

大数据时代电信网络诈骗的防范与治理

◆白莉莉 刘军怀

(新疆政法学院,新疆 图木舒克 844000)

【摘要】随着大数据的蓬勃发展,我国电信网络诈骗案件持续增多,受害群体愈加庞大,甚至出现了很多新型的诈骗方式,目前存在公民个人防范意识薄弱、行业治理缺乏以及社会诚信体系缺失等现状。本文以笔者辖区内发生的案件为例,就如何防范和应对电信网络诈骗提出治理措施,以期能为电信网络诈骗防范和治理提供有益参考。

【关键词】大数据;电信网络诈骗;治理

一、问题的提出

电信网络诈骗是随着互联网新型技术发展而衍生出的犯罪方式,诈骗分子借助网络平台,利用新型技术手段,通过远程操作,诱使受害者给诈骗分子打款或者转账的行为。主要通过利用虚拟电话、网站、App等媒介,收集公民个人信息,根据年龄、收益状况等进行分类,发送具有迷惑性信息或者拨打电话直接实施诈骗,通过虚构故事情节,利用受害者贪利或恐惧的心理,以非接触式的方式,转移受害者财产的犯罪行为。

在日常生活中,人们身边充斥着诈骗短信、诈骗电话,出现了很多区别于传统诈骗方式的诈骗案件,诈骗类型和手段也是多种多样,严重危害了民众的财产和信息安全,也损害了民众的获得感、幸福感、安全感。与传统诈骗方式不同的是,电信网络诈骗犯罪成本低、犯罪手段多样、涉猎范围广,诈骗分子可以依靠一台电脑、一个支付账号,借助大数据和智能技术拨打电话、发送信息即可实施犯罪,诈骗技术手段极其高明,如冒充微信工作人员谎称“您的微信百万保障”功能过期,需要向指定账户转移存款;利用AI技术生成虚拟的亲属语音信息,声称家中告急亟需紧急转账等。总之,电信网络诈骗越来越数字化、智能化,如何防范和应对电信网络诈骗是一大难题。

二、电信网络诈骗的类型

网络是一个虚拟空间,每天日新月异,面对各式各样的网络信息,稍有不慎就会落入诈骗分子的陷阱,无形之中丢失自己的财产。根据公安部2022年的统计数据,电信网络诈骗目前是发案最多的犯罪类型。以笔者身边辖区内居民遇到的诈骗案件为例,具体有以下几种类型。

(一)红包返利类

7月30日23时许,严某在家中玩手机时加入一微信群,群中一昵称为“木桶效应”的人告知其下载“百利商贸”App可获得红包返利。7月31日9时许,严某下载注册并登录“中原百货”App,根据App客服的指引,严某随

即向指定账户转账2次共计3.657万元,因未收到返利,意识被骗,遂报警。

(二)冒充客服类

8月3日19时30分许,洪某接到一陌生电话,对方称其微信已开通“百万保障”服务,如不解约将扣除9600元。洪某在对方指引下下载“云视远程协助”App,并与对方开启“屏幕共享”。随即洪某发现手机被对方控制并关掉该App,后在手机银行查询,发现卡内12万元已被转出。

(三)“AI换脸”新型诈骗

1.虚假音频诈骗

利用AI技术生成虚假的语音信息,冒充亲戚、朋友等身份进行诈骗。比如,不法分子使用AI技术生成了一段虚假的亲属语音信息,声称家中告急亟需紧急转账。受害者因为听到了亲属的声音,从而引起恐慌和焦虑,没有多想就进行了转账。

2.虚假视频诈骗

利用AI技术生成更加逼真的虚假视频,制造更加真实的人物或情境,让受害者更容易上当受骗。例如,近年来,有不法分子将现实中的一个人脸替换了电影明星的脸,并通过社交媒体传播,诱导用户和粉丝点击链接下载恶意软件或输入个人信息。

3.网络钓鱼诈骗

利用AI技术生成虚假的网站、邮件等,诱导用户输入个人信息或下载恶意软件。例如,在一个网络钓鱼事件中,黑客使用AI技术生成了一个虚假的银行网站,通过短信形式告知对方打开某银行网站,让受害人输入银行卡号和密码进行验证,导致受害人银行卡被盗刷。

4.进行定向攻击

黑客可以使用AI技术分析目标用户的行为特征和个人信息,进行精准定向攻击,窃取个人敏感信息。例如,在一次定向攻击事件中,黑客使用AI技术制作了虚假的社交媒体账号,并通过该账号发送钓鱼链接,成功窃取了目标用

