Open Journal of Legal Science 法学, 2023, 11(5), 3991-4000
Published Online September 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.115567

Hans汉斯

大数据时代公民个人生物识别信息的刑法保护

——从人脸识别角度切入

韩晨艺

扬州大学法学院，江苏 扬州

收稿日期：2023年7月7日；录用日期：2023年7月25日；发布日期：2023年9月12日

摘　要

大数据时代，人工智能科技的迅速发展与深入使用为人们生活提供了更加自动化、便捷化的生活体验的同时往往会产生一系列道德风险和法律问题。个人的生物识别信息如果被泄露或者滥用，给公民带来的不仅是财产损害，更有可能造成人身威胁。现行法律和司法解释对于生物识别信息的规定却少之又少，《刑法》也未将生物识别信息纳入侵犯公民个人信息罪的法益保护范围内。本文以人脸识别为切入点，针对非法利用生物识别技术、侵犯公民生物识别信息的行为进行分析；阐述我国《刑法》对于生物识别信息规制的缺陷并提出相应的完善建议，以实现《刑法》对于生物识别信息的特殊保护。

关键词

人脸识别，生物识别信息，个人信息，侵犯公民个人信息罪

Criminal Law Protection of Citizens' Personal Biometric Information in the Era of Big Data

—From the Perspective of Face Recognition

Chenyi Han

Law School, Yangzhou Universitiy, Yangzhou Jiangsu

Received: Jul. 7th, 2023; accepted: Jul. 25th, 2023; published: Sep. 12th, 2023

Abstract

In the era of big data, the rapid development and in-depth use of artificial intelligence technology

文章引用: 韩晨艺. 大数据时代公民个人生物识别信息的刑法保护[J]. 法学, 2023, 11(5): 3991-4000.
DOI: 10.12677/ojls.2023.115567

provide people with a more automated and convenient life experience. At the same time, it often produces a series of moral risks and legal problems. If personal biometric information is leaked or abused, it will not only bring property damage to citizens, but also pose a personal threat. The current laws and judicial interpretations have few provisions on biometric information, and the *Criminal Law* does not include biometric information in the scope of legal interest protection of the crime of infringing on citizens' personal information. Taking face recognition as the starting point, this paper analyzes the illegal use of biometric technology and infringing on citizens' biometric information, and expounds the defects of the regulation of biometric information in China's *Criminal Law*, and put forward corresponding improvement suggestions to realize the special protection of biometric information in the *Criminal Law*.

Keywords

Face Recognition, Biometric Information, Personal Information, Crime of Infringing on Citizens' Personal Information

1. 引言

由于人工智能科学技术的蓬勃发展，人脸识别这一技术名词得以出现，并成为了新一代的人工智能科技中最具标志性的一种科技类型。在中国，如今人脸识别科技开始广泛应用于支付、交通、医药等领域的广泛应用，表明了随着中国科技的日益成熟，人脸识别科技在中国应用市场有着巨大的发展潜力，但同时也产生了不少危害与风险，就如所谓的“深度伪造”，2019 年 8 月，人工智能换脸软件“ZAO”刚刚上线，就受到了中国网友的欢呼和热议，因为只要上传一张自己的人脸图片，就可以和影视作品中的演员实现换脸，但是由于涉及到对公民信息的过度采集，该开发公司随后立即被工信部门约谈[1]。再如杭州的“人脸识别第一案”中，该动物园要求顾客进行人脸识别，否则将无法使用其年卡，于是浙江理工大学的郭兵副教授随即以民事侵权为由将该动物园告上法庭[1]。更有一起相关性质更为恶劣的刑事案件，2018 年 9 月，犯罪嫌疑人唐杰从非法渠道获取到了唐某的支付宝账户信息，随后通过制作唐某的 3D 人脸动态图，破解了人脸识别认证系统，解除了支付宝限制登录这一障碍，盗窃了唐某支付宝账户里 2.4 万余元[2]。“技术一旦进入社会领域，必然会被社会制度、社会组织和社会群体的各种利益、诉求和价值判断所塑造和限制”[2]，我们应当认识到，科技发展带来的不仅仅只是智能与便捷，还会产生一系列道德风险和法律问题。法律在预防新兴技术的合理使用所蕴含风险的同时，更应积极回应科技的不当使用给人们带来的威胁。实质上，人脸识别信息属于个人生物识别信息的一种，具有特殊性、唯一性和不可替代性，并且不同于其他个人信息，如果一经泄露或者滥用，将难以救济。虽然目前《网络安全法》《个人信息保护法》等前置性法律已经相继对个人信息作出了详细规定，但生物识别信息这一概念却始终未被明确纳入我国目前既有的《刑法》中。生物识别信息是否应当被纳入公民个人信息犯罪所保护的法益范围，如何就既有刑事立法对其进行保护，成为亟待解决的问题。

