君合专题研究报告 JUNHE

2021年5月20日

人脸识别知多少——从“人脸识别第一案”说起

前言

随着大数据时代到来，人脸识别技术逐渐深入人们生活的各个角落。从银行业务到小区门禁，从登录App、面容支付到高铁过检，无不使用着我们的面部特征信息。在这种背景下，“人脸”采集和使用的边界何在？人脸识别技术为我们的生活带来诸多便利，但它存在的风险和隐患同样不容忽视。此前，某大学特聘某法学副教授（以下简称“**原告**”）因不满杭州某公园（以下简称“**园方**”或“**被告**”）改用人脸识别方式入园，而以侵犯个人隐私和服务合同违约为由起诉了园方。本案被称为“人脸识别第一案”，被认为在我国的个人信息保护方面具有标志性的意义。本文旨在通过此案在个人信息保护方面的判决，分析目前人脸识别信息在收集使用等方面的规则，给出企业使用人脸识别技术的合规建议，以期对企业的收集和使用人脸识别信息的相关业务有所助益。

一、 人脸识别第一案

（一）案情回顾

2019年4月27日，原告支付1360元购买了园方“畅游365天”双人年卡。年卡要求使用指纹识别入园方式。原告与其妻子在园方留存了姓名、身份证号码、电话号码等个人信息，并录入了指纹识别信息，此外还应园方对于年卡用户的规定“至年卡中心拍照”。此后，原告与其妻子多次入园游览。2019年7月、10月，园方两次向原告发送短信，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。原告与其妻子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入园方式，要求园方退卡。双方协商无法达成一致意见，2019年10月28日，原告向浙江省杭州市富阳区人民法院提起诉讼。

（二）法院判决

2019年11月3日，浙江省杭州市富阳区人民法院正式受理此案，于2020年11月20日出具（2019）浙0111民初6971号服务合同纠纷一审民事判决书，判令园方删除原告及其妻子的照片及面部特征信息。原告和园方均不服一审判决，均提起上诉。2021年4月9日，浙江省杭州市中级人民法院出具了（2020）浙01民终10940号民事判决书，除维持一审部分判决之外，还要求园方删除原告及其妻子的指纹识别信息。

本案一审二审的判决均体现了目前司法层面对于个人信息的保护，且体现了对于人脸识别信息的特殊考虑。二审判决中对面部识别特征收集的合法性和正当性进行了详细的阐述，例如，在合法性方面，“人脸识别信息相比其他生物识别信息而言，呈现出敏感度高，采集方式多样、隐蔽和灵活的特性，不当使用将给公民的人身、财产带来不可预测的风险，应当作出更加严格的规制和保护”；在正当性方面，“园方虽自述其并未将收集的照片激活处理为人脸识别信息，但其欲利用收集的照片扩大信息处理范围，超出事前收集目的，违反了正当性原则”。目前，原告向浙江省高院申请再审。我们将继续关注本案再审情况。

二、 常见的人脸识别适用场景

目前人脸识别技术在人们生活中的使用场景越来越广泛。根据全国信息安全标准化技术委员会

秘书处2021年4月23日发布的关于国家标准《信息安全技术 人脸识别数据安全要求》征求意见稿征求意见的通知（以下简称“**《人脸识别数据安全要求》**”），涉及人脸识别信息处理的主要包括三类场景，分别是：

1、人脸验证：将采集的人脸识别数据与存储的特定自然人的人脸识别数据进行比对（1：1比对），以确认特定自然人是否为其所声明的身份，主要包括机场、火车站的人证比对，移动智能终端的人脸解锁功能等。

