Doi:10.11835/j.issn.1008-5831.fx.2020.04.005

欢迎按以下格式引用:王德政.针对生物识别信息的刑法保护:现实境遇与完善路径——以四川"人脸识别案"为切入点[J].重庆大学学报(社会科学版),2021(2):133-143. Doi:10.11835/j.issn.1008-5831.fx.2020.04.005.

Citation Format: WANG Dezheng. The criminal protection about biological identification information: Current situation and perfection ways—Taking the case of "face identification" in Sichuan as starting point[J]. Journal of Chongqing University(Social Science Edition),2021(2):133-143. Doi:10.11835/ j.issn.1008-5831.fx.2020.04.005.

针对生物识别信息的刑法保护:现实境遇与完善路径
——以四川"人脸识别案"为切入点

王德政
(成都大学 法学院,四川 成都 610106)

摘要:当前生物识别信息在我国社会中的运用呈现逐年递增的趋势。生物识别信息具备本体特殊性和社会特殊性,这决定了其具备与普通公民个人信息不同的重要性,应受到刑法的特殊保护,但我国既定刑事立法对生物识别信息并未进行任何形式的特殊保护。可运用实质解释的方法,在不违反罪刑法定原则的前提下,充分利用两高《解释》第5条中第1款第10项和第2款第4项这两个兜底条款,将"侵犯生物识别信息5条及以上"认定为"情节严重",将"侵犯生物识别信息50条及以上"认定为"情节特别严重",由此降低针对生物识别信息原本的入罪和法定刑升格的数量,最终实现对生物识别信息的特殊刑法保护。

关键词:公民个人信息;生物识别信息;大数据;人脸识别;指纹识别

中图分类号:D294.34 **文献标志码**:A **文章编号**:1008-5831(2021)02-0133-11

一、问题的提出

当前,我国已全面迈入"互联网+"时代、人工智能时代和大数据时代。在这个科技日新月异的时代,信息的创制、利用和传播成为显著特征,这对我国公民个人信息的保护提出了严峻的挑战。在公民个人信息中,有些信息可以用来识别公民的身份,这些能识别公民身份的信息中又有一种特

修回日期:2020-12-10

基金项目:教育部人文社会科学研究青年项目"刑法目的解释研究"(18YJC820057)

作者简介:王德政,法学博士,成都大学法学院讲师,硕士研究生导师,Email:182402257@qq.com。

殊的信息——生物识别信息,诸如人脸、指纹、掌纹、耳廓、虹膜、视网膜、静脉、骨架、DNA、声纹、步态、笔迹等,因其反映了公民独特的人身特征而具备独一无二性,所以在识别公民身份上天然地具备极强并且迅捷的辨识效果,由此在我国社会生活中时常作为密码而被使用,比如在日常生活中经常用到的手机APP“刷脸”和指纹识别,以及越来越广泛运用人脸识别的住宅小区和连锁零售店,乃至智能门锁和受到年轻人欢迎的“换脸软件”[1]。而这只是基于个人感知的“冰山一角”,有记者调查后发现,国内利用生物识别信息的企业有千余家,市场约千亿规模,并且呈现迅速增长的趋势[2],生物识别信息的广阔市场前景及其在我国社会中所占的重要地位可想而知。

然而,生物识别信息所具备的独一无二性的另一面是不可替换性,即无法以同等种类的其他公民个人信息予以替换。因此,一旦作为密码使用的生物识别信息遭到泄露,将导致信息所有人无法像修改普通密码那样修改该密码,只能申请停用该密码,从而造成其在该密码的使用上遭遇较大的不方便,即便申请停用密码,也有两个问题:第一,由生物识别信息目前在我国的广泛运用性所决定,信息所有人必须在所有运用该密码的场合,都一一申请停用,否则可能导致该密码被他人在各种场合利用,从而遭受范围更广的损失,这进一步加剧了信息所有人通过四处奔波和彻底停用该密码所遭遇的不方便。第二,目前生物识别信息不像普通密码那样基本上可以通过网络上的自我操作(尤其是通过手机APP)迅捷、便利地申请停用,而在住宅小区和连锁零售店等多个场合,一般只能通过电话联络或现场办理等相对间接而迟缓的方式申请停用,在停用之前可能导致该密码被他人进行持续性的非法利用,从而导致信息所有人遭受持续性的损失。在生物识别信息的各类型中,人脸信息的采集和运用在我国社会较为广泛而常见,这意味着人脸信息泄露事件的发生更为频繁,由此决定了相关案件在我国司法实践中的多发性,其中的民事案件较为知名的是被媒体广泛报道的所谓“中国人脸识别第一案”。该案中,浙江理工大学郭兵副教授以杭州某动物园要求顾客进行人脸识别而影响其年卡的使用为由,于2019年10月28日将该动物园告上法庭,引发了社会的广泛关注。而相关的刑事案件中,比较典型的是发生在四川省成都市的一起性质更为严重的“人脸识别案”。该案中,唐杰非法获取唐某的支付宝账户信息和人脸肖像后,采用制作唐某3D人脸动态图的方式突破了支付宝人脸识别认证系统,后又将唐某的支付宝账户信息提供给张羽,张羽采取相关手段盗窃了唐某支付宝账户内的人民币2.4万余元①。该案的严重性体现在唐杰非法获取唐某的生物识别信息后非法提供给他人,引发了财产犯罪的发生,最终导致唐某的财产遭受侵害。但容易被忽略而更值得注意的是,即便唐某得知其人脸信息被泄露后想及时“止损”,都无法通过“换脸”的方式直接、迅速地修改该密码,而只能向支付宝企业申请停用该密码,更为麻烦的是,唐某还必须在所有运用其人脸信息的场合一一申请停用该密码,这可能造成其在支付、出行等各方面的不方便。此外,唐某在所有的场合都成功申请停用该密码之前,如果该密码继续被他人以各种方式利用,甚至有人利用该密码“刷脸”进入其居住的小区和住宅,唐某遭受的侵害可能不仅仅来源于财产犯罪,甚至可能是人身犯罪。

