财经法学 No. 1，2022
pp. 45 - 61

论侵犯公民个人信息罪的司法适用误区及其匡正

郑朝旭*

内容提要：在目前的司法实践中，对公民个人信息的认定同时存在着内涵不清与外延不当扩张的缺陷，其根源在于未能充分认识到识别性标准与个人信息权对于判断公民个人信息所具有的重要作用。理论研究一方面对识别性的识别限度未予以足够的重视，另一方面则缺失对个人信息权之权利属性与构造的深入挖掘，以致无法为实务提供理想的操作方案与背书理由。应当在限定识别深度与明确个人信息权之权利内涵的基础上，采取由识别性至个人信息权的双重检视路径，将侵犯公民个人信息罪的适用范围限制在因非法出售、提供、获取具备识别性的信息而侵害公民个人信息权的场合。

关键词：公民个人信息　识别性　个人信息权　双重检视

一、侵犯公民个人信息罪的适用误区：识别限度与法益的缺位

因个人信息被不当获取、滥用、泄露所引发的侵害公民人身、财产安全的案件，已成为困扰我国社会稳定、公民安全的严峻问题，且呈现愈演愈烈的态势。〔1〕《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）的颁行，使得我国在个人信息保护的制度构建上开始告别分散立法模式，〔2〕保护个人信息的规范性文件之间各行其是甚至相互矛盾的态势在一定程度上得到了扭转。但《个人信息保护法》所界定的“个人信息”和规定的信息主体权利，与《中华人

* 郑朝旭，中国人民大学刑事法律科学研究中心博士研究生。

〔1〕 本文以“刑事案由”为方向、以“侵犯公民个人信息罪”为案由，在中国裁判文书网共搜得 9438 份判决书。其中，2015 年计 24 份判决书，2016 年计 398 份判决书，2017 年计 1376 份判决书，2018 年计 2350 份判决书，2019 年计 2748 份判决书，2020 年计 2373 份判决书，而 2021 年，截止到 3 月 18 日，已公布了 169 份判决书。参见 https://wenshu.court.gov.cn/website/wenshu/181217BMTKHNT2W0/index.html?pageId=e372b9fd7664d99785f7484ced8ec8e8&s8=02，最后访问时间：2021 年 3 月 18 日。

〔2〕 参见齐爱民：《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 177 - 184 页。

民共和国刑法》（以下简称《刑法》）第 253 条之一侵犯公民个人信息罪中的“公民个人信息”及该罪法益内涵，存在着语境和规范目的上的差异，若奉行“拿来主义”对于改善当前的司法现状可能并无裨益。在当前的司法实践中，从认定公民个人信息出发，论证涉案行为构成侵犯公民个人信息罪，依然存在着方法论与基本立场上的缺陷。

案例一：马某、刘某（均另案处理）雇佣被告人胡某、王某通过驾驶汽车与网络实时定位等方式对某机关领导所配专用公车进行跟踪，胡、王二人将目标车辆行驶的路线、停车地点进行记录，并将相关信息交给马某、刘某。法院经审理认为，胡某、王某构成侵犯公民个人信息罪。〔3〕

案例二：被告人张某等为实施网络诈骗活动，通过在网上获取的企业信息及法定代表人通讯录，假冒公司负责人要求财务人员将钱款汇入到其指定的银行账户。对检方所控告之侵犯公民个人信息罪，辩护人辩称，该案中的公司信息属于公开信息，不应被认定为公民个人信息。但法院以涉案信息可以被用来识别特定自然人的身份，足以威胁他人人身、财产安全为由，认定张某等构成本罪。〔4〕

从上述代表性案例的具体论证过程、判决理由来看，当前的判决存在着以下不足之处：其一，虽然“识别性”已成为判断公民个人信息的标准，但受制于对“识别性”概念及识别深度缺乏具体的阐释，法院在判决书中并未就涉案信息是否具备识别性或其识别深度进行论证。例如，案例一的核心争议即在于是否可依据行踪轨迹识别出被害人，但法院并未从正面给出行踪轨迹属于公民个人信息的理由，而是以行踪轨迹具有个人专属性、能够反映公民的某些个人特征、关乎公民生活安宁等非法收集信息所可能导致的危害后果这一角度来反证行踪轨迹属于公民个人信息。〔5〕其二，公开信息处于任何人皆可获取的状态，并不具有隐私性，收集、编辑公开信息的行为并不违法，〔6〕但对于后续的利用行为是否成立侵犯公民个人信息罪，以案例二为代表的判决既没有从构成要件的角度论证这些利用行为符合该罪的实行行为之特征，也没有说明这样的行为侵犯了本罪的什么法益，而是以该行为对他人的人身、财产安全具有危害性为由，进而认定为本罪。如此模糊处理争议点、回避问题的操作使得判决结论在教义学上遭遇巨大的质疑。其三，上述判决均存在的问题是，没有将公民个人信息的识别性特征与本罪的法益结合起来，进而导致在判决中要么以相关信息具备识别性从而顺理成章地侵犯了本罪的法益为由，认定构成犯罪，要么以被告人利用信息的行为已危害到被害人的人身、财产安全、必定侵害了本罪的法益为由，证明涉案信息具备识别性。但是，识别性本身只是对公民个人信息的判断，并不能理所当然地代替对本罪法益的判断；同样，本罪法益可以涵盖对犯罪对象、行为方式的解释，是否侵犯本罪法益，需要在明确法益内涵的基础上，检验涉案信息是否属于公民个人信息。一言以蔽之，识别性

〔3〕 参见最高人民法院刑事审判第一、二、三、四、五庭主办：《刑事审判参考》2014 年第 4 集（总第 99 集），法律出版社 2015 年版，第 53－56 页。

〔4〕 参见广西壮族自治区宾阳县人民法院（2018）桂 0126 刑初 486 号刑事判决书。

〔5〕 参见前引〔3〕，最高人民法院刑事审判第一、二、三、四、五庭主办书，第 55－56 页。

〔6〕 根据《个人信息保护法》第 13 条第 2 款的规定，原则上，处理个人信息需要取得信息主体的同意；但有第 13 条第 1 款第 2 项至第 7 项所列之情形（基本属于为履行法定职责、承担法定义务、维护公共利益以及个人自我决定）的，不需要取得信息主体的同意。其中，只是收集或者编辑已合法公开的个人信息属于第 13 条第 1 款第 6 项所列之情形。另外，根据该法第 27 条，单纯的收集、编辑行为也不构成对信息主体的权益有重大影响的行为，不需要取得信息主体的同意。即便在该法颁行之前，单纯收集、编辑自行公开的个人信息或者依法公开的个人信息的行为，既没有违背信息拥有主体的意愿，也没有利用这样的信息实施其他违法行为的，不构成对他人信息权利的侵犯。

与本罪法益之间存在着双向的互动关系。这是目前司法实践在论证中最为薄弱的环节，也是理论研究亟待深化的方向。

二、公民个人信息的法益：个人信息权的确证

（一）法益之争与评析

总体来说，关于该罪法益的讨论可区分为非人格权论的立场与人格权论的立场，前者以公民个人信息所蕴含的经济价值或社会秩序为基础，主张从财产利益、公共安全的视角解读本罪的法益，后者则以公民个人信息是公民人格权的延伸、侵犯公民个人信息的行为是对人格利益的妨害为总论点。不过，基于非人格权论立场所展开的财产权说、〔7〕公共信息安全说、〔8〕新型民事权利说〔9〕等，由于存在着与保护个人信息安全、刑法平等保护的价值理念背道而驰、〔10〕贬损公民个体的信息安全价值、以经验事实代替规范判断、〔11〕与侵犯公民个人信息罪的体系位置相冲突等缺陷，已渐渐退出了该罪法益之争的视野。因此，立足人格权论的立场形成了隐私权说、信息权说的论争。

