

非法获取个人信息的处理规则*

文/赵 阳 梁依宁

【裁判要旨】手机MAC地址系设备识别编码，与其他信息相结合，即可精准获取手机号码，进而锁定特定自然人，故手机MAC地址属于个人信息。在手机实名制背景下，手机号码与个人身份证、金融账户等深度绑定，直接关涉信息主体财产安全，故手机号码属于敏感个人信息。案涉交易双方非法获取用户手机号码，基于违法行为所订立的分销协议，依法应认定为无效。

□案号 一审：(2019)津0114民初10664号 二审：(2020)津01民终3291号

【案情】

原告：成都某实业公司。

被告：天津某科技公司。

2017年以来，天津某科技公司与成都某实业公司就代理分销“招财宝”产品，签订了分销协议及补充协议，约定天津某科技公司授权成都某实业公司销售该产品，若合作期内该产品与国家法律法规冲突导致不能销售，则天津某科技公司应当按照双方约定价格回购未售出商品并全额退还保证金。协议签订后，成都某实业公司依约支付了货款及履约保证金。

2018年，经双方协商，天津某科技公司向成都某实业公司退还了部分货款及保证金，尚有276套“招财

宝”产品的货款325680元及保证金5万元未予退还。经查，“招财宝”产品系软件系统，内置于“招财喵”硬件产品中。2019年，中央电视台“3·15”晚会针对“招财喵”等探针盒子获取用户信息的情况进行了报道，称：“‘招财喵’等探针盒子，不仅可以收集用户手机号码，甚至可以对用户进行精准画像。当手机用户寻找无线网络的信号时，探针盒子能迅速识别出手机的MAC地址，通过大数据进行匹配，即可转换出用户的手机号码，实现拨打骚扰电话等功能。”

经央视“3·15”晚会报道案涉产品获取用户手机MAC地址后，成都某实业公司以产品违法已停止销售为由，起诉要求天津某科技公司回购剩余产品并退还保证金。

【审判】

天津市武清区人民法院经审理作出一审判决：驳回原告的诉讼请求。

一审宣判后，成都某实业公司提起上诉。

天津市第一中级人民法院经审理认为：“招财宝”产品可以不经用户同意收集不特定人手机MAC地址信息，MAC地址信息与其他信息结合可以获取手机用户的电话号码，手机MAC地址信息属于个人信息保护范畴。“招财宝”产品收集用户手机MAC地址信息未经过用户同意，非法获取公民个人信息。案涉双方签订的分销协议、补充协议，买卖非法获取不特定人的个人信息产品，违反了网

*入库编号：2023-08-2-084-002。

络安全法强制性规定，构成对社会公共利益的危害，协议应属无效。双方当事人签订合同时，均已意识到产品涉嫌违法，其订立并履行合同的行为系试法行为，任何一方欲通过诉讼得到司法保护的请求均不应得到支持。天津一中院遂作出二审判决：一、维持一审判决；二、上诉人成都某实业公司持有的276套“招财宝”产品予以收缴；三、被上诉人天津某科技公司收取的货款325680元及保证金5万元均予以收缴。

【评析】

一、手机MAC地址应纳入个人信息保护范畴

公民身份证号码、手机号码等信息应纳入个人信息保护范围，在司法实务中已达成共识。但案涉“招财宝”产品所收集的手机MAC地址是否应受个人信息保护规则调整，尚需根据民法典与个人信息保护法对“个人信息”的定义予以确定。

民法典第一千零三十四条规定：

“个人信息是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的各种信息。”个人信息保护法第四条规定：“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。”民法典以“可识别性”作为界定个人信息的辨识标准，该标准亦是区分个人信息与信息流通领域去标识

化、匿名化信息的核心辨识标准。

“可识别性”既包括对个体身份的识别（确定信息主体“是谁”），也包括对个体特征的识别（确定信息主体“是什么样的人”）。“可识别性”分为“单独识别”与“结合识别”，“单独识别”指仅凭单一信息内容，即可直接锁定特定自然人，公民身份证号码、手机号码等即属此类。需注意的是，直接锁定特定自然人并不要求必须知道特定自然人的姓名。“结合识别”指单凭某一信息无法锁定特定自然人，与其他信息结合后，才能锁定特定自然人。