户的个人信息。

红包返利类、冒充客服类、“AI 换脸”新型诈骗这三种类型是近期辖区内发生概率较高的案件，诈骗分子为了能保证诈骗成功，利用受害者心理实施诈骗，与受害者之间并无直接接触，通过技术手段诱导受害者输入个人信息，从而达到诈骗财产的目的，有因为贪心丢失财产的，也有没有贪心而中招的，防不胜防。为什么诈骗分子能够实施精准诈骗，是现代网络诈骗愈加地科技化还是公民防范意识不足？

三、电信网络诈骗频发的成因

(一) 公民个人防范意识薄弱

对于公民个人而言，有些公民保护个人信息的意识不强，甚至没有形成保护个人信息的意识，在街头随意扫码免费领纸巾、把含有个人信息的快递盒子乱扔乱放、登陆某些网站时，随意使用自己的真实信息办理各种会员卡等，为个人信息的泄露埋下了隐患。再者网络是一把双刃剑。一方面网络海量的资源能够给公民提供最前卫的讯息，另一方面也给诈骗分子带去了可乘之机，尤其在信息共享的时代，上网成为每一个公民生活中的一部分，公民难以甄别虚假诈骗信息，诈骗分子借此利用一些虚拟网站，如利用 AI 技术生成虚拟音频、视频、网站，盗取公民信息，诈骗公民财产。当然也有一些受害者被一时的蝇头小利蒙蔽双眼，如在面对红包返利时，因为自己的贪念想要获得红包返利，跟随诈骗分子的指示去下载 App，一步一步被套牢，最终因小失大，根源还是在于内心的贪利动机。当下也存在很多应用软件过度收集用户的通讯录、购物记录、消费记录等信息，对这些数据进行分析，根据用户的喜好，匹配用户可能需要的产品或服务，但是对于这些收集来的个人信息并没有很好地加以储存和保护，再次给了不法分子实施诈骗的机会。如冒充客服类诈骗，诈骗分子通过非法渠道获取受害者信息并致电，谎称自己是“百万保障”保险业务客服，以受害人购买商品时点击了“百万保障”需要取消，或者已到期需要续保等为由，引导其点开“百万保障”页面。谎称受害人已经开通“百万保障”服务，每月要扣费数百至数千元，引发受害人恐慌，骗子告诉受害人，可以将微信、支付宝绑定的银行卡中的存款转出，避免微信、支付宝扣款，同时引导受害人下载各类软件，利用受害人下载的软件，诱骗受害人将钱款转至“安全账户”，或通过“屏幕共享”窃取受害人银行卡号、短信验证码等信息，将受害人卡中资金转走。公民个人防范意识薄弱也给不法分子提供了诈骗空间。

(二) 行业治理缺乏力度

行业治理主要是指金融、通讯、互联网领域。根据 2022 年我国大数据应用市场发展现状及市场规模分析，互联网、主管部门、金融和电信引领大数据融合产业发展，合

计规模占比为 77.6%。互联网、金融和电信三个行业由于信息化水平高，研发力量雄厚，在业务数字化转型方面处于领先地位。目前电信业建设的 5G 网络处于全球领先水平，也已经实施电话号码实名制，但是仍然存在体制机制上的漏洞，在实名之前还有很大一部分的“黑号”“假号”等没有处理，这部分使用虚假身份信息办理的电话号码成了空白区。此外还有金融、互联网行业，出现了贷款诈骗、集资诈骗、“杀猪盘”类诈骗等，如某受害者因浏览网页看到贷款 App，声称无抵押、无担保、超低息，只需注册，贷款立马到账，随即下载 App 注册并申请贷款 15 万元，之后打开自己的银行账户，发现并未到账，咨询客服回复贷款已发放让按规定时间还清贷款。金融、互联网未履行好监督管理职责，也给诈骗分子提供了便利。当然电信行业、金融行业、互联网行业，如何统筹协调各方面工作的开展也是需要进一步探索的问题。

(三) 社会诚信体系缺失

诚信是社会的润滑剂。诚信体系建设不仅强调人们的诚信意识，更多地是要减少社会不诚实的现象，但是随着大数据技术的发展，掀起了某些网站、App、电商平台、社会中介机构等媒介的兴起热潮，这些机构在利益的诱惑下，故意出卖和泄露公民个人信息，还有一些黑客利用网站漏洞，非法盗取用户信息，进行买卖，诈骗分子利用买卖来的公民信息实施诈骗。有些幸运的公民，被公安机关通过大数据研判和分析，确定其正在遭遇电信网络诈骗，及时联系和劝阻，最终迷途知返，但是有些受害者分不清是非观念，缺少踏踏实实做人、克勤克俭致富的思想，总想不费吹灰之力得到高回报，最终得不偿失，给社会也带来了不良影响，更给蠢蠢欲动的诈骗分子提供了机会，让其抓住这一弱点，精准实施诈骗，这一方面对社会诚信体系也提出了新的挑战。

