

【个罪研究】

敏感个人信息的刑法特殊保护研究

刘宪权

【摘要】敏感个人信息具有极易诱发歧视性、极高人身依附性、极强财产关联性和有关儿童的特殊性。侵犯公民敏感个人信息行为对公民的人格尊严、人身安全和财产安全容易造成重大侵害。我国刑法相关规定应突出加大对敏感个人信息特殊保护的力度。在关于敏感个人信息的规定方面,刑法司法解释与《个人信息保护法》存在不一致。刑法司法解释对敏感个人信息进行分级,没有明确提及生物识别信息和不满14周岁未成年人的个人信息,对敏感个人信息规定的方式不符合逻辑的展开。《个人信息保护法》没有对敏感个人信息进行分级,明确将生物识别信息和不满14周岁未成年人的个人信息规定为敏感个人信息,对敏感个人信息采用“概括+列举”的规定方式科学、合理。刑法不应将侵犯公民敏感个人信息行为增设为新罪,应通过调整现有侵犯公民个人信息罪的规定,增加敏感个人信息特殊保护的内容。刑法司法解释应取消现有的关于敏感个人信息的分级,将非法获取、出售或者提供公民敏感个人信息行为的起刑点设定为“50条以上”,并保持侵犯公民敏感个人信息“情节特别严重”较“情节严重”10倍以上的认定标准。

【关键词】敏感个人信息;刑法规定;刑法司法解释;完善路径;分级取消

【作者简介】刘宪权,华东政法大学教授。

【原文出处】《法学评论》(武汉),2022.3.1~10

【基金项目】本文系国家社会科学基金重大项目“网络时代的社会治理与刑法体系的理论创新”(项目编号:20&ZD199)的阶段成果。

2021年8月20日,《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》)在第十三届全国人大常委会第三十次会议被正式表决通过。《个人信息保护法》在第二章第二节中专门规定了“敏感个人信息的处理规则”,以突出对敏感个人信息进行保护。该法第28条第1款规定,敏感个人信息是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14周岁未成年人的个人信息。虽然“敏感个人信息”作为一个法律用语是由我国《个人信息保护法》首次提出的,但是“敏感个人信息”这一相关提法早在2012年就已经在有关部门的规范性技术文件中出现。2012年11月由国家

质量监督检验检疫总局(已撤销)、国家标准化管理委员会联合发布的《信息安全技术公共及商用服务信息系统个人信息保护指南》(以下简称《指南》)中将个人信息分为个人敏感信息和个人一般信息。《指南》同时对个人敏感信息下了定义并列出了相关示例。^①其后,2017年颁布的《信息安全技术个人信息安全规范》(以下简称《规范》)对个人敏感信息的内涵和外延均作了较为确切的界定。^②在2017年版《规范》的基础之上,修订后的2020年版《规范》依旧保留了对敏感个人信息的定义,对个人敏感信息的内涵和外延作了进一步的丰富。^③然而,《指南》《规范》等文件仅是具有指导意义的规范性技术文件,并非具有强制性的法律文件,因而这些规范性技术文件的位阶远低于法律文件。但是,这些规范性技术文件

在对敏感个人信息定义方面所作出的“先行先试”的探路,无疑为立法者制定《个人信息保护法》中有关敏感个人信息的条款提供了重要的参考。在《个人信息保护法》已经对敏感个人信息的处理规则作出明确规定的情形之下,刑法是否有必要对敏感个人信息进行专门的特殊保护?如有必要,我们应如何对刑法进行完善,并确保其不与《个人信息保护法》等前置法产生冲突?本文主要针对上述问题展开讨论,以弥补刑法在理论上对于敏感个人信息的研究缺漏,并统一司法实践对于敏感个人信息的保护思路。

一、敏感个人信息需要刑法的特殊保护

在《个人信息保护法》已经明确规定处理敏感个人信息的规则这一前提之下,笔者认为刑法有必要对敏感个人信息予以特殊的保护,理由如下:

第一,敏感个人信息具有的特性决定了侵犯公民敏感个人信息行为更容易对公民的人格尊严、人身安全和财产安全造成侵害,且侵犯公民敏感个人信息行为的社会危害性要大于侵犯公民一般个人信息行为,因此,刑法有必要加强对敏感个人信息的特殊保护。

分析《个人信息保护法》对敏感个人信息的定义可知,敏感个人信息实际由三部分组成:(1)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的个人信息;(2)一旦泄露或者非法使用,容易导致自然人的人身、财产安全受到危害的个人信息;(3)不满14周岁未成年人的个人信息。笔者认为,这三部分的敏感个人信息分别具有以下特性:

上述第一部分的敏感个人信息具有极易诱发歧视性。例如,敏感个人信息中的宗教信仰信息虽然不必然与公民的人身安全和财产安全发生联系,但是与公民的人格尊严息息相关。公民是否信仰宗教,信仰何种宗教完全是公民的自由,与公民人格尊严具有极大的关联性。侵犯公民宗教信仰信息的行为,极易诱发对宗教信仰的歧视和偏见,从而对公民的人格尊严带来极大的伤害。现实中的确存在侵害公民宗教信仰自由,损害公民人格尊严的行为。对此,刑法分则第四章侵犯公民人身权利、民主权利罪中就规定了非法剥夺公民宗教信仰自由罪,以此

