论侵犯公民个人信息罪的保护法益

——场景化法益观的理论构造与实践立场

郑泽星

【摘　　要】侵犯公民个人信息罪的保护法益存在个人法益、超个人法益以及混合法益的观点聚讼，其争议的焦点在于个人信息的性质厘定。场景化视域下，以个人信息的性质为依据可以将个人信息区分为一般识别信息、敏感个人信息、复杂隐私信息和单纯隐私信息。其中，单纯隐私信息并非本罪的保护对象。一般识别信息场景中，本罪的保护法益主要表现为个人信息自决权；敏感个人信息和复杂隐私信息场景中，本罪的保护法益主要表现为公民信息安全。因此，侵犯公民个人信息罪的保护法益应为作为个人法益的个人信息自决权和作为超个人法益的公民信息安全。个人信息自决权与公民信息安全之间是并列择一关系，行为只侵害单项法益的情形下，依然可以成立本罪。

【关 键 词】侵犯公民个人信息罪；法益；场景化法益观；个人信息自决权；公民信息安全

【作者简介】郑泽星，中南大学法学院讲师，法学博士。

【原文出处】《清华法学》（京），2023.3.90～105

【基金项目】本文系教育部哲学社会科学重大课题攻关项目“习近平总书记关于尊重和保障人权重要论述研究”(22JZD002)的阶段性成果。

一、问题的提出与学说概况

近年来，随着人民群众生活水平的日益提高，人们对于尊严、体面生活的要求日益增长，个人信息保护作为与民众切身利益密切相关的新法治需求日渐成为全社会的共识。政策层面，党的二十大明确指出要“加强个人信息保护”，为公民个人信息保护擘画了顶层建构；规范层面，《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》(法释[2017]10号，以下简称《解释》)《民法典》《个人信息保护法》相继出台，为公民个人信息保护提供了法律保障；实践层面，司法机关坚决、严厉打击侵害公民个人信息的犯罪行为，为公民个人信息权益的保护奠定了实践基础。与此同时，理论上和司法实践中对于侵犯公民个人信息罪认定的争议依然存在，其中最核心的争议在于本罪的保护法益为何，并集中体现为对处理公开个人信息以及被害人同意情形下处理个人信息的不同处断。学理上关于本罪保护法益的主张存在个人法益说、超个人法益说和混合法益说的分野：

个人法益说观点中，隐私说、个人生活安宁说以及财产说占主导地位：隐私说认为本罪的保护法益为公民隐私权；生活安宁说则认为个人信息不被非法获悉的安宁状态是本罪的法益；财产说则将信息权人对于信息的支配权作为本罪法益。[①]近年来，个人法益论者主要集中于个人信息权说展开论述，总体主张本罪的保护法益为个人信息权，其归属于个人的具体人格权，具有完全私人属性。[②]个人信息权说内部存在多种不同法益主张：信息自决权说主张本罪的保护对象是作为新型权利的个人信息自决权；独立权能说认为个人信息权是一种包含多种权益的独立权能；专有权论者则主张，本罪的保护法益是个人对数据的专有权。[③]

超个人法益论者主张，侵犯公民个人信息罪的保护法益并非公民个人的人身权利，而是多数人法益，具体而言是公共信息安全。④理由在于：公民个人信息中“公民”概念的潜在意义是用以表明“公民个人信息”具有超个人法益属性；侵犯公民个人信息罪的立法宗旨以及该罪的现实状况也表明“公民个人信息”的超个人法益属性。⑤

混合法益说认为，个人信息不仅事关个人的信息安全与生活安宁，而且关系到社会公共利益、国家利益乃至信息主权。侵犯公民个人信息罪的法益结构并非单一的、平面的，而是多元的、立体的，不仅包含公民个人法益，而且包含超个人法益，前者在地位上优于后者。⑥

根据上述，个人法益论者主张本罪的保护法益是个人信息自决权，在处理公开个人信息以及被害人同意情形下处理个人信息场合，行为人因并没有侵害信息权人的信息自决权(个人信息权)而不构成犯罪；超个人法益论者主张本罪的保护法益是公民信息安全，上述情形因侵犯公民信息安全而构成犯罪。可见，侵犯公民个人信息罪保护法益的确定，决定了本罪的适用范围与界限。因此，正确确立本罪的保护法益有着重要的理论意义和实践意义。

鉴于此，本文将以侵犯公民个人信息罪的保护法益为主旨展开讨论。就行文结构而言，本文首先在厘清个人信息内涵的基础上阐释个人信息类型化主张；其次，在个人信息类型化的基础上证成本罪的应然法益，即场景化法益观；最后，在厘定本罪法益的基础上考察司法实务中处理上述案例的应然立场。

二、场景化法益观的理论前提：个人信息的场景化界分

上述个人法益说、超个人法益说以及混合法益说之间的论争焦点在于侵犯公民个人信息罪的法益对象是个人法益(个人法益说)还是集体法益(超个人法益说)，或是二者兼而有之(混合法益说)。三种观点争驳的核心在于个人信息的性质为何，即公民个人信息是个人隐私还是个人信息，公民个人信息权益是私法权利还是公法权利，并最终归结为侵犯公民个人信息罪的保护法益是个人法益还是社会法益的争论。由此，讨论侵犯公民个人信息罪法益，首先应当厘清公民个人信息的性质和类别，而讨论上述问题的前提在于确定公民个人信息的基本内涵。据此，下文将首先讨论公民个人信息的内涵，并在此基础上厘清个人信息与隐私信息的关系，进而对公民个人信息作出合理类型化。

(一)正本清源：公民个人信息内涵的厘定

学理上，关于如何界定个人信息的内涵存在不同的学说主张，包括隐私说、识别说、关联说以及新识别说。隐私说认为公民个人信息即为公民隐私信息，⑦侵犯公民个人信息罪强调通过打击非法取得涉及公民隐私性信息的行为，实现对公民人身权、财产权、隐私权的保护。⑧识别说认为，可识别性即个人信息与信息主体存在某一客观确定的可能性，是个人信息最重要的特征。识别说的目的在于平衡个人信息保护和信息流动之间的张力。⑨与识别说主张从信息到个人的识别不同，关联说主张从个人到信息的识别，即已知既定个人而知晓或者收集关于该个人的其他信息。⑩新识别说在传统识别说的基础上，将个人信息理解为“光谱”，对个人信息进行分层界分，由内向外分别为直接识别信息、间接识别信息以及不可识别信息。⑪综合来看，隐私说将个人信息与个人隐私等同，在大数据时代，这种混同的观点因为过度限缩了公民个人信息的内涵而日益被边缘化。在本文看来，识别说、关联说、新识别说实际上在一定程度上已经达成了理论共识，即公民个人信息是指具有可识别性的信息，在某种情形下，可识别性表现为关联性。易言之，如果通过与公民个人相关联的信息，可以追溯到某特定的自然人，此时，关联信息也表现出识别性。正如有学者指出的，“直接识别”信息之外，能够与个人“关联”或“绑定”的信息均属于个人信息，即是将关联信息与“间接识别”信息等同。⑫因此，将公民个人信息理解为既包含公民个人识别信息，也包含公民关联信息，是恰当的。

