Open Journal of Legal Science 法学, 2023, 11(1), 199-206
Published Online January 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.111028

Hans汉斯

人工智能时代下侵犯个人生物识别信息行为的刑事规制路径

谢倩倩

宁波大学法学院，浙江 宁波

收稿日期：2022年11月23日；录用日期：2022年12月5日；发布日期：2023年1月18日

摘 要

伴随着第三次人工智能浪潮的兴起，生物识别技术被广泛应用，与此同时，侵犯个人生物识别信息的行为时有存在，包括非法获取、提供、出售以及使用个人生物识别信息的行为，具有极大的社会危害性。由于民法、行政规制的不足，行为的社会危害性与特殊性，故有必要对侵犯个人生物识别信息行为进行特殊刑事规制，具体而言应将其纳入侵犯公民个人信息罪之中，明确该罪的犯罪对象，入罪标准以及行为方式，以达到对个人生物识别信息的特殊保护。

关键词

人工智能，个人生物识别信息，行为类型，刑事规制

Criminal Regulation of Personal Biometric Information Infringement in the Age of Artificial Intelligence

Qianqian Xie

School of Law, Ningbo University, Ningbo Zhejiang

Received: Nov. 23rd, 2022; accepted: Dec. 5th, 2022; published: Jan. 18th, 2023

Abstract

With the rise of the third wave of artificial intelligence, biometrics technology has been widely used. At the same time, the behavior of infringing personal biometrics information exists from time to time, including illegally obtaining, providing, selling and using personal biometrics infor-

文章引用: 谢倩倩. 人工智能时代下侵犯个人生物识别信息行为的刑事规制路径[J]. 法学, 2023, 11(1): 199-206.
DOI: 10.12677/ojls.2023.111028

mation, which has great social harm. Due to the inadequacy of civil law and administrative regulation, as well as the social harm and particularity of the behavior, it is necessary to carry out special criminal regulation on the behavior of infringing on personal biometric information. Specifically, it should be included in the crime of infringing on citizen's personal information, and the criminal object, criminalization standard and behavior mode of the crime should be defined, so as to achieve the special protection of personal biometric information.

Keywords

Artificial Intelligence, Personal Biometric Information, Type of Behavior, Criminal Regulation

1. 引言

伴随着第三次人工智能浪潮的兴起，以指纹验证、刷脸支付、声音解锁为代表的生物识别技术被广泛应用，并催生了大量的信息服务产业，成为数字经济的重要组成部分。然而，在生物识别信息被广泛应用的同时亦隐藏着诸多风险，可能会被用来获取个人隐私以实施犯罪；更有甚者，一旦个人生物识别信息被境内外不法分子利用，可能引发危害民族安全、国家安全的犯罪行为。2020 年 5 月颁布的《中华人民共和国民法典》首次明确将个人生物识别信息纳入个人信息的保护范畴，备受关注的《中华人民共和国个人信息保护法》也已于 2021 年 11 月 1 日起施行。种种举措无不彰显我国加强个人信息保护法治保障的决心和维护网络空间良好生态的宗旨，而生物识别信息的独特属性更加要求刑法保护不可缺位。然而，从现实情况来看，我国现行刑事立法对以人脸为代表的生物识别信息保护尚存在缺陷，忽略了该行为的独立危害性。故有必要对司法实践中侵犯个人生物识别信息行为的类型与特点进行探析，分析对此类行为进行特殊刑事规制的必要性，完善侵犯个人生物识别信息行为的刑事规制路径。

2. 人工智能时代下侵犯个人生物识别信息行为的类型

个人生物识别信息是指通过运用科学技术手段对人的身体特征进行数字化处理后得到的信息，如指纹、虹膜、面部特征、个人基因等。实践中，侵犯公民个人生物识别信息的行为类型主要包含以下五种：

