Open Journal of Legal Science 法学, 2022, 10(5), 814-822
Published Online September 2022 in Hans. http://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2022.105104

Hans汉斯

多维视角下小区门禁人脸识别系统的风险防范研究

姜含叶，孔静婷

宁波大学法学院，浙江 宁波

收稿日期：2022年7月22日；录用日期：2022年8月12日；发布日期：2022年9月8日

摘　要

人脸识别技术以其高效准确的技术特征推动其逐步应用于小区门禁系统，就此物业部门等收集主体需要收集业主面部信息加以处理。其中体现的业主知情权、表决权以及人脸信息至关重要的信息安全随之成为了保护难点。本文立足人脸识别门禁系统的业主、物业及政府三方视角，探讨小区门禁应用人脸识别系统中存在的各类问题及产生原因，基于此，应当切实保障业主知情权表决权，规范物业的告知义务与决策程序，推动政府加强数据库建设并加强信息安全监控，以期为人脸识别门禁系统提供更为完善有效的风险防护。

关键词

人脸识别，门禁系统，个人信息保护，表决权

Research on Risk Prevention of Face Recognition System of Entrance Guard in Residential Area from Multi-Dimensional Perspective

Hanye Jiang, Jingting Kong

Law School, Ningbo University, Ningbo Zhejiang

Received: Jul. 22nd, 2022; accepted: Aug. 12th, 2022; published: Sep. 8th, 2022

Abstract

Facial recognition technology is gradually applied to the community access control system with its

文章引用: 姜含叶, 孔静婷. 多维视角下小区门禁人脸识别系统的风险防范研究[J]. 法学, 2022, 10(5): 814-822.
DOI: 10.12677/ojls.2022.105104

efficient and accurate technical characteristics. In this regard, collection entities such as property departments need to collect the owner's facial information to deal with it. The information security of the owner's right to know, voting right and face information, which is very important, has become a protection difficulty. Based on the perspective of the owner, property and government of the facial recognition access control system, this paper discusses various problems and causes in the application of the facial recognition system for community access control. Based on this, it is necessary to effectively protect the owner's right to know and vote, and standardize the property's notification obligations and decision-making procedures, to promote the government to strengthen database construction and strengthen information security monitoring, in order to provide more complete and effective risk protection for the face recognition access control system.

Keywords

Facial Recognition, Access Control System, Personal Information Protection, Voting Rights

1. 引言

随着人工智能技术的日益突破，人脸识别技术的数据处理能力和识别准确率大为提升，逐渐走进人们的生活领域乃至小区门禁系统。人脸识别由于具有非接触性、不需要特定介质即可完成验证的特点，相比传统刷卡门禁方式它方便了使用者的识别操作，也减少了疫情期间的接触传播。但是，小区安装使用人脸识别门禁系统后，虽然物业可能会另外预留刷门禁卡的通道，但居民若想实现无卡自由进入小区，就需要向物业部门提供自己的人脸信息，此时信息泄露、信息滥用等风险接踵而至。同时，物业安装人脸识别门禁是否需要经得业主同意，采用何种表决程序等问题也为小区业主带来诸多疑惑。

这种忧虑也可从人脸识别技术应用公众反馈中得到共鸣。据 APP 专项治理工作组发布的《人脸识别应用公众调研报告(2020)》显示，在 2 万多名受访者中，64.39%的受访者认为人脸识别技术有被滥用的趋势，而在安全性感受方面，受访者给出的分数则明显偏低，仅有交通安检场景的平均分超过 4 分[1]。这表明，以个人信息收集、处理与使用为核心的人脸识别技术，加剧了社会公众对人脸识别技术滥用的担心，强化人脸信息保护的呼声日益高涨。人脸识别技术犹如一枚银色硬币，在照出了科技技术高歌猛进的同时，也反射出人脸信息受到侵害的阴暗面。

2. 人脸识别系统的定义及特点

就人脸识别技术的定义而言，广义的人脸识别主要有四个过程，分别为图像获取、人脸检测、特征提取、人脸识别与辨认。而狭义的人脸识别只针对第四步人脸识别与辨认，即将待识别的人脸特征与数据库中的人脸特征进行匹配，根据相似度进行结果判断。[1]广义的人脸识别可“见图 1”：

Figure 1. Diagram of generalized facial recognition
图 1. 广义人脸识别展示图

[1] 央广网. <人脸识别应用公众调研报告(2020)>出炉 六成受访者认为人脸识别技术有滥用趋势[EB/OL]. https://baijiahao.baidu.com/s?id=1680939962774852342&wfr=spider&for=pc, 2020-10-19.