从各国的立法实践来看，上述观点也可以得到

印证。各国法律关于个人信息的界定大致可以分为两类:第一类为综合模式,认为个人信息包含与自然人相关的所有信息。例如,欧盟2016年通过的《一般数据保护条例》中规定,个人信息指的是任何已识别或可识别的自然人(信息主体)相关的信息。[13]美国没有统一的个人信息保护法,而是通过隐私权对个人信息加以保护。美国司法部《1974年隐私法概述》中将个人信息定义为包括与可识别的特定信息相关的个人信息,不限于直接反映个人特点或特质的信息。[14]第二类为个人识别信息模式,认为个人信息仅仅包含个人识别信息。例如,日本《个人信息保护法》规定,本法所称"个人信息"是指可以通过信息中包含的姓名、出生日期和其他描述来识别特定个人的在世人的信息。[15]其中,综合模式是各国立法实践的主流。

我国的立法实践基本上采纳了学理通说:2017年出台的《解释》中对个人信息作出了明确界定:"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";2020年颁布的《民法典》将个人信息界定为:"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";2021年通过的《个人信息保护法》则将个人信息规定为:"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。"有学者指出,《解释》中对于公民个人信息内涵的界定超出了《个人信息保护法》中对公民个人信息的界定:前者所言的个人信息包含了"反映自然人活动情况的各种信息",而后者指称的个人信息仅仅指"识别信息";前者将个人信息的识别对象规定为"自然人身份",后者将个人信息的识别对象界定为"自然人"。[16]在本文看来,《解释》《民法典》以及《个人信息保护法》对于个人信息的界定是一致的:《民法典》中列举的个人信息包含了"行踪信息"等反映自然人活动情况的信息,《个人信息保护法》也规定"敏感个人信息"包含"行踪轨迹"等反映自然人活动情况的信息。而上述《解释》中识别特定"自然人身份"意为识别"自然人",而非识别"自然人的身份",原因在于,该解释所列举的"姓名、身份证件号码、通讯联系方式、住址"等识别信息,只能识别"自然人是谁"而不能识别"自然人是何种身份"。综合上述,从法域协调的角度来看,公民个人信息包括身份识别信息,也包括体现特定自然人活动情况的信息。[17]

(二)包容抑或区隔:个人信息与个人隐私信息的界分

个人信息与隐私信息的关系涉及侵犯公民个人信息罪保护对象的确立,是确定侵犯公民个人信息罪法益不可回避的问题。

关于个人信息与隐私信息的关系,学理上存在包容说、区分说和混合说的争驳。包容说认为,个人信息包含个人身份信息和隐私信息。具体而言,个人身份信息包括姓名、性别、年龄、有效证件号码、婚姻状况、工作单位等能够识别公民个人身份的信息,而个人隐私信息则包括个人财产状况、生理及健康状况、活动记录等信息。[18]混合说认为,隐私信息具有相对性,凡是个人不愿公开的个人信息都是隐私信息。个人信息与隐私信息的联系在于:一方面,许多未公开的个人信息本身就属于隐私的范畴;另一方面,部分隐私权保护的客体因其具有可识别性也属于个人信息的范畴。[19]区分说则认为,个人隐私信息与个人信息相互区分,前者仅涉及公民私密性信息或者活动,与国家或者公共利益无涉,也不涉及财产价值,更多与公民的人格尊严、精神、情感需求相关;后者的关键则在于信息的"共享",与公民人身安全和财产安全密切相关。[20]也有学者指出,对个人信息的保护主要包括个人信息的支配权和自我决定权的保护,而对于隐私权保护的重点在于防范个人秘密被非法泄露。[21]

在本文看来,上述诸说间的争论主要源自概念语意界定不清。一方面,个人信息表现出强烈的人身属性,即个人信息与自然人紧密相连,表现出可识别性和私密性;另一方面,个人信息则表现出财产性和公共性,与公民的个人财产安全甚至公共利益密

切相关。易言之,个人信息是个人隐私权、人格权乃至财产权的综合载体。[22]基于此,本文认为,个人信息可以区分为广义个人信息和狭义个人信息:广义个人信息是指与公民个人相关联的所有信息,包含个人隐私信息和个人识别信息,[23]包容说所指的个人信息即是广义个人信息;狭义个人信息即个人识别信息,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的各种信息,我国《民法典》中规定的个人信息即属此类。[24]个人识别信息(狭义个人信息)又可以区分为敏感个人信息和一般识别信息:前者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,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息;[25]后者则指敏感个人信息之外的其他能够识别公民个人身份的信息。广义个人信息语境下的个人隐私信息是指个人不愿披露且不涉及公共利益的个人私密性信息或者个人活动信息。[26]在本文看来,个人隐私信息仍可以区分为单纯隐私信息和复杂隐私信息:单纯隐私信息是指与公民人格尊严、精神情感密切相关,与公共利益无涉,“虽然其可以被利用,但其财产价值并非十分突出”[27]的隐私信息;复杂隐私信息是指既与自然人的人格尊严、精神情感密切相关,又与公民的经济利益、财产利益密切相关的信息。前者如自然人的特殊疾病病史等;后者如自然人购买私密物品的记录。这类信息一方面与个人私生活密切相关,另一方面对于特定商家而言,这些隐私信息又体现为经济利益,商家可以借此进行精准广告投放。对于单纯的隐私信息应否作为侵犯公民个人信息罪的保护对象,虽然有学者指出,“考虑到我国尚未设置侵犯个人秘密或隐私犯罪这一立法疏漏,不应将个人隐私排除在本条的犯罪对象之外。甚至可以期待,本条能发挥侵犯个人隐私罪或者泄露个人隐私罪的功能”,[28]但是这一论断显然有悖罪刑法定原则,而极易滑向罪刑擅断的深渊。根据《民法典》的规定,“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”,[29]因此,就侵犯公民个人信息罪而言,单纯的隐私信息并非其保护对象,而复杂个人信息因其涉及经济利益、财产利益而当然是本罪的保护对象。当然,上述关于个人信息和个人隐私界分的尝试必须认识到“个人隐私及个人信息保护的边界并非固定、僵化的,而是主观的、动态的,并受多重因素影响”。[30]事实上,前述复杂隐私信息与敏感个人信息之间的界限在有些情形下就是模糊不清、难以界分的。

(三)殊途同归:个人信息的分类保护思路与借鉴

个人信息种类繁多、形式多样,侵犯个人信息的行为也表现出多样性和复杂性,相应的,对于公民个人信息的保护也是一项“复杂工程”。理论上,个人信息分类保护的思路为多数学者所认同。分类保护思路下,仍然存在两种不同的思路,分别为个人信息分层思路和个人信息场景化思路:个人信息分层思路认为,应当根据个人信息的不同性质将个人信息划分为不同层级,根据不同个人信息类型的保护层级,合理确定保护的尺度,实现个人信息的保护强度与保护必要性的协调。[31]场景化思路的基本内涵是指个人信息原始收集时的具体语境应得到尊重,其后续传播及利用不得超出原初的情境脉络。具体而言,个人信息保护的合理程度要置于其所处的环境中具体审视,避免脱离场景做抽象预判。[32]

