doi:10.13582/j.cnki.1672-7835.2023.01.014

论个人信息中可识别要素的判断标准

刘宗胜,张毅
(湘潭大学 信用风险管理学院,湖南 湘潭 411105)

摘　要:个人信息与隐私信息的界限由混同走向清晰,其定义模式也从“识别说”发展到“关联说”。判断信息的可识别性有三项标准:在识别主体上,应采“主观说”,以实现个人信息保护与侵权责任构成要件的衔接;在识别对象上,需将“识别”限缩解释为“身份识别”,且完成身份识别至少需要两个以上的标识符,并至少包含一个社会意义上的标识符;在识别方式上,直接识别方式的存在与否有待商榷,以人格利益的关联性作为间接识别中个人信息的判断标准,可避免个人信息的外延失之过泛。

关键词:个人信息;身份识别;行为识别;直接识别;间接识别
中图分类号:D923.8　　**文献标志码**:A　　**文章编号**:1672-7835(2023)01-0100-09

一　问题的提出

在我国司法实践中,不同法院对于个人信息的认定存在不同的观点,导致在“类案”中对同种信息的裁判结果出现分歧。在“郭长城诉北京指云无线科技有限公司个人信息保护纠纷案”中,被告在未经原告同意的情况下,多次发送金融商业短信至原告的手机号码,原告据此主张自己的“生活受到侵扰,个人信息保护受到侵害”。北京市海淀区法院认为,被告系发送手机短信服务的提供者,但手机号和短信内容为短信发送公司所掌握,且仅有手机号无法识别手机号使用人的个人身份信息,因此被告不存在实施侵犯原告个人信息的行为①。但在“凌文君诉北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案”中,被告通过原告注册软件时使用的手机号码,对原告的社交信息、社会关系进行分析,原告据此主张被告“构成对原告个人信息的侵害”。北京互联网法院认为,姓名是自然人作为社会个体与他人进行区别,在社会生活中具备可识别性的称谓或符号。手机号码是电话管理部门为手机设定的号码,随着“手机实名制”政策的推行和普及,手机号码与特定自然人的关联性愈加紧密。因此,自然人的姓名与其使用的手机号码无论单独抑或组合均具有可识别性,属于个人信息②。

通过以上两个案例可以看出,对于“手机号码是否属于个人信息”这一问题,不同法院的认定标准并不一致,这有损司法裁判的统一性和权威性。为了解决上述问题,需要对个人信息的概念和认定标准作出清晰的界定,具体而言,需要回答如下两个问题:第一,什么是个人信息?第二,判断某个信息是否具有可识别性的标准是什么?

二　个人信息含义之变迁

通过梳理现行有效的规范性文件可知,个人信息的含义围绕着两条“明线”展开。一是关于个人信息与隐私信息的关系;二是个人信息定义的两种模式。

(一)个人信息与隐私信息“从融合到分立”

在个人信息与隐私信息的关系上,我国现行规范性文件的观点经历了“从融合到分立”的过程。

收稿日期:2022-08-25
作者简介:刘宗胜(1973—),男,苗族,湖南怀化人,博士,教授,主要从事民商法学、信用法学研究。
①郭长城诉北京指云无线科技有限公司个人信息保护纠纷案,北京市海淀区人民法院民事判决书,(2021)京 0108 民初 25670 号。
②凌文君诉北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案,北京互联网法院民事判决书,(2019)京 0491 民初 6694 号。

早期不少文件把隐私信息作为个人信息的一部分加以保护。2012 年《关于加强网络信息保护的决定》规定："一、国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。"其中"公民个人电子信息"包括了识别公民身份的信息和涉及公民隐私的信息两种类型，表明个人信息除有识别性特征外，还包括隐私信息。2013 年《关于依法惩处侵害公民个人信息犯罪活动的通知》延续了《关于加强网络信息保护的决定》的规范路径，规定公民的个人信息是指"能够识别公民个人身份或者涉及公民个人隐私的信息、数据资料"。2016 年的《网络安全法》首次从法律的角度把隐私信息排除在个人信息之外，明确了个人信息与隐私信息相比独有的特点——识别性①。2020 年的《民法典》将"隐私权和个人信息保护"作为章标题，并把隐私权保护与个人信息保护分列为两个部分进行规定，凸显了隐私信息与个人信息存在明确的边界，两者适用不同的保护模式：对隐私信息的保护属于隐私权的内容，除隐私信息外，隐私权同时保护自然人的私密空间和私密活动；对个人信息的保护则更多强调个人信息处理者的义务与信息主体基于个人信息权益的派生权利。此外，《民法典》第一千零三十四条第三款进一步回答了隐私信息与个人信息的关系，厘清了隐私信息与个人信息重合部分的保护规则②。

