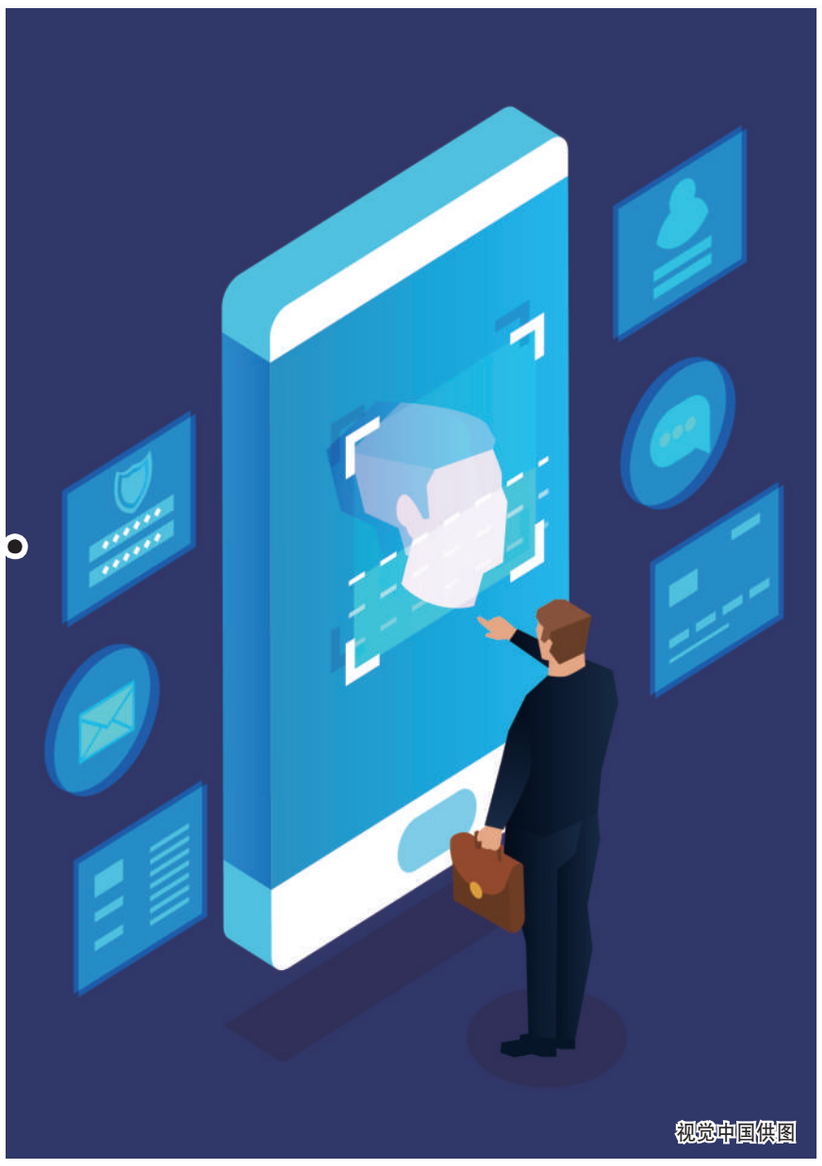
不少人对于人脸识别技术的应用表示担忧，主要认为其有照片泄露的风险。照片泄露就是人脸识别技术的“锅”吗？面对泄露风险，我们要如何应对？

当你的脸变成一串“密码”之后……


视觉中国供图

本报记者 **陈 曦**

伴随着人脸识别技术的发展，其争议始终存在。先是有因不接受动物园将入园方式改成“刷脸”，浙江理工大学副教授郭兵将杭州野生动物世界告上了法庭。而后又发生了清华大学法学院教授劳东燕遇到“不刷脸不让进小区”的情况，对此，劳东燕认为在小区安装人脸识别装置并无必要，并且不经同意收集人脸数据也违反了现行的法律规定，经协商，街道最终同意业主出入小区可以自愿选择门禁卡、手机或人脸识别的方式。