不难发现,个人信息分层视角以个人信息与自然人、自然人人身安全、财产安全的关联程度为依据区分个人信息的敏感程度,从而将个人信息予以分层,[33]而场景化理论则关注个人信息的使用场景或者侵权场景,在具体的场景中判断行为人合理使用信息的限度或者责任承担边界。个人信息分层观点与场景化理论在很大程度上是相互契合的:第一,正如有学者所指出的,个人信息场景化保护的依据在于信息权益的场景化,[34]而个人信息的性质很大程度上决定了其信息权益(被利用或者被侵害)场景。例如,对于个人识别信息而言,其通常被利用的场景在于对自然人的辨认或识别,侵犯个人识别信息通常侵

害的是自然人的信息支配权和决定权;[35]而对于一旦泄露将导致自然人的人格尊严受到侵害或者人身、财产安全受到侵害的敏感个人信息,除正常的业务授权外,一般不存在授权使用情形,此类信息的侵权场景通常是公民的信息安全。

应当指出的是,上述个人信息分层理论依据《解释》第5条的规定对个人信息进行分层,并将"行踪轨迹信息"单独列为最核心层级的观点是值得商榷的:其一,就规范的本意而言,《解释》第5条第1款第1项规定,"出售或者提供行踪轨迹信息,被他人用于犯罪的",其重心在于"被他人用于犯罪"的结果,事实上是针对"损害结果"的特别规定,而并非承认行踪轨迹信息具有更高的敏感性;其二,就对象的事实特征而言,虽然个人行踪信息更容易被用于针对公民人身的犯罪,但与同样规定在《解释》第5条第1款第3项的通信内容、征信信息、财产信息相比,个人行踪轨迹信息并不具有更高的敏感性,后者也极易被用于针对公民人身、财产的犯罪;其三,就法秩序的内部统一性而言,《个人信息保护法》将行踪轨迹信息与医疗健康信息共同规定为敏感个人信息,[36]而《解释》则将行踪轨迹信息与健康生理信息规定在不同项,[37]易言之,《解释》认为行踪轨迹信息与健康生理信息具有不同敏感性。因此,在法秩序内部规定并不统一的情形下仅以《解释》为依据对个人信息进行分层,是不妥当的。

综合上述,个人信息分层理论与场景化理论具有相互契合性,以《解释》为依据的个人信息分层理论不具有妥当性。因此,分类保护思路下,应当寻求更为妥帖的分类方法。基于此,本文更倾向于前文场景化个人信息的分类(分层)方法,即将广义的个人信息区分为个人识别信息(狭义个人信息)和个人隐私信息。其中,个人识别信息包含一般识别信息和敏感个人信息,而个人隐私信息则包含单纯隐私信息和复杂隐私信息。侵犯公民个人信息罪的保护对象包括一般识别信息、敏感个人信息和复杂隐私信息,单纯隐私信息并不属于本罪的法益对象。下文的相关论述也将基于这一分类展开。

三、侵犯公民个人信息罪的应然法益:场景化法益观概观

事实与规范的互动是司法活动的重要形式,法官需要心中充满正义,目光往返流转于事实与规范之间。司法实践中,侵犯个人信息的具体形式与具体场景复杂多变、多种多样,而加强个人信息保护是个人信息保护法律规范的基本共识与主要目的,[38]如何使复杂多样的个人信息实践侵犯样态与法律规范的具体保护规定相互契合,进而实现个人信息保护的规范目的,是法教义学的重要使命。场景化视域下确定侵犯公民个人信息罪保护法益的基本逻辑在于:出售、提供、非法获取公民个人信息行为之所以应受刑罚处罚是因为其侵害了刑法所保护的法益,在具体侵犯公民个人信息场景中,基于法规范,在对个人信息权益侵害进行犯罪现象论描述的基础上展开法教义学阐释,正是揭示具体信息场景中侵犯公民个人信息罪保护法益的过程。

在一般识别信息场景中,信息主体对于此类信息的支配通常表现为授权他人收集、使用、加工、处理、传输,甚至在某些情形下,只有授权信息收集才能使用商家的某些服务。例如,用户在使用某社交App时,要授权App收集其姓名、性别、年龄、手机号码等信息,如果用户拒绝授权,则不能使用此App。对于一般识别信息的处理通常不会直接侵害公民的人身安全和财产安全,而刑法却将出售、提供、非法获取公民此类信息的行为纳入规制范围,究其原因,上述行为侵害了信息权人的重要权益。而从犯罪现象描述角度看,出售、提供、非法获取公民个人信息的行为所侵害的个人信息权益表现为公民的"信息自决权"。[39]信息自决权最早形成于私权立场上抵制公权对于公民个人信息过度收集的努力:1983年德国联邦宪法法院关于人口普查的判决中确立了"信息自决权"的雏形,"个人数据免受无限制的收集、存储、使用和披露"。[40]2001年通过的《德国联邦个人数据保护法》规定了个人信息权的主要内容包括在收集、处理和使用信息过程中当事人的知情权和决定权,[41]将个人信息自决权从私权对抗公权的防守权利

扩展为公民排他的权利，“出于公共利益的考量”则否定了个人信息自决权的绝对排他属性。[42]我国《个人信息保护法》以个人同意为基础构建公民个人信息自决权，包括公民对于个人信息处理的同意、变更同意和撤回同意。[43]申言之，个人信息自决权具体表现为权利人对于个人信息的支配和自主决定，主要包括个人对信息被收集、利用等的知情权，以及自己利用或者授权他人利用的决定权等内容。[44]因此，既然在犯罪描述意义上，一般识别信息场景中侵害个人信息自决权是行为人构成侵犯公民个人信息罪的主要考量，相应地，在该信息场景中，侵犯公民个人信息罪的保护法益主要表现为个人信息自决权。

在敏感个人信息和复杂隐私信息场景中，除业务授权场合(例如，用户在某外卖平台上传自己的银行账户信息)，公民通常情况下不会授权他人收集、使用、加工、处理、传输自己的此类信息。因此，公民对此类信息所享有的“信息自决权”并不显见。而侵犯此类个人信息的场景中，行为人的行为之所以应受刑法规制，是因为此类信息通常与公民人身财产密切相关，信息泄露或者不当处理会直接或者间接侵害公民甚至公众的人身安全和财产安全，此类信息场景中，对于公民信息安全考量尤为重要。正因为敏感个人信息和复杂隐私信息场景中，行为人对此类信息的侵害往往表现为对公民信息安全的危害，因此，在此类信息场景中，侵犯公民个人信息罪的保护法益主要表现为公民信息安全法益。“安全”的基本内涵是不受非法侵害，亦即公民个人信息不被非法获取、出售和提供。其中，非法获取既包括未经允许获取公民信息，也包括经公民同意获取个人信息后，公民撤回同意情形下的个人信息处理行为；非法出售和提供既包括将公民个人信息出售或提供作侵害公民人身安全和财产安全的违法行为或犯罪行为，也包括超出个人信息原本用途出售和提供个人信息。

