为网络诈骗高发、受害者众多的国家之一，防范电信网络诈骗、打击电信网络诈骗以及相关行为是新时代国家必然关注的重大社会问题。为预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，经过长时间的讨论与审议，《中华人民共和国反电信网络诈骗法》(以下简称《反电信网络诈骗法》)于 2022 年 9 月经全国人大常委会表决通过。《反电信网络诈骗法》是依法应对电信网络诈骗违法犯罪的直观反映，是我国第一部专门、系统、完备规范反电信网络诈骗工作的法律，是党中央部署打击治理电信网络诈骗工作的标志性成果，是中国特色反电信网络诈骗犯罪制度的成功探索和具体实践[1]。

2. 电信网络诈骗的现状

随着信息社会快速发展，犯罪结构发生重大变化，传统犯罪持续下降，以电信网络诈骗为代表的新型网络犯罪已成为当前的主要犯罪形态。根据最新的统计数据，2022 年，全国共破获电信网络诈骗案件 39.1 万起，同比上升 5.7%，抓获犯罪嫌疑人数同比上升 64.4%，公安部会同最高法、最高检等相关部门开展联合工作，成功将 240 名电信网络诈骗犯罪集团重大头目和骨干缉捕归案，捣毁诈骗窝点 1800 余个，打击涉诈固话语音专线、简易组网 GOIP、跑分洗钱等各类集群战役 80 余起，累计推送预警指令 2 亿条，预警提示短信、闪信 4.7 亿条，处置涉诈高风险电话卡 1.1 亿张，拦截诈骗电话 18.2 亿次、短信 21.5 亿条[1]。当前，电信网络诈骗犯罪已经成为案发最多，上升最快、涉及面最广、人民群众反映最强烈的犯罪类型，其中刷单返利、虚假投资理财、虚假网络贷款、冒充客服、冒充公检法 5 种诈骗类型发案占比近 80%，成为最为突出的 5 大高发类案，其中刷单返利诈骗案发率最高，占案发总数的三分之一左右；虚假投资理财类诈骗涉案金额最大，占全部涉案金额的三分之一左右。以上说明，电信网络诈骗已然成为诈骗的主要来源。

[1]参见中华人民共和国公安部网站，https://app.mps.gov.cn/gdnps/pc/content.jsp?id=8812495，2023 年 3 月 2 日访问。

3. 打击电信网络诈骗犯罪的时代必要性

3.1. 打击电信网络诈骗犯罪，是贯彻落实党中央决策部署的重要举措

为应对电信网络诈骗违法犯罪行为带来的各种社会风险，习近平总书记高度重视打击电信网络诈骗违法犯罪活动的工作，曾多次对反电信网络诈骗工作的指导思想、基本原则作出重要指导和批示。2021年4月6日，习近平总书记对打击治理电信网络诈骗犯罪工作作出重要指示，强调要坚持以人民为中心，统筹发展和安全，强化系统观念、法治思维，注重源头治理、综合治理，坚持齐抓共管、群防群治，全面落实打防管控各项措施和金融、通信、互联网等行业监管主体责任，加强法律制度建设，加强社会宣传教育防范，推进国际执法合作，坚决遏制此类犯罪多发高发态势，为建设更高水平的平安中国、法治中国作出新的更大的贡献[2]。2021年12月，习近平总书记再次作出重要批示，“对人民群众反映强烈的电信网络诈骗、新型毒品犯罪和‘邪教式’追星、‘饭圈’乱象、‘阴阳合同’等娱乐圈突出问题，要从完善法律入手进行规制，补齐监管漏洞和短板，决不能放任不管。”[3] 2021年12月，为贯彻落实习近平总书记重要指示批示精神，中共中央办公厅、国务院办公厅印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》。打击电信网络诈骗违法犯罪活动，是贯彻落实习近平总书记重要指示精神和党中央决策部署的重要举措。

3.2. 打击电信网络诈骗犯罪，是践行总体国家安全观的重要组成

国家安全涉及国土安全、军事安全、科技安全、生态安全、生物安全等诸多维度，是安居乐业的基础，也是治国安邦的头等大事。总体国家安全观是对中国特色国家安全本质特征的概括与凝练，是新时代应对国内国际纷繁复杂安全形势的理论纲领，以总体国家安全观为总纲领的国家安全制度建设，必然是治理现代化视阈下实现国家长治久安的必要之举[4]。电信网络诈骗有别于传统诈骗罪，电信网络诈骗主要是利用电信通讯、互联网等技术手段，向社会公众发布虚假信息或者设置骗局，通过网络的远程控制，非接触性地诱使被害人交付财物的行为[5]。电信网络诈骗犯罪严重影响正常的网络安全，违反网络运行安全的一般规定和网络信息安全法律责任制度。打击电信网络诈骗犯罪，在基本价值上，是引领总体国家安全观的网络安全法律体系，贯穿网络运行安全、个人信息安全和网络信息内容安全的国家安全目标[6]。

