ICS 03.100.01

CCS A01

**团 体 标 准**

零售行业人脸识别技术应用指南

Face recognition technology in retail industry usage guideline

（征求意见稿）

|  |
| --- |
|  |
|  |

T/CCFAGS 0XX—2022

发布

中国连锁经营协会

XXXX-XX-XX 发布 XXXX-XX-XX 实施

 中国连锁经营协会 发布

目次

[前言 3](#_Toc102840075)

[1 范围 4](#_Toc102840076)

[2 规范性引用文件 4](#_Toc102840077)

[3 术语和定义 5](#_Toc102840078)

[3.1 人脸信息 face information 5](#_Toc102840079)

[3.2 人脸图像 face image 5](#_Toc102840080)

[3.3 人脸特征 face feature 5](#_Toc102840081)

[3.4 人脸识别 face recognition 5](#_Toc102840082)

[3.5 人脸识别数据 face recognition data 6](#_Toc102840083)

[3.6 人脸识别数据的处理 process face recognition data 6](#_Toc102840084)

[3.7 数据主体 data subject 6](#_Toc102840085)

[3.8 验证 authentication 6](#_Toc102840086)

[3.9 辨识 identification 6](#_Toc102840087)

[3.10 零售 retailing 6](#_Toc102840088)

[3.11 零售行业 retail industry 6](#_Toc102840089)

[3.12 零售场所 retail premises 6](#_Toc102840090)

[3.13 零售客户 retail customers 6](#_Toc102840091)

[3.14 不良行为 bad behavior 7](#_Toc102840092)

[4 人脸识别技术应用的能力要求 7](#_Toc102840093)

[4.1人脸识别技术应用功能要求 7](#_Toc102840094)

[4.2人脸识别技术安全和性能要求 9](#_Toc102840095)

[5 人脸识别技术应用的数据保护 11](#_Toc102840096)

[5.1人脸识别数据的采集 11](#_Toc102840097)

[5.2 人脸特征数据的传输、存储和删除 12](#_Toc102840098)

[5.3人脸识别数据的使用 13](#_Toc102840099)

[5.4人脸识别数据的委托处理、共享、转让、公开披露 14](#_Toc102840100)

[6 人脸识别技术应用的应急响应 15](#_Toc102840101)

[6.1应急预案和演练 15](#_Toc102840102)

[6.2应急处置 15](#_Toc102840103)

参考文献.....................................................................16

前言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》及中国连锁经营协会的行业标准规定起草。

本标准由中国连锁经营协会提出并归口。

本文件起草单位：中国连锁经营协会、上海盒马网络科技有限公司、沃尔玛（中国）投资有限公司、阿里巴巴集团控股有限公司、星巴克企业管理（中国）有限公司、福建冠业投资发展有限公司、上海悠络客电子科技股份有限公司、北京文安智能技术股份有限公司。

本文件主要起草人： 彭建真、白美蓉、焦伟、江宇烨、王炎、彭骏涛、张文文、余莲斌、贾娅玲、李炯、温贵华、周仁东、陈剑鸣。

零售行业人脸识别技术应用指南

1.范围

本标准规定了零售连锁企业在零售场所，使用人脸识别技术工作中的相关术语定义和技术应用指南，包括总体要求、规范设备技术运用、数据采集、安全维护及日常管理。

本标准适用于零售连锁企业开展人脸识别技术应用的相关管理工作，特指线下有店铺零售业态，包括便利店、超市、折扣店、仓储会员店、百货店、购物中心、专业店、品牌专卖店、集合店、无人值守商店等10种零售业态。

2.规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 信息安全技术 人脸识别数据安全要求 ——征求意见稿状态，尚未正式发布

GB/T 41479-2022 信息安全技术 网络数据处理安全规范

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 40660-2021信息安全技术 生物特征识别信息保护基本要求

GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB 37300-2018 公共安全重点区域视频图像信息采集规范

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 25724-2010 安全防范监控数字视音频编解码技术要求

