本刊特稿

论刑法中个人信息的识别

欧阳本祺

[摘　要] “识别”是个人信息概念中的核心和关键要素,是连结阻挡层法益和背后层法益的纽带。刑法中个人信息的识别困境,体现在外观识别、内涵识别和体系识别三个方面。应该结合场景理论来确立个人信息的识别标准。识别目的越明确,界定为公民个人信息的可能性越大;识别能力越强,界定为公民个人信息的可能性越大;识别后果越重,界定为公民个人信息的可能性越大;识别概率越高,界定为公民个人信息的可能性越大。刑法中的敏感信息不必与前置法中的敏感信息采取相同的识别标准,应该根据识别后果对背后层的人身、财产安全的危险程度来界定刑法中的敏感信息。

[关键词] 个人信息;非个人信息;敏感个人信息;识别

个人信息是一个工具性概念,个人信息的法益是一种阻挡层法益,保护个人信息是为保护个人信息背后层的实体性法益。而连结阻挡层法益与背后层法益的技术要素就是个人信息概念中的“识别”,各国法律无不把“识别”作为个人信息概念的核心关键词。只有能够识别特定自然人的信息才属于个人信息,不能识别特定自然人的信息不属于个人信息。但是,能否识别以及如何识别是一种抽象的价值判断,涉及个人保护与数据共享之间的平衡。由于价值立场的不同,刑法实践对于如何识别个人信息,呈现出多重困境,直接影响了罪与非罪、此罪与彼罪的认定。因此,需要深入研究刑法中个人信息的识别,并总结出具有可操作性的标准。

一、刑法中个人信息识别的困境

在大数据时代,与个人相关的信息或者数据无处不在。那么,个人信息与个人数据是否为同一概念,个人信息与非个人信息如何区别,个人信息内部的敏感个人信息与非敏感个人信息如何区别,刑法中的个人信息与前置法中的个人信息是否为同一概念?这些问题涉及个人信息的外观识别、内涵识别和体系识别,同时面临理论与实践存在脱节的困境。

(一) 刑法中个人信息外观识别的困境

刑法中个人信息的外观识别,是指在外观上对“个人信息”与“个人数据”这两个概念进行关系

欧阳本祺,法学博士,东南大学法学院教授、博士生导师,东南大学人权研究院研究员(南京 211189)。本文系国家社科基金重点项目“预防性犯罪化立法冲击下刑法教义学的应对与发展研究”(22AFX008)以及江苏省高校哲学社会科学重大项目“要素市场化配置视域下数据交易安全的刑法规制研究”(2022SJZD001)的阶段性成果。

识别。对此,我国刑法学界存在三种不同的观点。

“个人信息与个人数据等同说”认为,我国刑法中的“个人信息”的内涵外延等同于欧盟《通用数据保护条例》规定的“个人数据”,两个概念可以混同使用。①

“个人信息大于个人数据说”认为,个人信息的外延大于个人数据,个人信息的刑法保护包括三种模式:第一种模式是个人信息的保护依附于他权保护,个人信息体现为信用卡信息(第177条之一)、商业秘密(第219条)、信件(第252条)、邮件、电报(第253条)、电信号码(第265条)、居民身份证(第280条);第二种模式是个人信息的保护依附于数据保护,个人信息体现为计算机信息系统中的个人数据(第285条);第三种模式是个人信息的独立保护,个人信息体现为独立的个人信息权(第253条之一)。②

“个人信息小于个人数据说”认为,刑法中的个人信息只是个人数据的一部分。个人数据可以表现为人格利益,相关侵害行为构成侵犯公民个人信息罪;个人数据可以表现为财产利益,相关侵害行为构成侵犯财产犯罪;个人数据也可以表现为商业秘密,相关侵害行为构成侵犯商业秘密罪;个人数据还可以表现为计算机信息系统的安全,相关侵害行为构成非法获取计算机信息系统数据罪。③

本文认为,个人信息在我国法律体系中是一个法定概念,而个人数据是一个非法定的学理概念,在我国应该采取“个人信息小于个人数据说”的观点。理由如下:

首先,概念的使用离不开本国法律的规定。一方面,根据我国《个人信息保护法》《民法典》《网络安全法》的规定,“个人信息”不是“与个人相关的信息”,而是“个人可识别的信息”。欧盟与我国“个人信息”概念相对应的概念是“个人数据”。美国与我国“个人信息”相对应的概念是“个人可识别信息”(Personally Identifiable Information,PII)。④ 另一方面,我国法律只规定了数据的概念,而没有关于个人数据的规定。我国《数据安全法》把“数据”界定为任何以电子或者其他方式对信息的记录。学界主流观点把数据分为政府数据、企业数据、个人数据。⑤ 可见,前述“等同说”实际上是用欧盟《通用数据保护条例》来界定我国的个人数据概念,不合理地缩小了我国个人数据的外延。前述“大于说”则又忽视了我国前置法对于个人信息的明确限制,把“个人信息”理解为“个人相关的信息”,没有根据地扩大了我国个人信息的外延。

其次,概念的使用离不开互联网的分层构造。个人信息与个人数据的关系应该放在互联网的分层结构中来理解。一般认为,互联网的结构可以分为物理层、逻辑层、内容层。⑥ 物理层构成了互联网空间中的“一砖一瓦”,是分层结构的最底层。⑦ 它的功能在于创建数据传输的物理链路。⑧ 逻辑层建立在物理层所形成的传输链之上,是分层结构的中间层,它的功能在于通过数据的“封装”(从信息到比特流)与“解封装”(从比特流复原为信息),实现数据的传输。⑨ 内容层直接面对用户,是分层

---

①参见劳东燕:《个人数据的刑法保护模式》,《比较法研究》2020年第5期;王华伟:《数据刑法保护的比较考察与体系建构》,《比较法研究》2021年第5期。

②参见李川:《个人信息犯罪的规制困境与对策完善——从大数据环境下滥用信息问题切入》,《中国刑事法杂志》2019年第5期;于冲:《侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界》,《政治与法律》2018年第4期。

③参见杨志琼:《我国数据犯罪的司法困境与出路:以数据安全法益为中心》,《环球法律评论》2019年第6期;苏青:《数据犯罪的规制困境及其对策完善——基于非法获取计算机信息系统数据罪的展开》,《法学》2022年第7期。

④参见 P. M. Schwartz & D. J. Solove, “The PII problem: Privacy and a new concept of personally identifiable information”, *New York University Law Review*, Vol. 86, No. 6, 2011, pp. 1814 – 1894.

