

# 机器人来电 “AI 外呼电推”成骚扰电话帮凶

“这里是口腔医院,请问你有没有牙齿治疗方面的需求……”据报道,连续几个月来,大量上海市民频繁接到以上述话术开场的骚扰电话。记者调查发现,背后的原因在于,众多民营口腔诊所通过第三方公司开展“AI 外呼电推”。有关公司称,“几乎将上海市民的电话全部打了一遍”“效率很高,一天几十万、上百万条信息就发出去了”。AI 电销是如何运作的?海量的客户信息从何而来?其中又涉及哪些法律问题?



消费者手机中显示的未接电话多数被标记为骚扰电话

## “盲打”骚扰“拉黑”也没用

“先生您好,我们是做采耳养生的,方便加一个微信了解一下吗?”8月10日早晨,江西南昌市民杨先生被一通陌生电话吵醒。“本以为是工作电话,结果是广告骚扰电话。”被打扰的杨先生憋着一肚子火,话到嘴边却又咽下,只因“对方根本不是‘人’,说了也白说”。

杨先生的经历并非个例。前段时间,上海不少市民反映,接到了上海某口腔医院AI骚扰电话,“拉黑”和开启手机广告拦截功能都不管用,让人不胜其烦。不少消费者反映,这种AI骚扰电话所显示的号码,大多为本地区号的座机或虚拟运营商手机号。无论是明确表示没有需求,或是利用手机系统“拉黑”阻拦,都挡不住这类电话不断打来。这些由机器人拨打的电话会不停更换“马甲”来电,所以即使“拉黑”也没用。

根据媒体报道,有记者就“口腔诊所”这一类骚扰电话进行了深入探访。原来,是有第三方企业专门负责广泛拨打电话,来“挖掘”出有需求的消费者,进而再将这些消费者的信息出售给民营口腔诊所。这个“挖掘”业务被称为“AI 外呼电推”。这种利用AI技术在电话推广营销中挖掘潜在消费者的方式效率极高,但也导致大量民众深受其扰。

据称,这种服务是通过先“盲打”的方式,几乎将当地的手机号码全部打一遍,通过剔除明确拒绝的消费者后,再对剩下的人进行二次、三次拨打。不同企业轮番通过第三方公司开展“AI 外呼电推”,这就是消费者频繁收到骚扰电话且表示拒绝后仍会不断收到类似电话的原因。

## AI 外呼一天能拨出2万通电话

据《法治日报》报道,目前市场上的AI 外呼系统主要有两种形式,一种是购买AI 外呼机器,需搭配手机使

用;另一种是购买外呼管理系统,电脑端或手机端都可以操作。一位名为“aaa 外呼李老师”的人称可进行话术定制,如果对电话号码外显归属地有要求,则可让号码显示某个具体城市。购买AI 外呼系统后,会组建专门的群,发送话术框架,根据推销人员的需求,由录音员录制。据介绍,如果只是想单纯通过AI 外呼系统绕开监管,最后通话还是由人工来完成,一天可以通过系统拨打400通电话;如果既要规避监管又由AI 来完成通话,一天可以通过系统拨打3000至2万通电话。

社交账号名称为“外呼系统x经理”的业内人士揭开了“防封秘籍”：“进入AI 外呼电销系统后,可以自行设置本机号码,随后打开软件的拨号键盘,输入客户电话并拨打,此时电话不会直接打通。过两秒后,会有平台打电话进来,此时你接通后是和客户通话,但是你却从‘主叫’变成了‘被叫’,并且客户手机上显示的是你设置的号码。通过‘双向回呼’的方式来解决封号问题,在这种情况下,运营商查不到你的呼出记录,只能查到你的接听记录。这种‘拨打’电话的方式不会扣个人的话费,而是扣系统的话费,一般价格是每分钟0.13元至0.16元。”

记者调查发现,售卖AI 外呼系统的商家,往往也会将客户资料免费赠予或低价售予买系统的人。客户资料分为两种,一种是类似“xx查”上面的数据,比较便宜;还有一种数据偏贵,可以只导入关键人或法人的电话,数据更精准,号码来源更广、活跃度更高。有AI 外呼系统销售人员宣称:“我们收集的都是公开信息,不违法。”