规制国家机关工作人员非法剥夺公民的宗教信仰自由,情节严重的行为。

上述第二部分的敏感个人信息具有极高人身依附性和极强财产关联性。近年来,敏感个人信息中的生物识别信息受到了社会公众的广泛关注。2019年ZAO换脸事件引发的热议,就曾将生物识别信息中人脸信息的法律保护问题推向了舆论的风口浪尖。由于部分生物识别信息(尤其是人脸信息)能够通过摄像头被“无感”收集,因此,这些信息极易被窃取。同时,随着大数据时代下深度伪造技术不断成熟与发展,又导致人脸信息等生物识别信息极易被滥用。除了非法获取、出售或者提供公民生物识别信息的行为可能构成侵犯公民个人信息罪之外,非法使用公民生物识别信息的行为还可能构成侮辱罪或诽谤罪。例如,将公众人物的人脸信息用于替换淫秽视频中的人脸信息,并在互联网上公开传播的行为,可能对公民的人格、名誉造成极大的危害。另外,敏感个人信息中的金融账户信息涵盖的内容众多,包括公民的银行账户、存款情况、信贷记录、交易记录等与公民财产有着紧密关联的个人信息,一旦这些信息被他人窃取或通过其他手段非法获取,极可能引发诈骗或者敲诈勒索等犯罪,从而导致公民的财产遭受重大损失。以前述的生物识别信息为例,生物识别信息相较传统的数字信息本身具有更高的便捷性和安全性,因而该信息中的人脸信息、指纹信息等往往会作为一种特殊的“密码”广泛地在移动支付领域使用。这就导致生物识别信息与公民的财产之间实际存在着较为密切的联系。实践中就曾出现过行为人冒用他人的人脸盗取他人支付宝账户内钱财的情况,^④当然,这种窃取他人生物识别信息从而获取他人第三方支付软件内钱财的行为可能构成信用卡诈骗罪。

上述第三部分敏感个人信息具有儿童特殊性。不满14周岁的未成年人尚不具备完全的民事行为能力,在对个人信息的处理过程中不具备充分的认识能力和控制能力,且没有足够的自我保护或保障自己个人信息安全的能力。由此,该类群体的个人信息更容易成为犯罪分子实施犯罪的对象。又由于该

类群体身心发育尚未健全,其个人信息一旦被泄露极可能严重影响身心健康,并对其今后的成长之路埋下巨大隐患。^⑤基于此,《个人信息保护法》规定,无论不满14周岁未成年人个人信息是否与人格尊严、人身或财产安全有关,只要该信息的主体为不满14周岁的未成年人,一律都属于敏感个人信息。

需要注意的是,笔者在归纳敏感个人信息所具有的特性时特地使用了“极易、极高、极强”作为修饰程度的形容词,目的在于进一步体现敏感个人信息的特殊性。应该看到,一部分的一般个人信息虽然也具有人身依附性或者财产关联性等特性,但是并不具有极高人身依附性、极强财产关联性,因而侵犯公民一般个人信息行为对公民人身、财产安全造成的侵害有限。通常情况下,侵犯公民一般个人信息行为只可能构成侵犯公民个人信息罪,而不可能构成其他的犯罪。但是,敏感个人信息尤其与公民的人格尊严、人身和财产安全有着紧密的联系。这种尤其紧密的联系导致了侵犯公民敏感个人信息行为更容易对公民人身、财产安全造成危害。前文已经论述了侵犯公民敏感个人信息行为除了构成侵犯公民个人信息罪之外,还极易构成侮辱罪、诽谤罪、诈骗罪、敲诈勒索罪等其他具有严重社会危害性的犯罪。这也进一步证实了侵犯公民敏感个人信息行为的社会危害性要远大于侵犯公民一般个人信息行为。就此而言,笔者认为,为了更好地保障公民敏感个人信息的安全,刑法有必要加强对敏感个人信息的特殊保护。

第二,刑法侵犯公民个人信息罪所对应的重要前置法是《个人信息保护法》,该法对个人信息进行了分级,并突出对敏感个人信息的重点保护。为了维持法秩序的整体统一,使刑法与《个人信息保护法》之间的衔接更加顺畅,我们在修订侵犯公民个人信息罪时有必要参考和吸收《个人信息保护法》的相关规定。

分析我国刑法规定,我们不难发现,刑法主要通过设立侵犯公民个人信息罪对侵犯个人信息行为加以规制。侵犯公民个人信息罪中一个重要的构成要件是“违反国家有关规定”,据此,侵犯公民个人信息

犯罪行为的认定需要结合相关前置法的有关规范予以综合考量。在法秩序统一的视角下,侵犯公民个人信息行为刑事违法性的判断应从属于民事违法性和行政违法性的判断。如果相关行为不具有民事违法性或行政违法性,则该行为就肯定不具有刑事违法性。由于《个人信息保护法》细化了《民法典》《网络安全法》等法律和行政法规对个人信息保护的内容,并且较为系统地提出了个人信息处理的基本规则,因而在认定侵犯公民个人信息违法行为和犯罪行为时,《个人信息保护法》规定的内容无疑是一个重要的参考标准。

《个人信息保护法》将个人信息分为敏感个人信息和一般个人信息,并在第二章“个人信息处理规则”中专门设置一节内容对敏感个人信息的处理规则作出特别规定。^⑥由此,我们可以看到,《个人信息保护法》对个人信息处理者处理敏感个人信息的流程作出了严格规范,并且强调了敏感个人信息需要被特殊保护。需要注意的是,刑法虽然已经有相关条文(即侵犯公民个人信息罪)对个人信息予以保护,但并没有突出对敏感个人信息的重点保护。而依笔者之见,对于敏感个人信息的保护,刑法理应作出专门规定。因为立法者设定侵犯公民个人信息罪的立法目的在于规制社会危害性严重的侵犯公民个人信息行为。正如前述,不同类型的个人信息与公民人身、财产权联系的紧密程度不完全相同,因此侵犯不同类型个人信息行为的社会危害性显然会有很大不同。为了实现罪责刑的一致,突出强调刑法对该类个人信息的重点保护,将与人格尊严、人身权、财产权紧密相关的一部分个人信息在刑法上予以单独归类,是很有必要的。就此而言,笔者认为,我们完全有必要在刑法中对“敏感个人信息”的保护作出明确规定,并且在对侵犯公民个人信息违法行为中个人信息分级处理机制上保持与前置法规的一致,进而构建较为系统的敏感个人信息特殊保护的法律体系。

