《学术界》(月刊)
总第298期,2023.3
ACADEMICS
No.3 Mar. 2023

已公开个人信息刑法规制的边界〔*〕

姜　涛[1]，郭欣怡[2]
(1.华东政法大学　刑事法学院，上海　201620；
2.南京师范大学　法学院，江苏　南京　210023)

〔摘　要〕已公开个人信息的刑法规制欠缺合理界限，司法实务中的部分裁判不仅对已公开个人信息的属性、范围和体系地位定位错误，而且忽视信息公开场景的不同，未对相关行为进行类型化分析。刑法保护已公开个人信息的边界是一个综合性的存在，涉及已公开个人信息的保护范围、保护目的和具体方案等三方面问题。在保护范围上，基于“可识别性”的界定标准以及“信息状态”的分类依据，已公开个人信息属于个人信息的下位类型，其范围应划定为完全对外开放的个人信息。在保护目的上，刑法侵犯公民个人信息罪的保护法益应理解为个人法益，即个人信息自由与安全，对已公开个人信息案件的处理不能脱离法益论的指导。在具体方案上，提出“类型化公开标准说”，已公开个人信息案件内部应当分为非法公开、自愿公开和强制公开三类，并应分别从违法性认识、信息控制权范围以及利益衡量这三个角度进行考察。此外，在《个人信息保护法》出台的背景下，对相关案件的处理更应当重视与前置法的衔接。

〔关键词〕已公开个人信息；侵犯公民个人信息罪；可识别性标准；法益论；类型化公开标准说
DOI:10.3969/j.issn.1002－1698.2023.03.009

个人信息治理是一项综合性工程，涉及不同社会规制手段及法律规范，其治理目标已经超越单纯的权利保护，而是注重信息利用的兼顾发展，但信息权利保护和合理利用之间总会发生冲突，〔1〕这在已公开个人信息的刑法规制上得以集中体现。侵犯已公开个人信息的行为是否构成侵犯公民个人信息罪，理论界与实务界对此存在争议。司法实务在已公开个人信息案件的认定上，仍存在定性结论不统一、论证说理不精细、规范援引不正确等问题。随着《民法典》《个人信息保护法》(以下简称《个保法》)的颁布，特别是在《个保法》第27条延续《民法典》第1036条之规定，而再一次明确对已公开个人信息的特殊处理规则后，已公开个人信息的刑法规制需要进一步的讨论。

一、已公开个人信息案件的司法现状及问题

截至2023年3月，笔者对北大法宝收录的

作者简介：姜涛，华东政法大学刑事法学院教授、博士生导师，南京师范大学中国法治现代化研究院研究员；郭欣怡，南京师范大学法学院研究生。

〔*〕本文系国家社会科学基金重大项目“数字经济的刑事安全风险防范体系建构研究”(21&ZD209)的阶段性成果。

司法裁判文书进行检索,以“侵犯公民个人信息罪”为案由,并分别以“全文:公开信息”“全文:是公开”“全文:系公开”“全文:已公开”“全文:公开的”“全文:公开个人信息”“全文:天眼查”“全文:企查查”“辩方观点:公开”“法院查明:公开”“法院认为:公开”为并列条件进行高级检索,共检索出 510 份案例。经过整理,将其中与研究论题无关或重复的案例予以删除,筛选涉及已公开个人信息相关问题的案例,相关问题包括但不限于个人信息公开性的认定问题、公开的个人信息性质的认定问题、公开的企业信息性质的认定问题、公开的个人信息再利用行为性质的认定问题。最终,符合条件的裁判文书有 84 份。[2]这八十余份裁判文书的裁判理由和裁判结果反映出,目前司法实践对已公开个人信息案件的刑法认定仍未达成共识。

(一)司法实务中的定性分歧

在 84 份裁判文书中,大部分裁判最终以侵犯公民个人信息罪定罪处罚,只有少部分裁判认为已公开个人信息的再处理行为不构成犯罪,或是将个人信息已公开作为从轻量刑的情节考虑。

(1)无罪说。个人信息已公开这一情形多在无罪辩护的辩护意见中被提出,相关辩护意见认为已公开个人信息不属于个人信息,或是获取已公开个人信息的行为不属于非法获取。[3]对此,有裁判观点在一定的条件下采纳了相关辩护意见,即当个人信息在企业信息公示中被公开时,不再属于个人信息范畴。[4]极少部分裁判观点则是以“私密性”标准来定义个人信息,得出无罪的观点。[5]还有观点从信息公开后带来的结果出发,认为信息主体在公开信息时,必然会预见他人使用甚至不当使用的可能性,因此行为人的收集、交换、整理等行为不需要再次经过被收集者同意,故不构成犯罪。[6]也有观点从获取行为后的用途出发,认为购买信息用于合法经营活动,其行为不构成犯罪。[7]另有观点对侵犯公民个人信息罪的构成要件进行添加,认为该罪的构成要件中包含“违背权利主体个人意愿”这一不成文的构成要件要素,故对公民自愿,甚至主动公开的个人信息,可以合理推断出权利主体并不排斥公开的个人信息,行为人获取后提供、传播、出售的行为,不宜认定为侵犯公民个人信息罪。[8]

(2)有罪说。该说的内部还存在不同的论证思路。第一类裁判未区分已公开个人信息和未公开个人信息,对辩护意见中关于个人信息系公开的相关意见未作出回应或未经论述便不予采纳。[9]第二类裁判采取“二次授权”的处理方案。核心观点是,未经被收集者同意,获取、提供已公开个人信息的行为,构成侵犯公民个人信息罪,[10]其中还有部分裁判援引了《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 3 条第 2 款作为裁判依据。[11]第三类裁判采取“合目的、范围考察”的处理方案。核心观点是,获取、提供已公开个人信息,不符合原公开目的、范围的,仍构成侵犯公民个人信息罪。[12]还有裁判将第二、三类思路结合论证,认为超出原公开目的和范围处理已公开个人信息的,仍需经过被收集人同意。[13]

(3)区分说。这一类裁判对已公开个人信息的获取和提供行为作出了区分,认为获取行为不构成犯罪,但是提供行为构成犯罪。[14]

(4)从轻量刑说。还有一类裁判将个人信息已公开作为从轻处罚的依据,其基本观点在于,将已公开个人信息的再处理行为认定为犯罪,但是考虑到信息系公开的情节,故予以从轻处罚。[15]

(二)造成上述定性分歧的原因

上述分歧产生的原因有多种。首先,无罪说中“企业公示信息中的个人信息不属于个人信息”以及“以私密性标准界定个人信息”这两种观点,产生于实务界对个人信息认定标准的理解偏差。对“可识别性”标准的忽视,导致把不属于已公开个人信息的情况认定为已公开个人信息案件,或者相反,把属于已公开个人信息的情况认定为一般个人信息案件,从而导致案件定性错误。例如,“隐私性”并不是区分个人信息与

非个人信息的标准,而是区分私密信息和一般信息的标准。关于个人信息概念的界定,在《个保法》等前置法规中也有体现,刑法对此不能罔顾,而应当作出符合法秩序统一性原则的理解。对个人信息的错误定义,会导致对个人信息范围理解出现偏差,进而影响相关问题的正确处理。而且,正是因为对已公开个人信息识别标准的错误定位,导致有部分观点得出"信息一旦公开就丧失受到保护的权利"这一结论,这种观点仍是将"隐私性"作为个人信息界定的标准,这是有问题的。此外,还有部分裁判没有意识到行为对象和行为本身分属不同范畴的问题,将公开信息的属性和再处理行为的认定混为一谈,典型观点有,"因为获取公开信息未经被收集者同意,属于刑法规定的提供公民个人信息行为,所以被告人交换的公民个人信息属于刑法侵犯公民个人信息罪保护的客体"。[16]当然,也有裁判认识到行为对象和行为本身的区别,并先后分别对两个问题展开评判,这样的说理逻辑和层次较为清晰。[17]

其次,在规范依据上,有部分裁判援引《解释》第 3 条第 2 款,存在规范援引错误的问题。本款并非针对已公开个人信息再处理行为的规制,其规范对象范围更广,"合法收集"既包括收集已公开个人信息,也包括通过协议等合法渠道收集他人非公开个人信息,因此本款规制的个人信息的落脚点并非针对"已公开",而是"合法收集",不能将二者简单等同。此外,正是因为本款规制的对象是经过合法收集的个人信息,因此暗含了一个前提,即收集行为一定是合法的,否则便不可能受到本款的规制。但是对已公开个人信息的收集行为并不当然合法,可能存在虽然信息已经公开,但行为人却通过非法手段获取的情况,如果仍援引本款,则无论如何都会得出收集行为合法,并且这样的处理方式会忽视这类案件的真正争议焦点。