（二）个人信息定义从"识别说"到"关联说"

在个人信息的定义模式上，我国现行规范性文件的观点始终围绕着"识别说"和"关联说"两种模式展开。

"识别说"是指通过信息定位到个人，即"由信息本身的特殊性直接回溯到特定个人"；"关联说"是指从个人到信息，即"已知晓既定个人，进一步知晓'关于'该个人的其他信息"③。"识别说"的典型例证为《网络安全法》第十七条第（五）项和《民法典》第一千零三十四条第二款④的规定。"关联说"的规范表现包括 2012 年《规范互联网信息服务市场秩序若干规定》第十一条第一款中规定的"与用户相关的信息"、2013 年《电信和互联网用户个人信息保护规定》第四条中的"用户使用服务的时间、地点等信息"、2017 年《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》第一条和 2020 年《信息安全技术个人信息安全规范》（GB/T 35273—2020）（以下简称《个人信息安全规范》）规定的"反映特定自然人活动情况的信息"，这些规范虽然表述不同，但均指向与自然人相关的信息，系"关联说"的不同表达方式。至于《个人信息保护法》（以下简称《个保法》）采用的定义模式则存在分歧，有观点认为《个保法》采取了"关联说"⑤，也有观点认为采取了"识别说+关联说"⑥。本文认为，从条文表述来看，《个保法》第四条第一款规定："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，不包括匿名化处理后的信息。"因此可以认为，《个保法》采取了"关联说"的定义模式，但这并不意味着"识别说"被排斥在外，相反，"识别说"在解释"关联说"的定义中发挥了重要作用。"关联说"认为，个人信息是与已识别或可识别的自然人有关的各种信息，但对什么是"已识别的自然人"和"可识别的自然人"并没有给出明确回答。信息只有具备"可识别性"，才能把该信息与"已识别"和"可识别"的自然人"关联"起来，因此"识别说"依然存在发挥作用的空间，通过解释"已识别的自然人"和"可识别的自然人"，可以使"关联说"语境下个人信息的内涵更加明确。

综上所述，个人信息的内涵由最初兼顾个体关联性和内容私密性，发展为如今强调内容的"识别性"与"关联性"，并与隐私信息区分开来，《民法典》第一千零三十四条第三款的内容即为

①《网络安全法》第七十六条第（五）项规定："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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。"

②《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。"

③张新宝：《中华人民共和国个人信息保护法》，人民出版社 2021 年版，第 41 页。

④《民法典》第一千零三十四条第二款规定："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，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。"

⑤龙卫球：《中华人民共和国个人信息保护法》，中国法制出版社 2021 年版，第 16 页。

⑥张新宝：《中华人民共和国个人信息保护法》，人民出版社 2021 年版，第 42 页。

明证。根据《民法典》第一千零三十四条第三款的规定,若某自然人的日常生活受到了群发营销短信的影响,其应当根据《民法典》第一千零三十二条和第一千零三十三条第(一)项的规定寻求隐私权的救济,而非主张个人信息的保护路径。在区分隐私信息与个人信息的基础上,通过结合"关联说"对个人信息的含义进行解读,可将个人信息分为"与已识别的自然人有关的信息"和"与可识别的自然人有关的信息"。其中,"已识别的自然人"是指身份已经明确了的自然人,与此相对应的是,"与已识别的自然人有关的信息"则是指与身份既定的自然人具备关联性的各种信息,是从个人到信息的寻觅过程。"已识别"是"可识别"后的结果,而认定"与可识别的自然人有关的信息"的难点,在于什么是"可识别的自然人",换言之,判断某个信息是否具有可识别性的标准是什么?

三　个人信息中可识别要素的判断标准

通过信息定位到自然人的过程为:某识别主体通过某种方式识别到信息背后的自然人。通过分解前述识别过程,可以看到判断某个信息是否具有可识别性,可以从识别主体、识别对象和识别方式三个方面入手。