1. 隐私权说容易导致本罪适用混乱

该说的特色在于，对公民个人信息的保护最终指向或涵盖对隐私权的保护。不过，在是否完全以隐私权建构本罪法益这一问题上，有的观点认为，本罪法益是公民的隐私权，只有体现个人隐私权的那一部分个人信息才属于刑法保护的对象，〔12〕且将本罪视为保护隐私权的条款也有助于填补《刑法》缺失公民个人隐私保护条款的漏洞〔13〕。另有观点则在承认本罪的法益是公民的信息权益的同时，又认为隐私权属于与信息权相并列的权益，进而二者共同构成本罪的法益，其代表性的见解认为，本罪的法益除了公民个人的信息权外，还包括个人隐私不受侵犯的权利。〔14〕

〔7〕 参见刘德良：《论个人信息的财产权保护》，载《法学研究》2007 年第 3 期；汤擎：《试论个人数据与相关的法律关系》，载《华东政法学院学报》2005 年第 5 期。

〔8〕 参见王肃之：《被害人教义学核心原则的发展——基于侵犯公民个人信息罪的反思》，载《政治与法律》2017 年第 10 期；张勇：《APP 个人信息的刑法保护：以知情同意为视角》，载《法学》2020 年第 8 期。

〔9〕 参见刘艳红：《民法编纂背景下侵犯公民个人信息罪的保护法益：信息自决权——以刑民一体化及〈民法总则〉第 111 条为视角》，载《浙江工商大学学报》2019 年第 6 期。

〔10〕 参见王利明：《论个人信息权在人格权法中的地位》，载《苏州大学学报（哲学社会科学版）》2012 年第 6 期。

〔11〕 虽然《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》（以下简称《解释》）第 5 条第 1 款对本罪的成立提出了信息数量的要求，但这是司法定量的惯性使然，且按照司法解释的规定，侵犯一位公民的信息安全达到入罪数量时，依然构成犯罪，这也是公共信息安全说难以解释的。

〔12〕 参见蔡军：《侵犯个人信息犯罪立法的理性分析——兼论对该罪立法的反思与展望》，载《现代法学》2010 年第 4 期。

〔13〕 参见王昭武、肖凯：《侵犯公民个人信息犯罪认定中的若干问题》，载《法学》2009 年第 12 期。

〔14〕 参见周光权：《刑法各论》，中国人民大学出版社 2016 年版，第 71 页（需要说明的是，周光权教授原先认为，侵犯公民个人信息罪在保护公民个人信息权之外，还保护个人隐私。但其在 2021 年版的《刑法各论》中，一方面将本罪的法益总括为“公民的个人信息自由决定权”，其中既保护公民对个人信息享有自由使用的权利，也保护个人隐私，这基本沿袭了其之前的立场；但另一方面，其还认为，本罪法益具有多重性，除了公民个人的信息自决权外，与个人信息相关联的（狭义的）社会管理秩序也是本罪的保护法益。这使得本罪的法益兼具非人格权论与人格权论的色彩，虽然有积极性、全面性地预防与惩治因个人信息侵权问题所引发的各类犯罪的现实背景与需求，但就观点本身而言，似乎使得本罪法益出现了超出其保护公民人格权利之内容的些许瑕疵，导致本罪法益“不堪重负”。参见周光权：《刑法各论》，中国人民大学出版社 2021 年版，第 78 页）；黎宏：《刑法学各论》，法律出版社 2016 年版，第 269 页；张明楷：《刑法学》（下），法律出版社 2016 年版，第 921 页。

首先，所谓个人信息，是指可以识别公民身份的信息，而非泛指一切与个人有关的信息，如此一来，所有可以识别个人身份的隐私当被涵盖在个人信息范围之内，将不具有识别性的隐私也纳入本罪的规制范围，将使得本罪的适用范围无限扩张。其次，即便认为《个人信息保护法》第 4 条第 1 款规定的是与公民个人“有关”的信息，且《个人信息保护法》第 28 条将宗教信仰、行踪轨迹等更应被纳入个人隐私的信息作为个人信息甚至是敏感个人信息而予以特别保护，也难以认为本罪的法益就是隐私权。这是因为，对于涉及侵犯个人隐私的行为，完全可以通过保护个人隐私的民事法律来规制，而且对于宗教信仰、行踪轨迹这类不以身份信息为背书的信息，通常都是在已知晓特定个人的情况下才能获取的信息，这就脱离了识别这一方法的范畴，将其纳入敏感个人信息之中，只不过是出于这类信息被非法获取或利用后可能产生严重后果的考虑而非其具有识别性。这样的外延扩张纵使在《个人信息保护法》中有其最大化保护公民个人信息的必要性，但在以刑罚为惩治手段的《刑法》中，若也通过严重后果来反向扩张个人信息的外延，有类推之嫌。况且根据《个人信息保护法》第 73 条第 4 项的规定，匿名化后的信息是无法识别个人身份且不能复原的信息，那么具备识别性的信息才可被匿名化，而对于一些原本就不具有识别性的信息，将其纳入个人信息之中，稍显矛盾。再次，信息主体积极参与各种活动所导致的信息社会化也使得该说无法涵盖侵害此类信息的行为，即便是不属于隐私的信息，若没有经过信息主体的同意，而非法获取、泄露、使用该信息，则依然成立本罪。最后，个人信息与个人隐私是两个不同的法律概念，前者关注的是对信息的利用，后者关注的是与人格尊严密切相关的私生活秘密是否遭到泄露，由此导致对二者的保护、利用、责任承担均会存在显著的差别，〔15〕故不宜将二者混同。

2. 信息权益说存在方法论与前提证立不足的缺陷

该说认为，随着公民个人信息概念的急剧扩张，其不仅具有人格权的性质，还兼具财产权、其他信息相关权利等内容，因此，若将公民个人信息的权利属性局限于纯粹的人格权、财产权或隐私权等权利内，既不利于充分保护公民个人信息之安全，也不符合法律、司法解释对公民个人信息范围的界定。此外，就回应公民个人信息的保护需求与实践而言，将公民个人信息提升至权利保护的高度，也有其必要性。〔16〕

该说的缺陷是：其一，在信息权益的证成方面存在方法论上的不足，刑法作为保障法，其本身并不能也不应创设某种权利与利益，即不能用法益本身来论证法益，否则即是循环论证；其二，虽然在侵犯公民个人信息安全的场合可能伴随着对公民人身安全、财产的侵害，但这是犯罪客观现象，现有的理论与法条都足以对其做到充分评价，且《刑法》将侵犯公民个人信息罪置于侵犯公民人身权利、民主权利罪之中，着眼于对公民人格权利的保护，但该说所确立的信息权益不同于纯粹的人格权与财产权，而是介于二者之间，以至要对侵犯公民个人信息罪进行重新定位，将部分行为解读为“预备行为实行化”，〔17〕这既与《刑法》存在抵牾，也存在权利属性暧昧