人脸识别技术首先通过外部的摄像头采集人脸图像或视频传输至计算机，后由计算机将获取到的人脸图像与数据库中存储的图像进行特征匹配，选择分类算法的不同将直接影响着识别率和识别速度，依据所选的算法计算机比对人脸样本之间特征的差异程度，辨别待识别的人脸是否为本人。

人脸识别技术的深入应用一方面得益于人脸的独特性。每个人都有自己独一无二的面容，通过对人脸的检测、辨别即可以直接识别到主体个人。当然，如果结合其他个人信息进行识别则准确率更高。[2]另一方面，人脸识别技术具有采集便利的优点。人脸图像的收集，通常采用摄像头自动拍摄的收集方式，用户不需要和设备直接接触，只需以正常状态经过摄像头前或做出一定的配合动作如点头、眨眼，人脸识别即可获取人脸图像。在某些场所中，人脸识别摄像头甚至和监控摄像头的外观一样，可以做到全程“无感”抓拍。因此，人脸识别这种将个人人脸信息与计算机处理技术高度融合的科学识别方法，逐渐成为用户识别与确认的“新宠”。

3. 人脸识别门禁系统存在的问题

在小区安装人脸识别门禁系统的过程中，往往涉及到业主、物业部门、政府三方主体之间的配合。但是，由于三方在职责、地位等客观因素上的影响，导致实践中问题频出。

3.1. 业主知情权、决策权受限

3.1.1. 业主知情权难以得到保障

业主的知情权是业主自治权的重要组成部分，在安装小区人脸识别门禁系统之前，业主有权知道人脸信息将被合法收集以及使用的方式、范围。《物业管理条例》明确规定[2]，业主对物业共用部位、共用设施设备和相关场地使用情况享有知情权和监督权。《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》(以下简称《规定》)提出，信息处理者在开展人脸信息处理活动中，未公开处理人脸信息的规则或者未明示处理的目的、方式、范围的，属于侵害自然人人格权益的行为。因此，小区在安装人脸识别门禁系统之前未确保业主事前知情权的做法是对人格权益的侵犯。

在收集人脸信息这一敏感个人信息前是否正确履行告知义务是一个重要的问题。对于这一问题，《个人信息保护法》第十七条规定，处理者在处理个人信息前，应当以显著方式、清晰易懂的语言向个人告知处理个人信息的目的、方式，以及处理的个人信息种类、保存期限。因此，物业在收集业主人脸信息前应当尽到告知义务，确保业主的知情权。实践中物业未在合理期限内提前告知业主收集人脸信息便立即上门收集的做法存在明显不妥。

类似地，人脸识别门禁系统的采购、安装也应当确保业主的知情权。小区设备的采购、安装一般都需要使用建筑物及其附属设施的维修资金，根据《中华人民共和民法典》(以下简称《民法典》)[3]规定，建筑物及其附属设施的维修资金使用情况应当定期向业主公布。在选购人脸识别门禁系统设备的过程中，不明确向业主告知预采购设备与技术、相关安装费用的详情，以及征求其对预采购的反馈意见，明显违反《民法典》的相关规定，侵害业主对小区财产的共有权。

3.1.2. 业主对安装人脸识别的决策权利受限

就小区安装人脸识别门禁系统的全过程，物业通常占据主导地位，业主的个人意见与集体决策权利没有受到充分的尊重，其对决定结果所产生的影响力十分有限。

首先，根据《个人信息保护法》第二十九、三十条规定，处理敏感个人信息应当取得个人的单独同

[2]《物业管理条例》第六条：房屋的所有权人为业主。业主在物业管理活动中，享有下列权利：……(八)对物业共用部位、共用设施设备和相关场地使用情况享有知情权和监督权；(九)监督物业共用部位、共用设施设备专项维修资金的管理和使用。