GB/T 31488-2015 安全防范视频监控人脸识别系统技术要求

GB 5018-2011 民用闭路监视电视系统工程技术规范

GB/T 28449 信息安全技术 信息系统安全等级保护

GB/T 22239 信息安全技术 信息系统安全基本要求

GA/T 893-2010 安防生物特征识别应用技术

GA/T 1127-2013 安全防范视频监控摄像机通用技术要求

GA/T 922.2-2011 安防人脸识别应用系统   第2部分：人脸图像数据

GA/T 1093-2013 出入口控制人脸识别系统技术要求

GA/T 1126-2013 近红外人脸识别设备技术要求

GA/T 1325-2017 安全防范 人脸识别应用 视频图像采集规范

GA/T 1344-2016 安防人脸识别应用 视频图像采集规范

GA/T 1326-2017 安全防范人脸识别应用 程序接口规范

GA/T 893-2010 安全防范生物特征识别应用术语

GB/T 18106-2021 零售业态分类

3.术语和定义

下列术语和定义适用于本文件。

3.1人脸信息 face information

含有特定人的面部特征的图片或视频，以及基于生物识别技术形成的人脸特征数据。

3.2人脸图像 face image

自然人脸部信息的模拟或数字表示。

3.3人脸特征 face feature

自然人的人脸图像提取的反映或标识个人的参数。

3.4人脸识别 face recognition

人脸识别是基于人的脸部特征信息进行身份识别的一种生物识别技术。

3.5人脸识别数据 face recognition data

人脸图像及其处理得到的，可单独或与其他信息结合识别特定自然人或特定自然人身份的数据。

3.6人脸识别数据的处理 process face recognition data

人脸识别数据的处理包括人脸数据的收集、存储、使用、加工、传输、提供、公开等。

3.7数据主体 data subject

人脸识别数据所标识的特定自然人。

3.8验证 authentication

将人脸信息与存储的特定个人的人脸信息进行比对（1:1比对），以确定特定个人是否为其所声明的身份。

3.9辨识 identification

将人脸信息与已存储的指定范围内的人脸信息进行比对（1:N比对），以分辨特定个人。

3.10零售 retailing

主要面向最终消费者（如居民等）的销售活动，生产资料的销售不作为零售活动。

注：零售定义参考 GB/T 18106-2021 第2章

3.11零售行业 retail industry

开展有店铺零售及无店铺零售等业态的行业。

注：零售业态范围参考 GB/T 18106-2021 第4章

3.12零售场所 retail premises

零售连锁企业有店铺零售业态开展零售活动的场所。

3.13零售客户 retail customers

零售连锁企业提供零售服务并出现在零售场所的消费者，是潜在的人脸识别主体。

3.14不良行为 bad behavior

零售场所发生的威胁人身安全、盗窃行为、危害食品安全、交易异常行为等安全风险情形。

4．人脸识别技术应用的能力要求

4.1人脸识别技术应用功能要求

4.1.1人脸识别技术应用场景

零售行业人脸识别技术应用于零售连锁企业零售场所预防公共安全事件、预防盗窃事件、预防食品安全事件、日常运营及员工管理场景。识别存在或疑似存在不良行为，以及用于识别食品生产安全作业及员工管理，如员工考勤、检查工作人员口罩帽子是否按要求佩戴、头发是否盘好、处理食品前后是否洗手、生熟食品加工器具是否分开使用、工作人员健康证是否过期，是否有陌生人闯入等场景。

零售行业人脸识别技术应用于上述场景应符合国家有关规定，宜通过公开设置的门店摄像头，对相关人员的面部信息进行采集，并根据情况保存有关记录，根据需要向公安等主管部门报告。比如：用于防盗损功能和顾客人身安全理赔保障取证功能时，人脸识别系统不应主动抓取人脸，但在顾客受伤进行保险理赔取证时，或者不良顾客出现疑似逃单、疑似偷盗等异常行为时，由安保人员通过人工操作（系统辅助）截取人脸，并在零售门店的视频系统中，回溯该顾客过往有无实施过类似行为，如果综合判断顾客有盗窃嫌疑的，则移送公安机关处理。

4.1.2人脸数据采集设备

零售行业人脸识别技术应用于上述场景时，应使用符合国家安全认证的安防摄像头或抓拍枪型相机等相关型号产品设备，选择使用的人脸识别系统宜符合国家网络安全等级保护标准。

零售场所作为公共区域，采用的人脸图像采集设备应符合GB 37300和GB/T 28181要求。

4.1.3人脸识别系统

零售行业人脸识别系统为满足上述场景要求，应具备如下基本功能：

4.1.3.1人脸质量评估

人脸识别系统应具有人脸质量判断能力，质量判断应至少包括以下几个方面：

人脸图像的分辨率

人脸图像的清晰度

人脸图像的完整度

人脸图像的表情

人脸图像的姿态

人脸图像的光照

4.1.3.2不良行为库

系统须具备不良行为人员的建档能力，建档数据项要支持包括：人脸图像、证据视频、会员ID、大致年龄、性别、严重等级、建档门店、建档时间。不良行为库支持同一企业法人主体下跨门店共享，存档有效期为三年，过期清除。