〔15〕 参见韩旭至：《个人信息与个人隐私的区分》，载《网络法律评论》2016 年第 2 期。
〔16〕 参见刘艳红：《侵犯公民个人信息罪法益：个人法益及新型权利之确证》，载《中国刑事法杂志》2019 年第 5 期。
〔17〕 参见于志刚：《“公民个人信息”的权利属性与刑法保护思路》，载《浙江社会科学》2017 年第 10 期

不清的嫌疑；其三，公民对个人信息享有的究竟是民事权利抑或仅仅是受保护的民事利益，这取决于对《中华人民共和国民法典》（以下简称《民法典》）第111条〔18〕的解释，民法学界也因此存在权利说〔19〕与利益说〔20〕之争，在缺乏对观点之争予以充分讨论的前提下径直得出信息权益的结论，缺失了论证的过程与充分的理由；其四，虽然《民法典》将公民个人信息置于第五章“民事权利”中，但并未将其明确规定为权利，且《民法典》是在具体人格权的规定（第110条〔21〕）之后，身份权、财产权（第112条至第132条）之前，对公民个人信息作出规定。因此，从体系解释的角度而言，也有学者认为立法者更倾向于将其作为一项需要保护的人格利益，这也可以从《民法典》第111条的后半句得到印证，因为其是从其他民事主体对自然人的个人信息负有保护义务的角度所作出的规定。〔22〕

综上所述，以人格权为核心主张本罪法益系隐私权或信息权益的各种学说的症结在于，要么因未厘清个人信息与个人隐私之间的关系，从而陷入看似全面保护个人信息、个人隐私，却实际上混淆了保护对象与法益之区分的局面，要么没能在区分一般人格权与具体人格权的基础上论证信息权益为何是一项新型的具体人格权，以致在说理上有所欠缺。

（二）本文观点：具体人格权视角下的个人信息权

1. 具体人格权视角的优势

首先，公民的个人信息不仅是受保护的民事利益，还具备民事权利的内涵，有着显著的民事权利属性。这具体体现在，第一，姓名、性别、年龄、民族、婚姻、住址、个人信用等个人信息都以自然人的真实存在为前提，且大多通过自然人的社会活动产生，每个自然人都是自身信息的主体，可禁止、排除他人对这些个人信息的非法收集、利用、泄露等行为，归结起来便是处于对自身信息的绝对控制地位，“对这些个人信息的控制，本身体现的就是一种私益，这是个人信息能够成为民事权益的根本原因”〔23〕。第二，个人信息不只有受到侵害后需要保护的一面，还存在着通过积极利用个人信息创造经济价值的一面，因而在利用的过程中，权利人当然可以就利用的限度、方式、价值分配、损害赔偿等提出自己的要求，这也是为何理论上将其纳入财产权保护的原因所在。事实上，在当前社会中对个人信息的利用已经是无可避免且必不可少的，正因如此，才更应在权利观念的基础上，追求对其的合理使用，如匿名化处理、中性使用公开信息、基于公

〔18〕《民法典》第111条规定：“自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”

〔19〕 参见杨立新：《个人信息：法益抑或民事权利——对〈民法总则〉第111条规定的“个人信息”之解读》，载《法学论坛》2018年第1期；王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

〔20〕 参见王利明主编：《中华人民共和国民法总则详解》（上），中国法制出版社2017年版，第465页；叶金强：《〈民法总则〉“民事权利章”的得与失》，载《中外法学》2017年第3期。不过，也有观点认为，无论是权利说还是利益说，都是试图以传统的民事权利话语体系来界定个人信息的保护，难以避免地导致了各种矛盾，而将个人信息控制权认定为一项新型的公法权利或许更加合理。参见周汉华：《个人信息保护的法律定位》，载《法商研究》2020年第3期。

〔21〕《民法典》第110条规定：“自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。法人、非法人组织享有名称权、名誉权和荣誉权。”

〔22〕 参见程啸：《民法典编纂视野下的个人信息保护》，载《中国法学》2019年第4期；程啸：《论我国民法典中个人信息权益的性质》，载《政治与法律》2020年第8期。

〔23〕 前引〔10〕，王利明文，第69页。

共利益的有限使用等。〔24〕此外，相比于民事利益的设定，作为民事权利的个人信息权还存在着抗衡公权力不当利用、给受害人提供充分保护、为其他法律保护奠定基础、与其他保护机制相衔接和补充等优势。〔25〕

其次，将公民个人信息的法益定位于民事权利，存在着一般人格权与具体人格权两条路径。虽然站在一般人格权的层面建构个人信息权有高屋建瓴之效，但其本身内容的模糊性并不利于对本罪构成要件的解释。一般人格权是相对于具体人格权而言的，具体而言，一般人格权以人格尊严、人格平等、人格自由为内容，是具有高度概括性和权利集合性特点的权利。〔26〕具体人格权则以特定的人格利益为内容，具有明确的构成要件与救济手段。相较而言，一般人格权虽然以保护人的自由发展为核心价值理念，将人格尊严、人格平等、人格自由作为框架，能结合案件的实际情况，通过解释予以适用，但由于欠缺明确的构成要件，与其认为它是一项权利，不如说它提供了对具体人格权之创造、解释的价值指引功能。如果将公民个人信息视为一项一般人格权，极易导致在个案裁判中过于依赖裁判者个人的价值取舍与利益衡量，再考虑到在收集、利用公民个人信息的场合常存在着诸如集体法益与个人法益、人格自由与社会防卫等冲突，因此必然使得这样的价值判断与利益衡量不具有客观性与合理性。〔27〕

最后，以一般人格权作为公民个人信息的权利本质，即便肯定其对于保护人格尊严、人格平等、人格自由方面具有相比于具体人格权更为宽广的适用范围，但这正是该种观点最为致命之处。具体而言，第一，只有在具体人格权缺位或无法涵盖相应客体的场合，才考虑以一般人格权的价值理念来弥补具体人格权的有限性。然而，个人信息权以识别性信息为内容，由公民自身控制，禁止任何对其的非法收集、利用、泄露，否则需承担相应的法律责任，就此而言，个人信息权具备明确的构成要件与救济手段，不存在适用一般人格权填补漏洞的空间。第二，且不论前述的财产权、隐私权、信息权益等观点周延与否，就保护的路径而言，论者们均是在财产权、人格权的角度展开己见，这也从侧面说明，现有的民事权利类型已足以涵盖对公民个人信息的保护，只不过存在着因公民个人信息内容繁杂、价值多样而导致的保护取向偏差。第三，公民个人信息这一概念的最大问题在于，缺失对“识别性”的限定导致其外延不断扩张，若以同样抽象的一般人格权作为权利本质诠释个人信息权，其结果便是公民个人信息变得更加抽象与不确定，对公民个人信息的认定会陷入“公说公有理，婆说婆有理”的困境。

2. 个人信息权的法益构造：信息控制权与信息利用权

作为一项具体人格权，根据《个人信息保护法》第 44 条的规定，个人信息权由知情权与控制权构成，第 45 条至第 50 条对控制权的具体权能予以了展开，例如查阅、复制、更正、补充、删除等。就《刑法》第 253 条之一而言，其规制的是非法出售、提供及获取公民个人信息的行

〔24〕 参见刘艳红：《公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角》，载《法学论坛》2020 年第 2 期。