相较于民法典，个人信息保护法增加了“关联性”作为个人信息的识别标准。若信息满足以下要件之一，即可认定存在“关联性”：信息内容本身描述特定个体的情况、数据可能用于评估他人、数据使用可能影响特定自然人。^①但究其本质，个人信息核心辨识标准仍为“可识别性”，“关联性”标准依附于“可识别性”标准，脱离“可识别性”的“关联性”将丧失独立的规范意义。

本案中，案涉产品收集用户的手机号码，单凭手机号码足以锁定特定自然人，完全契合个人信息“可识别性”标准，且民法典第一千零三十四条明确将手机号码列为个人信息的典型范例，手机号码属于个人信息保护范畴。案涉探针盒子能迅速识别手机MAC地址，MAC地址作为设备序列编码，无法直接锁定特定自然人，但通过大数据匹

配，可转换识别用户手机号码，通过结合识别锁定特定用户。此情形下，MAC地址已从单纯的设备序列编码，转化为锚定自然人身份的索引标识，从而满足“可识别性”要件。同时，以“关联性”要件审视之，运营主体收集手机MAC地址，旨在获取手机号码以精准推送营销广告，该行为必然侵扰用户生活安宁，符合“数据使用影响自然人”的关联性特征。综上，手机MAC地址属于个人信息。

二、手机号码属于敏感个人信息，但不属于私密信息

民法典第一千零三十四条第三款规定：“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定”。私密信息应优先适用隐私权保护规则，同时以个人信息保护规则作为兜底。探求其立法本旨，私密信息以维护人格尊严为核心，具有绝对权属性；而个人信息权益兼具人格与财产属性，允许在权利人同意或符合公共利益等情形下合理利用。相较于个人信息，私密信息法益位阶更高，立法对私密信息的利用设置了更严格的保护规则。

私密信息的核心特征为私密性，强调权利人主观上不愿私密信息被公开披露的主观意愿，借此维持私密信息不为人知的状态，个人身体隐私、财产隐私、生理信息等均属此类。为防止私密信息被公开，私密信息应优先适用隐私权规则。由此，甄别手机MAC地址与手机号码是否属于私密信

^①商希雪：“数字行为痕迹的法律定位与权益保障研究——全面应对DeepSeek等AI平台的个人信息保护挑战”，载《暨南学报（哲学社会科学版）》2025年第2期。

案例

息,关涉是否应优先适用隐私权规范的前置问题。

手机MAC地址在Wi-Fi连接场景中自动对外传播,不具备隐秘性,不应优先适用隐私权规则。同理,手机号码设立初衷在于社交联络,手机号码持有人通常具有对外披露的预期,手机号码一经公开即丧失私密性,缺乏“不愿为他人知晓”的主观要件;并且,单独的手机号码仅能实现基础身份关联,不足以直接窥探个人隐私。除非手机号码与实时行踪轨迹结合,才具备高度私密性与敏感性,此时才应纳入隐私权保护范畴。由此,单独的手机号码不属于私密信息,不应优先援引隐私权制度加以保护。

民法典将个人信息分为私密信息与非私密信息,但个人信息保护法采取了不同分类路径。个人信息保护法第二十八条第一款规定:“敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”,个人信息可分为敏感个人信息与非敏感个人信息。民法典规定的私密信息侧重于信息主体主观上“不愿为他人知晓”的心理状态,而个人信息保护法规定的敏感个人信息,则关注信息被泄露所产生的风险后果,“容易受侵害”系判断敏感个人信息的核心标准。例如,家庭住址信息泄露可能招致上门滋扰、人身伤害,而财产状况被非法曝光,则可能引发针对权利人的暴力犯罪或诈骗犯罪,手

机号码、财产状况属于敏感个人信息。需注意的是,个人信息被单独识别的概率越高,则该信息具有更高的敏感性。^①

遵此逻辑检视,案涉手机MAC地址系移动终端的物理设备标识,其被泄露不会直接引发自然人人身、财产等权益受损,不符合敏感个人信息“容易受到侵害”的判断标准;手机MAC地址仅能反映硬件设备的使用情况,需结合其他数据方能锁定特定自然人,缺乏敏感个人信息“单独识别性”特征,手机MAC地址不应纳入敏感个人信息的保护范畴。