⑤参见王利明:《论数据权益:以“权利束”为视角》,《政治与法律》2022年第7期。

⑥参见 L. Lessig, “The architecture of innovation”, *Duke Law Journal*, Vol. 51, No. 6, 2002, pp. 1783 – 1801.

⑦C. Nazli & D. D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma*, Cambridge, MA: MIT Press, 2019, p. 3.

⑧对物理层的侵犯,可能构成故意毁坏财物罪、盗窃罪等犯罪。

⑨对逻辑层的侵犯,可能构成非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统罪、破坏计算机信息系统罪等。

结构的最高层，它的功能在于通过不同类型的文件实现对信息的呈现与处理。[①] 可见，数据属于逻辑层，信息属于内容层，数据与信息之间是载体与本体的关系。作为载体的数据应该包含作为本体的信息。

（二）刑法中个人信息内涵识别的困境

刑法中个人信息的内涵识别，是指刑法中个人信息与非个人信息的关系识别，以及个人信息内部敏感个人信息与非敏感个人信息的关系识别。其核心问题是如何理解个人信息的“识别”，主要体现为手机号码、IP 地址、cookie 记录的属性认定。

1. 手机号码是否属于个人信息

关于手机号码的属性，司法实践的争议主要集中在单位的手机号码是否属于个人信息，以及孤立的手机号码是否属于个人信息这两个问题。

在王健侵犯公民个人信息案中，被告人王健从阿里巴巴、天眼查、慧聪网等公共平台获取大量企业信息，然后将其中的法定代表人或者联系人的姓名、手机号码、单位名称编辑汇总用于出售或者提供给他人。检察院认为，根据《个人信息刑事案件解释》第 3 条，未经被收集人同意，将合法收集的公民个人信息向他人提供的，构成侵犯公民个人信息罪中的“提供公民个人信息”。但是，2018 年最高人民检察院《检察机关办理侵犯公民个人信息案件指引》（以下简称《检察机关指引》）规定，“由公司购买、使用的手机、电话号码等信息，不属于个人信息的范畴”。据此，应当区别由“由公司购买，归公司使用的手机号码”与“公司经办人个人登记的手机号码”两种不同情形，前者则不属于个人信息。[②] 但也有判决认为，从“国家企业信用信息公示系统”中查询到的手机号码，仍然属于个人信息。[③]

另外，即使手机号码被个人购买与使用，但一个孤立的手机号码能否被认定为刑法中的“个人信息”？对此，司法实践也存在很大的分歧。多数法院判决认为，孤立的手机号码不能单独识别特定自然人身份，不属于刑法中的个人信息。[④] 当然，也有法院认为，孤立的手机号码虽然无法单独识别个人身份，但结合其他信息是能够识别个人身份的，因此属于个人信息。[⑤]

2. IP 地址是否属于个人信息

计算机的 IP 地址由 32 位二进制数组成，包括网络标识与主机标识两部分，在互联网范围内是唯一的。在凌某某起诉抖音 APP 侵害个人信息权一案中，法院认为 IP 地址与其他信息结合，可以识别特定自然人，因而属于个人信息，这与 IP 地址的模糊或精确无关。[⑥] 相关的规范标准也将 IP 地址作为个人信息。[⑦] 但是，仍有部分刑事判决认为根据 IP 地址难以识别特定自然人的身份，而将其排除在个人信息条数之外。[⑧]

3. cookie 记录是否属于个人信息

在朱某诉百度公司隐私权纠纷案中，对于“丰胸”“减肥”“流产”等 cookie 检索记录的属性，一审

---

①对内容层的侵犯，可能构成侵犯知识产权类犯罪、侵犯公民个人信息罪等。对内容层中虚拟财产的侵犯，我国理论与实务界存在较大的争议。参见欧阳本祺：《论虚拟财产的刑法保护》，《政治与法律》2019 年第 9 期。

②参见江苏省苏州市姑苏区人民法院（2018）苏 0508 刑初 40 号刑事判决书。

③参见重庆市开州区人民法院（2017）渝 0154 刑初 342 号刑事判决书。

④参见安徽省合肥市包河区人民法院（2018）皖 0111 刑初 377 号刑事判决书；安徽省亳州市谯城区人民法院（2018）皖 1602 刑初 82 号刑事判决书；广东省深圳市福田区人民法院（2018）粤 0304 刑初 448 号刑事判决书；福建省永泰县人民法院（2019）闽 0125 刑初 44 号刑事判决书。

⑤参见山东省沂南县人民法院（2018）鲁 1321 刑初 89 号刑事判决书。

⑥参见北京互联网法院（2019）京 0491 民初 6694 号民事判决书。

⑦参见《信息安全技术：个人信息安全规范》（GB/T 35273 - 2020）“附表 A.1”。

⑧参见广东省深圳市龙华区人民法院（2020）粤 0309 刑初 614 号刑事判决书；陕西省西安市未央区人民法院（2019）陕 0112 刑初 880 号刑事判决书。

判决认为属于个人信息中的敏感隐私信息。[①] 二审判决认为 cookie 技术是一个合法、中立的工具，根据 cookie 记录无法识别特定的自然人，因而不是个人信息。[②] 这个案件的判决不仅涉及个人信息与非个人信息的识别，还涉及个人信息内部的敏感个人信息与非敏感个人信息的区别。

（三）刑法中个人信息体系识别的困境

刑法中个人信息的体系识别，是指在整个法律体系中刑法个人信息与前置法个人信息的关系识别。在我国法律系统中，最早规定个人信息概念的是2009年《刑法修正案（七）》，之后2017年《网络安全法》、2020年《民法典》和2021年《个人信息保护法》相继规定了个人信息的概念及其保护。立足于我国这种“刑法先行”的立法模式，识别刑法与前置法中个人信息的关系尤为必要。对此，我国学界也存在着以下三种不同的观点。

“等同说”认为，侵犯公民个人信息罪的成立以“违反国家有关规定”为前提，因此，刑法个人信息应当与前置法个人信息保持内涵外延的一致性。但是，对于同一概念，适用刑法时既可能作扩大解释，使其外延大于前置法（如刑法中的“丢失枪支”包括行政法中的“枪支被盗、被抢或者丢失”）；也可能作缩小解释，使其外延小于前置法（如刑法中“卖淫”的外延小于行政法）。