4.1.3.3预警跟踪

系统对不良行为人员到场可以及时、准确识别和预警，在提供人脸比对的基础上，具备位置信息和人体着装信息，以帮助安保人员辨识。在疫情防控戴口罩情况下，具备精准识别能力。

为提升安保人员工作效率，支撑现场追踪，系统可以在监控室通过视频自动追踪不良人员。

4.1.3.4回溯排查

在确认发现不良行为后，系统可以支持按照人脸或人体特征查询不良行为人历史到店记录，可回溯历史行为轨迹，并提供一键下载视频证据功能。

4.1.3.5实时找人

系统可以支持按照人脸或人体快速查询到目标人物的实时位置，以便快速定位目标人物（如人身安全意外、走丢、不良行为等）。

4.1.3.6员工识别

系统支持建立零售连锁企业员工人脸信息库，并支持与员工管理系统打通，对于员工进场及在场内活动，可根据管理需要识别员工身份、着装和行为规范等，并记录行为轨迹。

4.2人脸识别技术安全和性能要求

4.2.1安全预警及时性

人脸识别系统1:1身份验证和1:N身份辨识，从输入人脸图像到产出决策结果耗时需小于500毫秒。

4.2.2识别的准确性

a)1:1身份验证系统应满足在误识率0.1%时，识别正确率大于等于99%；

b)1:N身份辨识系统，具体指标要求：

对于人脸数据主体主动配合进行人像采集的场景，应满足识别底库N<=10W量级，误识率0.1%时，识别正确率大于等于98%

对于人脸数据主体非配合式即监控场景，应满足识别底库N<=10W量级，误识率0.1%时，识别正确率大于等于95%。

4.2.3人脸图像质量要求

人脸识别系统应根据相应的质量要求选取人脸数据用于人脸识别。

4.2.3.1 配合式人脸识别人脸质量要求

--人脸大小

 对于注册人脸图像，瞳间距应不小于60像素，宜大于90像素。

 对于识别人脸图像，瞳间距应不小于40像素，宜大于60像素。

--人脸清晰度

 对于注册人脸图像，运动模糊小于等于0.15，高斯模糊小于等于0.24。

 对于识别人脸图像，运动模糊小于等于0.2，高斯模糊小于等于0.25。

--人脸完整度

 对于注册人脸图像，几何失真应小于等于5%， 五官区域遮挡面积应小于50%。

 对于识别人脸图像，几何失真应小于等于10%，五官区域遮挡面积应小于60%。

--人脸图像的表情应合理，无夸张表情，如大笑、张大嘴等。

--人脸姿态

 对于注册人脸图像，旋转角应在$\pm 20°$以内，俯仰角应在$\pm 20°$以内，倾斜角应在$\pm 20°$以内。

 对于识别人脸图像，旋转角应在$\pm 20°$以内，俯仰角应在$\pm 20°$以内，倾斜角应在$\pm 20°$以内。

--人脸图像光照应均匀，对比度适中，脸部无明显阴影、无过曝或欠曝。

4.2.3.2 非配合式人脸识别人脸质量要求

--人脸大小

对于注册人脸图像，瞳间距应不小于40像素，宜大于60像素

 对于识别人脸图像，瞳间距应不小于30像素，宜大于60像素

--人脸清晰度

 对于注册人脸图像，运动模糊小于等于0.20，高斯模糊小于等于0.28

 对于识别人脸图像，运动模糊小于等于0.25，高斯模糊小于等于0.3

--人脸完整度

对于注册人脸图像，几何失真应小于等于5%， 五官区域遮挡面积应小于50%

 对于识别人脸图像，几何失真应小于等于10%，五官区域遮挡面积应小于60%

--人脸图像的表情应合理，无夸张表情，如大笑、张大嘴等

--人脸姿态

对于注册人脸图像，旋转角应在$\pm 30°$以内，俯仰角应在$\pm 30°$以内，倾斜角应在$\pm 30°$以内

 对于识别人脸图像，旋转角应在$\pm 45°$以内，俯仰角应在$\pm 45°$以内，倾斜角应在$\pm 45°$以内

--人脸图像光照应均匀，对比度适中，脸部无明显阴影、无过曝或欠曝。

4.2.4其它技术安全和管理要求

在验证和辨识过程中，应支持口罩、帽子等含遮挡人脸的识别，应仅反馈验证是否通过和自然人身份标识信息，应避免泄漏人脸特征信息和识别数据。

人脸识别技术应用于上述场景时，应保证自动化识别的透明性和公平性。

零售连锁企业应建立适用于人脸识别技术和数据管理需求的内部规范指引，明确人脸数据的安全防护措施和数据处理流程。应设立专职人员负责人脸数据的管理和维护，并定期开展风险评估。

