# 人脸识别技术中个人信息保护法律问题研究

董美玉
大连海洋大学海洋法律与人文学院　辽宁大连　116023

**摘　要：**当前人工智能时代，人脸识别技术俨然已经成为人们生活的一部分。人脸作为人类一生无法改变的生物信息，一旦被非法采集或利用便会造成无法挽回的损失。因此，个人信息需要法律严加保护，本文从法律、行政和个人三个维度进行规制，包括完善法律保障、建立专门信息监管机构和提高公民的信息保护意识，为妥善处理科技与个人信息保护的关系提供思路。

**关键词：**人脸识别；个人信息；法律保护

人脸识别技术以个人的面部特征为媒介，经过采集面部轮廓和立体信息，后用于验证个人身份信息，多被需要人身认证的场合采用。目前，人脸识别技术因其便捷性在生活中的应用越来越广泛，逐渐渗透公民的生活，如住宅门禁、企业打卡制度、支付、快递取件等。由于人脸信息采集的场合与途径广泛，有时无需当事人的同意便可采集到，公民对于自身的信息保护意识淡薄，加之相关法律规制不到位，使得个人信息裸露在市场上，存在泄漏和被非法买卖的风险，为不法分子利用人身信息实施诈骗、盗窃等犯罪活动提供空间。本文针对人脸识别技术的特点、个人信息现存的风险和亟待解决的法律规制漏洞，探析人脸识别技术中个人信息保护的对策。

## 一、人脸识别技术采集个人信息的应用场景与特征

### （一）应用场景

人脸识别技术的应用是根据所采集并存储的人脸图像，记录面部立体特征，在需要进行人身验证的场合，将现场输入的人脸图像和存储介质中的人脸图像进行比对，从而识别每个人的身份，核查是否为本人。目前，人脸识别技术被广泛应用于公共安全（罪犯识别、边防管理）、场所进出（机构门禁、物业服务）、信息处理（账户认证、文件解密）等领域，包括机场、高铁站、火车站、银行、博物馆、动物园等公共场所的出入和验票口，甚至部分公司考勤制度、快递取件以及学校上课的点名也采用人脸识别。

### （二）特征

1.非接触性

采集人脸信息时，用户不需要和设备直接接触，而是和机器保持一定距离，可以避免肢体接触，避免病毒的传播，并提高效率。在新型冠状病毒流行时期，非接触性具有极大的优越性，使用人脸识别，可以让被采集者与工作人员之间间隔规范的距离，且被采集者与机器交互，定时定点地对机器进行消毒，对防止病毒传播有促进作用。此外，中国是人口大国，交通出行的压力一直存在，春运更甚，大规模的人口迁移往往造成交通系统运行的瘫痪，因此，人脸识别技术不可避免地被应用在交通体系中，包括自动取票、检票，自动识别人脸缴费等，有效提高检票体系的效率，降低高速公路收费站拥堵状况。

2.非强制性

非强制性指的是无需其知情和配合即可获取人脸信息并存储，将人脸在指定位置曝光，被识别的人脸图像信息可以主动获取，这样自然人的面部特征可能在其不知情的情况下就被采集完成。而人脸以外的个人信息——指纹、虹膜等则需要被采集者的配合才能完成，当自然人在配合的过程中，代表其已经知悉并同意了个人信息被收集和存储，即《民法典》、《中华人民共和国网络安全法》所规定的“告知同意原则”，被采集者被告知将被采集人脸信息，配合的行动便是同意此项个人信息被采集。然而，人脸识别技术的非强制性，决定了对人脸这一生物识别信息的收集，只要存在采集设备和对象，无需配合便可获取。如遍布在道路、公共场合、酒店商场和企业单位的摄像头，即使行人没有发现摄像头的存在，人脸信息也会被收集并储存。这种具有隐蔽性的收集带来了极大的风险，不法分子利用摄像头针对特定的对象摆放，便可获取特定对象的人脸信息，进而使用非法采集的人脸信息进行非法活动。即使的合法的信息收集，存储不当产生泄露也容易被不法分子截留，为开展违法犯罪提供条件。过去十年，中国是监控摄像头增长最快的国家。根据咨询公司IHS Markit 2016年的数据，中国共装有1.76亿个监控摄像头，其中由公安系统掌握的，有两千万只（图1）。现代社会，人们生活在摄像头下。不同于其他个人信息，人脸这一个人信息具有