3.3. 打击电信网络诈骗犯罪，是坚持以人民为中心的必然要求

党的二十大报告把“坚持人民至上”作为贯彻习近平新时代中国特色社会主义思想的根本立场，并进一步指出，“我们要站稳人民立场、把握人民愿望、尊重人民创造、集中人民智慧，形成为人民所喜爱、所认同、所拥有的理论，使之成为指导人民认识世界和改造世界的强大思想武器。”[7]打击电信网络诈骗违法犯罪活动，是与坚持以人民为中心的根本立场高度一致的。近年来，电信网络诈骗犯罪活动形势严峻，在刑事犯罪案件中占据很大的比重。坚决遏制电信网络诈骗违法犯罪活动高发态势，提升社会治理水平，使人们获得感、幸福感、安全感更加充实，更有保障、更加可持续。加强打击治理电信网络违法犯罪行为，是党和国家对电信网络诈骗犯罪的高度重视，是坚定不移维护广大人民群众利益的决心，是建设更加高水平平安中国的鲜明态度。“天下无诈”是人民群众期待的美好愿望，也是党和国家笃行不怠的奋斗目标。

4. 电信网络诈骗犯罪的取证困境

4.1. 电信网络诈骗技术手段的高度隐蔽

利用技术手段进行诈骗是电信网络诈骗案件中常用的一种手段，而且一般被利用于攻击受害人的网络设备或者诱使受害人泄露个人信息和账户信息。违法犯罪分子常用的技术诈骗手段包括虚假网址、网

站和移动应用程序、电子邮件、社交媒体和通讯应用程序、恶意软件和病毒窃取个人信息和账户信息的技术等。虚假网址、网站和移动应用程序主要是骗取受害人的个人信息和账户信息。虚假网站网址往往具有非常逼真的外观和功能，很难让受害人分辨出真假。而移动应用程序则常常伪装成一些有吸引力的游戏或者应用，诱使受害人下载并安装后进行钓鱼活动。虚假网址、网站和移动应用程序常常能够对多个受害人进行同时攻击，从而提高攻击的效率。电子邮件、社交媒体和通讯应用程序通常是诱使受害人泄露个人信息和账户信息达到诈骗的目的。攻击者往往伪装成受害者信任的个人或者机构，如银行、电信运营商等，然后发送电子邮件或者在社交媒体上进行诈骗活动，引诱受害人点击链接或者下载文件。电子邮件、社交媒体和通讯应用程序诈骗的特点是快速传播和低成本，而且攻击者能够通过改变发件人或者伪装成其他个人或者机构来降低被发现的概率。恶意软件和病毒是通过攻击受害人的计算机或者移动设备，并窃取受害人的个人信息和账户信息。恶意软件和病毒通常会通过下载附件、点击链接或者访问感染网站来进行传播，攻击者可以通过恶意软件和病毒来窃取受害人的信息和密码，甚至远程控制受害人的设备。这类技术诈骗手段具有隐蔽性和毁灭性，攻击者能够通过多种手段来隐藏恶意软件和病毒的存在，防止被发现。窃取个人信息和账户信息主要是通过黑客攻击、社交工程等手段，此类诈骗技术手段也可以通过掩盖自己的身份和行踪来规避监视和追踪。这些技术手段具有一定的共性，一是难以追踪和追溯其技术路径，二是具有高度自动化和快速传播的特点，三是难以区分真伪和违法行为的模糊性，使得诈骗技术手段高度隐蔽。

4.2. 电信网络诈骗的证据来源具有不确定性

电信网络诈骗犯罪通常是通过网络技术进行的，包括网络攻击、欺诈、虚假信息传播等多种复杂手段。犯罪嫌疑人通过使用伪造的 IP 地址、匿名代理等技术来隐藏自己的真实身份，使得侦查机关追踪和取证的难度加大。IP 地址是网络通信的基本元素，技术侦查人员可以通过 IP 地址追踪到网络数据的来源，追踪找到犯罪嫌疑人。但犯罪嫌疑人通常的做法是使用伪造的 IP 地址来隐藏自己的真实身份，即使侦查机关使用数据取证、网络追踪、语音识别等高科技手段进行技术分析来进行取证工作，犯罪分子也可以轻易地逃过追捕。此外，违法犯罪分子还经常使用虚拟的专用网(vpn)等匿名工具来隐藏真实的 IP 地址，使用加密通信、混淆代码等技术来隐藏行踪，这都增加侦查机关的取证工作的难度，使侦查机关难以获取违法分子的违法犯罪证据。