目前，不少人对于人脸识别技术的应用表示担忧，主要认为其有照片泄露的风险。人脸照片泄露就是人脸识别技术的“锅”吗？面对泄露风险，我们要如何应对？

采集：人脸识别相对“温柔”

“在人脸识别技术出现之前，更早的生物特征识别的应用是指纹识别，因为人的指纹具有独一无二的特性以及相应的法律证物价值。从法律意义上讲，摁指纹在古代就已经被较为广泛地应用了。”河北工业大学电子信息系主任、教授邱波表示，其实指纹识别技术应用的历史，一路伴随着更多的反对声音，究其本质，指纹才属于真正的私密性特征，具有法律意义上的信用性。而且指纹需要人配合采集，往往对人心理的冲击力更大。

“因为有接触采集具有心理上的侵入性和强迫性，而非接触采集方式则不具有侵入性。指纹必须按压，才能被采集到，原本属于更难推广的技术。”邱波解释道，相对于指纹，人脸是外露的，并不需要如指纹识别的按压等操作，人脸数据即可被监测系统采集，类似的生物特征识别还有虹膜识别、步态识别等。所以从技术角度上看，指纹识别技术的阻力应该更大一些，而人脸识别相对来说是比较“温柔”的一种方式了。

但当今人脸识别技术变成热议话题，争论不断，邱波认为，这可能和现在人脸相关技术的发展有关。比如将一张人脸跟别的身体组合在一起，PS出一张照片，然后通过技术就可以把这张照片跟一个真实的三维人脸模型相结合，从而制造出一个和照片一模一样的虚拟人。这个虚拟人可以说你从来没说过的话，做你没做过的表情。“这种通过人脸技术做了违背本人意愿的事情，是导致人脸信息采集具有了侵入性的原因，与人脸识别技术本身具有侵入性不是一个层面的。从这个角度看，人脸信息被非法盗用的可能性增加，就导致了大家对人脸识别技术具有很强的戒备心理。”

“如果单从技术角度看，这种私密性争议毫无意义，因为我们正常情况下日常都会露脸，那就有人脸随时被‘抓取’到的可能性，脸本身没有秘密可言。”邱波说。

另一方面，让人们对人脸识别技术戒备心强的点在于，人们觉得看到脸的样子就能和个人其他信息关联起来，而指纹则不然，任何人看到一个指纹并不能立刻知道这个指纹属于谁，所以就觉得很安全。“其实这就是人的错觉，和实际技术识别是两回事。现在通过手机号码、身份证号码，甚至一张名片就能泄露出很多个人信息，脸的信息和这些信息目前也没太多区别。”邱波说。

“因此在录入环节，大家没必要过度纠结于人脸识别的侵入性。”邱波说。

存储：人脸识别并非比对原始照片

“其实人脸识别技术从诞生那天起，其技术就基本保证了存储环节的安全性。人脸识别的技术是不需要存储真实人脸照片的，每张人脸照片在存储的时候都会化为一个个经过精心构造的特征数字码。”邱波解释，人脸图像特征被提取后，就可以进行人脸的编码，生成一个人脸特征向量，从而进行存储和比较运算。也就是说在机器那里，人脸特征变成了一串数字，它们可以表示眼睛之间的距离，眼睛和眉毛的距离、耳朵的大小等等，具体是什么根据特征提取方法会有变化，这样每一张脸都存成了一个“密码”。机器在进行人脸识别的时候，就类似于在密码本中查找特定密码的过程，只需要比对这些数字即可。

那这些数字能随时恢复成照片吗？“实事求是地讲，通过技术是可以把数字‘密码’恢复成人脸照片的，目前有很多科研人员在研究这类技术，而且技术水平也越来越好。”邱波表示，但是防范这个问题也并不难。一方面我们未来在对人脸进行编码的时候，可以采用有损压缩和保密特征提取算法，这样就很难进行真实的高清恢复。另一方面，完全可以通过法律、法规的制定，禁止随意使用这种恢复人脸的软件。

