

上海市地方标准

《公共场所人脸识别分级分类应用指南》

编制说明

一、任务来源

根据《上海市标准化条例》、《上海市地方标准管理办法》，由上海华东电信研究院提出立项，经上海市市场监管局评审、公示，于2021年6月16日，《公共场所人脸识别分级分类应用规范》列入2021年第二批上海市地方标准修订项目计划（沪市监技标〔2021〕341号）。项目由上海市经济和信息化委员会提出并组织实施，上海市人工智能标准化技术委员会归口，上海华东电信研究院、上海市质量和标准化研究院、上海依图网络科技有限公司、上海商汤智能科技有限公司、上海市人工智能行业协会等单位共同起草。

二、背景情况

人脸识别是基于人的脸部特征信息进行身份识别的一种技术，是人工智能领域发展最成熟、应用范围最广的技术之一。随着人脸识别算法技术不断优化、技术成熟度快速提升，人脸识别在人们生活中的应用逐渐深入，人脸识别成为了人工智能应用落地最快最广泛的领域之一。在人脸识别为人们生活、工作带来便利的同时，也出现了技术滥用、隐私安全等问题，引发社会广泛关注。

近几年，人脸识别已在安防、交通、金融、教育、支付等领

域已得到了广泛应用，逐渐深入到人们生活的方方面面。如新冠肺炎疫情爆发后，人脸识别和智能测温技术在疫情防控和为有关部门提供人员信息方面起到了重要支撑作用。然而在一些公共场所的场景下，一些不规范的应用仍然导致不少问题，人脸识别技术有被滥用、监管缺失之嫌，比如侵犯消费者隐私、过度采集或者滥用、泄露个人生物特征信息等，造成了恶劣的社会影响。

2021 年初，时任上海市委书记李强提出规范本市人脸识别技术应用的批示要求。同时，随着《个人信息保护法》、《数据安全法》、《网络安全法》、《民法典》等相关法律法规的出台，在开展人脸识别业务时必须充分保障个人信息主体的权益，为用户带来更多的安全性、便捷性，提高用户办事效率的同时，也不能侵害个人信息主体的利益。所以在保障个人信息安全的前提下，通过规范公共场所人脸识别应用原则和相应管理要求，不仅具有普遍的社会意义，也能够促进人脸识别行业健康有序发展。

本标准项目组根据《个人信息保护法》、《数据安全法》等相关法律法规和标准规范的要求，聚焦于公共场所人脸识别系统建设前的分级分类评估及其应用要求。在明确公共场所人脸识别应用基本原则的基础上，对公共场所不同人脸识别应用场景进行分类，并根据人脸识别应用目的、底库规模等风险因素进行综合风险值评估，进而对公共场所人脸识别应用进行风险分级，并基于分级分类针对性地提出应用和管理方法，为规范应用人脸识别技术、保护公民隐私、促进行业发展提供支撑。

三、编制过程

本标准的修订主要包括以下几个阶段：

（一）立项准备阶段（2021 年 2 月—2021 年 3 月）

2021 年初，上海市经济和信息化委员会人工智能发展处召集相关单位组成标准编制项目组，项目组于 2021 年 2 月召开首次工作会议，讨论并确定本项目的重点任务、工作计划和任务分工。确定了由上海华东电信研究院、上海市人工智能行业协会、上海市质量和标准化研究院、上海依图网络科技有限公司、上海商汤智能科技有限公司组成的标准起草小组。

随后，项目组系统查阅和梳理了关于人脸识别风险防控的国内外文献以及相关标准，并进行预调研，深入分析了上海本地人脸识别的应用情况和风险现状，初步形成《公共场所人脸识别分级分类应用规范》的设计思路。

（二）标准起草（2021 年 3 月—2021 年 4 月）

2021 年 4 月份召开了项目推进会议，根据前期准备工作进一步明确本项目的具体方案和实施路径。在起草小组的通力合作下，初步确立了标准框架。工作组内部多次召开研讨会，讨论完善框架内容并初步确立了标准要素，并据此起草了标准草案。

（三）立项申请阶段（2021 年 4 月—2021 年 6 月）

项目组完成《上海市制修订地方标准项目建议书》和《公共场所人脸识别分级分类应用规范》标准草案，正式立项并完成立项答辩。经上海市市场监管局评审、公示，2021 年 6 月项目获

批。

同时，项目组广泛征集参与单位，邀请公安部第三研究所、上海计算机软件技术开发中心、上海市大数据中心、华东师范大学、同济大学法学院、中国社科院、上海交通大学、上海人工智能实验室等单位的专家参与标准的编制和讨论，开展了更广泛的理论研究和实际调研，形成了较为科学的标准框架和主要内容。