由此可见,在公民个人信息的保护中,给予生物识别信息一种特殊对待的重要性不言而喻。但就公民个人信息的种类而言,目前我国法律上各类个人信息都处于混同状态[3],我国《刑法》也未将生物识别信息从公民个人信息中独立出来并给予特殊的定罪量刑标准,这就提出了以下问题:第

①成都市郫都区人民法院(2019)川0124刑初610号刑事判决书。

一,如何全面分析我国刑事立法中对公民个人信息的不同分类所持的态度和表现,总结其问题和成因;第二,如何在理论上全面而详细地论证对生物识别信息应在刑法上进行特殊保护的必要性;第三,如何从立法修正或刑法解释的角度,提出对生物识别信息进行特殊保护的具体方案。笔者拟于下文中通过论证和提出具体方案来逐一解决上述问题,并以此求教于学界同仁。

二、保护现状的问题和成因

公民个人信息保护在我国刑事立法上,经历了一个渐进的过程。1949 年新中国成立后,从“79 刑法”到“97 新刑法”中都没有关于保护公民个人信息的罪名,但 2009 年出台的我国《刑法修正案(七)》作为一个转折点,在我国《刑法》第 253 条设立了“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”,这是一个巨大的进步,但囿于当时的时代局限,生物识别信息被侵犯的现象并未表现得较为严重,对其予以特殊保护的必要性也由此不太明显。因此,立法者在立法说明中仅将公民个人信息的外延解释为公民的姓名、住址等司法实践中经常被侵犯的信息,而没有明确列举生物识别信息,从而采取了一种对公民个人信息不分类而是统一保护的立法方式[4]。从 2009 年到 2015 年,我国公民个人信息被侵犯的现象呈现出大幅度严重化的趋势,无论是侵犯主体、侵犯行为方式、侵犯客体等方面,都发生了很大的变化,可以说,公民个人信息被侵犯在此期间经历了从简单到复杂、从轻微到严重的轨迹。有鉴于此,立法者迅速地因应客观实际的变化,于 2015 年出台了我国《刑法修正案(九)》,在形式和实质上都修改了我国《刑法》第 253 条的内容,具体表现为:第一,将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”这两个罪名,整合为“侵犯公民个人信息罪”。具体而言,是将“出售”“提供”“获取”三种行为方式,在语词上整合为“侵犯”。这属于形式上的改变。第二,将新罪名的行为主体从之前的特殊主体——国家机关或者相关单位的工作人员,扩大为一般主体——年满 16 周岁的人。这是从构成要件中行为主体要素的角度作出的实质性改变[5]。对于第二个改变,立法者指出,“近年来,出售、非法提供和非法获取公民个人信息的犯罪出现了一些新情况。根据《刑法修正案(七)》的规定,只能打击金融、电信等单位工作人员出售、非法提供公民个人信息的犯罪行为,而对于一般主体违背个人意愿,出售、非法提供公民个人信息的,难以依法惩治”[6]。可见,针对行为主体的修改,体现了时代和社会的新变化对立法完善的需求。但遗憾的是,立法者在立法说明中解释公民个人信息时,重复性地阐述了前次刑法修正案中的定义和种类,尚未前瞻性地以列举的方式将生物识别信息纳入其中。2017 年,由于司法实践中对侵犯公民个人信息罪需要相应具体解释的呼声较为迫切,最高人民法院、最高人民检察院联合制定了《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》(下文简称《解释》),对该罪的构成要件(如公民个人信息的内涵和外延等)和量刑标准(如罚金数额的确定)两个方面进行了具体的解释。但同样遗憾的是,该司法解释未对生物识别信息进行列举。尽管如此,侵犯公民个人信息罪从无到有、从粗略到细致的上述制定过程,体现了我国立法者负责地回应我国社会现实需求的敏感性,这种务实的态度可为今后我国刑事立法对生物识别信息的特殊重视埋下伏笔和作出铺垫。

立法者对侵犯公民信息罪构成要件的设计进一步贯彻了该罪立法说明中对公民个人信息不予分类的态度。该罪构成要件的优点是,在作为构成要件要素之一的实行行为的叙明上显得较为细致,其将实行行为具体分为获取、出售、提供三类[7],其中又将“获取”中的“盗窃”予以独立列举,这使得司法实践工作者在办理相关案件时,能借此对实行行为进行精确的界定。但这一细致性的优