最后,正因对本款的援引,部分裁判认为获取行为不构成犯罪而提供行为构成犯罪。暂且不考虑援引错误的问题,即便是按照本款的内容,对已公开个人信息的获取和提供行为的区别对待似乎也存在问题。本款之所以认为提供合法收集的个人信息构成犯罪,是因为本款的适用前提是被收集者的同意范围仅限于特定信息处理者。但是对于已公开个人信息,信息处理者收集的合法性来源于其公开状态,而公开状态是客观持续存在的,并非一次性的,也并非只存在于特定主体之间,那么同样是基于信息公开这一合法性来源,对第一次收集行为和作为提供行为对向行为的第二次收集行为为何要作出不同的认定?这两次收集行为的区别只在于直接收集还是通过中介主体间接收集,然而只要收集的是符合初次公开范围的信息,获取的渠道不应当影响获取行为的合法性。因此,虽然获取和提供行为在违法性程度上确实存在不同,但本款并非该结论的有力依据,甚至反而会得出二者的区分不存在合理性的结论。

从深层次分析,为何司法实践对个人信息是否属于已公开信息、处理已公开信息是否构成犯罪采取的标准不统一,存在两大原因:一是对侵犯公民个人信息罪的保护法益的理解不一。无罪说和有罪说截然相反的裁判结果反映了,由于对本罪规范保护目的理解不同,裁判者对案情类似的案件也会采取不同的处理方式和说理路径,特别是对个人信息治理目标应当侧重于个人信息权利保护还是信息合理利用的衡量尺度不尽相同。持有罪说的观点是多数观点,这类观点对侵犯公民个人信息罪的保护法益采取个人法益的立场是正确的,但是其在具体说理的过程中,既未意识到《个保法》等前置法规对此类案件的特殊规定,也未顾及个人信息的利用价值,对不同公开类型采取统一标准。持无罪说的观点,多侧重于对个人信息公共属性的强调,特别是已公开个人信息由于处于公开的特殊状态,其在保护必要性上有所减弱。这类观点关注到已公开个人信息的特殊性,对其作出不同于未公开个人信息的认定,具有一定的进步性,但若将侵犯公民个人信息罪的保护法益界定为公共法益,则存在

问题。二是缺乏类型化的思维方式。裁判者忽视不同案件事实中的公开场景,企图通过一种方案一劳永逸地解决所有类型的案件。在上述已公开个人信息案件中,鲜有裁判者分析信息公开的类型,忽视了不同公开类型下所要实现的不同的个人信息保护目标。这种统一且简单的论证思路看似容易为人所理解和掌握,但是过分的化繁为简无法解决复杂多变的个人信息案件,使其丧失对现实社会必要的诠释能力,[18]也不符合个人信息分级分类保护的治理趋势。在不同类型的已公开个人信息案件中,个人信息的公开主体、对象、目的等要素均不相同,这些要素组成了个人信息不同的公开场景,而恰恰是由于公开场景不同,其所要实现的个人信息治理目标侧重点亦不相同。比如,在强制公开和自愿公开两个场景中,在公开主体上,前者是国家机关,而后者则是信息主体个人;在公开目的上,前者多出于公共利益,而后者则只为满足个人需求。因而,这两种场景下的个人信息公开之时所体现的个人权利的行使程度和公共价值的发挥等本就不同,对后续再处理行为所要实现的治理目标理应与最初公开行为的基础逻辑保持相对一致,此时,如果仍对上述两类案件采用相同的处理方案,便无法凸显不同信息公开的价值,更难以实现个人信息分级分类保护理念。

对已公开个人信息的处理在价值理念上应当有所转变,特别是在前置法对此有特殊规范的情况下,刑事司法实践也应当予以重视。尽管属于不同部门法领域,但不同法规范之间追求的不是分裂,而是和谐统一,因此对于已公开个人信息在概念定义、处理规则等问题上也应当接受前置法的检验,避免出现违反法秩序统一原则的裁判。

基于上述,本文将具体讨论以下问题:一是如何确定已公开个人信息的体系地位和保护范围;二是如何理解刑法侵犯公民个人信息罪的保护法益,并确保已公开个人信息案件的处理能够体现法律保护个人信息之目的;三是如何建构一套具体方案,为司法实践处理这类案件提供理论指引。

二、保护范围的明确:已公开个人信息的认定标准

随着数字经济社会的发展,个人信息的内涵愈发呈现其独立价值,身份识别标准说已逐渐在学界成为通说,在确立了“可识别性”标准的基础性地位并对其进行动态性理解的基础上,依据“公开状态”的不同,个人信息又可划分为已公开和未公开个人信息两类。

(一)个人信息的内涵界定——“可识别性”标准的展开

1.“可识别性”标准的基础性理解

纵观有关个人信息的相关立法,个人信息认定标准已经从隐私标准转变为识别标准,以“可识别特定自然人”作为认定个人信息的标准,已成为理论界的共识。[19]在2016年《网络安全法》出台之前,相关立法对于个人信息的定义几乎都包括能够识别公民个人身份和涉及公民个人隐私两种类型,[20]直到《网络安全法》出台,删除了“隐私性”标准,将“可识别性”作为个人信息法律定义的唯一标准,个人信息的独立概念才开始成型,后续的诸如《民法典》《个保法》《解释》也都延续了这一标准。这一立法变化,不仅具有规范意义,更具有现实价值,使得个人信息的内涵呈现其自身的独立性,有助于数字经济背景下对个人信息的规范保护和合理利用。该标准虽然存在争议,但大部分观点没有完全否定“可识别性”标准在界定个人信息内涵和范围上的根基地位,只是对“可识别性”标准的具体展开提出修正意见。基于“可识别性”标准,将个人信息对外公开,带来的结果只是打破了信息的私密状态,但是该部分信息可以指向特定自然人的内在特性并未丧失。因此,个人信息在公开之后不会影响其个人信息的属性。对于认为公开信息并非个人信息的意见,少部分没有厘清个人信息的核心内涵,将其与个人隐私混淆,更大一部分可能仍存在将行为对象和行为本身混为一谈的嫌疑。在笔者看来,对于那些主张公开信息不属于

个人信息但并未说理论证的辩护意见，其实可能也明知已公开的个人信息也属于个人信息，只是为了加大胜诉的几率，将其列为辩护意见之一。然而，“是否属于个人信息”与“处理行为是否构成犯罪”这两者之间并没有直接的因果关系，即便承认公开信息属于个人信息，也可以“处理已公开个人信息的行为不构成犯罪”进行辩护，而后者可能才是这一类案件真正的辩护焦点。

此外，还有辩护意见认为，非法利用已公开的个人信息社会危害性小，不具有侵害人身、财产安全的危险，因此不属于刑法上的个人信息。[21]这就带来了一个问题：刑法规范意义上的个人信息是否具有特殊性，是否需要附加其他条件？类似观点还有，如认为刑法上的个人信息不需要“识别性”要素，还包括不要求识别身份的隐私信息；[22]又如有观点认为，事关公民隐私安全、财产安全、人身安全、生活安宁等方面的合法权益的信息是刑法意义上的个人信息。[23]对于上述观点，笔者并不赞同。首先，由于不同部门法的规范目的不同，对概念外延适用存在不同，是非常正常的现象。[24]但是，外延不同并不意味着概念的核心内涵也可以不同，换言之，刑法规范意义上的个人信息也应当坚持“可识别性”这一核心内涵，不应抛开前置法的规范特立独行，这也是法秩序统一原则的内在要求。其次，刑法谦抑性原则的落实主要不在于对犯罪客体的限缩，而是对犯罪行为的正确认定，亦即在前置法上认定为违法的行为，并非就一定构成刑事犯罪，还需要作出符合刑法规范保护目的独立性判断。最后，人身、财产安全的影响结果已经作为划定不同入罪标准的因素被纳入司法解释中加以考虑，是否可能影响人身、财产安全只涉及入罪标准的划分，而不涉及个人信息范围的确定。因此，主张已公开个人信息不属于个人信息的观点无论在何种规范意义上都站不住脚。

2.“可识别性”标准的动态性理解

“可识别性”作为确定个人信息内涵和范围的核心要素，已经成为通说，但是，泛化的身份识别标准会导致个人信息的范围无限扩张，削减个人信息法律保护的效果，挤压信息使用的空间。[25]这在已公开个人信息案件中体现为：被公开的信息常常同时混有个人信息和非个人信息，如果全部认定为个人信息，有过度惩罚之嫌；如果全部排除在个人信息之外，又会导致个人信息保护不力；如果区分保护，则又会带来边界模糊的问题，因为似乎任何信息通过与其他信息的结合都可以识别到特定自然人。举例来说，司法实践中对公开的企业信息及企业中法定代表人等自然人的信息是否属于已公开个人信息这一问题的认定上，反映出“可识别性”标准具体适用中存在的问题。对此也存在肯定说、否定说和区分说的观点。肯定说认为，公开的企业信息属于个人信息，包括公司名称、住址等在内的信息都属于个人信息范畴；[26]否定说认为，公开的企业信息不属于个人信息，其中涉及的法定代表人等自然人的信息也不属于个人信息；[27]区分说则是大部分法院采取的观点，认为公开的企业信息中能够识别到自然人的信息仍属于个人信息，比如个人姓名、联系方式、身份证件号码等，其他单纯的企业信息则不属于个人信息范畴。[28]由于公开的企业信息中既包含仅与企业相关的信息，如企业名称、注册资本、统一社会信用代码等，也包含相关自然人的信息，如法定代表人姓名、联系方式等。如果机械地以“可识别性”标准来判断，这些信息无疑都可以直接或间接地识别特定自然人，有罪说便是这样的观点；相反，如果只考虑整个信息集合，那么其中涉及的法定代表人的个人信息似乎属于企业信息的一部分，这就会得出无罪说的观点。这一类难题之所以出现，是因为对可识别性标准理解的机械化和抽象化，故应当对可识别性标准具体展开，从识别对象和识别场景两方面解决上述难题。