在北京汇祥律师事务所高级合伙人魏卓然看来,根据刑法第二百五十三条之一规定的侵犯公民个人信息罪以及《最高人民法院、最高人民检察院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》等相关司法解释,商家批量整合和出售、提供公民个人信息的行为涉及多个法律问题:批量整合公开联系方式的合法性。一些平台上的公民个人联系方式属于合法公开的信息,商家批量整合这些公开信息的行为本身不一定违法。但如果这些信息被用于未经授权的商业目的,尤其是用于骚扰电话或其他侵犯个人隐私的行为,则可能构成侵犯公民个人信息罪。赠送或售卖经批量整合的联系方式的合法性。将批量整合的联系方式赠送或售卖给外呼系统买家,若其用于AI骚扰电话等商业目的,可能构成侵犯公民个人信息罪。从刑法为侵犯公民个人信息罪设置的构成要件来看,该罪侵犯的客体是公民的“个人信息”,而不仅限于不为他人所知的“个人隐私”;该罪的行为方式也不仅限于“通过非法方式获取公民个人信息”。也就是说,未经信息主体同意,获取、出售或者提供公民个人信息,即使信息本身是公开的,也可能构成本罪。

## 治理AI电销需要技术向善向上

7月1日起施行的《消费者权益保护法实施条例》第二十三条规定,经营者应当依法保护消费者的个人信息。经营者在提供商品或者服务时,不得过度收集消费者个人信息,不得采用一次概括授权、默认授权等方式,强制或者变相强制消费者同意收集、使用与经营活动无直接关系的个人信息。第二十四条规定,未经消费者同意,经营者不得向消费者发送商业性信息或者拨打商业性电话。消费者选择取消的,经营者应当立即停止发送商业性信息或者拨打商业性电话。

江苏省消保委认为,科技是第一生产力。AI技术被人们赋予了智能家居、无人驾驶、图像复原等美好的憧憬,令人失望的是,消费者最常接

触到的AI技术却是AI骚扰电话。这种躲也躲不掉的“流氓行径”不仅给消费者的生活带来不便,更侵犯了消费者权益;如果被不法商家利用,还可能诱导缺乏判断能力的消费者走入消费陷阱。这背后映射出经营者与消费者之间的权责失衡,科技本无善恶,但是错误使用就会使科技沦为经营者侵害消费者合法权利的工具。引导科技向善向上,通讯运营商和行政监管部门责无旁贷。

那么该如何有效规范AI电销?江西朗秋律师事务所律师万浩认为,对于AI 外呼企业贩卖个人信息、商家拨打骚扰电话牟利等行为,一方面,要完善赔偿和处罚规则,支持消费者通过诉讼维权;另一方面,监管部门应积极介入,督促手机APP等获取个人信息的主要渠道采取安全保障措施,从源头上保护个人信息。

江苏省消费者权益保护委员会呼吁,AI技术亦可以用于深入学习骚扰电话的拨打规律,精准标记此类电话并进行阻断,以强大的技术支撑,让AI电销现原形、拨不通,翻不出监管的“手掌心”。同时,对于第三方“AI 外呼电推”企业贩卖个人信息和通过这类企业拨打骚扰电话并牟利的经营行为,监管部门理应以研究并定性,涉及违法犯罪的应严厉打击。另外,全面落实个人信息保护法要求,督促网站、APP等获取个人信息的主流渠道采取安全保障措施,发现问题及时下架、处理。

江苏省消保委鼓励消费者增强个人信息保护意识,使用软件时留意个人信息权益的勾选、授权。此外,消费者可以开通通信运营商提供的“骚扰电话拒接”服务,屏蔽部分骚扰电话;也可以积极标记骚扰电话或者向12321网络不良与垃圾信息举报受理中心投诉,共同监督电话营销环境。(综合)

# 频繁遭遇营销电话、垃圾短信骚扰怎么办？

“您有最高20万元借款额可于6月28日申请,请尽快确认!”“您的手机号即将于6月30日自动扣除2023年积累的298000分,换商品点(链接)”“恭喜您被天降福利砸中!现在申请借款额度即可免费获得大额月付金,活动时限有效,仅限点(链接)参与。”“提醒:您的4天免费课程已到!请24小时内点击(链接)验证码!”……

你是否经常收到培训学校、借贷平台、装修公司等“不请自来”的营销电话、垃圾短信?当频繁遭遇骚扰电话、短信时,你是否知道应该怎么做?

工信部发布的《2024年第一季度电信服务质量的通告》显示,全国电信用户申诉中,涉及服务争议的申诉占比38.7%,涉及营销、收费、资费争议的申诉占比44.9%,涉及网络、安全的申诉占比16.4%。

在12321网络不良与垃圾信息举报受理中心发布的2024年第一季度非应邀商业电子信息投诉情况盘点中显示,非应邀商业电话投诉情况方面,在所有的非应邀商业电话的拨打方式中,中国移动占比35.8%,中国电信占比26.7%,中国联通占比24.6%,移动转售占比7.6%,中国广电占比5.3%。