点并未在该罪另一构成要件要素——行为客体上体现出来。通过梳理立法史可知,历次刑法修正案和《解释》中,该罪的行为客体——公民个人信息的具体种类都会被立法者一一列举,其中生物识别信息自始至终的缺位反映了立法者对该种类所蕴含的特殊重要性欠缺充足的认识,以至于该罪的行为客体只能在法条表述中笼统地表现为"公民个人信息"这个庞杂的概念,而必然不可能划分为普通公民个人信息和生物识别信息两大类,从而也就不可能对不同的行为客体设计不同的构成要件和量刑标准,也就最终无法实现对生物识别信息进行特殊保护的目的。该罪被制定后,受刑事立法的影响,我国的刑法教科书论及侵犯公民个人信息罪时,一般都简单复述立法者在立法说明中对公民个人信息种类的既定划分,同样不列举生物识别信息这一种类[8],而个别刑法教科书列举了在表述上不同于生物识别信息的"生理信息"[9],长此以往,可能会从知识传递的角度,潜移默化地影响我国理论界和实务界对生物识别信息的重视度。

由此可知,我国现行刑事立法对生物识别信息保护尚存在缺陷,可简要归纳为两个方面:第一,从我国刑法历次修正案到《解释》,立法者对公民个人信息的种类进行列举时,从来都对生物识别信息未置一词,这降低了该种类在公民个人信息中的特殊重要性;第二,侵犯公民个人信息罪的法条表述中欠缺对生物识别信息针对性的定罪量刑标准,这不利于通过对行为人的定罪和量刑进行影响,去实现对生物识别信息的特殊保护。

之所以存在上述缺陷,是基于以下原因:第一,时代的局限性。2015年之前,虽然侵犯公民个人信息的案件在我国社会的发生呈现上升趋势,但这些案件中主要遭到侵犯的是诸如公民的身份证号、电话号码等常规个人信息,生物识别信息作为一种新兴而相对高端的个人信息,被侵犯的前提尚需一种相应的科技运用环境,而当时我国社会的科技环境尚不完善,生物识别信息被侵犯的频率较低,社会大众由此对该信息蕴含的特殊重要性欠缺感性和理性认识,自然无法让立法者对该信息的保护引起特殊重视;但在2015年以后,随着人工智能和大数据技术的突飞猛进和广泛运用,同时伴随着移动支付在商业中的大幅推广,诸如人脸和指纹识别等新技术逐渐在我国社会得到越来越广泛的采用,时代的局限性被突破,生物识别信息的特殊重要性也随之愈加凸显。就我国司法实践来看,通过对中国裁判文书网所公布的刑事裁判文书进行梳理可发现,从2017年到2019年,我国法院已审结的涉及侵犯人脸信息的案件分别为2件、3件、11件,共计16件,呈现逐渐递增的趋势,2019年是2017年案件的5.5倍。可以预测,2020年及其以后,随着人脸识别技术在我国社会的进一步推广,这类案件将继续呈现大幅增加的趋势。值得注意的是,生物识别信息的具体分类除了人脸信息之外还包含指纹等多种信息,如果将所有种类的生物识别信息都纳入其中并且将法院未进行审理的案件包括游离于刑法规制之外的"犯罪黑数"[10]都考虑进来,相关案件的数量将不可小觑。第二,罪名分类细致性的弱化。虽然我国《刑法》对少数犯罪的规定较为细致,比如,将诈骗罪分为普通诈骗罪和特殊诈骗罪两类,共计规定了包括诈骗罪、金融诈骗罪等在内的10多个罪名,相比德国《刑法》第263—264条规定的诈骗罪、计算机诈骗罪、捐助诈骗罪、投资诈骗罪这4个罪名[11],更为全面而细致,但在诸多犯罪诸如抢劫罪种类上的规定却稍显笼统。比如日本《刑法》对抢劫罪规定了普通型抢劫罪、事后抢劫罪、昏醉抢劫罪、抢劫致死伤罪、抢劫强奸罪、抢劫强奸致死罪6类[12],而我国《刑法》只规定了普通型抢劫罪、转化型抢劫罪,抢劫枪支、弹药、爆炸物、危险物质罪3类。这样粗略的立法方式还体现在侵占罪等罪上[13]。这说明,我国刑事立法在罪名设定上的具体、细致性需要进一步加强。反映在公民个人信息的刑法保护上,就必然导致不可能对公民个

人信息进行细致的分类并根据不同种类设定不同的定罪量刑标准。

三、特殊保护的必要性和方式

(一)必要性

既然我国现行刑事立法对生物识别信息的保护呈现较为不力的现状,那么需要在理论上深入讨论的是,生物识别信息相比其他公民个人信息究竟有何种不同而由此具备被特殊保护的必要性。如果从生物识别信息的本体特质和社会层面两个维度进行考察,可发现其具备明显不同于其他公民个人信息的特殊性。

