非法取得或利用人脸识别信息行为刑法规制论

李振林[1]

(华东政法大学 刑事法学院，上海 201620)

【摘 要】：人脸识别信息具备识别特定自然人身份的属性，应属于《刑法》第253条之一规定中的“公民个人信息”。对于非法取得或利用人脸识别信息行为，现行刑法主要存在以下规制困境：一是尚未明确对非法获取、出售或者提供人脸识别信息的行为进行规制；二是尚未对非法存储、使用、加工人脸识别信息等可罚性较高的行为进行规制。人脸识别信息实际上可以归为《解释》所规定的“其他可能影响人身、财产安全的公民个人信息”。对于非法获取、出售或者提供人脸识别信息行为，应通过进一步明确相关司法解释的规定进而将其认定为侵犯公民个人信息罪。对于合法获取公民人脸识别信息后非法存储的行为，可认定为不作为的非法获取人脸识别信息行为，继而以侵犯公民个人信息罪定罪处罚。对于非法使用、加工人脸识别信息的行为，可通过扩大解释侵犯公民个人信息罪中“非法”的范畴甚或增设非法利用公民个人重要信息罪加以规制。

【关键词】：人脸识别 侵犯公民个人信息罪 个人信息 生物识别

【中图分类号】:D924**【文献标识码】**:A**【文章编号】**:1001-4403(2022)01-0072-12

一、问题的提出

人脸识别技术是利用计算机来识别人脸图像，进而从中提取出有效的识别信息，用来辨认身份的一门技术。[1]在人工智能时代，计算机科学的飞速发展使得以人脸识别技术为代表的生物识别技术愈发成熟。进入家门不再需要携带钥匙，仅需“刷脸”即可完成身份认证;线下支付无须打开手机，“眨眨眼”便可迅速完成支付;公安机关也无须用肉眼一一比对犯罪嫌疑人信息，利用在全国范围内建立的逃犯追踪识别系统“天网”便可迅速锁定逃犯。人脸识别技术的发展极大便利了民众生产生活，迅速提升了社会的运行管理效率。但同时我们也应当看到，“越轨”后的人脸识别技术已为社会生活带来了诸多困扰，甚至为侵犯人身、财产犯罪的滋生提供了土壤。作为敏感信息的人脸识别信息，与一般公民个人信息相比，具有唯一性、不可更改性等特征。因此，一旦其被非法取得或利用于违法犯罪，其危害将难以补救甚至可能永久持续。从因民事纠纷而引发的“人脸识别第一案”——“郭兵诉杭州野生动物世界有限公司案”[2]，再到利用人脸识别技术实施犯罪的“四川省破解某宝系统案”[3]，“上海用‘活照片’破解人脸识别注册皮包公司虚开发票案”[4]等，无不反映着人脸识别技术发展背景下公民人脸识别信息被非法取得或利用的隐忧。实际上，目前利用人脸识别技术破解人脸识别验证的黑色犯罪产业链已相当齐全。购买一套包含身份证正反面照片、手持身份证照片点头、摇头、张嘴的视频仅需10元，而上述信息可以完成大多数App平台的验证流程。而且，这类交易通过QQ群及境外网站即可完成，由此可轻松购买数以万计的人脸识别信息。卖家可通过借贷软件、“走路赚钱”、网络兼职等形式获取用户信息，成本仅需一部手机及一套软件，并且可无限重复使用。[5]由此导致当前非法获取、提供、破解人脸识别数据及关联的电信网络诈骗、非法发放及催收贷款等违法犯罪案件层出不穷。通过刑法规制非法取得或利用人脸识别信息行为的必要性与紧迫性由此也愈发凸显。

[1]**作者简介**：李振林，华东政法大学刑事法学院副教授，主要从事刑法学研究。
基金项目：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);华东政法大学科学研究项目(项目编号：20HZK006)的阶段性成果

《个人信息保护法》的出台，可谓对包括人脸识别信息在内的公民个人信息进行了全面升级的保护，也为应对上述日益频发、应接不暇的非法取得或利用人脸识别信息行为的防治注入了一股强心剂。此外，《民法典》对公民人脸识别信息的保护作用也不可低估。但刑法也一定不能缺位，尤其是对社会危害性不断凸显的非法取得或利用人脸识别信息行为的规制，很大程度上需要依靠《个人信息保护法》等其他法律的保障法即刑法。然而，从现实情况来看，刑法对非法取得或利用人脸识别信息行为的规制似乎有捉襟见肘、力有不逮之感，相关司法实践也似乎呈现出无所适从、不知所措之象。主要表现为:目前对人脸识别信息的刑法属性尚缺乏准确的界定与认识，对于非法获取、出售或者提供人脸识别信息行为是否构成侵犯公民个人信息罪尚不明确，对于时下愈演愈烈且社会危害性愈发凸显的非法存储、使用、加工人脸识别信息行为无法以侵犯公民个人信息罪进行规制等。这些均是刑法规制非法取得或利用人脸识别信息行为过程中亟需解决的关键问题。

二、人脸识别信息的法律属性界定

人脸识别信息的法律属性是人脸识别相关法律问题适用法律规则的连接点，更是构建非法取得或利用人脸识别信息行为刑法规制体系的出发点。然而，在我国当前的法律规则体系中，人脸识别信息的法律属性尚未被真正界定，或者说界定并不统一。无论是日常生活中市民的认知，抑或是《个人信息保护法》《民法典》《网络安全法》等法律规范，均将人脸识别信息界定为公民个人信息。而“人们在解释具体犯罪的构成要件时，又习惯于将自己熟悉的事实视为应当的事实，进而认为刑法规范所描述的事实就是自己熟悉的事实”[6]。因此，在刑法尚未对人脸识别信息的属性进行明确界定前，能否直接照搬前述的属性界定，已成为是否可以以《刑法》第 253 条之一规定的侵犯公民个人信息罪对非法取得或利用人脸识别信息行为进行规制的前提问题。