4.3. 电信网络诈骗案件证据的跨境性

电信网络诈骗犯罪具有跨国、跨区域的特点，违法犯罪分子往往通过跨境转移等手段来掩盖其违法犯罪行为，给侦查机关的调查取证工作带来极大的困难。首先，不同国家和地区的调查取证的法律规定不同，意味着侦查机关在跨境调查取证时，必须遵守当地的法律规定和程序。如在一些国家，警方必须获得搜查令才能搜查嫌疑人的住所，而在其他国家则需要更为严格的程序和规定。不同的法律规定和程序，使得侦查机关跨境侦查获取证据之前，需要进行协调、协商，以确保取证工作的合法性与有效性，但这需要花费大量的时间，会导致证据的流失。其次，该类案件会涉及众多的犯罪嫌疑人、受害人和证人，这些人可能会分布在不同的国家和地区。侦查机关需要跨越时空的限制，对散布各地区的犯罪嫌疑人、受害人和证人进行调查取证，才能获得足够的证据来证明违法犯罪行为。如果侦查机关不具备较强的专业能力和技术以及没有及时与境外地区的机关进行协调合作，也会导致侦查机关难以获取充分的证据。

4.4. 电信网络诈骗的电子证据保全难、易篡改、易毁灭

根据刑事诉讼法的规定，电子证据是一类独立的证据种类。而且，电子数据可以被视为其他七类证据的电子数据化。“由于网络空间的虚拟化，网络犯罪行为留下的证据通常为电子数据。在互联网时代，

以计算机和网络为依托的电子数据在证明案件事实的过程中发挥着越来越重要的作用，缺乏电子数据的支撑将难以认定相关犯罪事实。”[8]但电子证据也有缺陷：一是，电信网络诈骗犯罪的电子证据保全难，电信网络犯罪案件中的电子证据与传统证据不同，它是以计算机、网络等为载体，对介质和运行环境具有很强的依赖性，因此对电信网络诈骗案件中的电子证据不能采取拍照、绘图等传统的保全方式。通常，公安机关使用光盘或其他电子设备等介质对电信网络诈骗案件中的电子证据进行提取、保全。但如果提取、保全的光盘或电子设备出现意外，会破坏电子证据，甚至灭失(如光盘和电子设备丢失或毁损，或者保全环境的强磁场、强电等对光盘和电子设备造成破坏)。此外，刑事侦查工作保密性强，电信网络诈骗案件中电子证据保全工作不能由公安机关以外的技术公司负责，更加大公安机关对电信网络诈骗案件中电子证据保全的难度[9]。二是，电子数据易被篡改，具有较强的隐蔽性、灵活性。部分犯罪分子反侦查意识极强，由专业团队在第一时间对电子数据进行加密、修改和隐藏。有经验的诈骗犯在诈骗成功后会诱导被害人将关键信息删除，或是立即自行销毁诈骗记录和诈骗网站的数据。电信网络诈骗案件的取证问题是对公安机关侦查能力的一大考验，电子证据容易损毁、消逝，很多犯罪分子在被逮捕前会迅速销毁相关数据并丢弃作案设备，能否在第一时间保住数据并提取出有效线索，是侦查电信网络诈骗案件的关键所在。