第一,本体特殊性。包括人身反映性、高度人格尊严性、独一无二性、不可替换性、不可改变性。(1)人身反映性是指生物识别信息能直接反映自然人的身体和行为特征,由此具备针对身体的直接指向性和紧密依从性。比如,人脸和指纹反映的是人的脸部和手指的特征;笔迹通过体现人书写的独特习惯,反映的是人用以写作的身体部位(多为手部)的行为特征,而人的行为特征恰恰反映了其身体特征,可以说前者对后者具备紧密的依从性。这就使得生物识别信息与并不直接反映人身特征的普通公民个人信息(如身份证号码、家庭住址等)截然区分开来。人的身体不仅仅体现了其核心隐私,更属于人生命的载体,对人的生命存续起着不可替代的重大作用,侵害身体的行为(尤其是故意杀人罪、故意伤害罪等)属于当今任何一个国家的刑法都严厉惩治的犯罪行为,生命和身体完整性随之成为刑法中最为重大的保护法益[14],这就需要对直接反映人身特征的生物识别信息,在刑法上给予特殊的重视。(2)高度人格尊严性是指生物识别信息能够极其强烈地体现自然人的人格尊严。自启蒙时代以来,人格尊严就属于人的重大权利之一,如耶林所言,没有权利就没有个人的权利,也没有民族的权利[15],其意义性不言而喻。就实定法的角度而言,人格尊严受到我国《宪法》第 38 条的明文保护,我国《刑法》中的侮辱罪、诽谤罪也专门保护人格尊严[16]。生物识别信息之所以具备高度人格尊严性,归根究底是因为其具备人身反映性,这两种性质紧密相连并且前者由后者所决定。具体而言,人的人格尊严一般可以通过人的身体、精神和财产被侵害而受到侵犯,尤其是人的身体被侵害时,只要被害人具备理性的认识能力和清醒的认识状态,都往往伴随着精神的痛苦而加剧了其人格尊严被侵犯的程度。公民的生物识别信息遭到侵犯时,被害人的核心隐私被泄露甚至利用,其人身受到某种程度的商品化,主观上可能产生一种特殊的受辱感,其人格尊严毫无疑问地受到了侵害。(3)独一无二性是指公民同种类的生物识别信息只有单独 1 份而没有多份,也与其他人同种类的生物识别信息不同,这是由每个人身体器官和行为特征的独特性所决定的。比如,人只有 1 个食指,从食指中采集的指纹则与自己其他手指和他人食指的指纹不同。尤其是 DNA 信息更加具备独一无二性,由于每个人 DNA 的不同在科学上是绝对的法则,其对于鉴定人的身份具备超强的优势,由此在世界各国的刑事侦查程序中,被广泛应用于辨认犯罪嫌疑人和尸体的身份、排除犯罪嫌疑人、亲子鉴定中[17]。值得注意的是,独一无二性并不等同于无法复制性或难以变造性,生物识别信息曾被学界认为具备防伪性强的特征,但近来时常发生通过技术手段冒充他人身份的案例,如本文开头所提到的四川“人脸识别”案,证明了某些种类的生物识别信息(如脸部信息)可以在技术支持下被轻易复制甚至变造。(4)不可替换性是指无法以同种类的生物识别信息去替代既定信息的运用,这是由独一无二性所决定和衍生出的性质。比如,公民的人脸信息被泄露后,无法像替换普通密码那样,可以通过采取自己“第二张脸”的信息,或者通过寻找一个外貌上与自己丝

毫无差的人采集其人脸信息,去替换自己被泄露的人脸信息。(5)不可改变性是指公民无法或者难以改变其生物识别信息的特征。虽然通过整容、手术、改变个人习惯等方式,可以有限地改变人脸、指纹、掌纹、耳廓、骨架、声纹、步态、笔迹等信息,但这种改变要付出较大的身体、技术和经济代价,可视为难以改变的信息,完全无法改变的信息包括DNA、虹膜、视网膜、静脉等,这意味着生物识别信息在应用中具备稳定性和可靠性。