5.人脸识别技术应用的数据保护

5.1人脸识别数据的采集

5.1.1采集原则

5.1.1.1告知同意和单独同意原则

在零售场所通过设备采集的人脸识别数据属于高度敏感信息，应用于预防公共安全事件、预防盗窃事件、预防食品安全事件、日常运营及员工管理场景时，零售连锁企业作为个人信息处理者应以显著方式向零售客户展示个人信息处理规则。显著方式通常是指在摄像头安装处的醒目位置悬挂警示标牌或张贴公告牌，同时告知获取人脸识别数据处理规则的途径，如二维码扫码告知、线下书面告知等。零售连锁企业所运营APP，如关联零售场所使用场景，应在隐私政策中明确说明人脸数据采集使用的范围、目的和用途。

如应用于熟客感知、人脸支付等智慧门店服务时，应征得零售客户的单独同意。零售连锁企业基于单独同意处理人脸信息的，不应使用一次概括授权、默认授权、与其他协议捆绑授权等方式获取零售客户的同意。

5.1.1.2最小必要原则

涉及人脸数据采集范围仅应用于维护公共安全，保障零售场所人员安全、食品安全、财产安全、营运安全所需。不应超出最小必要范围收集、使用零售客户的人脸信息，不应长期或永久保存人脸图像。

所有涉及人脸数据采集使用的产品，不应频繁采集人脸信息，应当采用收集用于生成人脸特征所需最小数量的人脸信息，并在可行的情况下向零售客户提供不收集人脸信息的方案。

5.1.1.3平等对待原则

平等对待客户主体，不应以确定宗教信仰、种族或民族、健康状况、遗传特征、政治观点、社会出身、经济状况等可能的歧视性目的收集客户人脸信息。

5.1.1.4公开透明原则

零售连锁企业处理人脸识别数据如使用算法，应在服务协议或隐私政策，向零售客户简明介绍算法的基本逻辑和对其权益的影响，不能通过自动化决策对零售客户个人在交易价格等交易条件实行不合理的差别对待。

5.1.2 采集方式

人脸信息采集的方式主要通过摄像机直接或间接抓拍、视频流截取、APP客户端业务场景识别等方式进行采集。采集的人脸数据可由零售连锁企业进行独立管理，如传送到第三方设备厂商平台或经过安全认证的云端服务器，应视同委托处理，具体要求参考5.4.1委托处理章节。

应用于线下商业流量统计、热力分析等客流分析场景，不应直接采集使用零售客户的人脸原图，应当采取无法识别个人身份且不能复原的的技术手段进行采集存储和统计分析，不应关联获取个人信息及商业化处理。

5.2 人脸特征数据的传输、存储和删除

5.2.1不应明文传输和存储

人脸信息在传输时应单独进行加密或混淆，并对两端的主体身份进行鉴别和认证，确保数据传输双方可信。人脸信息通过无线局域网络连接发送和接收通信时，需要采用可信的无线局域网协议。

人脸信息应进行加密或哈希存储，确保安全性和完整性。

5.2.3 单独存储

人脸信息应与个人身份信息应当通过逻辑隔离等方式分开存储并加强访问和使用的权限管理。

5.2.4 不存储原始人脸图像

除非有法律法规特别规定，原则上不应存储原始人脸图像。

5.2.5存储期限

基于法律规定保存原始人脸图像的，应当按照法律规定或者与零售客户协议的约定，设定最小化的保存期间，最长不宜超过3年，到期后删除人脸图像信息。

5.2.6本地化存储

在中华人民共和国或者其他司法管辖区境内收集或产生的人脸信息原则上应在本地存储。因业务需要确需出境传输、存储的，应当进行安全评估。

5.2.7 删除处理

零售连锁企业应建立删除人脸识别数据机制，当零售客户请求删除人脸识别数据时，应主动响应删除涉及相关个人人脸数据。人脸识别数据超出设定存储期限后，应当及时删除，仅可保留特征摘要信息。

