上海市公安局技术防范办公室

沪公技防〔2021〕5号　　签发人：单雪伟

关于印发《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）》的通知

各公安分局、市局有关单位技术防范办公室，各技防产品、工程检测机构，各技防从业单位，各技防专家：

根据《最高人民法院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》（法释〔2021〕15号）中对使用人脸识别技术处理个人信息的相关要求，为进一步规范本市安防工程中人脸识别技术的应用，确保公民权益不被侵害，我办组织相关企业、检测机构、专家等对《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）》（见附件，以下简称“《技术要求》”）进行了多次讨论研究。现将《技术要求》印发给你们，请遵照执行。

自2022年3月1日起，本市安全技术防范工程评审方案（以下简称“方案”）系统中使用带人脸识别技术的安防产品，除符合现行标准规范要求外，还应符合本《技术要求》要求（如相关要求有冲突，以本《技术要求》为准），原产品系统中不符合要求的安防产品不得在方案中继续使用。

特此通知。

附件:《本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）》

上海市公安局技术防范办公室

2021年12月13日

上海市公安局技术防范办公室　　2021年12月13日印发

附件：

本市安全防范涉及人脸识别应用产品及相关数据传输技术要求（试行）

1 应用范围

本要求规定了本市安全防范涉及人脸识别应用产品及相关数据传输（以下简称：人脸识别）的基本技术要求，是本市安全防范涉及人脸识别应用及相关数据传输产品选型、检测及工程设计、评审、验收的依据之一。

2 数据内容

本技术要求所涉及人脸识别的内容由人脸识别数据（含人脸图像、人脸特征）、个人身份信息及与之相关的智能分析结果数据等组成。

3 术语解释

本技术要求所涉及人脸识别的应用场景包括人脸验证、人脸辨识、人脸分析三类。

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。典型设备包括人员身份人像数据采集设备（系统）或由与其相关数据内容关联应用终端（含软件）所构成的系统等。

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。典型

设备包括出入口控制人脸识别装置（系统）或由与其相关数据内容关联应用终端（含软件）所构成的系统等。

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。典型设备包括人脸抓拍摄像机、人脸抓拍智能分析设备（系统）、智能人脸抓拍分析设备（系统）、人脸抓拍存储数字录像设备或由与其相关数据内容关联应用终端（含软件）所构成的系统等。

4 适用行业

4.1 人脸识别本地应用行业仅涉及《安全防范工程技术标准》（GB 50348）、《住宅小区智能安全技术防范系统要求》（DB31/T 294）、《单位（楼宇）智能安全技术防范系统要求》（DB31/T 1099）、《重点单位重要部位安全技术防范系统要求》（系列标准）（DB31/T 329.X）、《航空货运代理企业仓储场所安全技术防范系统要求》（DB31/T 512）等相关标准要求范围，无相关标准支持或职能部门要求不应配置及安装。

4.2 人脸识别联网应用服务仅涉及《公共安全重点区域视频图像信息采集规范》（GB 37300）等相关标准要求范围，无相关标准支持或职能部门要求不应配置及接入。

5 基本要求

5.1 人脸识别本地应用技术要求应符合《安全防范工程技术标准》（GB 50348）、《安全防范 视频监控人脸识别系统技术要求》（GB/T 31488）、《安防人脸识别应用系统 第2部分：人脸图像数据》（GA/T 922.2）、《出入口人脸系别系统技术要求》（GA/T 1093）、《安全防

范 人脸识别应用视频图像采集规范》（GA/T 1325）、《安防人脸识别应用 视频人脸图像提取技术要求》（GA/T 1344）、《安全防范人脸识别应用认证核验设备通用技术要求》（GA/T 1755）、《住宅小区智能安全技术防范系统要求》（DB31/T 294）、《单位（楼宇）智能安全技术防范系统要求》（DB31/T 1099）等相关标准要求。