其实,近年来国家相关部门着力整治骚扰电话扰民问题并取得一定成效。

国务院新闻办举行的2023年工业和信息化发展情况新闻发布会披露数据显示,2023年全年共拦截骚扰电话540亿次,公开通报1861款违规APP。深入开展非应邀电子信息治理,处置违规短信端口号码4212个,“来电免打扰”防骚扰服务用户达到6.2亿人。持续推进电信网络诈骗防范治理,拦截涉诈电话和短信近50亿次,核查处置涉诈高风险互联网账号超2亿个。

同时,为防范用户受到“不请自来”的营销电话侵扰,在工业和信息化部指导下,中国信息通信研究院组织中国电信、中国移动、中国联通三家电信运营商,面向全国用户免费提供“骚扰电话拒接”服务。

具体如何操作?中国移动用户可以关注“中国移动高频骚扰电话防护”微信公众号,点击菜单栏“电话防护”“骚扰拦截设置”,打开所有号段拦截开关,再返回点击“防护业务开关”,打开高频骚扰电话防护开关。中国电信用户可以关注“天翼防骚扰”微信公众号,点击菜单栏“来电防护”“本机号码一键登录”“立即开通”,再返回“来电防护”界面,添加免打扰的功能即可。中国联通用户可以打开中国联通APP,搜索栏搜索“手机助手”,绑定手机号、开通服务,再返回“手机助手”界面,勾选想要防护的选项即可。

当遇到骚扰短信内容已侵犯个人隐私权时,泰和泰律所律师尹晓东建议:一是要立刻收集证据。当收到骚扰短信时,应立即截图或拍照保存证据。这些证据包括短信内容、发送者的手机号码和发送时间等。同时,保留好手机的通话记录和短信记录,以备日后可能需要的调查或举证。二是及时报警处理。如果骚扰电话和短信涉及侮辱、诽谤、恐吓等违法犯罪行为,可以直接向公安机关报案。在报案时,提供骚扰电话或短信的内容、发送者信息以及收集的证据,警方会依法进行调查处理。三是积极寻求法律援助。如果骚扰短信对生活和工作造成了严重影响,还可以寻求法律援助。专业律师可以帮助用户评估情况,提供法律建议,并协助采取进一步的法律行动。除了采取上述措施外,还应加强个人信息安全保护,避免随意泄露个人信息,谨慎处理陌生人的短信和电话,及时更新手机系统和应用程序。

(四川发布)

## 观点

## 需打准AI电销的“七寸”

骚扰电话并不是新鲜事,如今,这一困扰社会的顽疾不仅久治不愈,还搭上了人工智能“快车”,升级成为AI电销。此类电销凭借足量的客户数据,永不断绝的“呼叫”系统,防“拉黑”的技术加持,成为电话销售行业高效率、低成本的“利器”。

从表面上看,AI电销用的是AI技术,实质上是对公民个人信息的侵犯。多家AI电销平台透露,此前与口腔医院有过“合作”,他们先通过AI盲打电话挖掘有需求的用户,再将用户信息出售给口腔医院从中获利,客户数据是用爬虫技术抓取获取的。事实上,此类行为涉嫌非法获取个人信息,侵犯个人隐私。一方面,电销平台可能通过非法手段获取用户个人信息,如技术抓取、购买非法数据等,违反了个人信息保护法的相关规定;另一方面,未经用户同意擅自利用AI向其拨打电话进行营销,侵害消费者生活安宁、不被打扰的权利,也属于侵犯个人隐私的行为。

AI电销为何像“牛皮癣”一样难治?首先在于个人信息的泄露途径难以确定。据披露,AI外呼系统一天可以自动拨打3000至2万通电话,这些电话来自不同的APP、网络平台、第三方营销公司等,均为虚拟号码,使得追踪和确定信息泄露的途径变得异常困难。

其次,部分电销平台将个人信息买卖做成黑灰产业链,销售对象不特定,进一步增加了监管的难度。再次,现实生活中,很少有消费者因骚扰电话而诉诸法律,对此类“小事”的维权意愿不强也客观纵容了此类行为。

为有效遏制AI电销泛滥,引导AI技术向上向善,应尽快通过法律惩治、技术创新等手段加强源头治理。首先,监管部门要对AI电销开展全链条整体打击,彻底拔除这颗“坏牙”;同时,更要加强针对性,突出重点打准“七寸”,牢牢抓住其中“侵犯个人信息”这个要害环节,全面落实个人信息保护法要求,如督促网站、APP等获取个人信息的主体,采取必要措施防止信息泄露,发现问题及时处理;另外,通过有效监管,督促电信运营商把好关口、当好“守门人”,开发更加智能精准的识别手段,对AI电销进行技术侦测、防范、拦截,牢牢遏制其发展势头。