可识别性标准指向的对象是自然人，而非其他主体或者物品。[29]公开的企业信息所反映的是企业的基本情况，包括企业的人事构造、持股情况、经营范围、登记情况等，其中涉及人事相关

的信息避免不了会存在透露个人信息的风险。但是只要理解了可识别性标准指向的对象是自然人而非企业,就可以解释人事信息并不属于个人信息,因为此时这些具有可识别性特征的人事信息所呈现的并非自然人作为“个体”的特质,而是自然人作为“企业一部分”的特质。因此,这种带有个人信息特征但作为企业信息一部分的人事信息原则上应当理解为企业信息而非个人信息。所以,如果行为人对企业信息以及企业中法定代表人等员工的信息作出一揽子处理的情况下,便不存在个人信息侵权的问题,而是企业信息侵权的问题。

但是,仅从识别对象的角度也无法一劳永逸地解决这类公开信息的问题,这是因为个人信息范围的界定还具有一定的场景依赖性,是动态发展的。个人信息在部分条件下不具有识别自然人的特性,并不意味着在所有条件下都不具备可识别性。[30]公开的企业信息中的人事信息作为企业信息的一部分不属于个人信息,前文已作论述,但是该结论的成立是以人事信息处于企业信息环境中为前提,一旦脱离企业信息环境,这些信息就不再属于仅为商业场景而存在的企业人事信息,而进入了特定自然人的具体生活、工作、交往场景中,其识别的对象便又从企业员工转变为一个特定的自然人,此时,这些信息又可能成为个人信息。因此,对于公开的企业信息,应当根据具体场景作出不同的认定,当且仅当个人信息处于企业信息环境中,才可以不被认定为个人信息,反之,则仍属于个人信息范畴。

(二)已公开个人信息的体系地位——状态标准下的分类范畴

1.已公开个人信息的分类依据:“公开状态”标准

“可识别性”标准划定了个人信息的范围,而个人信息还可以依据不同的标准,再进行细化分类,比如,根据性质分为敏感信息和一般信息;根据内容分为个人财产信息、生理健康信息、生物识别信息、身份信息……以上几个分类范畴的列举也只是个人信息分级分类保护的一部分。从不同维度对个人信息进行类型化体系的建构,系当前个人信息保护的发展趋势。已公开个人信息和未公开个人信息即是以公开状态为依据的分类范畴,将二者区分开来既具有规范指引,也有现实意义。《民法典》和《个保法》均对已公开个人信息作出单独规定,在前置法上首先作出限定,刑法对此也应当保持与前置法的统一性和自身的谦抑性。已公开个人信息由于处于特殊的状态,在信息获取方式、难易程度、规范依据等方面都区别于未公开个人信息,其在值得保护的程度上弱于未公开个人信息,因此需要对其采取不同的保护态度,这样既能将个人信息分类保护方案理论建构推向精细化,也使得投入到不同类型的个人信息案件的司法资源趋于合理化。

2.已公开个人信息的范围划定——对“客观开放程度标准说”的反思

作为个人信息的下位类型,已公开个人信息的范围是怎样的?也就是说,什么样的信息可以被认定为已公开个人信息,这就涉及对个人信息公开性的认定问题。

除了传统的“二次授权”方案和“合目的、范围考察”方案,近来有学者引入了“客观开放程度标准说”,也给处理该类问题提供了思考方向。“客观开放程度标准说”侧重通过信息的客观开放性程度,统一性地划定已公开个人信息处理者的刑事责任边界。[31]该方案虽然可以弥补“合目的、范围考察”方案在实际操作中的模糊性以及“二次授权”方案在规范依据上的不合理,但是这一学说亦存在问题。首先,该说仅仅依据信息公开的客观状态决定再处理行为的刑法评价,过于绝对化,忽视了个人信息公开场景的多元化和复杂化,这一具有强烈客观性、统一性的标准,并不适合具有灵活性的个人信息案件的处理。其次,尽管该方案也对强制公开、自愿公开和违法公开三种类型进行讨论,[32]但依照该观点,前两种行为只要处于完全开放的客观状态,对其处理行为就具有正当性,并没有考虑公开时的具体场

景,这就意味着,只要信息处理者处理信息的用途合法,对已公开个人信息的获取、提供行为就不会构成违法或者犯罪,这会导致对个人信息保护的削弱,而我国对个人信息保护的现状并不是太严而是太弱,“客观开放程度标准说”反而会加剧这种保护不力的状态。最后,该说似乎在已公开个人信息的范围划定上存在偏差,该说以公开程度为依据,将已公开个人信息分为完全开放、限制开放、违法公开三类,但问题是,限制开放的个人信息是否应当属于已公开个人信息?这就涉及已公开个人信息的范围划定问题。在笔者看来,只有完全对外开放的个人信息才属于已公开个人信息,限制开放的类型并不属于已公开个人信息的范围。

关于信息公开性的问题,在司法裁判中也存在争议。笔者在对案例进行分析的时候,发现有13份裁判的争议焦点落脚于涉案信息公开性的认定,有些辩护意见并未指出哪些信息属于已公开个人信息,只是笼统地将“可以公开获取的信息”作为无罪或罪轻的辩护意见。对此,有的裁判者并未予以认可,而有的裁判者则采纳了相关辩护意见,后者显然有轻纵犯罪行为的可能。

首先,已公开个人信息应当是任何公众都可以通过正规渠道获取的信息,如通过搜索引擎或只需要简单注册、支付一定金额就可以获得的信息,而那些只有内部人员可获得的信息就不属于已公开信息,或者虽然也对外界公开,但对外界公开和在内部可获取的信息范围、种类不同的,超出部分也不应当认定为已公开个人信息。[33]其次,信息的公开性判断是客观事实判断,与公开目的、合法性等价值判断无关。信息公开与否是一种客观的状态,不会受到公开主体的主观意志或公开来源的影响。因此,即便是有目的的公开或非法公开,也并不会造成公开范围的缩小或公开状态的改变,非法公开只是会涉及上游公开行为的认定以及后续信息处理者的违法性认识问题。部分裁判以公开目的特定、公开内容详尽和公开不合法的理由否认信息的公开性,存在问题。[34]最后,已公开个人信息的公开性还需要相关证据证明。这涉及举证责任的问题,要求辩方证明信息的公开性,可以减少辩方随意笼统辩护的情况发生,有利于法院精确认定已公开个人信息的范围。在有关裁判中也有一部分法院因证据问题而没有采纳相关辩护意见。[35]综上,笔者认为,只有完全对外公开的个人信息才属于已公开个人信息。

个人信息的保护范围是一张网,不同类型的个人信息以“可识别性”标准作为联结点,又依据不同的标准,形成不同的分叉。已公开个人信息是整个个人信息保护网中的一环,其自身又只能涵盖完全对外开放的个人信息。作为一类特殊类型,对已公开个人信息的保护所要实现的保护目的和所采取的具体方案存在不同。于前者,刑法对个人信息的保护目的涉及到对侵犯公民个人信息罪保护法益的理解;于后者,则需考虑到这类案件公开类型的不同,建构一套更加精细化的方案。

三、保护目的的厘清:侵犯公民个人信息罪的保护法益

如前所述,已公开个人信息案件的处理争议较大,存在无罪说、有罪说、区分说、从轻量刑说的观点,各学说内部还存在不同的处理方案。出现这种分歧的深层原因之一,在于案件的审理没有在法益论的指导下进行,或是对侵犯公民个人信息罪的保护法益理解不同,从而作出不同价值取向的裁判。

(一)理论界有关侵犯公民个人信息罪之保护法益的争议

关于侵犯公民个人信息罪保护法益的争议主要集中于两个方面:一是本罪保护的是超个人法益还是个人法益亦或是双法益。持超个人法益观的典型观点有公共信息安全法益观[36]、信息专有权法益观[37]等。持个人法益观的典型观点有隐私法益观[38]、个人生活安宁法益观[39]、个人人格法益观[40]、信息自决法益观[41]、个人