[3]《中华人民共和国民法典》第二百八十一条：建筑物及其附属设施的维修资金，属于业主共有。……建筑物及其附属设施的维修资金的筹集、使用情况应当定期公布。

意，并向个人告知处理敏感个人信息的必要性以及对个人权益的影响。因此，物业部门为维护小区公共安全安装图像采集、个人身份识别设备的，除需履行适当的告知义务前提，还需就收集并使用人脸信息取得业主的个人同意。物业未征得业主的单独同意而收集人脸信息作为小区出入验证方式的，应认定为侵害业主权益的行为。

其次，小区是自治空间，业主对于小区享有管理自治，即有权按照个人意志直接或者间接地处理小区公共事务的权利[3]。业主大会是业主行使自治权的主要手段，在《民法典》以及《物业管理条例》中都规定了业主有权成立业主大会对小区管理的相关事项做出表决。小区安装人脸识别门禁系统属于《民法典》第二百七十八条规定的业主共同决定事项，应该召开业主大会进行表决来形成决议。业主大会的决议是业主共同意志的最终表达，是集体权益的一致诉求。它表明了小区业主对于安装人脸识别门禁系统的态度倾向。虽然，小区在决定是否安装人脸识别门禁系统的过程中，召开业主大会并不是唯一途径，还可以通过个别询问业主的意见来使业主参与到决策的形成中。但是，基于效率最大化的原则，对于物业部门来说，相比逐个征求业主的明确同意的困难做法，建议召开业主大会一次性通过集体表决显然是更为效率的方式。但是就团队调查情况来看，83.05%的业主表示其小区在安装人脸识别门禁系统前没有召开过业主大会。并且，有 61.02%的业主表示物业在安装之前没有征求过其明确同意。这显示是不合理的，侵犯了业主的决策权利。

总之，就业主而言，无论是个人的明确同意抑或是业主大会的集体表决，业主的决策权利并未如愿受到良好尊重，其难以通过有效的途径干预小区人脸识别门禁的安装，自治权利受到严重侵害。

3.2. 物业视角下存在的问题

3.2.1. 物业与安装、技术公司对数据保护意识的薄弱

对于物业与安装、技术公司的在数据对接过程中如何防止个人信息泄露的问题，《个人信息保护法》第二十一条作出了基本规定。一方面，物业应当与受托方明确约定委托处理的目的、处理方式、保护措施，要求处理行为不应超出人脸信息主体授权同意的范围。同时，物业也需要对受托方的处理行为进行监督，及时纠正受托方不适当的处理行为。另一方面，受托方应当按照约定的目的及方式处理人脸信息，并应当在合同履行完毕或者委托关系解除后，将个人信息及时返还委托方或者予以删除。不得未经同意私自转委托他人处理个人信息。

简单来说，物业与安装、技术公司在数据对接中都不得超出收集目的处理业主的个人信息。但是该条规定中未对违反之后的责任做出进一步规定，对物业及安装、技术公司的约束力仍不够，个人信息泄露的风险仍然存在。

3.2.2. 人脸信息安全事件的应急处理滞后

大数据时代，信息技术的发展极大增加了个人信息泄露风险，威胁现有的储存和安防措施，个人信息安全面临更为严峻的挑战。但物业及受托公司作为个人信息处理者，对安全事件预防和应对能力却严重滞后。

例如，2019 年一家中国 AI + 安防行业的企业——SenseNet 在社交网站上被指控因人脸识别数据库没有密码保护发生大规模泄露，致使超过 250 万人的敏感数据包括身份证号码、地址、出生日期、识别其身份的位置可被获取，680 万条数据疑似泄露[4]。因此可见，人脸识别技术并不是绝对安全的，其存在着不少漏洞和缺陷，即使是所谓的安防公司也未能抵御人脸信息泄露的风险。而就一般的物业公司和技术外包公司而言，出于控制成本、人力资源等因素，其对人脸信息的保护水平几乎无法达到安防公司的

[4]南方网. 深圳一 AI 公司数据疑遭泄，超 256 万用户信息被指“裸奔”|附商汤回应. http://static.nfapp.southcn.com/content/201902/15/c1923796.html, 2019-02-16.