5. 电信网络诈骗证据困境的实务应对

5.1. 数据挖掘技术的应用

数据挖掘技术是一种从大量数据中提取有用信息的技术，它通过各种数据挖掘算法来分析和挖掘数据，从而发现数据中的规律和模式。电信网络诈骗是一种非常普遍的犯罪行为，它给国家、社会和个人带来巨大的财产损失，甚至影响到国家和社会的稳定和安全。为有效打击这种犯罪行为，有关部门需要使用各种技术手段来获取犯罪证据，以加强打击犯罪的能力和效果。在这个过程中，数据挖掘技术可以发挥重要作用。在电信网络诈骗犯罪中，数据挖掘技术可以通过通话记录分析、文本分析、地理位置分析等帮助相关部门获取犯罪证据，从而更好地打击电信网络犯罪。首先，通过分析通话记录，可以了解犯罪嫌疑人和被害人之间的通话情况，从而确定是否存在欺诈行为。如犯罪嫌疑人可能会使用虚假身份进行诈骗，而通话记录可以帮助相关部门找到虚假身份背后的真实身份信息。同时，通话记录也可以帮助相关部门分析通话时长、通话时段等信息，从而判断通话是否存在异常情况，以及诈骗的具体手法。其次，文本分析是数据挖掘技术在电信网络诈骗中的另一种应用方式。通过分析短信、邮件等文本信息，可以获取犯罪嫌疑人的欺诈手段、诈骗方式等信息，从而帮助相关部门确认犯罪嫌疑人的罪行。当犯罪嫌疑人发送欺诈短信骗取受害人的财物时，相关部门可以通过文本分析找到这些短信的特征和规律。此外文本分析还可以帮助相关部门对网络诈骗进行情报收集和研究，进一步提高对电信网络诈骗犯罪证据的收集能力。第三，地理位置分析是通过分析手机的位置信息和移动轨迹，帮助相关部门确定犯罪嫌疑人的所在位置和活动范围，以及与其他犯罪嫌疑人之间的关系，从而找到更多的犯罪证据。犯罪嫌疑人可能会使用多个手机号码来进行诈骗活动，但通过地理位置分析，相关部门可以发现这些手机号码背后的真实身份和联系方式，以及他们在诈骗活动中的相关协助证据。

5.2. 建立协作协同联动机制

为避免单一治理，强化协同联动机制建设，要求各个部门、单位之间密切配合，力图克服公安部门单打独斗露出的治理不足，转换现有事后回应模式的治理方略，跨越盲目信仰刑事治理的思维窠臼。在推进从事后回应到前端防范、从偶发性治理到常态治理、从犯罪治理到综合治理的美好期待下，依法以组合拳的方式规避电信网络诈骗中权责杂糅局面。

与应对其他犯罪一样，公安机关在应对网络诈骗方面同样带有“反应式”的特点，即只有发生网络诈骗案件且有举报信息后，才会介入案件的侦查活动。虽然目前一些地方公安机关已经建立一定的监控机制，但总体上，这种“反应式”或被动式的局面不会有根本的改变。相较而言，行政机关尤其是能跟踪、获取大量信息的部门具有发现诈骗线索的能力，并及时获取相关证据。因此，应当在行政机关与公安司法机关之间建立信息渠道，发现网络诈骗证据线索后，行政机关应当及时移送，分享相关信息源[10]。此外，为打击网络诈骗犯罪，公安机关需要与私营企业和金融机构加强合作。一方面，互联网企业具备发现和掌握网络诈骗信息的技术能力。另一方面，一些互联网企业提供的平台也是网络诈骗犯罪实施的场所。这些企业有义务提供相关犯罪线索，配合公安机关获取犯罪证据，协助查缉犯罪分子，追缴其犯罪所得和非法收益。这样，通过公安机关和企业的密切合作，能加强网络诈骗犯罪的打击力度，维护社会治安和公共利益。

电信网络诈骗治理的另一个难点，在于犯罪活动实施的跨地域和跨法域，因而在获取电信网络诈骗证据，打击网络诈骗活动中，必然要与境外相关主体进行合作。首先是侦查技术协同，在打击跨境电信网络诈骗的案件侦查中，与境外各机关建立信令追踪核查技术、异常银行往来账户的自动锁定、网络 IP 地址的追踪、口令登录上网等技术体系，通过电信信息流倒查，银行资金流向侦查以及网络痕迹侦查，同时辅以人工现场取证等获取电信网络诈骗的证据[11]。其次，在打击跨境电信网络诈骗违法犯罪中，需要凝聚证据协同共识。通过双边间的警务研讨、培训等方式，加强与其他地区警务机构间的证据协同共识，提高打击跨境电信网络诈骗犯罪的效率和准确性。针对我国在获取电信网络诈骗犯罪的证据时，可以制定我国法律框架下的证据标准，并与其他各地区进行分享和交流，请求对方按照我国的证据标准进行侦查和合作，确保获取的证据符合我国司法诉讼制度的要求。

5.3. 提升侦查人员的专业能力

电信网络诈骗案件是当前社会面临的重大安全威胁之一，其犯罪手段日益复杂和隐蔽。为精准打击这类犯罪，公安机关需要建立一支具备计算机、网络通信方面的专业知识的人才队伍，注重对电子数据取证专业人才的培养。然而，在当前的基层公安机关中，办理电信网络诈骗案件的警察多为普通民警，缺乏相关领域的专业知识，这导致办案效率低，电子数据难以保全。为提高办案效率，公安机关应当注重人才队伍的建设。