(一)主体标准:谁来识别

在信息识别的过程中,识别主体是一个不可忽略的要素。从我国已有的规范内容来看,并不存在对于识别主体的明确规定。但学界对于个人信息识别主体的讨论早已有之。

1.现有学术观点

对于个人信息在主体方面的识别,有学者将现有观点总结为"主观说""客观说"和"任一主体说"三种类型①。

"主观说"认为个人信息的识别性应以个人信息处理者自身的信息识别能力为判断标准。持此观点的学者认为个人信息的识别性要素具有"相对性"的特点,即对于被加密后的,或去标识化后的信息来说,社会公众一般无法通过此类信息识别特定的信息主体,但当个人信息处理者拥有破解密码等能力时,此类信息则具有可识别性。同时,个人信息保护相关法律规范的对象为个人信息处理者,而个人信息处理者之间和普通民众之间的技术能力差别巨大,因此采取"主观说"能够更加周全地保护个人信息②。"客观说"又称为"社会一般多数人说",即以社会一般多数人的识别能力作为判断信息可识别性的标准。该观点的理由在于,识别是不特定第三人对信息与自然人之间存在的联系因素的辨认过程,为避免发生纠纷时法官对信息的识别性进行二次判断,保证识别的客观性和合理性,应当从普通大众、社会一般人的角度出发判定某个信息是否能指向具体的自然人③。"任一主体说"认为,识别的主体应当是使用数据的任何人。持有该种观点的学者认为,个人信息处理者之外的人或者组织未经授权非法获取这些个人信息的情况并不少见,如果把这些人排除在识别机构之外,将不能全面保护信息主体的权益④。

2.对现有观点的评价

"主观说"主张根据个人信息处理者的识别能力确定信息的可识别性,在理论上具有正当性。根据《民法典》对于侵权责任构成要件的规定,除法律另有规定外,只有行为人在主观上具有过错时,才可能承担侵权责任。若行为人无法根据某信息识别特定主体,则其在处理该信息的过程中不具备过错,也无法构成侵权行为,因此不必承担侵权责任。同样,个人信息处理者也没有理由因他人的识别能力来确定自己是否要承担《个保法》中个人信息处理者处理个人信息时的义务。

"客观说"认为信息识别性的判断不会受到个人信息处理者识别能力差异的影响。依此观点,信息的识别性由"社会一般多数人"的识别能力决定。但识别能力有通常识别能力和特殊识别

①韩旭至:《个人信息概念的法教义学分析——以〈网络安全法〉第76条第5款为中心》,《重庆大学学报(社会科学版)》2018年第2期。

②范姜真媺:《他律与自律共构之个人资料保护法制——以日本有关民间法制为主》,《东吴法律学报》2009年第1期。

③杨咏婕:《个人信息的私法保护研究》,吉林大学博士学位论文,2013年。

④齐爱民:《拯救信息社会中的人格:个人信息保护法总论》,北京大学出版社2009年版,第86页。

能力之分①，用“社会一般多数人”对信息的通常识别能力掩盖个人信息处理者特殊的信息识别能力，会导致部分具有识别性的信息被排除在个人信息范围之外。例如就手机号码而言，只具有通常识别能力的“社会一般多数人”无法根据手机号码这一信息追溯到持有该手机号码的具体自然人，但具有特殊识别能力的电信运营商、国家公安、安全部门等主体则能够轻易明确手机号码背后自然人的身份。此外，在涉及互联网信息的判断情景时，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者借助自身的信息汇集数量和识别分析技术，往往具备“社会一般多数人”所不具有的特殊识别能力，此时采用“客观说”反而减免了此类个人信息处理者的信息保护义务，与《个保法》第五十八条的规定相悖②。

“任一主体说”主张社会上任何一个主体得以根据某类信息识别信息主体的情况下，此类信息即属于个人信息。从保护信息主体权益的角度来说，“任一主体说”比“主观说”和“客观说”更具优势，会使《个保法》覆盖更大范围的信息内容，但也正因如此，该说存在失之过泛的问题。在“任一主体说”的语境下，社会上的所有主体均是潜在的识别主体，这可能会消弭个人信息与非个人信息的区分价值。因为没有任何一个信息是所有人都不能识别的，反言之，任何一个信息，至少有一个人能识别，如该信息主体的至亲、好友。正是基于“任一主体说”的这一问题，该学说的反对观点认为，大数据技术的进步使得不同主体的信息识别能力与日俱增，以此为判断标准并不稳定③。本文认为，根据“任一主体说”进行推演可以发现，在其他主体能够通过某信息识别特定自然人，但个人信息处理者无法识别时，其仍应当承担个人信息保护义务与处理不当可能导致的侵权责任。但这一结论与侵权责任的构成要件无法衔接。如前所述，这种情况下个人信息处理者对于自己处理的信息并不具备识别能力，也就不存在侵犯个人信息权益的故意，由于缺乏主观上的过错，侵权行为的构成要件不足，因此侵权责任难以成立。

