

起底AI造谣乱象——

你被AI生成的假新闻骗过吗

近年来,人工智能(AI)技术发展迅速,成为全球科技领域的热点。AI已经从单纯的学术研究发展成为改变人类生活方式的重要力量。然而,却有一些别有用心之人将其变为造谣、敛财的工具。

今年6月,一条“广东省五华县华阳镇一70多岁老人被殴打致昏迷,其孙子为此跳河自杀,打人者一审被判九年十个月”的短视频在互联网平台传播,引发大量网民关注、讨论。经公安网安部门开展调查发现,该视频的图文内容系移花接木、肆意编造的网络谣言。据造谣人员某供述,这段长达几分钟、声色并茂的视频全是由AI合成的。目前,公安机关已依法对任某追究法律责任。

此事件并非个案,随着AI技术应用越来越普遍,一些网民为博眼球、蹭热度,将AI技术用以编“伪消息”、造“假新闻”,以此来获得网民关注和点赞量,进而实现流量变现。

专家表示,AI造谣具有定制化、门槛低、识别难、破坏大等特点,亟须加强监管。同时,可以通过设置AI生成内容提示标识、严格落实网络实名制等技术手段进行治理。

AI造谣门槛低、危害大

今年8月,一则“福建南平松溪县遭遇严重大风袭击,造成枣岭街一人死亡”的消息在网络上迅速传播。这则消息图文并茂,甚至还有逼真的视频片段,一时间引得大量网民关注和转发。但经公安机关核查发现,这竟然是用AI编造而成的网络谣言视频。

“当前AI网络谣言具有仿真性和规模性的特征。根据输入指令的不同,AI在短期内能够批量生成大量内容不同的网络谣言,而且生成的网络谣言信息内容更加贴合人类表达方式,并结合深度伪造技术生成图片、视频、录音,使得社会公众越发难以辨识网络信息的真伪性。”北京航空航天大学法学院副教授赵精武告诉记者。

记者随机用“AI文案速成”小程序测试,在对话框内输入“火灾”这一主题有关的内容创作指令,便生成了一篇新闻报道,甚至包括现场救援细节、及消防安全提示,让人真假难辨。赵精武指出,AI网络谣言的危害性主要表现为扰乱社会公共

秩序,削弱政府公信力、诱发电信网络诈骗等。

为牟取非法利益 造假涉嫌构成多种罪名

赵精武分析,个人或组织利用AI技术造谣背后的动机是复杂多样的,既包括部分网民为了寻求存在感、刺激感,故意编造AI网络谣言,也包括犯罪分子为了牟取非法利益,编造AI网络谣言,以便顺利实施电信网络诈骗等犯罪活动。

今年6月中旬,一家MCN机构的实际控制人王某某因利用AI软件生成虚假新闻并大肆传播,扰乱公共秩序,被警方行政拘留。据警方通报,王某某共经营5家MCN机构,运营账号842个,自今年1月以来,王某某通过AI软件生成虚假新闻,最高峰一天能生成4000篇至7000篇。

近日,浙江温州苍南公安成功打掉一个编传旧案谣言的MCN机构“网络水军”团伙。进一步侦查发现,相关账号和视频由某网络科技有限公司(实为以MCN模式运营的“网络水军”团伙)使用发布,该MCN“网络水军”团伙搜集全网敏感热点,随意设置虚假剧情,利用AI软件

根据剧情自动生成多处关键情节虚假的文案,安排真人出境解说,拼接网络中误导性素材后剪辑成所谓“原创”视频。该团伙明知上述视频充斥大量虚假、挑动群众情绪类信息,为博取流量、不法牟利,在多个平台公开发布,后造成虚假视频信息被大量浏览、传播,从而牟取非法流量返利。