水平高度，并且他们通常也不愿为人脸识别系统故障或黑客侵入等安全事件制定应急预案，没有定期组织内部相关人员进行应急响应培训，而是报着事件发生才处理的不良心态。若上述人脸安全事件发生，这种应对能力的落后无疑会扩大对个人信息主体造成的不利后果。

3.3. 政府视角下的问题

3.3.1. 人脸信息泄露的惩罚责任机制不足

由于法律的滞后性限制，对于人脸信息的泄露，现阶段只能在法律规定的限度内进行相关处罚，处罚力度较轻，不足以有效遏制侵犯人脸信息的违法行为。其次，行业协会有名无实，行业内部在个人信息保护领域没有制定相应的自律规范和自律公约，没有组织对可能接触个人信息的内部人员的相应培训、监管和教育，未能建立完善的防范泄露风险的惩罚责任机制，无法弥补法律法规滞后所带来的缺陷[4]。

3.3.2. 数据保存风险的管控不到位

一般地，对于收集到的业主人脸信息由物业公司负责保存。而物业公司的保存措施一般为将收集到的信息存储在机房内的服务器内，并对机房进行视频监控，同时物业公司将相关情况在公安部门进行报备。

因主客观的一些问题如经济因素、技术因素等，由物业公司负责保存数据和提升数据的安全保护程度存在显著困难。在主观上，物业关系基于控制成本的考虑，对于提高数据保护安全性的意愿较低。在客观上，物业公司主要从事小区的物业管理，其人员配套中缺乏相应的专业技术人员负责数据的安全存储。其导致的结果往往是，人脸识别门禁系统虽然可以日常正常运行，但一旦遇到技术错误甚至外来攻击，数据泄露现象就极易出现。

因此，由物业公司承担数据保存的全部责任是不合理的，这就必然要求政府承担更多的责任与风险义务。然而，多数政府在对小区人脸信息保管方面，其只进行备案工作且缺少对具体事项的充分监督，即使存在监督，也大多流于形式与表面。

4. 人脸识别入小区的立法规范及适用现状

2021 年《个人信息保护法》的正式适用为敏感个人信息的特殊保护奠定了深刻的基础，同年《信息安全技术人脸识别数据安全要求》(征求意见稿) (以下简称《人脸识别国标》)的发布也传递了立法者对于人脸信息保护特殊规则制定的迫切需求，最高院《规定》的通过更在一定层面直接赋予了小区业主的人脸识别门禁“拒用权”。

4.1. 对人脸信息保护的集中规定

人脸信息类属典型的生物识别信息，根据《个人信息保护法》“敏感个人信息的处理规则”一节中的规定，生物识别信息属于敏感个人信息分类，《网络安全法》第二十二条中规定，“网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意。”2020 年 3 月 6 日发布并于 10 月 1 日开始生效的《信息安全技术 个人信息安全规范》[5] 第四条中指明，收集个人信息的主体应当取得被征集人的“选择同意”——向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意；“确保安全”——具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。作为一个行业性标准，在法律规范上其未对信息的采集者做出具体的步骤规范与资格要求[5]。

2021 年 6 月最高人民法院通过的《规定》对信息处理者应用人脸识别技术处理人脸信息做出了严格

[5]《信息安全技术 个人信息安全规范》2020 年 3 月 6 日发布，2020 年 10 月 1 日实施。

限制，规定了信息处理者抗辩不能的具体情形、承担侵权责任的具体情形以及不同场所滥用人脸识别技术造成的侵权后果。而2021年《人脸识别国标》的出台细化了人脸识别在具体应用上的措施要求，对信息处理者和人脸信息的监管者提出了更高的要求，其中对于人脸识别在现实中的应用划清了界限：强调“明示同意”原则；坚持“非必要不使用”，只有在其他方式的安全性或便捷性显著低于人脸识别的情况下，方可开展；设立“资质门槛”，只允许数据安全防护和个人信息保护能力过关的开发商涉足。

4.2. 业主的决定性和知情权缺乏法律强制性规定

在安装人脸识别门禁的全过程中，有多个环节涉及业主的决定权和知情权，概括而言可以分为人脸信息处理——设备运行处理两个部分。根据《个人信息保护法》处理敏感个人信息的基本要求，收集使用人脸信息用做门禁系统首先需要获得业主的单独同意，并对业主进行充分告知，这里的告知包含处理敏感信息的必要性及对个人的影响等等。结合《规定》第10条直接而有效地明确业主有权拒绝物业将人脸识别门禁作为验证出入的唯一方式，在这个层面，业主具有概括的拒绝权。

