

社区人脸识别信息收集的法律风险分析

陈 胜

上海政法学院国际法学院, 上海

收稿日期: 2024年6月12日; 录用日期: 2024年7月28日; 发布日期: 2024年8月6日

摘 要

人脸识别信息因具有唯一性、可携带性、易于采集性, 在被技术开发后广泛用于各种场景中。根据《民法典》以及《个人信息保护法》的规定, 人脸信息属于生物识别信息, 同时也属于敏感个人信息。“人脸识别第一案”暴露出非必要收集人脸识别信息存在的法律风险。新冠疫情爆发后, 许多住宅社区都引入人脸识别门禁系统, 作为人们日常生活的中心, 社区对于住户的个人信息收集十分容易, 但仅凭物业公司的技术水平, 能否妥善保护用户信息防泄露是存疑的。现有学者多从商业领域, 如APP用户人脸信息收集、AI换脸技术等方面探究人脸识别的风险, 跟个人隐私密切相关的社区人脸信息收集却鲜少探究。因此, 本文旨在通过阐述目前社区收集人脸信息存在的住户敏感性偏低、社区以便利管理为导向的现状, 在“合法性、正当性、必要性”的敏感个人信息处理三原则的基础上, 探究其在法律以及实际应用层面的合理规制途径。

关键词

人脸识别信息, 社区, 必要性, 法律风险

Legal Risk Analysis of Community Face Recognition Information Collection

Sheng Chen

Department of International Law and Business, Shanghai University of Political Science and Law, Shanghai

Received: Jun. 12th, 2024; accepted: Jul. 28th, 2024; published: Aug. 6th, 2024

Abstract

Face recognition information is widely used in various scenes after technology development because

文章引用: 陈胜. 社区人脸识别信息收集的法律风险分析[J]. 争议解决, 2024, 10(8): 14-21.

DOI: 10.12677/ds.2024.108347

of its uniqueness, portability and easy collection. According to the provisions of the Civil Code and the Personal Information Protection Law, face information is biometric information and is also sensitive personal information. The “First Case of Face Recognition” exposed the legal risks of unnecessary collection of face recognition information. After the outbreak of the new coronavirus, many residential communities have introduced face recognition access control system, as the center of people’s daily life, the community is very easy to collect personal information for residents, but only by the technical level of the property company, whether the user information can be properly protected against leakage is doubtful. Existing scholars mostly explore the risks of face recognition from commercial fields, such as APP user face information collection, AI face-changing technology, etc., but rarely explore the community face information collection closely related to personal privacy. Therefore, this paper aims to explore reasonable regulatory approaches at the legal and practical application levels based on the three principles of “legality, legitimacy and necessity”, by explaining the current situation of the low household sensitivity and the convenience-oriented management of community in collecting face information.

Keywords

Face Recognition Information, Community, Necessity, Legal Risk

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

在信息化浪潮汹涌的今日，科技前沿的人脸识别与指纹验证等识别技术正日益融入人们的日常生活。特别是自 2019 年起，“刷脸支付”这一创新支付方式迅速崛起，引领支付潮流。这一模式深度融合了人工智能、生物识别技术，并结合大数据风控系统，为用户带来了前所未有的支付体验。仅需“一张脸”，便可实现快捷、高效且安全的支付操作，极大地提升了支付的便捷性和效率。电子科技大学信息与通信工程学院副教授曾辽原认为“人脸识别的便捷性与安全性不可兼得”[1]。人脸识别信息因其可携带性、易于采集性等特点被广泛运用，但同时也因唯一性、不可更改特性而在许多场景应用中存在风险。社区作为人们日常生活的中心，与人们个人信息、隐私密切相关，不能仅考虑管理便利性而忽略人脸信息收集的风险，应以“合法、正当、必要”原则为前提，审视人脸识别信息收集与利用必要性以及保护途径。

受新冠疫情影响，中国大部分社区都在疫情期间引入了人脸识别系统来管理进出人员。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》(以下简称“《规定》”)第五条规定，为了公共安全突发事件，信息处理者可以处理人脸信息，但鉴于目前疫情已经消失，社区继续使用人脸识别系统作为户主验证进出社区的方式合理性和必要性值得怀疑。