2.1. 非法获取个人生物识别信息的行为

实践中常常会出现未经个人同意原始采集公民个人生物识别信息的行为，包括安装隐秘摄像头抓取人脸信息，或者通过拍照或其他高科技手段抓取指纹信息等等。例如 2021 年央视“3.15”晚会曝光上海科勒卫浴、宝马汽车、正通汽车等多家企业安装带有人脸识别功能的摄像头，偷偷抓取人脸数据并生成人脸 ID，用于了解顾客进入门店及次数。[1] 除了通过原始采集方式获取公民面部信息之外，行为人大量购买或窃取他人个人生物识别信息的行为也应当构成“非法获取”个人生物识别信息。首先，无论出卖人是否合法获取他人个人生物识别信息，其均无权提供或出售公民个人生物识别信息；其次，从知情同意权的角度来看，买受人系从生物识别信息持有人手中直接获取他人生物识别信息，这些信息主体完全无法行使其知情同意权，买受人也根本无法取得信息主体的同意；而窃取则更无法实现被害人的知情同意权。因此，大量买入或窃取公民生物识别信息的行为属于“非法获取”行为。

[1] https://www.sohu.com/a/455762639_116237.

2.2. 非法提供个人生物识别信息的行为

主要包括两种类型：一是向特定人提供公民个人生物识别信息；二是通过信息网络或者其他途径发布公民生物识别信息，即向不特定多数人提供公民生物识别信息。这里仅仅限定的是“提供”，而没有限定来源是否合法、提供行为本身是否合法。在判断时，需要依据前述“违反国家有关规定”来分析。如果没有违反国家有关规定，即合法的提供公民个人信息，则不具有非法性，不在刑法调整之列。比如，提供前征得了个人信息被收集者的同意，或者提供了个人的已进行匿名化处理、无法再识别特定个人且不能复原的信息。

2.3. 非法出售个人生物识别信息的行为

非法出售指大量卖出生物识别信息进行牟利的行为。这些行为并不以非法持有公民生物识别信息为前提，若生物信息持有者已经获得了被采集者的同意，但其并未将获取、处理敏感个人信息的真实目的告知被采集者或违反约定进行违法犯罪活动，或者合法持有公民面部信息的企业、单位为了牟利而出卖个人生物识别信息，这些行为均构成出售个人生物识别信息。[1]实践中存在大量倒卖人脸，指纹等个人生物识别信息的黑灰组织，为犯罪活动提供了帮助。

2.4. 非法使用个人生物识别信息的行为

在司法实践中，对生物识别信息的非法使用行为是指违反约定的采集用途非法使用自己已经掌握的公民个人人脸识别信息以期实现自己特定目的的行为，包括实施违法、犯罪活动等，如利用他人生物信息私自建立数据库提供识人或寻人服务进行牟利。在“净网 2020”行动中，警方在全国多地布局，抓获数名利用他人人脸识别信息提供刷脸服务、窃取被害人财物的犯罪嫌疑人。[2] 再比如住宅小区物业公司与业主约定，该面部信息采集仅用于门禁和安保用途。[3] 若物业公司将采集的业主面部识别信息与其所有房屋、车辆绑定，私自收集进入业主房屋、乘坐业主车辆人员的身份，整理业主关系网络用于经营，该行为对于公民的个人信息具有较大的危害，严重威胁公民个人信息安全。[2]

