外滩大会上，“AI助手”绽放异彩

如何成为人类得力助手？真正挑战还在未知的远方

展台上正在展示如何鉴别不同类型Deepfake照片 记者 夏天 摄

□ 记者 夏天

聚焦

你知道吗，如今依靠AI技术，已经可以解读你的医疗报告，通过你的毛发测出一些健康状况，以及对长者进行便捷的认知症筛查和训练。你也可以“聘请”AI作为你的“金融管家”，帮助分析行业板块、完成基金加自选等理财动作。

当然，快速发展中的AI技术始终面临数据安全法治的战略考量以及数据安全与治理难题。

9月7日，备受瞩目的“2024 Inclusion·外滩大会”圆满落下帷幕。三天的会期里，这场国际权威科技媒体眼中的“2024下半年最值得期待的全球创新科技大会”，以“更开放、更前沿、更创新”的姿态，为全球观察中国AI产业落地和发展打开了重要窗口。记者获悉，本届外滩大会共吸引了5.2万人现场参会，无论是参会规模还是国际嘉宾的数量，均创下了历史新高。

先进鉴真技术下，越来越多Deepfake无所遁形

AI的发展也伴随着模型内部幻觉、安全漏洞、深度生成内容滥用、能源难题等挑战。带着这些疑问，记者参加了主题为“预见数智未来——科技创新与法治保障”的2024外滩大会检察分论坛。本次论坛由上海市人民检察院主办、黄浦区人民检察院承办。与会嘉宾围绕构建有竞争力的数据跨境流动制度、人工智能影响数据安全法治的战略考量、公共数据的开发与应用、AI时代的数据安全与治理、数据要素价值发展的司法驱动等主题作了主旨发言和与谈。

“在智能体的框架下，风险主要源于五方面。”蚂蚁集团数据安全总监杨小芳表示，一是使用GPT导致的机密泄露；其次是智能体中会加载非常多的插件，比如查天气、订车票这些，它们在带来便利的同时，也会带来新的威胁，比如被窃取用户的隐私信息等。在人工智能的领域，攻击者可以利用非常多的方法来获取并复制大模型。

杨小芳指出，风险中还包括了一些不良的企业和个人使用个人隐私、用户记录以及各类敏感信息直接用于模型训练，利用智能体开展黑客攻击等违法犯罪。在AI生图和AI生视频这种多模态技术的应用之下，以假乱真捏造各种各样的虚假新闻，在国外已经屡见不鲜。

那么，国内的行业领先企业在AI安全方面有哪些最新探索？杨小芳介绍：“今年我们增加了对于AI和服务供应链以及知识库这些因为智能体所带来的新型组件的安全扫描能力。在外置安全方面，我们也拓展到了针对于底层系统和服务的保护，以策略化的方式快速识别和处置风险。”

她还提及“蚂蚁大模型安全一体化解决方案”，叫做“蚁天鉴”。在展区“未来安全实验室”，记者就对“蚁天鉴2.0”的“AI鉴真”功能进行了一番深入体验。对于人脸识别、证照等受到Deepfake威胁的高发领域，目前都有了有效的应对策略。

“比如这张电子营业执照，我们的AI就能通过光照、材质、纹理等要素，鉴别出极有可能是伪造的。”展台技术专家向记者演示了一段鉴真案例。另外一位展台工作人员当场拍摄了一张自己的证件照，随即通过类Deepfake技术生成了大笑、配戴眼镜、嘴部动作视频等动静结合的三张伪造影像，并试图让影像通过人脸识别鉴定。但在人脸识别、活体检测、风险信号等技术的综合鉴别下影像并未通过，有效实现了在线欺诈检测和持续风险监控。

“未来健康”已来，AI会读报告、筛查认知症

“金融、医疗等高信息密度、专业严谨的领域会是最先看到AI应用效果的产业。”在今年外滩大会见解论坛“人工智能和金融世界的对话”中，美国著名学者凯文·凯利这样认为。蚂蚁集团总裁兼首席财务官韩歆毅也认为：金融行业已经高度数字化，医疗领域也沉淀了高价值的数据，AI能够针对专业领域做训练，又具备强大的通识、理解和沟通能力，有机会带来专业服务的普惠。

果不其然，记者在展厅中央，第一眼就被规模庞大的“未来健康”展区吸引。尤其是一块写有“眼科门诊、胸外科、健康体检、医保智付”的导览牌，让记者仿若置身医院，也彰显了AI在用户健康领域越来越大的覆盖面。