“其实包括手机号码、身份证号等都可以以向量的形式存储，把这些个人的隐私信息都编辑成一般人无法识别的代码。”邱波解释，因为经过编码，这些信息已经变成特定的码序列了，即便被泄露给某人，如果他想要拿到这些内容，还必须先进行解码。而解码器是可以从技术源头上进行适当控制的，因为一般人不具有解码能力，这样就能做到隐私信息不会被轻易泄露。这也涉及另外一个领域叫数据安全，就是怎么保证编辑后的码序列不会被轻易破解。

“虽然技术层面上是可以保证人脸识别技术的安全性的，但是也不能排除一些别有用心的机构，不管出于什么目的，私自保存人脸的原始照片。”邱波强调说。

对此中国政法大学知识产权研究中心特约研究员李俊慧表示，按照《民法典》第一千零三十四条规定，“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。”

其中，个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

按照《个人信息保护法（草案）》第四条规定，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

此外，在《网络安全法》中也有个人信息收集、存储及使用等方面的规定。“对于这些个人信息，只要是依法收集，获得授权，在授权范围内就可以使用。”

泄露：现阶段技术无能为力

“2元钱可买上千张脸的照片”类似事件经常见诸媒体报道，也加剧了人们对人脸识别技术的争议。

“不能一看到私人照片在网络流出，就认为是通过人脸识别采集上来的照片。”邱波表示，人脸照片的流出有多种途径，其中有一个很重要的途径就是“网络爬虫”。这种类似于搜索引擎之类的软件，通过编写好的网络程序，到各类网站上去抓取想要的照片信息，并保存下来。“这些照片很多都是我们自己传到网上去的，因此我们在上网过程中也要注重自我的隐私保护。”

此外，目前许多手机APP在超出产品功能目的范围之外大量收集用户个人信息，有的甚至是在未明确告知用户的情况下偷偷收集。“可能在无意间，我们照片就被别人所收集下来了。”邱波说。

李俊慧表示，目前《个人信息保护法》专门立法进程也在加快。2020年10月21日，全国人大法工委公开《个人信息保护法（草案）》，面向社会征求意见，目前还在征求意见阶段。

除了在法律法规上加以约束外，在技术层面上能否防止非法采集或者“网络爬虫”呢？

“我们无法阻止拍照，也无法阻止大家把照片上传到网上，更不知道这些采集人脸照片的机构是否偷偷保存了原始照片。”邱波说，但目前来说还不具备相应的技术手段防止这些情况的发生。如果强行阻止拍照的话，可以尝试在相机端想办法，比如把所有销售出去的数码相机软件做特殊化处理，以保护照片没有授权不被传播出去等。当然这也是设想，现阶段，还是得通过法律法规来保护我们的个人信息不被泄露。

情报所

北京人工智能专业可以评职称了

变“论文单选”为“成果多选”

本报记者 **华 凌**

11月6日，北京市人力资源和社会保障局发文新增设人工智能专业职称，并正式发布分类评价标准，首次人工智能专业职称评价工作将于2021年初启动。

人工智能是引领未来的战略性技术，是我国新一轮产业变革的核心驱动力。近年来，随着人工智能技术的广泛开发应用，北京作为全国科技创新中心，对人工智能领域人才的需求大幅增长。

当日，北京市人社局发布的《北京市工程技术系列（人工智能）专业技术资格评价试行办法》提出，在职称评价过程中采用“代表作”评审，让人才从“论文单选”到“成果多选”，真正让人才“干什么、评什么”。

谁能评：覆盖北京地区人工智能工程技术人才

人工智能是研究计算机模拟人的思维过程和智能行为的学科，涉及计算机科学、控制论、自动化、仿生学、心理学、逻辑学、医学和语言学等多门学科，研究成果广泛应用于教育艺术、医疗诊断、金融贸易、工业制造、新零售、物流运输、农业科技、无人汽车等领域，是首都“新基建、新场景、新消费、新开放、新服务”产业发展的重要组成部分。