3. 对侵犯个人生物识别信息行为进行特殊刑事规制的必要性

3.1. 民事、行政规制的不足

对人脸识别信息的救济需遵循一般的民事及行政诉讼规则，这对于人脸识别信息的保护较为不利。在民事救济过程中，保障生物识别信息主要可通过侵权或合同之诉实现，其困境主要体现在两个方面：一是举证难度大，二是保护力度小。一方面，人工智能时代具有信息高度不对称的特点，网络运营方对个人信息进行处理的行为具有隐蔽性，信息所有者获取网络运营方侵权或违约的证据难度较大，调查成本高昂，超出一般民事主体的负担能，生物识别信息所有者需证明网络运营方的行为、过错、损害结果及因果关系才能证明网络运营方构成侵权，而各要件的证明难度都非常大。[3]另一方面，《民法典》第1167 条规定了停止侵害、排除妨碍、消除危险等侵权责任，惩罚力度较小。与此形成鲜明对比的是，网络运营方通过实施生物别信息侵害行为可获得巨额利润，在低成本高收益的情况下，民事途径对网络运营方的规制作用将十分有限。在行政救济过程中，政府面临着主体分工不明、政策引导无力、救济力度不足的困境。《个人信息保护法》中各信息保护主体没有进行明确的分工，仅表述为“有关部门”或“履行个人信息保护职责的部门”等。同时，行政处罚也面临着处罚力度较小的问题，网络安全法中设置的行政处罚措施主要有责令改正、警告、罚款、责令暂停相关业务、停业整顿、关闭网站、吊销相关业务

[2]https://www.163.com/dy/article/FIT0H9AD05129QAF.html.
[3]https://baijiahao.baidu.com/s?id=1705949984251177728&wfr=spider&for=pc.

许可证或者吊销营业执照等，《个人信息保护法》第七章也规定了个人信息处理者的法律责任，除了网络安全法中的措施还规定了记入信用档案并公示等处罚途径。但与人脸识别信息泄露带来的损害相比，行政处罚的力度依然较小，仅有行政救济起不到对网络运营方设置法律底线的作用，无法从根本上遏制人脸识别信息侵害行为激增的势头。

3.2. 行为的社会危害性和刑事违法性

个人生物识别信息被侵犯的风险非常高，并且侵犯行为具有严重的法益侵害性。侵犯个人生物识别信息会严重的侵犯公民的人身权利，财产权利以及危害国家安全。智能时代的特色并不在于对零散数据的简单汇聚，更核心的是对数据的挖掘与利用，针对生物识别信息而言，最大威胁并非来自生物识别技术所作的正面识别，而是第三方以可识别方式访问该数据并将其与其他信息连接起来，从而导致在未经数据主体同意的情况下对该信息进行二次使用，这无疑侵蚀了个人对其信息的控制权。以工业社会为基础构建的事后回应为主的传统刑法理论体系面对生物识别技术的侵害后果有一定的规范性措施，但却忽略了侵犯生物识别信息行为的独立危害性，个人信息的价值很大一部分都体现在二级用途上，随着信息技术的发展，去识别化与分析解读手段可挖掘个人信息的潜在价值。强化对侵犯生物识别信息行为的刑法规制是基于其所凸显的严重社会危害性，以及加强相关民事法律、行政法规与刑法条文之间协调的现实需要。根据犯罪的二次违法性理论，将违反前置法作为启用刑法的前提。一般是刑法违法性=一般的违法性+可罚的违法性，任何一个行为都受到刑事方面的处罚，都必须符合一般的违法性，然后是可罚的违法性。[4]因此，侵害个人生物识别信息的行为如果要受到刑事规制，首先得具有一般违法性。侵犯公民个人信息罪中将明确违反有关国家规定作为入罪的前置要件，而且《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》)中也对违反国家有关规定进行了解释，包含法律、行政法规、部门规章等。人脸识别第一案说明了侵犯公民个人信息的行为具有一般违法性。侵犯个人生物识别信息的行为同样也具有可罚的违法性。无行为则无犯罪。很明显，侵犯个人生物识别信息所造成的危害结果，已经具有了明显的可罚性。[5]侵犯个人生物识别信息的行为人在非法获取个人的生物识别信息之后，往往会用于从事后续的违法犯罪活动行为，造成严重的后果。很明显，这些行为已经触碰了刑法的边界。

