新民环球

本报国际新闻部主编 | 第811期 | 2023年6月15日 星期四 本版编辑：丁珏华 编辑邮箱：xmhwb@xmwb.com.cn

拟声、换脸、生成假图片、炮制假新闻……

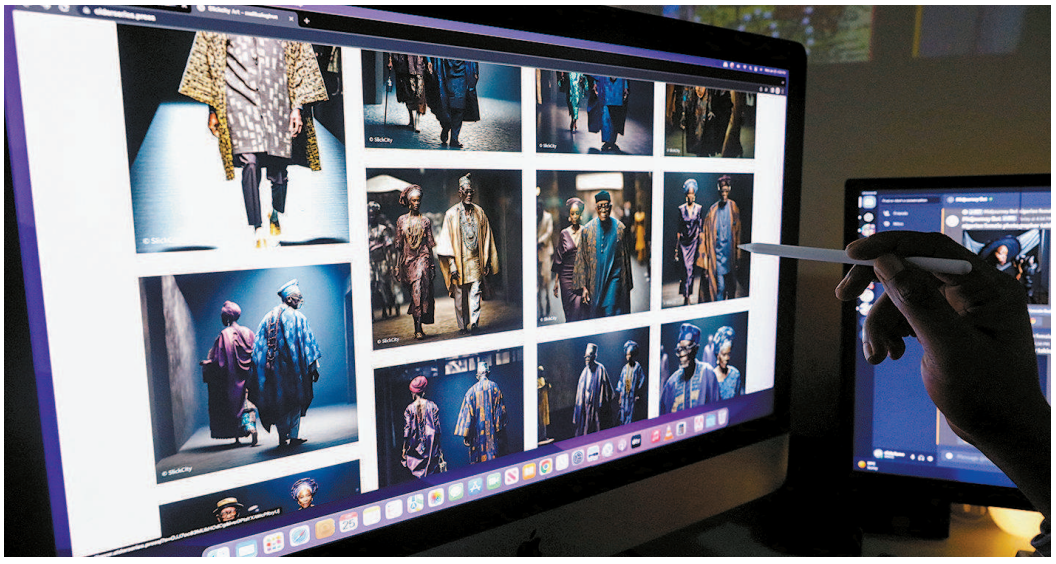
AI造假“浪潮”涌来 人们如何“上岸”？

文 / 本报记者 **王若弦**

这是一个人工智能（AI）技术飞速发展的时代，这是一个真实和虚假愈加难辨的时代。

一张美国前总统特朗普亲吻前白宫首席医疗顾问福奇的照片近日引发争议，后经网友仔细查证，这是一张AI生成图，由特朗普的党内竞争对手德桑蒂斯团队炮制，目的是抨击特朗普在任时抗疫不力。

克隆声音、一键换脸、炮制假新闻……当AI制造的谎言潜入现实，究竟该如何厘清真假的边界？



▲ AI软件可以轻易生成“逼真”图片

◀▼ AI软件生成的特朗普被捕图和特朗普福奇亲吻图 图GJ

拟声换脸骗局频现

当电话另一端传来亲友的呼救声，谁会想到这竟然是一个赤裸裸的AI骗局。前段时间，一对加拿大夫妇就经历了这样一场“声音克隆噩梦”。

据《华盛顿邮报》报道，这对夫妇3月接到一通电话，电话那头一名自称律师的男子说，他们的儿子珀金因在一场车祸中撞死一名美国外交官而入狱，出庭前急需21000美元律师费。

让故事显得更为逼真的是，电话中还传来了近似珀金的声音。这对夫妇挂完电话慌作一团，立刻跑去银行将钱转给“律师”。直到儿子当晚打电话过来，他们才发觉被骗。

这家人迅速报警，经警方调查，电话中“儿子”的声音是诈骗集团根据珀金在社交平台发布的视频，利用AI技术仿造他的声音。

尽管查明了事情真相，被骗的钱财却一去不复返。美国联邦贸易委员会（FTC）营销实践部助理主任威尔·麦克森表示，追踪语音诈骗者极为困难，他们使用的电话可能位于世界上任何角落。

同样在3月，美国的格雷格夫妇也接到了类似的电话。诈骗者模拟他们孙子布兰登的声音，称人在监狱，需要一笔保释金。

AI技术正在让冒名诈骗变得更容易，且成本更低。FTC最新统计结果显示，冒名诈骗已经成为当下美国第二大热门诈骗类型。2022年此类案件超过3.6万起，其中约5000起为电话诈骗，损失金额超过1100万美元。

加州大学伯克利分校数字取证学教授汉尼·法里德指出，AI技术的进步让诈骗者能够轻易地根据简短的音频样本来复制声音。“两年前，你可能需要大量音频来克隆一个人的声音。但现在，只要你在脸书或者TikTok发一段超过30秒的音频，复制声音就可以迅速实现。”

声音可以模仿，面容也可以替换，AI换脸早已不是新鲜事。美国游戏主播Atrioc就发现自己的脸被“偷”了，有不法分子利用AI换脸技术制作她的不雅视频，并发布在社交媒体上。崩溃的Atrioc试着向警方求助，等来的答复却是——她所在的州目前还没有相关法律可约束或惩罚这样的行为。