技术本身没有好坏之分,关键是看谁在用、如何使用。我们在拥抱人工智能技术进步的同时,要时刻提防技术的“另一面”,正如AI在医疗领域能拯救生命,但利用AI拨打骚扰电话却令人厌烦。技术创新固然重要,但更要记得,不要让技术影响人们享受生活的安宁。(检察日报)

## 以案说法

## 行业“内鬼”明码标价出售三十万条业主信息



图为民警在装修公司查获的被出售的业主信息。

一个接一个,他不分时候,不分你是在工作的时候,还是在休息的时候,他一直给你打电话,非常讨厌!”张先生怀疑自己的个人信息遭到了泄露,赶紧到曹县公安局磐石派出所报了警。

## 装修公司花钱购买业主信息

接警后,办案民警立即展开调查。“我们根据报警人张先生提供的电话号码单分析,发现有一个手机号,每天有大量向外拨打电话的记录。经过查询该号码基础信息,为一家装修公司所持有。”曹县公安局网安大队民警赵鹏介绍说。

根据这一线索,民警立刻对这家装修公司展开调查。通过走访摸排,办案民警很快发现了端倪。“我们在这家装修公司,现场查获了1.2万条曹县本地小区业主个人信息,而这些信息都密密麻麻地打印在A4纸上,上面有业主的姓名、手机号、楼房号以及户型面积,还有一部分有业主的身份证号以及银行贷款按揭等信息。”曹县公安局磐石派出所副所长陈恒说。

装修公司是怎么得到业主个人信息的呢?民警立刻对公司的负责人刘某展开审讯。据刘某交代,自己装修公司的生意不景气,于是就有了购买业主信息招揽生意的想法。他在另一家装修公司的介绍下,以1万多元的价格购买了一些业主个人信息。

购买信息后,刘某特意雇了一批业务员,每天不停地给名单上的业主拨打电话。每打一个电话,他们都会备注业主是否有意愿装修。如果有意向,他们就会持续跟进,不停打电话推销。对于没有意愿装修的业主,他们就把这些业主信息以较低的价格卖给别人。

## 以0.5元到10元一条价格出售信息

了解情况后,办案民警立刻对刘某的家属展开调查,并很快将专门在曹县倒卖小区业主个人信息的李某及其上线郭某抓获。在郭某手机里,民警查出大量已经分类整理好的个人信息。

据郭某交代,他出售给下家的业主信息,都是从曹县部分售楼处的售楼员手中购买。而像李某这样的下家,在从郭某手里购买到业主信息后,便会将信息全部出售给装修、家电、家具公司等行业。

通过大量调查,办案民警确定出售公民个人信息的为曹县多家小区的售楼部,而出售人为这些售楼部里的“内鬼”。他们利用职务便利,将平时

在工作中登记收集的客户信息整理后出售获利。他们还从公司电脑中窃取小区业主个人信息私自出售给别人。“每条大致在0.5元到10元不等,老小区由于业主的装修意愿不大,因此价格相对比较便宜,而那些新的小区 and 即将交房的小区、别墅区的业主信息,就比较贵一点。”赵鹏说。

经初步统计,本案涉案人员多达60余人,涉案总金额20多万元。“我们还要继续扩大战果,争取将整个黑灰产业链彻底打掉。同时,为了更有力度地打击犯罪,我们还将对此案进行通报,要求辖区内的房地产、装修、物业等相关行业从业者进行自查自纠。”曹县公安局网安大队大队长石更峰介绍说。

目前,案件正在进一步深挖调查中。(法治日报)

## 警方提醒:

出售公民个人信息是违法犯罪行为,相关企业要完善内部管理制度,加强数据信息防护及内部人员网络安全和法治教育,杜绝公民个人信息泄露。广大群众要增强安全防范意识,保护好个人信息。一旦发现相关违法犯罪行为应及时报警,依法依规维护自己的合法权益。

## 北京市丰台区市场监管局之窗

北京市丰台区市场监管局开展“守护儿童安全 远离产品伤害”暨质量安全进校园活动

近日,北京市丰台区市场监管局在北京市丰台区第三小学举办“守护儿童安全 远离产品伤害”暨质量安全进校园宣传活动,倡导社会各界关注儿童玩具和学生用品安全隐患,营造守护儿童和学生健康成长的消费环境。工作人员通过生动有趣的PPT讲解、播放缺陷产品召回动画、选购现场情景模拟、知识问答互动和发放宣传手册等环节,向广大师生全方位讲授儿童玩具、学生文具、童鞋童鞋、儿童化妆品等产品选购和缺陷召回相关知识。提示学生在选购儿童玩具、文具产品时,一定要注意查看产品标签是否标注“CCC”强制性产品认证标志,是否有厂名、厂址、警示说明、年龄限制等内容,是否有中文说明、产品质量合格

(刘 静)