“大于说”认为，刑法个人信息的外延大于行政法。有学者认为，“两高”《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》（以下简称《个人信息刑事案件解释》）把刑法中个人信息划分为两类：一类是“识别特定自然人身份的信息”，另一类是“反映特定自然人活动情况的信息”。而《个人信息保护法》等前置法只规定了识别性信息，没有规定反映特定自然人活动情况的信息。因此，刑法中个人信息的外延大于前置法。[③] 但是，这种观点值得商榷。

实际上，刑法中个人信息的外延远远小于《个人信息保护法》，这也是笔者更为赞同的“小于说”。理由如下：首先，对《个人信息刑事案件解释》不能作僵硬的形式化理解。《个人信息保护法》《民法典》《网络安全法》等前置法中的“识别”是指广义的识别，既包括狭义的身份识别信息，也包括能反映自然人活动情况的信息。《个人信息刑事案件解释》中规定的“行踪轨迹”等反映特定自然人活动情况的信息，同样必须具有识别性。刑法解释只是为了便于司法操作，才采取了“身份识别信息＋活动情况信息”的表述。[④] 仅仅根据刑法解释的表述形式而不分析其实质内涵，就断定刑法中个人信息的外延大于前置法，可能过于武断。其次，《个人信息保护法》中的“个人信息”范围相当宽泛。从立法表述看，《个人信息保护法》第4条采取的是“识别性＋相关性”的判断标准。识别性标准遵循“从信息到人”的路径，即能够识别出特定自然人的信息，才是个人信息。相关性标准遵循“从人到信息”的路径，即与特定自然人相关的信息，都是个人信息。相关性标准使得个人信息的范围相当宽泛且模糊。[⑤] 从立法价值来看，我国《个人信息保护法》采取的是欧盟模式，而刑事司法实践采取的是美国模式。欧盟把个人信息作为基本权利的客体，因此立法上扩大个人信息的保护范围；美国把个人信息作为言论自由的表达对象，因此个人信息的范围会受到多种因素的限制。[⑥]

---

①参见南京市鼓楼区人民法院（2013）鼓民初字第3031号民事判决书。

②参见南京市中级人民法院（2014）宁民终字第5028号民事判决书。

③参见刘宪权、王哲：《侵犯公民个人信息罪刑法适用的调整和重构》，《安徽大学学报》（哲学社会科学版）2022年第1期；李怀胜：《侵犯公民个人信息罪的刑法调适思路——以〈公民个人信息保护〉为背景》，《中国政法大学学报》2022年第1期。

④参见喻海松：《“刑法先行”路径下侵犯公民个人信息罪犯罪圈的调适》，《中国法律评论》2022年第6期。

⑤参见谢登科：《个人信息跨境提供中的企业合规》，《法学论坛》2023年第1期。

⑥参见丁晓东：《个人信息的双重属性与行为主义规制》，《法学家》2020年第1期；宋亚辉：《个人信息的私法保护模式研究——〈民法总则〉第111条的解释论》，《比较法研究》2019年第2期。

二、刑法中个人信息识别标准的确立

上述关于个人信息外观识别、内涵识别、体系识别的理论与实践困境表明，理解个人信息的识别性及其标准是走出困境的关键。个人信息的识别标准旨在将个人信息与非个人信息区别开来。

（一）确立个人信息识别标准的必要性

我国学界有一种代表性的观点认为，刑法中的个人信息无需具备识别性。例如，有的学者认为，要求刑法中的个人信息具有识别性，是一场美丽的误会；[①]即使是经过匿名化处理的信息，也属于侵犯公民个人信息罪的对象。[②] 张明楷教授认为，“凡是与自然人有关的各种信息，均属于公民个人信息”[③]，似乎也主张刑法中的个人信息不需要具备识别性。本文认为，这种观点值得商榷，刑法中的个人信息应当坚持识别性标准。

1. 识别性标准有利于维护法秩序的统一性

一个国家的所有法规范构成一个有机统一的法秩序。从纵向来看，法秩序统一性表现为以宪法为顶点的融贯性，部门法与宪法之间不存在矛盾和冲突。从横向来看，法秩序统一性表现为不同部门法之间的协调性，部门法之间不存在矛盾和冲突。[④] 就个人信息而言，法秩序统一性要求刑法的适用不能和前置法产生冲突和矛盾。从历史解释来看，在2009年《刑法修正案（七）》规定侵犯公民个人信息的犯罪时，其他法律尚无关于个人信息的规范，因此，当时关于个人信息的界定处于一个探索和混乱的状态。但是，现在已有多部前置法对个人信息概念作出了规定。例如，《网络安全法》把个人信息界定为“身份识别信息”；[⑤]《民法典》把个人信息界定为“自然人识别信息”；[⑥]《个人信息保护法》把个人信息界定为“识别性+关联性信息”。[⑦] 可见，前置法都把“识别性”作为个人信息的重要特征。

否定识别性的学者认为，虽然前置法规定了个人信息的识别性要求，但刑事司法解释把个人信息分为三类：身份识别信息+个人隐私信息+活动情况信息。[⑧] 因此，刑法中个人信息的范围大于前置法，无需具有识别性。然而，这种观点既是对司法解释的误读，也是对法秩序统一性的违反。虽然司法解释规定了“涉及公民个人隐私的信息”以及“反映特定自然人活动情况的信息”，但是，这两类信息并非对识别性的否定。

首先，“涉及公民个人隐私的信息”须以能够识别特定自然人为前提。如果某种隐私图片不能识别特定自然人，就无法认定为刑法中的个人信息。有学者认为，偷拍女性裙底的行为，非法获取了他人的隐私信息，应当构成侵犯公民个人信息罪，即使裙底照片无法识别特定自然人。[⑨] 但是，该论断

---

①参见晋涛：《刑法中个人信息“识别性”的取舍》，《中国刑事法杂志》2019年第5期。

②参见张勇：《个人信息去识别化的刑法应对》，《国家检察官学院学报》2018年第4期。

③参见张明楷：《刑法学》，北京：法律出版社，2021年，第1200页。

④参见欧阳本祺：《论行政犯违法判断的独立性》，《行政法学研究》2019年第4期。

⑤2017年《网络安全法》第76条规定，“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身份的各种信息”。

⑥《民法典》第1034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”。

⑦2021年《个人信息保护法》第4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相关的各种信息，不包括匿名化处理后的信息”。

⑧2013年最高人民法院、最高人民检察院、公安部《关于依法惩处侵害公民个人信息犯罪活动的通知》规定个人信息包括“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”。2017年《个人信息刑事案件解释》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”。