虚假信息混淆视听

不只是普通人，在AI的骗术面前，一些媒体也难以招架。

英国《每日邮报》4月报道，一名22岁的加拿大年轻人为了能在韩国娱乐圈出道，以某韩国男团成员的面容为模板，花了约22万美元整容了12次，最后在韩国一家医院不幸丧命。这则新闻一出，便引发了《纽约邮报》八卦版“第六页”、加拿大媒体公司Postmedia等媒体的跟风报道。

但没过多久，一些媒体进一步查证后发现，或许这根本就是个编造的故事，主人公可能并不存在。因为韩国媒体询问警方后得到的回答是——当时并未收到类似的死亡案例报告。而检测网站的结果显示，这名加拿大年轻人的照片有75%可能由AI生成。

面对公众质疑，《每日邮报》删去了这则报道。但意外的是，5月又有媒体报道，这名年轻人的家人站出来证明他们儿子的死亡和报道的真实性。不过，这篇报道没有提供任何实质性的证据，也没有提供家人的真实信息和照片。

如今，这名年轻人的身份和报道的真伪依旧成谜。在自由撰稿人拉斐尔·拉希德看来，这件事向媒体人发出了警示，就是现在比以往任何时候都更需要在核查事实、揭穿谣言以及问责方面发挥作用，提升自己的媒体素养和批判性思维能力。

AI生成的虚假信息还广泛出现在政治领域。几张特朗普在纽约街头遭警察围捕的图片3月在社交平台疯传，图片中特朗普被警察抓住双手摁倒在地，场面十分混乱。

而事实上，这些图片均出自开源信息调查网站bellingcat创始人、英国独立记者艾略特·希金斯之手。他利用AI绘图软件生成了特朗普被捕的图片，“我只是在闹着玩，原以为只有几个人会转发”。但令他没有想到的是，这条推文的浏览量在两天后就突破了500万次。

如果说这些AI炮制的假新闻只是混淆了视听，那还有些假新闻则对社会产生了实实在在的影响。

5月22日，一张五角大楼爆炸的AI生成图在网络上引起轩然大波。数字原创媒体Vox报道，在短短几天内，这一假图片就引起了一阵恐慌，甚至在短时间内撼动了美国金融市场。

值得注意的是，用AI技术抹黑政治对手并不只是民主党的伎俩。共和党也曾使用AI制作一段30秒的视频，呈现美国总统拜登连任后的场景：银行纷纷倒闭、金融市场崩盘、旧金山被封锁……用虚假的图片和报道描绘了一系列危机。

人工智能公司“抱抱脸”安全和政策专家艾琳·索莱曼认为，AI已经被广泛用于政治宣传和操纵选举，未来的道路将会十分艰难。观察人士担心，AI技术的快速普及可能会加剧2024年美国大选中虚假信息的传播。美国联邦众议员伊维特·克拉克警告，“如果AI技术在大选中被用来大规模操纵和欺骗选民，将会对美国的国家安全造成严重后果”。

如何治理面临挑战

虽然自互联网诞生以来，虚假信息就一直存在于网络世界，但近年来随着ChatGPT、Midjourney等AI工具的出现，以及Photoshop等绘图软件功能的更新，大规模生产超逼真的假图像、视频和文本变得更加容易便捷。

欧洲刑警组织一份报告预测，到2026年互联网上多达90%的内容可能由AI创建或编辑。目前，完全由AI生成的假新闻网站已经出现，而且在短短几周内这些网站的数量就上涨了两倍。

当AI造假的浪潮日益逼近，我们该如何分辨真伪、找寻真实？有媒体分析认为，或许应从技术研发、完善法律法规以及提高公众意识和教育等层面入手。

有业内人士建议加强AI反制技术研究。眼下确实有一些科技企业正在加强对图像、声音伪造技术的反制研究，但到目前为止，并没有一个通用的标准来识别真实或虚假的内容，AI反制技术要随着AI技术的进步而不断更新。

也有分析指出，AI技术的健康发展离不开相关法律法规的完善。例如，对于流媒体平台上AI高度模仿歌手的行为，完善版权法或许是一个相对有效的策略。

另有专家表示，未来AI可根据大数据创造出无比接近真实的“真实”，要通过不断的教育改变大众观念，让人知道眼见不一定为实，有图不一定有真相，对网络信息提升辨识力。

尽管对“AI造假”的有效治理道阻且长，但不少国家和地区已经开始着手应对。德国《世界报》近日报道，欧盟正在采取行动打击AI深度造假。欧盟委员会委员薇拉·尧罗娃表示，识别深度造假的技术已经存在，希望脸书、谷歌、TikTok等社交媒体平台能够大规模使用这些技术，并且通过软件发出警报提醒用户，而这项规则以后也可能被纳入欧盟正在制定的《人工智能法》。

诚然，AI技术的发展是把双刃剑，一方面，它以惊人的速度在推进医疗技术、改善人类生活质量等领域发挥着积极作用；另一方面，它也带来了一定的风险和挑战。

在5月召开的伯克希尔-哈撒韦公司的年度股东大会上，“股神”巴菲特谈及对AI的看法时流露担忧。他表示，尽管发明AI的初衷是好的，“但当某种事物可以做各种各样的事情时，我有点担心”。他将人工智能比作原子弹：“在二战期间，我们基于充分的理由发明了原子弹，但这项发明对未来世界而言，真的是件好事吗？”

巴菲特认为，AI将改变世界上的一切，除了人类的思维和行为方式。或许，在这个AI飞速发展的时代，在真实和AI营造的虚幻之间，我们应该思考的，是如何保持一个具备独立思维和理智思辨的头脑。