3.本文的结论

本文认为，上述三种观点各有千秋，但从平衡信息主体权益保护和信息利用的立场出发，“主观说”的观点相对更为可取。

首先，从保护信息主体权益方面来看，“主观说”是保证个人信息处理者在处理个人信息的过程中始终负有《个保法》第五章规定的安全保障义务、充分维护信息主体合法权益的前提。《个保法》以“保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用”为立法宗旨，而实现这一立法宗旨的重要途径，便是使个人信息处理者负担其所处理信息的安全保障义务，这同样也是落实《个保法》第四章信息主体在信息处理活动中权利的体现。基于此，《个保法》第五章以九个条文，从内部制度、识别技术、组织架构等多个方面构建个人信息处理者的安全保障义务体系。从第五章的规定来看，个人信息处理者承担安全保障义务均有一个前提，即个人信息处理者对其所处理的信息具备识别能力时，才需要负担《个保法》第五章规定的安全保障义务。例如《个保法》第五十一条第（二）款规定，个人信息处理者应当对个人信息实行分类管理。只有在明确所处理信息的识别性和内容的情况下，个人信息处理者才能确认信息的敏感程度，并进一步对其分类。

其次，从促进数字经济发展和信息流通方面来看，“主观说”能够兼顾不同个人信息处理者在识别能力上的差异。根据“主观说”，识别能力高的个人信息处理者应当负担更多的个人信息安全保障义务；识别能力低的个人信息处理者应当负担相对较少的个人信息安全保障义务。对于大型

①金泓序，何畏：《大数据时代个人信息保护的挑战与对策研究》，《情报科学》2022 年第 6 期。

②《个人信息保护法》第五十八条规定：“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；（四）定期发布个人信息保护社会责任报告，接受社会监督。”

③包文蕾：《个人信息“可识别性”规则的适用困境与破解》，https://mp.weixin.qq.com/s/Or1MyFyuEIPCJBd7veANLw。

互联网企业来说,其在互联网的技术环境和运营环境中占据了控制地位,并具备影响其他个人信息处理者信息处理能力的资源和技术水平,被称为互联网生态中的"守门人"①。相对于一般的个人信息处理者,"守门人"具备更强的信息识别能力,理应承担更重的个人信息安全保障义务,因此《个保法》第五十八条专门针对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者设置了特别义务,这与"主观说"所倡导的观点不谋而合。

最后,从与现行法律规范的衔接方面来看,"主观说"与《民法典》中有关侵权责任构成要件的内容一致。《民法典》承接传统民法理论,以过错责任原则为基本归责原则,如此既能够保障行为人对自身行为后果具有合理预期,同时也能够使因侵权行为受损的权益获得赔偿。根据通说,侵权责任中的过错可以分为故意和过失两种类型,其中故意要求行为人明知其行为会带来的损害后果,并具有实现此种损害后果的意愿,过失则要求行为人能够预见其行为会带来的损害后果,并具备避免此种后果的可能性②。由此可见,无论是故意还是过失,均要求行为人对其行为的损害后果达到了较高的认识程度。在个人信息的保护中,侵权责任的成立同样遵循过错归责原则,而这会推导出在判断个人信息可识别要素的主体标准上应当采取"主观说":只有个人信息处理者对其所处理的信息具备识别能力,明确信息所包含的内容时,才可能在个人信息处理活动中存在侵犯个人信息权益的过错,进而满足成立侵权责任的主观要件。反之,若个人信息处理者无法识别其处理的信息所包含的内容,则其无法辨别哪些属于个人信息,哪些不属于个人信息,难以认定其在侵犯个人信息权益的行为中存在过错。

(二)对象标准:识别什么?

可以看出,"主观说"是以信息识别主体的视角展开的,但从信息本身的角度来说,"可识别"仍然是一个有待进一步澄清含义的法律概念:对于某识别主体来说,其识别的对象是什么?要到何种程度才算完成了"识别"?这就涉及"身份识别"与"行为识别"的选择问题。

1."身份识别"与"行为识别"之争

在识别对象方面,有学者将"识别"进一步细分为"身份识别"和"行为识别"两种类型③。"身份识别"是指明确信息主体真实身份的识别,即"你是谁","行为识别"是指明确信息主体的行为习惯和行为偏好,即"你做过什么"。"行为识别"的支持者认为,在大数据时代,对于信息主体的识别已经实现了从单一的身份识别向个体不同特征识别的转变④。"身份识别"的支持者则认为,"个人信息是指能够单独或者与其他信息结合识别自然人个人身份的各种信息","个人信息"这一概念的核心在于能够通过信息内容明确信息主体的身份,其本质也在于能够单独或结合识别特定个人身份⑤。