关于场景化法益观，在其具体内涵之外仍有两个基本问题需厘清：

其一，关于场景化法益观中两种法益的关系。为在司法实践中正确适用本文所提出的法益观点，有必要对个人信息自决权与公民信息安全法益之间的关系以及具体判断规则进行阐述。从形式上看，两者关系类似复杂客体中不同客体要素之间的关系。其实不然，两者在生成逻辑上存在本质差异。复杂客体理论要求行为在同一犯罪场景中必须同时侵害主要客体和次要客体，[45]主要客体和次要客体之间的逻辑关系是联言命题关系，其逻辑构造为“P并且Q”，其构罪逻辑在于，只有同时满足P情形和Q情形才构成本罪。需要注意的是，如果行为只侵害复杂客体中的一种客体，可能成立犯罪未遂，此处仅讨论犯罪既遂情形。侵犯公民个人信息罪场合，由个人信息侵权状况复杂性所决定，存在多种应受刑法规制的侵犯个人信息场景。不同场景所对应的个人信息法益也有所不同，不同场景中行为是否构成犯罪的判断是独立开展的。易言之，侵犯公民个人信息罪场合，其法益侵害性判断是在不同场景中单独进行的，而在具体判断中，只要侵害一种法益，即构成本罪。本罪中，个人信息自决权法益与公民信息安全法益之间的逻辑关系是相容选言命题关系，其逻辑构造为“P或者Q”，其构罪的逻辑在于，满足P情形或者满足Q情形均构成本罪，同时满足P情形和Q情形，也当然构成本罪。因此，关于侵犯公民个人信息罪中两种法益之间的关系，本文的基本论断是：两者并非复杂客体理论不同客体之间的联言命题关系，即“与”的逻辑关系，而是受个人信息具体侵权场景的特殊性影响而形成较为独特的相容选言逻辑关系，即“或”的逻辑关系。在具体的判断场合，一般识别信息场景中，本罪通常侵害的法益为个人信息自决权，而在敏感个人信息和复杂隐私信息场合，本罪通常侵害的法益为公民信息安全。当行为人的行为侵害本罪的任一种法益时，行为人即可以构成本罪；当行为人同时侵害本罪的两种法益时，行为人当然可以构成本罪。

其二，关于“场景化法益观”的指称。场景化视域下侵犯公民个人信息罪法益观点本质上是一种混合法益观点，但其与传统混合法益观存在如下不同：其一，就理论内涵而言，场景化视域下的法益观点不

仅指出了侵犯公民个人信息罪的混合法益归属，而且揭示了本罪混合法益归属的实质，即不同的信息使用(侵权)场景对应不同的法益侵害内容。其二，就实践品质而言，场景化视域的法益观点指示了侵犯公民个人信息罪适用的实践立场，即基于不同的信息场景进行具体判断。因此，相较于传统混合法益观，场景化视域的法益观点理论内涵更加丰富、实践立场更加鲜明，倘以混合法益观指称，并不能体现其理论特色。有鉴于此，本文将场景化视域的侵犯公民个人信息罪法益观点称为“场景化法益观”。

四、混合法益实质：场景化法益观的理论证成

作为混合法益观的一种，场景化法益观的总体观点在于主张本罪一方面侵害作为个人法益的公民个人信息自决权，另一方面侵害作为超个人法益的公民信息安全。因此，对于本罪法益论争中针对个人法益和超个人法益的批评，场景化法益观也应当自觉予以回应。

(一)对于个人法益否定观点的回应

首先，个人法益观否定论认为，大数据环境下，公民对于个人信息并不具有自决权。就商业服务角度而言，网络服务提供者提供的看似保障公民个人信息自决权的使用协议实际上是公民放弃个人信息自决权的“声明”。就行政服务而言，行政主体从便于加强社会控制的角度出发，在不同场景中运用行政权力进行广泛信息收集和处理，公民个人信息自决权无从谈起。[46]在本文看来，公民个人信息自决权保护虚置的现状并不能成为否定公民个人信息自决权的理由，正如有学者所指出的，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。[47]《个人信息保护法》明确规定“个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务。处理个人信息属于提供产品或者服务所必需的除外”，[48]事实上已经宣示了公民个人信息自决权。在处理个人信息属于提供产品或者服务所必需的场合，个人信息和产品服务深度捆绑，用户选择接受产品和服务，实际上就已经行使了个人信息自决权。例如，手机App提供导航服务是以获取被服务者位置信息为必要的，如果用户选择接受导航服务，即已同意授权导航服务提供者使用其位置信息；另一方面，用户完全可以拒绝导航服务提供者使用其位置信息进而拒绝使用该导航服务。使用与不使用该服务之间，体现了公民个人信息自决权的行使。

其次，个人法益观否定论者还指出，个人信息的社会属性决定侵犯公民个人信息罪的保护法益并非公民个人信息自决权，刑法保护公民个人信息并非保护信息本身，而是保护关涉主体的相关权利。[49]个人信息的确带有社会属性，个人信息保护最终目的是保护信息背后的公民个人信息权益，这是毋庸置疑的。但是个人信息的社会属性并不能否定个人信息自决权作为侵犯公民个人信息罪的保护法益。个人信息的社会属性实际上是个人属性的集合，个人信息的社会属性所体现的实际上是超个人法益性质，而超个人法益应当是可以被还原为个人法益的法益类型，[50]因此，就侵犯公民个人信息罪的保护法益而言，其个人法益侵害性与其超个人法益侵害性(社会法益侵害性)并不冲突。

(二)对超个人法益否定观点的回应

首先，有学者通过区分个人数据和个人信息来否定公民个人信息的超个人法益属性。该主张认为，公民在使用导航类App时，只让渡了对数据的权属，而仍保留对个人信息的权属，仍然体现个人信息自决的特征，因而否定公民个人信息的超个人法益属性。[51]事实上，数据与信息的根本区别不在于形式上的差异，即无论其是“编程语言处理的对象”，还是“利用信息技术呈现的内容”，只要能够识别到具体自然人，就应当认为其属于个人信息。易言之，经过匿名化处理的个人数据并非侵犯公民个人信息罪所保护的对象，这与《个人信息保护法》中个人信息“不包括匿名化处理后的信息”的规定相契合。而对于导航类App而言，一方面，信息处理企业应当将使用者的信息进行匿名化处理，另一方面，基于网络信息实名制现状，在信息处理企业同时掌握使用者的个人身份信息的情况下，以编程语言为表现形式的数

据，随时可以通过技术手段还原成与特定自然人个体相关的信息。因此，在个人信息与产品服务深度捆绑的场合，区分个人数据和个人信息并非必要，公民让渡个人数据权属的实际效果与让渡个人信息的实际效果是一致的，公民对于个人信息的自决权体现在其有权决定是否使用该产品或服务。