二、刑法对敏感个人信息特殊保护切实可行

需要指出的是,我国刑法中没有直接出现“敏感个人信息”的用语,但部分条文中涉及个人信息的内

容与《个人信息保护法》所规定的敏感个人信息的范畴存在重叠。例如,刑法第177条之一第2款规定的窃取、收买、非法提供信用卡信息罪,涉及了敏感个人信息中的信用卡信息。又如,刑法第280条第3款规定的伪造、变造、买卖身份证件罪,第280条之一规定的使用虚假身份证件、盗用身份证件罪,第280条之二规定的冒名顶替罪,这些条文均涉及了敏感个人信息中的特定身份信息。其实,这些犯罪都属于侵犯公民敏感个人信息类的犯罪,但是这些犯罪因侵犯法益的侧重点不同而被分散规定在刑法分则第三章、第六章。例如,窃取、收买、非法提供信用卡信息罪侵害的法益主要是信用卡的管理秩序和信用卡持卡人的财产权益;伪造、变造、买卖身份证件罪、使用虚假身份证件、盗用身份证件罪和冒名顶替罪侵害的法益主要是社会管理秩序。^⑦尽管刑法分则第四章侵犯公民人身权利、民主权利罪这一章节中以侵犯公民个人信息罪规制侵犯公民个人信息,情节严重的行为,但是该罪的刑法条文表述中仍然没有直接出现“敏感个人信息”这一用语,当然我们也很难从条文的规定中分析出敏感个人信息刑法特殊保护的内容。由此不难看出,刑法在保护公民敏感个人信息时出发点主要是为了维护社会主义市场经济秩序,或者社会管理秩序,而不是基于保障公民个人信息安全。这多少反映出我国刑法对于公民敏感个人信息保护并没有持特别关注和突出保护的態度。

由此可知,我国刑法虽然有部分条文涉及了敏感个人信息的相关内容,但是保护的侧重点并不在于公民敏感个人信息的安全。也正是因为刑法没有突出对公民敏感个人信息的特殊保护,甚至不曾出现“敏感个人信息”这一用语,所以容易使人们产生一种错觉,刑法似乎将敏感个人信息与一般个人信息不加区别且等同对待,也即刑法对公民敏感个人信息的保护力度与对公民一般个人信息的保护力度是相等的。

2017年5月8日,最高人民法院、最高人民检察院联合颁行的《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》),对

于如何理解与适用刑法第253条之一规定的侵犯公民个人信息罪作出了较为具体的规定。应该看到,尽管“公民个人信息”的概念在《解释》中予以了明确的界定,却未曾对“敏感个人信息”下定义。但是,《解释》在对公民个人信息的分级中又列举了较多与《个人信息保护法》中敏感个人信息相关的具体内容。例如,《解释》第5条所提及的行踪轨迹信息、财产信息等,与《个人信息保护法》中列举的具体敏感个人信息的内容基本吻合。但笔者在比较《解释》和《个人信息保护法》中的有关规定后发现,两者规定之间仍存在较多的不一致内容:

第一,在个人信息的分级方面,《解释》与《个人信息保护法》规定完全不同。《解释》第5条第1款第3、4、5项规定对公民个人信息进行了分级。其中,第3、4项中所提及的个人信息都属于《个人信息保护法》中的敏感个人信息。^⑧就此而言,我们完全有理由认为,《解释》将敏感个人信息划分为“行踪轨迹信息、通信内容、征信信息、财产信息”一档和“住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息”一档。侵犯不同级别的敏感个人信息,认定“情节严重”的标准也不相同。《解释》认为,对于侵犯第3项规定的敏感个人信息,信息数量达到50条即可构成侵犯公民个人信息罪,而对于第4项规定的敏感个人信息,信息数量必须达到500条才能构成该罪。由此可知,《解释》对于不同级别的敏感个人信息,保护的力度不完全一致。与《解释》分级规定形成对比的是,《个人信息保护法》并没有对敏感个人信息作出分级规定。换言之,在《个人信息保护法》中不区分敏感个人信息的级别,且所有的敏感个人信息均被予以相同力度的保护。

第二,在对生物识别信息和不满14周岁未成年人的个人信息的保护方面,《解释》与《个人信息保护法》规定之间存在区别。《解释》第5条第1款第3、4项在列举个人信息时并没有明确提及生物识别信息和不满14周岁未成年人的个人信息,这就导致了在认定侵犯上述两种公民个人信息的行为是否构成“情节严重”时容易产生分歧意见。^⑨在笔者看来,对于

侵犯公民生物识别信息和侵犯不满14周岁未成年人的个人信息的行为,认定“情节严重”的标准都应该为“50条以上”。换言之,《解释》对生物识别信息和不满14周岁未成年人的个人信息的保护力度应该与对行踪轨迹信息、通信内容、征信信息、财产信息的保护力度持平。原因在于:生物识别信息和不满14周岁未成年人的个人信息的重要性与行踪轨迹信息、通信内容、征信信息、财产信息相当。生物识别信息和不满14周岁未成年人的个人信息不仅与公民的人格尊严、人身安全相关,还与公民的财产安全存在密切联系。如前所述,生物识别信息是反映自然人独有的生理特征和行为特征的生理信息。因而,生物识别信息与公民的人格尊严、人身有着紧密的关联。另外,由于生物识别信息被作为一种特殊的“密码”在移动支付领域广泛使用,这就使得生物识别信息与公民的财产出现了交集。由此可知,侵犯公民生物识别信息的行为不仅可能对公民人格尊严和人身安全造成侵害,也可能对公民财产安全造成损害。就不满14周岁未成年人的个人信息进行分析,我们也同样可以看到其信息内容的重要性。由于该类信息的主体没有足够的认识能力和控制能力,也缺乏自我保护的能力,所以涉该类主体的个人信息更容易被侵犯。加强对不满14周岁未成年人个人信息的特殊保护,显然也应该成为《解释》规定的应有内容。综上,笔者认为,生物识别信息和不满14周岁未成年人的个人信息应归入《解释》第5条第1款第3项规定中,但由于该项规定在列举行踪轨迹信息、通信内容、征信信息、财产信息后并没有使用“等”字,导致司法实践不能将这一标准扩大适用到同样重要而《解释》却未提及的其他类型个人信息中。这一情况多少反映了《解释》对生物识别信息和不满14周岁未成年人的个人信息未予以特别关注,也并没有强调特殊保护的立场。