3.3. 生物识别信息的特殊性

相较于其他个人信息，生物识别信息具有以下三个方面的特殊性，故有必要对其进行特殊规制。

第一，唯一性。每个人都是一个独立的生物体，对应一套独一无二的生物识别信息。以虹膜信息为例，虹膜图像存在许多随机分布的细节特征，而这些细节特征的形成主要取决于胚胎发育环境的随机因素。因此，即使是双胞胎、克隆人乃至同一个人的左右眼，虹膜图像之间也有显著差异，这也就决定了虹膜信息的唯一性。相较于其他个人信息，生物识别信息的唯一性为高精度的身份识别奠定了基础，因而得以在公共安检、商业支付、刑事侦查等领域广泛运用。

第二，不可更改性。以姓名、身份证号码、账号密码为代表的其他个人信息可以随时修改，但生物识别信息是个人的生理或行为特征，一旦形成便很难改变。例如，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。因此，生物识别信息一旦泄露就会给信息主体造成不可逆转的损害，而无法通过修改的方式加以弥补。

第三，易采集性。在生物识别技术迅速发展的今天，生物识别信息的采集往往不需要紧密接触，甚至可以做到，在信息主体毫不知情的情况下，采集其个人生物别信息。[6]无论是人脸、虹膜，还是笔迹、

步态或声纹等信息，都不可避免地在日常生活中展现出来。例如，在“晒自拍”的过程中对自己的照片不加处理，直接发布在社交媒体上，就极易被他人收集人脸信息。而只要拥有生物识别的智能装置，就能在信息主体毫无意识的情况下收集其生物识别信息。从这个角度而言，生物识别信息相较于其他个人信息更加容易受到侵害。

4. 关于侵犯个人生物识别信息行为的刑事规制路径完善

为改变非法经营罪兜底条款不断扩张的乱象，难以从立法角度入手，法律条文本身已经不是解决问题的核心。为应对此类司法适用中出现的问题，法教义学不失为一种很好的方法，通过对法律条文的限缩解释，为法律适用提供一个统一的标准，可以缓解目前非法经营罪不断扩张的乱象。

4.1. 刑事规制的路径选择

关于刑事规制路径，理论界主要存在两种观点：第一种观点，建议设置侵害个人生物识别信息的相关新罪名，打击非法使用和交易指纹、声纹、虹膜、DNA 等生物识别信息的违法犯罪行为。例如李怀胜教授主张修改现有的招摇撞骗罪以及设立身份盗窃罪的罪名。[7]蔡士林，王厅烁教授主张增设侵犯公民个人生物识别信息罪。第二种观点，建议完善侵犯个人信息罪，对一般个人信息与个人生物识别信息的保护进行区分处理。[1]关于侵犯公民个人生物识别信息的刑法规制路径选择问题，本文认为应完善侵犯个人信息罪，对一般个人信息与个人生物识别信息的保护进行区分处理。张明楷教授曾经指出，增设新罪名必须符合必要性、明确性、类型性、协调性的原则。[8]必要性原则是指如果按照现有的罪名能够进行规制，就没必要增设新罪名。类型性原则是指刑法的条文规定既不能够太抽象，也不可按照现实中的个别案件去进行描述，而是应当将构成要件描述为可以与具体案件相类比的类型。协调性原则是指增设的新罪必须与已有的罪名之间保持协调关系，不能够产生冲突，也要尽量避免罪刑不均衡的行为发生。明确性是对刑事立法提出的一个重要要求，是指刑事立法必须符合明确性的原则，不得随意对公民定罪。

本文认为修改现有的侵犯公民个人信息罪的罪名完全能够满足对个人生物识别信息的保护。主要理由如下：

第一，通过完善现有的罪名，能够满足个人生物识别信息刑事立法的规制要求，如果增设新罪，明显不符合必要性原则，而且我国的民事法律中也将个人生物识别信息归入了个人信息的范畴。因此，没必要设立单独的罪名。第二，对当前侵犯公民个人信息罪的罪名进行完善，完全可以满足对个人生物识别信息的保护，并且罪名的设置也符合刑法的明确性原则，对侵犯个人生物识别信息的行为也能够进行全面的规制。第三，对现有的侵犯公民个人信息罪的罪名进行完善，也完全能够容纳现实中侵犯个人生物识别信息的行为，符合刑法罪名设置的类型性原则。第四，通过完善罪名，使得条文之间能够保持协调一致的原则，再者如果单独设立罪名，立法成本太高，会极大的浪费司法资源。综上所述，对于侵犯公民个人生物识别信息行为的罪名设置，完全可以通过对侵犯公民个人信息罪罪名进行修改的方式，来对其进行刑事规制。