首先，公安机关应当加强对电子数据取证专业人才的培养。在公安队伍中选拔合适人选，对其定期开展培训、传授实战经验，以弥补现阶段侦查人员网络取证、网络溯源能力的欠缺。经过培训的侦查人员能具备数据侦查意识和挖掘数据的能力，能够合理适用程序，对电信网络诈骗案件展开侦查。其次，对于特大诈骗团伙犯罪中，犯罪手段极其隐秘且充满技术含量，即使是具备一定专业知识的侦查人员，在遇到此类特大疑难案件时也难免犯难。因此，公安机关应建立电子数据取证专家人才库，聘请技术专家协助开展取证工作。这样可以为侦查人员提供技术支持，帮助他们更好地提取电子数据，并针对涉案网站中的电子数据进行深入的分析和研究。最后，必须建立精英团队，组织多学科交叉、多领域融合的技术研究和技术攻关，提高电子数据取证的技术水平。该团队可以由公安机关内部的专家和外部的技术公司、高校等单位组成，共同致力于电子数据取证领域的技术创新和研发，为打击电信网络诈骗犯罪提供技术支撑。要而言之，须灵活制定公安科技人才政策，综合运用公务员编制、事业编制、长聘合同等多种形式，应对公安科技人才力量不足、高科技人才留不住、用不好的困境，同时要依靠地方高校、政法类专业院校或科研机构，采取订单模式培养自身人才[12]。

5.4. 完善电信网络诈骗电子证据的取证制度

为确保侦查机关获取的电子证据的真实性和完整性，侦查机关必须贯彻《2012 年刑诉法解释》《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》《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》等相关法律法规关于电子数据“以扣押原始存储介质为原则，以提取电子数据为例外，以打印、拍照、录像等方式固定为补充”的原则要求。

完善电信网络诈骗电子证据的取证制度，主要是针对电子数据的收集与提取、移送与展示、审查与判断环节，确保电子数据的真实性与完整性。首先，在收集与提取电子数据方面，收集、提取的主体应该是具有相关专业知识的侦查人员，必要时可以聘请相关网络技术人员提供协助。同时采用以下一种或者几种方法保护电子数据的完整性：1) 扣押、封存电子数据原始存储介质；2) 计算电子数据完整性校验值；3) 制作、封存电子数据备份；4) 冻结电子数据；5) 对收集、提取电子数据的相关活动进行录像[2]。其次，在移送与展示环节，为防止电子数据被改动，导致电子数据丢失，原则上应对收集提取的电子数据以封存状态移送，同时制作移送电子数据的备份件。最后，在审查与判断环节，侦查人员要从真实性、完整性、合法性、关联性四方面对电子数据进行审慎判断。

参考文献

[1] 谢俊思. 依法而治, 推动反电信网络诈骗工作深入健康发展[N]. 人民公安报, 2022-12-02(002).

[2] 坚持以人民为中心全面落实打防管控措施坚决遏制电信网络诈骗犯罪多发高发态势[N]. 人民日报, 2021-04-10(001).

[3] 习近平. 坚持走中国特色社会主义法治道路更好推进中国特色社会主义法治体系建设[J]. 中国人大, 2022(4): 6-9.

[4] 蒋华福. 新时代国家安全治理体系的理论逻辑、实践逻辑与思维方法[J]. 国家安全研究, 2022(3): 119-133+158.

[5] 张恒, 杨立敏. 电信网络诈骗犯罪治理的困境与对策探究[J]. 山西警察学院学报, 2023, 31(1): 94-99.

[6] 张慧. 建构融贯的网络安全法律体系[N]. 中国社会科学报, 2023-02-22(004).

[7] 习近平. 高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的报告[J]. 中国人大, 2022(21): 6-21.

[8] 喻海松. 刑事诉讼法修改与司法适用疑难解析[M]. 北京: 北京大学出版社, 2021: 174-175.

[9] 李强. 电信网络诈骗案件中电子取证问题研究[J]. 警学研究, 2022(6): 52-57.

[10] 时延安. 个人信息保护与网络诈骗治理[J]. 国家检察官学院学报, 2017, 25(6): 3-24+169.

[11] 彭金. 中国-东盟治理跨境电信网络诈骗警务合作研究[J]. 云南警官学院学报, 2022(6): 80-83.

[12] 申蕾. 电信网络诈骗案件证据困境与实务应对[J]. 政法学刊, 2022, 39(6): 23-29.

[2]《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》，(法发〔2016〕22 号)，第 5 条。