第二,社会特殊性。包括广泛运用性、密码使用性、人身和财产犯罪关联性、停用带来的不方便性、停用前损失的持续性、法益特殊性。(1)广泛运用性是指生物识别信息已在我国社会生活、学习、商业等各方面得到了越来越多的运用,其最大市场主要是电子商务、电子政务、个人用设备[18],这一点可以说已被我国广大群众所熟知。生物识别信息一旦运用于社会实践,就必然决定了其不仅具备该特殊性,下文中其他各种社会特殊性也由此而生。(2)密码使用性是指生物识别信息通常被公民当作密码使用,常见的操作如在支付宝、淘宝、银行等手机APP上以"刷脸"和验证指纹的方式进行登录和支付,不少住宅小区也以"刷脸"作为进入小区的方式。尤其是生物识别信息被某单位或个人强制作为唯一可用的密码使用时,比如本文开头提到的杭州动物园"人脸识别"案,相关冲突和诉讼发生的概率便有所提升,生物识别信息对于公民的特殊重要性及其特殊保护必要性亦随之增加。(3)人身和财产犯罪关联性是指当生物识别信息被当作密码使用时,一旦该密码被泄露,他人可能利用该密码从事相关财产和人身犯罪,以致造成信息所有人的财产权乃至人身权被侵害。这种伴随而生的财产犯罪在司法实践中主要是盗窃罪,人身犯罪可能涉及非法侵入公民住宅罪、强奸罪、强制猥亵罪、绑架罪,乃至故意杀人罪、故意伤害罪,同时还可能诱发入户型抢劫罪,这种关联性应引起全社会的高度警惕。本文开头提到的四川"人脸识别案"就是被害人的人脸信息被泄露后用于实施盗窃罪的典型案例。(4)停用带来的不方便性是指作为密码使用的生物识别信息由于无法以同种类的信息替换而只能由信息所有人申请停用,但由于该密码可能被用于多个场合,信息所有人只能逐一申请停用而带来奔波之苦,停用还意味着信息所有人从此无法使用这类密码,转而只能将普通公民个人信息作为密码使用,尤其是在生物识别信息被强制作为唯一的密码使用这种情况下,更会给信息所有人带来不方便。(5)停用前损失的持续性是指由于当前我国社会对生物识别信息的运用还没有达到一种程度,以至于信息所有人本来完全可以直接通过网络上的操作去申请停用被泄露的密码,却只能通过电话或现场办理的方式申请停用,停用成功之前的时间差可能导致该密码被他人继续非法利用,从而使信息所有人受到持续性的损失。(6)法益特殊性是指生物识别信息承载的法益相较于普通公民个人信息所具备的不同之处。我国刑法学者一般将侵犯公民个人信息罪的保护法益界定为以下两大类:一是公共法益,又分为公共信息安全[19]、公权主体及其关联主体对公民个人信息的保有[20]、个人信息安全的社会信赖[21]、社会信息管理秩序[22]4类;二是个人法益,又分为公民的隐私权[23]、公民人格尊严与个人自由[24](或以人格权为内核的个人信息权[25])、信息自决权[26](或称信息专有权[27])3类。但立法者在立法理由中指出,设立侵犯公民个人信息罪是为了保护公民的人身财产安全,保护个人隐私和正常的生活、工作不受侵害与干扰,通过历史解释(立法者原意解释)的方法[28],可以直接排除公共法益,而在个人法益的上述种类中,可发现生物识别信息承载的法益并非普通公民个人信息一般所承载的单一法益,而是复合法益,包括公民的信息自决权、人格尊严、核心隐私权、人身和财产安全、生活安宁权、信息运用的便利性。这种复合法益成为应对生物识别信息进行特殊刑法保护的理由。

生物识别信息所具备的上述本体特殊性和社会特殊性,使其具备了与普通公民个人信息不同的重要性。这意味着,对生物识别信息采取与普通公民个人信息相同的刑法保护方式明显欠妥,既定保护方式不仅由于违反了生物识别信息的特殊性而在逻辑上无法自洽,还将导致侵犯生物识别信息的行为由于无法受到比侵犯普通公民个人信息的行为更重的否定性评价和刑罚制裁,从而导致公民的人格尊严、核心隐私权、人身和财产安全、信息运用的便利性等一系列法益无法得到应有的保护,也无法对侵犯生物识别信息的犯罪实现一般和特殊预防的刑罚目的[29],无论是在理论上还是实践上都存在巨大的漏洞和弊端。因此,改变我国刑事立法对生物识别信息保护不力的现状,反过来对其进行特殊保护很有必要。

(二)方式

在对我国刑事立法提出完善方案之前,有必要从比较法的角度简要地梳理和评析一下国外对生物识别信息的立法模式。在当今世界各国的法律体系中,对生物识别信息进行特殊保护的立法模式体现为两类:一是在统一的信息或数据法中保护生物识别信息,如欧盟、印度、巴西等国,这是主流模式;二是出台专门的生物识别信息保护法来进行保护,这主要是美国的各州[30]。我国有不少学者赞同采取与美国相同的立法模式[31],以专门立法的方式来应对我国当前个人生物识别信息法律保护的现实需要[32]。毫无疑问,以专门的法律来保护生物识别信息会起到更全面的保护效果,但考虑到我国至今连统一的信息保护法都未出台,制定专门的法律在当前看来似乎不切实际并且“远水不解近渴”。但我国将来无论采取何种保护模式,都绕不开一个现实问题,那就是在我国既定刑事立法中如何就生物识别信息进行针对性的完善。有学者认为我国《刑法》对公民个人信息采取统一保护的立法模式存在弊端,并据此提出个人信息的分类保护模式[33],这显然是从修改法律的角度提出的建议,但问题在于,在我国将来出台新的旨在对生物识别信息进行特殊保护的《刑法修正案》之前,如何从刑法解释的角度,对既定的侵犯公民个人信息罪进行解释,使其能起到对生物识别信息进行特殊保护的效果,对司法实践中紧迫的办案需求而言,应该更具备现实意义。因此,可以从刑法解释而非修改法律的务实角度来实现我国刑事立法对生物识别信息的特殊保护。