〔25〕 参见前引〔10〕，王利明文。

〔26〕 参见王利明：《人格权法研究》，中国人民大学出版社 2012 年版，第 147 页。

〔27〕 参见杨惟钦：《个人信息权之私权属性与内涵思辨——以实现个人信息权益的合理保护为视角》，载《晋阳学刊》2019 年第 2 期。

为，因此，本文认为，应当结合该罪的实行行为来理解个人信息权的法益构造。具体而言，包括以下两个方面：

其一，信息控制权，即权利主体对自我信息的控制与排除他人非法获取的权利。虽然公民个人信息不是以有体物的形式存在，无法对其进行物理上的占有与支配，但这并不意味着信息主体无法对其进行控制，相反，信息主体的地位使其实现了对公民个人信息的法律控制。这种控制意味着，除了《个人信息保护法》第13条第1款所规定的例外情形，信息主体的同意或授权是其他组织或个人收集与利用个人信息的必要前提。况且，依据公共利益所收集的个人信息也仅限于在特定的方面或特定的目的下使用，而不得随意向任何人透露甚至公开。当然，针对信息主体的同意究竟在多大程度能发挥其作为合法化事由的效力及是否有必要维持此种知情同意的架构，存在着不少质疑。例如，有观点认为，以同意作为个人信息的保护架构已过时且无益，理由在于许多人并不会认真阅读关于个人信息的隐私声明，或为使用产品、服务而被迫同意，抑或对个人信息被收集的事实并不知情，难以及时行使权利进行救济；〔28〕还有观点认为，同意原则作为犯罪阻却事由存在着难以求知真实意愿及不确定等缺陷，进而主张在涉及公共利益时以比例原则作为收集、利用公民个人信息的正当性基础〔29〕。本文认为，公民个人信息可被视为公民人格尊严的表征之一，以同意原则作为收集、利用个人信息的合法化事由是对公民人格尊严、自由的尊重和保障。尽管在实践中出现基于防控疫情或社会安定的需要，而未能充分征得公民同意即收集其个人信息的情况，但这不是同意原则本身所引发的缺陷，而是法律体系完善与执法文明的问题。换言之，“法律不能以个人信息用户行使权利困难为由，虚置或抛弃个人信息知情同意的基本原则”〔30〕。因此，解决问题的理想方案并不是否定或者弱化同意作为个人信息保护的合法性与正当性基础，而是应当通过构建更为精细、清晰的同意规则来协调个人信息保护与利用上的冲突，例如从同意的形式到实质加强对同意的审查。〔31〕而且在《个人信息保护法》中，信息主体的同意得到了进一步的强调，例如该法第15条、第16条即明确了信息主体可拒绝或撤回其所作出的同意，第17条也要求信息处理者必须以显著方式、清晰易懂的语言真实、准确、完整地向信息主体告知信息处理事项，且针对当前许多并不需要以个人信息作为使用该产品或服务的条件的应用程序，其中的“不同意隐私条款即不可使用本产品或服务”条款违反了该法第16条的规定。至于以比例原则作为收集、使用公民个人信息的正当化根据，这在《个人信息保护法》中也得到了确证，但其本身是利益衡量的产物，且也仅适用于维护公共利益的场合，并不是降低同意作为处理个人信息的终极原则之地位的理由。

其二，信息利用权，即信息主体决定是否使用个人信息及如何使用的权利。应当说，从《个人信息保护法》的控制权角度而言，其包含了如何利用个人信息的内涵，只不过出于具体化法益

〔28〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016年第5期。

〔29〕 参见江海洋：《论疫情背景下个人信息保护——以比例原则为视角》，载《中国政法大学学报》2020年第4期。

〔30〕 叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018年第5期，第154页。

〔31〕 参见陆青：《个人信息保护中“同意”规则的规范构造》，载《武汉大学学报（哲学社会科学版）》2019年第5期。

的考虑，本文将其中的利用权能予以单独、特别地解释。随着信息时代的发展，公民个人信息已经成为一项具有丰富价值的社会资源，由此催生出基于各种目的的利用方式。根据《个人信息保护法》第 1 条的规定，制定该法的目的之一即在于“促进个人信息合理利用”，同时该法第 10 条禁止的是非法处理个人信息的行为，而依法利用个人信息的行为受法律保护。既然信息利用权是公民个人所享有的人格权，那么对公民个人信息的利用必须由信息主体决定，这是民事权利的应有之义。公民个人无疑可以在遵守法律的前提下，对本人信息予以利用，包括公开信息、编辑个人信息等；信息主体也可以授权或同意他人基于合法目的将其个人信息运用于商业、公益等活动，例如，实践中常见的通信运营商根据用户协议收集用户个人信息，并将之用于改善用户体验等情形。因此，由公民的信息利用权所引申出来的当然结论是，即便公民自行决定公开个人信息，或同意、授权其他组织、个人获取其个人信息，甚至政府基于公共利益公开公民个人信息，虽然取得公民个人信息的行为并不违法，但若未就利用公民个人信息取得相关权利主体的同意，依然属于侵权（犯罪）行为。例如，《个人信息保护法》第 24 条禁止利用个人信息在交易中实施差别化待遇，第 26 条也规定出于维护公共安全所收集的个人信息仅限用于维护公共安全的目的，第 27 条虽然支持合法处理公开信息的情形，但是如果这些处理行为对个人权益有重大影响，也应当另行取得信息主体的同意，而且在该法第 29 条进一步重申或加强了对信息利用的事先同意。因此，就侵犯公民个人信息罪而言，将收集或编辑后的公开信息予以非法出售、提供的，才属于本罪之中的非法利用情形。

三、识别性：模式选择、必要性与限制

《刑法》本身并没有对“公民个人信息”这一构成要件作出明确的规定，这导致对“公民个人信息”的认定需要结合相应的前置法来判断。虽然许多规范性文件已将“识别性”作为认定公民个人信息的核心标准，但其内涵与限度并不明确，以致在司法实践中对“公民个人信息”的认定相当恣意。此外，还存在着放弃“识别性”标准的见解与规定，对这些见解与规定又该如何看待？是否还有必要维持其核心标准的地位？对其限度又该如何限制？

（一）识别模式的选择

大体上，我国的规范性文件对公民个人信息的定义模式经历了由混合模式到识别模式的转变。

1. 混合模式。起先，《全国人民代表大会常务委员会关于加强网络信息保护的决定》（以下简称《决定》）第 1 条〔32〕提出认定公民个人信息的两个要点，即识别性与隐私性。换言之，能够识别公民个人身份和暴露公民个人隐私的信息才能被纳入公民个人信息的范围（混合模式）。随后，紧接着《决定》出台的《关于依法惩处侵害公民个人信息犯罪活动的通知》（以下简称

〔32〕《决定》第 1 条规定：“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。任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。”

《通知》）第2条〔33〕基本沿袭了《决定》判断公民个人信息的两项标准，并没有就“识别性”的概念与范围作出明确定义，而且《通知》突破了《决定》针对公民个人信息进行保护的立场，将“数据资料”也纳入公民个人信息的范畴。应当说，单个的、零星的个人数据并不成为信息，只有经过数据处理后，其所蕴含的信息价值才会有所增长，进而可能形成个人信息，由此才能提供可识别性的内容。换言之，个人数据“可以”但不“必然”是个人信息的形式，个人信息也“可以”但不“必然”是个人数据所反映的内容。〔34〕因此，区分信息内容与信息载体的意义，更多在于对犯罪对象的法律识别，对二者的区分需要根据较为客观的技术标准来判断，而不必考虑信息载体与信息主体之间的联系。〔35〕

