

# AI“换脸”有风险,你还敢“ZAO”吗?

近日,一个叫 ZAO 的 AI 换脸 APP 突然火了。其号称“仅需一张照片,出演天下好戏”。通过 AI 换脸技术,用户上传一张照片,就能按照所给的模板制作视频,成为梦寐以求的“戏中人”。身边真有些人参与了 ZAO 的视频制作,或用自己照片或恶搞别人。由于 ZAO 满足了普通用户的猎奇心理,一夜之间,便迅速占领了朋友圈和各大头条的阵地。

ZAO 的一夜爆红,让 AI 换脸软件引发广泛关注,一系列问题和质疑也随之而来:用户照片会不会被恶意使用?刷脸支付还安全吗?视频素材是否拥有合法版权……

据悉,9月3日,工信部已对北京陌陌科技有限公司相关负责人进行了约谈,ZAO 也更新了隐私协议以及用户协议,删除可免费使用用户肖像权条款。在肖像权属问题上,ZAO 强调,其为保证肖像权不被冒用,设置了真人验证环节。

不过,ZAO 换脸事件引发的隐私安全争议却仍在继续,人们对人工智能未来走向的探讨更趋激烈。

## 为啥 ZAO 能爆红?

从 faceu 的换脸功能,到 zepeto 的捏脸游戏,“换脸”已经不是什么新鲜事,但 ZAO 的爆红比之前同类型的 APP 更为迅速。

8月30日上线,不到24小时,ZAO 就以火箭般的速度在各应用商店免费应用排行榜中攀升至第二位,同期更是微博热搜前十话题。

与 faceu 和 zepeto 不同的是,ZAO 把“展现理想中的自己”这件事更往前推进一步。只需上传一张照片,就可以迅速生成视频,实现与明星“同台”的机会,还可以与朋友共同“出演”。客观来讲,虽然在人物移动的过程中,人脸边缘会有接缝瑕疵,但总

体来说十分神似,一颦一笑都很有感觉。

将换脸从过去的静态图片,带入到动态的视频动画之中,让网友身临其境,置身于各种经典的电视电影桥段中,并显现出 AI 换脸技术从专业化到平民化的趋势,可以说是 ZAO 一夜爆红的最大原因。

## 最大的隐患和风险

伴随 ZAO 病毒式流行的背后,其暗藏的隐患也不可忽视。围绕法律、版权、隐私等诸多问题,网上涌现出大量质疑声。

不过,在业内看来,落在用户身上真正的风险,既不是通过诉讼或监管即可确认无效的用户协议、不合理的肖像权归属,也不是著作权侵权问题,而是用户一旦提供或让渡,即可能完全失控的“生物识别信息”的安全问题。

“人脸识别是人可识别的个性化信息中的核心,同时也是隐私权保护的核心。”业内认为,一旦泄露,远比上网时产生的数据信息遭泄露的风险更大。

据了解,换脸技术主要涉及生物信息的采集,属于敏感信息。根据网络安全法第四十一条规定,网络运营者收集、使用个人信息,应当遵循合法、正当、必要的原则,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息,不得违反法律、行政法规的规定和双方的约定收集、使用个人信息,并应当依照法律、行政法规的规定和与用户的约定,处理其保存的个人信息。

业内专家表示,这款应用的出现还意味着,AI 深度换脸技术的使用门槛大幅降低,一旦相关伪造音视频被不法分子利用,将对国家安全、新闻舆论、公众安全、刑事审判、政府通信等领域带来众多难以预测的风险。比如,如果 AI 深度换脸技术制造的虚假视频与社交网络相结合,不仅会

让假新闻更难鉴别,也会导致谣言的迅速传播;再如,不法分子可利用图片、视频冒充他人跟另一个人聊天、交易,在司法机关调查取证、审判等阶段伪造出来的影音视频证据,也可能对司法程序产生干扰。

## 人工智能渴望前瞻性立法

“核心风险是个人信息安全问题,换脸软件一旦被滥用将会产生消极影响。相关部门的立法重点应该关照到未来人工智能下的数据滥用和信息防范,研究者们应该遵循科技伦理,企业合规和风控部门应当加强法律风险的审查,政府部门应当加强监管,行业组织加强自律,公民积极投诉举报。”有业内表示。

北京师范大学法学院网络与智慧社会治理研究中心主任刘德良认为,相关法律法规的建立完善要具有可操作性,要有利于大数据和人工智能产业的发展。大数据、人工智能产业本身就需要数据搜集,现在我们的个人信息已经存在于 N 个商家和机构中,泄露了也不知道是从哪里泄露的,防止的不是泄露,关键在于不能滥用。

他表示,要从立法上让进行身份识别的机构或者平台(比如银行、支付平台、电信公司、保险公司)去承担责任。如果用户的个人信息被盗用、滥用,有两种思路去问责:一是对这些机构、平台进行过错推定,除非能证明履行了核实比对义务,这种义务的标准随着技术、时代的变迁也会不断升级改变,需要司法按照这个标准去判定取证,来确定是否尽到义务,才可以免责,否则就要和假冒者一起承担连带责任;二是更加严苛,承担无过错责任。如果法律有这种规定,就会倒逼机构、平台认真核查比对,甚至会想方设法开发更新的技术手段,来有效避免身份被假冒滥用。如果不这样立法,掌握个人信息的机构、平台就会把风险转嫁给假冒者,让个人承担风险。