⑨参见晋涛：《刑法中个人信息“识别性”的取舍》。

在逻辑上是混乱的。偷拍他人裙底的行为当然是侵犯隐私的行为，但是该偷拍行为只是《治安管理处罚法》第42条第6款规定的违法行为，并不构成犯罪，当然也不会构成侵犯公民个人信息罪。如果行为人出售偷拍的裙底照片，因裙底照片无法识别特定自然人，出售行为可能构成贩卖淫秽物品牟利罪，但不会构成侵犯公民个人信息罪。“隐私信息无疑是针对某特定个人的信息，当然属于可以识别公民个人身份的信息”。① “个人私密信息在本质上仍然属于个人信息，只不过个人信息主体希望使其保持于私密状态而已”。② 但是，裙底照片如果不能识别特定自然人，则只是与隐私相关的信息，还不构成个人信息中的隐私信息或者私密信息。

其次，“反映特定自然人活动情况的信息”也以具有识别性为前提。例如，作为个人信息的行踪轨迹，必须与可识别的特定自然人相关联。如果行踪轨迹无法识别特定自然人，那就是关于物流、车流、人流统计的数据。非法获取或者提供这些数据，不可能构成侵犯公民个人信息罪。司法解释中规定的反映特定自然人活动情况的信息，只是对可识别信息的具体化，并不是对识别性的否定。

2. 识别性标准有利于个人信息的类型化分析

否定个人信息识别性要求的观点，实际上把个人信息当做“个人相关的信息”，缺乏对个人信息的类型化分析。所谓“识别”（identify），是指根据该信息把特定自然人从其所处的群体中挑选（single out）出来（例如通过人脸信息认出某人），或者通过该信息联络（contact）到特定自然人（例如通过电话号码联系到某人）。③ 只不过，不同信息对特定自然人的识别程度有大小之别。最高识别程度为已经识别，这类信息被称为已识别（identified）信息。最低识别程度是零，即根据该信息不能识别特定自然人，这类信息被称为不可识别（non-identifiable）信息或者匿名信息。介于最低程度和最高程度之间的信息，为可识别（identifiable）信息。④

可见，个人相关的信息包括三类：已识别信息、可识别信息、不可识别信息。其中，已识别信息属于个人信息，不可识别信息不属于个人信息，对此不存在争议。有争议的是可识别信息是否属于个人信息，司法实践中的难题也主要集中在可识别信息的属性认定上。从理论上来说，对于任何一条可识别信息，只要补充足够多的其他信息，就可以识别出特定的自然人。但是，司法实践中能够获得的个人相关信息总是有限的。因此，可识别信息是否属于个人信息，需要具体判断，不是“全有全无”的判断，而是“或有或无”的判断，即有的可识别信息属于个人信息，有的可识别信息不是个人信息。司法解释中的“隐私信息”与“身份活动信息”，实际上都属于可识别信息的范畴。前述否定个人信息识别性要求的观点，对“识别”作了狭隘与片面的理解，认为“识别”仅指“已识别”，而不包括“可识别”。

（二）确立个人信息识别标准的价值基础

由上可知，可识别信息是否属于个人信息的判断，是“或有或无”的判断，而不是“全有全无”的判断。那么，什么场合可识别信息属于个人信息，什么场合可识别信息不属于个人信息呢？这种判断实际上是一种价值判断，这种价值判断受制于国家保护个人信息的力度以及国家促进数据共享的力度。

从比较法的角度来看，在保护个人信息与促进数据共享之间，欧盟与美国体现出两种不同的价值倾向。欧盟倾向于把个人信息作为基本权利的客体，把个人信息权界定为宪法上的信息自决权，

①赵忠东：《可识别性是公民个人信息的根本特性》，《检察日报》2018年7月8日，第3版。
②王利明：《和而不同：隐私权与个人信息的规则界分和适用》，《法学评论》2021年第2期。
③参见范为：《大数据时代个人信息定义的再审视》，《信息安全与通信保密》2016年第10期。
④参见P. M. Schwartz & D. J. Solove，“The PII problem：Privacy and a new concept of personally identifiable information”.

并赋予个人对其信息的一系列消极防御权和积极控制权。[①] 欧盟这种侧重个人信息保护的立场，反映了其对数据共享与利用的忽视。因此，在这种背景下，欧盟《通用数据保护条例》（GDPR）规定，个人信息是指与已识别或可识别的自然人（数据主体）有关的任何信息。这意味着立法上通过从“已识别”到“可识别”的延展，极大地开拓了个人信息的范围。尤其是在数化万物的大数据时代，可识别与不可识别（匿名）之间的界限，非常微妙难分。[②]

美国不存在专门的个人信息保护立法。个人信息的保护散见于《儿童在线隐私保护法（COPPA）》《视频隐私保护法（VPPA）》《金融服务现代化法案》等法案。这种分散的立法模式本身反映出美国对个人信息的保护力度小于欧盟；相反，美国促进数据共享的力度大于欧盟。另外，美国的个人信息作为言论表达的对象，还受到言论自由的限制，无法形成欧盟式的宪法性信息自决权。[③] 因此，美国的立法、法官与政治制定者都倾向于把个人信息（PII）限缩解释为与“已识别”个人相关的信息。例如，美国联邦贸易委员会认为，cookie 只有在与“已识别”个人相关时，才属于个人信息（PII）。[④] 换言之，在美国，可识别信息一般不作为个人信息。

我国《个人信息保护法》采取欧盟模式，扩大个人信息的范围，把与“已识别或者可识别”的自然人相关的各种信息，都界定为个人信息。那么在司法实践中，应当在多大程度上把“可识别”信息认定为个人信息呢？这实际上涉及的是多方利益平衡的问题。有的学者把这种利益平衡概括为“两头强化、三方平衡”，即强化对敏感个人信息的保护，强化对一般个人信息的利用，同时协调信息主体对个人信息保护的利益、信息业者对个人信息利用的利益、国家管理社会的公共利益三者之间的平衡。[⑤] 有的学者把这种利益平衡概括为“合法性”“正当性”“必要性”三个原则。[⑥] 这种利益平衡，实际上是场景理论的应用。因此，可识别信息能否认定为个人信息，归根到底应该结合具体场景进行具体判断。