4.2. 扩展侵犯公民个人信息罪的犯罪对象

《最高人民法院、最高人民检察院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》第二百五十三条之一规定的“公民个人信息”，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身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。从上述规定可以看出司法解释对公民个人信息的认定采取了概括加列举的方式，“等”字在兜底的同时也导致公民个人信息的范围不明。而要明确

生物识别信息是否属于公民个人信息，将其纳入侵犯公民个人信息罪的范围之中，首先需要明确公民个人信息的认定标准。

关于公民个人信息的认定标准，理论界存在识别不要说和识别必要说，识别必要说又分为双标准说和多标准说。识别不要说即认为可识别性不是公民个人信息的必要判断标准，不应以身份识别为主要判断标准，而应以对人格权和财产权的实质危害为判断标准，方能实现对个人信息的有效保护和利用。识别必要说即认为可识别性是公民个人信息的必要判断标准，除此之外还应该有其他辅助标准，例如“关联性”“隐私性”“记录性”等等。

在侵犯公民个人信息罪中，本罪法益的确定，也会导致公民个人信息的保护方向的不同。因此，在研究有关公民个人信息保护等方面的问题时，应先明确本罪的法益属性。笔者认为，本罪所要保护的法益个人信息的自决与安全。首先，本罪保护法益的根本性质为个人法益，并非超个人法益，侵犯公民个人信息罪位于侵犯公民人身权利、民主权利罪该章节，本章保护的主要客体为公民人身权利等价值，本罪被纳入本章，说明本罪的主要法益为个人法益。其次，于个人法益立场之下，公民个人信息兼具多重权利属性，若将本罪保护法益内容定位为隐私权抑或财产权等，皆存在权利属性单一、周延性阙如等问题，难以全面有效保护公民个人信息。在大数据时代的背景之下，新型个人法益的信息自决与安全可以兼顾公民个人信息全面保护与信息资源流通利用的现实需求，基于此，本文认同本罪保护法益的实质内容其实为信息自决与安全。“个人信息自决”是指个人信息权人得以直接控制与支配其个人信息，并决定其个人信息是否被收集、处理与利用以及以何种方式、目的、范围收集、处理与利用。“个人信息安全”是指公民个人的姓名、住址、电话、指纹等身份信息不被违法使用而附带保障的人身、财产安全。个人信息本身对他人可能具有商业价值，但对个人而言，则只是身份属性的一部分，其背后关联的人身、财产安全才是个人信息安全评价的核心，才是值得受刑法保护的且可能被侵害的有价值的真实事物，这也是法益保护之真实性、价值性的体现。

故公民个人信息的认定标准包括“可识别性”“安全价值性”以及“自诀性”。首先，生物识别信息具有唯一性，不像姓名、住址等可能同时很多人拥有，通过指纹、人脸、声音等都迅速对应到具体的个人，具有直接可识别性；其次，生物识别信息背后附带着不被违法使用而附带保障的人身、财产安全，保护生物识别信息不被侵犯即是在保护其背后的人身、财产安全，具有安全价值性；最后，个人信息权享有直接控制与支配其个人生物识别信息，并决定其个人生物识别信息是否被收集、处理与利用以及以何种方式、目的、范围收集、处理与利用的权利。综上所述，个人生物识别信息满足公民个人信息的认定标准，故应纳入侵犯公民个人信息罪中公民个人信息的范畴。