（四）集中编写和讨论阶段（2021 年 7 月—2022 年 12 月）

项目组按照 GB/T 1.1—2020 的最新要求，进一步完善了标准草案内容并撰写了《地方标准编制说明》，组织了多轮内部讨论会，以专家学者、业务骨干座谈会以及企业调研等形式进行深入调研和讨论，进一步提升了标准内容的科学性和可操作性，形成标准征求意见稿。

（五）征集意见阶段（2023 年 1 月—2023 年 10 月）

项目组、项目提出单位、人工智能标委会面向相关主管部门、技术机构、高校、社会公众等相关主体，开展线上、线下相结合，会议、访谈、问卷等多种形式的公开意见收集，其中：

- 发送“征求意见稿”的单位数：31 个。
- 收到“征求意见稿”后，回函的单位数：17 个。
- 收到“征求意见稿”后，回函并有建议或意见的单位数：9 个。
- 没有回函的单位数：14 个。

- 标委会网络系统专家给出建议和意见数：0 个。

根据相关意见，项目组进一步完善标准内容，形成了标准送审稿。

（六）送审稿阶段（2023.10 月）

2023 年 10 月 31 日上海市市场监督管理局组织召开了本标准的审定会，与会专家听取了标准起草组关于标准编制说明，标准技术内容和征求意见汇总与处理的汇报，并对标准送审稿进行逐条审议，提出了相关意见建议，并提出将标准名称变更为《公共场所人脸识别分级分类应用指南》。项目组采纳了全部意见，并对相关内容进行了完善。

四、标准编制原则

（一）规范性原则

标准内容符合国家和本市现行法律、法规和规范性文件以及上海市市场监督管理局的相关方针政策。

（二）科学性原则

标准科学性体现在项目成员构成、标准内容和研制过程三个方面。一是标准项目组组织了哲学、伦理、法学、公共安全、人脸识别技术、人脸识别技术应用等领域的专家学者，从不同维度对标准内容进行充分广泛的讨论，以保证本标准立场的公平性和科学性；二是本标准的风险评估方法通过广泛讨论确定，具体涉及的参数也是通过广泛调研、资料查询、专家座谈会获取，体现了标准内容编制方法论的科学性；三是标准的修订过程严格遵循

上海市地方标准制修订程序，坚持问计于民，广泛召开座谈会、深入开展调研，确保标准修订过程的科学性。

（三）系统性原则

本标准系统性地考虑了公共场所人脸识别应用事前、事中、事后的管理闭环，立足于事前评估管理的基本定位，按照系统性原则，与事中、事后管理需求紧密联系，形成系统性方案。

（四）实用性原则

本标准提出的人脸识别分级分类评估方法立足实际，考虑评估依据的可获取性和方法的可操作性，为公共场所人脸识别事前风险评估提供技术支撑，具备较强的实用性。

五、标准的主要技术内容

本标准以“分类分级”为总体思路，在对公共场所进行“分类”的基础上，进一步对人脸识别应用风险进行“量化”，并结合 2 个维度的分析结果，构建人脸识别技术在公共场所应用的“分级”方法，提出不同应用场景下的分类分级方法，主要架构分为“基本原则”、“分级分类方法”、“应用方法”和“附录”等部分。

本标准旨在为公共场所人脸识别技术的应用提供一个明确的框架，确保技术的应用既能够满足社会管理的需求，又能够保护个人隐私和数据安全，同时符合法律法规的要求。通过制定和实施这些标准，可以促进技术的健康发展，增强公众对人脸识别应用的信任。

（一）基本原则

《个人信息保护法》、《数据安全法》、《网络安全法》以及《民法典》等相关法律法规的出台，为公共场所人脸识别技术的应用提供了法律依据和规范框架。这些法律法规共同构成了个人信息保护和数据安全的法律体系，确保了个人信息的合法收集、处理和使用，强化了数据安全和网络安全的保护措施，以及明确了个人信息主体的权利和义务。基于此项目起草组认为，在公共场所应用人脸识别技术时，必须遵守这些法律法规的要求，以保护个人隐私和数据安全，维护网络空间的秩序和安全。在应用层面的分级分类原则条款制定时，需要强调：一是在收集和使用个人人脸信息时必须遵循合理性原则，确保信息收集的最小必要性、目的明确性和一致性；二是良性发展原则，要求系统建设和应用的公开透明性和准入控制；三是权责一致原则，确保信息处理者明确并承担相应责任；四是安全性原则，强调事前风险评估、事中安全保障和事后追溯机制；五是未成年人保护原则，要求在处理未成年人信息时获得监护人同意并采取特殊保护措施。这些原则共同构成了确保人脸识别技术合法、合规且安全应用的框架。

（二）分级分类方法

1. 人脸识别公共场所分类

在标准研制阶段，标准编制组认为，鉴于人脸识别技术具有非接触性、隐蔽性等特点，公众在人脸识别技术面前实际上是完全暴露，开放程度相同（100%），因此人脸识别分级分类应用从