（三）确立个人信息识别标准的具体场景

任何个人信息都存在于一定的场景中，我们上班时可能需要刷指纹，入住宾馆时需要登记身份证信息，就医时需要填写个人健康信息。我们与熟人聊天时，可能会交流很多敏感信息，但我们初识陌生人时可能只会留下手机号码。可见，个人信息的使用和界定离不开特定的场景。所谓场景，是指以活动、角色、关系、权力结构、规范、价值理念为特征的结构化的社会环境。[⑦] 场景的构成要素多种多样，有的学者概括为信息发送者、信息接受者、信息主体、信息类型、信息传输原则。[⑧] 有的学者把信息场景的构成要素概括为信息主体、信息处理者、第三方主体、信息性质、处理目的。[⑨] 还有的学者认为，场景的构成要素包括信息的敏感度、数量、收集方式、信息接受者的状况、信息的使用目的与后果、与其他信息的比对情况、科技水平等等，不一而足。[⑩]

《个人信息保护法》把识别分为“已识别＋可识别”；《个人信息刑事案件解释》把识别分为“单独

---

①G. G. Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, New York: Springer International Publishing, 2014, p. 264；丁晓东：《个人信息的双重属性与行为主义规制》。

②参见齐爱民、张哲：《识别与再识别：个人信息的概念界定与立法选择》，《重庆大学学报》（社会科学版）2018 年第 2 期。

③参见丁晓东：《个人信息的双重属性与行为主义规制》。

④参见 P. M. Schwartz & D. J. Solove, “The PII problem: Privacy and a new concept of personally identifiable information”.

⑤参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期。

⑥参见冯恺、杨润宇：《人脸识别信息处理中的“合法、正当、必要”原则的区分审查》，《东南法学》2022 年第 1 期。

⑦参见［美］海伦·尼森鲍姆：《场景中的隐私》，王苑译，北京：法律出版社，2022 年，第 122 页。

⑧参见［美］海伦·尼森鲍姆：《场景中的隐私》，第 130 页。

⑨参见王苑：《敏感个人信息的概念界定与要素判断——以〈个人信息保护法第 28 条为中心〉》，《环球法律评论》2022 年第 2 期。

⑩参见范为：《大数据时代个人信息定义的再审视》。

识别+与其他信息结合识别”。这两种表述,本质上并无不同。“已识别”就是“单独识别”,指的是直接识别;“可识别”就是“与其他信息结合识别”,指的是间接识别。把直接识别信息界定为个人信息,一般争议不大;有争议的是,间接识别信息能否认定为个人信息。单独的手机号码在朋友之间可以直接识别特定自然人,但在陌生人之间则需要结合其他信息进行间接识别。那么,影响间接识别的场景因素有哪些?对此,存在不同观点。

“一要素说”认为,影响间接识别的场景因素是识别主体的能力。具体而言,关于识别主体的能力,又存在主观说、客观说、折中说三种不同看法。① “二要素说”认为,影响间接识别的场景因素,除了识别主体的能力外,还包括获取其他参考资料的难易度。② 实际上,“二要素说”与“一要素说”并无本质区别。所谓获取其他参考资料的难易度,就是主体识别能力的反映。识别能力越强的,获取其他参考资料的难度越小;识别能力越弱的,获取其他参考资料的难度越大。“三要素说”认为,在间接识别的场合下,需要考虑三个方面的要素:一是信息本身的重要性程度,如果涉案信息与人身、财产安全密切相关,则倾向于认定为个人信息;二是需要参考的其他信息的数量,如果涉案信息需要结合的其他信息少,则认定为个人信息的可能性大;三是行为人的主观目的,如果行为人获取信息不是为了识别出特定自然人,那么就不宜认定为公民个人信息。③ “四要素说”认为,影响间接识别的要素有四个:识别目标是什么、由谁来识别、识别概率多大、识别的后续风险多大。④

实际上,影响个人信息界定的场景因素多种多样,甚至无法穷尽列举。例如,谁在收集信息,谁在分析信息,谁在传播信息,向谁传播信息,信息的性质,各方之间的关系,甚至还包括更大的制度和社会环境。⑤ 本文参考上述观点,提出间接识别的四条基本规则。

1. 识别目的越明确,界定为公民个人信息的可能性越大

根据识别目的之明确性大小,识别可以分为四种:查找型识别(lookup)、确认型识别(recognition)、归类型识别(classification)、会话型识别(session)。⑥ 其中,目的越靠前,认定为公民个人信息的可能性越大;目的越靠后,认定为公民个人信息的可能性越小。刑法中的公民个人信息,应仅限于查找型识别的场景。例如,就单独的手机号码而言,陌生人可以利用手机号码与被害人进行对话以获得更多的信息,从而进行广告推销甚至诈骗。但是,陌生人难以利用单独的手机号码查找出特定的自然人。所以单独的手机号码,仅仅属于“会话型识别”信息,而非“查找型识别”信息,不应构成刑法中的公民个人信息。实践中多数判决也把单独的手机号码排除在公民个人信息的条数之外。2018年《检察机关指引》认为由公司购买、使用的手机号码不是公民个人信息,也是考虑该类手机号码能够查找到的主要是公司,而不是特定自然人。再如,利用cookie信息可以了解网络用户的检索记录、消费偏好、生活习惯、性别等,以至于可以对其进行大致归类。所以cookie信息只属于“归类型识别”信息,不足以实现查找特定自然人的目的,一般不应作为刑法中的公民个人信息。

2. 识别能力越强,界定为公民个人信息的可能性越大

对于部分信息,一般人可能缺乏识别能力,但是特殊职业的工作人员却具有识别能力。就孤立的手机号码而言,一般人可能无法依此识别特定自然人,但电信服务行业的工作人员却能轻易地查

---

①参见韩旭至:《个人信息概念的法教义学分析——个人信息概念的法教义学分析》,《重庆大学学报》(社会科学版)2018年第2期。

②参见齐爱民、张哲:《识别与再识别:个人信息的概念界定与立法选择》。

③参见喻海松编著:《实务刑法评注》,北京:北京大学出版社,2022年,第1061页。

④参见丁晓东:《论个人信息概念的不确定性及其法律应对》,《比较法研究》2022年第5期。

⑤H. Nissenbaum, “Privacy as contextual integrity”, *Washington Law Review*, Vol. 79, No. 1, 2004, pp. 119 – 157.

⑥参见R. Leenes, “Do they know me? Deconstructing identifiability”, *University of Ottawa Law & Technology Journal*, Vol. 4, No. 1&2, 2008, pp. 135 – 161.