2."身份识别"之再提倡

司法实践中对于"身份识别"和"行为识别"的探索早已有之。以"朱烨与北京百度网讯科技公司隐私权纠纷案"⑥为例,二审法院把网络精准广告中使用的cookie技术收集的信息视作"行为识别信息",并将其和"与网络用户个人身份对应以识别特定个体"的"身份识别信息"相区分。实际上,根据cookie技术的工作原理,网络服务提供商会在用户的计算机或移动设备上存储名为cookie的数据文件,这些数据文件包含了标识符和站点名称等内容,便于服务器对用户浏览的网页内容进行分析,进一步推算出用户可能的个性化需求,进而基于这种分析和推算向使用浏览器的不特定主体提供个性化的推荐服务⑦。从这个过程来看,cookie所收集的信息对象为用户的使用行为和使用习惯,与具体的使用者身份无关,不具备定位到特定自然人的识别性特征。除了用户

①张新宝:《互联网生态"守门人"个人信息保护特别义务设置研究》,《比较法研究》2021年第3期。
②程啸:《侵权责任法(第三版)》,法律出版社2021年版,第291—292、295页。
③苏今:《〈民法总则〉中个人信息的"可识别性"特征及其规范路径》,《大连理工大学学报(社会科学版)》2020年第1期。
④苏今:《〈民法总则〉中个人信息的"可识别性"特征及其规范路径》,《大连理工大学学报(社会科学版)》2020年第1期。
⑤张新宝:《〈民法总则〉个人信息保护条文研究》,《中外法学》2019年第1期。
⑥朱烨与北京百度网讯科技公司隐私权纠纷案,江苏省南京市中级人民法院民事判决书,(2014)宁民终字第5028号。
⑦《百度隐私政策总则》,百度隐私保护平台,http://privacy.baidu.com/policy。

的使用习惯信息，司法实践中还把用户电脑中常见软件的安装情况视为“行为识别信息”，并排除在个人信息的保护范围之外①。至于可以直接与特定主体相联结的“身份识别信息”，例如自然人的出行规律②等，则属于个人信息。有观点认为，cookie 记录具备能够单独或者与其他信息结合识别特定自然人个人身份的可能性，根据《网络安全法》第七十六条的规定，属于个人信息③。但 cookie 记录之所以能够达到上述观点所称的“识别特定自然人个人身份”的特征，是与其他信息相结合的结果，这属于识别方式中间接识别的讨论范围，容下文详述。但可以明确的是，cookie 记录本身并不能完成识别身份目标，因此单独的 cookie 记录仅属于“行为识别信息”，不属于“身份识别信息”，进而不属于个人信息。从本质上来说，本案中的“行为识别信息”之所以不属于个人信息，是由于其定位的对象是浏览器或计算机设备，而非特定自然人，因此与“识别身份”相距甚远④。

本文认为，将个人信息中的“识别”限缩解释为“身份识别”更加符合“识别”的本质。对个人信息进行保护的原因在于网络环境中的虚拟人格与现实生活中的真实人格具有对应性，进而导致信息主体的人身安全和财产安全存在被侵害的可能性，信息主体的隐私存在被暴露的可能性。为了维护信息主体的权益，需要将能够识别出信息主体真实身份的信息纳入法律的保护范围，才能最大限度地减少个人信息泄露带来的风险。至于反映了信息主体行为偏好的“行为识别”信息，其作用更多体现在预测信息主体的行为走向及特定群体的活动倾向，为商业决策提供参考，而非对于信息主体的身份识别。若信息主体因自身的行为识别信息泄露而受到营销广告、垃圾邮件的影响，则只是影响了“自然人的私人生活安宁”，而不能识别出“他到底是谁”，属于自身隐私权被侵犯的情形，而不属于个人信息权益被侵犯的情形，此时可参考前述内容适用《民法典》第一千零三十二条、第一千零三十三条隐私权保护的规定。

从我国已有的部分规范性文件的规定也可以发现，其内容实质上明确规定了个人信息的识别是指身份识别，如《网络安全法》《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》和《个人信息安全规范》明确规定能够（单独或与其他信息结合）识别自然人（公民）身份的信息属于个人信息。部分规范性文件的表述则无法直接读出“身份识别”的含义，如《民法典》规定能够单独或与其他信息结合识别“特定自然人”的信息属于个人信息。《个保法》则将个人信息表述为与已识别或可识别的“自然人”有关的信息。