2、人脸辨识：将采集的人脸识别数据与已存储的指定范围内的人脸识别数据进行比对（1：N比对），以识别特定自然人，主要包括公园入园、居民小区门禁等。

3、人脸分析：不开展人脸验证或人脸辨识，仅对采集的人脸图像进行统计、检测或特征分析，主要包括公共场所人流量统计、体温检测、图片美化等。

在实务中，以下场景都可能使用到人脸识别技术，需要收集使用人脸识别信息的企业格外关注相关业务上的数据合规风险。

- 刷脸打卡/考勤：企业门禁
- 刷脸进入社区：小区门禁
- 刷脸进入公共场所：刷脸进公园/校园
- 刷脸支付：App刷脸线上支付/商场、便利店等刷脸线下支付
- 刷脸认证：刷脸认证登录App和小程序如健康宝、个人所得税App等
- 刷脸解锁：刷脸打开手机
- 刷脸办业务：银行业务，酒店入住，自App或小程序获取医院出具的线上报告等
- 刷脸安检：铁路/航空刷脸过检
- 智慧安防：使用人脸识别技术监控阻挡可疑人员
- 智慧交通：使用人脸识别技术如闯红灯记录系统

在以上场景中均可能涉及到人脸识别信息的收集、使用、存储、共享等处理，相较一般个人信息需要企业遵循相关法律法规和国家标准，进行更加严格和谨慎的处理和予以额外的关注。

三、 人脸识别规制要求

人脸识别信息属于个人生物识别信息，个人生物识别信息进一步属于个人敏感信息，相较于其他个人信息应当受到更加谨慎的处理和保护。目前我国的法律法规和国家标准例如《信息安全技术 个人信息安全规范》（以下简称“**《个人信息安全规范》**”）、《人脸识别数据安全要求》、国家标准化管理委员会关于对《安防人脸识别应用 程序接口规范》（征求意见稿）等国家/行业标准公开征求意见的通知等对于人脸识别信息的收集、使用、存储、共享的全生命周期做出了较为严格的规定，需要企业参照遵守。

总体来说，处理人脸识别信息需遵循处理个人信息的一般规定，必须符合“合法、正当、必要”三原则。其中，处理人脸识别数据时应遵循最小必要原则，应当满足非人脸识别方式安全性或便捷性显著低于人脸识别方式的条件，并且应同时提供非人脸识别的身份识别方式供选择使用。此外，应提供安全措施保障个人的知情同意权。

在收集上，收集人脸识别信息前，应单独向个人信息主体告知收集、使用人脸识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。同时，人脸识别信息应仅收集和使用摘要信息，避免收集其原始信息。在自然人拒绝使用人脸识别功能或服务后，不应频繁提示以获取自然人对人脸识别方式的授权同意。此外，《数据安全管理办法（征求意见稿）》还规定，网络运营者以经营为目的收集人脸识别信息的，应向所在地网信部门备案。

在使用上，企业应在完成验证或辨识后立即删除人脸图像，应生成可更新、不可逆、不可链接的

人脸特征，应具备防护呈现干扰攻击的能力，在本地和远程人脸识别方式均适用时，应使用本地人脸识别。同时，人脸识别数据不应用于除身份识别之外的其他目的，包括但不限于评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等。此外，原则上不应使用人脸识别方式对不满十四周岁的未成年人进行身份识别。

在存储上，人脸识别信息应与个人身份信息分开存储。原则上不应存储原始人脸识别信息（如样本、图像等），可采取的措施包括但不限于：

- 仅存储人脸识别信息的摘要信息；
- 在采集终端中直接使用人脸识别信息实现身份识别、认证等功能；
- 在使用人脸识别信息实现识别身份、认证等功能后删除可提取人脸识别信息的原始图像。

在共享上，人脸识别信息不应公开披露，原则上不应共享、转让。因业务需要，确需共享、转让的，应单独向个人信息主体告知目的、涉及的人脸识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。并且，人脸识别信息原则上不应进行委托处理，确需委托处理的，应在委托处理前审核受委托者的数据安全能力，并对委托处理行为开展个人信息安全影响评估。

在数据出境上，原则上在我国境内收集或产生的人脸识别数据应在我国境内存储。因业务需要确需出境的，应按照个人信息出境相关规定进行安全评估。此外，《个人信息出境安全评估办法（征求意见稿）》还规定个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估。

