Research On The Comprehensive Governance Of Telecommunications Network Fraud

Li Chang[1,a],Liang Xiao[1,b]

[1]Changchun University of Science and Technology Law School,Changchun,Jilin,China

[a] lichang0825@qq.com

[b]liangxiao9529@163.com

Keywords: Telecommunications network fraud; Personal information protection; Comprehensive control

Abstract. The development of science and technology has brought great convenience to our work and life, but also allow the illegal elements to take advantage of them. Telecommunications network fraud is a frequent crime in China in recent years. There are numerous victims. The amount of fraud is huge, and the public is deeply hurt, but there is no way to deal with it. This paper analyzes the new characteristics of the telecommunication network fraud under the Internet age,and traces the deep reasons for the frequent occurrence of the telecom network fraud. Based on the national conditions of our country and drawing on the experience of other countries, we should explore new methods and Countermeasures of China's telecommunications network fraud in order to protect the legitimate rights and interests of citizens and maintain social harmony and stability.

电信网络诈骗的综合治理研究

李畅 [1,a]，梁潇 [1,b]

[1] 长春理工大学法学院，长春，吉林，中国

[a] lichang0825@qq.com

[b]liangxiao9529@163.com

关键词：电信网络诈骗；个人信息保护；综合治理

中文摘要.科学技术的发展在带给我们工作生活极大便利的同时，也让不法分子有机可乘。电信网络诈骗是近年来我国高发的刑事犯罪，受害者不计其数，诈骗金额庞大，民众深受其害却无应对良策。本文剖析当今互联网时代下电信网络诈骗的新特点，追溯电信网络诈骗频发的深层原因。立足我国国情，借鉴他国经验，探索我国治理电信网络诈骗的新方法、新对策，保障公民合法权益，维护社会长治久安。

1. 引言

电信网络诈骗，是指不法分子通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人转账或窃取受害人个人信息转移其存款的犯罪行为。在我国，电信网络诈骗犯罪的起刑点为人民币 3000 元，最高刑期为无期徒刑。电信网络诈骗最早是 1997 年前后在我国台湾地区开始兴起，并迅速发展蔓延。2008 年时，此类犯罪已在台湾省内泛滥成灾，成为岛内“十大民怨”之首。2003 年，电信网络诈骗跨越台湾海峡，进入我国东南沿海一带，且发展迅速。此类犯罪手法逐渐被大陆的不法分子吸收掌握，效仿传播。随着 2010 年我国大陆地区网络电话、电子银行、网络银行等应用陆续开

通，电信网络诈骗案件发案率居高不下，社会危害加剧。虽然近年来，公安部针对电信网络诈骗展开多次专项打击行动，但收效不尽人意。2014—2017 年，我国电信网络诈骗案件数量一直呈上升趋势，案件数量以每年 20%~30%的速度增长，还有相当一部分电信网络诈骗没有立案。但是，面对发案率较高的电信网络诈骗案件，公安机关的破案率却只有 1%~3%，远不足以保障公民财产安全。

我国“十三五规划纲要”中明确提出，我国将实行国家大数据战略，将大数据作为基础性战略资源，全面实施大数据发展行动，加快推进数据资源共享开放和开发应用，助力产业转型和社会治理创新[1]。但是，大数据对个人信息的收集和利用，在给社会公众、企业、政府带来无限便利的同时，也让个人信息处于危险境地，个人信息的使用缺乏立法保护和行业规范，使犯罪分子有机可乘，利用大数据信息进行电信网络诈骗成为了他们的生财之道。2016 年，山东准大学生徐玉玉，因遭遇电信诈骗，被骗走 9900 元学费，郁结于心，骤然离世。这一案件引发了社会广泛关注，在各方努力下，徐玉玉案的主犯在几个月内相继落网，案件始末也水落石出。徐玉玉案是一件典型的由于个人信息泄露引发的精准型诈骗案件，主犯陈文辉从黑客杜天禹手中购买山东省高考考生信息，针对掌握的受害人详细身份信息设计诈骗方法进行诈骗活动。这样“窃取——出售——使用”个人信息的黑色产业链，已让不少人上当受骗，蒙受巨大的经济损失和精神打击。