2. 识别模式。与《决定》《通知》所采取的混合模式不同，《中华人民共和国网络安全法》（以下简称《网络安全法》）第76条第5项、〔36〕《民法典》第1034条第2款〔37〕与《解释》第1条〔38〕未将公民个人信息与个人隐私相并列规定，而是直接对公民个人信息作了定义，采用“概括＋列举”的方式初步明确了公民个人信息的内涵与外延，并将识别性标准细化为单独识别与结合识别两种方式。

3. 第三条路径：识别性舍弃论。就《个人信息保护法》第4条第1款相比于前述的规范性文件针对个人信息的定义而言，存在着极为扩张个人信息外延的一面。虽然《决定》《通知》也将个人隐私纳入个人信息的范围，但却是通过“识别性”与“隐私性”相并列的方式展现的，最少在表面上保持了二者的区别，但《个人信息保护法》在判断某项信息是否属于个人信息时，只要是“与自然人有关”的各种信息都属于个人信息，即该信息与自然人“有关”即可，如此一来，即便该条款中存在着“识别”二字，也可以说是放弃了“识别性”的要求。这样的条文设计虽然在侵权案件中可以大大降低甄别个人信息的难度，为被侵权者提供较为充分的保护，在我国信息侵权形势较为严峻的当下有着巨大的法律价值和实践意义，但如果对侵犯公民个人信息罪中的“公民个人信息”也作此安排或理解，则无疑使得本罪的适用范围被无限扩张。例如，按照这样的理解，偷拍裙底这样的行为属于获取“与已识别的自然人有关的信息”，从而构成本罪。因此，将识别公民身份的信息置换为与自然人相关的个人信息，这导致该概念的适用空间极为巨大，以致刑事法网过于扩张。而且匿名的状态是相对的，在大数据技术下完全存在着被

〔33〕《通知》第2条规定：“……公民个人信息包括公民的姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历、家庭住址、电话号码等能够识别公民个人身份或者涉及公民隐私的信息、数据资料。……”

〔34〕参见周斯佳：《个人数据权与个人信息权关系的厘清》，载《华东政法大学学报》2020年第2期；王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

〔35〕参见岳林：《超越身份识别标准——从侵犯公民个人信息罪出发》，载《法律适用》2018年第7期。

〔36〕《网络安全法》第76条第5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。”

〔37〕《民法典》第1034条第2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。”

〔38〕《解释》第1条规定：“……（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。”

破解的风险，即匿名化处理后的个人信息依然存在着被再识别的风险，将其排除在个人信息的范围外，不具有合理性。有鉴于此，本文认为，必须在与识别模式保持一致的前提下，对《个人信息保护法》所规定的“个人信息”在《刑法》第 253 条之一的适用中进行目的性限缩，只将其中具备识别性的信息纳入规制范围。这既避免了规范上的条文冲突，也给刑事制裁、行政处罚、民事侵权诉讼各自留下了必要的适用空间。所以，第三条路径在刑事层面上是不应当得到承认的。

我国关于公民个人信息的定义模式经历了混合模式到识别模式的转变。但是，这一定义模式只不过解决了认定公民个人信息判断方向上的问题，就识别的程度或范围而言，任何规范性文件都未就“识别性”作进一步解释或规范，由此导致司法者在判断某些信息是否属于公民个人信息时，需首先定义“识别性”。但就公布的判决书来看，几乎都未涉及对“识别性”的解释，仅简单地以“涉案信息可反映公民的某些特征”等为由径直得出犯罪成立的结论，故稍显语焉不详、论证粗糙。〔39〕由此，需要进一步回答的问题是，虽然判决回避了对识别性的考察，但从全面保护个人信息的立场出发，是否需要在公民个人信息中保持“识别性”及如何限定识别深度。

（二）保持“识别性”标准的必要性

识别性是否属于公民个人信息的题中应有之义？换言之，识别性是判断公民个人信息的附加性要求，还是其本身即为公民个人信息的本质特征。若持前者的观点，则可能基于扩大公民个人信息认定范围的立场，否认识别性存在的必要性，也即前文所称的“识别性舍弃论”。除了《个人信息保护法》第 4 条第 1 款所提供的法条根据外，理论上也存在着这样的见解。例如，有观点认为，由于《刑法》并未针对个人隐私设置保护规范，出于弥补处罚漏洞的需要，应当放弃对公民个人信息附加识别性的要求，还其本来面目，即侵犯公民个人信息罪的法益是个人信息权，此处的个人信息既包括身份信息又包括隐私信息，识别性只是身份信息的必备特征，在隐私信息中则无其存在的余地，如此一来，非法出售、提供、收集隐私信息的行为亦应以侵犯公民个人信息罪论处。〔40〕

本文认为，识别性舍弃论的观点存在着可商榷的余地。其一，公民个人信息不同于与公民个人有关的信息，〔41〕前者仅指可以识别公民个人身份的信息，后者则是指一切与公民相关的、反映公民之存在的信息，其范围极为广泛，无论是否具备隐私性、是否可以识别个人身份，都可被纳入其中，可见将不具备识别性的个人隐私解释为公民个人信息，并不符合公民个人信息的本意，且有为了论证自身预设的观点而牵强地解释法条用语的嫌疑。其二，既认为本罪的法益是公民个人对信息的自我决定权，又进一步舍弃了识别性的标准，则侵犯任何与公民个人相关的信息

〔39〕 本文以“刑事案由”为方向、以“侵犯公民个人信息罪”为案由，在中国裁判文书网共搜得 9438 份判决书，再以“识别”为关键词对这些判决书进行筛选，共得 934 份判决书，即大约仅有 9.90％的判决书涉及对身份识别的说理。但深究发现，其中要么是对立法规定、司法解释关于公民个人信息之定义的表述，如江西省兴国县人民法院（2019）赣 0732 刑初 202 号刑事判决书，要么只是在阐述某项信息属于公民个人信息时作为结论性表述使用，如江苏省苏州市中级人民法院（2019）苏 05 刑终 488 号刑事判决书。

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

〔41〕 参见周光权：《侵犯公民个人信息罪的行为对象》，载《清华法学》2021 年第 3 期。

都属于侵犯了本罪法益。虽然在扩张本罪处罚范围的立场上可谓一以贯之，但将诸如不具备识别性的个人隐私等与公民个人相关的信息都纳入公民个人信息的范围，必定导致本罪适用范围的极度膨胀，从而使得本罪成为一切与个人信息相关之犯罪的兜底条款。其三，个人隐私常常与公民的个人关键信息密切相关，且大多包含着有关公民的人身安全、财产安全的信息，明显应当给予更为严格的保护，将其排除在公民个人信息的范围外，似有立法缺陷之嫌。但是，既然认为个人隐私与个人信息密切相关，那么将可以识别个人身份的个人隐私纳入个人信息的范围内，自然不存在解释上的障碍，且这样的解释并非扩大解释，而是个人信息的应有之义。即便认为个人隐私与个人信息有别，那么基于识别性判断标准，对于无法识别个人身份，亦无法威胁到人身安全、财产安全的个人隐私而言，其自始至终便不在本罪的保护范围之内，也就谈不上立法缺陷。况且就保护公民个人信息的旨趣与保护公民隐私的旨趣而言，二者亦有所区别：在当前的数字经济时代，公民个人信息具有巨大的经济价值，因此法律注重的是规范公民个人信息的收集、利用等行为；而对于隐私而言，法律则关注的是保护此类信息不被非法披露或公开。因此，对公民个人信息的保护不能也不宜采取与传统隐私权相同的方式，那么对个人信息的界定则应与个人隐私有所区别。〔42〕其四，以刑事政策上的处罚必要性来论证对个人隐私的全面保护，也会遭到刑法谦抑性的质疑，即在尚未穷尽行政规制措施与民事救济手段的情况下，径直对收集、出售或提供不具备识别性的个人隐私的行为予以刑事处罚，未免操之过急。因此，识别性作为公民个人信息的本质特征，仍有其理论意义与实践价值。