[1]杭州市富阳区人民法院(2019)浙 0111 民初 6971 号民事判决书。
[2]成都市郫都区人民法院(2019)川 0124 刑初 610 号刑事判决书。

2. 人脸识别信息的法律属性及潜在风险

2.1. 人脸识别的定义

人脸识别又称人像识别或者面部识别。从技术层面来看，人脸识别技术旨在通过自然人的脸部特征信息识别或验证自然人的身份，根据 2018 年欧盟《通用数据保护条例》的规定，人脸识别信息是指通过抓取人的面部特征等，进行一定的技术处理后形成的能识别到特定自然人的信息[3]。但从法律角度出发，人脸识别信息这一概念未被定义。立法和理论上都忽视了这一问题，进而导致司法实践的混乱，在上文提到的“张羽、唐杰、李瑞安侵犯公民个人信息案”中，被告人唐杰最终被判决构成非法获取计算机信息系统数据罪，而非侵犯公民个人信息罪，前罪属于社会秩序犯罪，后罪规定在人身犯罪中，二者所保护的法益并不相同，设立前罪的目的主要是为了保护数据安全，维护正常的社会管理秩序，而后罪主要强调对公民人身安全法益的保护[4]。不难看出法院最终认定唐杰构成非法获取计算机信息系统数据罪是存在问题的，判决的结果值得我们深入探讨。通过本案不难看出，认定这一行为的性质以及人脸识别信息的法律属性对于司法实践显得尤为重要。

2.2. 人脸识别使用目的和特点

近年来，人脸识别技术通常被使用在自然人的身份认定上，适用场景主要都是在宾馆、机场、高铁站等公共场所。所谓使用目的，主要是为了公共安全。对此，根据《个人信息保护法》第 26 条[3]，总结起来有以下几点值得我们注意：第一，在公共场所收集个人身份识别信息，需要尽到合理的提示义务；第二，要基于公共安全的目的；第三，是基于合理使用的目的，即除了用于维护公共安全的目的之外不能用于其他目的。实际上这三点中限定用于维护公共安全的目的才是实质性的限制条件，个人的人脸信息或者其他生物识别信息一旦被收集，收集的方式和渠道我们却无从知晓，且对于后续的使用环节我们个人是毫无控制力的，但如果仅有此目的性限制的话，如此一来，我们会发现没有哪个地方不符合此目的，小区、地铁、商场内使用人脸识别都可以说是为了公共安全目的。如果是为了所谓的公共安全，那么小区、商场完全可以将此信息收集归入监控，电视，发现违法犯罪行为时直接调出即可，而为什么非要识别特定的个人呢？近日，北京地铁五个站点开始推行人脸识别，实行“实名常乘客快速进站通道”，即乘客“刷脸”可免去部分安检，并将此与个人信用挂钩，认为这是一种奖励措施。清华大学法学院劳东燕教授指出，飞机场和高铁安装人脸识别设备或与反恐有关，一旦遭受恐怖袭击，危害性特别大。但与飞机场和高铁不同的是，地铁涉及到乘客的日常生活，并且客流量巨大。“如果识别出具体是谁在乘坐地铁的话，乘客的日常行踪轨迹很可能被追踪，收集人脸信息或超出了法律规定的必要原则。”“为什么一定要识别出来每一个乘坐地铁的人呢？”她认为，地铁安检的重点应该在于识别出有人带了危险用具会危及公共安全，而非识别出乘坐地铁的每一个人的具体身份[5]。实际上，根本没有必要将每一个人都识别出来，并且更夸张的是与个人信用相挂钩。一个人的个人信用有问题并不代表他就对公共安全存在威胁。由此，我们不难看出《个人信息保护法》中这种关于公共安全的个人条款其实缺乏边界，任何以公共安全为名的措施好像都能符合现有的法律，这一点值得我们深入思考。

2.3. 推广适用的潜在危险以及当前涉及人脸识别犯罪的主要场景

人脸识别技术的推广适用固然存在许多好处，适用上存在便利，有利于企业获得商业利益以及产业的发展，但其使用的风险远大于好处。首先，人工智能大数据时代人脸识别易使我们成为透明人，危险

