

谁在出卖你的隐私

——最高法亮剑惩治侵犯个人信息犯罪

延伸阅读

侵犯个人信息 最高可判七年

最高法公布的侵犯公民个人信息犯罪典型案例中,有一起为五人通过微信朋友圈,发布出售个人户籍、车辆档案、手机定位、个人征信、旅馆住宿等各类公民个人信息的广告,寻找客户并获利,最终被判刑。

实践中对于“公民个人信息”的范围尚存争议,这次发布的司法解释予以明确规定:刑法相关规定中的“公民个人信息”,是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息,包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

最高人民法院研究室主任颜茂昆表示,这样的规定是基于全面保护公民个人信息的现实需要。“对于例举以外的个人信息,当然还有很多,司法实践中要根据司法解释规定,把握‘公民个人信息’的要件特征,准确作出判断。”他说。

刑法规定,违反国家有关规定,向他人出售或者提供公民个人信息,情节严重的,处三年以下有期徒刑或者拘役,并处或者单处罚金;情节特别严重的,处三年以上七年以下有期徒刑,并处罚金。

对此,司法解释进一步明确规定,向特定人提供公民个人信息,以及通过信息网络或者其他途径发布公民个人信息的,应当认定为刑法规定的“提供公民个人信息”。未经被收集者同意,将合法收集的公民个人信息向他人提供的,也属于“提供公民个人信息”,但是经过处理无法识别特定个人且不能复原的除外。

根据刑法规定,侵犯公民个人信息罪的人罪要件为“情节严重”。对于这里的“情节严重”,本次出台的司法解释明确了违法所得5000元以上等十项认定标准。

值得注意的是,根据不同类型公民个人信息的重要程度,司法解释设置了不同的数量标准。对于行踪轨迹信息、通信内容、征信信息、财产信息,非法获取、出售或者提供50条以上即算“情节严重”;对于住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息,标准则是500条以上;对于其他公民个人信息,标准为5000条以上。

“定罪量刑标准的确立有利于法律的统一、准确实施,对严厉打击侵犯公民个人信息犯罪提供了有力的法律武器。”最高人民检察院法律政策研究室副主任缪杰说,办案部门对于涉案的公民个人信息,首先应当分类进行分析,如果每一个类型相对应的公民个人信息都没有达到50条、500条、5000条的,司法解释规定还要对其按照相应比例进行合计。

缪杰举例说,某个案件涉及公民轨迹信息等敏感信息20条,住宿信息等重要信息350条,就要按照1和10倍比关系进行折算。350条重要信息折算成35条敏感信息,两项合计55条,就要追究刑事责任。

据央视网



刚拔完牙就频繁收到种植牙电话推销,乘车信息被无关第三人知晓,正规预约网站却被骗子“钓鱼”……生活中,像这样令人尴尬又后怕的场景你遇到过吗?

随着数字经济的发展,很多个人信息在指尖轻轻一点就完成收集,但信息泄露问题也随之而来。最高人民法院5月8日发布5起侵犯公民个人信息犯罪及关联犯罪的典型案例,严惩行业“内鬼”和个人信息关联犯罪,切实筑牢清朗网络空间法治防线。

源头斩断“内鬼”链条

信息技术收集者肩负着源头守护信息安全的责任。然而,有人监守自盗,甘当行业“内鬼”。

在最高法披露的一起案例中,博某软件有限公司就在为医院开发、维护网上挂号系统时动了歪心思。

2015年至2020年间,博某软件有限公司法定代表人何某暗中收集从后台非法获取的某医院挂号用户个人信息,并安排公司员工熊某等将信息数据导入公司自建数据库。2021年初,熊某又安排人员在为该院开发的软件上安装接口,自动将挂号信息导入该公司自建数据库。