总之，企业需在人脸识别信息收集、使用、存储、共享的全生命周期遵守法律法规和国家标准的相关规定，如“人脸识别第一案”一审法院所述，在前端收集个人信息阶段需要遵循“合法、正当、必要”的原则和征得当事人同意的规则，在中端控制信息过程中需要遵循确保安全原则，不得泄露、出售或者非法向他人提供个人信息，在末端出现个人信息被侵害之时，企业依法需要承担采取补救措施等相应的侵权责任。在发生或者可能发生人脸识别数据泄露、损毁、丢失的情况时，应立即采取补救措施，按照规定及时告知数据主体，并向相关主管部门报告。

四、合规建议

目前政府部门对于人脸识别信息的收集使用高度重视，针对人脸识别的相关法律法规和国家标准将陆续出台，例如《个人信息保护法（草案二次审议稿）征求意见》中特别指出，针对人脸识别等新技术、新应用，制定专门的个人信息保护规则、标准，由国家网信部门统筹协调有关部门依据本法推进相关工作。同时，社会公众对于人脸识别信息的关注度也大幅提高。面对目前较为严格的监管动态，企业可以采取以下措施加以应对：

1、充分了解人脸识别信息的相关法律法规和国家标准，在收集、使用、存储、共享的全生命周期流程上均需严格遵守相关规定，确保“合法、正当、必要”，同时应采取安全措施确保数据主体权利，包括但不限于获取人脸识别数据使用情况、撤回授权、注销账号、投诉、获得及时响应等。此外，企业应注意需同时提供非人脸识别的身份识别方式供选择使用。

2、就人脸识别信息的处理，积极建立完善公司对外业务以及内部规范的相关制度，建立相关内部控制制度，促使员工在处理人脸识别信息的相关业务中遵守相应制度规定。

3、如果通过App进行人脸识别信息的处理，那么应当进一步遵循App相关的法律法规。（相关内容请详见App合规系列文章，如《App合规系列——企业可以收集哪些个人信息（兼论必要原则）》、《App合规系列——企业收集使用个人信息时如何取得同意》等）

4、企业应具备与其所处理人脸识别数据的数量规模、处理方式等相适应的数据安全防护和个人

信息保护能力，例如企业应当积极开展网络安全等级保护工作，按照相应的级别开展相应的等级测评、制度建立、开展自查、备案报告等工作，为人脸识别信息的处理打好数据安全防护基础，确保数据安全（相关内容请详见《新基建浪潮下企业开展网络安全等级保护的关注要点》）。

5、持续关注人脸识别信息方面的法律法规、国家标准出台、生效情况和相应监管动态，根据政府部门的监管动向随时调整自身处理人脸识别信息的制度规范。例如在小区物业的人脸识别上，杭州、四川等地方相继修订发布物业管理条例草案，拟将“不得强制业主通过指纹、人脸识别等生物信息方式使用共用设施设备”纳入条例。诸如此类立法动向值得智慧安防、智慧社区业务的企业重点关注。

结语

大数据让生活越来越方便，但任何技术都不应背离以人为本的原则。“人脸识别第一案”体现了个人信息主体对于个人信息保护关注度的提升，社会公众对于人脸识别信息的重视度日益增加；也体现了司法层面对于个人信息的保护，已充分关注到企业收集使用个人信息必须遵守“合法、正当、必要”三原则；同时也为企业敲响了警钟，提醒企业在收集使用个人信息的业务中应当更加注重合法合规，收集使用人脸识别信息必须遵守合规要求，防止因处理个人信息不当造成企业风险，防止因此而陷入民事诉讼或行政处罚乃至牵涉到刑事责任。

杨锦文　合伙人　电话：86 10 8553 7608　邮箱地址：yangjw@junhe.com
高　健　律　师　电话：86 10 8519 1359　邮箱地址：gaojian@junhe.com
李圆圆　律　师　电话：86 10 8540 8665　邮箱地址：liyuanyuan@junhe.com