信息安全法益观[42]等。持双法益观的学者,则认为本罪既保护个人法益也保护超个人法益。[43]二是本罪保护的是传统法益还是新型法益。传统法益观多认为侵犯公民个人信息罪的保护目的通过现有法益观就可以有效评价,无须另行创造新的法益。相反,新型法益观则认为本罪保护的法益"是在网络信息时代作为新型权利的个人信息权"。[44]类似观点还有如,侵犯公民个人信息罪的保护法益仅限于"个人信息权"中的"信息自决权"[45];再如,"本罪法益应当完整概括为公民个人信息自决权及相关社会交往利益"[46];又如,"本罪的保护法益是公民的个人信息权,包括个人信息不被不正当收集、采集的权利,不被不正当扩散的权利,以及不被滥用的权利"。[47]尽管对作为新型法益的个人信息权的理解不同,但无疑新型法益观已成为多数观点。

(二)新型的个人法益观之提倡

针对上述争议,笔者赞同新型的个人法益观,具体表述为个人信息自由与安全[48],下面将予以具体阐述。

1. 对超个人法益论的质疑

个人信息的治理目标有个人信息权利保护和信息合理利用两个维度,前者体现为个人权利的保护,后者则体现为公共利益的实现。这似乎意味着刑法对个人信息的保护也应当体现这两种政策导向。但是作为刑法中的一个罪名,侵犯公民个人信息罪只是整个个人信息治理系统中的环节之一,其既不能也无法独自承担起整个个人信息的治理任务,这种机械的理解甚至会导致侵犯公民个人信息罪在教义学内部的混乱;反之,将超个人法益作为侵犯公民个人信息罪的违法阻却事由,不仅可以较好地实现个人信息的刑法保护目标,也使得对个罪保护法益的理解经受住教义学的检验。

持超个人法益论的学者在对个人信息法益的理解上存在以下两个问题:第一,混淆侵犯公民个人信息罪的保护法益和个人信息的宏观治理目标。如前所述,主张本罪的保护法益应当体现公共价值的观点,便来自于个人信息治理中信息合理利用目标的实现。但是,这种理解"陷入了大而化之地探讨信息流通及利用问题的窠臼"。[49]具体而言,宏观个人信息治理目标并非可以直接全部转化为侵犯公民个人信息罪保护法益的价值来源,相反,侵犯公民个人信息罪作为刑法"侵犯公民人身权利、民主权利罪"章节下的一个罪名,只体现了个人权利保护这一维度的治理目的,并非为了同时促进信息的合理利用,否则也会与其所处的章节体系相悖。个人信息治理目的的实现,不可能也不应当完全依赖刑法,相关前置法、行业规范、国家标准的内容应当成为"实现个人信息在安全中得以合法利用"这一目标的主力军,刑法则应当坚守其个人信息权利维护的保卫者角色,而不应当为了顺应数字经济的发展而改变对本罪法益的理解。换言之,对个人信息合理利用的发展需求不应当由侵犯公民个人信息罪保护法益的修正来满足,而应将其作为权利保护的例外,进行相应的价值权衡。《个保法》中的相关立法例似乎也印证了这一点。《个保法》明确将公共利益作为处理个人信息的例外情形,这就意味着为了公共利益处理个人信息的,并非个人信息处理规则的常态,而是以一种例外的情形出现,这就可以印证,公共利益并非个人信息保护法益的当然内容,而是独立于个人信息权利之外的另一种利益。在刑法层面,为了其他利益对个人信息进行合理利用的行为也可能构成行政许可、法定事由等违法阻却事由,但不能成为法益保护的一部分,否则会使得本罪的保护法益模糊。主张双法益的观点也存在类似的问题,甚至还会导致法益概念冲突,因为这类观点兼顾个人信息权利维护和合理利用两个维度,但这两者本身就可能存在冲突,从而导致本罪的法益内容也存在冲突,进而在认定行为性质的时候也会出现不协调。此外,如果认为本罪既包括个人法益也包括超个人法益,那么行为是要侵害一个法益就可以定罪还是需要同时侵害两个法益才能定罪;如果是前者,就会导致

本罪的保护法益存在不确定性,既可以是个人法益也可以是超个人法益,如果是后者,就会出现“只要行为人主张是为了信息的合理利用,无论其是否侵害了个人法益,都可以受到本罪超个人法益部分之庇护”的乱象,那么超个人法益就会被无限放大,个人法益将形同虚设。

还有观点认为,《解释》第 5 条第 2 款,将“造成重大经济损失或者恶劣社会影响的”认定为“情节特别严重”,在某种程度上体现了本罪的超个人法益属性。[50] 该理由也并不合理。首先,存在将造成的社会效果作为加重情节的立法例,并不能当然得出本罪的法益包括超个人法益,这甚至有混淆法益和情节之嫌,《解释》之所以将某一情形规定为加重情节,是因为该情形同时也侵犯了别的法益,这恰恰可以说明,《解释》的这一条款将“重大经济损失或者恶劣社会影响”作为独立的法益看待,即超个人法益,但是这种超个人法益是独立于侵犯公民个人信息罪而存在的。类似的情况还有“入户抢劫”是抢劫罪的加重情节,原因就在于该情形侵犯了抢劫罪保护的法益和非法侵入住宅罪保护的法益,但并不能由此得出抢劫罪的保护法益包括财产法益和基于住宅权产生的法益。其次,将超个人法益作为影响犯罪认定的立法例,只是意味着这一犯罪行为有可能造成一定的社会危害后果,且具有高发性,因此有必要将其类型化为影响定罪量刑的情节之一。

第二,超个人法益观施加侵犯公民个人信息罪过重的个人信息治理任务。一方面,“个人信息法益保护需要依靠各种法律手段共同发挥作用”,刑法应秉持谦抑性精神,[51] 由此看来,要求扩大、丰富本罪的保护法益内容,并非解决个人信息保护问题的最佳路径;另一方面,如果侵犯公民个人信息的行为带来了对社会乃至国家的不利影响,也可以通过刑法中的其他罪名加以规制,并不一定要通过强行改变一个罪的保护法益,来实现整个信息治理目标,这似乎强加本罪乃至整个刑法规范在个人信息治理过程中过高的责任。也许,通过非法获取、提供个人信息这一手段进行其他犯罪的现象越来越多,甚至有可能成为一种新的具有高伴随性的牵连关系类型,[52] 但这是罪数论的问题,而并非法益论的问题,因而也不能因其有间接导致其他犯罪的高概率性,而将下游犯罪的法益内涵也纳入本罪规制。另外,还有部分学者意识到,超个人法益观混淆信息和数据,因而产生了误解。[53] 笔者赞同这类观点,本罪保护的对象表述为信息而非数据,前者聚焦于对每一条信息的保护,而后者则是对经过一定技术分析后的数据集合的保护。单独的每条信息很难形成较大的数据价值,更无法产生侵害社会、国家权益的水波效应。

总之,应当将个人信息相关权益作为侵犯公民个人信息罪的保护目的,为了公共利益侵害个人信息法益的,原则上构成本罪,但其可能构成本罪的违法阻却事由,从而得出无罪或者罪轻的结论。

2. 本罪的保护法益:个人信息自由与安全

对个罪保护法益的理解应当立足于该罪所涉及的先法性事实基础,就侵犯公民个人信息罪而言,有必要站在刑法体系外部,从数字经济的社会背景以及个人信息治理要求所产生的客观需求出发,明晰法律所要实现的个人信息保护目标,从而解释本罪保护法益的内涵。而对个人信息保护目标的明确仍绕不开“可识别性”标准,这一标准的提出在个人信息权利保护层面的重要意义在于,其划分了网络世界的公共领域和私人领域,这也是“隐私性”标准失灵的原因。在信息网络时代,人们在虚拟空间的活动可能已经在各种信息技术的作用下被记住或者被其他主体利用,而为了得到相应的服务,人们往往又不得不以自己的私人信息作为交换的“对价”。因此,在网络世界中已经难以找到真实存在的“隐私”,“去识别化”(也可称为“匿名化”)便成为了划分公共领域和私人领域的新的边界,[54] 被匿名处理的个人信息,由于不具有可识别性,无法联系到特定个人,其他主体也无法通过该信息抵

达个体的私人领域。因此,尽管这些个人信息被他人获取、处理,不再具有私密性,或是处在公开状态,但这类信息具有的也只是“信息价值”而不体现“个人价值”。也就是说,其他主体只能获得基于信息内容本身产生的价值,而不能通过该信息指向某个特定人。因此,不涉及个人领域的匿名化信息无论被怎样处理,都不会让信息主体产生失控感和不安感。