找(识别)到特定自然人。就孤立的身份证号码而言,一般人同样难以通过一串数字识别特定自然人,但公安机关的工作人员、酒店服务行业的工作人员却具有识别能力。那么,对于这些信息,应该以谁的能力作为识别标准?“主观说”主张以行为人的识别能力为标准,“客观说”主张以社会一般人的识别能力为标准,折中说主张以任一主体的识别能力为标准。① 2015 年《刑法修正案(九)》颁布以前,侵犯公民个人信息罪的主体是特殊主体,即“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员”,采取的是以行为人识别能力为标准的“主观说”。《刑法修正案(九)》把侵犯公民个人信息罪的主体由特殊主体扩增为一般主体,因此,刑法中的公民个人信息也应采取以一般人识别能力为标准的“客观说”。

3. 识别后果越重,界定为公民个人信息的可能性越大

《个人信息刑事案件解释》把个人信息分为高度敏感信息、低度敏感信息和非敏感信息。这三类信息的私密性依次递减,社会性依次递增;同时,这三类信息对人身、财产安全的危险也依次递减。第一类信息处于个人最核心的私密领域,对人身、财产安全的危险最大;第二类信息处于中间层的私人领域,其私密性有所降低,社会性有所增加,对人身、财产安全的危险较大;第三类信息处于最外层的社会领域,其私密性最低,社会性最高,对人身、财产安全的危险相对较小。② 因此,信息的私密性越高,对人身、财产的危险越大,界定为公民个人信息的可能性越大;反之,信息的社会性越高,对人身、财产的危险越小,界定为公民个人信息的可能性越小。

4. 识别概率越高,界定为公民个人信息的可能性越大

如前所述,根据识别特定自然人概率的高低,可以把信息依次分为已识别信息、可识别信息、不可识别信息。其中,已识别信息属于个人信息,不可识别信息不属于个人信息。可识别信息内部也有识别概率高低的差异,越靠近“已识别”一端,需要结合的其他资料越少,识别概率越高,认定为公民个人信息的可能性越大。反之,越接近“不可识别”一端,需要结合的其他资料越多,识别概率越低,认定为公民个人信息的可能性越小。

三、刑法中敏感个人信息识别标准的确立

如前所述,个人相关信息分为已识别信息、可识别信息、不可识别信息三类。其中,已识别信息属于个人信息;不可识别信息不属于个人信息;可识别信息中有的属于个人信息,有的不属于个人信息。上文提出的识别个人信息的四条具体标准,旨在把个人信息与非个人信息区别开来。接下来面临的另一个问题是,个人信息又包括一般个人信息与敏感个人信息,敏感个人信息又包括高度敏感个人信息与低度敏感个人信息,刑法对一般个人信息、低度敏感信息、高度敏感信息分别规定了不同的立案标准。因此,需要在个人信息的识别标准之外,进一步研究敏感个人信息的识别标准。

从字面上来看,个人信息敏感与否,似乎是个人心理感受的问题。因此主观说认为,个人信息敏感与否应该以个人的主观反应为标准。③ 但我国的立法和司法解释并没有采取主观说,而是以个人信息所涉及的法益为标准来界定个人信息的敏感与否,实际上采取的是客观说。《个人信息保护法》第 28 条规定,敏感个人信息是指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,以及不满 14 周岁未成年人的个人信息。可见,《个人信息保护

①参见韩旭至:《个人信息概念的法教义学分析》。

②参见欧阳本祺:《侵犯公民个人信息罪的法益重构:从私法权利回归公法权利》,《比较法研究》2021 年第 3 期。

③参见宁园:《敏感个人信息的法律基准与范畴界定——以〈个人信息保护法〉第 28 条第 1 款为中心》,《比较法研究》2021 年第 5 期。

法》界定敏感信息的法益标准包括三类：人格尊严法益、人身财产安全法益、未成年人法益。对比《个人信息刑事案件解释》和《个人信息保护法》，可以发现有两个问题值得研究：一是刑法中的敏感信息是否应该与《个人信息保护法》中的敏感信息完全一致；二是刑法中的高度敏感信息与低度敏感信息如何区分。这两个问题的解决有赖于刑法中敏感个人信息识别标准的确立。

（一）刑法中敏感个人信息的识别标准应否与前置法相同

关于刑法中敏感个人信息的识别标准是否应该与《个人信息保护法》等前置法保持一致，我国学界存在同一标准说与独立标准说之分。同一标准说认为，关于敏感个人信息的识别标准，刑法应该与前置法保持一致。《个人信息保护法》依据法益的不同，把敏感信息分为三类。而《个人信息刑事案件解释》只承认前置法中的第二类敏感信息，这就会导致刑法与前置法的冲突。因此，应该修改刑法解释，扩大刑法中敏感信息的范围，即把前置法中的三类敏感信息，都作为刑法中的敏感信息。[①] 独立标准说认为，刑法与前置法的规范目的不同，刑法只承认《个人信息保护法》中的第二类敏感信息，具有合理性。[②] “没有必要过于追求不同立法中敏感个人信息的含义完全一致，这与法秩序统一性并不矛盾”。[③] 本文赞同独立标准说，理由如下：

1. 独立标准符合刑法的法益保护目的

目的是全部法律的创制者，每条法律规则的产生都源于一种目的。[④] 实际上，个人信息本身并无价值，使用才产生价值；同样，个人信息本身并无危险，使用才产生危险。[⑤] 因此，保护个人信息，并不是为了保护个人信息本身，而是为了保护个人信息背后的实体法益。个人信息是阻挡层法益，其他法益是背后层法益。立法区分敏感信息与非敏感一般信息的依据，不在阻挡层法益，而在背后层法益。不同的部门法因对背后层法益的保护立场不同，会对阻挡层个人信息采取不同的保护力度，并设置不同的敏感信息识别标准。例如，《个人信息保护法》的目的是规范信息处理活动，因此区分敏感信息与非敏感信息，是为了对敏感信息实行特殊的处理规则。[⑥]《民法》第1034条区分私密个人信息与非私密个人信息，是为了对私密个人信息进行隐私权的保护。再如，《汽车数据安全管理若干规定（试行）》对汽车数据中的敏感个人信息作了特别规定。《个人信息安全规范》更是把敏感个人信息分为五大类，50余种。这些部门规章和行业规范规定敏感个人信息的目的，主要是为了行政管理。那么，刑法是否应该像《个人信息保护法》一样，把涉及人格尊严的信息和涉及未成年人的信息都规定为敏感个人信息呢？本文对此持否定态度。

首先，人格尊严宽泛而模糊，无法作为刑法中敏感信息的识别标准。人格尊严既可以指基础性的价值原理，也可以指个别性权利。作为个别性权利的人格尊严，又包括广义、中义和狭义三种学说。广义上的人格尊严几乎无所不包，凡是涉及人的身体或者精神的权利或利益都可以称为人格尊严；中义上的人格尊严包括名誉权、荣誉权、姓名权、肖像权、隐私权、自我决定权等；狭义上的人格尊严，仅指侮辱、诽谤、诬告陷害所侵害的权益。[⑦]