（三）对识别深度的限制

侵犯公民个人信息罪的重点是判断某项信息是否具备识别性，而就判断的方法或路径而言，可从以下两个方面展开：一是识别，即基于信息来识别特定个人身份；二是关联，即在已知特定个人的情况下判断某项信息是否有助于识别出该人。上述两种路径之间并不是互相独立或毫无关系的，事实上，在一些情形中，通常都需要将两种路径结合起来判断某项信息是否属于公民个人信息。〔43〕但是，特别需要强调的是，在利用关联方法的场合，不能因为已知特定个人，进而先入为主地将涉案信息认定为公民个人信息，必须站在事前的立场，基于当时的技术条件、行为人的认识能力来判断这些信息是否有助于识别特定个人身份。

识别性信息包含直接识别（单独识别）与间接识别（结合识别）两大类信息。顾名思义，前者是指某项信息单独即可识别出公民个人身份，如身份证号；后者是指某项信息必须与其他信息结合在一起后方能识别出公民个人身份，如重名是司空见惯的现象，依据姓名尚不能识别公民个人身份，但若将其与出生年月日、家庭住址、工作单位、职务等信息结合在一起后便能实现对公民身份的识别。在大数据时代，能直接（单独）识别出特定个人的信息自不待言，即便是一些非常边缘的信息，一旦被结合起来依然可以识别出特定个人，由此导致几乎所有与个人相关的信息

〔42〕 参见田宏杰：《窃取 APP 里个人信息的性质认定——兼及个人信息与个人隐私之界分》，载《人民检察》2018 年第 7 期。

〔43〕 例如，有观点认为，关联是识别的前提阶段，关联是可识别的决定因素，即先判断涉及个人信息的要素是否与信息主体存在关联，而后再根据具体场景判断是否达到了“可识别”的程度。参见商希雪：《个人信息隐私利益与自决利益的权利实现路径》，载《法律科学（西北政法大学学报）》2020 年第 3 期。

都可以借助“识别性”被纳入公民个人信息的范围，但如此扩张的信息范围自然面临着刑事法网过分严密的诘难。例如，有观点指出，间接识别这一方法看似最大限度地保护公民个人信息，但实际上是将公民个人信息置于动态化和场景化的危险之中，且适用间接识别时还将遭遇以何种知识水平的人为认定标准，以及是否对能用来判断公民个人信息的资料予以限制的问题。〔44〕破解这一困境的最有效路径便是对“识别性”的深度进行限定。对此，理论上存在以下观点。一种观点认为，判断相关信息是否属于公民个人信息时，可以从信息的重要程度、需要结合其他信息的程度、行为人主观目的三个方面考察。〔45〕另一种观点认为，即便间接（结合）识别类信息可以被用来识别特定个人，但如果其与国家认证身份之间的关联异常遥远，则没有必要将其纳入公民个人信息的范围。〔46〕

总体而言，上述观点都存在值得商榷的余地。第一种观点的问题在于，各个要素之间并不存在先后位次或内在逻辑，以致考虑的要素越多，越会造成要素之间取舍的困难。例如，行为人的主观目的并非指向识别特定个人，但该信息又很重要，此时，是否应将该信息纳入“公民个人信息”的范畴呢？该观点的初衷是通过考察信息的客观价值、主观用途来限定“识别性”的识别深度，但这样主客观混杂的方案在现代大数据技术的冲击下，可能无法达到论者所预期的效果。第二种观点将公民个人信息同国家认证身份结合起来的思路具有启发性，但其问题在于如何判断一项信息与国家认证身份之间的关联异常遥远。

本文认为，对识别深度应做以下几点限制。其一，公民个人身份信息并不限于国家认证身份，对于一些虽不是由国家赋予但在特定领域内具备识别特定个人身份效果的信息，依然具有保护的必要性。例如，学号是每个学校为在该校就读的学生所编制的号码，其本身不一定属于国家认证的身份，也无法单独识别特定个人，但若将其与学校结合起来，即可确定到特定个人。其二，概念本身的模糊性虽然确实导致公民个人信息的范围不断扩张，但必须承认的是，大数据技术的进步、信息社会的发展同样是造成这一局面的原因。因此，在判断某项信息是否属于公民个人信息时，应当考虑行为时的方法、技术是否可以通过该信息识别出特定个人。换言之，识别具有相对性，应当结合行为人的识别能力、技术方法等进行综合判断。其三，某项信息与公民身份之间的关联是否遥远，取决于该信息是否包含涉及公民身份的因素。详言之，对于行为人来说，其最终需要的是可以识别特定个人身份的信息，其他一些信息即便对此有所助益，但若本身无法指向特定个人，则不能被纳入公民个人信息的范围。同样的，对于司法人员来说，其也需要对涉案的信息进行甄别，从中区分出哪些属于公民个人信息、哪些不属于公民个人信息。例如，病床号、用药情况虽然可以通过结合姓名、身份证号等精确定位公民个人，但其自身并不包含任何涉及公民身份的因素，至多只是一项辅助判断的信息。〔47〕因此，最为重要的问题是，如何将这种辅助信息与公民个人信息区分开来。本文认为，直接（单独）识别类信息由于具有较强的识别

〔44〕 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》，载《重庆大学学报（社会科学版）》2018 年第 2 期。

〔45〕 参见喻海松：《侵犯公民个人信息罪司法适用探微》，载《中国应用法学》2017 年第 4 期。

〔46〕 参见岳林：《超越身份识别标准——从侵犯公民个人信息罪出发》，载《法律适用》2018 年第 7 期。

〔47〕 参见喻海松：《侵犯公民个人信息罪的司法适用态势与争议焦点探析》，载《法律适用》2018 年第 7 期。

性，故一般较为稳定，能够清晰地与间接识别类信息、辅助信息区分开来；但是，间接识别类信息是通过各项信息之间的相互印证来识别出特定个人身份，其与辅助信息之间的界限较为模糊，所以辅助信息与识别类信息的区分才是重点。辅助信息与间接识别类信息之间最为关键的区别在于是否具有身份指向性。所谓身份指向性，是指某项信息需要以公民的个人信息为背书或需要公民的个人信息为条件产生某项信息，如此一来，辅助信息所包含的信息只不过反映了自然人的活动轨迹或存在，如通话记录、行动轨迹等。相反，间接识别类信息则可以基于与其他信息（不论是辅助信息还是其余的间接识别类信息）的结合来识别出特定个人的身份，如在现今实名制要求下的微博账号等。