就这样,287万余条个人信息无声无息地被非法泄露。

经审理,法院对博某软件有限公司以侵犯公民个人信息罪,判处有期徒刑三十万元;对何某等人以侵犯公民个人信息罪,判处有期徒刑五年六个月至一年六个月不等,并处相应罚金。

除了挂号信息,公民的乘车时间、车次等,也成为了一些“内鬼”眼里的“生意”。铁路车站客运员陈某2019年1月通过铁路车票系统查询他人搭乘高铁的具体信息,并以每条10元至60元不等的价格出售牟利。未在岗期间,陈某以每条5元至10元不等的查询费,通

过同事曾某等人代为查询相关信息。

这其中,不少数据被出售给林某等人用于有偿查询演艺人员等的行程信息。截至2021年9月,陈某违法所得共计约19万元。

出行计划、生活规律、社交关系等个人隐私被泄露,无论是普通人还是公众人物,都可能面临生活安宁被破坏,甚至人身、财产安全遭到威胁的后果。

法官提醒,负有接触、收集、处理个人身份信息职责的从业人员,应严格履行保障个人信息安全及防止外泄的义务,如泄露个人信息构成犯罪的,将承担相应的刑事责任。

筑牢政企单位数据安全防线

近年来,一些政企单位内部数据信息及其在提供互联网服务过程中收集的个人数据,同样面临被窃取贩卖的风险。

一起案例中,不法分子通过租用手机号接收验证码、伪造身份证图片及动态验证视频等技术手段,绕过“学信网”实名认证系统,非法获取学历信息后出售,形成“租用设备—注册账号—虚假验证—下载信息—贩卖获利”的黑灰产业链。

2021年8月以来,黄某通过“中间

人”刘某,接受查询他人学历信息的委托,由同伙李某伪造身份证图片,同伙高某租用手机号,接收短信验证码,然后再通过技术手段,骗过动态视频认证,登入“学信网”下载学历证书电子注册备案表,并出售牟利。截至案发,黄某等人违法所得分别为30万元至6000元不等。

北京市西城区人民法院以侵犯公民个人信息罪,对黄某等人判处有期徒刑三年八个月至八个月不等,并处相应罚金。对于检察机关提起的附带民事

公益诉讼,判决责令黄某等人公开赔礼道歉,删除非法持有的公民个人信息,注销侵权使用的通信软件,支付公益损害赔偿金。

“此类犯罪所获取的信息往往会被用于伪造学历、骗取就业资格或特殊行业资质等,严重破坏社会诚信体系及国家人才管理秩序。”案件审理法官表示,这一判例彰显了依法维护政企单位平台信息安全、打击数据犯罪的态度和决心。

严惩个人信息关联犯罪

不法分子挖空心思获得公民个人信息,往往是为了信息背后潜在的经济利益。最高法分析数起案件发现,公民个人信息被收集后,常被用于电信网络诈骗、敲诈勒索等关联犯罪,是黑灰产业链的上游环节。

作为预防宫颈癌的重要手段,接种HPV(人乳头瘤病毒)疫苗的市场需求很大。2022年2月至7月间,梁某、王某盯上某预约注射疫苗的正规网站,共同出资在互联网黑灰产业平台购买木马程序并向该网站植入,进而获取网

站存储的HPV疫苗预约订单信息29万余条。

拿到这些信息后,梁、王二人又费尽心机地制作仿冒的钓鱼网站,并纠集多人分工协作,群发疫苗“预约成功”的短信,诱使预约人员点击短信中的钓鱼网站链接,冒充网站医生、客服,对疫苗预约者实施精准诈骗。最终,51名被害人损失58万余元。

法院审理认为,被告人梁某、王某的行为均已构成侵犯公民个人信息罪、诈骗罪,分别决定对梁某、王某执

行有期徒刑十二年、十一年九个月,并处罚金。

“强化打击利用个人信息实施的下游关联犯罪,让窃取、交易个人信息的上游犯罪无利可图,有利于遏制黑灰产业链条的蔓延。”案件审理法官说。

个人信息绝非“敛财筹码”,隐私泄露往往牵扯利益黑手。相关行业主体须严格履行保障个人信息安全的责任。最高法此番亮剑,意在全链条打击涉个人信息犯罪,释放“谁卖隐私就严惩谁”的强烈信号。

据新华社