而深入门禁安装的各个环节之中，也存在着涉及业主决定权知情权的众多事项。人脸识别在替代原有门禁系统时，需要动用物业或业主大会的储备资金，用于人脸门禁系统的安装、维修及日常的管理活动。在《民法典》第二百八十一条中规定，“建筑物及其附属设施的维修资金，属于业主共有。经业主共同决定，可以用于电梯、水箱等共有部分的维修。维修资金的筹集、使用情况应当公布。”2010年《宁波市业主、业主大会、业主委员会指导规则》[6]第十一条关于业主的权利与义务中也对此作出了类似规定。在这之中，明确赋予了业主对于维修资金有关情况的知情权。这缘于实践中，建筑物及其附属设施的维修资金对于小区的正常维护的重要性，以及在管理及归属等方面存在的问题比较突出。但在安装人脸识别门禁的实践中，很难界定新增或替换一项门禁系统是否属于“建筑物及其附属设施”的范畴，若将在小区内安置的门禁系统视为小区共有部分的一块，则适用“业主共同决定”、“向业主公布”的规定才具有当然性。

北京法院参阅案例第49号《王某等与某小区业主委员会业主知情权纠纷案》[7]中，王某以小区存在公共收益账目不透明，未经过招标就动用维修基金维修电梯等问题，但业委会拒不向业主公开相关情况为由，要求业委会允许其查阅复印历次业主大会决定及会议记录等材料，依据是小区投票通过的《小区业主大会议事规则》中关于业主委员会接受业主监督、依法管理保存会议记录并应当为业主查询相关资料提供便利的规定。北京海淀区人民法院作出的(2015)海民初第28547号判决书中支持了王某要求业委会配合其查阅、复印业主大会、业主委员会的决定及会议记录等材料的诉讼请求。本案中法院认为，王某作为小区建筑区划内的区分所有人，对于涉及小区共有部分以及共同管理事项的处理享有知情权，这种权利限于业主查阅、复印涉及其自身利益或直接关系全体区分所有人共同利益或间接关系其自身利益的事项。根据《民法典》中对建筑物区分所有权的规定，我们应当认为小区住户出入的门禁设施属于“建筑区划内的其他公共场所”，属于全体业主共同管理、使用的共有部分，全体业主对其当然享有共有权以及附随权利，也当然享有对出入门禁系统的修建、日常管理和维护享有知情权。

在此之中，人脸信息的采集以及人脸识别门禁系统的安装是否属于“其他应当向业主公开的情况和资料”存在一定争议，笔者认为安装设置门禁系统的相关设施所在的位置应当参考“建筑区划内规划用于停放汽车的车位、车库的处分情况”，因为其具有建筑区划内公共区域的特征且使用用途与设施安装涉及大部分小区业主的切身利益，因此业主对其应当享有知情权。

[6]《宁波市业主、业主大会、业主委员会指导规则》第11条：业主有权请求业主委员会公布下列情况和资料：(一) 专项维修资金筹集、使用情况；(二) 管理规约、业主大会议事规则；(三) 业主大会和业主委员会的决定及会议记录；(四) 物业服务合同；(五) 共有部分的使用和收益情况；(六) 物业管理区域内规划用于停放汽车的车位、车库的处分情况；(七) 其他应当向业主公开的情况和资料。

[7]2020北京法院参阅案例第49号，北京海淀区人民法院(2015)海民初第28547号判决书。

4.3. 应用门禁系统表决程序规则的缺失

在人脸信息保护上的法律缺失与业主被采集人脸信息时知情权的保护困难使得人脸识别门禁系统在宁波市多个小区安装实施后存在一系列的法律风险。而此项政策的实施源头——人脸识别门禁系统的应用究竟应当如何落地小区却在实践中面临着无数的问题。

《民法典》第二百七十八条中规定，“业主决定建筑区划内重大事项及表决权，下列事项由业主共同决定……(二)制定和修改建筑物及其附属设施的管理规约……(五)筹集和使用建筑物及其附属设施的维修资金；(六)改建、重建建筑物及其附属设施；(七)有关共有和共同管理权利的其他重大事项。决定前款第五项和第六项规定的事项，应当经专有部分占建筑物总面积三分之二以上的业主且占总人数三分之二以上的业主同意。决定前款其他事项，应当经专有部分占建筑物总面积过半数的业主且占总人数过半数的业主同意。