四、识别性与个人信息权的双重检视

就目前的司法实践而言，对识别性的适用缺乏深刻的认识导致常常出现以行为妨害了公民个人隐私、生活安宁、公共安全等利益来反证涉案信息属于公民个人信息的论证路径，或者在确认相关信息属于公民个人信息的情况下，径直地得出行为人构成侵犯公民个人信息罪的结论，而并未考虑是否存在法益受到侵害的事实。此外，学界也对识别性与个人信息权在实际案件的适用中的关系没有给予足够的关注，难以为司法实务提供成熟、充分的理论指导。本文认为，识别性与个人信息权对判断相关行为是否构成侵犯公民个人信息罪发挥着不可替代、相辅相成的作用。就具体的适用而言，需要考虑以下两个方面：一方面，虽然个人信息权作为本罪的法益，对构成要件的解释具有方向性的指引作用，但也需要警惕以法益侵害反证客观行为之危害的倾向，故对侵犯公民个人信息罪的认定而言，不能因为确认相关行为侵犯了本罪法益，便径直地将所有的涉案信息认定为公民个人信息；另一方面，以识别性为标准确定了涉案信息属于公民个人信息之后，尚需进一步检验相关行为是否侵害了个人信息权，换言之，识别性的价值仅在于判断某项信息是否属于公民个人信息，而是否成立侵犯公民个人信息罪尚需在此基础上进一步结合本罪的其他主客观要件予以考量。

（一）坚持对“识别性”的优先判断

如前所述，目前实务对将识别性与个人信息权结合起来运用在侵犯公民个人信息罪之证立上的重视不足，且呈现出立场不一、论证粗糙、逻辑混乱的倾向。例如，在案例一中，法院的审判逻辑是，跟踪车辆、利用工具对手机进行实时定位等行为所获取的行动轨迹具有个人专属性，且侵犯了公民的隐私与生活安宁，所以被害人的行动轨迹便属于公民个人信息。〔48〕不难看出，法院在审理该案时并没有从正面定义何为公民个人信息，然后据此论证行动轨迹是否属于公民个人信息，而是以行动轨迹反映公民个人的社会活动及一旦暴露会危及公民的生活安宁等危害后果来反证其属于公民个人信息。且不说是否要以识别性为标准将不具有识别性的个人信息排除在外，这种以“危害结果补充行为不法”的司法操作必然导致任何信息都可以借助危害后果被纳入公民

〔48〕 参见前引〔3〕，最高人民法院刑事审判第一、二、三、四、五庭主办书，第55－56页。

个人信息的范围，由此使得本罪的公民个人信息丧失单独判断的意义。此外，虽然存在着像陈明侵犯公民个人信息罪案〔49〕那样尝试从正面认定涉案信息的判例，但遗憾的是，法院并未坚定地贯彻识别性标准，舍弃了对邮箱的账号和密码具备可识别性的论证，而是以邮件内容可以反映用户的活动情况来反推邮箱的账号和密码属于公民个人信息，由此导致判决立场模棱两可、论证思路自相矛盾。既然能够通过邮箱的账号和密码识别出公民个人身份，则完全满足了识别性的要求，可以确认邮箱的账号和密码属于公民个人信息，且判断的对象是邮箱的账号和密码本身，应围绕账号和密码是否具备识别性展开，而不能以邮件来证成账号和密码具有识别性，否则便偏离了判断的基准。

另一种情况是，在依据部分涉案信息即可认定犯罪成立的前提下，将全部涉案信息认定为公民个人信息。换言之，以个人信息权遭受侵害为前提代替或舍弃了对全部涉案信息的再次判断，如通话记录、行踪轨迹等信息，其本身难言包含着识别性信息，以犯罪成立为前提将其理所当然地纳入犯罪对象的范围，明显不当，赵某某侵犯公民个人信息罪案〔50〕即是适例。该案涉及的公民个人信息种类较多，其中如车辆信息、征信、住宿等信息由于记载有公民的身份信息，故将其纳入公民个人信息的范围并无问题，但对于行踪轨迹、通话记录等信息为何具备识别性进而可被纳入公民个人信息的范围，法院在判决中并未言及。由此可见，实践所暴露出的问题并非可以仅通过强调贯彻或细化操作标准、补充论证解决的，而是需要审视识别性与个人信息权之间的适用逻辑、互动关系，以二者的双重验证解决涉案信息判断和罪名成立上的反证操作、逻辑矛盾等问题。

只有具备识别性的个人信息才会侵害公民的个人信息权，因此，对任何一起侵犯公民个人信息的案件来说，首先需要判断的是，涉案信息是否具备识别性。如果从一开始即以行为人主观上具有侵犯他人个人信息权的故意，且客观行为对他人的生活、安全产生不良影响等为由，认定行为人所获取的信息属于公民个人信息，则几乎可以在任何案件里得出行为人构成犯罪的结论。认定犯罪成立的合理路径当是，优先判断客观上是否存在侵害或危及法益的实行行为，这既有利于规制故意的认识对象、明确过失的认识能力标准，也有助于避免主客观混合判断所导致的主观归罪倾向。就侵犯公民个人信息罪的客观行为判断而言，主要包括是否存在非法出售、提供、获取等行为及该行为是否指向公民个人信息两个方面。

如前所述，对识别性的适用围绕身份指向性展开，不具备身份指向性的信息充其量只是辅助信息，而仅有辅助信息根本不足以侵害公民的个人信息权，也就应以不存在非法出售、提供、获取公民个人信息的行为排除犯罪的成立。案例一中行踪轨迹本身只不过反映了自然人的移动范围，并不需要以自然人的身份信息作为产生条件，法院之所以将其视为公民个人信息，是因为认

〔49〕 本案案情为：被告人陈明通过黑客网站下载获取他人的邮箱账号和密码，后通过 QQ 等渠道多次提供给赵某等人。一审法院判决陈明构成侵犯公民个人信息罪，但陈明以仅凭邮箱账号和密码无法识别出特定自然人的身份为由提出上诉。二审法院经审理，认为可以根据邮箱的注册信息对应使用人的身份情况，甚至可以通过查看邮件知晓使用人的活动情况，故认定邮箱账号与密码属于公民个人信息。参见江苏省苏州市中级人民法院（2019）苏 05 刑终 488 号刑事判决书。

〔50〕 本案案情为：被告人赵某某以非法牟利为目的，通过购买等方式非法获取行踪轨迹、车辆信息、征信、通话记录、住宿信息等各类公民个人信息后，将上述信息出售、提供给他人。参见江苏省无锡市中级人民法院（2018）苏 02 刑终 418 号刑事判决书。

为收集行踪轨迹的人员在事先便已知晓被害人的身份，那么所获取的行踪轨迹当然可以对应到该被害人，但这不过是循环论证。事实上，若是以被害人从工作单位地址到家庭住址的行踪来证明行动轨迹属于公民个人信息，则恰恰说明行踪轨迹本身就不是公民个人信息。理由在于，具备识别性的是被害人的工作单位、家庭住址等信息，若是将这些信息指代成行踪轨迹，那么行踪轨迹的内涵就并非如法院所认为的那般系指自然人的移动范围。不过，实践中也存在着从正面肯定身份指向性进而以识别性认定涉案信息属于公民个人信息的判例。在杨木侵犯公民个人信息罪案〔51〕中，被告人一方最为重要的上诉理由是，涉案手机号码及其套餐情况并不以身份信息为产生条件，也就无法识别公民个人身份。二审法院并未以被害人获利数额巨大、利用职务便利实施犯罪、出售号码的行为影响机主的生活安宁等避实就虚的理由回避对涉案手机号码是否可以识别公民身份的认定，而是首先从正面肯定识别性系判断公民个人信息的标准，然后通过抽样鉴定的方法确认该案中的绝大多数号码都属于实名制信息，也即具备身份指向性，进而认定涉案手机号码属于公民个人信息。像这样以识别性为出发点判断涉案信息的属性，而后再据此论证其他犯罪成立要件的司法逻辑应当得到足够的重视与严格的贯彻，使涉案信息接受识别性的全面验证，充分发挥识别性作为侵犯公民个人信息罪第一道关卡的作用。