[3]《个人信息保护法》第 26 条：在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

无处不在，人脸数据的安全可能会涉及到个人方方面面的隐私。其次，一旦人脸数据被泄露，将引发更多难以预料的风险。近年来黑市上兴起了人脸数据的买卖，通过一些大公司买入人们的人脸数据然后再售出用于非法用途，这些数据的泄出通常来自小区的物业、商场和相关平台等，泄露出去的数据一旦被非法滥用，将导致犯罪行为，其中包括利用他人人脸信息直接开设银行或者支付宝账户，用于贷款、境外赌博、洗钱等一系列犯罪活动，甚至还有犯罪分子直接嫁接他人人脸信息到淫秽视频中以进行非法牟利。广西更是有一例人脸犯罪案件直接通过利用他人人脸信息将被害人的房屋过户。此外，人脸识别技术的广泛运用还使得原先普通的电信诈骗转为精准诈骗。最后，人脸识别信息泄露具有相比于其他生物识别信息泄露更加难以救济的特点。不同于其他个人信息，电话号码、密码等个人信息一旦泄露可以通过更换、找回的方式予以弥补，而人脸识别信息一旦泄露将造成难以挽回的后果，打开的可能是潘多拉的魔盒。个人的隐私如果被无限地泄露，终有一天我们的社会将沦为英国思想家边沁所构想的“全景敞式监狱——监控型社会”。

3. 以人脸信息为代表的生物识别信息概述

3.1. 生物识别信息的特征及权利属性

3.1.1. 生物识别信息的定义

最新颁布的《民法典》《网络安全法》《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》中，个人生物识别信息这一名词均被多次提及，但也都是简要对其种类加以列举或者说明其属于个人信息的范畴。2020 年由国家标准化管理委员会发布的《信息安全技术个人信息安全规范》也只是对生物识别信息的种类做了列举，将“个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等”包括在内，但是这些法律法规均未对生物识别信息下定义或给予明确的概念界定[6]。简单地下定义，生物识别信息事实上就是指能够通过一定的生物识别技术进行分析所获得的个人信息。再根据 2021 年发布的《生物特征识别学科发展报告》中所定义的“生物识别”这一概念，我们可知生物识别是指通过智能机器获取和分析人体的生理和行为特征，进而实现身份鉴别(你是谁)、状态分析(姿态、喜怒哀乐)、属性估计(性别、年龄、人种)的科学技术[7]，由此我们就可以将生物识别信息详细界定为用于自动身份鉴别、状态分析、属性估计的人体生理和行为特征信息。从这些概念之间的种属关系看，形成了“人脸信息－生物识别信息－个人信息”的上位概念关系[8]。遗憾的是，我国的立法目前尚未形成对人脸信息以及生物识别信息体系化的保护模式。

3.1.2. 生物识别信息的主要特征

相比于其他个人信息，公民个人的生物识别信息具有如下的几个特征：首先，生物识别信息在性质上天然具有可识别性。以人脸识别信息为例，其能迅速准确地识别到特定的自然人，而电话号码、住址等个人信息若想直接锁定到特定的个人，可能还需结合人脸信息等其他生物识别信息才能进行身份认证，做到精准定位。此外，生物识别信息必须经过计算机算法的鉴定，而传统的个人信息并不需要经过此程序。其次，生物识别信息具有较强的稳定性。其一经形成便很难再去进行修改，例如人体的虹膜组织，虹膜从婴儿胚胎期的第 3 个月起开始发育，到第 8 个月主要纹理结构成形，在角膜的保护下，发育完全的虹膜很难受到外界的伤害，除非经历危及眼睛的外科手术，此后几乎终身不变[9]。生物识别信息也不同于账号密码、身份证号码等个人信息可以通过找回、重设等方式予以补救，其造成的损害往往是永久性的。最后，生物识别信息具有极易采集的特性。在人工智能技术如此发达的今天，很多时候个人完全意识不到自己的生物识别信息被无声采集。大多数人在互联网大数据平台上传自己的自拍或者照片时，不对相片做任何处理，无形中其实已经暴露了自己的人脸信息，导致个人信息的外泄。有很多不法分子

就通过这一方式将网络上他人的人脸照片嫁接到淫秽视频中或者通过换脸制作色情图片进行非法牟利，给他人的隐私权和名誉权造成了极大的影响甚至是不可挽回的后果。而电话号码、住址一类个人信息的获取则需要与他人进行交涉与接触，相较于此，人脸、指纹这一类生物识别信息的极易采撷性导致了其更容易受到侵害。