2.当前我国电信网络诈骗的新特点

传统的电信诈骗，犯罪分子多采用随机拨打电话或发送短信的形式引诱受害者上钩，但随着大数据技术的发展，个人信息成为互联网重要资源，由于个人信息保护不仰慕，犯罪分子能够轻易获得个人信息，从而进化了诈骗手法。当前电信网络诈骗主要有以下特点：

2.1 隐蔽

在互联网技术还未大规模应用的年代，电信诈骗也具有一定隐蔽性，诈骗者利用电信通信技术，不与受害者谋面进行诈骗活动。而的现今的电信网络诈骗的不法分子，大多躲在互联网技术背后，进行远程诈骗，受害人不但对于诈骗者的面貌、位置等信息均不知情，甚至接到的诈骗电话也是虚拟号码，登陆的钓鱼网站也使用的是境外服务器。比如诈骗者利用伪基站等方式伪造通讯号码，行骗成功后就将诈骗号码丢弃，受害者发觉受骗后，再回拨电话就已经无法接通了，报警后警方倒追该号码，也无法查到任何有用的信息，增加了案件破获难度。其次，诈骗者利用银行监管漏洞，盗用他人身份信息开户，用于接收赃款，在诈骗得手的第一时间，将赃款转移，等公安机关追查到该涉案账户时，才发现户主并不是作案者，真正的犯罪嫌疑人已经不知去向。即使公安机关在不法分子尚未转移赃款前便锁定了诈骗账户，等待犯罪分子来转移赃款时实施抓捕，但由于电信网络诈骗多为团伙作案，内部分工明确，来转移赃款露脸的人往往是临时雇佣的“马仔”，对团伙上层人员身份知之甚少，当“马仔”被公安机关抓获的时候，首要分子很可能已经销声匿迹了。

2.2 精准性

电信诈骗案件久治不愈，其根本原因是个人信息泄露严重。个人信息泄露渠道主要是两种：其一是黑客入侵互联网系统非法获取，如徐玉玉案中徐玉玉的个人信息就是黑客杜天禹入侵山东省高考招生信息平台系统窃取后贩卖的。其二是内部人员利用职务之便非法贩卖个人信息，如南京一政府机关工作人员在任职副主任科员、主任科员期间，利用职务之便对外出售、提供包含公民个人信息的企业信息 82 万余条。由于取得个人信息的手段隐蔽，且出

[1] 陈平，朱劲松，钟奇：“集成电路、通讯、大数据领域的十三五规划要点分析”，《集成电路应用》，2016 年 4 期，第 6—7 页。

售后获益颇丰，便有很多人走上这条违法犯罪道路，长此以往，便形成了个人信息买卖的黑市，黑市上贩卖的个人信息数量庞大，且覆盖面广，种类繁多，通过这样的“地下大数据库”，几乎可以构建出一个人的大部分隐私信息和财产信息，为犯罪分子实施精准诈骗提供便利。犯罪分子根据获取的个人信息，有针对性地制定诈骗策略，受害人在与犯罪分子交流过程中发现对方对自己的真实信息掌握的一清二楚，往往就会放松警惕，更容易相信犯罪分子的谎言，掉入陷阱。

2.3 技术性

科学技术的发展不但便利我们的工作和生活，也更新了犯罪分子的作案手法。这里主要介绍三种常见技术：“猫池”、“伪基站”、“木马病毒”。

猫池（ModemPOOL）就是将相当数量的 Modem 使用特殊的拨号请求接入设备连接在一起，可以同时接受多个用户拨号连接的设备。猫池广泛应用于大量具有多用户远程联网需求的单位或需要向从多用户提供电话拨号联网服务的单位，但被不法分子利用，用于提高发送短信和拨打电话的效率，猫池不仅能够实现集群发布，而且使用方便成本低廉，成为电信网络诈骗的热门手段。但是，猫池也有弊端，由于需要通过插手机卡配合电脑端群发短信，在发送一定数量短信后，电话卡会被锁死，需要大量的电话卡用以更换和备用。