（二）犯罪成立的二次检验：个人信息权

涉案信息经过识别性的检视而被确认为公民个人信息后，排除犯罪成立的另一道关卡是行为是否侵犯了公民的个人信息权。然而，实践中频繁采取的操作却是在得出涉案信息属于公民个人信息的结论后，直接绕过或放弃第二道关卡的检验，未能进一步考虑是否存在非法出售、提供、获取等侵犯公民个人信息权的实行行为，从而也就难以确保判决结论合理。例如，在案例二与连福顺侵犯公民个人信息罪案〔52〕中，且不说公司名称、注册资本等法人信息难以被视为公民个人信息，即便认为涉案的姓名、电话号码等信息属于公民个人信息，也需要考虑涉案信息作为工商登记信息或公开信息，企业本身有向社会公开的义务或信息主体已自我决定向公众公开，根据《个人信息保护法》第27条的规定，这样的行为不构成对信息主体权利的侵犯，况且其他公民也可通过相关主管部门的信息公开制度或其他合法渠道获取。以“天眼查”为代表的企业信息查询软件，其数据的主要来源渠道是政府、法院等官方网站，〔53〕任何人都可以在这些网站上获取企业的登记信息，只不过“天眼查”基于其所开发与应用的数据技术，将企业或某个股东、企业高

〔51〕 本案案情为：被告人杨木系中国移动通信集团四川有限公司成都分公司员工。某公司负责人李某因公司开展业务需要，遂与杨木商议以每条0.1元的价格购买移动公司的客户消费信息（含电话号码和资费情况）。其后，杨木分多次向李某出售移动客户信息数百万条。一审法院判决杨木犯侵犯公民个人信息罪，但宣判后，杨木及其辩护人以涉案数据为电话号码及相应套餐情况，并不能据此识别特定自然人身份及反映自然人活动信息，认为本案不应被定性为侵犯公民个人信息罪等为由，提出上诉。二审法院经审理认为，涉案信息包含用户电话号码及相应资费信息，且根据公安机关筛选了96000条数据并经核实后，仅有2084条系非实名制的情况，可以认定本案所涉绝大多数信息属于实名制信息，故维持了一审判决对本案系属侵犯公民个人信息罪之定性。参见四川省成都市中级人民法院（2019）川01刑终211号刑事判决书。

〔52〕 本案案情为：被告人连福顺为实施诈骗，购买了一个名为“天眼查”软件的会员，从该软件上收集姓名及电话号码等公民个人信息，并将事先编写好的诈骗短信发送给机主。案发后，公安机关从其电脑内提取到公民个人信息共计11578条。参见广西壮族自治区田林县人民法院（2019）桂1029刑初43号刑事判决书。

〔53〕 参见“天眼查”官网免责声明条款，载https://www.tianyancha.com/property/5，最后访问时间：2021年3月18日。

层的所有企业相关信息整合在一起，以便查询人省时省力地直观了解其所要查询的企业或公民个人的企业信息。由此，通过这些渠道获取公民个人信息并不违法，所支付的会员费等不过是购买大数据集合技术服务的使用费。但这两起案件的审理法院却没有考虑到这一情况，而是以这些信息属于公民个人信息且被用于实施诈骗犯罪为由认定行为人构成侵犯公民个人信息罪，不得不说在论证上稍显草率。如果考虑到个人信息权的法益构造，这样的问题就能得到妥善的解决。

详言之，本罪规制的是非法获取与非法利用公民个人信息的行为，其中，非法利用具体表现为非法提供和非法出售两种形式。在案例二中，在确认行为人获取公民个人信息的行为并不违法后，只需要考虑其后利用公民个人信息实施诈骗的行为是否属于非法提供或非法出售公民个人信息这两种实行行为。案例二的行为人从一开始就形成了诈骗罪的共犯，在共同获取涉案信息后便将之用于骗取财物，并未向其他人提供或出售涉案信息，也就不存在非法提供或非法出售公民个人信息等侵犯信息利用权的行为，对行为人等只能论以诈骗罪。因此，基于识别性的标准确认涉案信息属于公民个人信息之后，个人信息权作为第二道关卡的价值在于判断获取、利用公民个人信息的行为是否违背了权利主体的意思自治，从而检视是否存在非法获取、非法利用公民个人信息的行为。以前述赵某某侵犯公民个人信息罪案为代表的判例虽然在论证涉案信息属于公民个人信息上存在些许瑕疵，但该判决既评价了行为人非法获取公民个人信息的事实，又论证了行为人此后的非法出售等行为，可谓充分考虑了个人信息权的法益构造，依然有值得肯定之处。

任何以识别性、个人信息权相互代替来判断彼此是否成立，从而论证侵犯公民个人信息罪是否成立的理论方案或实务操作必然遭遇逻辑混乱、立场颠倒的诘问。将识别性与个人信息权作为两道关卡检视侵犯公民个人信息案件的实务操作，并非出于学术上的自我满足，而是以正确适用罪名、严格贯彻逻辑推演、规范评价为价值取向，呼吁在实践之中形成从以识别性认定公民个人信息到通过个人信息权验证客观危害行为的司法适用逻辑。应当说，如此从客观行为入手、判断犯罪是否成立的方案相较于目前的司法实务现状，有其优势。

五、结　论

综上所述，可以得出以下几点结论：

第一，以识别性为标准判断公民个人信息具有妥当性，仍有必要保留，因此不宜直接采纳《个人信息保护法》对个人信息的定义。不过，必须对识别性的识别深度予以限定，既要把握只有以公民的身份信息为背书，才可能被认定为公民个人信息的方向，也要结合现存的技术手段、行为人的认识能力等来具体判断涉案信息是否可以被用来识别特定个人的身份。

第二，相较于一般人格权视角下的个人信息权，以具体人格权为基础建构的个人信息权无论是在解释的明确性上，还是在实务判决的说理上，都存在着明显的优势。就侵犯公民个人信息罪的具体适用而言，应当重点考察是否存在对信息控制权与信息利用权的侵害。

第三，在涉嫌侵犯公民个人信息的场合，首先必须以识别性为标准判断涉案信息是否属于

公民个人信息，只有在得出肯定结论的前提下，方可进入下一层面的判断，即是否存在非法出售、提供、获得公民个人信息的行为，以及这样的行为是否侵害了公民的个人信息权。因此，将识别性与个人信息权作为检视侵犯公民个人信息罪实务操作的两道关卡，并以此二者作为论证判决的逻辑进路，更有利于合理划定本罪的适用范围，在刑法的积极适用与必要谦抑间保持平衡。

Abstract: In the current judicial practice, there are some defects in the identification of citizens' personal information, such as unclear connotation and improper extension. The root of the defects lies in the failure to fully realize the important role of identification standard and personal information right in judging citizens' personal information. On the one hand, the theoretical research does not pay enough attention to the identification limit of identifiability; on the other hand, it lacks the in-depth exploration of the right attribute and structure of personal information right, which makes it impossible to provide ideal operation scheme and endorsement reason for practice. On the basis of defining the depth of identification and clarifying the connotation of the right of personal information, we should take the dual inspection path from identification to the right of personal information, and limit the scope of application of the crime of infringing citizens' personal information to the occasions where citizens' personal information right is infringed by illegally selling, providing and obtaining the identifiable information.

Key Words: personal information of citizens, identifiability, personal information right, dual inspection

(责任编辑：简　爱　赵建蕊)