相较而言,手机号码与个人银行账户、金融账户等深度绑定,系自然人身份验证、财产交易的重要识别载体,手机号码已经成为身份验证与财产交易的“数字钥匙”,与个人主体的财产安全直接相关。一旦被泄露,极易引发电信诈骗、敲诈勒索等风险,完全契合敏感个人信息“容易受到侵害”的认定标准。同时,单凭手机号码可直接锁定特定自然人,符合敏感个人信息的“单独识别性”特征,手机号码应纳入敏感个人信息保护范畴。

三、敏感个人信息的处理规则

关于私密信息的处理规则,民法典第一千零三十三条规定,法律另有规定或者权利人明确同意,才能处理个人私密信息。其法理基础在于,私密信息承载着人格权利,侧重保护信息主体不愿他人知晓的主观意愿。而

对于敏感个人信息的处理规则,个人信息保护法第二十九条规定:“处理敏感个人信息应当取得个人的单独同意”。单独同意指采取黑体、标红等显著方式提示信息主体,确保其能够有效阅读相关条款,不得采取概括的、一揽子同意方式,杜绝格式条款下的无效同意问题,不得强迫用户勾选“同意”,应设置“跳过”“拒绝”等勾选方式,确保用户作出有效的意思表示。

除前述单独同意要件之外,个人信息保护法第二十八条第二款规定:

“只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下,个人信息处理者方可处理敏感个人信息”。在满足“具有特定目的”“充分必要性”和“采取严格保护措施”三要件时,信息处理者可处理利用敏感个人信息。

第一,就“特定目的”要件而言,该要件包括目的具体明确与目的正当两层规范。“目的具体明确”旨在控制敏感信息的泛化,明确排斥笼统、模糊的用途表述,要求信息处理者确定清晰的数据使用场景。以采集生物基因信息为例,不得宣称为了信息主体健康的宽泛目的采集信息,须将目的界定为例如筛选癌症指标的可操作范畴。处理敏感个人信息时,目的不得与法定合理使用目的相违背。^②质言之,敏感个人信息承载着信息主体人格利益,唯有为保护更高位阶法益时,方可在必要限度内限制敏感个人信息权益。

^①丁晓东:“敏感个人信息保护制度的解释性重构”,载《中国法学》2025年第2期。

^②李世刚、屈然:“论敏感个人信息的合理使用”,载《江苏社会科学》2022年第6期。

第二,关于“充分必要性原则”要件,个人信息保护法第六条第一款规定,处理个人信息应当与处理目的直接相关,并采取对个人权益影响最小的方式。“充分必要性”强调手段与目的相匹配,处置敏感个人信息应当保持最大的克制。^①“充分性”要求信息处理行为与处理目的相匹配。

“必要性”则要求筛选对个人权益损害最小的实现路径,唯有穷尽其他方式仍无法达成目的时,才能以处理敏感个人信息的方式达到目的。立法层面设置该层审查标准,旨在防止信息处理者无节制地归集、处置敏感个人信息。

第三,关于“采取严格保护措施”要件,该要件是敏感个人信息保护的最后一道防线。根据个人信息保护法第五十一条,信息处理者应当依据个人信息的处理目的、处理方式、个人信息的种类以及可能存在的安全风险等因素,采取防止个人信息泄露、篡改、丢失相关保护措施。例如,采取加密、去标识化技术保护措施,经由该技术改造后的信息,自然人身份的可识别性会大幅削弱,即使数据被泄露,在无其他配套数据印证的前提下,无法识别特定自然人,阻断了敏感个人信息被不当利用的可能性。可见,该要件旨在通过技术性手段事先防范,而非依赖事后救济的方式消除个人信息泄露隐患。

综上,敏感个人信息的合法处

理,以信息主体单独同意为前提,同时须满足特定目的、充分必要性、严格保护措施三项法定要件。然而,反观案涉“招财喵”探针盒子的信息处理行为,其未能达成各项法定审查标准:“招财喵”探针盒子未以任何显著方式提示信息主体,信息主体丧失了作出单独同意意思表示的可能性;

“招财喵”探针盒子收集电话号码系为了商业营销,并非基于增进社会公共福祉或保护生命健康目的,与个人信息保护法界定的“特定目的”明显相悖;案涉产品获取手机号码的手段亦不具备合法性,未能通过信息主体点击“同意注册”的方式,或邀请信息主体自主填报手机号码,却暗中获取手机号码,完全不符合“充分必要性”要求;“招财喵”探针盒子未采取去标识化措施消除身份识别要素,在技术层面未能保障个人信息安全,与“采取严格保护措施”之要求存在明显差距。综上,“招财喵”探针盒子处理敏感个人信息系违法行为。