(一)刑法与他法对人脸识别信息属性界定之差异

日常生活中，人脸识别信息是重要的个人信息。在熟人社会中，“每个孩子都是在人家眼中看着长大的，在孩子眼里周围的人也是从小就看惯的”[7]。因此，对方的姓名、住址可能不得而知，但一看脸就能识别出对方的身份。而在陌生人社会中，即使能够获取姓名、住址等信息，往往也需结合人脸才能识别到特定的人。[8]因此，人脸识别信息附有与个人身份相伴随的一系列标签和属性，相较于姓名、身份证件号码、通信通讯联系地址，人脸具备更强的可识别性。那么，从规范的角度来看，人脸识别信息是否属于公民个人信息呢?目前有关人脸识别信息的规范主要包括《个人信息保护法》《民法典》《网络安全法》《信息安全技术个人信息安全规范》等。其中，《个人信息保护法》第 28 条第 1 款将人脸识别信息(生物识别信息)作为敏感个人信息加以规定。《民法典》第 1034 条第 2 款与《网络安全法》第 76 条第 1 款第 5 项则通过列举的方式将人脸识别信息(生物识别信息)明确规定为个人信息。国家市场监督管理总局、国家标准化管理委员会 2020 年 3 月 6 日发布的《信息安全技术个人信息安全规范》第 3.1 条注 1 也明确规定了人脸识别信息(生物识别信息)属于个人信息。

由此可见，《个人信息保护法》《民法典》《网络安全法》《信息安全技术个人信息安全规范》等民事、行政法律法规及行业规范均将人脸识别信息明确纳入了公民个人信息的范畴。但既有的刑法条文以及相关司法解释对人脸识别信息的规定却模棱两可。《刑法》第 253 条之一规定了侵犯公民个人信息罪用于规制非法获取、出售或者提供公民个人信息的行为。然而，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》(以下简称《解释》)第 1 条将侵犯公民个人信息罪中的“公民个人信息”解释为:“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。”显然，人脸识别信息并未在列。

在刑事立法以及《解释》均未明确将人脸识别信息纳入公民个人信息范畴的情形下，如何界定人脸识别信息的刑法属性，便成为规制非法取得或利用人脸识别信息行为的基础与前提。

(二)人脸识别信息应属于侵犯公民个人信息罪中的“公民个人信息”

关于侵犯公民个人信息罪中的“公民个人信息”是否需与其他法律规范保持一致，学界主要存在“一致说”和“差别说”两种观点。“一致说”认为，公民个人信息作为法律共同保护的对象，无论是刑法还是民法、行政法等其他法律规范，各种法律保护的信息类型范围应当是一致的。只是各种规范根据公民个人信息所被侵犯的严重程度而采取了不同的规制手段，其中只有达到刑法所规定的“情节严重”的程度，刑法才予以规制。[9]另外，法秩序的统一性要求各个法律部门之间就某一概念不得作出不尽相同，甚至对立、冲突的解释。[10]因此，侵犯公民个人信息罪中的“公民个人信息”在范围上应与《民法典》等规范中的“公民个人信息”保持一致。“差别说”则认为，由于刑法与其他法律规范在规制手段的严厉性上存在悬殊差异，故而二者对公民个人信息的保护范围也当有所区别。因此，侵犯公民个人信息罪中“公民个人信息”的概念不能完全照搬其他法律规范的界定。[11]

笔者认为“差别说”较为合理，理由在于刑法与《个人信息保护法》《民法典》《网络安全法》等规范的保护目的并非完全相同。由于民事性法律规范以形成意思自治、契约自由的社会秩序为目的，因此其规制手段为确定行为主体、行为方式以及行为结果，从而调整民事权利与义务关系。而刑法更注重的是对已达到一定社会危害性的行为的惩治。[12]例如，《网络安全法》第 1 条规定:“为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。”据此，《网络安全法》主要是从网络信息安全的角度对个人信息作出规定，而《刑法》第 253 条之一的主要目的在于惩治严重侵害公民个人信息安全和相关合法权益的行为，二者的规范保护目的不完全一致。[13]规范保护目的的差异，为刑法单独划定公民个人信息的范围提供了合理性基础。

然而，“差别说”内部还存在“扩大说”与“缩小说”两种观点。“扩大说”认为，刑法中的个人信息内涵大于其他法律中的个人信息的内涵。[14]“缩小说”认为，由于刑法的构成要件设计上存在缩小处罚范围的政策考虑，也由于刑法主要在与公民人身、财产权利相关联的意义上把握个人信息，因此侵犯公民个人信息罪中个人信息的范围要小于《民法典》等其他法律规范所划定的范围。[15]笔者认为，上述两种学说对于人脸识别信息是否属于公民个人信息的判断似乎更进一步，但由于扩张与限缩的程度并不明确，因此在具体判断中难以起到实质效果。欲解决这一问题，应当遵循实质判断的标准，即遵循《解释》第 1 条规定的“识别特定自然人身份或者反映特定自然人活动情况”这一标准。只有当人脸识别信息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时，才能将其纳入侵犯公民个人信息罪中“公民个人信息”的范畴。而这便需对人脸识别技术的运作流程进行解构。

人脸识别技术的具体运作流程包括:人脸检测→人脸图像预处理→人脸特征选择→分类判别→人脸识别→输出结果，其又可简化为:人脸检测、人脸特征提取和人脸识别三个环节。其中，人脸检测环节是在所给定的任意静态的人脸图像或者动态的人脸视频之中，通过特定的方法对其进行检索，判定其中是否包含人脸信息。人脸特征提取环节是选择提取人脸的特征，将现实空间的图像映射到机器空间的过程。因此，前两个环节本质上属于人脸信息的获取，即检测到图像或视频中的人脸之后进行定位和识别，并选择提取人脸的特征。最后的人脸识别环节则是将待识别的人脸与已知人脸进行比对，在特征空间中用分类方法将被识别对象归为某一类的过程。[16]通过上述解构可以看出，人脸识别强调的是人脸之间的个体差异，并利用该差异判断所要识别的人脸图像是否属于某个特定的个体。[17]其方式在于结合人脸数据库用于验证和鉴别场景中单个或者多个人的身份，从而关联到特定的公民个人，并按图索骥识别到本人。这无疑满足了《解释》第 1 条规定的“识别特定自然人身份”的要求。因此，从实质判断的角度来看，人脸识别信息应当属于侵犯公民个人信息罪中的“公民个人信息”。

