羊城晚报记者 张闻 周哲

目前市面上常见的半球形监控摄像头、枪型监控摄像头、云台旋转摄像头、云台室外球机摄像头，哪一款是用于人脸识别的摄像头？答案可能出乎人们的意料——只要经过简单的后台改装，它们都能用于人脸识别。

近日，针对公众普遍关注的“人脸识别”等信息安全问题，羊城晚报记者走进佛山的商场、楼盘营销中心等地，调查了营销场所的摄像头安装情况，并多方求证是否存在“偷脸”风险。

针对人脸识别等信息安全问题，羊城晚报记者进行实地调查

警惕！任何摄像头经改装都可人脸识别

走访 监控摄像头已成各大商铺“标配”

今年3月下旬，佛山市人民检察院牵头，联合佛山市市场监督管理局、佛山市公安局、佛山市住房与城乡建设局在全市范围内开展人脸识别摄像头专项行动。3月26日上午，执法人员在佛山市南海区一楼盘营销中心发现了11个尾部接有网线的长焦摄像头，执法人员随后来到该营销中心机房，发现其中一台设备电线上竟贴有“人脸识别”的字样。随后，执法人员依法查封了摄像头和主机设备，进行了进一步调查处理。

该事件经媒体曝光后，立刻引起公众关注。不少网民在留言中投诉佛山多个楼盘营销中心都装有人脸识别监控摄像头。有的楼盘安装人脸识别摄像头，是便于销售人员“看人下菜碟”。

根据网友提供的线索，记者对佛山禅城、南海、顺德三个区部分楼盘和商场进行了走访。记者首先来到上述被曝光的某楼盘。在该楼盘的营销中心，记者发现，被执法人员拆走摄像头后，营销中心的一楼和负一楼统一换上了体积更小的半球形摄像头。而在佛山新城华润旗下某楼盘、禅城区朝安路某楼盘营销中心等，均装有枪型摄像头。

在禅城区印象城商场以及商场店铺内，记者发现数量众多的监控摄像头。其中，商场侧门处的枪式摄像头后侧有多个接口，十分便于改装。商场内优衣库店铺在收银台设有两个半球形摄像头；商场内的名创优品店除设有半球形摄像头外，还装有一个体积较大的云台旋转摄像头。

揭秘 靠摄像头外观不能判断是否可人脸识别

上述走访看到的摄像头是否具有人脸识别功能呢？记者随后进行了多方求证。

记者首先登录多个网购平台查找类似型号。在淘宝平台上，搜索“人脸识别摄像头”已显示不出任何商品，但通过“人脸识别”等关键词搜索，依然有不少“漏网之鱼”。而在拼多多平台，最便宜的人脸识别摄像头标价不到200元。多个平台对购买人脸识别摄像头均无任何限制。对于记者发给客服人员走访时拍下的摄像头，客服人员均否认这些摄像头有人脸识别功能。

然而，多位行业内部人士表示，从技术上说，即使是最简单的半球形摄像头，经过后台改装也具有人脸识别功能。

“通俗来说，人脸识别的实现有两种方式。一种是前端识别，也是目前人脸识别的主要方式，即在摄像头里安装人脸算法的芯片；但其实还有后端识别，可以通过加装后端服务器，对抓拍的人脸‘按图索骥’。”长期从事人脸识别设备产品解决方案的段浪（化名）告诉记者，后端识别方式耗费成本较高，“但理论上，所有摄像头，不管是否安装人脸算法芯片，都可以通过后台改装实现人脸识别。”

段浪表示，目前，除了必要的公共职能部门使用人脸识别摄像头外，一些商场、景区、楼盘等也搭建起人脸识别的网络平台。其中，使用摄像头联网，通过人脸识别进行数据关联收集客户信息，成为部分楼盘的“潜规则”。

那么，能否通过摄像头外观判断摄像头是否具有“人脸识别”功能？段浪明确表示，基本不可能。

另一位长期从事电子设备采购业务的赖先生告诉记者，客户完全可以要求摄像头生产厂商打造定制版本，“虽然这样价钱比较高，但隐蔽性更强，一般人很难发现。”

维权 遇到人脸识别侵权申诉时要“证据保全”