2. 社区人脸信息规制现状与不足

北京科学学研究中心副主任伊彤在其《关于开展公民个人生物信息立法的建议》中提到个人生物信息不同于密码，密码泄露可以更换，但个人生物信息一旦泄露就是终身泄露，作为个人生物信息中极易被采集的人脸识别信息更应受到着重保护[1]。鉴于我国不同于西方国家体制，住户对含有一定公众管理的社区往往信赖程度较高、防范意识不足，加之物业公司并非专业技术公司，在技术操作方面水平层次不齐，社区收集并利用人脸信息存在极大风险。

2.1. 规制现状

2.1.1. 住户对个人人脸信息敏感性偏低

笔者以“社区”、“人脸”作为关键词,以民事案件中个人信息保护为专题在北大法宝上进行搜索,总共出现了 17 个案例,以“社区”、“人脸信息”在威科先行进行搜索,总共出现了 20 个案例,在排除重复以及与社区人脸识别信息不相关的案件后,仅 7 例案件比较相关,且其中 4 例为安装“电子猫眼”收集人脸信息侵犯他人隐私权¹,1 例为在疫情管控期间社区安装刷脸系统与用户起冲突的偏向刑事类案件²,剩下的 2 例涉及社区收集人脸信息的案件均以物业服务合同纠纷³为案由提起,尽管有部分住户认识到人脸信息的重要性,但目前并无直接对社区收集人脸信息进行分析的案例。可见对于社区进行人脸信息收集,住户出于疫情防控期间的先例,对该行为并不抵触,公众敏感度不高。

2.1.2. 社区优先考虑管理便利性

其次,根据笔者线下走访上海市松江区住户调查显示,以万科金色华庭苑为代表在内的多个小区⁴现在均使用了新型刷脸刷卡一体机作为户主进入小区的验证方式,但多数用户表示自己只是接到社区录入人脸信息的通知,物业并未明确提供正式文件对人脸信息收集方式、储存方式以及用户具体权利行使途径进行说明,上海沐雅房地产开发有限公司甚至仅以刷脸作为住户验证进入小区的唯一方式。根据《规定》第十条第一款⁵以及国家互联网信息办公室 2023 年 8 月 8 日发布的关于《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第十四条⁶规定,社区不得将使用人脸识别技术验证个人身份作为出入物业管理区域的唯一方式,但目前大多社区仍以管理便利性为前提而忽视人脸信息的重要性,如在对北京市十个安装人脸识别门禁的小区调查中发现,尽管文件明令禁止,但强制刷脸现象在北京仍然普遍存在,所测十个小区中,有六个以不同形式强制居民录入人脸[2]。

2.2. 社区收集人脸信息存在的不足

目前立法层面已意识到人脸信息的敏感性以及重要性,对社区收集人脸信息有了初步法律规定,但并未对社区在正常情形下(非疫情期间)收集人脸信息的合法、必要以及正当性进行说明。根据《民法典》第一千零三十五条⁷以及 2021 年出台的《中华人民共和国个人信息保护法》(以下简称“《个人信息保护法》”)第二十八条规定⁸,对敏感个人信息的处理应当符合“合法、正当、必要”三原则,但对于三原则的具体内涵,目前已有司法实践和立法层面均未作充分说明[3],存在模糊性。以“人脸识别第一案”为例,法院虽基于三原则对被告动物园处理原告人脸识别信息的行为是否构成侵权作出了分析,但并未

¹四个案件分别为:邓某与李某隐私权、个人信息保护纠纷(2021)京 0108 民初 39401 号、黄某与邵某隐私权纠纷(2020)沪 0118 民初 15600 号、孙某与荆某隐私权纠纷(2021)京 0114 民初 29114 号以及杨淑芬等与汪鹏等隐私权、个人信息保护纠纷(2021)京****民初 6268 号。

²吴某等生命权、身体权、健康权纠纷(2021)京**民终 16806 号。

³乐生活智慧社区服务集团股份有限公司与黄嘉芸物业服务合同纠纷(2022)京****民初 4310 号、刘同铨、陆卫俊等物业服务合同纠纷(2022)浙 0114 民初 3550 号之一。