3.2. 生物识别信息属于刑法上的个人信息

纵观我国《刑法》，将侵犯公民个人信息罪规定在了“侵犯公民人身权利、民主权利”这一章中，说明其旨在保护的法益是公民的人身和财产安全，这也是刑法评价的核心所在[10]。以人脸信息为例，通过人脸所识别出来的信息代表着个人的喜怒哀乐，能够反映人的心情、代表人格尊严。人脸识别这一类生物识别信息不仅能影响人们的人身安全，更多时候是直接被当作密码来使用，直接与个人账户挂钩。大量司法实践证明，不法分子通过非法获取的人脸信息直接破解他人的财产账户，进行财产犯罪，其性质较普通的盗窃罪、诈骗罪更为恶劣。对此，生物识别信息作为个人信息的一种，能够单独识别特定的自然人，个人生物识别信息一旦被当作密码来使用，就更加容易造成公民的人生权利和财产权利受到侵害，进而引发相关人身和财产犯罪[10]，因此必须将生物识别信息作为个人信息安全法益纳入刑法保护范围，采取严厉的措施对其进行针对性保护。反观“张某、唐某、李某侵犯公民个人信息”一案[4]，法院判决唐某构成非法获取计算机信息系统数据罪而非侵犯公民个人信息罪，是有失偏颇的。非法获取计算机信息系统数据罪是利用信息网络所进行的犯罪，其侵犯的法益是计算机信息系统内的数据安全，旨在保护数据安全，而侵犯公民个人信息罪侧重于保护公民个人信息的内容，以及能够直接体现其内容本身的特定自然人[4]。因此只有将本案中唐某犯罪行为侵害的法益准确定性为公民个人信息安全法益而非计算机信息系统的数据安全，才能严厉制止不法，准确打击犯罪。

4. 对个人生物识别信息进行专项立法或完善刑法保护的必要性

刑法作为一部公法，是最严厉的部门法并且是法律的最后一道防线，因此当我们认定某一行为构成犯罪时，必须严格遵守罪刑法定原则，从该罪所要保护的法益出发，对其构成要件进行合理的、实质的解释。如今《个人信息保护法》的出台，从个人信息的收集、提供和利用角度做出了详细规定，一定程度上完善了公民个人信息保护领域的法律，而刑法作为第二次法，与《个人信息保护法》这一前置性法律所要保护的对象应当是统一的。如前文所述，个人生物识别信息是个人信息的下位概念，应当被纳入侵犯公民个人信息罪保护的法益范围，因此刑法不应当再去独立创设新的保护对象。对此，本文从目前《个人信息保护法》所保护的对象范围展开论述，来探讨当前对于公民个人生物识别信息适用刑法保护模式的必要性。

4.1. 保护的对象范围

目前出台的《个人信息保护法》对一般个人信息和敏感个人信息进行了分类，以人脸识别信息为例，当下，一种选择是是否应当将人脸信息这一类生物识别信息放入敏感个人信息的范围内进行规制，另一种就是进行专项立法。个人认为，第一种选择即将生物识别信息归入个人敏感信息进行保护是有问题的，因为根据《个人信息保护法》的规定，敏感个人信息与一般个人信息的区别主要就在于是否需要征得个人知情并同意，但我们很容易发现知情同意机制的不足之处，目前对于敏感信息的使用需要单独征求同意，或者超出使用范围时需要再次征求同意。实际上，个人信息中真正有价值的是二次使用，鉴于当今数据库中的数据都是千万级甚至上亿级的，如果企业改变数据用途需要重新征求用户的意见其实是不现实的。其次，对于个人来讲，如果主要还是依靠知情同意机制来保护个人信息的话，只要个人同意使用，

[4]成都市郫都区人民法院(2019)川 0124 刑初 610 号刑事判决书。

那么因为滥用所带来的风险，就必须由个人来承担。这就会面临一个问题，在整个个人信息大数据领域中，我们个人并不是最大的利益获得者，使用人脸信息所带来的风险并不是我们个人所创造的，而相应产生的风险却要由个人来承担，这对个人来说是十分不利的。法律应当把重点放在信息收集者与处理者的合规义务上。眼下还应当将对象范围从人脸信息扩大到生物识别信息上，除了对人脸的识别技术外，对指纹、虹膜、声音、步态、基因等的识别技术都如今都已经很发达了。基于此，立法应当具有一定的前瞻性。