基站是指通过接收和发送无线电信号，在移动设备之间实现信息交换的一种用于移动信息通讯的设备，一般需要审批获得许可，才能进行无线电信号收发。而“伪基站”不具备合法审批手续，也没有办理无线网络入网许可证，其设备工作便是非法占用频率资源。伪基站设备一般由电脑和手机组成，通过群发器、短信发信机等设备，能够搜到以伪基站设备为中心，一定范围内的移动通讯用户的电话号码，通过伪装成运营商的基站，冒用他人手机号或者公共服务号码，向用户发送诈骗短信。利用伪基站获取信号或者发送短信的时间极短，不易察觉，因此未见设备难以被公安机关找到，其次，也因为伪基站设备体积小，可以安装到车辆上使用，增强了伪基站的流动性，也使得伪基站即使被发现，也能轻易逃脱公安机关的法网。

植入手机木马病毒，也是电信网络诈骗的惯用伎俩。不法分子从网上购买手机病毒，通过伪基站群发带毒短信，一旦有人打开病毒链接，手机会自动下载并安装木马病毒 APP，手机便被不法分子所控制，不法分子会获取受害者手机中的通讯录信息，以受害者的名义将带毒短信发送给通讯录中的联系人，使木马病毒呈几何级扩散。同时，由于控制了受害者手机，手机验证码、绑定的银行卡号、身份账号等个人信息也被不法分子掌握，便可以通过快捷支付平台将受害者与手机绑定的银行卡中的资金进行套现。

3. 国外个人信息保护的立法实践

2014 年—2017 年，全国电信网络诈骗案件数量呈上升趋势，自 2015 年起，每年犯罪嫌疑人从群众手中骗走的财产都超过百亿人民币。当然，电信网络诈骗并不是我国特有的犯罪，在其他发达国家也很普遍，但相较于我国的案件数量和诈骗金额，便不可同日而语。据统计，美国电信网络诈骗案件数量，仅为我国二成，日本电信网络诈骗最为猖獗时期，诈骗总额也只有 559.4 亿日元，约合人民币 33 亿元。其中原因有很多，比如发达国家科学技术水平高，相应的网络通信安全系数也比较高，民众有较强的自我保护意识，最为关键的是发达国家拥有比较完善的个人信息保护法律体系，面对向精准化方向发展的电信网络诈骗，增加了犯罪分子获得公民个人信息的难度，遏制电信网络诈骗泛滥的势头，我国在个人信息保护的法律空白，的确成为导致电信网络诈骗高发的一个重要因素。

3.1 美国

反观域外，欧美国家的个人信息保护法律是随着互联网技术的发展而逐步完善的。美国模式，是通过建立政府引导下的行业自律机制，政府在不干预商业主体正常商事活动的前提下，保护公民个人信息安全。国家立法上，美国将个人信息纳入隐私权范畴进行保护，虽然也是采取分散式立法的途径，但保护范围十分全面：如 1974 年《隐私法案》，用于规范联邦政府处理个人信息的行为；1998 年《儿童在线隐私保护法》，用于保护互联网中的儿童信息；1999 年《金融服务现代化法》，要求金融机构尊重消费者隐私权，保证消费者个人非公共信息的安全和保密；HIPAA 法案，用于保护公民个人医疗信息安全等。

当然，美国作为一个资本主义国家，奉行个人至上和财产私有制，更注重个人利益和自由，因此面对个人信息保护问题，行业自律作用大于法律规制作用。美国最有特点的行业自律模式，便是“在线隐私联盟”和“网络隐私认证计划”。在线隐私联盟（OPA）是美国互联网领域的一个产业联盟，通过公布“在线隐私指引”，来规范成员公司收集和使用用户信息的行为，虽然成员有义务遵循该指引的规定，但联盟并不会主动监督成员行为，需要成员自觉主动遵守指引。网络隐私认证计划，是指被许可张贴隐私认证标志的网站，必须遵守网上收集信息的行为准则，服从认证机构和行业组织的监督管理。目前最有名的网络隐私认证组织是“TRUSTe”和“BBBonline”。