相比之下,《个人信息保护法》在敏感个人信息的定义下提及了生物识别信息,且为了突出对该信息的特殊保护将其确立在该法所列举的众多敏感个人信息中的首位。需要特别指出的是,《个人信息保护法》在敏感个人信息的规定中还提及了不满14周

岁未成年人的个人信息,并将该信息单独作为一种类型加以特别列举。如此规定带来的优势即在于,无论不满14周岁未成年人的个人信息是否会因为泄露或者非法使用,从而导致不满14周岁未成年人的的人格尊严受到侵害或者人身、财产安全受到危害,只要是不满14周岁未成年人的个人信息,在《个人信息保护法》中一律被认定为是敏感个人信息。另外,《个人信息保护法》还在第31条明确规定敏感个人信息的处理者在处理不满14周岁未成年人的个人信息时应当履行的特定义务,从而在一定程度上解决了未成年人个人信息处理者的义务边界模糊的问题。^⑩可见,与《个人信息保护法》突出对生物识别信息特殊保护一样,该法对不满14周岁未成年人的个人信息的保护也是较为全面的且保护力度也是相对较强的。

第三,在有关敏感个人信息相关内容的规定方式上,《解释》与《个人信息保护法》规定之间存在差异。具体而言,《解释》第5条第1款第3项采用的是“列举”的方式,第4项采用的是“列举+概括”的方式。笔者认为,上述规定的方式存在一定的缺陷。《解释》该条该款第3项采用单纯列举的方式,实际上导致了该项规定不可能穷尽所有类型的“敏感个人信息”。虽然是出于条文简洁性的需要,该项规定中仅列举了四种类型的“敏感个人信息”,但是正如笔者前文所述,对于应纳入该项规定的生物识别信息和不满14周岁未成年人的个人信息,《解释》却未将这两种类型的“敏感个人信息”纳入该项规定中。这应该是单纯列举方式所导致该项规定存在一定不合理性的原因。《解释》该条该款第4项采用“列举+概括”的方式,看似能够涵盖更多的敏感个人信息,但实际存在一定的问题。因为按照常理,对于某一类事物的定义需要先概括出该类事物所具有的共同特征,之后为方便实际操作,进而对该类事物所包含的典型示例再进行列举。换言之,“概括+列举”才符合正常的逻辑展开。而《解释》该条该款第4项所采用的“列举+概括”的方式明显与正常的逻辑相悖,极易给人造成一种错觉,那就是《解释》原本仅打算列举一部分的敏感个人信息,但又担心所列举的敏感个

人信息不够全面,因而借助于将“概括”规定在后的方式,从而起到对前述敏感个人信息“补强”的作用。同样是对敏感个人信息作出定义,《个人信息保护法》采用的是“概括+列举”的方式,即先归纳出敏感个人信息的特征,再详细罗列部分典型的敏感个人信息。毋庸置疑,在有关敏感个人信息相关内容的规定方式上,《个人信息保护法》明显更加科学、合理,符合正常的逻辑展开。

综上所述,《解释》虽没有明确提及“敏感个人信息”这一用语,但是与敏感个人信息相关的内容确实存在于部分条文中。时下,尽管对敏感个人信息保护的雏形在《解释》中已有确立,但是,由于《解释》与《个人信息保护法》规定之间仍存在较大的区别,导致了《解释》对敏感个人信息的刑法特殊保护无法得到充分的贯彻与体现。就此而言,笔者认为,在《个人信息保护法》已经颁行的当下,我们当务之急是调整《解释》与《个人信息保护法》规定不一致的内容,将《个人信息保护法》对敏感个人信息特殊保护的内容较为完整地融入《解释》的条文中,从而突出并强化刑法对敏感个人信息的特殊保护。

三、刑法对敏感个人信息特殊保护的途径

笔者认为,加强对敏感个人信息的刑法特殊保护,可能存在两条不同的路径:其中一条路径是,在刑法中增设一个全新的罪名——“侵犯公民敏感个人信息罪”,以规制侵犯公民敏感个人信息,情节严重的行为。也即可以将侵犯公民敏感个人信息罪增设为刑法第253条之二,使第253条之一的侵犯公民个人信息罪仅规制侵犯公民一般个人信息行为。这样可以较为直接地反映出刑法对不同类型的个人信息保护力度的不同。另一条路径是,调整侵犯公民个人信息罪的现行刑法条文,也即将敏感个人信息的相关内容明文增加到刑法有关侵犯公民个人信息罪的原规定中。例如,我们可以增设一款刑法条文规定刑法侵犯公民个人信息罪中的“公民个人信息”包含公民一般个人信息和公民敏感个人信息,从而突出强调刑法对敏感个人信息的关注。而关于敏感个人信息特殊保护的具体标准,则由刑法司法解释予以细化。

对于上述有关增设新罪抑或调整侵犯公民个人信息罪的规定两条不同路径的选择,笔者倾向于选择后者,理由在于:《个人信息保护法》和刑法对个人信息保护的出发点不同。我们不能因为《个人信息保护法》对敏感个人信息的处理规则单独设置了一节内容,就当然地认为刑法也必须相应地增设一个新的罪名。相比增设一个新的罪名,调整现有罪名中的内容,同样能够反映立法者对敏感个人信息的重视。就此而言,择优选择调整现有侵犯公民个人信息罪不失为一条比较妥当的路径。