根据我国《刑法》第 253 条并结合犯罪论体系的理论,可将侵犯公民个人信息罪的构成要件简要归纳为行为人非法获取、出售或者提供公民个人信息,情节严重,其基本刑为 3 年以下有期徒刑或者拘役,并处或者单处罚金。法定刑升格的情形为情节特别严重的,处 3 年以上 7 年以下有期徒刑,并处罚金。可见,行为人的行为是否“情节严重”或者“情节特别严重”,对于该行为是否构成侵犯公民个人信息罪或者应当被加重处罚,显得极其重要。情节在犯罪论体系中的定位,根据陈兴良教授的观点,属于罪量要素而非构成要件要素[34]。这意味着,我国《刑法》中的情节对应的是德国、日本刑法中的客观处罚条件[35]。这种定位在司法实践上的意义是,根据刑法通说中故意的成立要求——行为人必须对所有的客观构成要件要素有认识和意欲[36],判断行为人是否具备侵犯公民个人信息罪的故意时,不要求其必须认识到情节是否严重或特别严重。对情节严重或特别严重的具体界定,《解释》第 5 条进行了详细的阐述。问题是,如何运用这一既定立法资源去实现对生物识别信息的特殊刑法保护?《解释》第 5 条第 1 款第 3—5 项本质上是对公民个人信息进行了分类并给不同的种类设定了相应的入罪数量,可以试图从中找到一个突破口。具体而言,第 3—5 项对公民个人信息的种类和入罪数量确定为:第一,行踪轨迹信息、通信内容、征信信息、财产信息 50 条及以上;第二,住宿信息、通信记录、健康生理信息、交易信息等 500 条及以上;第三,其他信息 5 000 条及以

上。然而,生物识别信息并未被明文归入第1、2类,只能被归入“其他信息”的范畴,这非但无法实现对生物识别信息特殊保护的目的,相反,还由于必须满足最高的入罪数量而提高了侵犯生物识别信息行为的入罪门槛。如果认为“健康生理信息”这一概念等同于生物识别信息,或者将“健康生理信息”作扩大解释,将生物识别信息硬性地涵摄其中,则会导致这两个概念发生混淆,因为全国信息安全标准化技术委员会制定的《信息安全技术 个人信息安全规范》已明确将生物识别信息和健康生理信息规定为公民个人信息的不同种类。根据逻辑常识,并列的两个概念不可能在外延上存在包容或交叉的关系,而只能是互斥的关系。如果运用第2类中的“等”字,将生物识别信息归入“等”字之内而成为与住宿信息等并列的第2类信息,也无法实现对生物识别信息特殊保护的目的,因为按照体系解释的要求[37],既然生物识别信息的重要性明显大于第1类中诸如通信内容等普通公民个人信息,要求生物识别信息达到500条才能入罪,而通信内容只需要50条即可入罪,会导致轻重失衡,显然不合理。如果违反语义解释的要求[38],转而将生物识别信息纳入第1类,又会破坏罪行法定原则的明确性要求[39]。这是因为,生物识别信息不仅不属于第1类中任何一种信息,并且第1类的语词表述中也没有“等”字这一解释空间,此外,即使强行纳入,也会造成轻重失衡。因为前文已述,生物识别信息的重要性大于第1类中的任何信息,毋宁说,第3—5项中所有信息的特殊性和重要性都不及生物识别信息。可见,无论是从形式解释的角度,还是基于实质解释的立场,沿用第3—5项对公民个人信息的既定分类,根本无助于对生物识别信息进行特殊保护。

但立法者可能也预见到充满活力的我国社会将不断发生始料未及的新情况,在《解释》第5条第1款第10项以“兜底条款”的方式规定了“其他情节严重的情形”,为解决新情况留下了一个解释空间,而这正是对生物识别信息进行特殊保护的真正突破口。虽然有学者认为兜底条款可能与罪刑法定原则相冲突而提出批评[40],但考虑到当前我国社会中新现象不断发生的实际情况,在刑事立法中保留和运用兜底条款而不是采取彻底否定的态度,更能解决一些现实问题。可以考虑通过将“非法获取、出售或者提供生物识别信息5条及以上”解释为该项规定的“其他情节严重的情形”,这就能从刑法解释的角度实现对生物识别信息的特殊保护,理由在于:第一,既然生物识别信息的重要性大于第3—5项的任何信息,将侵犯一定数量的生物识别信息直接认定为“其他情节严重的情形”,会起到超越任何其他种类公民个人信息的超强保护效果;第二,无须将生物识别信息的入罪数量设定为1—4条,这是考虑到刑法的最后手段原则[41]提出的谦抑性要求;第三,将生物识别信息的入罪数量设定为5条而非更多,是为了与其他信息的既定数量(50条、500条、5 000条)形成与其重要性成比例的梯次。因此,只要行为人实施非法获取、出售、提供生物识别信息的行为,只要该信息的数量达到5条,其行为就因“情节严重”而可能构成非法侵犯公民个人信息罪。据此,由不同种类公民个人信息的重要性所决定,我国刑事立法可通过对之设定不同的入罪数量而体现出轻重不同的保护力度:第一,侵犯生物识别信息5条才能入罪;第二,侵犯行踪轨迹信息等50条才能入罪;第三,侵犯住宿信息等500条才能入罪;第四,侵犯其他信息5 000条才能入罪。