3.2 欧盟

欧盟于 1995 年颁布的《个人数据保护指令》，是世界个人信息立法保护领域中里程碑式的法律，许多国家都效仿该指令的内容，来修订本国的个人信息保护法。《个人数据保护指令》的目的，一是为了保护自然人在数据处理中的合法权益，二是为了促进个人数据在各成员国之间的有效流通，减少个人数据跨国流通的限制。指令确定的六大原则：合法原则、终极原则、透明原则、适当原则、保密和安全原则，以及赋予数据主体查阅权、拒绝权、救济权等核心内容，成为此后其他国家制定个人数据保护法的重要参考。

但是信息技术的更新换代使得《个人数据保护指令》逐渐不符合社会发展的需要，随着“ABC 时代”的到来，AI（人工智能），BigDate（大数据），Cloud Computing（云计算）技术已经不能被《个人数据保护指令》所规制，因此，2016 年，欧洲议会通过了堪称史上最严格的个人数据保护规则《一般数据保护条例》，条例同样旨在加强对自然人的数据保护，并统一此前欧盟各成员国国内零散的个人数据保护规则，将适用主体范围扩大到了境外的企业，增加了透明原则、数据最小化原则、目的限制原则、存储限制原则等一般性保护原则，开创性地引入了被遗忘权、反对权等民事权利，具体规定了罚款金额上限。

3.3 日本

作为一个善于学习借鉴，并将本国国情与别国先进经验高度融合的国家，日本对于个人信息保护领域依旧做到了“师夷长技”，选择了专门性立法和行业自律模式并行的途径。日本地方自治条例对个人信息保护要早于国家立法。其中，最早的地方立法是 1973 年 6 月日本德岛市制定的《电子计算机处理的个人信息保护条例》。截至 1999 年 4 月，日本 72.3% 的地方自治团体，确立了包括条例、规则或者规程等手段在内的个人信息保护制度，其中的 46.1% 制定了条例。[2] 1988 年，日本国会通过《关于对行政机关所持有之由电子计算机处理的个人信息加以保护的法律》，规范国家行政机关利用计算机处理个人信息的行为，是日本政府颁布的第一部用以保护个人信息的法律。此后日本其他诸多部门法的修订过程中，均包含保护个人信息安全的条款。直至 2003 年，受欧盟《个人数据保护指令》影响，日本国会陆续通过以《个人信息保护法》为首的“个人行保护五连法”，联同其他专

2 [日] 新史保生：“プライバシーの権利の生成と展開”，株式会社成文堂，2000 年 12 月，第 349-350 页。

门性立法，日本基本确立了个人信息保护的法制化框架。[3]《个人信息保护法》的形式和基本原则与欧盟《个人数据保护指令》很接近，但又不同于欧洲的严格保护思想，《个人信息保护法》对非公共部门利用个人信息的规定较为灵活，鼓励非公共部门进行根据自身情况制定自律规范，加强行业自律。

4.我国综合治理电信网络诈骗的路径

4.1 建立健全个人信息保护法律体系

追根溯源，电信网络诈骗案件频发的根源是个人信息泄露严重，因此要治理电信网络诈骗，需从源头着手，保护个人信息安全。

我国个人信息保护的相关法律条文，散见于各个部门法之中，重点的法律条文和司法解释有《中华人民共和国网络安全法》第四章、《刑法》第 253 条，《身份证法》第十三条第二款、《护照法》第十二条第三款、《传染病防治法》第十二条、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等。虽然诸多法律条文都涉及到公民个人信息保护，但大多法律条文规定过于原则，不具体，操作性差。目前，我国还没有一部专门性法律对个人信息安全加以保护，虽早在 2003 年相关部门就着手《个人信息保护法》草案拟定工作，但十多年过去，仍未采取正式立法措施。当然，这与我国在社会主义建设关键时期，互联网产业发展处于蓬勃阶段不无关系。