在笔者看来,《个人信息保护法》单独设置一节内容规定敏感个人信息的处理规则,是为了强调敏感个人信息的处理者相较一般个人信息的处理者需要履行更多的义务,从而提醒敏感个人信息的处理者在处理敏感个人信息时要尤其谨慎。如果《个人信息保护法》不单独对敏感个人信息的处理规则设立一节内容,而是将敏感个人信息的处理规则与一般个人信息的处理规则混同在一起,无法重点突出敏感个人信息处理规则的特殊性,《个人信息保护法》重点保护敏感个人信息的立法原意也就无法被凸显。

相比之下,刑法对个人信息保护的出发点并非在于要求个人信息的处理者履行更多的义务,而是为了打击犯罪,规制严重侵害公民个人信息安全的犯罪行为。尽管敏感个人信息在信息敏感程度上远远高于一般个人信息,但从行为角度来看,无论是侵犯公民一般个人信息行为,还是侵犯公民敏感个人信息行为,这两种行为在表现方式上是一致的。由于侵犯公民敏感个人信息行为和侵犯公民一般个人信息行为侵害的法益基本相同,因而,我们没有必要将敏感个人信息从个人信息的概念之中分离出来,并专门为侵犯公民敏感个人信息行为单独设立一个新罪名。有学者也指出,刑法是法益保护法,有无值得刑法保护的法益,是刑事立法上增设新罪的前提。^⑩笔者认为,《个人信息保护法》强调敏感个人信息的处理者应履行更多义务,从而单独设置一节内容规定敏感个人信息的处理规则的这一缘由,不足以成为支撑刑法专门增设新罪的理由。凸显对敏感

个人信息的刑法保护并不仅有增设新罪名这一条途径,我们完全可以从现有罪名入手,调整侵犯公民个人信息罪中的部分规定,将与敏感个人信息有关的内容充实进侵犯公民个人信息的法条规定中,以体现立法者重视与关注敏感个人信息的刑法特殊保护。

具体而言,侵犯公民个人信息罪中使用的是“公民个人信息”这一较为笼统的表述,如果刑法规定要在这一罪名中突出敏感个人信息,只能通过明确该罪中的“公民个人信息”包含“公民一般个人信息”和“公民敏感个人信息”的立法方式才能做到。因而,笔者建议在该罪中增设第5款规定,即“公民个人信息包含公民一般个人信息和公民敏感个人信息。”这样看似只是简单地增设一款规定,但实际上能够起码带来三点好处:一是可以维持现有侵犯公民个人信息罪第1至4款条文的稳定性;二是可以证明立法者已经关注到敏感个人信息刑法特殊保护的问题;三是可以与刑法司法解释中与敏感个人信息相关的规定形成有效的衔接,能够为刑法司法解释的修订提供依据与支撑。

在《解释》已经出现有关敏感个人信息规定之雏形的前提之下,该如何进一步凸显《解释》对敏感个人信息的特殊保护。为此,笔者有以下几点建议:

1. 建议取消敏感个人信息的分级

笔者之所以建议取消敏感个人信息的分级,主要出于两方面的考虑:

首先,对于同一行为中涉及不同类型的敏感个人信息的保护力度不应该存在差异。应该看到,对于他人利用公民个人信息实施犯罪的行为,《解释》实际上存在保护力度上的差异。例如,《解释》第5条第1款第1项与该条该款第2项都是关于他人利用公民个人信息实施犯罪行为的规定。区别在于第1项中的对象仅限定在行踪轨迹信息,并且不需要行为人知道或应当知道他人利用行踪轨迹信息实施犯罪,而第2项中的对象包含了除行踪轨迹信息之外的所有个人信息,并且要求行为人必须知道或应当知道他人利用个人信息实施犯罪。^⑩依笔者之见,第2项规定实际上比第1项规定提高了证明要求,即对于

出售或者提供行踪轨迹信息之外的其他类型的敏感个人信息行为构成犯罪的要求更高,必须证明行为人对于他人利用这些个人信息实施犯罪的情况是明知的。但事实上,这种证明要求的提高反而不利于对除行踪轨迹信息之外的其他敏感个人信息的保护。因为除行踪轨迹信息之外其他类型的敏感个人信息也同样可以被他人用于犯罪,行为人出售或者提供这些敏感个人信息给他人时,可能完全不知他人会用于犯罪。其实所有类型的敏感个人信息都存在被犯罪分子用于犯罪的可能性,就行踪轨迹信息与其他类型敏感个人信息被他人用于犯罪而言,并无很大的差别。《解释》对行踪轨迹信息与其他类型敏感个人信息予以有差别的保护,似乎缺乏充足依据支撑。对于非法获取、出售或者提供个人信息的行为,《解释》同样存在保护力度上的差异。同样以《解释》第5条第1款第3项和该款第4项为例,在认定信息的数量标准上后者是前者的10倍。由于第3项、第4项规定的这些都属于《个人信息保护法》规定的敏感个人信息的范畴,而《解释》却作了分级保护规定,即对第3项规定的敏感个人信息的保护力度明显大于第4项规定的敏感个人信息。《解释》作此规定可能是基于这样考虑:第3项规定的个人信息对公民的人身和财产安全最为重要,在数量上只要达到50条即可构成侵犯公民个人信息罪;而第4项规定的个人信息在重要程度上则略低于第3项中所规定的四种个人信息。但是,由于第4项规定的这些个人信息又与公民人身、财产安全直接相关,所以在数量上可以相对放宽,达到500条才能构成侵犯公民个人信息罪。^⑪然而,笔者认为,《解释》以信息重要性的不同作为划分第5条第1款第3项与第4项的理由,似乎欠缺说服力。因为敏感个人信息的重要性实际上会随着场景的不同而发生变化。在某些场景下,第3项规定的个人信息的重要性可能会略高于第4项规定的个人信息,但在另一些场景下,则完全可能出现相反的情况。例如,就杀人犯罪而言,第3项规定的行踪轨迹信息的重要性高于第4项规定的交易信息。因为行为人在非法获取他人的行踪轨迹信息后,更容易精准定位到他人的具体位置,较方便实