三、非法取得或利用人脸识别信息行为的刑法规制困境

虽然我们可以通过刑法解释将人脸识别信息认定为侵犯公民个人信息罪中的“公民个人信息”，进而可以通过侵犯公民个人信息罪来规制向他人出售或者提供公民人脸识别信息，以及窃取或者以其他方法非法获取公民人脸识别信息等行为。但面对非法取得或利用人脸识别信息这样一个新概念、新问题和新现象，在经济发展的复杂社会与重视人权的法治时代，我们不可能直接根据正义理念或法律属性即将其认定为犯罪;否则，“尤像 18 世纪自然法所展示的，结果走入法的不确定性和任意性”[18]。实际上，在对非法取得或利用人脸识别信息这一具有鲜明时代特征的新现象、新行为进行规制时，现行刑法已呈现捉襟见肘之象，以致司法实践呈现无所适从之感。

(一)尚未明确对非法获取、出售或者提供人脸识别信息的行为进行规制

首先，人脸识别信息未被明确规定为侵犯公民个人信息罪中的个人信息。无论是《个人信息保护法》《民法典》抑或《网络安全法》，在规定公民个人信息或敏感个人信息的含义时，均将人脸识别信息予以明确列举。基于法秩序的统一性，且为避免适用《刑法》第253条之一规定时出现司法不准确、不统一的问题，较为稳妥的做法自然是在刑法中将人脸识别信息作为与姓名、身份证件号码等信息并列的公民个人信息予以规定。然而，关于公民个人信息的概念，《解释》第1条虽采取定性加列举的方式对其予以了明确，但在其列举的公民个人信息的类型中，却并未将人脸识别信息纳入其中。《解释》第1条将重要性明显弱于人脸识别信息的姓名、身份证件号码等信息均明确列举为个人信息的类型，却没有列举对公民人身、财产权益影响更为深远、更为重要的人脸识别信息，其合理性也值得怀疑。

其次，即使可以运用解释学的方法将人脸识别信息纳入公民个人信息的范畴，但在具体司法适用中也难以把握“情节严重”的标准。上文笔者从实质判断的角度对人脸识别信息属于侵犯公民个人信息罪中的“公民个人信息”予以论证。但《解释》第5条在列举“情节严重”的情形时，并未将侵犯人脸识别信息的行为予以列举，如此也就难以判断非法获取、出售或者提供人脸识别信息行为的入罪标准。在“对于现代型犯罪构成要件加以描述时，立法者在不得已而采用兜底式规定的同时，必须有意识地将其和明示列举相结合，并尽可能详细、充分地列举已经认识到的常见的相应犯罪类型”[19]。非法获取、出售或者提供人脸识别信息的行为已然属于侵犯公民个人信息罪中的常见类型，因此《解释》第5条第1款也应明确该类行为“情节严重”的标准。然而，《解释》第5条第1款并未予以明确，这势必会导致对非法获取、出售或者提供人脸识别信息行为的刑法规制陷入困境。

(二)尚无法对非法存储、使用、加工人脸识别信息的行为进行刑事规制

首先，从司法实践来看，非法存储、使用、加工人脸识别信息的行为已呈现出愈演愈烈之象。非法存储、使用、加工人脸识别信息是指未经信息主体许可，非法存储、使用、加工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。如果司法实践中出现通过合法手段获取他人人脸识别信息后再非法存储、使用、加工等情形，现行刑法势必难以应对。例如，2019年，一款名为“ZAO”的换脸软件风靡网络，用户仅需上传自己的一张正面清晰照片即可合成换脸为某位明星，甚至可以合成自己老年时的模样。依据“ZAO”的用户协议相关条款，用户一旦上传自己的照片进行视频“换脸”，将在全球范围内完全免费、不可撤销地将包括人脸照片在内的肖像资料授权给该公司和其关联公司。如若认为“ZAO”软件用户协议相关条款合法，那么对于其合法获取人脸识别信息后非法存储、使用、加工的行为，司法机关便难以通过刑事手段加以规制。再如，社会生活中已经出现了大量非法存储、使用公民个人人脸识别信息的行为。例如，某市市民李某想在某App上注册账号，却发现怎么也注册不成功。李某确定自己是第一次使用该平台，但页面却显示自己的身份已经被实名注册了。而此App注册需要填写姓名、身份证号以及进行人脸识别。[20]诸如此类非法存储、使用公民个人人脸识别信息的行为，现行刑法似乎也无法进行规制。

其次，从人脸识别信息犯罪的整体链条来看，刑法对人脸识别信息犯罪部分环节的规制存在缺失。人脸识别信息犯罪链的上游是非法获取行为，中游是非法出售、提供、加工、存储行为，下游则是非法使用行为。然而，根据《刑法》第253条之一的规定，侵犯公民个人信息罪的行为方式仅有非法获取、出售、提供三种。因此，对于在人脸识别信息犯罪链中下游高发的非法存储、使用、加工人脸识别信息的行为，现行刑法便无法规制了。

最后，从刑法与其他规范的规定来看，二者的衔接不甚流畅。《个人信息保护法》第4条第2款规定:“个人信息的处理行为包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。”由此可见，侵犯公民人脸识别信息的行为类型不仅包括收集[21]、传输、提供、公开行为[22]，还包括存储、使用、加工等行为。同时，《个人信息保护法》第10条规定:“任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息;不得从事危害国家安全、公共利益的个人信息处理活动。”第71条规定:“……构成犯罪的，依法追究刑事责任。”《网络安全法》第41条第2款规定:“网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。”第74条规定:“……构成犯罪的，依法追究刑事责任。”

由此可见，对于《个人信息保护法》第 4 条第 2 款、第 10 条以及《网络安全法》第 41 条第 2 款规定的非法存储、使用、加工人脸识别信息的行为，现行刑法中并无相应罪名可以进行规制，刑法与《个人信息保护法》《网络安全法》的衔接明显出现了“脱节”问题。

四、非法取得或利用人脸识别信息行为的刑法规制路径

法律规范总存在这样的悖论——法律是立法者根据过去的经验总结而制定的规范，但是其规范的却是未来的行为。这也因此成为法律适用过程中不可避免的缺陷。非法取得或利用人脸识别信息行为的刑法规制困境正是因为这一缺陷而产生的。但由于刑法规范自身有着极强的概括性与包容性，即使面对上述困境，释法者仍可以通过穷尽解释方法的方式，如释法者通过解释这一方式仍不能解决，则立法者可通过积极立法的方式予以治理。