⁴分别是万科金色华庭苑、玉乐小区、海尚名都、华亭新家百合苑等共计 10 个小区。

⁵《规定》第十条第一款:物业服务企业或者其他建筑物管理人以人脸识别作为业主或者物业使用人出入物业服务区域的唯一验证方式,不同意的业主或者物业使用人请求其提供其他合理验证方式的,人民法院依法予以支持。

⁶《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第十四条:物业服务企业等建筑物管理人不得将使用人脸识别技术验证个人身份作为出入物业管理区域的唯一方式,个人不同意通过人脸信息进行身份验证的,物业服务企业等建筑物管理人应当提供其他合理、便捷的身份验证方式。

⁷《民法典》第一千零三十五条:处理个人信息的,应当遵循合法、正当、必要原则,不得过度处理。

⁸《个人信息保护法》第二十八条:敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下,个人信息处理者方可处理敏感个人信息。

严格区分三者，对每项原则作出审查；从表述上看，它甚至将“必要性”纳入“正当性”的范围之中关系界定及审查标准并不十分明确⁹，上海市地方标准 DB31/T 1467-2024 文件直接将三项原则都包含进合理性原则当中¹⁰。人脸信息属于敏感个人信息，社区对其进行收集利用也必须符合合法性、正当性以及必要性。

2.2.1. 合法性基础薄弱

目前专门规范公共场所收集、利用人脸信息的相关法律法规较少，高层次法律同样较少，基本维权途径是将其视为敏感个人信息或隐私权的一部分通过《个人信息保护法》或《民法典》来进行保护，除此之外，多数文件为人脸识别的技术要求(见表 1)。

Table 1. Laws and regulations directly related to face recognition in China at present (taking Shanghai as an example)
表 1. 我国目前直接涉及人脸识别的法律法规及规定(地方以上海市为例)

《中华人民共和国民法典》2021 年 1 月 1 日起施行	第四编人格权中第六章隐私权和个人信息保护。
《个人信息保护法》2021 年 11 月 1 日起施行	第二节敏感个人信息的处理规则。
《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》2021 年 8 月 1 日起施行	规范“人脸信息的处理包括人脸信息的收集、存储、使用、加工、传输、提供、公开”。
《人脸识别技术应用安全管理规定(试行) (征求意见稿)》暂未通过	由国家互联网信息办公室发布的为规范人脸识别技术应用所制定的规定。
《信息安全技术人脸识别数据安全要求》(GB/T 41819-2020)现行有效	适用于数据处理者安全展开人脸识别数据处理活动。
《数据安全技术数据分类分级规则》(GB/T 43697-2024)暂未生效	主要在附录 B 个人信息分类示例以及其他部分中提到。
《人脸信息合规操作指南》2022 年 1 月起对外发布	中国信通院云计算与大数据研究所联合相关机构和专家依托所编写，将合法、正当、必要、诚信四大法律基本原则具象化为九项原则性要求 ¹¹ ，并将其贯穿于人脸信息全生命周期处理环节的合规要求、其他合规要求，以及具体行业应用场景的相关要求。
《公共场所人脸识别分类分级应用指南——上海市地方标准》(DB31/T 1467-2024)现行有效	作为全国首个公共场所人脸识别分类分级管理的标准，本文将其作为地方性代表结合上述所提松江区实地调查报告一并分析。
《上海市数据条例》2022 年 1 月 1 日起施行	第二章第二节个人信息特别保护。

但人脸识别信息与隐私权和敏感个人信息之间也有区别。敏感个人信息的界定因具有客观性，其敏感与否并非由个人的主观意愿决定，而是根据社会普遍认知和共识来评判；隐私权所保护的私密信息则融合了客观与主观的特质，它不仅强调信息在客观层面上的隐秘状态，更加强调个体主观上不愿为他人所知的内心愿望[4]。人脸信息因暴露在外而不属于私密信息范畴，其风险在于与其他个人信息结合后容易获得主体的身份以及大量财产等信息，单纯的人脸信息并不十分“敏感”。

