居民画像数据应用背景下的个人隐私保护问题初探

张正初
广东南方电信规划咨询设计院有限公司　广东省　深圳市　518000

摘　要：随着智慧城市的深入推进，“人工智能、大数据、云计算等技术已广泛运用于各业务场景，居民画像正是基于机器视觉、数据挖掘等技术能够有效提升对数据的利用，正是这种对数据的利用衍生了各种新的服务、新的管理方法，对人们的日常生活带来极大便利，对基层治理工作带来新的能力。但居民画像数据给管理者提供管理效能、给人们带来方便的同时，也对人们隐私权的保护提出了更高要求。我国对公民隐私权的保护立法相对较多，如《宪法》、《民法总则》、《侵权责任法》、《数据安全法》等，但在实施过程中却暴露出诸多新的问题，导致对公民隐私权的保护难以发挥应有之效。对此，本文主要就当前智慧城市快速推进的时代背景下对个人隐私权保护中存在的问题及完善路径进行分析，期于为完善相关制度、立法，保护公民隐私权尽一份绵薄之力。

关键词：大数据时代；居民用户画像；个人隐私权；法律保护

引言：随着智慧城市建设发展越来越深入，智慧城市建设对大数据的应用场景需求也越来越广泛，对数据采集的维度也越来越多元化，对数据采集的颗粒度也越来越细小，居民画像数据作为智慧城市建设应用中的核心数据，其在综合治理和公共服务应用场景中起到核心纽带的作用，综合治理强调“以人为中心”进行数据治理，强化治理共建共治共享，公共服务强调 “以人为中心”进行精准服务推送，强化精准服务精细管理[1]。因此，居民画像数据在智慧城市、出行服务等应用场景中被广泛利用，并不断被解构、重组、关联，其中有大量数据信息涉及到个人隐私问题，存在较大的个人隐私泄露的问题，怎么样在智慧应用中保护个人隐私，是目前亟待思考的问题。

1 居民画像数据分类

居民画像数据范畴包括其基本属性（性别、婚姻状态、学历、收入水平、健康状况等），社会/生活属性（包括职业、职务、孩子状态、车辆使用情况、房屋居住、手机号码等），行为习惯（常住城市、作息时间、交通方式、居住酒店类型、经济及理财特性、饮食习惯、网购特性等），兴趣偏好/倾向（购物偏好、浏览偏好、音乐偏好、体育偏好、游戏偏好、旅游偏好等），心理学属性（生活方式、个性、价值观等），及人脸识别特征信息、指纹信息、视网膜识别特征信息等。以及以人为中心的显性关系（人与车、同行人、同住、人与房、人与单位、房屋与租客等）均属于居民数据画像范畴。

通讯作者：张正初，1980年9月26，民族：汉、性别：男，籍贯：湖北孝昌，单位：广东南方电信规划咨询设计院有限公司，职位：部门经理，职称：工程师，学历：硕士研究生，邮编：518000,研究方向：信息资源开发利用

2 居民画像数据的应用场景举例分析

2.1 综合治理的安全管理目标是着力解决以下问题

一：安全隐患多，一方面老旧小区的消防检测装置比较少，电动车充电也不规范，容易引发火灾；另外单元楼门禁智能化程度不高，有的居民嫌麻烦，故意把门长期置于敞开状态，也带来了安全方面的隐患。

二：出租房多，租住人员流动性大，陌生面孔多，成分复杂，安全事故频发。

三：治安防控效率低，传统小区治安监控多采用普通的视频监控，普通的视频监控多用于事后取证，难以实现事前防范、事中预警。

四：管理难度大，管理部门主要靠人工管理，工作超负荷，多部门信息不共享，难以开展一体化治理。

五：城市流动人口多，归属感低，对 “有温度的社区”，“安全的社区”需求强烈，需通过精准服务和精准管理满足其要求。

试想，如果能够通过出租房管理、小区门禁、闸机、小区入口监控人脸识别、车辆识别、物业数据、快递、消防采集、保安数据、水电信息、租赁数据等各种数据为社区人口做画像并持续跟踪，进行数据分析碰撞，则一定可以清楚了解小区状态—即使是几千人的大社区。当各个小区如此操作，形成规模覆盖，则可实现事前预防、事后侦查过程发挥价值。