4.2. 保护模式的选择：以刑法保护为主的公法保护模式

目前现有的《民法典》《网络安全法》《个人信息保护法》均已经详细对公民个人信息作出了许多规定，但生物识别信息始终未被明确列入我国私法体系的保护范围[11]，《刑法》也只是草草地将侵犯公民个人信息罪规定在了人身犯罪这一章中。眼下，将公民个人的生物识别信息纳入私法还是公法的保护范围，是一个值得斟酌的问题，本文认为应当以当前既有的刑事立法为具体思路，对个人生物识别信息予以针对性的保护。理由如下：

4.2.1. 当事人双方法律地位的不平等：难以对个体进行有效救济

如果仍以私法保护为主，以民法即调整平等主体之间的法律进行保护，难以对个体进行有效救济。这体现在法律条款的薄弱上，《个人信息保护法》第 69 条[5]采取了过错推定的保护模式，这对个人来说是十分有利的，也即数据处理者必须证明自己是合规的。但是除此之外，若个人想就此条进行赔偿，需要证明对方侵害了你的权益并且需要证明对方造成了你的损失，并且还需证明对方的侵权行为与所造成损失之间具有因果关系，这在民法以及民诉法上是非常困难的，此外在当今多头主体掌握个人信息的情况下，很难去证明到底是谁违规泄露了个人信息、造成了相应的风险并给个人造成了损害，更难去证明对方的侵权行为给你造成了损害和侵权行为和损害结果之间的因果关系，因此个体很难在诉讼中证明一系列侵权行为要件。实质上，这种侵权条款仍属于适用于平等主体之间的责任条款，而我们个人与平台、企业、国家等根本就不处于平等的地位，这类看起来平等的法律条款客观上其实根本不足以保护个人的信息权益。因此，仅以平等主体之间的私法去保护这类个人信息，是远远不够的。

4.2.2. 立法规制主体的多样化

其次从立法规制的主体类型来看，国内学界易受国外影响，目前国外针对政府部门和科技企业使用人脸识别技术的行为，前者倾向于有法律授权才能够进行使用，而后者往往倾向于通过市场来决定。但根据中国现实，凡是企业收集的个人信息，政府最后都能拿到，因此基于中国国情的考虑，如果不对政府和企业收集个人信息的行为分别处理，很容易使政府部门收集个人信息时绕过法律上的制约。且我们不难发现，如今一些企业对于个人信息的支配甚至超过了国家对个人的支配。如前所述，往往个人信息被滥用最后的风险都是由个人来承担，但事实上，谁在整个领域中获益最大，谁才应当承担最大的风险，在风险预防问题上，企业和政府也显然比个人更具有风险预防的能力。个人信息收集与使用主体的多样化决定了仅以私法对生物识别信息加以规制并不合理，因此对于人脸识别信息进行专属立法，完善刑法规制甚至产生新的公法是完全有必要的。

5. 现行刑法对生物识别信息保护存在的缺陷

从前，虽然侵犯公民个人信息的案件在我国时有多发，但基于科技发展的滞后性和时代的局限性，当时的生物识别技术还没有那么发达，被侵犯的个人信息仅限于电话号码、密码等常规信息，当时社会

[5]《个人信息保护法》第 69 条：在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

大众对于这种刚刚兴起的新型生物识别信息并不敏感，导致立法者甚至全社会都未给予生物识别信息应有的关注和重视。15 年左右，随着科技的迅猛发展和人工智能技术的广泛运用，指纹支付、人脸支付等新型支付手段兴起，生物识别信息的特殊性和重要性逐步为人们所认识。根据裁判文书网的数据，我国法院自 2017 年至 2019 年来审结的人脸犯罪案件数量呈现出递增的趋势。值得注意的是，生物识别信息除了人脸信息以外还涉及指纹、声纹、虹膜等生物识别信息，如果将这些涉及其他生物识别信息的案件都算在内，那么相关案件量则不容小觑，更何况还有很多法院未受理的案件或者未被纳入刑法规制的“犯罪黑数”[12]。目前，我国刑事立法对于生物识别信息的保护仍然处于较为不力的状态，上文中已经论述了生物识别信息不同于普通个人信息的主要特征，如果采取与普通个人信息相同的保护模式对其进行保护显然与其本身的特殊性不符，目前《刑法》保护模式存在的不足，具体表现为以下方面：