文/丰雪

## ★ e 周关注

## 阿里花 20 亿美元成网易考拉的“爸爸”

在近一个月的传闻发酵后,网易考拉最终还是加入了阿里“动物园”。近日,阿里确认以 20 亿美元收购网易考拉,考拉将保持独立品牌运营,天猫进出口事业群总经理刘鹏兼任考拉 CEO。经过多次传闻转折,最终尘埃落定,此次收购案例也被业界称为“中国进口跨境电商并购‘第一案’”。

对此,专家评论称,收购后,会降低竞争强度,大家都得以喘息,各得其所。而阿里收购网易考拉,是在扩充其全球供应链的版图。

“这次收购将一定程度上削弱竞争强度。网易考拉在海淘领域的市场份额仅次于天猫国际,而海淘的畅销商品以标准品为主,价格透明,多家公司竞争意味着难以盈利。网易考拉牵手天猫国际,将占据中国跨境电商市场的半壁江山。”一位电商界人士分析称。

数据显示,截至 2019 年 7 月份,网易考拉月活跃用户数达 935.27 万人。在业内看来,阿里如果收购网易考拉,既“消灭”了自己最大的竞争对手,也成为行业内绝对的老大。而且,以母婴产品起家的跨境电商网易考拉,正好可以弥补以美妆为主的天猫国际。以新品首发定位的天猫国际平台,擅长一线品牌首发,考拉则侧重二三线品牌,双方的有效融合将形成业务上的优势互补。

不过,阿里系的交易总量还是远远低于庞大的代购微商群体,腾讯系用社交电商对中心化电商,用小众非标垂直对货架电商标品,用供应链服务赋能小 B,阿里系依然面对腾讯系或者京东系的激烈竞争。

而对丁磊而言,20 亿美元卖身阿里,显然是一个务实的决定。跨境监管日益严格,阿里的天猫国际和京东的海淘全球紧跟其后,网易考拉增速逐步放缓。同时,仓储物流的短板和较低的毛利率,对于网易考拉而言,也存在不小的压力。此次“转会”阿里,“考拉”将获得阿里的资金、流量与生态支持,在跨境电商领域取得长远发展。

跨境电商是中国消费升级的产物,丁磊进入的时机踩点很准,依靠自采自营的高品质、高体验管理迅速赢得用户。但跨境进口市场空间大,群雄角逐,价格战激烈,GMV(成交总额)数字好看,但都不赚钱。

“考拉这种自采自营的,成本尤其高,烧钱冲量不是丁磊的个性。阿里不一样,市场份额是首选,盈利次之。收购后,会降低竞争强度,大家都得以喘息,马爸爸要江湖地位,丁总想赚钱,可谓各得其所。”业内分析道。

《2018 年度中国进口跨境电商发展报告》指出,进口跨境电商形成了“三个梯队”:第一梯队为网易考拉、海淘全球、天猫国际等“头部平台”,规模大、流量大、品牌多;第二梯队为洋码头、唯品国际、小红书、聚美极速免税店等;第三梯队大多为蜜芽、贝贝、宝宝树、宝贝格子等母婴类产品平台。

分析人士认为,此次并购有望实现“1+1>2”的效果,是一场双赢的并购案。一方面,一旦阿里收购网易考拉成功,意味着阿里将占据整个中国跨境进口市场一半以上份额,形成强势的市场领导效应;另一方面,阿里可以阻击拼多多的新品牌计划,也丰富了其产品线,在某种程度上抑制了其他平台的市场扩张。

文/容和



## 25 家中国企业跻身领英“顶尖创业公司排行榜”

## 人工智能赋能企业多赛道创新

全球领先的职场社交平台 LinkedIn(领英)近日在中国首次发布“顶尖创业公司排行榜”,25 家上榜的中国本土初创公司,被评为最具人才吸引力的热门企业,其中字节跳动、滴滴出行、比特大陆、依图科技、Momenta 位居榜单前五。值得注意的是,在 25 家上榜企业中,有 11 家企业的主营业务是以人工智能为核心并与产业落地应用相结合的,如比特大陆、依图科技、第四范式等,分别以“人工智能+”的形式,聚焦芯片研发、

面部识别算法、科技金融、智能医疗、智慧城市、新零售、智能制药等众多领域,从影响单一行业,逐渐向赋能百业发展,这个榜单也是人工智能赋能百业的一个缩影。此外,当资本热钱的刺激逐渐褪去,这些潜心研发产品、完善技术,打磨商业模式的企业始终保持屹立不倒。伴随着国家产业政策的扶持,将人工智能等核心领先技术与企业产品及解决方案深度融合,不仅助力企业创新性发展,更加速产业智能化进程,实现

产业全面升级。

领英“顶尖创业公司排行榜”连续三年在全球多个国家及地区发布,由领英编辑团队基于全球超过 6.45 亿会员的实际行为数据,以员工增长速度、会员参与度、职位关注度、对顶尖人才的吸引力四个维度进行分析得出。该榜单首次落地中国,旨在展示优秀初创企业的卓越表现及对顶尖人才的吸引力,以及为中国职场人士提供更多职业发展的可能性。

文/叶梓