(一)非法获取、出售或者提供人脸识别信息行为的规制路径

尽管上文已从实质判断的角度论述了人脸识别信息具备识别特定自然人身份的功能，属于侵犯公民个人信息罪中的个人信息。但这仅仅从宏观的角度为非法取得或利用人脸识别信息行为的刑法规制提供了可能性。事实上，在具体司法适用中，人脸识别信息究竟属于《解释》第 5 条第 1 款规定的何种信息，以及具备何种可罚程度的非法获取、出售或者提供人脸识别信息的行为才能以侵犯公民个人信息罪定罪处罚才是真正需要解决的问题。一言以蔽之，欲以侵犯公民个人信息罪规制非法获取、出售或者提供人脸识别信息的行为，必须明确这一行为应适用《解释》第 5 条第 1 款的何项规定。

综观《解释》第 5 条第 1 款的规定不难发现，能够为非法获取、出售或者提供人脸识别信息的行为提供解释空间的规定仅有第 4 项、第 5 项与第 10 项。相应地，学界对此主要存在四种观点。第一种观点将人脸识别信息解释为“健康生理信息”，从而适用第 4 项的规定[23];第二种观点将人脸识别信息解释为“其他可能影响人身、财产安全的公民个人信息”从而同样适用第 4 项的规定[24];第三种观点将人脸识别信息解释为“第三项、第四项规定以外的公民个人信息”，从而适用第 5 项的规定[25];第四种观点则直接适用第 10 项这一兜底规定，并将非法获取、出售或者提供人脸识别信息 5 条以上解释为“其他情节严重的情形”。[26]笔者认为，上述第二种观点较为合理，在《解释》尚未将人脸识别信息明确列举之前，将其解释为“其他可能影响人身、财产安全的公民个人信息”，并适用 50 条的入罪标准是目前最为妥适的规制路径。

首先，从权利属性上看，人脸识别信息具备财产与人身权益的双重属性，属于影响人身、财产安全的公民个人信息。尽管学界对人脸识别信息的权利属性仍无定论，存在“财产权说”“隐私权说”“人格权说”“个人信息权说”等观点，但上述学说的交锋也从侧面表明，人脸识别信息同时具备了财产权、隐私权、人格权的色彩。在财产权方面，人脸识别信息作为商业价值以及财产价值的载体，可以用于多数交易的场合，具备着所有权的属性与排他效力。[27]在隐私权方面，滥用人脸识别信息极可能侵犯公民的人身尊严以及生活安宁，暴露公民的个人隐私。[28]因此，其属于民事权利的一类，可以被纳入隐私权的大范畴。[29]在人格权方面，从域外各国来看，将人脸识别信息作为人格权益加以保护时，有利于维护公民的人格平等。当人格权遭受侵权损害，被害人可以主张人身损害赔偿。[30]因此，人脸识别信息具备一定程度的财产权、隐私权、人格权的色彩，若其受到侵害，必将威胁公民个人的人身、财产安全。

其次，从其他规范的规定来看，将人脸识别信息解释为“其他可能影响人身、财产安全的公民个人信息”与法秩序统一性的要求相契合。《个人信息保护法》《信息安全技术个人信息安全规范》均将人脸识别信息归类为敏感个人信息，且认为其一旦泄露或非法使用，可能危害自然人的人身、财产安全。[31]因此，将其纳入“其他可能影响人身、财产安全的公民个人信息”中加以保护也与《个人信息保护法》《信息安全技术个人信息安全规范》等规范的规定相契合，从而可以保证法秩序的统一性。

再次，从客观结果上看，侵犯人脸识别信息将致人身、财产犯罪的实施更为轻易化，故人脸识别信息属于“其他可能影响人身、财产安全的公民个人信息”。人脸识别信息具备身份识别、信息核对、位置追踪等功能。因此，其一旦泄露，将致人身、财

产犯罪的实施更为轻易。例如，在人脸识别的黑产业链中，行为人只需获取被害人的一张或多张照片即可使用软件将其制作为符合人脸识别要求的包含左转脸、向右转脸、抬头、低头、眨眼等动作的连续视频，从而可用于破解小区门禁、人脸支付进而窃取公民财产，甚至实施非法侵入住宅、绑架、故意伤害等侵犯公民人身权利的犯罪。24 再如，当前许多房地产销售商利用人脸信息识别系统收集进入售楼部大厅消费者的人脸识别信息[32]，而这些信息被行为人收集用于售房诈骗也并非难事。另外，司法实践中屡见不鲜的利用人脸识别信息实施侵财类犯罪的案例[33]已经成为其属于“其他可能影响人身、财产安全的公民个人信息”的客观印证。

最后，人脸识别信息属于“其他可能影响人身、财产安全的公民个人信息”已经得到了司法裁判的认可。在我国“人脸识别第一案”即“郭兵诉杭州野生动物世界有限公司案”的二审裁判中，杭州市中级人民法院明确指出，“生物识别信息是敏感的个人信息，深度体现自然人的生理和行为特征，具备较强的人格属性，一旦被泄露或非法使用，可能导致个人的人身、财产安全受到危害，因此应谨慎处理并严格保护”[34]。

当然，仅论述人脸识别信息属于“其他可能影响人身、财产安全的公民个人信息”尚不足以成为仅将其纳入《解释》第 5 条第 1 款第 4 项保护的理由。笔者认为，其余三种观点无论是在对人脸识别信息的定性上还是在规范适用的规则上均存在一定偏颇。

首先，第一种观点将人脸识别信息纳入“健康生理信息”的范畴加以保护，陷入了法秩序不相统一的泥沼之中。《信息安全技术个人信息安全规范》第 3.1 条明确指出，个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。由此可见，在《信息安全技术个人信息安全规范》中，人脸识别信息(个人生物识别信息)与健康生理信息是互为并列、不相包容的两个独立概念。若将其他法律规范上互斥的“健康生理信息”与“人脸识别信息”解释为刑法上的种属关系，不仅有违逻辑，也将破坏法秩序的统一性。[35]值得一提的是，这一解释方法其实沿用了《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》中将信息网络传播行为解释为发行行为的旧路[36]，但《刑法修正案(十一)》的出台已证明其属于类推解释，故而更应摒弃。