此外,针对法定刑升格的认定,《解释》第5条第2款具体解释了何种情形为“情节特别严重”,该款第3项将“数量达到前款规定第3项至第5项规定标准的10倍以上”的情形认定为“情节特别严重”,然而,《解释》第5条第1款第3—5项规定的公民个人信息在字面上并不包含生物识别信息,无法直接从中推导出“侵犯生物识别信息50条及以上为‘情节特别严重’”的结论,否则将成为不利于行为人的类推解释而违反罪刑法定原则[42],但这一结论可以通过适用同为兜底条款的《解

释》第5条第2款第4项并参考该条款第3项来推导得出,具体而言,第4项规定了“其他情节特别严重的情形”,这当然可以涵括“侵犯生物识别信息5条及以上”的情形,但既然该项规定了“特别”二字,显然就意味着侵犯生物识别信息的数量要极大地超越5条的限定,而第3项中“10倍”的数量较好地体现了这种特别严重的程度,可由此被沿用为对生物识别信息数量的限定。因此,“侵犯生物识别信息50条及以上”属于《解释》第5条第2款第4项的“其他情节特别严重的情形”,行为人的行为如果具备该情形并构成非法侵犯公民个人信息罪,行为人将被判处升格后的法定刑。

概言之,通过运用实质解释的方法,在不违反罪刑法定原则的前提下,充分利用《解释》第5条中第1款第10项和第2款第4项这两个兜底条款,将“侵犯生物识别信息5条及以上”认定为“情节严重”,将“侵犯生物识别信息50条及以上”认定为“情节特别严重”,借此降低针对生物识别信息原本的入罪和法定刑升格的数量,可实现对生物识别信息的特殊刑法保护,并且完全不影响对其他种类公民个人信息既定的定罪量刑条款的适用,由此在我国刑事立法中呈现出一种于法有据、条理分明、轻重有序并能兼顾生物识别信息特殊性的合理保护格局。

四、结语

当前生物识别信息在我国社会中的运用呈现逐年递增的趋势,这首先带给我国公民极大的便利,其次也隐藏着诸多刑法上要解决的问题。放眼国外最新的立法情况,2018年5月25日,欧盟出台了《通用数据保护条例》,给予生物识别信息明确的定义[43],并对公民个人信息进行分类和设定不同的保护方式[44],能提供给我国一个借鉴的思路。在这个公民个人信息在全球和我国都越来越重要、相关法律体系越来越完善的新时代,我国的立法者和司法实践工作者都有必要敏捷和充分地认识到生物识别信息相对于普通公民个人信息所蕴含的特殊性、重要性和超强保护必要性,尤其是对于司法实践工作者而言,在办理侵犯公民个人信息的案件时应避免机械地适用我国刑事立法中的相关条款,而不至于无法对生物识别信息进行特殊保护,可转而运用刑法解释的方式,在合法、合理的前提下,实质、灵活地运用既定立法资源,在涉及生物识别信息的入罪和法定刑升格这两个方面,都采取相较于普通公民个人信息更为宽松的认定方式,以最终通过办案实践来实现对我国公民生物识别信息的超强刑法保护,有效地回应新时代的司法需求。

参考文献:

[1]刘春泉.换脸软件涉嫌公众安全 人体生物识别信息管理要跟上[N].第一财经日报,2019-09-24(A11).

[2]王丽.生物识别信息滥用催生灰色产业[J].方圆,2019(24):18-23.

[3]付微明.大数据时代个人生物识别信息法律保护的重要意义[J].研究生法学,2019(4):134-140.

[4]全国人大常委会法制工作委员会刑法室.中华人民共和国刑法条文说明、立法理由及相关规定[M].北京:北京大学出版社,2009:515.

[5]ZIESCHANG F. Strafrecht allgemeiner teil[M]. Berlin:Richard Boorberg Verlag,2017:24.

[6]全国人大常委会法制工作委员会刑法室.中华人民共和国刑法修正案(九)条文说明、立法理由及相关规定[M].北京:北京大学出版社,2016:127.

[7]魏东.刑法各论[M].北京:法律出版社,2015:152.

[8]魏东.刑法:原理·图解·案例·司考[M].北京:中国民主法制出版社,2016:534.

[9]张明楷. 刑法学[M]. 北京:法律出版社,2016:921.

[10]王震. 刑法的宣示性:犯罪黑数给我们带来的思考[J]. 烟台大学学报(哲学社会科学版),2015(5):34-43 .

[11]SCHÖNKE A, SCHRÖDER H. Strafgesetzbuch kommentar[M]. Berlin:C. H. BECK, 2014:2485.

[12]山口厚. 刑法各论[M]. 王昭武,译. 北京:中国人民大学出版社,2011:248.

[13]陈璇. 论侵占罪处罚漏洞之填补[J]. 法商研究,2015(1):136-146.

[14]KUNDLICH H. Strafrecht besonderer teil Ⅱ: Delikte gegen die person und die allgemeinheit[M]. Berlin: C. H. Beck, 2009:51.

[15]鲁道夫·冯·耶琳. 为权利而斗争[M]. 郑永流,译. 北京:法律出版社,2007:9.

[16]黎宏. 刑法学[M]. 北京:法律出版社,2012:688.