中国人民大学刑法学博士、北京市京律师事务所实习律师黄福涛告诉记者,编造虚假的险情、疫情、灾情、警情,在信息网络或者其他媒体上传播,或者明知是上述虚假信息,故意在信息网络或者其他媒体上传播,严重扰乱社会秩序的,处三年以下有期徒刑、拘役或者管制;造成严重后果的,处三年以上七年以下有期徒刑。如果行为人不只制作、传播虚假信息,而且目的是骗取互联网平台上不特定多数人的财产,则涉嫌诈骗罪。

如何治理和防范AI网络谣言

为治理AI乱象,深化网络生态治理,近年来相关部门出台了多项政策和措施。

2023年1月10日起施行的《互联网信息服务深度合成管理

规定》指出,任何组织和个人不得利用深度合成服务制作、复制、发布、传播法律、行政法规禁止的信息,不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动。

2023年8月15日起施行的《生成式人工智能服务管理暂行办法》规定,提供和使用生成式人工智能服务,应当遵守法律、行政法规,尊重社会公德和伦理道德。不得生成煽动颠覆国家政权、推翻社会主义制度,危害国家安全和利益,损害国家形象,煽动分裂国家、破坏国家统一和社会稳定,宣扬恐怖主义、极端主义,宣扬民族仇恨、民族歧视,暴力、淫秽色情,以及虚假有害信息等法律、行政法规禁止的内容。

“加强AI领域的司法治理,需要立足于‘安全与发展并重’和‘分级分类监管’的基本原则,针对诸如生成网络谣言等技术滥用现象,既需要在事前阶段明确研发者、服务提供者以及网络平台的主体责任,还需要在事后阶段严格追究违法行为人的刑事责任、行政责任。”赵精武强调。

据央广网

酒店偷拍黑产调查——

酒店偷拍直播“不愁卖”,万部视频付费看

10月28日晚,酒店房间灯光亮。关门声后,一对年轻男女进入房间。

两人也“走进”正对大床高处的一处隐蔽摄像头,最后被定格在手机APP里一个3CM×6CM、名为“A6”的视频画面中。

他们交谈、嬉笑甚至更私密的行为实时传来。画面之外,是一双双窥私的眼睛。

在这些“眼睛”背后——摄像头安装工的招募,每天在各平台、社交软件里发布;摄像头被“种”进酒店、民宿的客房后,又以“直播台”的名义被打包出售。

一名卖家说:“只要我不被抓,永远都可以看。”

招募安装工 偷装摄像头

10月14日,某网站“摄像头吧”内,网友“上帝有只眼”发帖:有“台”了,都是精品。

每个“台”对应一个酒店房间内的摄像头。每新增一个“台”,意味着又一枚摄像头被偷装进酒店房间开始运行。

在卖“台”过程中,卖家通常会从偷录的视频中截取一些“精彩”画面,并打上“完美视角、真实刺激、高清有声”等吸睛标签,招揽买家。

同一时间,在一款加密社交软件中,十多个群正在高价招募针孔摄像头的安装工。这些群的名称都含有“偷拍”“酒店”“针孔”“安装”等关键词,每个群的订阅者有数千人至上万人不等。

记者随机进入一个有着2700多名订阅者的群,以安装工的身份向群主咨询安装事宜。

按群主的说法,安装工需先

支付摄像头押金以获取群主邮寄的偷拍摄像头。到酒店安装时,会有专人通过视频指导并进行调试。安装完成后,群主退回押金,报销酒店房费,并付给安装工一笔佣金。记者了解到,一台摄像头的押金多在500元—1200元之间,安装后将支付8000元至上万元的佣金。

偷拍摄像头优先安装在入住率较高的酒店或大学城附近的酒店。“这样可以拍摄到更多私密视频。”群主说。

其提供的多张摄像头照片显示,只有绿豆大小的插电式摄像头,由排线连接电路板。摄像头电源线与酒店房间电源相连,插入房卡通电后,摄像头开启录像,录制时不会发光。

一些偷拍摄像头还可以连接锂电池或充电宝,操作更简单。“放在房间的排风口、空调软管、天花板灯带等隐蔽处附近,一块电池能拍一两个月。”群主说。

这类充电式摄像头也多被装进抽纸盒、驱蚊灯等常见日用品的内部,成为与房间陈设“融为一体”的偷拍设备,受到多位群主推荐。

酒店“直播台” 被打包出售“不愁卖”