5.1. 侵犯公民信息罪中未对生物识别信息进行明确界定

我国《刑法》自颁布以来，经历了许多次修改，其中最早的 79 刑法和 97 刑法对公民个人信息犯罪未置一词，随着科技的快速发展，人们对隐私保护及个人信息安全越发重视。2009 年《刑法修正案(七)》的出台，标志着我国刑事立法迎来了关于公民个人信息保护的第一个转折点，在第 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”两个罪名。但是由于当时个人信息犯罪并不多发，严重侵犯个人信息的情况也并不常见，所以在当时没有特别给予个人生物识别信息特殊保护的必要[13]，立法者对此采取的是传统化的概括列举模式，仅列举了电话号码、家庭住址等常见的一些个人信息，对个人信息立法上采取的还是统一保护的模式。随后，2009 到 2015 年这短短的几年之间，公民个人信息犯罪案件频发，且其中犯罪的主体、客体、行为方式都发生了很大变化，因此，15 年立法者迅速出台的《刑法修正案(九)》对第 253 条做出了变化较大的修订。首先体现在罪名上，《刑法修正案(九)》将原先的“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”合并为一个新的罪名——“侵犯公民个人信息罪”，其次扩大了本罪的行为主体范围，根据《刑法修正案(七)》的规定，原罪规制的犯罪主体主要是金融、电信等单位工作人员，而针对普通个人非法出售、提供和获取他人个人信息的行为却未加以打击和规定，修改后的行为主体从原来的国家机关或者相关单位的工作人员扩大为年满 16 周岁的人，即一般行为主体[14]。这一改变突破了许多限制，实现了立法对于时代和社会变化的需要。不过此次修改只对《刑法修正案(七)》中个人信息的定义和种类进行了重复，生物识别信息这一概念尚未被列入其中。2017 年，基于司法实践的迫切需要，由最高人民法院、最高人民检察院联合制定的《关于办理侵犯公民个人信息刑事案件适用法律的若干问题的解释》(下文中简称《解释》)迅速出台，针对侵犯公民个人信息罪的构成要件、犯罪情节以及量刑标准等做出了具体解释，《解释》中还将个人信息分为了三类并设置了相应的入罪门槛，已经实现了很大的进步，其中入罪门槛最低的是高度敏感信息，与生物识别信息的关联性最强我国曾有很多学者建议将生物识别信息归入敏感信息进行规制，如前文中所述，本文认为还是欠妥，《解释》中也同样直将高度敏感信息限缩为行踪轨迹信息、通信内容、征信信息和财产信息四种，不允许司法适用中通过等外解释再予以扩大[15]，因而无法涵盖生物识别信息个人财产信息但遗憾的是该解释仍未对生物识别信息这一概念加以界定，也未对其种类加以列举。基于生物识别信息所具有的可识别性、稳定性和极易采集性，其一旦被泄露或者用于违法犯罪活动，对信息主体、甚至是社会和国家都会造成巨大威胁和不可挽回的损害。因此，对生物识别信息的保护水平相较于其他个人信息应当更高，立法应当予以明确规定。

5.2. 犯罪行为方式规定的欠缺

依据我国《刑法》规定，侵犯公民个人信息罪的主要行为方式为“非法获取、出售和提供”三种，

不同于刑法，“识别、存储、加工和使用”等行为方式也被纳入《民法典》和行政法律法规加以规制，这是因为在民法中，生物识别信息被作为一种人格权益来加以保护，上述识别、存储、加工和使用等方式实质上是对公民个人信息保护的一种全面考虑，全方位体现了对人格权益的尊重。但是对于生物识别信息生命周期中“获取、出售和提供”以外的其他环节，现有《刑法》的框架下并未予以规定，作为个人信息的一种，生物识别信息的生命周期包括收集、储存、使用、共享、转让、公开披露与删除等环节[10]，这些中间环节实质上都属于对外提供个人信息的行为，虽然《刑法》规定的获取、出售和提供三种行为方式内在包含了收集、使用、共享、转让和公开披露等环节，但是储存和删除这两个生命周期环节却不能被涵盖在内，对于企业和平台未按规定储存数据信息的非法储存行为，例如未对生物识别信息进行加密储存或者未与其他信息进行分类储存，所造成的违法后果，《刑法》未加以规定，在数据使用完毕后的删除环节，若存在非法删除或者非法泄露行为，又应当如何处理，对此《刑法》均未加以说明。相较之下，对于盗窃罪和诈骗罪，《刑法》对其种类与行为方式的规定就较为细致，由此可见，现行《刑法》对于侵犯公民个人信息罪的行为方式规定明显存在不足，有待进一步增设和细化。