[17]林钰雄. 刑事法理论与实践[M]. 北京:中国人民大学出版社,2008:309.

[18]宋子晴. 生物识别信息安全新主张[J]. 中国公共安全(综合版),2006(10):84-87.

[19]赵军. 侵犯公民个人信息犯罪法益研究:兼析《刑法修正案(七)》的相关争议问题[J]. 江西财经大学学报,2011(2):108-113.

[20]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[J]. 政治与法律,2017(10):27-38.

[21]江海洋. 侵犯公民个人信息罪超个人法益之提倡[J]. 交大法学,2018(3):139-155 .

[22]凌萍萍,焦冶. 侵犯公民个人信息罪的刑法法益重析[J]. 苏州大学学报(哲学社会科学版),2017(6):66-71.

[23]王昭武,肖凯. 侵犯公民个人信息犯罪认定中的若干问题[J]. 法学,2009(12):146-155.

[24]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[J]. 政治与法律,2017(2):46-55.

[25]冀洋. 法益自决权与侵犯公民个人信息罪的司法边界[J]. 中国法学,2019(4):66-83.

[26]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[J]. 浙江工商大学学报,2019(6):20-32 .

[27]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[J]. 法学评论:2018(2):116-127.

[28]KINDHÄUSER U. Strafrecht allgemeiner teil[M]. Berlin:Nomos,2015:43.

[29]FREUND G,ROSTALSKI F. Strafrecht allgemeiner teil[M]. Berlin Heidelberg:Springer Berlin Heidelberg, 2019.

[30]赵淑钰. 生物识别信息法律规制的国际经验与启示[J]. 中国信息安全,2019(11):37-39,43.

[31]马斯蒙. 美国个人生物识别信息法律保护路径探析[J]. 法制博览,2019(4):258.

[32]付微明. 个人生物识别信息的法律保护模式与中国选择[J]. 华东政法大学学报,2019(6):78-88.

[33]董悦. 公民个人信息分类保护的刑法模式构建[J]. 大连理工大学学报(社会科学版),2020(2):80-89.

[34]陈兴良. 规范刑法学[M]. 北京:中国人民大学出版社,2013:196.

[35]FRISTER H. Strafrecht allgemeiner teil[M]. Berlin:C. H. Beck,2015:91.

[36]FRISTER H. Vorsatzdogmatik in deutschland[J]. Zeitschrift für Internationale Strafrechtsdogmatik,2018, 7:381-386.

[37]STRATENWERTH G,KUHLEN L. Strafrecht allgemeiner teil[M]. Berlin:Vahlen,2011:46.

[38]MAURACH R,ZIPF H. Strafrecht allgemeiner teil 1 grund lehren des strafrechts und aufbau der straftat[M]. Berlin:C. F. Müller,1992:116.

[39]HOFFMANN-HOLLLAND K. Strafrecht allgemeiner teil[M]. Berlin:Mohr Siebeck,2015:9.

[40]刘沐阳. 兜底条款的局限性及其实践运用[J]. 人民检察,2014(8):58-60.

[41]JESCHECK H,WEIGEND T,STRAFRECHTS L,et al[M]. Berlin:Duncker & Humblot,1996:53.

[42]SCHMIDHAUSER E. Strafrecht allgemeiner teil lehrbuch[M]. Berlin:J. C. B Mohr(Paul Siebeck) Tübingen,1970:110.

[43]EUROPEAN UNION. General Data Protection Regulation[EB/OL]. (2018-05-25)[2020-2-12]. http://eurlex. europa.

eu/legal content/EN/TXT/?uri=uriserv:OJ. L_. 2016. 119. 01. 0001. 01. ENG&toc=OJ:L:2016:119:TOC.

[44]全国信息安全标准化技术委员会. 网络安全实践指南—欧盟 GDPR 关注点[EB/OL]. (2018-05-25)[2020-2-12]. https://www. tc260. org. cn/upload/2018-05-25/1527251794595094938. pdf.

The criminal protection about biological identification information: Current situation and perfection ways ——Taking the case of “face identification” in Sichuan as starting point

WANG Dezheng

(*Law School*, *Chengdu University*, *Chengdu 610106*, *P. R. China*)

Abstract: Currently the application of biological identification information in our society shows a more and more increasing tendency. Biological identification information has its own particularity and social particularity, which decides that it has an importance which is different from common personal information of citizens, so it deserves to be specially protected by criminal law. However, there is not any form of special protection about biological identification information in current criminal law of China. Substantial interpretation method could be used to sufficiently take advantage of the two miscellaneous provisions of paragraph 1, item 10 and paragraph 2, item 4 in Article 5 of “Interpretation” of Supreme People’s Court and Supreme People’s Procuratorate under the premise of obeying principle of legality. We could consider “violating 5 or more pieces of biological identification information” as “gravity of the circumstances”, and consider “violating 50 or more pieces of biological identification information” as “especially serious circumstances”. By this way could the original quantities of conviction and promotion of legal penalty about biological identification information decrease. Finally, the special protection of biological identification information could be achieved.

Key words: personal information of citizens; biological identification information; big data; face identification; fingerprint identification

(责任编辑　胡志平)