据介绍，人工智能工程技术人员是从事与人工智能算法技术的研究开发和系统设计应用的工程技术人员。他们普遍具有较高的学历和专业技术能力，但由于属于新兴、交叉学科领域，没有合适的职称晋升渠道，缺乏规范的行业资格评定标准，影响到技术交流合作和人才职业发展。

此次开设人工智能职称专业，纳入工程技术系列，并设置正高、副高、中级、初级四个层级，将满足北京地区各梯次人工智能工程技术人员的职业发展需要，为人工智能产业发展和全国科技创新中心建设提供有力的人才支撑。

评什么：分别制定两类人员的业绩条件

据介绍，人工智能专业四个层级全部采取评审方式进行，并按照北京市深化职称制度改革的要求，将申报人分为人工智能研究和人工智能应用两类，除申报职称所需要的基本条件外，按照“干什么、评什么”，分别制定两类人员的业绩条件。

以申报正高级职称为例，从事人工智能研究的申报人，应具有很强的研究能力：主持省部级及以上人工智能领域研究项目、课题；或制定国家、省市或行业人工智能领域发展规划、重大战略决策等相关政策、标准、规范；或发表的研究成果，推动人工智能专业发展，取得显著的经济社会效益。

从事人工智能应用的申报人，应具备很强的生产、技术管理实践能力：在技术革新、引进和推广新技术等方面实现重大突破；或研制开发高难度、较复杂的人工智能领域新产品、新设备、新工艺等已投入生产；或完成本单位人工智能工程项目的规划和实施工作，在项目管理、科研开发、技术推广应用等工作中成效显著，取得显著的经济社会效益。

除此之外，北京市还为业绩突出人才制定破格申报条件。申报人员只要满足破格条件之一，可以不受学历、资历、次级职称等限制，直接申报副高级职称。

据介绍，人工智能专业职称评价工作打破“唯论文”桎梏，全面推行代表作评审制度，申报人员可自主选择发明专利、技术报告、研究报告、设计文件、技术标准、专业论文、专著编著等最能体现自己能力水平的代表性成果参加职称评审。

怎么报：实行职称全程网上申报

此次人工智能专业职称评价工作实行社会化评价，采取“个人自主申报、行业统一评价、单位择优使用、政府指导监管”的方式，每年开展一次。其中，正高级评审由北京市人事考评办公室组织开展；副高级及以下层级评审由北京信息产业考评服务中心组织开展。

每年1月，北京市人力资源社会保障局将发布全市年度职称评价工作安排，申报人可对照《北京市工程技术系列（人工智能）专业技术资格评价基本标准条件》确定申报层级需求，并查阅年度评价工作安排，在市人力资源社会保障局网站申报。经过评审机构网上初审、工作单位推荐公示、评审机构网上复审缴费、答辩评审、验收公示等流程，申报人取得北京市人工智能专业职称证书，用人单位可根据岗位需要，择优聘任专业技术职务。

AI化身调解员，每天解决4万个网约车投诉

本报记者 **张佳星**

“我们的平台每天接待大概4万个投诉。”10月29日，在“智能出行、引领未来”媒体沟通会上，首汽约车CEO魏东坦言，每个投诉要核实、要给双方反馈、要敦促车队长问询……整个沟通过程繁琐冗长。

投诉尽是负能量，如何让它在最短时间结束？AI或许能帮上忙。

“行程录音是解决投诉的重要依据，人工智能如果能够自行锁定纠纷关键点，将大大缩短处理时间，也能给出司乘均认可的判断。”魏东说，智能出行行业正探索大数据、人工智能等技术在出行行业中的创新应用，为用户带来更安全、舒适的出行体验。

炼成金牌调解员，AI要会的不止一项

“我们在全国160个城市都部署了网约车平台，因此投诉会来自全国各地，各种各样的口音，凭人工去听是根本不可能的。”魏东说，人工智能语音识别技术为“不可能”带来了可能的解决方案。