基于“可识别性”标准可以得出,只有当个人信息启动识别功能时,个人的私人领域安全才会受到侵犯,因此,信息主体在个人信息被处理的过程中都有着“不愿被识别”的需求和期待,[55]由此产生出本罪保护法益的第一项内涵,笔者将其表述为“个人信息自由”。这种个人信息自由可以从积极自由和消极自由两个角度理解。一方面,个人享有对个人信息在整个信息生命周期中的决定性权能,此乃积极自由;另一方面,个人还享有在个人信息被处理过程中不受侵害的防御性权利,此乃消极自由。具体而言,在法益的核心内容上,应当更侧重于个人信息自由的积极控制权能层面,因为只有这样才能“扭转个人在异化的信息社会结构中所处的绝对弱势地位”,[56]突出信息主体所享有的个人信息权利,否则会使得前置法规定的知情权、决定权、查阅权、复制权、更正权、删除权等流于形式,个人如果只能享有不被侵害的合理期待和信赖利益,势必会沦为信息关系中的被控制一方,无疑会加剧信息的滥用。但是,仅仅强调个人信息的积极控制权能似乎也存在难以实现的问题,这是因为积极自由的实现有赖于信息主体的权利行使,但现实中信息主体往往存在不知权利被侵犯、明知权利被侵犯却维权无门等问题,导致对个人信息的控制权利无法实现。而消极防御权能则可以指引法益作出可操作性层面的转换,消极防御权能体现在个人信息相关权利不被侵害,这就要求相关信息处理者做好信息合规事项,在合乎规范的情况下处理个人信息,才能确保个人信息权利在处理过程中不被侵犯,这就意味着信息保护的风向从“呼吁信息主体行使权利”转变为“要求信息处理者履行合规义务”。唯有建立完备的合规制度,才能保证信息主体的权利不受侵害,“为信息社会的每个自然人筑起一道坚实的法律保护屏障,使之免于遭受上述危险现实化后所带来的损害”,[57]同时也能确保信息主体行使权利有相应的制度配合,解决维权无门之困境。因此,综合上述两方面,个人信息自由法益的内涵理解应当以信息控制权能为主,以信息防御权能为辅。

此外,处于不被识别的私人领域中的个人还享有一定的私域安全感,这就是侵犯公民个人信息罪保护法益的另一层内涵,即个人信息安全。具体而言,也存在两层具体含义,第一层含义是指个人信息所表征的私人领域中的个人安全感;更重要的另一层含义则是本罪作为刑法规范区别于其前置法规范所涉及的个人信息相关的人身、财产安全。如前所述,对个人信息的法律保护乃各种法律法规的综合适用,刑法在这一过程中应当保持谦抑性,而且侵犯公民个人信息罪作为行政犯,应当具备行政和刑事的双重违法性,才能受到刑事制裁,处罚并不是实现个人信息保护的最佳手段。因此,个人信息的违法处理行为,只有涉及个人人身、财产安全的,才有必要纳入刑法规制。不同类型、场景下的个人信息被非法处理后所造成的危害后果都是不一样的,个人信息的处理也应当作出类型性、场景化的分析,避免妨碍个人信息的合理利用,《解释》第5条将“影响人身、财产安全”作为划分不同入罪标准的做法,也体现了这样的理念。

综上所述,基于“可识别性”标准,将侵犯公民个人信息罪的保护法益理解为个人信息自由和安全,其核心在于,个人享有信息控制权能,包括决定信息处理行为的对象、主体、时间和场景等。同时,还应当让信息处理者负担合规义务,以实现个人信息不被侵害的防御性权能,确保个人信息相关权利的实现。

(三)对已公开个人信息处理方案的再反思

侵犯公民个人信息罪的保护法益是解决所

有个人信息刑事案件的规范前提,对已公开个人信息的处理应当符合刑法规范的保护目的,不能侵害本罪的保护法益。现有处理方案并未意识到这一点。首先,占少数观点的“无罪说”会得出已公开个人信息的再处理行为不侵害本罪法益的结论,或者对本罪的构成要件进行了不当添加,对个人信息的保护力度较弱,显然不合理。该说认为信息主体公开个人信息必然会预见他人使用,因此再处理行为并不违背公民个人意愿的观点,亦存在对本罪法益的误读。一方面,将信息公开体现了个人对其个人信息权利的处分,但是该自由意志只存在于特定的场景下,也就说超出一定合理目的和范围的场景中不存在信息主体的自由意志,尽管行为人可能预见他人使用,但其并不希望甚至极力反对个人信息被不当使用,更何况其中还有被强制公开未体现个人自由意志的情形,因而无法不加区分地当然得出对已公开个人信息的处理不违背个人自由意志的结论。另一方面,即使信息主体可能预见个人信息会被不当使用,但并不意味着这种不当使用行为合法合理,否则,恐怕没有主体愿意轻易公开自己的个人信息,这无疑会阻碍信息的进一步利用;相反,这一部分已公开的个人信息被不当使用的风险增高,这一部分增高的风险也应当由收集这部分信息的信息处理者共同承担,因为“没有无义务的权利”,[58]信息处理者在利用信息的过程中是获益者的角色,因此其也应当承担起与收益相匹配的责任,确保信息的处理是在安全的环境下进行的。

在“有罪说”的观点中,“合目的、范围考察”方案更有利于对个人信息法益的保护,其涉及对信息主体公开信息时的信息控制权所及范围的理解。该方案严格依循个人公开信息时的主观意志表达,有利于实现对个人信息自由和安全的保障,但是,这种处理方案并不适用于部分强制公开的场景,该类型的公开实际上并不体现个人自由意志,甚至有违个人自由意志,且由于此类信息的公开多为了公共利益,因而也无法找到信息主体的公开目的,遑论对再利用行为作出“合目的”的判断。而“二次授权”方案则完全忽视已公开个人信息系个人信息保护中的特殊类型,罔顾前置法对其的不同规范要求,有违法秩序统一原则,在案件处理的模式选择上缺乏类型化的思维。“区分说”和“从轻量刑说”的观点则从违法性程度出发,考虑到不同行为的法益侵害程度不同,虽有一定合理性,但其并不能给出一套完整的认定方案,只涉及对个案细节的讨论。

综合上述,对已公开个人信息的刑法保护应当实现刑法对个人信息的保护目的。在对个人信息的治理目标逐渐走向保护与利用双维度兼顾的背景下,刑法对个人信息的保护目的,即侵犯公民个人信息罪的保护法益的认定也应在这样的治理目标下展开。对此,正确的理解应当是,严格坚持本罪的个人法益保护内涵,超个人法益仅可作为违法阻却事由加以考虑。已公开个人信息案件的处理也应当以该规范保护目的为前提,分析案件涉及的法益种类,如果仅仅涉及个人法益,则应当采取严格的个人权利保护态度;而如果同时涉及公共利益,则需要转向利益衡量的思考路径。进一步而言,对于司法裁判中的现有观点,无论哪一种方案都无法很好地实现个人信息的治理目标,这是因为已公开个人信息案件中涉及不同的保护法益,只有采取不同的考察方案,才能够实现个人信息保护与利用的双重目标。

四、具体方案的建构:已公开个人信息的刑法类型化规制

已公开个人信息案件尤为复杂,合理界定个人信息可识别性标准和正确定义侵犯公民个人信息罪的保护法益,可以在刑法对已公开个人信息保护范围和保护目的上予以一定的限制,但是上述两个维度的问题仍较为抽象,还需要一套更具体的方案,为刑法保护已公开个人信息的展开提供可操作性依据。现有司法实践所采取的方案,仍是对这类案件进行笼统的规制,忽视了对已公开个人信息内部的再分类。不同的公开类

型有其自己的场景特点,背后蕴含的价值理念也不相同,如果想要通过某一种方案解决所有公开场景下的案件类型,显然力有不逮,这也是为什么“二次授权”方案和“合目的、范围考察”方案被一些学者批判的原因,已有方案并不是完全没有适用余地,只是同一方案可能并不能适用于所有的案件类型。正确的选择是,根据公开信息的不同类型及其场景,建构不同的判断标准。

(一)类型化公开标准说之提倡

已公开个人信息系以“公开状态”为依据的一类特殊个人信息,而在已公开个人信息案件内部,公开状态所表征的公开目的、公开合法性来源还存在不同。而且,不同的公开场景下,所要实现的个人信息保护目的也侧重不同。因此,对于已公开个人信息案件的处理,不能脱离信息行为所涉及的场景,并对此进行类型化分析。

1.类型化公开标准说的分类方法

类型化公开标准说主张,由于个人信息公开主体、对象、目的、合法性依据不同,已公开个人信息又可以具体分为自愿公开、强制公开和非法公开三种类型。这三种公开类型的区分依据,除了在公开主体、对象等事实要素上存在不同,更重要的是在公开目的、公开的合法性依据以及背后体现的公开价值等规范要素上亦存在不同。自愿公开的公开主体一般为信息主体本人,其公开的合法性依据系信息主体在特定场景下的法益处分行为,背后体现的是个人信息权利的行使,而并不涉及公共利益价值;强制公开的公开主体则多为国家机关,其公开的合法性依据源于公共利益与个人信息法益相互衡量与妥协的结果,这类案件便涉及个人权利和公共利益的双维度考虑;而非法公开的公开主体既可能是信息主体以外的第三人,也可能是国家机关,其公开行为侵犯了信息主体的法益,不具有合法性依据,这类案件主要考虑的是,信息再处理者的违法性认识问题。