4.3. 设置侵犯公民个人生物识别信息行为的入罪标准

《最高人民法院、最高人民检察院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》第五条规定，非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为《中华人民共和国刑法》第二百五十三条之一规定的“情节严重”：(三) 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的；(四) 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五百条以上的；(五) 非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的。

从上面的规定可以看出，司法解释将公民个人信息分为 3 类，分别是行踪轨迹信息、通信内容、征信信息、财产信息(第一类信息)；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、财产安全的个人信息(第二类信息)；以及上述两类信息之外的个人信息(第三类信息)。对于不同的信息规定了不同的定罪量刑标准。但笔者认为上述分类存在两大问题：第一，缺乏明确的分类标准。第二，有

的分类方式会导致信息类型的交叉重合，例如作为重要信息的交易信息和作为敏感信息的财产信息的界限并不那么清晰。

故有必要对该分类进行调整。根据法益危害程度和法益侵害可能性将公民个人信息分为高度敏感个人信息，相对敏感个人信息以及一般公民个人信息。其中法益危害程度按照生命健康、人格尊严、大额财产、小额财产递减，法益侵害可能性分为大，中，小三级。危害生命健康或者人格尊严 + 法益侵害可能性大即为高度敏感个人信息，50 条入罪；危害小额财产+法益侵害可能性小即为一般个人信息，500 条入罪；其他的属于敏感个人信息，5000 条入罪。

笔者认为个人生物识别信息应当属于高度敏感个人信息，即侵犯了人格尊严，并且法益侵害可能性极大，因此应当在入罪的数量方面低于其它个人信息，即 50 条即入罪，以实现对于生物识别信息的特殊保护。具体理由如下：第一，对于生物识别信息而言，由于它具有唯一性和可识别性，一旦泄露，会造成难以挽回的后果。因此应当在入罪的数量方面应低于其它个人信息。第二，将侵犯个人生物识别信息的入罪标准低于其它的个人信息，能够更好地实现刑法的梯次保护，按照个人信息的重要程度和被侵犯之后的危害程度对个人信息进行保护，完全能够满足当前紧迫的司法现实对侵犯个人生物识别信息打击的要求。第三，将侵犯个人生物识别信息的行为在入罪的标准方面低于一般的个人信息，也是贯彻罪责刑相适应原则的体现，罪责刑相适应要求对于犯罪分子所判的刑罚与罪刑轻重相适应。侵犯个人生物识别信息的行为既然危害性大于侵犯一般的个人信息，那么在入罪标准方面低于其它的个人信息也是理所应当的。

4.4. 扩展侵犯公民个人信息罪的行为方式

目前刑法只规制非法获取、出售、提供的行为，规制范围较小，可以通过增加刑法规制的行为种类实现对生物识别信息的全方位保护。侵犯公民个人生物识别信息行为的构成要件中已经对非法获取和非法提供的行为类型做出了规定，实践中，针对侵犯个人生物识别信息的行为类型还有非法利用的行为。对于将非法获取、非法提供规定为侵犯个人生物识别信息的行为类型并没有什么争议，因为我国侵犯公民个人信息罪的犯罪行为类型已经列明，但是对于是否要将非法利用个人生物识别信息行为列入犯罪行为类型，学界存在争议。主要有以下两种观点：第一种观点认为不用单独列明非法利用公民个人生物识别信息行为，将非法利用行为解释进非法提供、出售的行为方式里面即可。其理由是非法利用行为与非法出售、提供的内涵并无本质区别，将其解释到非法提供、获取中去完全可以满足对于非法利用个人生物识别信息的保护要求。第二种观点主张单独对非法利用行为进行规制，可以在侵犯公民个人生物识别信息行为的构成要件中规定“非法利用”的行为方式，与非法获取、提供公民个人信息的行为一并构成一款。其理由有二。[9]第一，非法利用公民个人生物识别信息的行为具有明显的独立性，非法获取、非法提供行为的概念均无法涵盖，三者的内涵明显不一致。第二，非法利用行为产生的危险性明显高于非法提供和非法获取的行为，非法利用行为是对个人生物识别信息的二次侵害，行为人受损害的不仅仅是个人的生物识别信息，而且还会引发人身、财产权利方面的犯罪。