5.3. 缺乏针对性的量刑标准

根据《刑法》第253条的规定可知[6]，“情节严重”和“情节特别严重”对于本罪的定罪量刑十分重要。对此，《解释》对“情节严重”和“特别严重”做出了详细说明，《解释》第5条实质上是对公民个人信息的种类做了简要分类并给予了相应的入罪标准，第5条第1款规定将个人信息分为三类且规定了入罪数量，第一类是行踪轨迹信息、通信内容、征信信息、财产信息50条以上，第二类是住宿信息、通信记录、健康生理信息、交易信息500条及以上，第三类是其他信息5000条以上[13]。由于《解释》已经对第一类、第二类信息的内容种类做了明确规定，因此生物识别信息就不能适用前两类的量刑标准，然而如果将其放入第三类“其他信息”加以规制，无形地又提高了侵犯生物识别信息的入罪门槛，如果将第二类中的“健康生理信息”扩大解释包含生物识别信息，将违反全国信息标准化委员会制定的《信息安全技术个人信息安全规范》，因为该规范已经明确将健康生理信息和生物识别信息划分为两种不同种类的信息[16]。可见，无论强行生物识别信息归为《解释》第5条中的哪一类进行解释，都会造成信息的不当分类或者量刑的失衡。

6. 完善个人生物识别信息刑法保护的路径

6.1. 明确个人信息的范围

如前所述，公民个人信息的种类实在纷繁复杂，不利于我们进行分类保护，然而生物识别信息不同于其他个人信息的重要性随着时代发展不断显现，它关系着每个自然人的身份特征与人格尊严，因此《刑法》必须对其加以保护和特别规定，当前《刑法》对于个人信息的保护主要体现在侵犯公民个人信息罪这一罪名的规定上，本文认为，应当尽快将生物识别信息纳入侵犯公民个人信息罪的个人信息法益保护范围。

6.2. 增设入罪的行为方式

上文中我们已经提到，针对侵犯公民个人信息罪，《刑法》虽然对“非法获取、出售和提供”三种行为方式做了规定，但是却忽略了生物识别信息生命周期中的“储存与删除”环节，非法储存、非法删除行为的社会危害性实际上不比非法获取和使用小[17]，它们同样能使犯罪分子实现对于个人信息的留存

[6]《刑法》第253条：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

和控制，甚至会导致更为严重的犯罪结果，对此，本文认为在未来的刑事立法中，可以考虑将“持有”这一行为方式与“获取、出售和提供”并列纳入侵犯公民个人信息罪的规制范围，因为“持有”这一环节能够将“储存、删除”等一系列生物识别生命周期中的环节包含在内，也可以考虑增设更多侵犯公民个人信息罪的行为方式，进而实现对个人信息非法留存行为的刑法规制。

6.3. 实质解释兜底条款

很多学者认为，对现有的《刑法》或《解释》中某些条款进行解释可能会违反罪行法定原则[18]，但是根据我国目前的司法实践状况，采用刑法解释的方法可能会更好更快地解决一些棘手的现实问题。首先，如前文所述，虽然无法将生物识别信息归入或者解释为《解释》第 5 条第 1 款第 3 项第 4 项规定的个人信息，但立法者也可能是基于时代的变化，考虑到了这一点，《解释》第 5 条第 1 款第 10 项规定了一项兜底条款——“其他严重的情形”，因此，我们不妨从此处入手，将“非法获取、出售或提供生物识别信息 5 条及以上”归入第 10 项中，作为侵犯个人信息的“其他严重的情形”。考虑到两方面，一方面，将侵犯生物识别信息的入罪标准设定为 5 条及以上，可以与第 3 项、第 4 项、第 5 项中的“50 条”、“500 条”、“5000 条”形成梯次[13]，使量刑规则规范化，体现出对不同种类个人信息不同的保护力度；另一方面，正因为生物识别信息对个人的重要性远远高于其他个人信息，因此将其归入兜底条款“其他严重的情形”反而更能加强对这类信息的保护力度。