其次，第三种观点将人脸识别信息定性为一般个人信息，且将其入罪标准设置为 5000 条，与《个人信息保护法》等规范对人脸识别信息的保护力度不相匹配。第三种观点将人脸识别信息解释为行踪轨迹信息、通信内容、征信信息、财产信息、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、财产安全的信息以外的公民个人信息。暂且不论在规范适用的先后顺序上，“其他可能影响人身、财产安全的公民个人信息”应优先于“第三项、第四项规定以外的公民个人信息”这一兜底条款加以适用。该观点最为明显的缺陷在于为侵犯人脸识别信息的行为设置了 5000 条的入罪标准，而这一标准与《个人信息保护法》《信息安全技术个人信息安全规范》对人脸识别信息的保护力度不相匹配。《个人信息保护法》《信息安全技术个人信息安全规范》均将人脸识别信息与健康生理(医疗健康)信息作为同一梯次的个人信息即敏感个人信息加以保护。因此，在刑法规制过程中，人脸识别信息也应与健康生理(医疗健康)信息处于同一位阶。然而，根据上述观点，侵犯健康生理信息的入罪标准为 500 条，而侵犯人脸识别信息的入罪标准却为 5000 条，这明显与《个人信息保护法》《信息安全技术个人信息安全规范》对二者采取同等保护力度的做法不相匹配。

最后，第四种观点存在以突出保护人脸识别信息为由，违背兜底条款的适用规则，突破罪刑法定原则限制的嫌疑。作为当前学界较为有力的一种观点，第四种观点认为，应突出人脸识别信息刑法保护的重要性，通过第 10 项这一兜底条款将非法获取、出售或者提供人脸识别信息的行为加以规制，并创造性地将其入罪标准设置为 5 条。[37]论者以刑法规制人脸识别信息犯罪的重要性为由，认为应为其设立最低的入罪标准。在《解释》第 5 条第 1 款第 3—5 项均不符合入罪数量要求的情况下，将第 10 项作为强化人脸识别信息刑法保护的适用规范。但该观点存在三大问题。

第一，为实现低标准的入罪数量，牺牲了对人脸识别信息刑法属性的研判。这种“先定量后定性”的规范适用方式与立法者、司法者普遍遵循的“先定性后定量”的方式相悖，实为本末倒置。

第二，违背了兜底条款的适用规则。“风险的泛在化、人脸识别信息的敏感性，不应成为刑法适用极端扩张化的藉口。”[38]因此，兜底条款应发挥着“补充法”的作用，“用以‘其他……’为内容的堵截构成要件，必须受到限制才能‘避免被任意解释’，即限于‘不得已’的场合”[39]。如若某一行为可以适用已被明确列举或尚未明确列举但足以通过解释的方式加以囊括，便无须适用兜底条款。在人脸识别信息可以解释为“其他可能影响人身、财产安全的公民个人信息”的前提下，自然不应再多此一举适用兜底条款。

第三，在第 3—5 项已保护所有个人信息类型的前提下，对其中的人脸识别信息另设数量标准将致《解释》内部条文体系的紊乱。《解释》第 5 条第 1 款采取了混合认定模式，从信息用途(第 1—2 项)、信息类型与数量(第 3—6 项)、违法所得数额(第 7 项)、主体身份(第 8 项)、主观恶性(第 9 项)等多种不同性质要素方面对侵犯公民个人信息罪中的“情节严重”作了明确规定。[40]根据同类解释规则，既然明确列举的“情节严重”是多种不同性质要素的混合，那么在认定“其他情节严重的情形”时也应按照混合认定模式进行认定。[41]按照这一观点，对于非法获取、出售或者提供人脸识别信息的行为，在《解释》尚未列举的情况下，似乎可以另设一项“信息类型与数量”的标准，从而将其纳入侵犯公民个人信息罪的规制范围。但笔者认为，《解释》第 5 条第 1 款第 3—5 项已经从“信息类型与数量”的角度穷尽了所有类型的个人信息。在个人信息类型已规定周延的状况下，不应再对其中某一信息类型另设数量标准，否则将导致《解释》第 5 条第 1 款条文的冗杂重复，甚至紊乱。事实上，这种指摘兜底条款可以包罗万象的观点不过是对兜底条款的曲解。[42]通过对其所在条文本身的理解，兜底条款的内涵和外延是可以明确的。[39]即使难以做到足够明确，但至少可以排除部分行为(如侵犯人脸识别信息的行为)不应纳入兜底条款规制的范畴。在该兜底条款中可以排除的是，其不应再采取“信息类型与数量”的认定模式。

综上所述，在《解释》尚未明确列举侵犯人脸识别信息入罪标准的现状下，将人脸识别信息解释为“其他可能影响人身、财产安全的公民个人信息”并适用《解释》第 5 条第 1 款第 4 项规定，是当前最为妥适的刑法规制路径。

(二)非法存储、使用、加工人脸识别信息行为的刑法规制路径

鉴于目前司法实践中已经出现了以非法存储、使用、加工人脸识别信息为手段进而实施违法犯罪活动的案件。因此，如何运用刑法规制上述手段以遏制违法犯罪活动的产生便显得尤为重要。有学者认为，基于罪刑法定原则的要求，由于《刑法》第 253 条之一仅将非法获取、提供公民个人信息的行为入罪，对于实践中业已出现的非法存储、使用、加工公民个人信息的行为，难以直接入罪。[43]但笔者认为，在遵循罪刑法定原则的前提下，对于非法存储、使用、加工公民个人信息的行为，完全可以通过解释学或立法学的路径对上述行为建构合理的刑法规制路径。

首先，对于非法存储人脸识别信息的行为，可以认定为不作为的非法获取人脸识别信息行为，继而以侵犯公民个人信息罪定罪处罚。需要明确的是，这里所讨论的是行为人已合法获取公民人脸识别信息前提下的非法存储人脸识别信息行为的定性问题。对于公民个人不知情而被非法获取或网络爬虫爬取后继而保持非法存储状态的行为，实际上可直接以侵犯公民个人信息罪、非法获取计算机信息系统数据或非法控制计算机信息系统罪等犯罪定罪处罚即可，故不在本文讨论之列。关于合法获取公民人脸识别信息后非法存储的行为，《民法典》《网络安全法》《电子商务法》已作出了较为详细规定。《民法典》第 1037 条第 2 款规定:“自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。”《网络安全法》第 43 条规定:“个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息;发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。”《电子商务法》第 24 条第 2 款规定:“电子商务经营者收到用户信息查询或者更正、删除的申请的，应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的，电子商务经营者应当立即删除该用户的信息;依照法律、行政法规的规定或者双方约定保存的，依照其规定。”因此，合法获取公民人脸识别信息后非法存储的情形仅限于信息收集主体合法获取了人脸识别信息，但其违反法律法规或者双方的约定擅自存储个人信息，在公民个人发出删除通知后，仍不予以删除，抑或在公民个人用户注销后无正当理由继续保留和处理该信息。由此可见，当信息收集主体合法获取公民人脸识别信息后非法存储的行为，在公民个人发出删除通知后，该信息收集主体即具备了采取措施予以删除的法定义务。当然，这并不意味