2.2 居民用户画像应用场景

2.2.1 居民公共安全场景应用

（1）人房/人车关联场景应用

在小区的出入口部署人脸闸机、在小区的单元门部署人脸门禁；通过“刷脸开门”可以为居民带来更好生活体验，同时促使居民主动到物业或通过手机APP自助登记基本信息，包含了：身份信息、人脸照片、住址、联系电话、居住类型；居民采用刷脸开门的方式经过人脸闸机/门禁的同时，设备采集了居民的轨迹信息。

分析居民登记信息和居民轨迹信息，通过（未办居住证人员筛查、漏登记人员分析、疑似搬离人员分析、房屋产权变更分析、房屋性质变更分析）五种分析模型，得到精准的实有人口、房屋线索。通过数据碰撞实现访客长期逗留预警、孤寡老人预警、重症精神疾患预警、老年痴呆人员预警、流动人口迁入迁出预警、访客长期逗留预警。

（2）人车关联场景应用

通过人车关联，在社区建立安全防线：

在行人出入口，居民通过人脸闸机刷脸进出小区，实现业主通行、访客放行、尾随告警，进出人员全抓拍；在车辆出入口，不仅可以车牌识别、停车收费，还可以识别车辆前排司乘人员；真正做到小区出入口人过留像、车过留牌。

2.2.2 居民公共服务场景应用

通过居民用户画像，利用大数据分析能力和互联网移动终端，为居民推送政务办事提醒服务，提供健康管理提醒服务，消费偏好推送服务和周边便利设施推送服务等服务内容，增强居民获得感。

2.2.3 居民生活服务场景应用

通过居民用户画像，利用大数据分析能力和互联网移动终端，为居民推送餐饮服务、交通出行、娱乐等生活服务精准推送，偏好设置等。

3 公民隐私权保护的重要性

通过上述居民用户画像应用场景分析，居民用户画像数据社区管理带来了高效、精细的管理能力，同时为居民带了精准的便利服务，但同时我们可以看到，居民画像运用了大量居民隐私数据，如何有效利用居民画像数据，同时建立居民个人隐私保护机制，确保居民个人隐私不受侵害，是本文研究的主要方向。

个人隐私又称私人生活秘密或私生活秘密，是指私人生活安宁不受他人非法干扰，私人信息保密不受他人非法收集、刺探和公开。随着经济快速发展，我国城镇化速度不断加快，人口大量流动的现状推动着社会形态逐步从传统熟人社会向现代陌生人社会转变，公民对隐私权保护的诉求日益高涨[2]。

3.1 隐私权的法律保护现状

3.1.1 宪法保护现状

我国现行宪法没有明确对隐私权保护作出规定，间接对“公民的隐私信息不容侵犯”给予了确认，为其他部门法进一步对隐私权进行保护提供了宪法依据。

3.1.2 民法保护现状

2017 年10 月1 日起正式施行的民法总则中第一百一十一条规定：“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开个人信息。”由于我国宪法没有明确“隐私权”这一概念，因此新的民法总则中依旧没有出现“隐私”字眼，但明确了自然人的个人信息受到法律保护，实现了对公民隐私更为深入的保护。

3.1.3 刑法保护现状

刑法第二百四十五条第一款规定：“非法搜查他人身体、住宅，或者非法侵入他人住宅的，处三年以下有期徒刑或者拘役。”第二百五十二条规定：“隐匿、毁弃或者非法开拆他人信件，侵犯公民通信自由权利，情节严重的，处一年以下有期徒刑或者拘役。”第二百五十三条第一款规定：“邮政工作人员私自开拆或者隐匿、毁弃邮件、电报的，处二年以下有期徒刑或者拘役。”通过对侵害隐私权的行为追究刑事责任，为保护公民隐私权提供了的有效保障。

3.1.4 数据安全法保护现状

数据安全法第二十七条规定“开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。”

第三十八条规定“国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。”

3.1.5 其他法规

（1）侵权责任法

在我国现行法律中，只有《侵权责任法》第二条讲民事权益范围中包括了隐私权根据我国国情及国外有关资料，下列行为可归入侵犯隐私权范畴:

序号	行为分类
1	未经公民许可，公开其姓名、肖像、住址、身份证号码和电话号码。
2	非法侵入、搜查他人住宅，或以其他方式破坏他人居住安宁。
3	非法跟踪他人，监视他人住所，安装窃听设备，私拍他人私生活镜头，窥探他人室内情况。
4	非法刺探他人财产状况或未经本人允许公布其财产状况。
5	私拆他人信件，偷看他人日记，刺探他人私人文件内容，以及将他们公开。
6	调查、刺探他人社会关系并非法公诸于众。
7	干扰他人夫妻性生活或对其进行调查、公布。
8	将他人婚外性生活向社会公布。
9	泄露公民的个人材料或公诸于众或扩大公开范围。
10	收集公民不愿向社会公开的纯属个人的情况。
11	未经他人许可，私自公开他人的秘密。

（2）未成年人保护法

第三十九条 任何组织或者个人不得披露未成年人的个人隐私。

对未成年人的信件、日记、电子邮件，任何组织或者个人不得隐匿、毁弃;除因追查犯罪的需要，由公安机关或者人民检察院依法进行检查，或者对无行为能力的未成年人的信件、日记、电子邮件由其父母或者其他监护人代为开拆、查阅外，任何组织或者个人不得开拆、查阅。

4 居民画像数据个人隐私权保护存在的法律问题

大数据时代，居民个人隐私权保护存在较多问题未得到有效解决，个人隐私保护的存在可操作性缺失、监管职责不明、司法救济困难等问题[3]。

居民画像数据的个人隐私保护更是在上述问题的基础上，存在诸多共性的问题，例如数据生产过程的隐私泄露保护技术问题，数据生成后的数据主权问题[4]，数据关联碰撞后产生新的数据隐私问题，数据关联显性关系人隐私问题等。

（1）数据生产过程中的隐私泄露保护技术问题

在居民用户画像数据运用过程中，为满足精细管理和精准服务需要，会大量使用个人隐私数据，此时应从技术手段上，对网络和数据进行加密，遵照网络安全等级保护制度将隐私数据泄露风险降调到最小。

（2）数据主权问题

在大数据发展过程中，基于大数据产生了诸多数据权利，涉及到个人隐私、信息产权、国家主权等各种权利类型，这些权利类型主体归属不同、权利信息不同，但相互依赖、相互制约，在博弈过程中形成新的权利格局。隐私、产权、主权和霸权主要对应了个人、组织（含个人）、国家和国际之间的数据权利问题，这4 种权利各有不同，不是同一性质的权利，形成数据不同级次、不同范围和不同性质的权利归宿[5]。

（3）数据的数据隐私问题

运用个人隐私数据形成的新的数据同样存在着不同维度的新的个人隐私数据的问题，例如部分商业服务软件对居民画像利用个人身份信息和人脸识别特征信息等个人隐私数据刻画出该行为人的酒店开房记录数据，行车轨迹记录，行踪记录数据等，此类数据能更显性的描述该行为人的隐私。

（4）数据关联显性关系人隐私问题

在居民用户画像数据的运用过程中，很容易能关联到与居民关系紧密和密切联系的人隐私数据，例如同行人关系、同居关系、同车关系等，显性关系人的个人隐私保护问题同样重要。

5 居民画像数据个人隐私保护完善路径

陈帆路学者认为大数据时代背景下个人隐私保护应明确侵犯隐私权的侵权责任，加强监管质量并推动行业自律[6]，居民画像数据个人隐私保护除需完善上述路径外，还需进一步完善数据保护技术手段，明确数据主权，并建立数据生产、数据创新过程中数据的应用规则，标准，从而指导个人隐私数据能更好的运用且又能得到有效保护。

6 结语

大数据时代，公民个人隐私权的保护已是迫在眉睫。由于我国刚进入大数据时代不久，尚未形成一套系统性、规范性的法律体系及管理措施，导致公民个人隐私权在网络上被肆意侵害。居民画像数据给人们日常生活、工作带来的便利性已使人们无法脱离其而生存，故如何在大数据时代加强对公民个人隐私的保护是时代性问题。囿于笔者学识所限，本文所探讨的问题及提出的完善路径均属基础，有待学者进行完善。

参考文献：

[1]2019年11月5日电 《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》（bm01000001）.中国政府网.政务.[2019-11-05].http://www.gov.cn/xinwen/2019-11/05/content_5449023.htm.

[2]徐颖，夏天. 居民家庭经济状况核对工作中公民隐私权保护研究. 经济与法,2018(09):167-170.

[3][6]陈帆路.大数据时代个人隐私权的法律保护研究.法制博览，2019（8）：122-123.

[4-5]冉从敬,肖兰,黄海瑛. 数据权利博弈研究：背景、进展与趋势[A].图书馆建设,2016(12):028-033.