比如在蚂蚁医疗开发的“报告解读”功能中，用户只需上传图片或10MB以内的PDF医疗报告，AI就可提供专业的医学解读，给出针对性的分析和建议，可以显著缩短用户在医院线下奔波的时间；“脑健康”板块具备简易的3分钟小游戏大脑健康测试，以及7分钟专业大脑测评，让老年用户自己或在亲属协助下，仅需使用手机，即可接受AI阿尔茨海默症筛查，比社区筛查更为便捷，在一定程度上进一步便于人们提早发现隐患，并展开有针对性的训练和治疗。据展台技术人员介绍，大脑测评引入了医院认知症筛查内容进行模型训练，具备较高的可信度。

本报此前曾报道过，上海检察机关针对药品说明书上字体过小、不便于老年人等群体无障碍使用展开公益诉讼的成功案例。在未来健康展区，记者也看到了通过AI技术赋能，这一问题有了另一种解法：“AI识药盒”“测毛发”等系列家庭健康服务。用户只需拍摄自己手中的药品包装盒，就能通过AI识别，于屏幕上清晰展现其应对症状、用法用量等关键信息。此外，全国首个数字健康人“安诊儿”也来到展台，利用AI大模型、数字人等技术，帮助医疗机构为患者提供覆盖就医前、中、后的“AI陪伴就诊”服务。这一数字人的推出，也为老年人的就医提供了便利。

记者还参观了“未来财富空间”，“沉浸式”感受AI原生体验的理财服务，用语音唤起AI金融管家的全程陪伴，帮助解读市场热点、分析行业板块、完成基金加自选等理财动作，体验个性化的理财小简报、智能化的实时解答、专业化的投资分析等。

20多位“AI助手”大放异彩，彰显“科技为人”

据悉，本届外滩大会共有1场开幕主论坛、36场开放见解论坛，500位演讲嘉宾聚焦“AI产业新实践”“科技人文新思考”“金融科技新探索”等领域，带来了深度的思想交锋。35项行业领先的科技成果首次亮相和落地，其中包括蚂蚁集团推出的AI生活管家支小宝、AI健康管家和智能体开发平台“百宝箱”，复旦大学研发的纳米线人工视网膜修复视觉，西湖心辰公司研发的端到端语音大模型心辰Lingo等重量级科技产品。

来自全球105家科技企业参展，15家头部大模型企业携手亮相，20多个AI助手在展区大放异彩：数字分身辅助完成工作、赛博宠物消解孤单、脑机辅助深度睡眠、人造肌肉纤维给你温暖拥抱等。

在为期三天的大会中，与会嘉宾共同探讨并总结出当前AI产业实践的六大趋势：端智能成AI应用的关键引擎；异构算力助力抢跑大模型应用之战；高质量数据成为企业AI战略制高点；专业领域应用成大模型技术加速发展的“探照灯”；智能体是新型终端形态，孕育新一代超级平台；具身智能变革智能陪护与未来制造。国际嘉宾普遍认为，2024外滩大会已经成为全球观察中国AI产业落地和发展的重要窗口。

本届大会新增设的“创新者舞台”和“AI创新赛”也引起参与者的热烈反响。44位科技才俊在创新者舞台上展示了他们精致而富有创意的科技探索成果。AI创新赛共吸引了来自超过20个国家和地区的7000多支参赛队伍、近万名选手报名，选手们来自北京大学、复旦大学、斯坦福、麻省理工学院、新加坡国立大学等高校，以及微软、谷歌、中科院自动化研究所、微软亚洲研究院等企业和科研机构。

大会发布的“科技人文十问”引起了与会者的广泛共鸣和热烈讨论。如何应对AI与人类抢饭碗？人类的思考力会因为AI退化吗？“人机共生”时代还有多远？AI可能超越工具属性，获得意识，甚至建立AI文明吗？……“科技为人”是外滩大会给出的答案。美国著名学者凯文·凯利在大会演讲中表达：“我们今天所担心的许多问题，或许并不是最难解决的，真正的挑战可能是我们还未曾想象到的未知问题。要实现我们期望的由人工智能驱动的未来，最好的途径之一就是积极参与其中。”

作为全球金融与科技创新的中心，上海这座充满活力的城市为外滩大会这场科技大会注入了其开放与包容的基因。外滩大会正在成为上海科创生态系统的重要组成部分，以及上海科技创新活动的标志性事件之一。