“使用主体”角度来划分相对比较科学。一般而言，政府社会管理（to Government，简称 toG）相关使用主体要求更加严格规范；商业相关行业应用（to Business，简称 toB）主体的个人信息保护意识和管理水平相对较弱；公众服务（to Customer，简称 toC）相关主体能力介于前述二者之间，暂可认为与商业（toB）相当。经组织企业座谈和专家讨论，将公共场所应用人脸识别的常见应用场景分为社会管理、行业应用、其他三类。社会管理包括公共安全、司法、政务、公共服务、交通以及其他具有社会管理属性的细分场景；行业应用包括金融、医疗、教育、建筑、房地产、商业、娱乐等细分场景；其他包括社区和园区等细分场景。

2. 综合风险值评估

公共场所实施人脸识别时宜充分考虑的风险要素包括五项：应用目的风险、底库规模风险、覆盖密度风险、管理水平风险和网络环境风险，见表 1。

表 1：人脸识别应用要素风险评估表

风险要素		风险值参考 取值范围
应用目的 (M)	安全防范	1~3
	人员管理	2~4
	商业分析	3~5
	娱乐体验	4~5
底库规模	0~1000 人	1~2

(D)	1000~10000 人	2~3
	10000 人及以上	3~5
覆盖密度 (F)	0~50 路/平方公里	1~2
	50~100 路/平方公里	2~3
	100 路/平方公里以上	3~5
管理水平 (G)	政策和制度、机构和人员管理水平、风险管理等方面水平分别达到或超过 GB/T 20269—2006 6.3.2、6.3.3、6.3.4 的相关要求	1~3
	政策和制度、机构和人员管理水平、风险管理等方面水平分别达到 GB/T 20269—2006 6.2.2、6.2.3、6.2.4 的相关要求	2~4
	政策和制度、机构和人员管理水平、风险管理等方面水平分别达到 GB/T 20269—2006 6.1.2、6.1.3、6.1.4 的相关要求	3~5
网络环境 (W)	政府专网或离网	1~3
	局域网	2~4
	公网	3~5

标准项目组邀请了来自权威产业研究机构、人脸识别研发头

部企业、人脸识别应用单位、高校等 17 家单位参与讨论，采用层次分析赋权法，计算出各影响要素的权重，构建出的“人脸识别应用综合风险值”计算方法见公式(1)。标准编制过程中组织了超过十次的全体或核心讨论会议、发起了多次企业沟通和专家座谈、进行了两次次问卷调研，从而确定了各项风险要素宜采用的取值范围可参考下表。

$$R = 0.28M + 0.17D + 0.12F + 0.23G + 0.20W \dots\dots (1)$$

式中：

R——表示综合风险值；

M、D、F、G、W——分别表示五个单项风险得分。

3. 公共场所人脸识别应用风险分级

标准编制组借鉴风险评估矩阵方法，综合考虑上述“公共场所分类”和“人脸识别应用综合风险值”2大维度，将“公共场所人脸识别应用风险等级”划分为5级，如图 1 所示。其中，绿色（A）代表低风险，青色（B）代表中低风险，黄色（C）代表中风险，棕色（D）代表中高风险，红色（E）代表高风险。

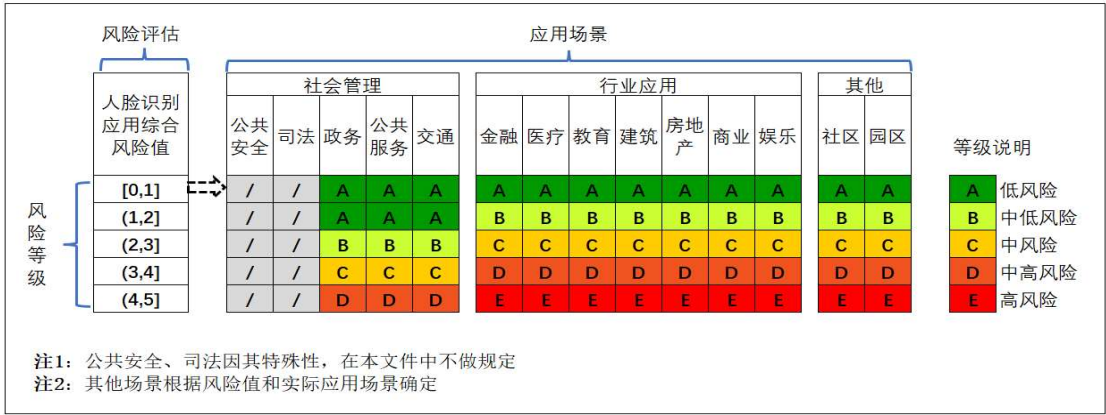


图 1：公共场所人脸识别应用风险分级

（三）分级分类应用方法

1. 应用概述

公共场所人脸识别应用宜遵循最小必要原则，具体分级如下：
A 级（低风险）：认可使用；B 级（中低风险）：允许使用；C 级（中风险）：适度使用；D 级（中高风险）：审慎使用；E 级（高风险）：不应使用。鉴于当前社会管理领域人脸识别使用主体一般具有较高的管理和技术水平，因此对于风险等级总体上进行了降档处理。公共安全、司法场景不做讨论。另外，需要强调的是高风险（E）等级，不应开展人脸识别应用。