其次，有否定论学者认为，超个人法益观点在法益理论上倾向于集体法益一元论，而在个人法益与集体法益同时存在于刑法中时，尤其应当警惕集体法益的扩张性潜能。[52]事实上，集体法益与个人法益并非天然冲突，集体法益的价值支撑和预设是对人的利益的保护，在人的利益这一终极意义上，个人法益与集体法益得到了统一。[53]警惕集体法益的扩张性潜能和风险的担忧具体体现在个人法益与集体法益相冲突的场域，而对于侵犯公民个人信息罪场合，个人法益与集体法益是高度统一的。“公民个人信息”首先是个人法益，然后才具有超个人法益属性：[54]一方面，个人信息与公民个人是深度捆绑融合的，个人信息法益必须依附于个人法益存在；另一方面，对于个人信息的刑法保护，尤其是对于敏感个人信息和复杂隐私信息的保护，不可否认体现了集体法益(超个人法益)的特征。

再次，有学者指出，如果将侵犯公民个人信息罪的法益认定为信息安全(作为公共安全的一种)是不正确的，因为无法证成侵犯公民个人信息的行为能够危害不特定多数人的生命、身体和财产权利。[55]上述论断混淆了“公共安全”与“安全”的概念：法规范语境下的安全是指法益的安全，内涵是防止法益侵害危险；[56]解释论上，公共安全可以理解为公众安全，意指不特定多数人的生命、身体和财产权利不受非法侵害，“公共安全”与“安全”的内涵是完全不能等同的。例如，盗窃罪侵害的法益是公民财产安全，其正确理解应当是公民财产不受非法侵害，如果依照上述论者的逻辑，将盗窃罪的保护法益理解为财产公共安全，要求判断盗窃罪在侵犯公民财产的同时是否侵害不特定多数人的生命、身体安全，这显然是荒谬的。有超个人法益论者以“公共信息安全”[57]指称个人信息罪的保护法益，“公共信息安全”意指公众信息安全，是指公众的信息不受非法侵害的状态，其区别于“信息公共安全”。在本文看来，“信息公共安全”是一个伪概念，信息受侵害很难直接导致公共安全法益的减损。

复次，有学者指出，就体系地位而言，侵犯公民个人信息罪在刑法典中的章节地位决定了该罪侵犯的是个人法益。就犯罪性质而言，侵犯公民个人信息罪是带有法定犯气质的自然犯，因此，其侵害的法益应为个人法益而非超个人法益，理由在于，保护超个人法益的规定，很可能安排危险构成要件；保护个人法益的规定，大多以实害或具体危险的构成要件陈述，而侵犯公民个人信息罪的构成要件是典型的实害犯构成要件。[58]

以某一罪名在刑法典中的章节地位来确定该罪名所侵害的法益，显然是不足取的。[59]刑法典中规定的罪名并非都是侵害单一法益的，其在刑法典体系中的排序是以其所侵害的主要法益为依据的。例如，抢劫罪规定在侵犯财产罪一章，但不可否认的是抢劫罪同时侵害公民的人身安全法益。侵犯公民个人信息罪置于侵犯公民个人权利一章，完全可以因为侵犯公民个人信息罪的法益基础是个人法益，但并不能以此作为否定其侵害超个人法益的理由。至于本罪的犯罪性质，在本文看来，侵犯公民个人信息罪的犯罪构成并非典型实害犯，而带有危险犯的性质。从侵犯公民个人信息罪的立法背景来看，《刑法》第253条之一对本罪作出修改完善的直接原因是“侵犯公民个人信息犯罪仍处于高发态势，不仅严重危害公民个人信息安全，而且与电信网络诈骗等犯罪存在密切关联，甚至与绑架、敲诈勒索等犯罪活动相结合，社会危害日益突出”。[60]可见，保护公民个人信息安全的根本目的在于防止公民个人信息泄露而导致的针对公民人身和财产的犯罪。正如有学者所指出的，侵犯公民个人信息犯罪在实际生活中主要表现为对公众个人信息的侵犯，以及由此而产生的间接侵害与威胁。[61]假设个人信息泄露不具有导致侵害公民人身和财产犯罪风险，那么对于个人信息

泄露行为也无须进行刑事处罚。由此可见,侵犯公民个人信息罪是行为犯,[62]而刑法对其处罚的依据在于行为的抽象危险,即强调在行为造成抽象危险时刑法就提前介入,这种危险是立法者拟制的危险或抽象的危险,由此形成法益保护的前置化现象。[63]就此种意义而言,实定法层面的侵犯公民个人信息罪并非实害犯构成要件,而具有了抽象危险犯的性质。因此,据此否定本罪保护超个人法益的观点,也是值得商榷的。

(三)场景化法益观的再阐释

综合上述,侵犯公民个人信息犯罪的保护法益既非个人法益论者所主张的单纯个人法益,也非超个人法益论者所主张的单纯超个人法益,而是既包含个人法益又包含超个人法益的混合法益类型。学理上,混合法益论者的论证并不充分,因此,混合法益说并没有被学者们广泛认同。以个人信息场景化分类为基础的场景化法益观可以较好解决混合法益说论证不足的问题:对于一般个人识别信息而言,通常情况下公民行使的是对个人信息的知情权和决定权,也即公民个人信息自决权;而对于敏感个人信息和复杂隐私信息而言,通常情况下公民并不会授权他人收集、使用、处理自己的此类信息,因此,在此类场景中,刑法所保护的是公民个人信息不被非法获取、出售和提供的权利,也即公民信息安全。由于侵犯公民个人信息罪通常表现为对数量庞大的公民群体个人信息的侵害,侵害对象表现出不特定性,并且利用个人信息针对信息主体或者其他公民的犯罪具有不确定性。公民信息安全不再是个人法益而集合成超个人法益。因此,敏感个人信息和复杂隐私信息场景中,本罪的保护法益应为超个人法益,具体而言是公民信息安全法益。

五、场景化法益观的实践立场

基于上文对场景化法益观的阐述,本文结合司法实践中的具体案例,阐明场景化法益观的实践立场。

(一)侵犯公民个人信息罪典型案例评析

案例1:吴某在天眼查、企查查等网站下载公开的各地企业工商登记信息,梳理分类后共出售1.8万余条,获利1万余元。公安机关以涉嫌侵犯公民个人信息罪传唤吴某,后该案被移送人民检察院审查起诉。检察机关基于《民法典》的规定,建议公安机关撤销案件。[64]

案例2:孙某将自己从网络收集、互换得到的4万余条含自然人姓名、电话号码、电子邮箱等的个人信息,通过微信、QQ等方式以人民币34000元的价格贩卖给案外人刘某。案外人刘某在获取相关信息后用于虚假的外汇业务推广。公益诉讼起诉人据此提起民事公益诉讼。杭州互联网法院判决孙某支付侵害社会公共利益的损害赔偿款34000元,并向社会公众公开赔礼道歉。[65]