施后续的杀人行为。就窃取他人信用卡信息资料犯罪而言,行踪轨迹信息的重要性却不及交易信息。因为即便行为人非法获取了他人的行踪轨迹信息,由于该信息与他人的信用卡信息资料之间并无直接的关联,因而非法获取他人的行踪轨迹信息对行为人达到窃取他人信用卡信息资料的最终目的没有很大的帮助。而如果行为人非法获取了他人的交易信息,则更容易达到窃取他人信用卡信息资料的最终目的。因为在大数据时代,大部分交易都是通过第三方支付平台得以实现,而依托于第三方支付平台的交易必须以信用卡信息资料为媒介,行为人非法获取他人的交易信息后就很容易“顺藤摸瓜”获取他人的信用卡信息资料。可见,在不同的犯罪中,敏感个人信息的重要性并不是完全确定的。所以,我们很难对不同的敏感个人信息进行比较并做出重要性高低的绝对判断。就此而言,我们再以所谓重要性高低为标准对敏感个人信息进行分级似乎就很不合理。况且,第3项规定的信息与第4项规定的信息之间存在交叉、重合的问题。例如,疫情防控下人们使用的“健康码”既能作为健康生理信息反映特定自然人的身体健康状况,同时又能作为行踪轨迹信息反映特定自然人的行程情况。由此就产生了应将“健康码”归类于第3项还是第4项的困惑。另外,有学者还指出,第3项规定的财产信息与第4项规定的交易信息难以辨明,存在重合的问题。^⑩综上,笔者建议,应修改或取消《解释》对敏感个人信息进行分级的规定。

其次,《解释》对敏感个人信息认定和处理应与《个人信息保护法》保持一致。以行踪轨迹信息为例,与《解释》对行踪轨迹信息与其他类型敏感个人信息进行分级规定形成对比的是,《个人信息保护法》没有将行踪轨迹信息与生物识别、宗教信仰、特定身份、医疗健康、金融账户等敏感个人信息作区别对待,而是将这些信息并列规定在同一款。与此同时,《个人信息保护法》在“敏感个人信息的处理规则”这一节内容中也没有提出行踪轨迹信息的处理者相较其他敏感个人信息的处理者要履行更多的义务。纵观《个人信息保护法》中有关敏感个人信息的

规定,我们不难看出,《个人信息保护法》没有对敏感个人信息进行分级,因而该法也就没有对行踪轨迹信息与其他类型敏感个人信息予以有差别的保护。对此,有学者指出,《个人信息保护法》未对敏感个人信息进行分级,略显粗糙。^⑪但是,在笔者看来,《个人信息保护法》对敏感个人信息不作分级而是采用“一刀切”的认定方式,实质上能够使司法实践对敏感个人信息的保护力度更加均衡。如果立法者在制定《个人信息保护法》时有意强调敏感个人信息的有差别保护,那么就应该直接在法条中明确提出划分不同级别敏感个人信息的标准。既然《个人信息保护法》没有作出这样的规定,我们就应当认为立法者是排斥对敏感个人信息进行分级的。更何况,如前所述,敏感个人信息的重要性会随着场景的不同而发生变化;特别是某一类型的敏感个人信息还可能涉及多重属性。这些情况的存在就必然导致我们很难甚至不能对相关类型的敏感个人信息进行精准的分级。所以,为了与《个人信息保护法》形成有效的衔接,《解释》应该与《个人信息保护法》中的相关规定保持一致,而无须专门对敏感个人信息进行分级。

综上,在《个人信息保护法》颁行的当下,审视《解释》中关于敏感个人信息分级的规定,我们确实发现《解释》中的规定存在一定的问题,建议应该适时对其予以修订。笔者建议在对《解释》进行修订时取消敏感个人信息的分级,作此修订不仅能够解决前述《解释》对生物识别信息和不满14周岁未成年人的个人信息未予以特别关注的问题,而且还有利于真正落实对敏感个人信息的刑法特殊保护。笔者建议对《解释》可以具体作如下修订:一是需要修订《解释》第1条规定,建议在第1条之下设置两款内容。其中第1款对公民个人信息下定义,而第2款则对公民敏感个人信息下定义。二是需要修订《解释》第5条第1款第1项、第2项规定,建议将第1项规定的“行踪轨迹信息”扩展为“公民敏感个人信息”。如此,《解释》原该条该款第2项中的“公民个人信息”就要相对应限缩为“公民一般个人信息”。也即建议将《解释》第5条第1款第1项修订为“出售或者提供公

民敏感个人信息,被他人用于犯罪的”,将第2项修订为“知道或者应当知道他人利用公民一般个人信息实施犯罪,向其出售或者提供的”。三是需要修订《解释》第5条第1款第3项、第4项规定,建议以“敏感个人信息”这一提法替代原有关于敏感个人信息的列举示例,并设置统一的起刑点,从而实现对敏感个人信息标准一致的刑法特殊保护。

2. 建议将非法获取、出售或者提供公民敏感个人信息犯罪行为的起刑点设定为“50条以上”

应该看到,《解释》不仅对敏感个人信息进行分级规定,而且还对侵犯敏感个人信息犯罪行为的起刑点作了区别规定。《解释》第5条第1款第3项中规定的起刑点为“50条以上”。但是,该条该款第4项中规定的起刑点为“500条以上”。如果依照《个人信息保护法》规定以“敏感个人信息”这一统称替代第3项、第4项所列举的信息,那么势必会面临如何设定或调整非法获取、出售或者提供公民敏感个人信息犯罪行为起刑点的问题。