刑法当然要保护人格尊严。从广义上来讲，刑法分则第四章中所有的侵犯公民人身权利、民主

---

①参见刘宪权：《敏感个人信息的刑法特殊保护研究》，《法学评论》2022年第3期；周光权：《侵犯公民个人信息罪的行为对象》，《清华法学》2021年第3期。

②参见喻海松：《“刑法先行”路径下侵犯公民个人信息罪犯罪圈的调适》。

③张勇：《敏感个人信息的公私法一体化保护》，《东方法学》2022年第1期。

④参见[美]E. 博登海默：《法理学：法哲学与法律方法》，邓正来译，北京：中国政法大学出版社，1999年，第109页。

⑤参见范为：《大数据时代个人信息定义的再审视》。

⑥《个人信息保护法》第1条规定，“为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，制定本法”。另外，该法第二章第二节规定了“敏感个人信息的处理规则”。

⑦参见林来梵：《宪法学讲义》，北京：清华大学出版社，2018年，第410—411页。

权利犯罪，都是在保护人格尊严；从狭义上来讲，侮辱罪、诽谤罪、诬告陷害罪、拐卖妇女儿童罪保护的是特定的人权尊严。当然，还有大量的人格尊严（如个人不受歧视和平等对待的人格权益）尚未被刑法类型化地予以保护。《刑法》与《个人信息保护法》的最大不同在于，《刑法》坚持罪刑法定原则，追求类型化和明确性，反对象征性立法。而《个人信息保护法》却保留有大量前瞻性和象征性的立法。将涉及人格尊严的个人信息规定为敏感信息，是《个人信息保护法》中明显的象征性立法。但是，以追求明确性为宿命的刑法，不可能以模糊的人格尊严为标准来界定敏感信息。

其次，未成年人的特殊法益，也无法作为刑法中敏感信息的识别标准。《个人信息保护法》之所以把未满14周岁未成年人的信息规定为敏感信息，目的是要求个人信息处理者制定专门的信息处理规则，并征得未成年人监护人的同意。而《刑法》只是在强奸罪、拐骗儿童罪、组织儿童乞讨罪、引诱幼女卖淫罪中规定了对未满14周岁未成年人的特殊保护。这些犯罪与未成年人个人信息之间并无直接的对应关系，即使把未成年个人信息作为敏感信息，也无法预防或者减少这些犯罪的发生。实际上，只有当个人信息事关个人的人身、财产安全时，刑法才有必要特殊对待，将其作为敏感个人信息。而这时的敏感信息，与被害人的年龄无关，而只与人身、财产法益有关。

总之，刑法保护个人信息是为了保护背后的其他法益，个人信息是阻挡层法益，其他法益是背后层法益。因此，当不存在背后层的核心和关键法益时，就不应该有阻挡层的敏感个人信息。按照这个逻辑，刑法只应该把危及人身、财产安全法益的个人信息规定为敏感信息，而不应该把模糊的人格尊严和特殊的未成年人法益作为敏感信息的识别标准。

2. 独立标准能够保持刑法的罪刑均衡

同一标准说认为，《个人信息保护法》把生物识别、宗教信仰列为敏感信息，利用生物识别信息可能构成侮辱罪、诈骗罪等，侵犯宗教信仰可能构成非法剥夺公民宗教信仰自由罪。因此，生物识别和宗教信仰也应该成为刑法中的敏感信息，而且是高度敏感信息，50条即构成犯罪。[①] 本文认为，生物识别只有在特定场景下才可以成为刑法中的敏感信息，而宗教信仰不能成为刑法中的敏感信息。

生物识别信息具有识别性，无疑属于刑法中的个人信息。但生物识别信息并非必然属于刑法中的敏感信息，只有当生物识别信息危害人身、财产安全时，才可以成为刑法中的敏感信息。换言之，生物识别信息能否成为刑法中的敏感信息，需要依据具体场景来认定。有的学者认为，用公众人物的人脸信息替换淫秽视频中的人脸信息，是对公众人物人格、名誉的极大侵害，因此人脸识别信息应当作为刑法中的高度敏感信息。[②] 首先需要明确的是，利用AI换脸技术侵犯他人名誉的行为，无疑可以构成诽谤罪；非法获取或者提供他人人脸信息的行为，无疑也可以构成侵犯公民个人信息罪。[③] 但是，AI换脸场景中的人脸信息不属于敏感个人信息。因为，人脸信息背后的法益是他人的名誉，换脸行为情节严重的构成诽谤罪，法定刑为3年以下有期徒刑或者拘役、管制。根据我国司法解释，利用换脸技术制作的淫秽视频只有被点击5000次或者转发500次才可能构成诽谤罪。而按照上述同一标准说，非法获取或者提供人脸信息，50条就可以构成侵犯公民个人信息罪，并且处3年以下有期徒刑或者拘役。这会导致明显的罪刑不均衡。因为预备行为实行化的犯罪（侵犯公民个人信息罪），处罚不应该重于实行犯（诽谤罪）。同样道理，非法剥夺公民宗教信仰自由罪的法定刑很轻，情节严重的才处2年以下有期徒刑或者拘役。如果按照前述同一标准说，非法获取或者提供50条宗教信仰信息，就构成侵犯公民个人信息罪，并且处3年以下有期徒刑或者拘役。这也会导致明显的罪刑倒挂。

---

①参见刘宪权：《敏感个人信息的刑法特殊保护研究》。

②参见刘宪权：《敏感个人信息的刑法特殊保护研究》。

③参见欧阳本祺、王兆利：《涉人脸识别行为刑法适用的边界》，《人民检察》2021年第13期。

（二）刑法中高度敏感信息与低度敏感信息的识别标准

《个人信息刑事案件解释》对敏感信息实行分级分类保护，即把敏感个人信息分为高度敏感信息与低度敏感信息，高度敏感信息50条构成犯罪，低度敏感信息500条构成犯罪。因此，探索刑法中高度敏感信息与低度敏感信息的识别标准具有重要的实践意义。这主要体现为以下两个问题。