案例3:张某通过网络寻找愿意出售个人信息者注册网络店铺账号,再将账号注册人的身份证、银行卡等整套个人信息打包为“产品”,通过QQ“卡商群”和交易网站“叫卖”,明码标价转卖给他人。该类信息大多被用于售假、诈骗等违法犯罪活动。[66]

案例4:解某、辛某雇佣多人通过在网络、微信公众号上发布贷款广告吸引有贷款需求的人填写“姓名、手机号、有无本地社保和公积金、有无负债、房产和车辆持有状况、工资收入、有无保险、征信情况、借款需求、还款周期”等信息,共收集信息31万余条。再通过微信群、微信公众号获取银行、金融公司信贷员的姓名和手机号码。后将信息以每条30元至150元的价格出售给信贷员。通过出售上述信息,解某、辛某共获利450余万元。后解某、辛某等被告人被以侵犯公民个人信息罪判处有期徒刑三年六个月到一年四个月不等。[67]

在上述案例中,案例1、案例2中行为人的行为均表现为收集公开的个人信息并转售获利,但其所受到的司法处遇大不相同:案例1中案件被撤销,案例2中的行为人被公益起诉并承担民事赔偿。案例3和案例4中,行为人转卖他人自愿出售或者自愿提供的个人信息,是否构成侵犯公民个人信息罪,在理论上和司法实践中也存在不同意见。[68]

由上述案例可知,公开个人信息以及被害人同

意情形下处理个人信息案件的处理在司法实践中是存在争议的。对此,本文在场景化法益观视角下予以分别阐释。

(二)处理已公开个人信息的刑法规制

处理已公开个人信息是否受刑法规制的问题,在《民法典》《个人信息保护法》通过之前,一直存在有罪说和无罪说的争论,而且有罪说占据多数说的地位。上述两法通过之后,基于其规定,[69]处理已公开个人信息在司法实践中出现了无罪化的处理倾向。对于此类案件的处理,在司法实践中存在二次授权的观点,即在个人信息已被公开的情况下,如果收集这些信息并再次向他人提供,即需要获得权利人的二次授权。事实上,二次授权方案在法律层面和实践层面均受到质疑:法律层面,二次授权方案缺乏实定法支撑,《民法典》第1036条、《个人信息保护法》第27条的规定已经否定了二次授权方案。[70]表面来看,《民法典》第1036条和《个人信息保护法》第27条的规定与《解释》第3条第2款的规定似有冲突之处。事实上,前者明确规范对于公开个人信息处理的行为,而后者则侧重于强调信息收集者对于已合法收集到的个人信息的妥善保管义务,两者并不冲突。实践层面,二次授权面临着诸如"难以对一次授权和二次授权进行区分"以及"在实践中难以操作,容易压缩信息公开的空间"等诘难,[71]存在实际操作的困难。如何合理保护公开个人信息并限制刑法适用的边界,有学者提出了合目的性考察的思路,认为处理已公开个人信息的行为应否入罪,应当结合处理公开信息的目的和用途综合考量。具体而言,对于已公开个人信息的处理只有在"明显违背已公开个人信息的公开目的""明显改变已公开个人信息的用途"以及"利用已公开个人信息实施可能危及公民人身或财产安全的违法犯罪行为"时,才成立侵犯公民个人信息罪,否则,不构成本罪。[72]但是,在司法实践中,合目的性考察的思路又面临着诸如"个人信息公开的目的和用途具有多元性、复杂性和模糊性"以及"主观的目的性与客观的公开性之间存在一定的内在冲突"等实践困境。[73]

本文认为,处理已公开的个人信息应否受到刑法责难,应当考察其是否侵犯公民个人信息罪的法益。根据本文所提出的场景化法益观,本罪的保护法益为混合法益,即既包括对公民个人信息自决权的保护,又包括对公民信息安全的保护。有学者指出,对于公开个人信息的保护应当区分个人信息公开是否出于自愿:对于自愿、主动公开的个人信息不宜以本罪论处;对于非自愿、非主动公开的个人信息,可以构成本罪。[74]《个人信息保护法》则规定,公开的个人信息包括个人自行公开和已经合法公开的个人信息,并对两者进行无差别保护。[75]而对于非自愿、非法公开的个人信息,当然应当受到刑法保护。在本文看来,合法公开的个人信息是基于法定事由依法进行公开的,其通常与公民的权利或者权益密切相关。例如,有关部门为救济、救助或者奖励而公示的公民个人信息是基于程序公正的要求而依法公开。在某种程度上可以认为,公民接受救济、救助或者奖励的同时,即已放弃了对于此类信息公开的自决权。因此,对于合法公开的个人信息,无须再考虑公民是否自愿公开。本文认为,对于已公开个人信息,可以区分为非自愿且非法公开的信息与自愿或者合法公开的信息进行保护。[76]前者如行为人通过公开的账号和默认密码登录平台获得商家的诚信通账号密码信息;后者如律师为拓展案源主动在互联网上公布自己的联系方式、执业经历等。前一种情形中,对于非自愿且非法公开的个人信息,公民不仅享有信息安全权益,而且依然享有个人信息自决权,此种情形下,当行为人收集权利人的信息,即已侵害了公民的个人信息自决权,从而具备了构成本罪的可能,即便行为人没有后续的"提供"或者"出售"行为也依然可以成立本罪。后一种情形中,行为人主动公开自己的个人信息即已是对个人信息自决权的行使,刑法不再保护其信息自决权。但是,即便对于可以公开且必须公开的个人信息,个人应当也有一定的控制权,[77]这种控制权体现在,如果行为人"提供"或者"出售"上述信息,侵害公民信息安全的,依然可以成立本罪。公民信息安全的基本内涵是个人

信息不受非法侵害，亦即公民个人信息不被非法获取、出售和提供。其中，非法获取既包括未经允许获取公民信息，也包括经公民同意获取个人信息后公民撤回同意情形下的个人信息处理行为；非法出售和提供既包括将公民个人信息出售或提供作侵害公民人身安全和财产安全的违法行为或犯罪行为，也包括超出个人信息原本用途出售和提供个人信息。

依照《民法典》和《个人信息保护法》的规定，对于公开个人信息，可以在合理范围内进行处理。司法实践中，司法机关援引《民法典》第1036条、《个人信息保护法》第27条的规定对处理公开个人信息行为人予以出罪(如前述案例1)是不存在争议的，但如果直接援引该二条规定的“自然人明确拒绝或者处理该信息侵害其重大利益”“个人明确拒绝”或者“对个人权益有重大影响”等否定条件作为入罪的标准则并非合理：“由于刑罚手段的严厉性，进入刑法视野的法益必然具有相当程度的重要性。而且，个人信息的法律保护是一个体系，根据对于个人信息侵犯的程度不同，应该由不同的法律予以保护”。[78]本文认为，出售、提供公开个人信息的入罪门槛应当高于出售、提供非公开个人信息的入罪门槛。具体而言，对于处理公开个人信息的，只有当行为人的获取、提供行为危害公民或者公众财产安全或者人身安全时，才构成本罪。合理范围内的盈利行为，不宜认定为本罪。例如，上述律师公开个人信息的案例中，如果行为人收集律师公开的个人信息在某找法平台上出售，不构成本罪；如果行为人收集律师公开的个人信息打包出售给境外诈骗团伙，则侵害了公民信息安全法益，仍然可以构成本罪。