恒久性，即这个信息几乎不可更改（即使整容，面部特征依然可以被识别），一旦泄漏对自然人所产生的的危险是难以消除且长期存在的。

**图1　街角的摄像头**

3.并发性

实际应用场景下可以进行多个人脸的分拣、判断及识别，即使有多个人脸面孔出现，人脸识别技术会自动分拣，摄取所需的人脸信息。这种并发性极大的提高效率和便捷性，解释了公共交通和公共场合大量应用人脸识别技术的原因。并发性和非强制性使得在采集人脸信息时无法落实法律规定的“告知同意原则”。此时，便需要其他法律对此种个人信息采集作出规制，对采集者的规范，对采集场合和采集形式的规范，以及明确公民个人生物识别信息禁止任意采集，这些在我国的法律中尚无规定，配套法律亟待完善。

## 二、人脸识别技术中个人信息的风险

我国对于人脸信息收集并没有设置相应的门槛要求，任何部门、机构和公司都可以某些目的来收集公民信息，人脸信息存在诸多泄漏风险——信息存储不当、信息泄漏、非法信息买卖等。

### （一）缺乏法律规制

我国目前并没有成体系的法律对人工智能采集个人信息进行规制，不同法律部门中分散相关条文，如《宪法》中规定了公民享有人格权；《刑法》中就非法提供公民个人信息罪、非法获取公民个人信息罪等，就个人信息安全进行保护；《行政法》中出台了个人信息保护的规定，将可识别出公民身份公民的电子个人信息纳入保护范围，此外，我国工信部还发布了关于公民个人信息保护的相关规定；《民法典》的人格权、《网络安全法》和相关司法解释也有个人信息保护的相关规定。

我国针对某些领域的个人信息保护，分散在不同的法律部门中，没有形成较为完备的体系，导致现有条款对相应个人信息保护并不全面和深入，在诉诸法律时甚至“无法可依”，不仅如此，在实务中由于维护特定个人信息——如人脸信息，的法律条文具有特殊性，一般只保护某一类个人信息——如指纹、电子信息资料，有的并不包含人脸信息，对于人脸信息无法全部适用。但是基于人脸信息的重要性和难以改变的唯一性，应当有更多的相关法律法规进行规制。缺乏健全和完善的保护机制，使得公民的个人信息时时刻刻受到威胁。

### （二）缺乏监管风险

基于人脸信息于公民的重要性，在繁杂的政府部门和其他单位中进行使用时，采集、存储和保护规则不一，技术良莠不齐，存储信息量巨大，一旦泄露则会造成不可恢复的后果，因此国外较多国家和地区都专门设立了个人信息监管机构——加拿大设立的隐私保护机构，在个人信息保护法律之外，设置隐私保护机构又增加了一层保护措施；在香港，公民除了使用《个人资料条例》作为法律武器，私隐专员公署也为个人信息保护保驾护航。我国除了不同法律部门间对个人信息保护的一些条例和法律条文，并没有专门机构对公民个人信息进行监管，对已经涉及此种职责的部分监管部门没有明确规定权责归属，多个具有监管职责的部门间如果没有较为系统和完善的法律规范和明确的分工，容易出现权责推诿现象，降低相关部门的工作效率，同时让非法采集个人信息的不法分子有机可乘。

### （三）个人信息保护意识淡薄

人脸识别技术无需配合且采集过程不会被发觉，当不法分子读取或收集个人信息时难以察觉，公民对人脸识别采集个人信息包容度较强，对人脸采集并不敏感，不经告知便同意采集，对采集者资质、采集形式不加审查，个人信息保护意识淡薄。泄漏的个人信息侵权后难以恢复原状，即使维权成功，公民人脸信息作为永久性信息却无法更改。海量的人脸信息一旦泄露，就会因人脸的难以更换而导致终身泄露，信息主体即使法律维权成功，也难以恢复原状。因此，无论是政府部门还是商业机构，若在收集、存储、运用人脸信息过程中没有遵守法律法规所确定的“合法、正当、必要”和“告知——同意”原则，都可能因侵犯公民个人信息而引起相应的法律责任。