对于未明确规定“身份识别”的规范性文件存在可解释的空间。首先，如何理解《民法典》中规定的“特定自然人”？由于民法典的立法内容借鉴了欧盟《一般数据保护条例》（《General Data Protection Regulation》，以下简称《GDPR》）的规定，因此可以参考欧盟第二十九条资料保护工作组发布的《第 4/2007 号意见书：个人资料的概念》（《Opinion 4/2007 on the concept of personal data》）中的解释：“识别”的效果是特定对象能够与其他主体区别开来，以此推之，《民法典》中可识别或已识别的“特定自然人”也是能够与其他主体相区别的主体。其次，《个保法》中“可识别的自然人”又作何解释？在《第 4/2007 号意见书：个人资料的概念》中，列举了一个“可识别自然人”的案例：通过查阅相关时期的报纸，逐步确定刑事案件中未被公布信息的涉案人员的身份。在这一过程中获得的信息可被视为“有关可识别人员的信息”（information about identifiable persons）。可以看出，欧盟的个人信息立法中对识别的界定限于明确该主体身份的程度。将《个保法》中的“可识别自然人”解释为“明确身份的自然人”与《第 4/2007 号意见书：个人资料的概念》内容的精神相似，也符合《民法典》“特定自然人”的含义。由此可见，“识别”的对象应当为信息主体的明确身份，而非仅仅是信息主体的某些特征。

①顾俊与奇智软件（北京）有限公司等隐私权纠纷案，浙江省杭州市中级人民法院民事判决书，（2014）浙杭民终字第 1813 号。

②刘嘉龙与沈榕隐私权纠纷案，北京市第二中级人民法院民事判决书，（2020）京 02 民终 1641 号。

③陈鱼诉杭州阿里妈妈软件服务有限公司网络服务合同纠纷案，浙江省杭州市中级人民法院民事判决书，（2018）浙 01 民终 7505 号。

④但是，行为识别信息不能定位到特定自然人，并不代表此类信息不具备导致侵权行为的可能性，典型例证如大数据“杀熟”。

3.“身份识别”之再明确:两类标识符的提出

在明确了个人信息识别对象是信息主体身份的基础上,还应作进一步区分:信息所指向的特定自然人身份,是抽象意义上的一一对应,还是能够明确地指向具体的自然人?以身份证号码为例,理论上来说,每一个身份证号码只能对应一个特定自然人,已经达到将该信息主体与其他主体相区别的程度,若承认此种识别是身份识别,则身份证号码属于直接识别性个人信息。相反,若认为单纯的身份证号码虽然在理论上能够实现与信息主体的一一对应,但依然无法确定是具体的“谁”,仍需要和其他信息结合(如姓名)才能达到身份识别的程度,则身份证号码属于间接识别性个人信息。目前对于身份识别的讨论似乎并未深入研究“什么是身份”,或者说“识别到什么程度就算是识别了身份”这个前置性问题,但对这一问题的回答决定了身份识别的内涵和外延。

本文认为,“身份”是指“某个主体是谁”,即描述自然人在不同场景下存在形式的标识符。以存在的场景为标准,标识符可以分为社会意义上的标识符和自然意义上的标识符两种类型。在社会意义上,标识符的表达形式包括姓名、身份证号码、手机号码、职业、民族、荣誉称号等,此类标识符是自然人出生后被社会赋予的内容,只有在人类社会中才有意义,脱离了人类社会,此类标识符就不再具备存在的价值。除人类社会外,自然人在自然意义上也有特定的标识符,如面貌、指纹、DNA、血型等,这些标识符从自然人出生之时起便附着于人体本身,是自然人与生俱来的生物学特质,不受社会生活的影响,可独立于社会生活而存在,而且专属于特定自然人。通过信息识别信息主体身份的过程,就是对信息主体进行定位的过程,即发现代表信息主体存在形式的标识符的过程,这种标识符既包括社会意义上的标识符,也包括自然意义上的标识符。需要区分的是,作为识别标准的身份和《个保法》中敏感个人信息中的特定身份并不相同。作为识别标准的身份包括社会意义上的标识符和自然意义上的标识符,涵盖了所有可能存在的标识符内容。但敏感个人信息中的特定身份,仅指部分社会意义上的标识符,如种族信息、民族信息、社团组织的会员信息等①。因此,识别标准中身份的范围可以覆盖敏感个人信息中特定身份的范围。