四、电信网络诈骗应对措施

(一) 强化宣传引导，增强公民个人防范意识

加强面向全社会的有针对性的宣传教育，积极引导大众加强防范，提高大众防范意识和诈骗能力，公民个人也要主动去了解新型电信网络诈骗的手段、方式，掌握诈骗分子的套路，从自身出发去有效避免和减少财产损失。虽然相关职能部门一直在做法治宣传工作，但是宣传内容缺少一些生动的案例，应该充分利用网络新媒体平台等渠道开展线上、线下宣传，针对易受害群体，特别是老年人、青少年等群体，用生动、鲜活的案例揭示花样百出的电信网络诈骗行为，即以案说法、以案释法，让法治宣传进社区、进农村、进家庭、进学校、进企业，提高宣传的覆盖面和精准度，努力保护好人们的钱袋子。如“百万保障”案件，要让公民了解微信、支付宝“百万保障”均为自动开启的安全设置，完全免费且不会影响个人征信，只要接到陌生来电，无论以

何种理由，只要提到关闭微信、支付宝“百万保障”设置的，就是诈骗！一旦发现被骗保留证据，第一时间向公安机关报案。还要提醒居民接到自称客服的来电，不要轻信。如有疑问，直接拨打官方客服电话进行咨询核实。对于使用AI技术虚拟亲友音频实施诈骗的，若涉及汇款问题一定要与亲友确认，不能盲目相信对方，以防上当受骗，要有保护个人信息的意识，对陌生人保持足够的警惕，不轻易向对方泄露个人信息。

（二）源头管制、深化行业治理

从源头上打击电信网络诈骗是最具可行的方式。电信网络诈骗离不开金融、通讯、互联网，诈骗分子利用这些信息优势，钻行业管理漏洞，加强对这些领域的源头治理更是防范电信网络诈骗的关键和重点，也是难点。2022年12月1日开始实施《中华人民共和国反电信网络诈骗法》，这是我国第一部专门、系统、完备规范反电信网络诈骗工作的法律，设立专门机构、升级技术手段等，强化打击电信网络诈骗犯罪，特别是对电信、金融、互联网治理要承担风险防控责任，建立内部控制制度和安全责任制度，不断提升企业自律，还可从技术角度防范用户个人信息泄露，形成一套防范信息泄露的完善制度，并落实好用户信息安全保护主体责任，实现跨行业、跨地域协同配合，有效打击治理电信网络诈骗活动。

（三）构建社会诚信体系

商鞅徒木立信到最终成就秦国一番大业，就是从树立诚信开始。诚信，诚实守信，即要遵纪守法，信守承诺。社会诚信体系建设三大主体是诚信行政机构、诚信企业、诚信个人。诚信行政机构是一切诚信的前提，企业诚信是诚信的主体。首先，诚信行政机构要以政务诚信示范引领全社会诚信建设。其次，诚信企业要不断加强行业规范和自律，像金融、通讯、互联网行业领域，缺失诚信会影响金融、通讯、互联网市场的健康运行。最后，诚信个人要严格自律，严格遵守相关法律法规，树立正确的世界观、人生观、价值观。因为社会诚信体系从宏观上来讲属于我国核心价值体系的组成部分，从客观上来讲，关键还是在于个

人，每个人的诚实守信意识提高了，那么社会诚信水平也会不断提高。

五、结束语

电信网络诈骗手段千变万化，但是需要谨记“未知链接不点击，陌生来电不轻信，个人信息不透露，转账汇款多核实”这二十八个字，平时生活中注意保管好密码账号，不要主动添加陌生人为好友，凡是以各种理由要求转账的，不论转账金额的大小，一定是诈骗，更不要轻信“免费领取”“大额返利”等说辞，提高警惕不要轻易落入诈骗分子的陷阱。我国第一部反电信网络诈骗法已经实施，为有关职能部门提供了相应的法律依据，期盼电信网络诈骗能早日根除，还大众一个清朗的网络空间。

参考文献：

- [1]李富成,李富金.电信网络诈骗套路揭秘与防范[M].北京:中国检察出版社,2018.
- [2]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(01):94-99.
- [3]刘慧.大数据时代电信诈骗犯罪防治研究[D].大连:大连海洋大学,2023.
- [4]温金泉.定西市打击防范电信网络诈骗协同治理研究[D].兰州:兰州大学,2023.
- [5]刘磊.大数据背景下电信网络诈骗的防范难点及对策[J].网络安全与应用,2023(02):152-153.

基金项目：

新疆政法学院校长基金项目,项目名称:新疆南疆电信网络诈骗调查与防范研究,项目编号:XZSK2021008。

作者简介：

白莉莉(1995—),女,汉族,甘肃金昌人,硕士,讲师,研究方向:法学理论。

刘军怀(1993—),女,汉族,甘肃白银人,硕士,讲师,研究方向:法学理论。