5.3人脸识别数据的使用

5.3.1合法性基础

零售连锁企业人脸识别信息处理的合法基础，包括授权同意、为订立或履行个人作为一方当事人的合同所必需、履职必需、应对突发公共卫生事件、在合理的范围内处理已公开的信息、公益目的等，使用人脸识别数据信息时应优先采取保护个人权利和社会公共利益。除非有法律法规特别规定，原始的人脸图像应在完成验证、辨识等用途后立即删除。

5.3.2生成人脸特征

应生成可更新、不可逆、不可链接的人脸特征。可更新指从同一人脸图像可产生不同的人脸特征。当特定人脸特征泄露时，可重新生成不同的人脸特征。不可逆指无法从人脸特征恢复人脸图像。不可链接指根据同一人脸图像产生的不同人脸特征之间不具备关联性。

5.3.3抗干扰

针对无人值守时的配合式人脸识别系统，即人脸数据主体主动配合进行人像采集进行人脸识别的应具备防护呈现干扰攻击（活体检测）和注入攻击的能力。呈现干扰攻击包括使用人脸纸质照片、人脸屏幕照片、纸质面具、人脸视频、人脸合成动画、人脸三维面具等攻击和干扰人脸识别。

5.3.4本地数据优先

在本地和远程人脸识别方式均适用时，宜使用本地人脸识别，即优先在采集终端（边缘设备）完成人脸数据的采集和识别。

5.3.5产品管理平台使用要求

涉及人脸信息收集使用的产品管理平台，应当默认采用去标识化脱敏和水印背景等防护方式展示人脸信息，便于便于快速对泄漏的数据信息进行有效溯源。

5.3.6人脸数据使用的禁止性要求

零售连锁企业不应超出合理应用场景，私自采集、使用、加工、传输人脸识别中的个人信息数据，不应将所采集的数据通过网络平台或其它方式进行交易，不应提供或在公共区域公开披露人脸识别个人信息，禁止从事危害国家安全、社会安全、公共利益的人脸数据信息处理活动。

5.4人脸识别数据的委托处理、共享、转让、公开披露

5.4.1委托处理

因算法训练、模型开发等必要，委托其他公司或者第三方处理人脸信息的，应当征得零售客户的单独同意，并完成个人信息保护影响评估。评估前的准备包括：

(1)已就委托处理的目的如算法模型训练等向零售客户进行告知。

(2)已对第三方数据保护能力进行调查和评估，并与第三方签订数据委托处理协议。

5.4.2共享、转让

除法律、行政法规另有规定外，人脸信息原则上不应向第三方共享或转让。因业务需要，确需共享或转让的，应当征得零售客户的单独同意，完成个人信息保护影响评估。评估前的准备包括：

（1）已告知零售客户共享、转让的目的、接收方身份、联系方式、接收方数据安全能力、可能产生的影响等相关信息。

（2）单独授权同意需要单独告知零售客户其人脸信息共享或转让的目的、接收方身份、接收方数据安全能力、数据类别、可能产生的影响等相关信息。

（3）已对第三方数据保护能力进行调查和评估，并与第三方签订数据共享协议。

5.4.3公开披露

除非征得零售客户的单独同意，否则不得公开披露人脸信息，包括任何可能存在公开风险的场景等。

6.人脸识别技术应用的应急响应

6.1应急预案和演练

6.1.1应急预案

为防范网络攻击、侵入、干扰、破坏和非法使用以及意外事故，保障零售客户人脸信息安全，零售连锁企业应制定信息安全事件应急预案，并对应急预案进行定期更新。

6.1.2应急演练

零售连锁企业应按照应急预案，定期组织应急演练，以保障遇到紧急情况时，应急预案有效被执行。

6.2应急处置

6.2.1记录事件日志

发生针对人脸数据的信息安全事件后，零售连锁企业应根据应急响应预案记录事件内容。

6.2.2影响性评估及控制措施

评估人脸数据信息安全事件可能造成的影响，并采取必要措施控制事态，消除隐患。

6.2.3 上报和告知

按照有关规定，及时向有关部门上报事件情况，事件可能会给零售客户的合法权益造成严重危害的，应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的零售客户。

参考文献

[1] 《中华人民共和国个人信息保护法》，2021年11月1日实施。

[2] 《中华人民共和国民法典》，2021年1月1日实施。

[3] 《中华人民共和国网络安全法》，2017年6月1日实施。

[4] 《中华人民共和国数据安全法》，2021年9月1日实施。

[5] 《互联网信息服务算法推荐管理规定》，2022年3月1日实施。

[6] 《中华人民共和国消费者权益保护法》，2014年3月15日第2次修正实施。

[7] 《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》，2021年7月28日实施。