2. 应用主体条件

公共场所应用人脸识别需考虑各应用主体条件，包括使用主体、实施主体以及其他服务提供方。虽然人脸识别应用风险等级有高低之分，但对于人脸识别应用的使用和实施主体而言，有一些管理要求是共性的、基础的。

（1）对于使用主体而言，首先人脸识别系统的使用主体具有良好的信用情况；其次应按照《个人信息保护法》、最高法关于人脸识别的司法解释等上位法要求，获得人脸识别对象的正式同意授权、在显著位置设置采集提示标识；再次宜参照 GB/T 20269—2006《信息安全技术信息系统安全管理要求》要求，做好组织的策略和制度、机构和人员管理、风险管理等方面的要求；最后，宜采用必要的安全技术确保系统和数据安全，并建立相应的应急预案对使用中的危险行为进行溯源。

(2) 对于实施主体而言，系统集成商和供应商宜通过质量管理体系认证和信息安全管理体系认证，并取得符合国家或行业要求的信息安全管理体系相关资质证书，以及根据业务需求所需的特定资质证书。信息安全工程管理要求参考 GB/T 20282—2006 的规定。

(3) 其他服务提供方管理参考 GB/T 32914—2016 的规定。

3. 实施环节及措施

人脸识别涉及的环节较多，因此有必要按照《个人信息保护法》、GB/T 35273—2020 等法规、标准规范的要求，逐一对收集、传输、存储、使用、删除等环节的要求进一步细化。应用人脸识别逐一考虑这些环节可采取的技术措施，以及各环节的个人信息主体、使用主体、人脸识别系统技术提供者或设备供应商等主体的权限和责任。

4. 不同应用等级建议采取的措施

不同应用等级建议采取的措施从“风险管理”、“抗攻击能力”、“安全管理制度”、“安全管理组织”、“安全管理人员”、“安全计算环境”、“环境和资源”、“监督和检查管理”八个维度考虑，风险水平越高对应越严格的措施。

(四) 附录

附录 A 提供了一个关于公共场所人脸识别应用的分类说明，这有助于理解和指导不同场景下的人脸识别技术应用。它包括了场所的名称、应用目的、必要性分析以及可能的替代方案，为人

脸识别技术的分级分类应用提供了实用的指导。

六、与国内外同类标准技术内容的对比情况

经查询，国内外标准主要是从产品端开展，对于应用端特别是涉及公共利益、应用场景复杂的公共场所，并没有给出相关的应用规范。例如 IEEE Std 2790—2020《生物特征识别活体检测标准》、GB/T 41819—2022《信息安全技术 人脸识别数据安全要求》、GB/T 41772—2022《信息技术 生物特征识别 人脸识别系统技术要求》以及 GA/T 1470—2018《安全防范 人脸识别应用 分类》等。这些标准均是在产品端提供了详尽的技术规范，它们在教育应用层面，尤其是针对那些涉及公共利益且应用场景复杂的公共场所，尚未提供充分的应用规范。《公共场所人脸识别分级分类应用指南》则聚焦于公共场所用人脸识别系统的应用场景分类、事前应用风险评估需考虑的因素、应用中需考虑的责任主体和实施环节及措施等，旨在为公共场所人脸识别技术的应用提供明确的指导，与相关标准并无冲突。

七、与有关法律、行政法规及相关标准的关系

本标准作为推荐性标准，制定的内容符合各类法律法规要求。经检索，该标准为上海首创，无相关国外标准、国家标准以及行业标准。本标准可与其他人脸识别相关的国家标准、行业标准、地方标准等协调使用。

八、重大分歧意见的处理经过和依据

无。

九、实施标准的措施建议

本标准发布后将尽快组织宣贯，加大贯彻实施力度。第一，在适用主体中推广应用该标准，开展公共场所人脸识别分级分类应用试点示范，形成经验；第二，根据试点经验，推动标准在应用人脸识别的公共场景中的实施，切实提升公共场所人脸识别应用安全；第三，广泛收集意见和建议，及时归纳和总结，并不断完善标准，必要时提出标准修订。

十、其他应当说明的事项

无。