四、违法处理个人信息的法律后果

个人信息保护法第十条规定:“任何组织、个人不得非法收集、使用、加工、传输他人个人信息。”同时,民法典第一百五十三条规定,违反法律、违背公序良俗的行为无效。案涉“招财喵”探针盒子为商业营销目的拨打骚扰电话,侵扰社会公众生活安宁,该合同的订立、履行系以侵

扰他人生活安宁为代价换取商业利益,与公序良俗显相违背,合同赖以成立、履行的核心目的欠缺正当性,合同效力应遭到法律的否定评价。^②

为了兼顾个人信息权益保护与数据流通需求,现行立法允许对匿名化信息进行商业化利用,匿名化信息无法识别、关联特定自然人,无法描绘用户画像,可以进行开发利用。^③反之,若数据能够识别特定自然人,在未满足法定条件之前,数据交易各方不得用于商业开发。案涉“招财喵”探针盒子非法收集用户手机号码,手机号码属于禁止交易的敏感个人信息,案涉产品分销协议及补充协议均应当被认定为无效。

案涉信息交易行为发生于2017年至2018年期间,案涉交易行为无效的法律后果,应适用当时仍有效的合同法规定。合同法第五十九条规定:

“当事人恶意串通,损害国家、集体或者第三人利益的,因此取得的财产收归国家所有或者返还集体、第三人。”案涉分销协议约定“若因政府限制使用等政策原因导致合同不能继续,以及法律和司法问题不能正常在市场销售”,足以印证双方在缔约时已预见案涉产品涉嫌违法,主观上均具有可归责性,应认定双方构成恶意串通;“招财喵”探针盒子擅自收集、拨打用户手机号码,该行为骚扰不特定公民生活安宁,使得社会公众对正常的交往、(下转第102页)

①杨尚东:“论大数据时代政府信息公开中的敏感个人信息保护”,载《行政法学研究》2025年第4期。

②林涸民:“个人数据交易的双重法律构造”,载《法学研究》2022年第5期。

③武腾:“最小必要原则在平台处理个人信息实践中的适用”,载《法学研究》2021年第6期。

(上接第058页)交易等产生不信任感,影响国家治理,损害社会公共利益,在司法层面应作出否定性评价,对交易双方施以法律制裁。

秉持合同法本意,追缴当事人所取得的违法财产,此乃基于公法管制立场对不法行为人施制裁,借此抑制此类交易的发生,达到一般预防之效果。若财产给付人享有请求受领人返还财物的权利,则无法威慑、惩罚财产给付人。基于本案事实与原合同法规定,法院最终作出裁判,收缴案涉货款、保证金及违法产品。

然须辨明者,依现行法律法规审视,“收缴”之法律定性本质上属行政责任范畴,人民法院收缴财产系代为行使行政处罚权。依据行政处罚法,只有行政机关、被授权组织有权进行“收

缴”,基于处罚法定原则之拘束,现阶段人民法院并不具备作出“收缴”行政处罚的权限。相反,观诸民法典第一百五十七条之规定,民事法律行为无效的后果为返还财产、折价补偿及过错赔偿等私法救济路径,并不包括“收缴”这一公法制裁手段。“收缴”系以国家公权力强制介入私权领域,将其置于民法体系中确有不当,民法典编纂之际遂删除了合同法第五十九条关于“收缴”的规定。私法层面废止“收缴”规则,并不代表立法放弃对不法交易利益的惩戒。

个人信息保护法第六十六条规定,交易主体未依法履行个人信息保护义务的,由监管部门责令整改、没收违法所得。依托公私法衔接机制,民事审判庭可向有关行政管理部门提出司法建

议,从而依法启动行政处罚程序。若行为涉嫌构成刑事犯罪,民事审判庭亦可将犯罪线索移交刑事侦查机关,藉此激活公法制裁功能。

循此公私法衔接处置思路,将没收违法所得的公法制裁功能交由行政、刑事法律规范,更有助于彰显非法处置个人信息行为对社会公共利益的危害。同时,本案于2020年12月作出生效判决,民法典于次年1月1日生效,该案判决收缴违法所得,系依据当时有效法律规范予以裁判。进言之,该案收缴货款、保证金等违法所得的裁判结果,从规范目的角度审视,与个人信息权益保护的立法旨趣高度契合。

(作者单位:天津市武清区人民法院)