其次，针对“情节特别严重”即法定刑升格的情形，《解释》第 5 条第 2 款第 3 项将“数量或者数额达到前款第 3 项至第 5 项规定标准十倍以上的”规定为情节特别严重的情形，但是由于我们在前文中已经得出生物识别信息不属于第 1 款第 3 项至第 5 项中个人信息的内容，因此无法推知“侵犯生物识别信息 50 条以上”为“情节特别严重”的情形，如果进行这样的类推解释，将违反罪刑法定原则。庆幸的是，第 2 款第 4 项仍然规定了兜底条款——“其他情节特别严重的情形”，因此我们同样可以依照上述解释方法，将“侵犯生物识别信息 50 条以上”解释为“其他情节特别严重的情形”，如此，“10 倍”恰好与上文中提到的“非法获取、出售或提供生物识别信息 5 条及以上”相对应，“其他情节严重”也恰好与“其他情节特别严重”相对应。总结起来，将“侵犯生物识别信息 5 条及以上”解释为“情节严重”，将“侵犯生物识别信息 50 条及以上”解释为“情节特别严重”，这样的实质解释方法既能在不违反罪刑法定原则的条件下对其他条款的适用不造成任何影响，又能降低侵犯生物识别信息的入罪门槛，实现对其针对性的特殊保护[19]。

7. 结语

当代社会，科学技术日新月异，个人信息种类越来越多，传播途径也越加广泛。并且随着人们法律意识的提高，生物识别信息这一新型个人信息的特殊性与重要性逐步体现。纵观我国立法，对于生物识别信息的保护情况不容乐观，特别是作为法律的最后一道防线，《刑法》也未将生物识别信息从个人信息中独立出来并给予特殊的定罪量刑标准，对此，我们可以考虑从刑法解释的角度为侵犯生物识别信息设定入罪标准与提出量刑建议，以期为我国司法实践提供有益借鉴，回应新时代的司法需求。

参考文献

[1] 赵鹏, 殷呈悦. 换脸软件 ZAO 被工信部约谈[N]. 北京日报, 2019-09-05(011).

[2] 郑玉双. 破解技术中立难题——法律与科技之关系的法理学再思[J]. 华东政法大学学报, 2018, 21(1): 85-97.

[3] 李爱君, 苏桂梅. 国际数据保护要览[M]. 北京: 法律出版社, 2018: 344.

[4] 王文娟. 生物特征识别信息失范性传播的刑事治理困境及其出路[J]. 科技与法律(中英文), 2021(5): 55-64.

[5] 华政法学. 劳东燕: 人脸识别技术运用中的法律隐忧[EB/OL].

https://mp.weixin.qq.com/s/RA7mFr9B4XhiTVQqw-PeQQ, 2020-12-09.

[6] 焦艳玲. 个人生物识别信息的界定[J]. 重庆大学学报(社会科学版), 2021(12): 1-13.

[7] 刘宪权, 陆一敏. 生物识别信息刑法保护的构建与完善[J]. 苏州大学学报(哲学社会科学版), 2022, 43(1): 60-71.

[8] 李振林. 非法取得或利用人脸识别信息行为刑法规制论[J]. 苏州大学学报(哲学社会科学版), 2022, 43(1): 72-83.

[9] 马永强. 侵犯公民个人信息罪的法益属性确证[J]. 环球法律评论, 2021, 43(2): 102-118.

[10] 张勇. 个人生物信息安全的法律保护——以人脸识别为例[J]. 社会科学文摘, 2021(8): 8-10.

[11] 黄陈辰. 无感抓拍行为的刑法规制研究——兼论设备生产者的刑事责任[J]. 天府新论, 2021(4): 127-135.

[12] 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, 28(5): 34-43.

[13] 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, 27(2): 133-143.

[14] 刘宪权, 何阳阳. 《个人信息保护法》视角下侵犯公民个人信息罪要件的调整[J]. 华南师范大学学报(社会科学版), 2022(1): 141-154+207-208.

[15] 喻海松. 最高人民法院、最高人民检察院侵犯公民个人信息罪司法解释理解与适用[M]. 北京: 中国法制出版社, 2018: 38.

[16] 杜嘉雯, 皮勇. 人工智能时代生物识别信息刑法保护的国际视野与中国立场——从“人脸识别技术”应用下滥用信息问题切入[J]. 河北法学, 2022, 40(1): 144-167.

[17] 刘伟东. 探究个人信息的刑法保护[J]. 法制博览, 2019(26): 227-228.

[18] 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.

[19] 欧阳本祺, 王兆利. 涉人脸识别行为刑法适用的边界[J]. 人民检察, 2021(13): 13-20.