2.类型化公开标准说的场景特征

上述三种类型下的公开行为都具有一定的类型化特征。自愿公开的场景多为信息主体为了实现一定的个人目的,例如在微博发布动态、分享日常,以进行个人形象的塑造或完成个人情绪的宣泄等;又如在相亲网站发布自己的个人信息,以实现交友的目的等,其公开的合法性基础是个人行使信息权利,这种公开暗含了一定程度和范围上信息主体的知情同意以及对个人信息相关权益的处分。而强制公开的合法性基础显然并非基于信息权利的行使,是信息主体“不得不”进行公开的信息,甚至可能是信息主体不知情或违背信息主体意愿的(比如失信被执行人个人信息的公布)。但是在数字经济社会的背景下,信息、数据的流通、共享又是必要的,因此,其合法性来源在于个人信息治理中权利保护维度向合理利用维度作出的一定程度上的让步。换言之,强制公开的场景下,虽然也存在一定的公开目的,但该目的多为具有公共性质的目的,比如,企业信息公示网公开企业信息,以便于“强化企业信用约束,维护交易安全,提高监管效能”,[59]再比如,裁判文书网公开裁判文书,以便于“落实审判公开原则,规范人民法院在互联网公布裁判文书工作,促进司法公正”。[60]归根结底,这是一种利益衡量与博弈的结果。非法公开多为信息公开者未经信息主体授权或违背其意愿,擅自公开其个人信息的行为,往往表现为两类行为:一种是第三人的法益侵害行为,比如对个人信息的非法泄露导致信息处于公开状态;另一种是国家官方机构不符合比例原则的信息强制公开,这两类公开行为或多或少地都对信息主体的个人信息权利造成了一定的侵害。

在不同的公开场景下,信息主体对个人信息的自我决定权利和不被侵害的合理信赖程度不同,再处理行为对信息主体人身、财产权利造成的影响也不同,所体现的个人信息保护侧重点亦不同。总体来说,对于非法公开类型,涉及到信息处理者对信息公开系违法是否具有认识的问题。对于自愿公开类型,由于其公开的合法性源自于对部分个人信息法益的处分,故对这类信息

的再处理行为原则上也不能超越公开时法益处分所及的合理范围,即对于个人信息在何种范围内、基于何种目的、被用于何种用途等事项,信息主体具有控制的权利,而这种自我控制权利既包括积极的决定权利,也包括消极的不被侵犯的期待。而对于强制公开类型,由于其合法性源自于个人权利的让步以及信息流通的社会需求,故对这类信息的再处理行为也应当以利益衡量为出发点,需要考虑合理利用带来的效益。当然,对于强制公开中存在的一些有可能违背信息主体意愿的场景(比如裁判文书网公开的信息没有隐去个人身份、住址等敏感信息),则需要另外讨论,如果仍然坚持利用效益优先,无疑会给信息主体带来二次伤害。

(二)类型化公开标准说之实践

已公开个人信息内部存在不同的公开场景,进而构成不同的公开类型,不同类型的案件背后体现的规范依据、政策理念、教义学理论并不完全相同,正确的做法应当是选择类型化分析进路,对不同的案件类型,采用不同的考察标准。

1. 非法公开型个人信息案件:违法性认识的考察

需要再次强调的是,非法公开的个人信息仍属于已公开个人信息范畴,但由于其明确被排除在《个保法》第 27 条规定的范围之外,故不受相关内容的约束,但这并不意味着处理非法公开的个人信息没有任何规范依据。因为信息虽系非法公开,但其公开状态客观存在,信息处理者基于这一客观公开的状态实施的再处理行为并不必然因为公开行为侵害法益而不具有出罪可能性,因为行为人可能对信息公开系违法不具有认识可能性。特别是一些不符合比例原则的强制公开情景,信息主体的个人信息遭受过度曝光,现有制度对相关个人信息予以公开的做法可能并不一定真正合理合法,[61]但是,基于对国家公信力的信赖,信息处理者一般不会对这类信息公开的合法性产生质疑,否则无疑会抑制信息的再利用。因此,这种非法公开导致的不利后果不应当由信息处理者承担。对于其他从非官方渠道公开获得个人信息的情况,可以从证明的角度判断行为人的违法性认识,即“无法证明行为人主观上认识到,且一般人也难以认识到的,则应当按照有利于被告人的处理规则,可以适用公开个人信息的处理规则认定行为性质”。[62]这也是存疑时有利于被告原则的体现。

2. 自愿公开型个人信息案件:信息控制权的考察

信息主体自愿公开个人信息,系对个人信息权利的处分,属于信息控制权的一部分,因此信息处理者若要合法合理地开展二次处理行为,则不能侵害信息公开时信息主体对于信息将在何种范围内进行流动的决定权利,以及超越上述范围之外不被侵害的合理期待。换言之,信息处理者应当尊重信息主体公开时的处分状态,具体而言,应当考虑目的、用途、方式和结果这几个要素,确保二次处理在“合理范围”内。有部分持“合理预期”“场景理论”“情景脉络”[63]观点的学者也是从尊重信息主体公开时的意愿出发,最终也落脚在对公开时各种要素的考察上,与本文观点殊途同归。且这类观点在民法和刑法学者之间都有一定数量的支持者。[64]其大致可以总结为目的合理、用途合法,未产生影响他人人身、财产安全的结果,只有满足这三条才属于合理处理。

笔者对这三点要求基本赞同,但问题在于,是否只要违反其中一条就应当以侵犯公民个人信息罪加以认定?笔者认为并非如此,否则似乎会导致刑法的过度介入。首先,对于仅仅不符合公开目的,但用于合法途径,也并未造成严重人身、财产危险或侵害的行为,不应当认定为侵犯公民个人信息罪,如果给公民带来了损失,可以通过民法或者行政法的手段加以规制,对此刑法应当采取审慎介入的态度。其次,对于侵害他人人身、财产安全的行为,原则上应当以侵犯公民个人信息罪论处,而且这一类情况多数也是不符合公开目的的,但是,不能否认造成损害的行为可能存在用途合法的情形,比如为了合法经营,

这种情况下可能会改变行为所依据的规范,适用《解释》第6条的规定,合法经营的用途也有可能成为从轻处罚的依据。

另外,笔者想要强调的是,对于自愿公开的个人信息的再处理行为的认定,应当采取严格的保护个人权利的态度,不存在需要考虑利益衡量的问题。因为个人自愿公开信息往往只是为了达成一种基于生活、工作、娱乐等需求而产生的私人交往、形象塑造的目的,不存在个人利益向公共利益让步的情况,个人也并没有放弃个人信息权利,其基于"可识别性"产生的信息自由和对信息不被非法利用的安全感并没有丧失,仍受到法律的保护。恰恰相反的是,个人基于对信息权利的行使,将个人信息予以公开,使其暴露在公共视野里,其被非法利用的可能性升高,但这一部分风险并不应当由信息主体承担,否则网络世界难有自由和安全可言。

3.强制公开型个人信息案件:利益衡量视角的考察

强制公开的场景下,不存在个人行使信息权利的自由意志,而其信息被强制公开也会给信息主体带来一定的不安感,超越信息主体的控制范围。因此,从严格的法益保护的角度来看,这一类型的行为似乎都侵犯了侵犯公民个人信息罪的保护法益,但是,对其作入罪处理显然不符合信息治理的要求,也会阻碍个人信息的自由流通。对于这一类案件,宜作为一种符合违法阻却事由的例外情形,在违法性阶层作出罪处理。原因在于,侵犯公民个人信息罪保护的是个人法益,而强制公开个人信息则多体现为公共目的之需要,因而,对其再处理行为的合法性也只能来自于个人法益向公共利益作出的让步,实质上是一种利益衡量的结果。因此,强制公开的个人信息案件应当兼顾个人权利保护和合法利用的双重治理目的,确保信息主体的信息权利得以充分行使,并在最大程度上充分发挥信息价值。

这一类案件多见于国家官方机构对个人信息的公开发布,比如政府公开的信息、裁判文书网公开的信息、国家企业信用信息公示系统公开的信息等,以及对上述官方公开的信息加以汇总整合后的信息公开,比如北大法宝网、企查查、天眼查等收录的信息。对于这类案件,可以从以下两个方面考虑。

第一,单纯的合法获取、查询行为不构成犯罪。原因在于,这些直接或间接通过官方渠道公开的个人信息,其公开目的本身就在于资源整合和便利查询,因此单纯的获取和查询行为本身就在公开目的、范围内,不应当认定为非法利用,否则,公开的信息便无法发挥其价值。这种情况下,由于二次处理行为仍在原公开目的、范围内,因此也不存在对个人权利的再一次剥夺,故不存在侵权的可能,遑论犯罪。