一般来说,若要准确定位一个信息主体在社会生活和自然生活中所处的“位置”,似乎最少只需一个标识符即可完成,如信息主体的身份证号码、手机号码、指纹等,此类标识符在抽象意义上确实只对应唯一一个自然人主体,满足了识别所要求的定位作用。但从《个保法》的立法宗旨来看,对个人信息的处理活动进行规范,是为了避免“自然人的人格尊严、人身自由等基本权利以及人身权益、财产权益造成危险或者损害”②。相反,若通过某类标识符进行定位后,无法导致上述后果,则可以认为此类标识符并未达到《个保法》对识别的最低要求。在此基础上重新审视两类标识符,会发现《个保法》所要保护的主体一定是处于社会生活中的“人”,而非单纯的自然状态下的“生命体”。如《个保法》第二十八条列举的敏感个人信息种类包括行踪轨迹信息,单从行踪轨迹信息本身来看,似乎这是一种脱离了社会生活也可以继续存在的信息,但行踪轨迹信息泄露后使自然人的人身受到危害的前提,是这一信息主体的社会标识符是明确的、具体的、能够与其他社会主体区分开的,否则单纯的行踪轨迹信息泄露并不会对信息主体的人身权益造成危险。由此可知,《个保法》语境下的身份识别,需要借助两个或两个以上的标识符才能完成,其中一个标识符必定是社会意义上的标识符,其他标识符既可能是社会意义上的标识符,也可能是自然意义上的标识符。

(三)方式标准:如何识别

识别方式是指某类信息指向特定自然人身份的途径。根据《民法典》第一千零三十四条第二款的规定,个人信息的识别方式包括单独识别和不同信息结合识别两种方式,学界分别称之为直接识别方式和间接识别方式③。以前文提及的身份识别标准来看,直接识别方式似乎无法达到

①江必新,郭锋:《个人信息保护法条文理解与适用》,人民法院出版社2021年版,第268页。

②程啸:《个人信息保护法理解与适用》,中国法制出版社2021年版,第9页。

③李黎:《个人信息概念的反思:以“识别”要件为中心》,《信息安全研究》2021年第8期。

《个保法》所要保护的识别标准，间接识别方式则会随着信息识别技术的发展不断扩张其所覆盖的信息范围。为了明确个人信息的边界，防止个人信息的外延泛化，需要用体系解释的方法对间接识别方式中个人信息的范围进行限缩。

1.直接识别方式之质疑

直接识别是凭借单独的信息即可定位信息主体的识别方式。需要讨论的是何为单独的信息？首先应当排除的是单独的信息载体。《个人信息安全规范》的附录 A 中对个人身份信息进行了列举，如身份证、工作证等。本文认为上述列举的“个人身份信息”实质上并非个人信息，而只是记载了个人信息内容的物理载体，识别的过程借助的是证件上的姓名、号码等信息，而非证件这一客观实物，因此身份证并不属于个人信息，身份证上所记载的姓名、性别、民族、出生日期、住址和身份证号码等内容才是个人信息。进一步而言，单独的信息应当是指独立存在的、不与其他内容结合的信息，身份证号码即为一例。除此之外，自然人的指纹信息、DNA 信息均是单独的信息。

那么，单独的信息可否完成《个保法》所要求的身份识别？前文已述，《个保法》所要保护的是处于社会中的人，则社会意义上的标识符自然为识别身份所必需，在此基础上辅以其他标识符，识别过程才能完成。前述单独的信息不能满足《个保法》所要求的身份识别标准。如身份证号码只能在抽象意义上对应社会中的“某一个”信息主体，但这一信息主体在社会中的姓名、存在状态、社会关系、财产状况等内容均无从得知，也就不存在对这一信息主体的人身权益和财产权益造成侵害的可能。指纹信息和 DNA 信息也是如此，只有这些自然意义上的标识符和社会意义上的标识符结合，才能明确、具体地定位这些信息究竟为哪个社会主体所拥有。因此，单独的信息无法完成《个保法》的识别要求，直接识别的方式或许并不存在。但是这并不代表前述的身份证号码、指纹信息等不是个人信息，这些信息只是不属于能够直接识别特定自然人身份的信息，但依然属于与已识别的自然人相关的信息，因此依然会受到《民法典》《个保法》等规范的保护。

2.间接识别方式之限制

间接识别方式是指将不同的信息结合在一起定位信息主体的识别方式。间接识别方式的最大特征在于信息的“结合”，围绕间接识别方式的争论也在于此：在多个信息结合识别自然人身份的过程中，是每个单独的信息均构成个人信息，还是不同信息结合后的整体才属于个人信息[①]？例如单独的甲信息和乙信息均无法识别信息主体的身份，但甲信息和乙信息结合时可明确信息主体的身份，此时便存在两种可能：其一，单独的甲信息和单独的乙信息均是个人信息；其二，单独的甲信息和单独乙信息均不是个人信息，只有甲信息和乙信息结合后的整体信息才属于个人信息。