着不履行该法定义务即构成不作为的侵犯公民个人信息罪。成立不作为犯罪，还要求行为人以不作为实现的不法构成要件与作为实现的不法构成要件在刑法上之非价，彼此相当。[44]因此，在明确信息收集主体具备删除义务的前提下，还需探讨其不履行删除义务(非法存储)行为与非法获取行为之间是否等价。而认定不作为行为与作为犯罪是否等价，必须证明不作为人故意或过失行为导致了侵害特定法益的现实危险性[45]，且与作为行为对法益侵害所起的作用和效果相当。[46]笔者认为，一方面，导致公民个人信息法益侵害结果的原因仅限于信息收集主体在收到公民通知后仍不删除进而存储的行为，并不包含其他可能具备法益侵害性的起因;另一方面，合法获取公民个人信息后经要求删除仍不删除的行为与非法获取公民个人信息行为对法益侵害所起的作用相当，这在刑法中已经有相关立法例。例如,《刑法》第128条第1款规定了非法持有、私藏枪支、弹药罪。其中，“私藏”是指依法配备、配置枪支、弹药的人员，在配备、配置枪支、弹药的条件消除后，违反枪支管理法律、法规的规定，私自藏匿所配备、配置的枪支、弹药且拒不交出的行为。笔者认为，刑法之所以将本罪规定为“持有”与“私藏”并列的选择性罪名，是因为丧失合法持有枪支、弹药资格后私藏枪支、弹药的行为与本不具备合法持有枪支、弹药资格而非法持有的行为所具备的法益侵害性相当。[47]由此可见，既有立法已肯定了非法持有(获取)行为与丧失合法持有(获取)资格后非法藏匿(存储)的行为具备相当的法益侵害性。因此，信息收集主体在应履行删除义务却继续予以存储时，实质上等同于其非法获取了该人脸识别信息，故而可认定为不作为的非法获取人脸识别信息的行为，以侵犯公民个人信息罪定罪处罚。[48]

其次，对于非法使用、加工[49]人脸识别信息的行为，可通过扩大解释“非法”的范畴甚或增设非法利用公民个人重要信息罪加以规制。

第一，在立法尚未先行的现状下，将侵犯公民个人信息罪中的“非法”解释为“以非法利用为目的”可解燃眉之急。当前对于侵犯公民个人信息罪中“非法”的含义一般理解为“以非法的方式”或“以非法的状态”，即将“非法”作为“获取”的修饰词。如果遵循这样的解释逻辑，非法利用人脸识别信息的行为自然无法纳入刑法规制的范畴。为此，有学者提出将“非法”解释为“以非法利用为目的”。[50]笔者较为赞同这一观点。首先需要明确的是，“非法利用”这一主观目的并不为侵犯公民个人信息罪的直接故意所包含，这一目的的实现有待于行为人进一步实施利用人脸识别信息的客观行为，如非法使用、非法加工。因此，相对于非法获取行为而言，非法利用的目的是一种超过的主观要素[51]，这一目的需通过行为人事后对个人信息的使用状态是否合法加以推定。如此，即使行为人获取个人人脸识别信息的方式合法，但只要其对该信息的利用非法，便可推定其在获取人脸识别信息时具备非法利用的目的，从而认定为非法获取人脸识别信息的行为，以侵犯公民个人信息罪定罪处罚。

第二，刑事立法仍是规制非法利用人脸识别信息行为的治本之策。尽管可以通过解释学的路径对非法利用人脸识别信息的行为加以规制，但这一解释进路是否合理、是否超出国民预测可能性仍有待审视。因此，规制非法利用人脸识别信息行为的治本之策仍是刑事立法，即增设能够规制非法利用人脸识别信息等在内的可能严重影响人身、财产安全的个人信息行为的非法利用公民个人重要信息罪。实际上，因“非法利用”特定对象而构成犯罪的情形在我国刑法中已有规定，例如《刑法》第284条规定的非法使用窃听、窃照专用器材罪、第375条第3款规定的非法使用武装部队专用标志罪和第287条之一规定的非法利用信息网络罪等。[52]上述前两个“非法使用”型犯罪中非法使用的对象均为专用物品，具有较强的排他使用性，即只能由特定的主体或只能在特定的场合进行使用。然而，人脸识别信息等可能严重影响公民人身、财产安全的个人信息并不具备这样的特征。因为只要经过公民个人的单独同意，第三人便可使用其人脸识别信息。因此，笔者认为，在非法利用公民个人重要信息罪行为方式的规定上，可以借鉴非法利用信息网络罪的规定模式。至于其刑度的选择，由于非法利用人脸识别信息等个人信息所导致的后果一般较轻，且若涉及其他犯罪如敲诈勒索罪等会另罪处罚，故而本罪的起刑点不应过高，宜与侵犯公民个人信息罪相当。[53]因此，可将非法利用公民个人重要信息罪作为《刑法》第253条之二，并将其罪状表述为:

未经许可，利用公民个人人脸识别信息等可能严重影响人身、财产安全的个人重要信息实施下列行为之一，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:

(一)伪造、变造、冒用公民个人重要信息的;

(二)将公民个人重要信息用于实施威胁、恐吓、挟制等行为的;

(三)将公民个人重要信息用于营利活动的。

尽管明确了非法利用公民个人重要信息罪的罪状，但根据罪刑法定原则，仍需将其“情节严重”的情形具体化。立法者之所以对某些犯罪采取情节犯的立法模式，主要是考虑到现实生活中有许多行为，虽然在一般情况下其社会危害性还没有达到应受刑罚处罚的程度，却又难以通过强调犯罪构成的某一方面的具体内容或者增加某一具体要素来使之达到这种程度，或者不能预见所有情节严重的情况而无法作出具体规定，或者虽能预见但需做冗长的表述，使刑法丧失简短价值。于是，立法者作出一个综合性规定，如“情节严重”便认定为犯罪，否则不以犯罪论处。因此，实践中对于情节是否严重的判断，应当尽可能考虑案件的全部情况。[54]笔者认为,《解释》对于侵犯公民个人信息罪中的“情节严重”已经规定了较为明确的考量标准。因此，行为对象数量标准、行为性质标准、后果标准、又犯标准可在判断非法利用公民个人重要信息罪的“情节严重”时予以参考。但同时，由于非法利用公民个人信息行为具备行为手段上的特殊性，因此也应根据利用行为的特点确定其“情节严重”的额外标准。例如，欺诈型利用、隐瞒型利用、大规模反复利用等均体现出较一般不当利用行为更为严重的危害性，故而同样可以作为认定非法利用公民个人重要信息罪“情节严重”的标准。[55]