人脸识别门禁系统是否属于上款规定中 2/5/6 项提到的“建筑物及其附属设施”，又是否属于“有关共有和共同管理权利的其他重大事项”，应当经不同比例的业主投票同意方可通过，在法律规范上属于一个空白点。参考 2020 年《杭州市物业管理条例(草案)》中第五十五条的规定“既有住宅需要加装电梯的，应当经本单元专有部分占建筑物总面积三分之二以上且占总人数三分之二以上的业主参与表决，并经参与表决专有部分面积四分之三以上的业主且参与表决人数四分之三以上的业主同意。”门禁系统的公共安全性对大部分小区居民影响虽具有广泛性，但加装人脸识别门禁系统与加装楼道电梯进行横向比较时，从安装的必要性和通用性考虑，加装楼道电梯的切实必要性一般大于加装人脸识别门禁系统，电梯的通用性和必须性也高于人脸识别门禁系统，就此将加装电梯的表决程序与安装人脸识别门禁系统等同并不合理。应将其参照第二百七十八条规定，应当经参与表决专有部分面积过半数的业主且参与表决人数过半数的业主同意，方可达到立法与实践的平衡。

5. 人脸识别门禁系统风险防范可行性建议

业主、物业、政府机关三方主体在人脸识别小区门禁安装中代表着不同的利益群体，承担着截然不同却息息相关的利益与风险得失。笔者认为，完善人脸识别门禁系统的风险防范，需要保障业主的知情权、参与权决定权，规范信息控制者物业的告知义务，设定门禁预留方案，着力建立政府人脸信息数据库，加强人脸数据监管。

5.1. 保障业主的知情权、参与权

业主作为人脸识别应用于门禁系统的重要主体，理应参与到人脸识别应用于门禁系统的全过程。但实践中，业主对人脸识别门禁落地全过程的参与时常难以得到有效保障，人脸信息如何被采集；人脸信息如何被存储；门禁设备安装的必要性、重要性等问题很难被充分释明。不充足的知情及参与难以体现业主的意志，保障业主的权利。要全面保障业主的知情权，需要严格规制物业行为。

其一，在公示环节，在人脸识别门禁系统安装前，可采用多途径公示，保证小区业主知晓信息采集的基本事项及安装所涉各个方面，在公示的形式要件上应保证公示内容的真实、准确、完整性，做到内容清晰易懂，符合通用的语言习惯，避免使用高深拗口的词汇和有歧义的语言。

其二，在业主的参与权决定权上，参与权与决定权是否充分行使，直接决定了人脸识别能否规范地应用于小区门禁系统。应当要求在业主充分知情的前提下，明确人脸识别应用于小区门禁系统的决策机制，根据上文所述，应当召开业主大会，经参与表决专有部分面积过半数的业主且参与表决人数过半数的业主同意，方可实现人脸识别门禁系统的程序规范。

其三，在信息处理的同意上，由于人脸信息采集的无接触性，信息采集容易变得难以察觉，征得业主的有效同意在这一层面尤为重要。首先，应当排除口头意思表示的同意，将书面同意认定为业主同意将人脸识别系统应用于小区门禁的唯一标准，更能够从形式上让业主感受到正式感和严肃性。其次，同意应当是单独而明确的，确保对人脸信息的采集符合《个人信息保护法》单独同意的基本要件，将其与采集其他一般个人信息和物业服务的通知严格区分。

5.2. 规范物业的告知义务与决策程序

物业全程主导着小区人脸识别门禁系统的选定、安装、人脸信息收集之后的储存、保护等流程问题。人脸识别门禁系统的风险防范必须严格规范物业告知义务与决策程序。

5.2.1. 规范物业的告知义务

在告知的内容上，结合《个人信息保护法》及《解释》、《人脸识别国标》等规范，告知的内容应当详尽而具体，告知信息处理的各类事项。人脸识别应用于门禁系统中时，应当事先告知业主人脸识别适用于小区门禁系统的目的、好处、风险、条件；业主的权利，包括知情权，查阅权，复制权，补正权以及退出权等；如何存储、管理业主人脸信息；处理业主人脸信息的限制条件以及信息泄露，使用，转让，买卖的归责以及处罚方案等。在告知的形式上，告知应当是明确而清晰的。在告知的具体途径上，应当公开发布且易于让业主知悉。考虑到小区业主的多样性，可以充分完善告知的情形：考虑告知的效果有效性，将告知以公告栏、微信群等媒介予以传播。在时间上，物业应及时确定公告的时间，提前予以通知全体业主，给业主充足的时间了解人脸识别门禁系统，从而做出是否同意人脸识别应用于小区门禁的决定。此外，物业在告知小区业主信息时，应当保证所告知的信息真实、准确、完整。同时应当做到内容清晰易懂，符合通用的语言习惯，尽量避免使用高深拗口的词汇和有歧义的语言。