从法益保护的角度来说，个人信息之所以需要保护，是因为其附着了诸多利益，如信息主体的隐私权益、人身权益和财产权益等，个人信息能够附着上述利益的关键，就在于其内容具有明确的指向性。在个人信息中，信息主体不愿为他人知晓的内容指向信息主体的隐私权益，信息主体的健康状况和行踪轨迹等内容指向其人身权益，信息主体的金融账户信息等内容则指向其财产权益。从这一立场来看，前述两种信息结合的情况，会发现单独的甲信息和单独的乙信息均不具备明确的指向性，无法连接到信息背后的特定信息主体，因此尚未达到需要法律予以保护的程度。但当甲信息和乙信息结合形成整体信息时，该整体信息具备了连接信息主体的指向性，信息主体的权益与整体信息的内容产生了勾连，在这种情况下需要对该整体信息施以更强有力的保护，进而维护信息主体的合法权益。因此，在间接识别的情况下，只有两个以上的信息结合后形成的整体信息才与信息主体法益联系密切，应当被视作个人信息予以保护。

从法律规范的内容来看，《民法典》第一千零三十四条第二款的文字表述说明，能够与其他信息结合识别特定自然人的信息均为个人信息，因此条文的字面规定似乎意味着在间接识别的情况下，单独的信息也可被视作间接识别性个人信息。若以此为标准，在信息识别技术不断发展的背景下，个人信息的范围会无限扩大，由此会造成个人

①杨楠：《个人信息“可识别性”扩张之反思与限缩》，《大连理工大学学报（社会科学版）》2021 年第 2 期。

信息处理者承担巨大的合规压力,并严重限制数字时代的经济发展和社会主体的行为自由。为了避免这一情形,可从体系解释的角度对间接识别方式中个人信息的外延进行限缩:在体例安排上,《民法典》将“隐私权和个人信息保护”作为人格权编中的一章,说明个人信息是作为人格权项下的权益加以保护的,所以个人信息必定是和自然人的人格利益相关的信息①。据此可以得出结论:能够与其他信息结合识别特定自然人,且与自然人的人格利益相关的信息属于间接识别方式中的个人信息,如自然人的生物识别信息、宗教信仰信息等。用这一视角检验现有规范性文件中的内容可以发现,其中列举的诸多个人信息其实并非可识别性信息,如《个人信息安全规范》附录 A 中列举的个人信息包括硬件序列号、设备 MAC 地址、唯一设备识别码等个人常用设备信息,根据这些信息能够识别某一特定设备,但与自然人的人格利益无关,也无法定位到具体的自然人,因此上述信息并非可识别性信息,至多只能属于“与已识别的自然人相关的信息”。同理可得,前文中提及的 cookie 信息只能记录特定设备的使用情况,而不能反映设备使用者的身份信息,因此单纯的 cookie 信息不属于间接识别方式中的个人信息,手机号码亦然。

综上,在间接识别的过程中,通过体系解释的方法,将间接识别方式中个人信息的范围限制在与特定自然人的人格利益相关的信息范围内,既保持了与《民法典》规范文义和体例安排的一致性,又可以防止信息识别技术导致的个人信息范围过宽的问题,不失为一条可行的进路。以这一观点重新审视前文中提到的案例和问题可以得出结论:案件中的被告并不具备特殊识别能力,因此对其来说,单独的手机号码无法识别定位到明确手机号码的主体,所以不属于个人信息,故本文赞成北京市海淀区法院的裁判理由。在甲信息和乙信息结合识别信息主体的情况下,甲信息和乙信息结合后的整体信息属于个人信息,对于单独的甲信息和乙信息来说,只有其和信息主体的人格利益相关时,才属于个人信息。

Criteria for Judging the Identifiable Elements in Personal Information

LIU Zong-sheng & ZHANG Yi

(School of Credit Risk Management, Xiangtan University, Xiangtan 411105, China)

Abstract: The boundary between personal information and private information has changed from being mixed to being clear, and its definition mode has also developed from “identification theory” to “association theory”. There are three criteria for judging the identifiability of information, i.e. the identification subject should adopt the “subjective theory” to realize the connection between personal information protection and the constituent elements of tort liability. On the identification object, the “identification” limit needs to be interpreted as “identity recognition”, at least two or more identifiers are required to complete the identification, and at least one identifier in the social sense is required. In terms of identification methods, the existence of direct identification methods is debatable, and taking the correlation of personality interests as the criterion for judging personal information in indirect identification can avoid excessive extension of personal information.

Key words: personal information; identity recognition; behavior recognition; direct identification; indirect identification

(责任校对　龙四清)

①苏今:《〈民法总则〉中个人信息的“可识别性”特征及其规范路径》,《大连理工大学学报(社会科学版)》2020 年第 1 期。