笔者同意第二种观点，在侵犯公民个人信息罪的犯罪构成要件中，应当将非法利用行为单列出来，以弥补侵犯公民个人信息罪在对非法利用个人信息的行为方式保护的不足。其理由如下：

第一，而非法利用的主体既包括有权取得公民个人生物识别信息的单位，也包括无权取得公民个人生物识别信息的单位，而非法获取的主体仅为无权取得公民个人生物识别信息的自然人和单位，二者的内涵明显不一致，因此需要单独进行规制。[10]第二，非法利用行为造成的法益侵害性远远高于非法提供和非法获取的行为，按照举轻以明重的原则，将其纳入刑事规制的范围完全合理。并且现实中已经出现大量非法利用个人生物识别信息的行为，对其单独做出规定，也能够进行有效的打击此类行为，做到罪

刑法定，符合刑法立法的明确性原则。第三，非法利用行为虽然能够用其它罪名来进行处罚，但由于侵害法益的不同，用其它罪名进行评价往往会造成法益保护的不够周延。比如行为人利用他人的人脸识别信息制作淫秽物品并传播，往往会被处以传播淫秽物品罪或者是侮辱罪，但是对于侵犯个人生物识别信息的行为并不能很好地保护，因此，将非法利用他人生物识别信息的行为进行规制，也可以实现刑法对该行为的全面保护。最后，在增加非法利用个人生物识别信息的行为方式，这样，既可以使得刑法的规制更加周延，也能够对侵犯个人生物识别信息的行为提供更加全面的保护。

具体而言，笔者建议，在《刑法》第 253 条之一侵犯公民个人信息罪的规定中增加非法利用公民个人信息的行为方式，以实现对非法利用包括生物识别信息在内的个人信息的刑法保护。

5. 结束语

关于个人生物识别信息的刑事规制路径，完全可以通过对侵犯公民个人信息罪罪名进行修改的方式，来对其进行入罪。在侵犯公民个人信息罪中，本罪法益的确定，也会导致公民个人信息的保护方向的不同，本罪所要保护的法益个人信息的自决与安全，故公民个人信息的认定标准包括“可识别性”“安全价值性”以及“自诀性”。个人生物识别信息满足公民个人信息的认定标准，故应纳入侵犯公民个人信息罪中公民个人信息的范畴。侵犯个人生物识别信息即侵犯了人格尊严，并且法益侵害可能性极大，应当属于高度敏感个人信息，50 条即入罪，以实现对于生物识别信息的特殊保护。实践中，针对侵犯个人生物识别信息的行为类型还有非法利用的行为，故刑法应将非法利用公民个人生物识别信息的行为纳入规制范围。

参考文献

[1] 任和和. 论我国人脸识别信息侵害行为的刑法规制[J]. 上海法学研究, 2021(1): 269-276.

[2] 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(1): 72-83.

[3] 郑妤婕. 人脸识别信息的法律属性与刑法保护[J]. 北京警察学院学报, 2021(6): 13-18.

[4] 贺刚飞, 王利苹. 个人生物识别信息刑事保护探索[J]. 中国检察官, 2021(23): 38-41.

[5] 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.

[6] 李明鲁. 深度伪造技术滥用行为的刑法治理路径[J]. 法治社会, 2021(6): 92-101.

[7] 李怀胜. 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[J]. 政法论坛, 2020(4): 144-154.

[8] 赵小涵. 滥用人工智能深度伪造技术的刑法评价进路[J]. 宿州教育学院学报, 2021, 24(4): 15-18.

[9] 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(1): 60-71.

[10] 刘方可. 论人脸识别信息的三个基础性问题——兼论侵犯公民个人信息罪行为方式补充[J]. 前沿, 2021(4): 85-90.