第二,对于除个人或企业内部使用以外的加工、传输、共享等可能使得个人信息所反映的内容超出原范围的情况,也不应当完全禁止,而应要求信息处理者做好信息合规工作,确保个人信息在安全中发挥价值。笔者认为,合规是调和信息权利和信息利用之间矛盾的极佳措施。因为,一方面合规不阻碍信息的再次流动,另一方面合规对信息处理者施加保护义务,既能缓和信息主体在信息关系中的弱势地位,也能使得从信息利用中获益的处理者承担起应有的责任。个人信息的合规建设是一个庞大而复杂的工程,本文限于篇幅无法全面展开,但归根结底,个人信息的合规应当秉持全过程、分级别的理念,对个人信息的收集、存储、加工、传输、提供等处理行为进行全面规制,根据个人信息的重要程度、敏感程度等制定分级分类的合规体系。比如,在获取的已公开个人信息中,既可能存在生物识别、宗教信仰、金融账户、行踪轨迹等敏感程度较高的个人信息,也可能存在姓名、电话号码等非敏感个人信息;既可能存在成年人的个人信息,也可能存在未成年人的个人信息……对此,应当对个人信息进行分级分类保护,这样不仅能实现对重要、敏感信息的着重保护,还能够保证个人信息的灵活利用。

五、简要的结论

本文所收集的已公开个人信息案件多发生在《民法典》《个保法》实施之前，由于缺乏前置法的支撑，法院在裁判过程中多未能对已公开个人信息的处理作出合理的认定，定罪者居多。但随着前置法对个人信息保护规范的趋于完善，以及信息治理目标从保护到保护与利用兼顾的转变，对已公开个人信息可以采取一定程度上的弱保护态度，这“也是平衡信息保护负担的务实选择”。[65]因此，如何结合前述的可识别标准、个罪的保护法益和类型化规制路径，合理定位已公开个人信息案件的规范依据就至关重要。

《个保法》的出台使得个人信息治理的法律规范体系更加完备，形成民法、行政法、刑法全面保护的局面。考虑到个人信息治理的目的并非打击个人信息非法处理的行为，而是要使得个人信息在安全中得以利用，而刑罚处罚具有制裁性和严厉性，其过分介入无疑会打压信息的合理利用，因此，相较于刑法规范，民法和行政法规范似乎应当承担起信息治理中更重要的角色，特别是在前置法对相关问题作出规定的情况下，刑法更加不能罔顾前置法规，作出与其相违背的认定。《个保法》第 27 条对已公开个人信息作出特殊规定，其核心内容基本延续《民法典》第 1036 条第 2 款的规定，即对于已公开（包括自行公开和合法公开）个人信息，信息处理者可以在合理范围内加以处理，但例外情况有二，一是个人明确拒绝，二是对个人权益有重大影响。基于此规定，相较于未公开个人信息，对已公开个人信息的权利保护，立法采取了相对宽松的态度。这一立法态度是合理的，因为个人信息包括很多种类，对个人也有着不同的意义，应当依据个人信息类型提供不同程度的保护。[66]

问题在于，这一规范应当如何指引侵犯公民个人信息罪的认定。笔者认为，这一规范应当首先在价值立场上指引本罪的适用，由于本条的存在，已公开个人信息的处理问题在前置法上的定性都存在问题，[67]那么刑法认定需要更加谨慎，即这些行为是否违法的认定都是模糊的，是否构成犯罪的认定应当采取更为严格的入罪态度。其次，刑事案件的认定过程也可以借鉴本条的规制思路，即对“合理范围”“个人明确拒绝”“对个人权益有重大影响”等规范要件作出合理理解以对行为的违法性质作出正确认定。最后，结合司法解释对“情节严重”“情节特别严重”的规定，再对行为违法性程度是否达致刑事违法性作出认定，以得出与前置法不相违背又具有刑法独立性的裁判。以上仅对刑法与个人信息保护法的衔接适用进行框架性梳理，其具体展开还有待继续研究。

注释：

〔1〕〔57〕参见程啸：《论公开的个人信息处理的法律规制》，《中国法学》2022 年第 3 期。

〔2〕案件如有一审、二审、再审判决的，视为同一组判决。

〔3〕参见福建省安溪县人民法院（2018）闽 0524 刑初 932 号刑事判决书；广东省珠海市中级人民法院（2020）粤 04 刑终 59 号刑事裁定书；广东省佛山市南海区人民法院（2020）粤 0605 刑初 2812 号刑事判决书；河南省济源市中级人民法院（2019）豫 96 刑终 36 号刑事裁定书；上海市黄浦区人民法院（2017）沪 0101 刑初 968 号刑事判决书；江西省南昌市中级人民法院（2021）赣 01 刑终 116 号刑事裁定书；山东省青岛市中级人民法院（2019）鲁 02 刑终 318 号刑事判决书；上海市第一中级人民法院（2018）沪 01 刑终 1184 号刑事裁定书；广东省深圳市龙华区人民法院（2020）粤 0309 刑初 770 号刑事判决书；浙江省杭州市滨江区人民法院（2019）浙 0108 刑初 118 号刑事判决书；重庆市第二中级人民法院（2018）渝 02 刑终 277 号刑事裁定书；江苏省南京市鼓楼区人民法院（2017）苏 0106 刑初 653 号刑事判决书；江苏省南京市鼓楼区人民法院（2016）苏 0106 刑初 943 号刑事判决书；广东省深圳市福田区人民法院（2020）粤 0304 刑初 151 号刑事判决书；福建省安溪县人民法院（2018）闽 0524 刑初 932 号刑事判决书；重庆市渝中区人民法院（2018）渝 0103 刑初 156 号刑事判决书；湖北省随县人民法院（2017）鄂 1321 刑初 223 号刑事判决书；河南省登封市人民法院（2019）豫 0185 刑初 144 号刑事判决书；浙江省温岭市人民法院（2017）浙 1081 刑初 1926 号刑事判决书；四川省叙永县人民法院（2020）川 0524 刑初 6 号刑事判决书；广东省深圳市南山区人民法院（2020）粤 0305 刑初 183 号刑事判决书；河南省太康县人民法院（2018）豫 1627 刑初 464 号刑事判决书；浙江省台州市中级人民法院（2019）浙 10 刑终 857 号刑事裁定书；福建省龙岩市中级人民法院（2018）闽 08 刑终 180 号刑事裁定书。

〔4〕参见广东省广州市中级人民法院(2019)粤01刑终2121号刑事裁定书;重庆市第五中级人民法院(2017)渝05刑终1090号刑事判决书;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;重庆市渝中区人民法院(2018)渝0103刑初591号刑事判决书;浙江省杭州市下城区人民法院(2020)浙0103刑初299号刑事判决书;广东省珠海市香洲区人民法院(2020)粤0402刑初73号刑事判决书;重庆市渝中区人民法院(2018)渝0103刑初156号刑事判决书。

〔5〕参见广东省深圳市龙华区人民法院(2020)粤0309刑初727号刑事判决书;上海市黄浦区人民法院(2017)沪0101刑初932号刑事判决书。

〔6〕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。

〔7〕参见江苏省南京市鼓楼区人民法院(2017)苏0106刑初653号刑事判决书。

〔8〕参见北京市第三中级人民法院(2019)京03刑终47号刑事裁定书。

〔9〕参见广西壮族自治区南宁市中级人民法院(2020)桂01刑终372号刑事裁定书;江西省南昌市中级人民法院(2021)赣01刑终116号刑事裁定书;河南省夏邑县人民法院(2018)豫1426刑初324号刑事判决书;广东省深圳市福田区人民法院(2020)粤0304刑初151号刑事判决书;江苏省南通市通州区人民法院(2017)苏0612刑初692号刑事判决书;浙江省台州市中级人民法院(2019)浙10刑终857号刑事裁定书;天津市南开区人民法院(2018)津0104刑初323号刑事判决书;安徽省涡阳县人民法院(2018)皖1621刑初220号刑事判决书。

〔10〕参见上海市黄浦区人民法院(2017)沪0101刑初968号刑事判决书;安徽省蚌埠市蚌山区人民法院(2021)皖0303刑初173号刑事判决书;广西壮族自治区宾阳县人民法院(2020)桂0126刑初104号刑事判决书;北京市昌平区人民法院(2020)京0114刑初509号刑事判决书;浙江省杭州市滨江区人民法院(2019)浙0108刑初118号刑事判决书;福建省安溪县人民法院(2018)闽0524刑初932号刑事判决书;广西壮族自治区宾阳县人民法院(2018)桂0126刑初329号刑事判决书;上海市黄浦区人民法院(2017)沪0101刑初969号刑事判决书;河南省登封市人民法院(2019)豫0185刑初144号刑事判决书;浙江省温岭市人民法院(2017)浙1081刑初1926号刑事判决书;江苏省无锡市新吴区人民法院(2018)苏0214刑初15号刑事判决书;安徽省淮南市中级人民法院(2018)皖04刑终102号刑事裁定书;广东省广州市越秀区人民法院(2020)粤0104刑初421号刑事判决书;四川省成都市高新技术产业开发区人民法院(2018)川0191刑初94号刑事判决书。