依笔者之见,在设定非法获取、出售或者提供公民敏感个人信息犯罪行为起刑点时需要注意以下两点:一是不能将起刑点设置得太低,否则侵犯公民敏感个人信息的违法行为动辄上升为犯罪行为,极有可能压缩前置法的适用空间,使侵犯公民个人信息罪沦为一个新的“口袋罪”。二是不能将起刑点设置得太高,否则对敏感个人信息进行刑法特殊保护的力度势必会被减弱。同时,还需要考虑到敏感个人信息与一般个人信息之间的差异性。拉开与非法获取、出售或者提供公民一般个人信息犯罪行为起刑点之间的距离,才能突出对敏感个人信息的刑法特殊保护。可见,设定起刑点是一个权衡利弊的过程。如何准确把握侵犯公民敏感个人信息行为入罪的“度”,是我们在修订《解释》时不得不面对的一个难题。

据此,笔者建议将非法获取、出售或者提供公民敏感个人信息犯罪行为起刑点设定为“50条以上”。提出该建议的理由在于,现有《解释》第5条第1款第3项规定的起刑点即为“50条以上”,而这一起刑点是《解释》对于非法获取、出售或者提供公民个人信息

犯罪行为所设定的最低起刑点。最低起刑点意味着最强刑法保护,因而继续沿用第3项规定的“50条以上”的认定标准,实际上是一个比较合理的选择。值得一提的是,《解释》第5条第1款第5项规定,非法获取、出售或者提供公民一般个人信息犯罪行为的起刑点为“5000条以上”,如果我们将非法获取、出售或者提供公民敏感个人信息犯罪行为的起刑点设定在“50条以上”,在认定信息的数量标准上前者是后者的100倍,显然就能充分突出对公民敏感个人信息的刑法特殊保护。就此而言,笔者建议将《解释》第5条第1款第3项修订为“非法获取、出售或者提供公民敏感个人信息50条以上的”,同时将原《解释》该条该款第4项规定内容归入修订后第3项规定的敏感个人信息中,从而既在“敏感个人信息”这一法律用语的使用上,又在起刑点的设置上保持了统一,以最大程度有利于对敏感个人信息进行刑法特殊保护。

这里需要注意的是,上述取消《解释》第5条第1款第4项规定并不意味着不需要对原该项规定的敏感个人信息特殊保护,而是因为修订后的《解释》第5条第1款第3项规定所涵盖的对象包括了原有第4项规定的敏感个人信息。为了体现《解释》对敏感个人信息刑法特殊保护的相对一致性,笔者建议取消第4项规定。同时将涉及第4项规定的信息构成侵犯公民个人信息犯罪的起刑点,由原本为“500条以上”统一修订为“50条以上”。通过这一修订,实际上降低了原有第4项规定的侵犯公民个人信息犯罪行为的起刑点,或者说提高了对该项规定的个人信息的保护力度。对此,可能会有人会质疑,提高对原有第4项规定的个人信息的保护力度,将其与原有第3项规定的个人信息的保护力度持平,是否合理?是否会产生量刑上的不平衡?笔者认为,这种质疑似乎有些多虑。因为原有第4项规定的个人信息和第3项规定的个人信息本身就具有一定的相似性,并且依据《个人信息保护法》,两者均属于敏感个人信息这一范畴。既然如此,《解释》将这两项规定中的个人信息统一规定在第3项敏感个人信息中并设定同样的起刑点,也就不存在任何问题了。“50条以上”的起刑点与“500条以上”的起刑点相比,我们当然选择“就低

不就高”即采纳“50条以上”的起刑点,否则如果将起刑点设定为“500条以上”相当于降低了对原有第3项规定的个人信息保护力度,有违对敏感个人信息刑法特殊保护的基本内涵。另外,笔者认为,设置统一的“50条以上”的起刑点并不会造成量刑上的不平衡。例如,侵犯50条公民生物识别信息的行为和侵犯50条公民宗教信仰信息的行为,这两种行为同样都是侵犯公民敏感个人信息行为,且都已经达到了起刑点,但在具体量刑上完全可以体现出差异。具体如何量刑?实际判刑多少?完全可以由裁判者根据不同案件涉及敏感个人信息重要性的情况,在量刑幅度内灵活掌控。可见,对侵犯公民敏感个人信息犯罪的起刑点规定统一标准,不会产生量刑不平衡的问题。

3. 建议保持侵犯公民敏感个人信息“情节特别严重”较“情节严重”10倍以上的认定标准

《解释》第5条第2款列举了四项侵犯公民个人信息罪“情节特别严重”的认定标准,其中该条该款第3项规定,数量或者数额达到前款第3项至第8项规定标准10倍以上的,应当认定为侵犯公民个人信息罪“情节特别严重”。若继续保留该项规定,则侵犯公民敏感个人信息“情节特别严重”与侵犯公民一般个人信息“情节特别严重”的认定标准均是各自“情节严重”数量或者数额规定标准10倍以上。这里需要重点讨论的是,笔者在前文已经论述了敏感个人信息的重要性是要明显大于一般个人信息的,那么《解释》对敏感个人信息的保护是否也应该体现在相关情节的认定标准规定上?在认定“情节严重”时,侵犯公民敏感个人信息的起刑点相较侵犯公民一般个人信息,显然存在较大的差异,那么在认定“情节特别严重”时,是否也需要进一步拉开两者的差距?由此便产生了认定侵犯公民敏感个人信息“情节特别严重”与侵犯公民一般个人信息“情节特别严重”均是各自“情节严重”数量或者数额规定标准10倍以上是否合理的疑问。

笔者认为,在认定“情节特别严重”时,侵犯公民敏感个人信息与侵犯公民一般个人信息均采用较“情节严重”10倍以上的认定标准并无不妥,理由是:

认定侵犯公民敏感个人信息构成“情节严重”的起刑点为“50条以上”,认定侵犯公民一般个人信息构成“情节严重”的起刑点是“5000条以上”,而“情节特别严重”的认定标准是建立在“情节严重”的认定标准之上的。虽然在字面上两者采用的都是10倍以上的认定标准,但事实上认定侵犯公民敏感个人信息构成“情节特别严重”的起刑点是“500条以上”,而认定侵犯公民一般个人信息构成“情节特别严重”的起刑点则是“50000条以上”。尽管10倍以上数量的敏感个人信息泄露的社会危害性可能会远远大于10倍以上数量的一般个人信息泄露的社会危害性,但是这种看法显然忽略了比较的基数。如前所述,侵犯公民敏感个人信息“情节严重”的起刑点和侵犯公民一般个人信息“情节严重”的起刑点已经存在很大差别,因而即便从形式上看在认定“情节特别严重”时两者采用的都是10倍以上的认定标准,但是从实质上看两者的差距仍然是比较明显的。退一步讲,如果改变现有的认定标准,假设认定侵犯公民敏感个人信息“情节特别严重”的标准是“情节严重”5倍以上,认定侵犯公民一般个人信息“情节特别严重”的标准仍然保留原有的较“情节严重”10倍以上,看似进一步拉开了认定标准上的差距,但是,实际可能会压缩侵犯公民敏感个人信息行为适用“情节严重”这一档法定刑的空间,进而造成对敏感个人信息的过度保护。

需要指出的是,笔者早前曾发表观点认为,由于我们身处被各类信息包围的大数据时代,人们获取信息的途径愈来愈广泛,获取信息的途径越来越便捷,所以就导致了司法实践中行为人非法获取或者提供个人信息的数量动辄几十万甚至上百万条。因此,笔者担忧,以较“情节严重”10倍以上作为认定“情节特别严重”的标准,客观上可能会引发对侵犯公民个人信息罪实际“量刑不平衡”的状况出现,^⑥但是,当时的观点是在没有《个人信息保护法》的情况下形成的,特别是在刑法与刑法司法解释中没有敏感个人信息提法的情况下提出来的。现在在《个人信息保护法》颁行的背景下,我们又要通过修订《解释》规定增设“敏感个人信息”这一概念,如果不在

《解释》中设定一个明确的统一标准很难开展相关的司法活动。就此而言,笔者几年之前的担忧似乎也是多余,因为规范上的平衡显然更为重要。如此看来,我们在认定侵犯公民敏感个人信息与侵犯公民一般个人信息“情节特别严重”时均采用较“情节严重”10倍以上的认定标准并无不妥。

四、结语

在《个人信息保护法》对敏感个人信息下了定义并对敏感个人信息的处理规则作出明确规定的前提下,刑法以及相关刑法司法解释应当及时调整与《个人信息保护法》不一致的内容,以实现不同部门法之间对敏感个人信息保护的有效衔接。敏感个人信息与公民的人格尊严、人身安全和财产安全密切相关,因而刑法必须强化对公民敏感个人信息的保护力度。相关刑法司法解释应取消敏感个人信息的分级,实现对各种类型敏感个人信息一视同仁的特殊保护。在设定侵犯公民敏感个人信息行为“情节严重”以及“情节特别严重”的起刑点和量刑标准时,应当仔细考量敏感个人信息的特殊性,充分保障公民敏感个人信息的安全。

注释:

①参见《信息安全技术公共及商用服务信息系统个人信息保护指南》第3.7条。

②参见2017年版《信息安全技术个人信息安全规范》第3.2条。

③参见2020年版《信息安全技术个人信息安全规范》第3.2条。

④参见:《庐山市法院审理一起利用人脸识别方法盗取他人支付宝账户资金案》, http://k.sina.com.cn/article_3177450665_bd640ca902000vxxk.html, 2021年10月7日访问。

⑤参见蔡一博、吴涛:《利益衡量与场景实践下的未成年人信息保护研究》,载《青少年犯罪问题》2021年第4期。

⑥例如,处理敏感个人信息必须具有特定目的和充分必

要性(第28条第2款);处理敏感个人信息必须取得信息主体单独同意或书面同意(第29条);敏感个人信息的处理者须履行更严格的告知义务(第30条);处理不满14周岁未成年人的个人信息必须取得其父母或其他监护人的同意,且需制定专门规则(第31条);处理敏感个人信息应当遵从其他法律、行政法规中的特殊限制等(第32条)。

⑦参见刘宪权:《网络支付环境下涉信用卡犯罪对象新解》,载《法律科学》2021年第4期。

⑧《解释》第5条第1款第3项规定,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50条以上的,应认定为“情节严重”;该条该款第4项规定,非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息500条以上的,应认定为“情节严重”;该条该款第5项规定,非法获取、出售或者提供第3项、第4项规定以外的公民个人信息5000条以上的,应认定为“情节严重”。

⑨参见欧阳本祺、王兆利:《涉人脸识别行为刑法适用的边界》,载《人民检察》2021年第13期。李怀盛:《滥用个人生物识别信息的刑事制裁思路——以人工智能“深度伪造”为例》,载《政法论坛》2020年第4期。

⑩参见张继红、尹菡:《数字时代未成年人个人信息的法律保护》,载《青少年犯罪问题》2021年第2期。

⑪参见姜涛:《基因编辑之刑法规制及其限度》,载《东方法学》2021年第2期。

⑫《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,应认定为“情节严重”;该条该款第2项规定,知道或者应当知道他人利用公民个人信息实施犯罪,向其出售或者提供的,应认定为“情节严重”。

⑬参见绿杰、宋丹:《〈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〉理解与适用》,载《人民检察》2017年第16期。

⑭参见周光权:《侵犯公民个人信息罪的行为对象》,载《清华法学》2021年第3期。

⑮参见田宇申:《互联网保险中个人信息保护的法律规制——以个人信息保护政策为切入》,载《兰州学刊》2021年第9期。

⑯参见刘宪权、房慧颖:《侵犯公民个人信息罪定罪量刑标准再析》,载《华东政法大学学报》2017年第6期。