除此之外，根据上述规定，社区管理者应为人脸数据的信息/数据处理者，至于社区是否为公共场所，

⁹郭兵诉杭州野生动物世界有限公司服务合同纠纷案，杭州市富阳区人民法院(2019)浙 0111 民初 6971 号民事判决书。
¹⁰上海市地方标准《公共场所人脸识别分类分级应用指南》，DB31/T 1467-2024，第 4.1 部分合理性原则：1) 最小必要；2) 目的明确；3) 一致性。
¹¹《人脸信息合规操作指南》将“合法、正当、必要、诚信”具象为“合法性基础、目的特定、充分必要、公开透明、告知同意、权益保障、信息质量、信息安全、可问责”九项原则性要求。

法律法规中并无直接说,仅有国务院 1987 年 4 月 1 日发布的《公共场所卫生管理条例》中将公共场所共 7 类 28 种进行了划分,但并未将社区划入其中。维基百科将公共场所定义为“一个不限于经济或社会条件(纵然实际情况未必如此),任何人都权进入的地方”,社区因仅有户主可以自由出入,应当认为小区不属于公共场所的概念范围。但上海市地方标准 DB31/T 1467-2024 认为社区属于“其他类”公共场所,将其划入公共场所范围,如附录 A 表 A.3 公共场所分类表(其他)中细分场景社区中应用包括:1) 在社区场景中可利用人脸识别进行对于人员进行身份核实和管理,具体应用可包括但不限于住宅楼栋、小区业主出入口的监控和小区楼栋以及业主出入口处的门禁等;2) 本细分场景下人脸识别系统的主要目的可为安全防范、身份验证,该场景下的必要性分析认为个人人脸信息与身份信息弱相关,可能与行踪轨迹有关,并认为监控场景下人脸识别应用难以被替代,但是门禁类可用证件、密钥等方式替代,但该文件缺乏对公共安全风险评估以及必要性的具体说明¹²。

根据《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第七条“在公共场所安装图像采集、个人身份识别设备,应当为维护公共安全所必需,遵守国家有关规定,设置显著提示标识”,目前对于公共场所的定义、社区是否属于公共场所我国法律并无明确规定,社区若使用基于技术标准等相关文件对其行为合法性进行说明效力略显不足。

2.2.2. 正当性证明不足

我国《个人信息保护法》第六条第一款提出了对“正当”原则的审查要求,即处理个人信息应当具有明确、合理的目的,并应当与处理目的直接相关,采取对个人权益影响最小的方式。目前社区收集利用人脸信息的正当性证明仍存在途径不明、用户权利未得到充分保障以及物业水平较低的问题。

根据《个人信息保护法》第二十九条,收集户主人脸信息需取得个人的单独同意,为了管理便利,部分物业公司存在未经同意即采集用户人脸信息的情况,在江海区人民检察院所处理的“保护个人信息安全行政公益诉讼案”中,有 7 家住宅小区物业管理公司未经行政主管部门审批,擅自部署并使用了“人脸识别识别”门禁系统,进而完成了对众多小区业主人脸信息的非法采集¹³。根据屿果与户主签订的《温馨提示》(实为人脸信息的授权同意书)所显示,为了推行智慧安防系统,其在社区安装了具有采集人脸生物识别信息功能的设备,用来“提供公寓安全保障、识别住户身份、提供更好的入住服务”,由上海象屿物业管理有限公司对数据进行收集、保存。其他经调查的社区也都以“社区安全、便利用户及社区管理”为目的使用人脸识别系统。在对人脸信息进行收集和使用来看,物业的目的是明确的,但合理性说明并不充分。美国 2019 年《商业人脸识别隐私法案》(Commercial Facial Recognition Privacy Act)第 3 节(d)项规定提到“Application Programming Interface—A covered entity that makes a facial recognition technology available as an online service shall make available an application programming interface to enable at least 1 third party that is legitimately engaged in independent testing to conduct reasonable tests of the facial recognition technology for accuracy and bias.”为在线服务提供面部识别技术的覆盖实体,应开放应用编程接口(API),确保至少有一家合法从事独立测试的第三方机构能够对面部识别技术的精确性和潜在偏见进行公正、合理的评估与测试。从我国目前的相关文件来看,结合《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第十一条¹⁴规定,除了国家安全、公共安全、紧急情况以及取得个人单独同意这四种明