注释:

1 张翠平、苏光大:《人脸识别技术综述》,《中国图象图形学报》2000 年第 11 期，第 885 页。

2(1)2019 年 4 月，郭兵支付 1 360 元购买野生动物世界双人年卡，确定指纹识别入园方式。2019 年 7 月、10 月，野生动物世界两次向郭兵发送短信，通知年卡入园识别系统更换事宜，要求激活人脸识别系统，否则将无法正常入园。但是，郭兵认为人脸信息属于高度敏感个人隐私，不同意接受人脸识别，要求园方退卡。参见新华网:《“人脸识别第一案”宣判野生动物世界被判赔 1 038 元》，https://baijiahao.baidu.com/s?id=1683930258051178093&wfr=spider&for=pc,2021 年 11 月 24 日访问。

3(2)2018 年 8 月，唐某通过他人介绍先后两次前往山东省菏泽市李瑞安处学习制作用以破解某宝人脸识别认证系统的 3D 人脸动态图，并从李瑞安处购买了相关设备，支付李瑞安人民币 2.3 万元。后唐某在网络上发布信息称能够提供破解某宝人脸识别认证的服务。2018 年 9 月，唐某从“半边天”(另案处理)处获得唐甲的某宝账户信息，受“半边天”委托破解某宝对唐甲账号的限制，唐某采用制作唐甲 3D 人脸动态图的方式突破了某宝人脸识别认证系统，解除了某宝对唐甲账号的限制登录，后唐某将唐甲某宝账户信息提供给张羽，张羽通过伪造唐甲手持身份证、同意(承诺)函的照片并拨打某宝客服电话的方式解除了某宝对唐甲账户的资金冻结，后张羽采用购买话费的形式将唐甲某宝账户内的人民币 2.4 万余元转移。参见界面新闻:《人脸识别如何侵犯公民个人信息?不法分子制作 3D 人脸模型骗过支付宝》，https://baijiahao.baidu.com/s?id=1686826513510180399&wfr=spider&for=pc,2021 年 11 月 24 日访问。

4(3)犯罪嫌疑人通过破解人脸识别技术等方式，注册“皮包公司”用于虚开增值税普通发票，价税合计超过 5 亿元。该案中的关键环节，是犯罪嫌疑人利用他人高清头像及身份证信息，破解相关政务平台的人脸识别，成功注册“皮包公司”。据该案中专门从事人脸识别破解的犯罪嫌疑人交代，其一般先从他处以 30 元每个的价格购买他人的高清头像和身份证信息，之后对高清头像进行处理，让照片“动起来”，形成包括点头、摇头、眨眼、张嘴等动作视频。在人脸识别认证环节，犯罪嫌疑人利用特殊处理“劫持”手机，使系统不启动摄像头，而是获取之前做好的视频，最后通过认证。用这套办法，犯罪嫌疑人破解了政务、安防、金融、支付、生活消费等多款用户量巨大的 App，每单的破解价格从 25 元到 300 元不等。参见南方都市报:《又有人用“活照片”破解人脸识别，注册皮包公司开发票超 5 亿》，http://m.mp.oeeee.com/a/BAAFRD0000202104014633 85.html,2021 年 11 月 24 日访问。

5(4)新京报:《人脸识别黑产:真人认证视频百元一套》，https://baijiahao.baidu.com/s?id=1696883210420732243

&wfr=spider&for=pc,2021 年 11 月 24 日访问。

6(1)张明楷:《刑法分则的解释原理(上)》，法律出版社 2011 年版，序说第 9 页。

7(2)费孝通:《乡土中国》，北京出版社 2011 年版，第 7 页。

8(3)郭春镇:《数字人权时代人脸识别技术应用的治理》,《现代法学》2020 年第 4 期，第 21-22 页。

9(4)王哲:《侵犯公民个人信息罪中“个人信息”的限定》,《青少年犯罪问题》2021 年第 3 期，第 80 页。

10(1)松宫孝明:《刑法总论讲义》，钱叶六译，中国人民大学出版社 2013 年版，第 81 页。

11(2)吴盛:《对〈刑法修正案(七)(草案)〉第六条的完善建议》,《检察日报》2008 年 9 月 16 日。

12(3)秦天宁:《论网络服务提供行为的著作权刑民规制衔接——兼析〈刑法修正案(九)〉第 29 条关于中立帮助行为的规定》,载魏昌东、顾肖荣:《经济刑法(第 17 辑)》，上海社会科学院出版社 2017 年版，第 252 页。

13(4)喻海松:《侵犯公民个人信息罪司法适用探微》,《中国应用法学》2017 年第 4 期，第 175 页。

14(5)杨帆:《刑法新增侵犯个人信息两罪之评析》,《铁道警官高等专科学校学报》2010 年第 3 期，第 60-63 页。

15(6)参见王哲:《侵犯公民个人信息罪中“个人信息”的限定》,《青少年犯罪问题》2021 年第 3 期，第 80 页。

16(7)肖若秀、王志良:《机器智能:人脸工程》，机械工业出版社 2017 年版，第 199-200 页。

17(8)熊欣:《人脸识别技术与应用》，黄河水利出版社 2018 年版，第 7 页。

18(1)阿图尔·考夫曼、温弗里德·哈斯默尔主编:《当代法哲学和法律理论导论》，郑永流译，法律出版社 2002 年版，第 18-19 页。

19(2)付立庆:《论刑法用语的明确性与概括性——从刑事立法技术的角度切入》,《法律科学(西北政法大学学报)》2013 年第 2 期，第 95 页。

20(1)广东商讯:《工行佛山分行温馨提示:防范“人脸信息”被非法利用》,https://page.om.qq.com/page/O-Aioa Nz Xsmz EMDLr F6Dzk6AO,2021 年 11 月 26 日访问。