“人脸识别”逐渐泛滥，如何监管成为公众关心的问题。以记者走访的佛山为例，据悉，佛山市检察院等部门持续跟进人脸识别摄像头专项行动，将在近期公布相关推进情况。

如果市民发现被商业机构摄像头进行人脸识别，该怎样维权？广东省律师协会民事法律专业委员会副主任、广东宝慧律师事务所主任律师蔺存宝表示，人的面部特征具有唯一性，不经同意的人脸识别肯定是侵权。但目前《民法典》等对于个人信息的保护尚无明确规定。

蔺存宝表示，目前因刷脸造成的个人信息被侵犯主要集中在消费领域，消费者可通过消委会等组织进行上诉。然而，由于很多“人脸识别”具有隐蔽性，证据并不在公民一方，所以若要上诉可向公诉机关或法院要求先进行证据保全。此外，公民也可以通过一些迂回的方式，比如说与商场签订谅解书等，把证据先确定下来。

面对人脸识别，下一步该如何监管？佛山市政协委员、民建佛山市委会副主任梁永流建议，对人脸识别技术从开发应用的源头进行监管，对人脸信息在事关公共利益的领域和在商用的领域做分级管理。对安装人脸识别设备的要求必须进行申报，并进行详细的审核。同时，媒体对个人面部信息的安全性也要加大宣传力度，让市民认识保护面部信息的重要性。

“目前随着大数据在社会各领域应用越来越多，政府也在不断积累大数据治理的相关经验。”蔺存宝表示，建议未来政府要有专门针对大数据监管的机制，加强对个人数据的保护力度。

一个App控制18万个摄像头 会员注册付费偷窥他人隐私

不法分子利用黑客技术轻易破解并控制家用及公共场所摄像头，搭建App或利用其他视频管理平台向客户收取“会员费”“套餐费”牟利，无数隐私画面通过“第三只眼”被窥探无余……4·15全民国家安全教育日前夕，记者调查发现，在相关部门加大对网络摄像头隐私泄露黑灰产打击力度的同时，仍有不法分子采用隐蔽的方法出售破解摄像头ID及破解软件，且价格“水涨船高”，对公民隐私安全带来巨大的威胁和隐患。

隐私监控黑灰产仍存在“隐秘角落”

日前，记者调查发现，在部分社交软件中，不法分子通过较为隐蔽的方式出售已经被破解的摄像头ID和破解软件。例如，在QQ上，他们以“摄像头”为用户名吸引客户，在客户添加好友时，会收到提醒，需添加另一个名为“客服”的QQ号才能通过。

简单咨询后，这名客服人员列出“价目表”。其中，包括168元、238元的“家庭套餐”以及收费更高的“酒店套餐”和大学附近酒店，破解摄像头ID数量在12个至15个之间。当记者询问是否用某App（可公开下载的网络监控系统）进行绑定观看时，对方表示，现在不能用了，需换成另一款远程监控系统。

此外，该客服列出的价目表中还包括摄像头破解软件，可扫描破解附近摄像头，价格为520元。记者注意到，随着相关部门和网络平台加强该黑灰产业的防范打击，这些违法资源价格也有所上涨，破解软件的价格上涨了200元，破解ID的单价也上涨了近一倍。

记者采访发现，在执法部门查处的案件中，犯罪分子正是利用了客户偷窥心理非法牟利。在北京市第三中级人民法院日前审结的一起案件中，被告人巫某某控制了全球18万个摄像头。“我收藏或录制的都是一些私人住宅里人体裸露的视频。”一名巫某某的“客户”李某证言称，他注册这个App的会员后，分两次支付668元成为终身会员。“观看不限时间，随机出现6个镜头内容，可以收藏、录制，内容有私人住宅、公共场所、培训机构等。”

低门槛为违法犯罪大开“方便之门”

据了解，摄像头隐私泄露黑灰产的门槛非常低，一些不法分子甚至不需要拥有较高的计算机水平，只需要买到“傻瓜操作”的黑客软件或付费寻找技术人员帮助，就可获取大量破解的摄像头ID。

上述案件的承办法官告诉记者，巫某某就是从网上购买了一款“反编译软件”，并非法获取了某品牌网络摄像头的用户数据库，在这个数据库的基础上搭建了名为“上帝之眼”的App，后又重新经营名为“蓝眼睛”的App，数据从“上帝之眼”导入，服务器挂在境外。再通过吸引用户有偿登录应用程序，观看网络摄像头实时监控内容。

根据百度去年发布的《2020网络黑灰产犯罪研究报告》，网络犯罪将会是未来十年全球显著的风险之一，同时黑灰产犯罪即将进入AI时代，AI安全也将成为各行各业不容忽视的关键问题。