¹² 上海市地方标准《公共场所人脸识别分类分级应用指南》, DB31/T 1467-2024, 第 5.3 部分公共场所人脸识别应用风险分级和附录 A 表 A.3。

¹³ 广东省江门市江海区人民检察院督促整治保护个人信息安全行政公益诉讼案, https://mp.weixin.qq.com/s/RdUVJN6rC-Zdw9A5y_N84Q。

¹⁴ 《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第十一条:除维护国家安全、公共安全或者为紧急情况下保护自然人生命健康和财产安全所必需,或者取得个人单独同意外,任何组织或者个人不得利用人脸识别技术分析个人种族、民族、宗教信仰、健康状况、社会阶层等敏感个人信息。

面合理性行为，其他行为是否合理并无相关的合理性测试的流程及法律规定。

除此之外，根据《个人信息保护法》第四十四至四十八条，户主对于自己的人脸信息的处理享有知情权、同意权、更正权、访问权、删除权以及自动化决策的拒绝权等，但实际用户的各项权利并未得到充分保障。根据上海市地方标准 DB 31/T 1467-2024 第 6.3.5.4 条“个人人脸信息的使用主体可通过授权方式允许授权人对其个人人脸信息进行查询、变更、删除等操作，并确保过程安全”，据笔者调查，多数受访者表示自录入人脸信息后自己对人脸信息的具体流向以及是否用作其他途径并不知晓，人脸信息目前并不同于其他 APP 中个人信息可以被“一键查询”状态，想获知具体信息还需跟物业进行沟通且授权书中大多未提及住户对其人脸信息可以行使删除权、撤销同意授权的权利以及上述权利行使的途径，户主的个人信息权实际受保障程度较低。

另外，根据《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第十五条¹⁵以及第十九条规定可知，作为人脸识别技术的使用者，物业公司需进行预先的个人信息保护影响评估，并须每年对使用的人脸识别设备的安全性及潜在风险进行全面且细致的检测与评估。而人脸信息的社区实际应用中，出于技术原因，人脸识别系统会出现“化妆不认人”、“错误识别”等情况，导致人脸识别错误[5]。以笔者在国家企业公示系统所查询的上海象屿物业管理有限公司为例，其在 2022 年 7 月 26 日前仅能经营物业管理、房地产经纪、停车场(库)经营管理、房地产租赁经营、自有设备租赁等事项，之后虽扩大经营范围但也只是增加一些基础性服务，未体现出“专业数据”处理相关能力，且在今年 1 月份上海市松江区市场监督管理局的抽检里显示特种设备常规检查需整改，仅靠物业公司的技术水平能否充分保护属于敏感个人信息的人脸识别信息不被泄露是存疑的。

2.2.3. 必要性条件不充分

必要性原则主要体现为比例原则。法国数据保护机构 CNIL 在 2019 年发布的《Facial Recognition for a debate living up to the Challenges》中认为对于生物识别信息“Only in cases of absolute necessity and in the absence of any alternative may centralised storage be considered, subject to strict security measures”¹⁶即只有在绝对必要且没有任何替代方案的情况下，才能考虑集中存储，但须采取严格的安全措施，并提到因“Like other similar techniques, facial recognition thus inevitably leads to ‘false positives’, ‘there is a significant element of bias inherent in this technology’”即人脸识别技术的误差以及无法忽视的内在偏见，将决定了需要将成本预算和社会角度纳入考虑以及就人脸识别而言，并非一切都被允许或将被允许，应认识到其某些用途的合法性和合比例性，以及某些用途是被禁止的¹⁷。美国第 117 届国会(2021~2022)通过的《Consumer Online Privacy Rights Act》SEC. 108. CIVIL RIGHTS 中(a) Protections.第(1)款“IN GENERAL—A covered entity shall not process or transfer covered data on the basis of an individual’s or class of individuals’ actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability”也强调实体不得基于生物特征信息来处理 and 传输涵盖数据。