1. 财产信息与交易信息的识别

根据司法解释，财产信息属于高度敏感信息；交易信息属于“其他可能影响财产安全”的低度敏感信息。实践中的识别难点为房产信息和车辆信息的属性认定。例如，关于小区的“业主姓名＋联系电话＋楼号＋房号＋建筑面积＋购房价格”等个人信息的属性，检察院一般认为是高度敏感信息，有的法院认定为高度敏感信息的财产信息，有的法院认定为低度敏感信息中的交易信息。① 再如，有的法院认为，“姓名＋电话＋车牌＋品牌＋颜色”信息属于高度敏感信息中的财产信息，而“姓名＋电话＋车牌”信息只属于低度敏感信息中的交易消息。② 那么，应该如何来识别财产信息与交易信息呢？有的学者认为，在难以区分的情况下，应该按照有利于被告人的原则来确定信息类型。③ 有的学者认为，应从实质上判断所涉信息是否危及人身、财产安全。④

本文认为，采用存疑有利于被告的原则可能值得商榷。因为存疑有利于被告人的原则只与事实之认定有关，而不适用于法律解释。因此，当法律适用有争议时，依法律解释之原则即使对被告应为不利之决定时，法院也应如此。⑤ 换言之，存疑有利于被告只适用于事实判断的场合，而不适用于价值判断的场合。对已经查明的个人信息，判断其是属于高度敏感信息还是低度敏感信息，原本是一个价值判断的问题，而不是事实判断的问题。因此，财产信息与交易信息的区分，无法适用有利于被告的原则，否则就会把所有信息认定为交易信息。

实质判断说基本是准确的。因为是否属于高度敏感信息，原本就是一个价值判断问题，只能从实质上判断该信息是否会高度危及人身、财产安全。问题是，信息是否会危及人身财产安全，与器物是否会危及人身财产安全的实质判断完全不同。例如，一般认为“凶器”，是指在性质上或者用法上足以杀伤他人的物品。某物品是否凶器，应该考虑几个方面的要素：物品杀伤机能的高低；物品供行凶的盖然性程度；物品对人的危险感程度；物品被携带的可能性大小。⑥ 可见，物品是否危害人身、财产安全，是从物品本身的不同角度来判断的。而个人信息是否危害人身、财产安全，无法单独从信息本身来判断；信息有利或者有害，主要不取决于信息本身，而取决于信息的使用者。因此，信息是否会高度危害人身、财产安全，主要应从使用人的角度来判断，而不能只从信息本身的角度来判断。大体上，需要考虑行为人非法获取或者提供个人信息的目的、时间、地点、人际关系等具体场景要素。例如，如果行为人获取房产信息只是为了推销家具，推销装修业务，一般不宜认定为财产信息，认定为交易信息即可。但如果行为人获取房产信息是为了诈骗、入户盗窃等目的，那么该房产信息就应该认定为高度敏感信息中的财产信息。同样道理，如果行为人获取车辆信息只是为了推销车辆保险等业务，那么车辆信息只能认定为交易信息。但如果行为人获取车辆信息是为了进行盗窃，那么该信息就应该认定为高度敏感信息中的财产信息。

---

①参见广西壮族自治区桂林市秀峰区人民法院（2019）桂0302刑初71号刑事判决书；山西省太原市中级人民法院（2020）晋01刑终247号刑事判决书。

②参见广东省中山市第一人民法院（2021）粤2071刑初1951号刑事判决书。

③周光权：《侵犯公民个人信息罪的行为对象》。

④参见喻海松：《“刑法先行”路径下侵犯公民个人信息罪犯罪圈的调适》。

⑤参见［德］Claus Roxin：《德国刑事诉讼法》，吴丽琪译，台北：三民书局，1998年，第145页。

⑥参见张明楷：《刑法学》，第1245页。

2. 行踪轨迹与交通信息的识别

根据《个人信息刑事案件解释》,行踪轨迹属于高度敏感信息;交通信息属于“其他可能影响人身、财产安全”的低度敏感信息。那么,应该如何来识别这两种不同的信息呢?羊某非法获取公民个人信息案集中反映了行踪轨迹和交通信息区分上的难点。在该案中,羊某非法获取的6383条公民个人机票信息记载了他人乘坐飞机的航班、时间、始发地、目的地等要素。检察院起诉书认为,这些机票信息属于高度敏感信息中的“行踪轨迹”;一审判决认为,这些机票信息不是高度敏感信息,也不是低度敏感信息,而属于非敏感的一般个人信息;二审判决认为,这些机票信息属于低度敏感信息。① 该案二审判决的意见,为司法实践的主流观点。② 与机票信息不同,车辆GPS定位信息、手机定位信息往往被认定为高度敏感信息中的行踪轨迹。③

可见,作为高度敏感信息的行踪轨迹与作为低度敏感信息的交通信息的识别标准,在于其对人身、财产安全的危害程度。而危害程度又取决于这些信息是否反映了他人的实时活动情况。申言之,反映实时活动情况的信息,对人身、财产安全具有高度危险性,应认定为高度敏感信息;反映过往活动情况的信息,对人身、财产安全的危险相对较小,应认定为低度敏感信息。

(**责任编辑**:邵泽斌)

On the Identification of Personal Information in Criminal Law

OUYANG Benqi

Abstract: “Identification” is the core and key element in the concept of personal information, serving as a link between the barrier layer of legal interests and the back layer of legal interests. The dilemma of identifying personal information in criminal law is reflected in the following three aspects: external identification, internal identification and systematic identification. The criteria for the identification of personal information should be established in conjunction with scenario theory. The clearer the purpose, stronger the ability, heavier the consequences, and higher the probability of identification, the greater the possibility of defining it as citizen personal information. Sensitive information in criminal law does not have to be subject to the same identification criteria as sensitive information in prior laws, and should be defined according to the degree of danger to the personal and property safety of the back layer of legal interests caused by the identification consequences.

Keywords: personal information; non-personal information; sensitive personal information; identification

About the authors: OUYANG Benqi, PhD in Law, is Professor and PhD Supervisor at School of Law, and Researcher at Institute for Human Rights, Southeast University (Nanjing 211189).

①参见海南省第二中级人民法院(2019)琼97刑终222号刑事判决书。

②参见海南省儋州市人民法院(2018)琼9003刑初242号刑事判决书;浙江省苍南县人民法院(2019)浙0327刑初655号刑事判决书;浙江省温州市中级人民法院(2019)浙03刑终1689号刑事判决书。

③参见2022年最高人民检察侵犯公民个人信息犯罪典型案例之四(陈某甲、于某、陈某乙侵犯公民个人信息案);江苏省盐城市亭湖区人民法院(2021)苏0902刑初301号刑事判决书;山东省沂水县人民法院(2020)鲁1323刑初122号刑事判决书;广东省广州市黄埔区人民法院(2019)粤0112刑初289号刑事判决书。