国家谨慎对待个人信息法，因为加强对个人信息的保护势必限制互联网巨头对个人信息的利用，影响个人信息的流通，限制互联网产业的发展。但是，在个人信息被肆意传播而没有法律规制的情况下，以牺牲公民的合法权益换来的信息技术的发展，最终还是会投以恶果于公众。我们要做的，不是对个人信息安全问题视而不见，一心只想谋发展，而是寻找个人信息保护和流通的平衡点，兼顾经济发展需求和个人信息保护。我们要做的，是在加快《个人信息保护法》专项立法进程的同时，对刑法、民法、行政法领域进行补充立法，形成《个人信息保护法》为主，其他部门法为辅的个人信息保护的法律体系。

4.2 建立“警企联动”的反诈骗信息平台

商业信誉是企业的立身之本，信誉和口碑是商事主体的经济命脉，因此，“重利轻安”式的发展模式已经渐渐被企业所摒弃。与电信网络诈骗密切相关的行业，金融业和电信业，面对电信网络诈骗的日渐猖獗，都纷纷展开“反诈骗行动”。而公安系统作为打击电信网络诈骗的主力，除了承担刑事案件的侦破责任，还着手利用大数据平台，研发智能防控系统，如广东省佛山市公安局研发的“天盾”平台，就是专攻事前提醒和防控电信网络诈骗。

工商银行研发并投产的“外部欺诈风险信息系统”，是运用风险信息大数据，进行电信诈骗防控的代表。该系统收录了来自行内、金融同业以及司法行政部门提供的各类风险客户和账户信息，经过分类评级后的信息按照不同的业务需求分别在银行核心系统以及个人金融、信贷、授信、银行卡等业务领域投入使用，为相关业务审核和办理提供预警和控制支持[4]。电信行业，三大电信运营商在反电信诈骗中起到了重要作用，加强技术防范管控手段，采取主动堵截“虚假来电”、退出防欺诈提醒服务、建立“伪基站”侦测平台等手段，最大限度降低市民受欺诈的可能性。虽然三大运营商均采取措施有效打击电信网络诈骗，但仍有未尽之处。工信部在 2013 年出台了《电话用户真实信息登记规定》，在全国范围内推行电话用户实名制，但电信企业实名制还未能做到位，“黑卡”泛滥依旧未能得以解决，为电信移动诈骗提供滋生温床。“天盾”，是我国公安系统首款反信息诈骗平台，将公安大数据运算的“时效性”与“可靠性”充分应用到防范电信诈骗的民生工程之中。“天盾”体系由手

[3]吕艳滨:“日本的个人信息保护法制”,《个人信息保护前沿问题研究》,北京:法律出版社.2006 年 ,第 156 — 160 页。

[4] 蒋浩，易月：“交通银行首家成功对戒期货互联网开户云平台”，《金融经济（市场版）》，第 1 页。

机 APP、微信公众号和官方网站组成，组建三重防诈骗体系：第一重，运用公安大数据平台资源，采取“事前发现、事中干预、事后打击”工作模式，及时推送电信诈骗新型作案手法及特征；第二重，即时发布高发电信诈骗预警，准确压制电信诈骗嫌疑账号、直接干预电信诈骗实施：第三重，智能识别、拦截、封堵涉电诈黑名单号码对民众的呼入、呼出、短信发送行为[5]。

然而，公安机关、银行、电信运营商的“各自为战”，虽然在一定程度上压制了电信网络诈骗的高发态势，却不能形成一个完整的防控链，各方拥有的优势和资源不能互通共享，打击效果也大打折扣。因此，为更加有效的保护公民的人身财产安全，维护社会的和谐稳定，政府、企业和社会团体应当通力合作，形成“反信息找联盟”，各取所长，建立警企联动的反诈骗信息平台。360 公司成立的“猎网平台”，全面开放 360 公司安全大数据，提供大数据分析技术的支持，协助公安机关打击电信网络诈骗，这就是“警企联动”打击电信网络诈骗的成功实例。

4.3 提高公民防范意识

想要杜绝电信网络诈骗，保护个人财产安全，不能只把责任推给政府和社会，作为电信诈骗罪直接的受害者，我们每个人也要提高自身的防范意识，不使不法分子有机可乘。其要点有三：一是防范个人信息泄露，二是涉及钱财交易要小心谨慎，三是遭遇诈骗及时报警，留存证据。