(三)被害人同意情形下处理个人信息的刑法规制

对于被害人同意情形下的获取、提供和出售个人信息的行为应否承担刑事责任，否定论者主张，在被害人知情同意的场合，如果相关信息的获取及其用途得到公民个人的同意，即便被用于针对个体公民的人身犯罪或财产犯罪活动，基于被害人同意的原则，仍不能认为行为人成立本罪。[79]事实上，被害人同意的内容往往是个人信息的利用，而对于个人信息被非法利用而造成的自身或者他人财产损失或者人身伤害，显然超出了被害人同意的范畴。因此，上述认识显然不利于公民个人信息的有效保护，也违背了本罪设立的初衷。刑事责任肯定论者则主张，所谓“被害人同意”不能作为出罪事由，不能排除信息“叫卖者”行为的刑事违法性。[80]根据本文所主张的场景化法益观，被害人同意情形下的信息收集行为并不侵害公民的个人信息自决权。但如果行为人后续的提供、出售行为仍然具有侵害公民人身安全和财产安全的可能，那么，行为人依然可以侵害公民信息安全法益，可以构成本罪。不同于上述否定论者所主张的“公民个体社会交往利益的侵害衍生自信息自决权的侵害，其在位阶上从属于个人信息自决权”，[81]本文所主张的个人信息自决权法益和公民信息安全法益之间并非从属关系，而是并列关系。易言之，即使行为没有侵害被害人的个人信息自决权，而只侵害信息安全法益，仍然可以成立本罪。

(四)场景化法益观视域下前述案例的应然立场

案例1中，行为人从网站上下载的已公开企业工商登记信息，严格意义上并非公民个人信息。如果企业工商登记信息中包含企业负责人的姓名、联系方式等个人识别信息，因其属于已公开个人信息并且信息权人并未明确拒绝，所以原则上并未侵害信息权人的个人信息自决权。同时，由于所收集的是个人识别信息，其对公民信息安全法益的侵害并不显见。因此，检察机关基于《民法典》的规定，建议公安机关撤销案件，是恰当的。

案例2中，行为人将收集、互换得到的4万余条自然人姓名、电话号码、电子邮箱等个人识别信息出卖给他人。如果行为人收集、互换的信息内容为非公开个人信息，那么则可能构成侵犯公民个人信息罪。如果行为人收集、互换得到的是他人已公开的个人信息，那么其行为并未侵害信息权人的个人信息自决权，也就不构成侵犯公民个人信息罪。造成较严重后果的，信息权人仍可要求侵权人承担民事

责任，检察机关也可以通过提起民事公益诉讼的方式，要求行为人承担民事责任。

案例3中，行为人购买被害人的个人身份信息以及银行账号信息，开设店铺后再将信息打包出售，而上述信息则被用于售假和诈骗。被害人出卖自己的个人信息属于被害人同意，不再侵害被害人个人信息自决权法益。银行卡账号信息作为公民的敏感个人信息，与公民财产安全密切相关，将该类信息打包出卖后用于诈骗和售假，则侵害公民信息安全法益，依然可以构成本罪。

案例4中，行为人基于被害人同意收集被害人的信息，并不会侵犯公民个人信息自决权。如果所收集信息中并不包含个人敏感信息和复杂隐私信息，则不会侵害公民信息安全法益；如果行为人所收集的信息中包含个人敏感信息和复杂隐私信息，则仍可以侵害公民信息安全法益，进而构成本罪。本案例中，并没有证据表明行为人所收集的信息包含个人敏感信息和复杂隐私信息，因此并不侵害公民信息安全法益。行为人的行为实际上是一种信息居间行为，行为人虽有获利，但并不侵害本罪法益，入罪主张是值得商榷的。

六、结语

侵犯公民个人信息罪保护法益的确定关系到本罪的正确合理适用。诚然，法律保护个人信息的目的在于防范相关风险，促进个人信息在具体场景中的合理流通。[⑫]确定本罪的法益，一方面要有利于实现本罪的立法目的，预防公民个人信息侵害风险以及由此导致的公民人身安全和财产安全侵害；另一方面，应当合理把握公民个人信息刑法保护的“度”，对于合理的、不具有法益侵害风险的信息合理利用甚至收益行为应当排除在刑罚处罚的范围之外。场景化法益观为公民个人信息的刑法保护提供了较好的路径，既以保护公民个人信息自决权的方式保护公民对于个人信息的基本权利，又以保护公民信息安全的方式，将提供、出售个人信息导致公民人身安全、财产安全受侵害(风险)的情形纳入刑法的规制范围。与此同时，对于合理利用公开个人信息以及信息权人同意的信息之情形，则被排除在刑法的规制范围之外。总体而言，场景化法益观既有利于防范相关风险，又有利于促进个人信息在具体场景中的流通，是侵犯公民个人信息罪合理的、适当的法益观点。

注释：

①参见王昭武、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，第147-148页；胡胜：《侵犯公民个人信息罪的犯罪对象》，载《人民司法》2015年第7期，第39页；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》2000年第5期，第40-41页。

②参见冀洋：《法益自决权与侵犯公民个人信息罪的适用边界》，载《中国法学》2019年第4期，第83页。

③参见刘艳红：《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》，载《浙江工商大学学报》2019年第6期，第28页；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》，载《政治与法律》2018年第4期，第21页；马永强：《侵犯公民个人信息罪的法益权属确证》，载《比较法研究》2021年第5期，第114页；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》，载《法学评论》2018年第2期，第123页。

④参见皮勇、王肃之：《大数据环境下侵犯个人信息犯罪的法益和危害行为问题》，载《海南大学学报(人文社会科学版)》2017年第5期，第120-121页。

⑤参见曲新久：《论侵犯公民个人信息犯罪的超个人法益属性》，载《人民检察》2015年第11期，第5-6页。

⑥参见同上注，第6-7页；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，第116页。

⑦参见余筱兰：《论法学上的个人信息与个人数据》，载《上海法学研究》2021年第19卷，第131页。

⑧参见付强：《非法获取公民个人信息罪的认定》，载《国家检察官学院学报》2014年第2期，第117页。

⑨参见高秦伟：《个人信息概念之反思与重塑》，载《人大法律评论》2019年卷第1辑，第212页。

⑩See National Institute of Standards and Technology, SP 800-122, Guide to Protecting the Confidentiality of Personally

Identifiable Information(P II).

⑪See Paul M. Schwartz & Daniel J. Solove, The P II Problem: Privacy and a New Concept of Personally Identifiable Information, 86 New York University Law Review 1814, 1814(2022).

⑫参见范为:《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,第101页。

⑬See The European Parliament and of the Council, General Data Protection Regulation, Article 4.

⑭See United States Department of Justice, Overview of the Privacy Act of 1974, 2020 Ed., p. 28.