网友“上帝有只眼”发帖后不久,便有多人评论留言,提出观看意向。

记者私信获取“上帝有只眼”的微信后,对方将16个针孔摄像头捕捉到的住客私密图片,以5张或6张拼为一组,发给记者选购,“5个‘台’580元,6个‘台’680元。”

从这些图片可以看出,偷拍



摄像头被安装在不同类型酒店的房间高处,能俯瞰整张床,但角度各有不同。“你喜欢看什么样的角度,就选哪组‘台’购买。”对方称。

付款后,“上帝有只眼”让记者下载一款名为“TP-LINK物联”的手机软件,并发了来虚拟号码注册的登录账户和密码。记者登录该APP后,发现在“设备”栏中已有5个房间的直播画面。5台设备分别被命名为A3、A4、A5、A6、A7。

记者随机点开一个房间,不仅可以观看房间内的实时画面,还能查看该房间7天内被摄像头偷拍的全部视频。这些视频被随机切分为10多秒钟至几分钟不等的片段存储在云端。其中一个房间的云端存储显示:今日新增271段录像。

“上帝有只眼”告诉记者,这些摄像头连接着房间内的线路,只要房间插卡通电,设备就会从“离线状态”自动进入拍摄模式,实时直播,并上传至云端存储,“确保房间有人时,摄像头就会

直播、录制,这样能节省存储空间。”购买者在登录账户后30天内,可以随意观看直播和录制的视频。

“一组5个‘台’,880元一个月。”该网友称,这些偷拍摄像头的观看权并不愁卖,他们除了在网站发帖外,还通过社交平台等渠道推广,“只是发得隐晦一些,然后引导意向客户购买”。

在某加密社交软件的群里,摄像头直播台被冠以“情趣酒店”“入住率高”等各类标签,明码标价售卖。

卖家一般将4个至8个直播“台”打包成组出售,平均每个“台”的价格百余元。一次性购买的“台”越多,价格越便宜。

代理发展下线 卖“台”层层分利

卖“台”是个一本万利的生意。

在摄像头偷拍黑色产业链中,受利益驱使加入“下线代理”的人迅速扩张,已成为偷拍视频“滚雪

球式”快速传播的重要一环。

一名安装代理告诉记者,他是一级代理,从境外赌场获取摄像头,“一次拿一两百‘台’”。偷拍画面会打上赌博游戏的广告,以卖“台”和出售视频的方式为境外赌场引流。

他自称手下的二级代理每安装一台摄像头,能拿到1.8万元佣金。二级代理再找人代安装,会支付1.2万元佣金。逐层递减,每级代理既自己安装挣佣金,也招代理挣差价。

另一名长期招安装工的代理表示,安装工每安装一台可以得到数千元至上万元的佣金。他同时也招募销售代理,只要给他交代理费,他可以将部分“台”的权限卖给记者,由记者再加价售卖。

偷拍摄像头 “借”合规APP直播

记者再次打开“TP-LINK物联”APP,发现从“上帝有只眼”处购买的5个直播台中,有两个显示“设备已离线”,点击后,虽无实时画面,仍能查看过往7天已上传至云端保存的视频。

多个售卖酒店偷拍直播台的商家表示,他们的直播,均通过下载“TP-LINK物联”APP实时观看。

前述网友向记者介绍,有人购买直播台后,他们会提供登录“TP-LINK物联”APP的账户和密码,然后将摄像头主账号的观看权限,分享给购买人,“一个主账号,可以将观看权限分享给几十人”。

多位卖“台”者也提到,摄像头分享的人数越多,收益越大,传播范围也越大。 据《新京报》