北京师范大学刑法所副所长彭新林认为，各部门应联合行动，加大对利用物联网设备犯罪行为的打击力度，在鼓励创新发展的同时加强行业监督和指导。网民也要增强安全意识，强化安全防护措施，发现黑客违法犯罪线索后要及时举报。

受访人士同时指出，企业要重视办公环境网络安全，定期检查摄像头等设备，建立网络安全防护体系。网民对网络社交平台的账号、密码尽量采取分类管理，针对各个平台使用不同的密码，且尽量使用高强度的密码，还要经常性地更新重要网络平台的密码。

（据新华社）

中国社科院法学所发布法院信息化发展报告

未来机器人极可能取代法官写判决书

羊城晚报记者 董柳

机器人能不能像人一样撰写出专业的法律文书？中国社会科学院法学研究所、社会科学文献出版社，14日在江苏南通联合举办的“《法治蓝皮书·中国法院信息化发展报告No.5（2021）》（以下简称《法院信息化蓝皮书》）发布会”上，一项研究报告给出了参考答案：“实践证明，在未来，它极有可能取代法官完成判决书的撰写。”

眼下，“AI法官”“AI律师”等已经从概念走向现实，人工智能应用于司法裁判已成为热点话题。那么，机器人取代法官撰写判决书，未来在哪些领域可行？它是否能够精准平衡案件中的法、理、情？

机器人用15秒完成文书撰写

“机器人能否像人一样撰写出专业的法律文书？这是我们实验室的重要实验课题。”发布会上，中国社会科学院法学研究所研究员、科技与法研究中心主任，法律人工智能实验室首席顾问杨延超发布了《人工智能应用于司法裁判的法理分析》成果报告。

杨延超介绍，对这一问题的研究，首先是从撰写律师专业的代理意见开始着手的。“我们对一部叫‘FILE’的机器人进行了大量的实验，最终发现它可以在知识产权领域为律师撰写专业的代理意见。”

在一项实证研究中，实验中的证据材料有6页（均为PDF版本），机器人从阅读证据材料到完成文书撰写共耗时15秒。

“当然它一定会比人快，重点是人工智能跟专业的法律人相比，谁写得更好？”杨延超举了两个较为经典的案例，这两个案例是关于商标领域的行政裁决。相关法律文件通过机器人撰写后被递交上去，为相关企业赢得了权利。

“按照我们之前的测试要求，机器仅负责撰写初稿，律师要修改完善。但在这两个例子中，律师并没有修改。最终，负责裁判的评委会委员也没有识别出代理文件是完全由机器撰写的。”杨延超说，这样的实验对于进一步研究人工智能在司法中的应用提供了很多启示。

对交通肇事案学习效果较好

“不同于律师的代理意见，法院的判决书还需要综合各方面的意见，它并非一方利益诉求的无限延展，其价值体系中应当包含公平、制衡的理念，我们实验室正在展开这项研究。实践证明，在未来，它极有可能取代法官完成判决书的撰写。”杨延超说，一个优秀的判决包含两个核心要素，一个是结果要公正，一个是论理要充分。要让机器人完成判决书撰写，就需要在这两个方面下功夫。

他表示，为了保障结果公平，让机器人学习既往与此相关的大量判例，依据是数学中一个重要的定理——正态分布定理。事实上，机器人基于正态分布及一系列数学原理，可以完成对前人经验的汲取，对于类似案件，其所完成的判决结果呈现既不偏激也不保守的均衡态势。

“基于机器学习的需要，我们把案件总体上分为两种：个性化案件和共性案件。像‘杀人罪’就属于个性化案件，每个案例的发生背景、人物关系、被告人内心演变都存在极强的个性化特征，即使用数学原理和统计学原理亦难以找到神经网络的建构规律。当前，此类案件用于机器学习的效果并不理想。相比较而言，像交通肇事罪以及知识产权类侵权案件，可以划归共性案例，借助数学原理可以实现其神经网络的建构，此类案件机器学习的效果较好。”杨延超表示，我国当前90%的知识产权侵权案件实行法定赔偿原则，即原告方难以找到被告方侵权赔偿的相关证据，于是法官们在判赔时主要适用知识产权法上的“法定赔偿原则”，即由法官在法定赔偿额以下实行自由裁量。在此类案件上，人工智能借助机器学习的原理来给法官提供强有力的裁判示范参考。