目前，国内普遍通过行程录音辅助安全监控以及用户问题投诉处理相关问题。然而，现有的语音解决方案常常因为录音质量问题难以达到预期目标。

“如果涉及到骚扰，比如说了脏字，需要来回核实、定位，还存在方言的问题，而在各种各样杂音的干扰下，很多时候录音是很不清楚的。”魏东说，处理投诉必须要保证乘客的体验、给乘客好的答复，也要保证公平、不冤枉司机。

解决投诉，AI需要集“听风者”“方言通”“金牌调解”于一身，这样的AI哪里有？

“我们调研后发现，出行行业没有现成的、能够排除干扰、准确识别不同方言的、锁定纠纷关键词的录音识别模型可以直接拿来用。”首汽约车副总裁闫磊说，越细分的任务越需要自己开发模型。

“然而，从头自行开发的话成本高、也缺乏基层架构的人才。”闫磊说，首汽约车的技术研发人员更多的是数据工程师，而自己搭建整套的人工智能平台，包括模型的系统训练都需要专业平台和团队。

过去优秀的AI那么多，它们的“成才”经历一定能够帮助有特定任务的AI成才。“这就跟给孩子找教辅差不多，要寻求专业的团队合作。”魏东说，语音识别的模型、语义判别的模型、机器学习的适宜算法……这些如果可以和首汽约车的大数据、司乘场景等结合，将能够形成适用于出行行业的智能语音解决方案。

对此，亚马逊云服务（AWS）提供了相应的开发平台。双方团队进行合作，在平台上进行模型的定制、算法的定制，团队在深入了解行程录音的特点及技术需求后，开发了语音降噪和导航音分离算法。首汽约车的数据科学家和算法工程师只需要专注数据和业务逻辑，将数据的“灵魂”输注给AI，无需运营和管理复杂的机器学习系统。

把AI打造成“听风者”“方言通”还有“金牌调解”，是之前没有的。“合作团队要从零开始对模型进行训练、调优，包括让AI与出行的业务部门进行沟通磨合，因为他们对行业非常了解，所以是最资深的评委。”AWS大中华区产品部总经理顾凡说。

预判，是未来智能出行的“基本功”

还有相当一部分投诉产生在服务发生之前，乘客投诉司机推单，司机投诉乘客找不着，AI能不能把这些误会压缩到最少；还有司机巡游的情况，一天开12个小时车的司机，多少个小时是空驶，AI能不能帮他们找到客户？

在魏东看来，这些智慧出行中需要解决的“痛点”，通过人工智能和机器学习未来都会得到缓解。

“过去的智慧出行1.0中，通过平台调度匹配模型，司机能够看到哪里是热点区域，就会来这个地方等单。”魏东说，这种模式其实可以更智慧一些，比如热点区域有十个需求，从东边过来几辆车合理、西边过来几辆车合理，后台需要通过预判来告知司机。

预判是未来智能出行中调度AI的“基本功”。“单纯的热点区域展示，还算不上智能调度。”魏东说，AI要有本领能够使得司机相信听它的确实能拉到很多单。

基于对历史数据的分析、推测、预判，调度AI将告知司机，去哪个方向、哪个目的地，去多少量车是合理的。通过精准的调配，按照指令行动的司机90%以上可以提前赶到乘客预计的出发地，进而提升订单的匹配成功率，减少司机的盲动。

此外，安全，无论是驾驶安全还是司乘人身安全，是网约车从诞生以来一直必须面对的问题。

预判也可能会成为解决这个问题的“钥匙”。魏东说，当碰到乘客情绪波动时，会产生什么后果，期望在未来更进阶的人工智能能够给出早期干预。

图说智能

对话未来

第三届进博会技术装备展区内各式先进机器设备随处可见，高度智能化的机器应用场景让人大开眼界。

图为11月6日，在进博会技术装备展区微软展台，一名观众与EX仿生机器人对视。 新华社记者 **李任滋**摄