⑮参见《個人情報の保護に関する法律》第2条。

⑯参见刘宪权:《擅自处理公开的个人信息行为的刑法认定》,载《中国应用法学》2022年第5期,第25页。

⑰参见周加海、邹涛、喻海松:《〈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〉的理解与适用》,载《人民司法》2017年第19期,第32页。

⑱参见同前注⑤,曲新久文,第8页。

⑲参见王利明:《论个人信息权在人格权法中的地位》,载《苏州大学学报》2012年第6期,第72页。

⑳参见田宏杰:《由APP引发的多重犯罪研究》,载《人民检察》2018年第7期,第29页。

㉑参见王利明:《论个人信息权的法律保护——以个人信息权和隐私权的界分为中心》,载《现代法学》2013年第4期,第61-63页。

㉒参见蔡军:《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,第107页。

㉓对于这一论断,亦有立法规定予以支持,例如全国人大常委会《关于加强网络信息保护的决定》中规定:"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。"

㉔参见《民法典》第1034条。

㉕参见《个人信息保护法》第28条。

㉖参见同前注㉑,王利明文,第66页。

㉗同上注,第66页。

㉘同前注①,王昭武、肖凯文,第148页。

㉙《民法典》第1034条第3款。

㉚同前注⑫,范为文,第97页。

㉛具体而言,公民行踪轨迹信息处于公民个人信息的最核心层级,通信内容、征信、财产信息处于次核心层级,住宿、通信记录、健康生理、交易等其他可能影响人身、财产安全的公民个人信息处于更外围的层级。参见陈俊秀:《大数据时代个人信息"合理使用"制度研究》,载《大连理工大学学报(社会科学版)》2019年第2期,第89页。

㉜参见同前注⑫,范为文,第97页。

㉝从司法解释的规定来看,敏感程度表现为个人信息被用于犯罪的便利程度:《解释》将"非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上"与"非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他公民个人信息五百条以上"规定为侵犯公民个人信息罪"情节严重"的情形。其作出区分规定的原因在于,公民的行踪轨迹、通信内容、征信、财产信息等可以直接被应用于针对公民人身或财产的犯罪,而住宿、通讯记录、生理健康、交易等信息则通常需要与其他信息相结合才能实施针对公民人身或财产的犯罪。由此可见,个人信息敏感程度方面,立法者更关注的是公民个人信息是否具有被应用于针对公民人身或财产犯罪的便利性。

㉞参见丁晓东:《个人信息私法保护的困境与出路》,载《法学研究》2018年第6期,第203页。

㉟参见同前注㉑,王利明文,第61-63页。

㊱参见《个人信息保护法》第28条。

㊲参见《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5条。

㊳《个人信息保护法》第1条的规定揭示了本法制定的目的在于"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";《解释》则指出,基于"依法惩治侵犯公民个人信息犯罪活动,保护公民个人信息安全和合法权益"而作出本解释。此即明证。

㊴See Adam Carlyle Breckenridge, The Right to Privacy, University of Nebraska Press, 1970, p. 1.

㊵Ulrich Meyerholt, Vom Recht auf informationelle Selbstbestimmung zum Zensus 2011, Datenschutz und Datensicherheit 35 (2011), S. 683.

㊶Vgl. Spiros Simitis, Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., 2003, S. 129.

㊷§ 23-§ 31 Bundesdatenschutzgesetz.

㊸参见《个人信息保护法》第13-46条。

㊹参见同前注⑲,王利明文,第73页。

㊺参见高铭暄、马克昌主编:《刑法学》(第10版),北京大

学出版社、高等教育出版社2022年版，第53-54页。

㊻参见同前注③，敬力嘉文，第119页。

㊼参见叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018年第5期，第154页。

㊽《个人信息保护法》第13条。

㊾参见同前注③，敬力嘉文，第120页。

㊿参见张明楷：《法益初论》，中国政法大学出版社2000年版，第166页。

(51)参见同前注③，马永强文，第104-105页。

(52)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》，载《比较法研究》2021年第3期，第62页。

(53)参见孙国祥：《集体法益的刑法保护及其边界》，载《法学研究》2018年第6期，第47-48页。

(54)参见同前注⑤，曲新久文，第7页。

(55)参见同前注③，敬力嘉文，第122页。

(56) Vgl. Berner/Köhler/Käß, Plizeiaufgabengesetz, 20 Aufl., 2010, Rn. 4 ff.

(57)参见同前注④，皮勇、王肃之文，第120-121页。

(58)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确证》，载《中国刑事法杂志》2019年第5期，第27-29页。

(59)参见同前注②，冀洋文，第70页。

(60)参见同前注⑰，周加海、邹涛、喻海松文，第31页。

(61)参见同前注⑤，曲新久文，第8页。

(62)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，第11页。

(63)参见姜涛：《论集体法益刑法保护的界限》，载《环球法律评论》2022年第5期，第117页。

(64)参见卢志坚、白翼轩、田竞：《出卖公开的企业信息谋利：检察机关认定行为人不构成犯罪》，载《检察日报》2021年1月20日，第1版。

(65)参见朱韬：《一语道破：人格权保护网如何理性编织?》，载《民主与法制周刊》2021年第4期，第25-29页。

(66)本案例为笔者根据实际案例改编。

(67)最高人民检察院：《关于印发检察机关依法惩治侵犯公民个人信息犯罪典型案例的通知》，https://www.spp.gov.cn/xwfbh/wsfbt/202212/t20221207_594915.shtml#2，2022年12月8日访问。

(68)肯定观点参见同前注⑥，张勇文，第124-125页；否定观点参见同前注③，马永强文，第114页。

(69)《民法典》第1036条规定：处理个人信息，有下列情形之一的，行为人不承担民事责任：(一)在该自然人或者其监护人同意的范围内合理实施的行为；(二)合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；(三)为维护公共利益或者该自然人合法权益，合理实施的其他行为。《个人信息保护法》第27条规定：个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

(70)参见喻海松：《〈民法典〉视域下侵犯公民个人信息罪的司法适用》，载《北京航空航天大学学报(社会科学版)》2020年第6期，第7页。

(71)参见王华伟：《已公开个人信息的刑法保护》，载《法学研究》2022年第2期，第194页。

(72)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，第38-40页。

(73)参见同前注(71)，王华伟文，第195-196页。

(74)参见喻海松：《侵犯公民个人信息罪的司法疑难之案解》，载《人民司法》2018年第32期，第13-15页。

(75)参见《个人信息保护法》第27条。

(76)其中，自愿与合法公开是择一关系，满足其中之一即可；非自愿与非法公开是并列关系，必须同时满足。对于虽然非法公开，但是公民知晓之后自愿公开的信息，可以认为是自愿公开的信息。

(77)参见同前注⑲，王利明文，第73页。

(78)参见同前注④，皮勇、王肃之文，第121页。

(79)参见同前注③，马永强文，第114页。

(80)参见同前注⑥，张勇文，第125页。

(81)同前注③，马永强文，第114页。

(82)参见同前注㉞，丁晓东文，第194页。