〔11〕参见福建省安溪县人民法院(2019)闽0524刑初397号刑事判决书;浙江省杭州市滨江区人民法院(2019)浙0108刑初118号刑事判决书;福建省安溪县人民法院(2018)闽0524刑初932号刑事判决书;浙江省温岭市人民法院(2017)浙1081刑初1926号刑事判决书。

〔12〕参见上海市金山区人民法院(2018)沪0116刑初839号刑事判决书;广东省佛山市中级人民法院(2021)粤06刑终345号刑事裁定书;山东省青岛市中级人民法院(2019)鲁02刑终318号刑事判决书;江苏省徐州市云龙区人民法院(2018)苏0303刑初17号刑事判决书。

〔13〕参见江苏省宿迁市中级人民法院(2019)苏13刑终32号刑事裁定书。

〔14〕参见河北省涿州市人民法院(2020)冀0681刑初507号刑事判决书;湖南省永顺县人民法院(2018)湘3127刑初105号刑事判决书。

〔15〕参见广东省深圳市罗湖区人民法院(2016)粤0303刑初2302号刑事判决书;广东省深圳市宝安区人民法院(2017)粤0306刑初4930号刑事判决书;北京市西城区人民法院(2018)京0102刑初780号刑事判决书。

〔16〕参见浙江省杭州市滨江区人民法院(2019)浙0108刑初118号刑事判决书。

〔17〕参见广东省佛山市中级人民法院(2021)粤06刑终345号刑事裁定书。

〔18〕参见劳东燕:《风险社会中的刑法——社会转型与刑法理论的变迁》,北京:北京大学出版社,2020年,第148页。

〔19〕〔29〕赵精武:《个人信息"可识别"标准的适用困局与理论矫正——以二手车车况信息为例》,《社会科学》2021年第12期。

〔20〕例如,2012年12月28日实施的《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》第1条第1款规定:"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。"2013年4月23日实施的《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》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个人隐私的信息、数据资料。"

〔21〕参见广东省深圳市龙华区人民法院(2020)粤0309刑初770号刑事判决书。

〔22〕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。

〔23〕参见田宇航:《我国公民个人信息刑法保护范围研究》,《福建农林大学学报(哲学社会科学版)》2016年第6期。

〔24〕〔41〕参见周光权:《侵犯公民个人信息罪的行为对象》,《清华法学》2021年第3期。

〔25〕参见杨楠:《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。

〔26〕参见广东省佛山市中级人民法院(2021)粤06刑终345号刑事裁定书;河南省济源市中级人民法院(2019)豫96刑终36号刑事裁定书;广西壮族自治区宾阳县人民法院(2019)桂0126刑初77号刑事判决书。

〔27〕参见广东省广州市中级人民法院(2019)粤01刑终2121号刑事裁定书;重庆市渝中区人民法院(2018)渝0103刑

初156号刑事判决书;浙江省杭州市下城区人民法院(2020)浙0103刑初299号刑事判决书。

〔28〕参见广东省珠海市香洲区人民法院(2020)粤0402刑初73号刑事判决书;辽宁省沈阳经济技术开发区人民法院(2018)辽0191刑初418号刑事判决书;广东省珠海市中级人民法院(2020)粤04刑终59号刑事裁定书;上海市黄浦区人民法院(2017)沪0101刑初968号刑事判决书;江苏省南京市鼓楼区人民法院(2016)苏0106刑初943号刑事判决书;上海市黄浦区人民法院(2017)沪0101刑初969号刑事判决书;湖北省随县人民法院(2017)鄂1321刑初223号刑事判决书;上海市静安区人民法院(2017)沪0106刑初960号刑事判决书;江苏省宿迁市中级人民法院(2019)苏13刑终32号刑事裁定书;湖南省永顺县人民法院(2018)湘3127刑初105号刑事判决书。

〔30〕参见苏宇、高文英:《个人信息的身份识别标准:源流、实践与反思》,《交大法学》2019年第4期。

〔31〕〔32〕〔61〕参见王华伟:《已公开个人信息的刑法保护》,《法学研究》2022年第2期。

〔33〕相关判决参见安徽省马鞍山市雨山区人民法院(2018)皖0504刑初299号刑事判决书;四川省成都市高新技术产业开发区人民法院(2019)川0191刑初145号刑事判决书;河南省太康县人民法院(2018)豫1627刑初464号刑事判决书。

〔34〕参见上海市金山区人民法院(2018)沪0116刑初839号刑事判决书;上海市第一中级人民法院(2017)沪01刑终279号刑事判决书;广东省江门市中级人民法院(2020)粤07刑终261号刑事裁定书;山东省成武县人民法院(2019)鲁1723刑初397号刑事判决书。

〔35〕参见北京市通州区人民法院(2018)京0112刑初935号刑事判决书;浙江省金华市中级人民法院(2020)浙07刑终33号之二刑事判决书;四川省成都市双流区人民法院(2019)川0116刑初376号刑事判决书;上海市黄浦区人民法院(2017)沪0101刑初932号刑事判决书。

〔36〕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法益的反思》,《政治与法律》2017年第10期。

〔37〕参见敬力嘉:《大数据环境下侵犯公民个人信息罪法益的应然转向》,《法学评论》2018年第2期。

〔38〕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》,《法学》2009年第12期。

〔39〕参见胡胜:《侵犯公民个人信息罪的犯罪对象》,《人民司法》2015年第7期。

〔40〕参见高富平、王文祥:《出售或提供公民个人信息入罪的边界——以侵犯公民个人信息罪所保护的法益为视角》,《政治与法律》2017年第2期。

〔42〕姜涛:《新罪之保护法益的证成规则——以侵犯公民个人信息罪的保护法益论证为例》,《中国刑事法杂志》2021年第3期。

〔43〕参见曲新久:《论侵犯公民个人信息犯罪的超个人法益属性》,《人民检察》2015年第11期。

〔44〕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——以〈个人信息保护法(草案)〉为视角之分析》,《中国刑事法杂志》2019年第5期。

〔45〕〔63〕参见张忆然:《大数据时代"个人信息"的权利变迁与刑法保护的教义学限缩——以"数据财产权"与"信息自决权"的二分为视角》,《政治与法律》2020年第6期。

〔46〕〔49〕〔53〕马永强:《侵犯公民个人信息罪的法益属性确证》,《环球法律评论》2021年第2期。

〔47〕张明楷:《刑法学》第六版,北京:法律出版社,2021年,第1199页。

〔48〕参见高铭暄、马克昌主编:《刑法学》第十版,北京:北京大学出版社,2022年,第488页。

〔50〕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。

〔51〕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。

〔52〕参见王彦强:《牵连关系的类型——基于刑事立法、司法解释规定的分析》,《法学研究》2022年第3期。

〔54〕参见劳东燕:《个人信息法律保护体系的基本目标与归责机制》,《政法论坛》2021年第6期。

〔55〕目前很多公民明知个人信息被侵犯,却选择沉默的现状较为严重。究其原因,是因为个人信息侵权泛滥,而维权困难。正因为这种侵权现状不容乐观,就更应当采取措施加以改变,而不是选择与其和解,在主观上予以认同,容忍其持续存在。

〔56〕〔66〕劳东燕:《个人数据的刑法保护模式》,《比较法研究》2020年第5期。

〔58〕田宏杰:《合作共治:行政犯治理的路径选择》,《法律科学(西北政法大学学报)》2022年第5期。

〔59〕国务院2014年8月7日发布《企业信息公示暂行条例》(中华人民共和国国务院令第654号)。

〔60〕最高人民法院2016年8月29日发布《关于人民法院在互联网公布裁判文书的规定》(法释〔2016〕19号)。

〔62〕喻海松:《〈民法典〉视域下侵犯公民个人信息罪的司法适用》,《北京航空航天大学学报(社会科学版)》2020年第6期。

〔64〕参见刘双阳:《论个人信息自决权刑事司法保护的边界——以已公开个人信息为中心的分析》,《人权》2021年第5期;梁桂平:《已合法公开个人信息再处理的合理限度及侵权认定》,《人民司法》2021年第32期等。

〔65〕马新彦、刘睿佳:《已公开个人信息弱化保护的解释论矫正》,《吉林大学社会科学学报》2022年第3期。

〔67〕参见刘晓春:《已公开个人信息保护和利用的规则建构》,《环球法律评论》2022年第2期;宁园:《"个人信息已公开"作为合法处理事由的法理基础和规则适用》,《环球法律评论》2022年第2期等。

〔责任编辑:邹秋淑〕