在人脸识别系统引入之前，户主通常以密钥或者身份凭证等方式进入社区，同样便利且易于社区管理。在上文所提上海市地方标准 DB31/T 1467-2024 中也仅认为社区场景下人脸识别是“难被替代”而非“不可替代”。根据 GB/T 41819-2022 的安全通用要求在相同目的或者同等安全要求下应优先非人脸识

¹⁵《人脸识别技术应用安全管理规定(试行)(征求意见稿)》第十五条：人脸识别技术使用者处理人脸信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录。第十九条：人脸识别技术使用者应当每年对图像采集设备、个人身份识别设备的安全性和可能存在的风险进行检测评估，并根据检测评估情况改进安全策略，调整置信度阈值，采取有效措施保护图像采集设备、个人身份识别设备免受攻击、侵入、干扰和破坏。

¹⁶Facial Recognition for a debate living up to the Challenges, p.6 (2019).

¹⁷Facial Recognition for a debate living up to the Challenges, p.8, 9 (2019).

别方式，应仅在人脸识别方式比非人脸识别方式更具安全性或便捷性时，采用人脸识别方式进行身份识别¹⁸，文件以机场、火车站来举例使用非人脸识别方式会明显导致相关服务便捷性下降，但社区人口的日流动量与上述两种公共场所相比实在过少，以人脸识别方式作为验证进入方式不能满足必要性要求。

3. 社区人脸识别收集法律规制途径

根据上文分析，目前为止社区收集仍存在主体法律地位尚不明确、合理性无法测试以及必要性不充分的问题。物业公司，作为一个以盈利为导向的商业实体，在追求利润的过程中，若缺乏相应的监管机制，极有可能导致人脸数据的泄露与滥用。这不仅会削弱社区的安全防线，还可能成为滋生违法犯罪的温床。清华大学法学院教授劳东燕表示，人脸识别技术并非仅限于捕获面部特征，而是通过比对既有数据库中的数据，能够揭示个人的身份信息、行为习惯以及社交脉络，这些信息的泄露将对个体造成终生的影响[6]。因此，对于社区这一与居民生活紧密相连的场所而言，我们必须全面审视并改进人脸信息收集的各个环节，以确保数据的安全与合规。

3.1. 尽快推进相关立法进程

我国目前对于敏感个人信息的保护，主要依赖于《个人信息保护法》这高层级法规以及最高人民法院发布的司法解释作为法律支撑。然而，这些规定在细节上尚显粗略，主要依赖于“同意告知原则”作为处理敏感个人信息的核心准则，实际上户主的知情同意机制存在失灵风险[7]。为了更全面地保护个人隐私，我们有必要进一步完善和细化相关法规，确保个人敏感信息得到更为严格和有效的保护。直接涉及人脸信息具体的文件目前只有《人脸识别技术应用安全管理规定(试行)(征求意见稿)》，该规定第十六条规定“在公共场所使用人脸识别技术，应当在 30 个工作日内向所属地市级以上网信部门备案”，但该规定未对“公共场所”进行定义，社区是否属于公共场所只有参照数据技术标准文件以及各级行政法规进行规制，如 GB/T 41819-2022、上海市地方标准 DB31/T 1467-2024 等，层级较低且分散[8]。

3.2. 以专业数据处理器者为收集人脸信息

根据物业公司作为以提供管理为主的服务类型公司，对于数据方面的处理能力与专业公司之间存在较大差距。在此可借鉴欧盟《通用数据保护法案》(GDPR)的相关规定，GDPR 第 28、29 条要求 Processor 即数据控制者必须采取“足够的措施”来确保其数据安全。具体包括：数据控制者本身需要具备 GDPR 要求所要具备的专业知识，除此之外还需工作身份须独立，不受他人或其他部门干扰、与外界沟通渠道须畅通，联系方式向公众公布、工作内容向管理部门备案，向上级监管部门对接、汇报工作结果¹⁹。其次，依据 GDPR 第 30 条“Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information”，即数据控制者必须详实地记载其处理数据的全过程，分门别类留档保存。包括信息数据的类型、处理方式和传送、接收数据的类别等。最后，GDPR 第 33 条规定：“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it”，一旦数据泄露事故发生，数据控制者必须在发现此类事件后的 72 小时之内，迅速而准确地向相关监管机构提交详尽的事故报告。