涉及情感性论理需法官完成

“机器人在撰写裁判文书时，还需要完成逻辑论证。”杨延超说，仅有结果而缺乏论理的判决不能称其为正义的判决，因此机器人撰写判决时需要阐述论理过程。

杨延超介绍，从实验室完成的大量实验看，机器人基于对同类案例的学习，完成论理描述是完全可能的。在以犯罪四要件为模型建构的神经网络中，机器人会汇总本案全部事实，针对一项具体犯罪指控，完成对犯罪主体、犯罪客体、犯罪主观方面、犯罪客观方面的论述。在这一过程中，机器人的任务系将本案的基础事实与法律规范紧密结合在一起，进而完成判决的论理部分。

杨延超也指出，机器人的论理并非取代人类的论理，尤其是涉及情感性的论理部分，法官仍需基于自身的价值观完成论理说明。正确认识人工智能在法律中的应用，不能过分夸大，这里还需要认知人工智能在多元法律复杂思维以及情感思维方面还存在着技术瓶颈和障碍。让机器去做什么，让人去做什么，合理地划分人与机器的边界对于未来法律人工智能的战略制定具有重要意义。

“人工智能在法律应用上的最大价值，不是效率，而应当是公平正义。”杨延超说，“此前，我们对公平正义的理解，往往基于法官个人或者法律人个体的经验、阅历，但极为有限。人工智能算法模型的一个重要价值在于它可以极大地拓展人类的认知和智慧，以同案同判为例，机器算法模型可以告诉我们历史上这个案件是如何判的，全国以及全球这个案件是如何判的，从而极大地拓展了我们追求公平正义的广度与深度，从有限走向无限。”

业内争论

支持派强调应用价值 反对派担忧法律危机

《法院信息化蓝皮书》同时指出，当下人工智能应用于司法裁判，理论上存在一定的争议。支持派凸显人工智能应用于司法裁判的价值，并试图将价值论应用于司法裁判的全流程；反对派更侧重于强调人工智能应用于司法裁判带来的负面影响，其中较为典型的便是机器审判人类的法律危机。这也暴露了人工智能应用于司法裁判的两对主要矛盾——

一是“效率价值”与“正义价值”之间的矛盾。“弱人工智能”时代，机器人法官系作为人类法官的辅助而存在，并非是由机器独立完成对于人类的审判。在“人机合作”模式下，机器人虽未能达到与人具有同等法律地位的地步，但它的作用已经远远超过工具的范畴，基于深度学习而实现的“自我决策”可以让机器人更大程度地影响法官，由于“算法黑洞”（即不知道人工智能是依据何种算法逻辑审判）等问题的存在，其决策公平性仍需进一步明确。

二是“算法局限”与“裁判扩张”之间的矛盾。基于当下人工神经网络的算法，人工智能只能解决司法裁判中的某些具体问题，还很难贯穿于司法裁判的各个环节，其在事实认定和法律适用方面均存在一定局限。

建议构建算法审查制度

编写《法院信息化蓝皮书》的专家们提出，为了实现对人工智能在司法裁判中的有效规制，未来要在两方面予以完善——

一是人工智能适用空间的分割。其中要实现情感价值与法律价值的二元分割，将情感的问题交给人，将法律的问题交给机器人，准确地划分人工智能的适用空间；事实认定与法律适用的二元分割，案件事实认定的部分主要由人来解决，涉及法律适用的问题则主要由机器人来解决；新型案例与常规案例的二元分割，常规案件更多依赖机器人解决，以期发挥机器人基于以往案例的学习经验，新型案件更多依赖人来解决，以期在缺乏基础数据的情况下，更多发挥人的价值判断。

二是算法审查制度的构建。为解决当事人提出的“算法黑洞”的法律质疑，应构建机器人算法审查制度。主要包括：人工智能算法公开制度，应用于司法裁判中的机器人，因其决策会影响当事人的财产权利与人身权利，在对其算法技术秘密保护方面应奉行有别于一般商业机器人的原则，其算法理应向社会公开，并应当遵循“全面公开”“网络公开”“初始公开”三项原则；人工智能算法裁决制度，诉讼当事人一旦对机器人算法提出质疑，则需要一个专门的算法裁决机构完成审查和裁决。人工智能算法救济制度，一旦算法本身被确认为违法，该司法裁判机器人的算法应当停止使用或者被修正。