5.2.2. 落实小区业主的集体决策程序

在小区业主知悉什么是人脸识别，了解人脸识别应用于门禁系统优势和风险之后，应当召开业主大会对是否同意引进人脸识别门禁系统进行表决，表决程序的合理设置事关业主能否有效的行使表决权。具体而言，业主大会关于人脸识别应用于小区门禁的决策程序如下：物业须提前一定的期限告知小区业主关于人脸识别门禁系统的详细信息；业主大会召开时，物业应就公告内容做出详细说明，并回答业主提出的问题；业主同意安装人脸识别系统的，应在物业发放的征求意见表上签字，征求意见表一式两份，一份由业主保管，一份由物业存留；专有部分占建筑物总面积二分之一以上且占总人数二分之一以上的业主同意，方可安装人脸识别门禁系统。

5.2.3. 预留除了人脸识别门禁之外的替代通行方案

考虑到有部分业主不同意人脸识别系统安装于小区门禁，以及考虑到门禁系统有出现故障的可能性，在安装人脸识别门禁系统的过程中，应当预留除了人脸识别门禁之外的替代通行方案，以保证顺利通行。例如，对于不同意使用人脸识别门禁系统的业主，仍可使用传统的门禁卡通行；在人脸识别门禁系统出现故障时，采用人工登记的方式通行。

5.3. 政府加强数据库建设与信息安全监控

在政府层面对人脸识别小区门禁做出规范，需要借助其强大的资源整合优势与公权力监管，确立人脸信息实践应用的较一般个人信息更为严格的桂规制监管以及辅助建立人脸识别社区数据库[6]。人脸信息被收集之后储存在哪里，怎样储存，由谁储存等问题也亟待规范，明确人脸信息的储存机制将会在很大程度上保证业主人脸信息的安全。

作为个人信息保护的职能部门，国家网信部门和地方政府应当着重对人脸信息的应用和处理进行监管，考虑到由各个小区业主建立人脸信息库不具有整合性，让每个小区都聘请专业的信息管理人员监管信息也不具备可行性。可由政府建立专门的人脸识别门禁数据库，各小区物业将收集到的业主人脸信息数据上传至政府建立的人脸识别门禁数据库，进行统一监管[2]。在公权力层面采用技术手段与管理手段相结合的方式，采取防范计算机病毒等危害网络安全行为的技术措施；采取监测、记录网络运行状态、网络安全事件的技术措施；采取数据分类、重要数据备份和加密等措施；建立可追踪的技术体系，谁在何时何地查询、使用、修改、下载了人脸信息，事后都可查证。

6. 结语

人脸识别作为一种新兴技术，将其引入小区门禁系统，极大提升了业主出入效率和门禁管理效能，但与此同时也为业主的个人信息安全、业主决定权表决权带来了些许挑战。《个人信息法》、《规定》等规范的出台在一定程度上让我国在法律层面对人脸信息的保护摆脱了“无法可依”的局面。实践中，人脸识别门禁系统的风险防范离不开物业及政府对业主的制度涉及与决策保护。经由法律在对人脸信息的严格保护之外，推动物业政府及业主三方，以更加立体的约束和指导人脸识别门禁系统的信息处理及程序落地，努力实现人脸数据的一体化监控，相互协力促进技术安全与实践效能的共同进步！

参考文献

[1] 方程. 人脸识别技术研究[J]. 信息技术与信息化, 2014(11): 53-55.

[2] 邢会强. 人脸识别的法律规制[J]. 比较法研究, 2020(5): 51-63.

[3] 周安平. 社会自治和国家公权[J]. 法学, 2002(10): 15-22.

[4] 史卫民. 大数据时代个人信息保护的现实困境与路径选择[J]. 情报杂志, 2013, 32(12): 154-159.

[5] 劳东燕. 潜在风险与法律保护框架的构建[N]. 检察日报, 2020-10-12(4).

[6] 林凌, 贺小石. 人脸识别的法律规制路径[J]. 法学杂志, 2020, 41(7): 68-75.