## 三、人脸识别技术中个人信息保护的途径

### （一）完善法律保障，厘清人脸识别应用边界

我国有关个人信息安全和保护的法律亟待增设和完善，在对人脸信息等个人信息进行保护时，重点限制企业采集信息。然而公权力收集人脸信息并未得到限制和规制，只规定了“正当性”这一采集原则，但是具体实施时，何为正当性是个模糊不清的定义，更无法落实到具体的措施，不具有操作性。且相关的法律零散的分落在多个部门法中，没有一部专门性法律，如香港的《个

人资料条例》，实务中对个人信息的侵犯五花八门，复杂多变，救济途径也只能根据侵权维权。完善个人信息保护相关法律，设立个人信息保护专门性法律，为公民保护个人信息不受侵害和维护自身权益保驾护航。同时，规范和限制公权力对个人信息的采集，加强对采集公众数据的监管，使人脸识别技术采集人脸信息的透明化，此外，赋予法官由裁量权来实现公平正义。

（二）建立专门信息监管机构

建立专门的个人信息监管机构，严格管理人脸识别数据，依法对政府部门、商业机构和企业等采集人脸信息进行规制，统筹控制采集的途径和设备，有利于发挥最大效率，避免各部门间的权责推诿。在此规制过程中，进一步形成对对人脸信息等个人信息保护的原则和具体规则，极大的推进对公民人脸信息的保护。建立专门信息监管机构具有预防法益受到侵害，提高公民维护个人信息权的便利性。公民不再只能通过个案分析，根据不同案件不同分析的原则，向相应的部门进行投诉或起诉，而是一旦人脸等个人信息存在泄露风险，即可通过专门信息监管机构举报，对采集主体的行为进行调查，必要时给予警告和处罚，将犯罪行为扼杀在摇篮里。

（三）提高公民的信息保护意识

作为人脸识别技术采集的直接对象，个人的主动防护是保护个人信息的第一性的。人工智能时代，人们不可避免的跟随时代的潮流接受各种科技融入生活，在这些科技方便人们生活的时候，我们应该加强自身信息保护意识，做好个人防范，在填写个人信息或者使用智能软件时，认真核对隐私条款，仔细辨别采集机构，不能不加审视地，同意个人信息条款让不法分子非法采集个人信息无机可乘。此外，当遇到对个人信息被过度采集和非法采集的情况，即时举报给相应机关处理。政府部门也应加大相关普法宣传，告知个人信息保护的迫切性和重要性，以及当个人信息受到侵犯时可诉诸的法律途径。

**参考文献：**

[1]尚世芳，焦艳玲.人脸识别技术应用中个人信息保护的伦理思考[J].中国医学伦理学，2021，34（09）：1133-1138.

[2]武安宁.人脸识别技术应用法律规制研究[D].安徽财经大学，2021.

[3]李保锦.从“人脸识别第一案”看个人信息保护[N].江苏经济报，2021-04-28（B03）.

[4]石佳友，刘思齐.人脸识别技术中的个人信息保护——兼论动态同意模式的建构[J].财经法学，2021（02）：60-78.

[5]张宇轩.人脸识别技术下的个人信息保护——以设计保护为进路[J].河南理工大学学报（社会科学版），2021，22（02）：18-24.

[6]胡建兵.“人脸识别第一案”提示个人信息保护重要性[N].长春日报，2020-11-24（006）.

[7]闫双巧.人脸识别等生物识别技术侵权救济——以个人信息保护为视角[J].河南工学院学报，2020，28（06）：74-80.

[8]袁俊.人脸识别国际监管经验及规制建议[J].网络空间安全，2020，11（07）：120-124.

[9]郭春镇.数字人权时代人脸识别技术应用的治理[J].现代法学，2020，42（04）：19-36.

[10]蒋淑旭，胡丹.人脸识别中个人生物识别信息的法律保护[J].淮北职业技术学院学报，2020，19（03）：74-77.

[11]牛海虹.人脸识别运用中的个人信息保护[D].中国社会科学院研究生院，2020.