5.2 人脸识别联网应用服务技术要求应符合《公共安全重点区域视频图像信息采集规范》（GB 37300）等相关标准要求。

5.3 人脸识别信息安全要求应符合《信息安全技术 信息系统通用安全技术要求》（GB/T 20271）、《信息安全技术 个人信息安全规范》（GB/T 35273）、《信息安全技术 生物特征识别信息保护基本要求》、《信息安全技术 网络数据处理安全规范》等相关标准要求。

6 人脸识别应用技术要求

6.1 人脸验证和人脸辨识

6.1.1 人脸验证和人脸辨识收集人脸识别数据时，应向被收集者告知收集规则，包括但不限于收集目的、数据类型和数量、处理方式、存储时间等，并征得被收集明示同意。

6.1.2 人脸验证和人脸辨识应仅收集用于生成人脸特征所需的最小数量、最少图像类型的人脸图像，人脸验证应在完成验证后立即删除证件原始图像，人脸辨识在完成辨识后应立即删除人脸图像。

6.1.3 人脸验证和人脸辨识应生成可更新、不可逆、不可链接的人脸特征：

a）可更新：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；

b) 不可逆：无法从人脸特征恢复人脸图像；

c) 不可链接：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。

6.1.4 人脸验证和人脸辨识应具备包括使用人脸照片、纸质面具、人脸视频、人脸合成动画等防假体攻击能力。

6.1.5 人脸验证和人脸辨识应采用物理隔离或逻辑隔离方式分别存储人脸识别数据和个人身份信息，数据使用期限到期应自动删除人脸识别数据或进行匿名化处理。

6.2 人脸分析

6.2.1 人脸分析不应开展人脸验证或人脸辨识应用，如需结合人脸验证和人脸辨识的人脸特征数据、个人身份信息实现智能分析应用的，建设单位或使用单位在采用人脸验证和人脸辨识收集人脸识别数据时，应向被收集者告知收集规则，包括但不限于收集目的、数据类型和数量、处理方式、存储时间等，并征得被收集者明示同意。

6.2.2 人脸分析应仅收集用于生成人脸特征所需的最小数量、最少图像类型的人脸图像，应具有连续去重和间断去重处理功能。

a) 连续去重的最小时间单位为秒。在连续抓拍过程中，抓拍去重后输出人脸图像应包括首尾人脸或最优人脸等。

b) 间断去重的最小时间单位为分。在非连续抓拍过程中，抓拍去重后输出人脸图像应包括首尾人脸或最优人脸等。

6.2.3 人脸分析通过统计、检测或特征的智能分析应实现禁行闯入、异常滞留、异常徘徊、出现异常等预警提示应用。

6.2.4 人脸分析应采用物理隔离或逻辑隔离方式分别存储人脸图

像和人脸特征。数据使用期限到期应自动删除人脸识别数据。

7 人脸识别数据传输要求

7.1 人脸识别应采用数据结构独立的专用网络（可采用 VLAN 的独立网段），应对系统中所有接入设备的网络端口予以管理和绑定。

7.2 人脸识别相关数据内容关联应用终端的所有 USB 端口应采用可通过出入口控制系统授权刷卡认证的 USB 防拔插设备予以绑定管理，并不应通过互联网与其他应用实现实时联网。

7.3 人脸验证和人脸辨识在采集端完成人脸识别数据采集并在服务器端完成人脸识别的，系统建设应满足《信息安全技术远程人脸识别系统技术要求》（GB/T 38671）的相关要求。

7.4 人脸识别由与其相关数据内容关联应用终端（含软件）所构成系统的，系统建设应满足《信息安全技术远程人脸识别系统技术要求》（GB/T 38671）相关要求。

7.5 除用于维护所提供的产品或服务的安全稳定运行所必须，以及智能分析结果数据外，人脸识别数据、个人身份信息不应在智能集成数据服务设备、智能安防集成应用系统体现或展示，对确有除此以外应用需求的，系统建设应满足《信息安全技术 远程人脸识别系统技术要求》（GB/T 38671）的相关要求。