2016 年发布的《公共个人信息安全和隐私保护报告》显示，由于对个人信息泄露渠道的不了解，虽然大多数人意识到个人信息泄露的严重程度，但相当高比例的人群并不知道如何防范个人信息要害，在使用个人信息载体疏忽大意或不知如何采取防范行动。不注意标注证件复印件的用途，不撕毁或涂抹快递单信息，不确认免费 wifi 的安全便连接使用等等行为，都有可能成为泄露公民个人信息的缺口。而这些因疏忽大意而泄露的信息，都可能被不法分子利用，成为其进行电信网络诈骗的工具。

在电商行业发展迅速，智能手机普及率大大提高的信息化时代，我们更要注意保护个人信息。网购后销毁快递单，不下载安全系数未知的手机软件，不随意连接陌生 WiFi，从生活中注意这些细微之处，防范个人信息泄露。网络银行、支付 APP 等电子支付手段固然方便，但提高了金融交易的风险系数。涉及大额转账交易时，应当在确认对方身份后进行，对于不熟悉的金融业务，尽量不要在 ATM 机上操作，应去柜台办理。如若不慎遭遇电信网络诈骗，不应当息事宁人，自认倒霉，而应当在第一时间保留证据，向公安机关报案，积极维权，及时止损。对于不良信息，诈骗电话或骚扰短信，可以向 12321 网络不良与垃圾信息举报受理中心网站进行举报投诉，防止更多的民众掉入诈骗陷阱。

5. 结语

当今的电信网络诈骗手法隐蔽，取证困难，影响恶劣，波及范围广却难以侦破。民众深受其害，百姓多年积蓄一朝灰飞烟灭，受骗者在承受巨大经济损失的同时，还承受着更大的精神打击。信息技术的发展不能成为不法分子违法犯罪的嫁衣，要治理电信网络诈骗，不能将压力统统给予公安机关，而应当建立健全相关法律法规，着力于事前预防、事中干预、事后侦破三阶段，联合政府、企业、社会团体以及每个公民的力量，编织一张疏而不漏的“法网”，让电信网络诈骗无处遁形。

[5] “网业创新”，《中国信息安全》，2016 年第 9 期，第 87 页。

References

[1] Hu Xiangyang,Liu Xiangwei,and Peng Wei, Research on the countermeasures for the prevention and control of the crime of telecommunication fraud, Journal of Chinese People's Public Security University(Social Sciences Edition),vol.5,pp.90-98,2010.

[2] Li Weiqiang,The study of the telecommunications fraud criminal law and harnessing countermeasures,Master's thesis,LanzhouUniversity,Lanzhou,Gansu,China,2012.

[3] Wu Tao,Li Chengxu,and Ma Liuxia, China credit reporting legal system construction based on general data protection regulation, Credit Reference,vol.12,pp.50-53,2016.

[4] Qi Aiming, Draft proposal on the draft model law on People's Republic of China's personal information protection law, Hebei Law Science,vol.6,pp.3-5,2005.

[5] Liu Jinghui, Comprehensive governance of telecom fraud in the era of "Internet+", Modern Science & Technology of Telecommunications,vol.4,pp,61-66,2016.

[6] Hei Jing, Discussion on the working principle of pseudo base station and its identification and detection methods, Information Technology and Informatization,vol.4,pp.251-253,2014.

[7] Jiang Hailong,Wu Xiaodong,and Chen Xuehao, Research on unified design and construction pattern of traffic management online service system of public security ministry, China Public Security(Academy Edition),vol.2,pp.67-71,2014.

[8] Huang Xinrong, Reflection on ethic of Mega - Data technique, Journal of Xinjiang Normal University(Edition of Philosophy and Social Sciences),vol.3,pp.46-53,2016.

[9] Wu Chaoping, The development and change of telecom fraud and its prevention and control of "Internet+", Journal of People's Public Security University of China(Social Sciences Edition),vol.9,pp.108,2016.

[10] Zhu Shaolong, The countermeasures about current investigation and prevention of telecommunications fraud, Master'sthesis,Southwest University of Political Science & Law,Chongqing,China,2016.