21(2)收集行为本质上属于获取行为。

22(3)传输、提供、公开行为本质上属于提供行为。

23(4)欧阳本祺、王兆利:《涉人脸识别行为刑法适用的边界》,《人民检察》2021 年第 13 期，第 17-18 页。

24(1)(9)宋行健:《论非法获取人脸识别信息的刑法规制》,《山西警察学院学报》2020 年第 2 期，第 6 页。

25(2)任和和:《论我国人脸识别信息侵害行为的刑法规制》，载施伟东:《上海法学研究(第 14 卷)》，上海人民出版社 2021 年版，第 274-275 页。

26(3)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》,《重庆大学学报(社会科学版)》2021 年第 2 期，第 140 页。

27(4)刘德良:《论个人信息的财产权保护》,《法学研究》2007 年第 3 期，第 80-85 页。

28(5)张新宝:《隐私权的法律保护》，群众出版社 2004 年版，第 139 页。

29(6)朱巍:《人脸识别的法律性质认定》,《检察日报》2019 年 11 月 6 日。

30(7)王利明:《论个人信息权在人格权法中的地位》,《苏州大学学报(哲学社会科学版)》2012 年第 6 期，第 68-75 页。

31(8)尽管《个人信息保护法》与《信息安全技术个人信息安全规范》对于敏感个人信息的定义存在差异，前者将敏感个人信息定义为“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”;后者定义为“一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息”。但不可否认的是，二者均认为敏感个人信息与公民个人人身、财产安全密切关联。

32(10)收集消费者的人脸识别信息已成为全国房地产销售方的惯用手段，相关案例如“佛山招商果岭房地产有限公司侵害消费者依法得到保护的个人信息权利案”，参见顺市监一队罚字[2021]16 号行政处罚决定书;“苏州东澄房地产开发有限公司侵害消费者依法得到保护的个人信息权利案”，参见相市监处字[2021]227 号行政处罚决定书;“无锡鸿誉房地产开发有限公司侵害消费者依法得到保护的个人信息权利案”，参见锡山市监处字[2021]03037 号行政处罚决定书。

33(1)如“唐某、张某利用人脸识别技术盗窃案”，参见成都市郫都区人民法院(2019)川 0124 刑初 610 号刑事判决书;“白某宽‘刷脸’骗贷案”，参见贵州省遵义市红花岗区人民法院(2018)黔 0302 刑初 22 号刑事判决书。

34(2)任和和:《论我国人脸识别信息侵害行为的刑法规制》，载施伟东:《上海法学研究(第 14 卷)》，上海人民出版社 2021 年版，第 269 页。

35(3)欧阳本祺、王兆利:《涉人脸识别行为刑法适用的边界》,《人民检察》2021 年第 13 期，第 18 页。

36(4)《刑法修正案(十一)》出台前,《刑法》第 217 条侵犯著作权罪的行为方式主要包括复制、发行行为，不包含信息网络传播行为。为规制实践中愈演愈烈的通过信息网络传播侵犯著作权的行为，在《著作权法》已将信息网络传播权、发行权规定为两项独立的权利的情况下,《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》仍将“信息网络传播”解释为“发行”。《刑法修正案(十一)》的出台，将信息网络传播规定为与复制发行并列的一项侵犯著作权的独立行为，从而《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》扩大解释“发行”的正当性受到冲击。

37(1)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》,《重庆大学学报(社会科学版)》2021 年第 2 期，第 140 页。

38(2)欧阳本祺、王兆利:《涉人脸识别行为刑法适用的边界》,《人民检察》2021 年第 13 期，第 16 页。

39(3)(7)储槐植:《刑事一体化与关系刑法》，北京大学出版社 1996 年版，第 359、358-359 页。

40(4)喻海松:《侵犯公民个人信息罪司法解释理解与适用》，中国法制出版社 2018 年版，第 37-46 页。

41(5)石聚航:《侵犯公民个人信息罪“情节严重”的法理重述》,《法学研究》2018 年第 2 期，第 63 页。

42(6)李军:《兜底条款中同质性解释规则的适用困境与目的解释之补足》,《环球法律评论》2019 年第 4 期，第 117 页。

43(8)喻海松:《〈民法典〉视域下侵犯公民个人信息罪的司法适用》,《北京航空航天大学学报(社会科学版)》2020 年第 6 期，第 4 页。

44(1)林山田:《刑法通论(下)》，台湾台大法学院图书部 2006 年版，第 226 页。

45(2)何荣功:《不真正不作为犯的构造与等价值的判断》,《法学评论》2010 年第 1 期，第 111 页。

46(3)袁爱华、李克艳:《不真正不作为犯的等价性问题研究》,《云南大学学报(法学版)》2013 年第 3 期，第 81 页。

47(4)当然，非法私藏仅仅是非法持有的一种表现形式，且依法配备、配置枪支、弹药的人员，在配备、配置条件消除后，将枪支、弹药丢弃，不再事实上支配枪支、弹药的，难以评价为“私藏”(有可能成立丢失枪支不报罪或者其他犯罪);如果只有行为人知道枪支、弹药藏于何处，则仍然属于持有枪支、弹药。因此，笔者认为并无必要将“私藏”独立于“持有”。参见张明楷:《刑法学(下)》，法律出版社 2021 年版，第 916 页。

48(1)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》,《前沿》2021 年第 4 期，第 89 页。

49(2)在刑法视域下，“加工”一词过于模糊，其行为方式主要表现伪造、变造等手段，本质上仍属于非法利用行为。故下文笔者将省略“加工”，将其与“使用”统称为“利用”。

50(3)王哲:《侵犯公民个人信息罪中“个人信息”的限定》,《青少年犯罪问题》2021 年第 3 期，第 80 页。

51(4)陈兴良:《目的犯的法理探究》,《法学研究》2004 年第 3 期，第 73 页。

52(5)李振林:《非法利用个人金融信息行为刑法规制强化论》,《华东政法大学学报》2019 年第 1 期，第 81 页。

53(6)吴苌弘:《个人信息的刑法保护研究》，上海社会科学院出版社 2014 年版，第 184 页。

54(1)利子平、周建达:《非法获取公民个人信息罪“情节严重”初论》,《法学评论》2012 年第 5 期，第 148 页。

55(2)李川:《个人信息犯罪的规制困境与对策完善——从大数据环境下滥用信息问题切入》,《中国刑事法杂志》2019 年第 5 期，第 46 页。