3.3. 政府与企业公私合作共建“云平台”

考虑到人脸信息的特殊性以及社区本身负担一定的公共管理职责，可与政府共同搭建“云平台”来

¹⁸ 国家市场监督管理总局、国家标准化管理委员会《信息安全技术 人脸识别数据安全要求》，GB/T 41819-2022，第 5 部分安全通用要求 a) 及 b)。

¹⁹ General Data Protection Regulation, §28, 29.

共同进行管理。最近成都市第十八届人民代表大会常务委员会已于 2024 年 4 月 25 日通过了《成都市数据条例》，预计于同年 9 月 1 日起施行，条例第十二条规定说明政务部门和公共服务组织可以委托第三方收集相关公告数据，同时该条第三款规定“除法律、行政法规另有规定外，可以通过共享获取的公共数据，不得重复收集、多头收集”，人脸信息因被常用于火车站、机场等涉及公共管理的区域，政府部门实际已对人脸信息进行过收集，作为同样承担部分公共管理职责的社区，可以通过共建专门服务于智慧城市的全国联网人脸信息大规模数据库“云平台”，让用户随时可以查阅自己人脸信息的具体利用情况以及是否要撤回授权，社区报批经过政府审核后直接向政府申请来调取个人人脸信息。这样对于户主来讲，可以保障知情权、删除权等权利的正常行使，使户主与社区对于人脸信息的处理处于实质平等地位，对于社区来讲，也免去收集、储存以及暴露数据风险，政府还可实时作为“监管者”来履行维护公共安全的职责，比如及时提醒社区不可将人脸验证作为唯一进入社区的方式等。

4. 结语

随着新时代的到来，技术的迅速更新换代让人们深切体会到科技所带来的便捷。然而，新技术的兴起也必然带来新的问题，这无疑对现行法律提出了更高的要求。例如，人脸识别技术的开发与应用，让人们在各种场景下通过简单的“刷脸”方式进行验证，彻底摆脱了繁琐密码的束缚。然而，人脸识别信息的唯一性、不可更改性以及与其他个人信息的结合所带来的巨大商业价值，使其一旦泄露将对个人造成无法挽回的损失。因此，我们必须对人脸识别信息给予高度的关注。社区作为一个兼具公共管理与隐私保护双重属性的特殊区域，在收集人脸信息时应格外谨慎，仅凭物业公司的力量难以确保所有户主人脸信息的绝对安全，同样以便利管理为目的而使用人脸识别不可取。在科技发展迅速的时代，社区应当拓展合作方式，寻求专业技术人员的支持或与政府协力，以共同构建一个既便捷又安全的社区环境。

参考文献

- [1] 张凯伦, 王倩. “刷脸”的风险, 你知道多少? [J]. 新华月报, 2019(10): 78-81.
- [2] 小区强制刷脸现象突出 App 有泄露人脸信息风险[EB/OL]. 南方都市报. <https://new.qq.com/rain/a/20211218A01K1E00>, 2021-12-18.
- [3] 冯恺, 杨润宇. 人脸识别信息处理中“合法、正当、必要”原则的区分审查[J]. 东南法学, 2022(1): 18-35.
- [4] 焦艳玲. 人脸识别的侵权责任的认定[J]. 中国高校社会科学, 2022(2): 117-128+160.
- [5] 胡昕怡. 人脸识别技术应用法律规制研究[J]. 河南司法警官职业学院学报, 2022, 20(2): 74-78.
- [6] 徐子凡. 劳东燕: 我为何对小区人脸识别说“不” [EB/OL]. 南方都市报. <http://www.fxqwx.org.cn/dyna/content.php?id=14508>, 2020-10-14.
- [7] 张敏, 罗雨. 住宅小区人脸识别门禁系统的应用风险及其法律规制[J]. 江西科技师范大学学报, 2022(3): 39-48.
- [8] 王毓莹. 人脸识别中个人信息保护的思考[J]. 法律适用, 2023(2): 15-24.