

当下,在短视频平台或者是直播平台上购物成了很多人的新选择。刷视频的时候,还经常会冒出熟悉的明星,用流利的乡音推销农产品,有的还进行直播带货。这些所谓的明星很可能是仿冒的。近段时间,网络上一些商家利用AI技术仿冒带货。有的借助名人效应,仿冒专家学者、奥运冠军、影视明星,也有的借助产地效应,冒充知名品牌。消费者、粉丝难辨真伪,慕名下单,却不知道自己被蒙了。这些游走在灰色地带的“AI李鬼”,正考验着我们的数字治理能力。

据央视新闻



直播间现水中摘辣椒画面



真的樟树港辣椒很矮



AI生成的画面,辣椒有一人多高 视频截图

起底AI仿冒带货新骗局

你刷到的奥运冠军代言,可能是假的

违背常理,直播间出现水中采摘辣椒画面

近段时间,一些网络直播间,打着樟树港辣椒旗号的辣椒种,成了主播推销带货的重点。记者注意到,这些直播间的销售人气很旺,不时有人咨询或下单购买。

湖南岳阳的樟树港辣椒属国家地理标志农产品,有400多年的种植历史,因量少质优,特级产品可卖到300元一斤。

而在这些网络直播间,记者看到,画面中展示的辣椒成串垂挂,产量奇高。当记者在直播间询问辣椒种子是否保真,种出来有没有这么大时,主播纷纷表示,所见即所得。

奇怪的是,就在主播回答提问的时候,背景视频却出现了农户站在快要没过膝盖的深水中采摘辣椒的场景,这样的场景显然不符合常理,而类似的画面在其他直播间也有出现。

当记者追问这些场景是不是AI生成时,主播并没有正面回应。

为了一探究竟,记者找到了相关技术专家了解情况。

奇安信集团副总裁刘浩告诉记者,画面中女士拿了辣椒以后后退,甚至她整个腿部下半身和辣椒融为一体,这明显是有悖真实世界规律的,这个在行业里面有专业名词叫“穿模”。数字世界内容的建模现在核心还是基于语言,而对于真实世界的物理规律,它是没有办法感知和预测的。

记者了解到,“穿模”是典型的AI生成视频中容易出现的漏洞。

技术专家指出,像直播间无人

机喷洒农药的片段,水雾的形态呈现规则的三角形,而不是自然的雾化状态,这都是技术上的漏洞。

实地求证,网售辣椒原产地并非樟树港

随后,记者来到湖南岳阳樟树港辣椒的产地,进一步求证。

湖南岳阳湘阴县樟树镇高级农艺师黄源介绍,樟树港辣椒植株很矮小,视频中的辣椒植株有一人多高,花根本就不是辣椒的花。另外,叶片也不是辣椒苗叶片的形状。这个视频的辣椒从产量上来看,每亩可能超过了6000斤,但是樟树港辣椒的产量大概每亩两千斤到三千斤。

法律专家指出,利用AI制作不符合现实或不存在的商品内容,甚至冒用品牌进行牟利,涉嫌民事侵权甚至刑事犯罪。

中国法学会消费者权益保护法研究会副秘书长陈音江表示,上述行为涉嫌侵犯消费者的知情权和选择权。《中华人民共和国消费者权益保护法》和《中华人民共和国电子商务法》都明确规定,经营者在推荐商品和服务信息的时候,要做到真实、准确、全面。如果经营者故意通过AI视频或者图片来欺骗消费者,让消费者误以为可以长出这样,但实际上长不出图片和视频里样子,这种行为还可能构成欺诈。

中国社会科学院法学研究所研究员支振锋认为,这里边还涉及对市场秩序的破坏,对于原产地的正牌樟树港辣椒来讲,构成了民事上的侵权。量比较大的话,有可能构成刑法上的犯罪。如果销售的是种

子,还可能违反《中华人民共和国种子法》的相应规定,情况可能会更严重。

利用AI技术仿冒知名产品,误导消费者

事实上,除了利用AI技术仿冒知名产品、驰名品牌带货,不法商家还利用AI技术仿冒名人非法牟利,一些专家学者、奥运冠军、影视明星等公众人物成为“被代言”的对象。

这不仅侵犯了当事人的人格权,还消解了这些公众人物的知名度和信誉度,更误导了消费者。

一段北京大学国家发展研究院李玲教授的采访视频,被不法人员利用AI技术篡改为一股虚假的推销视频,在网络上大肆传播。

为此,李玲教授公开发表声明称:网上出现了大量假冒本人推销医药书籍和治疗手段的虚假视频,大多是人工智能AI合成。本人从未在任何平台推销过医药书籍和医疗产品,请大家不要上当受骗。

然而,对于普通大众来讲,想要分辨清楚传播内容是否AI仿冒的并不容易,被蒙在鼓里,慕名而来购买这些产品的人也不在少数。

记者在销售评论区看到,有不少购买者对产品质量提出质疑;有的提出产品并非公众人物本人带货;有的甚至直呼上当受骗。

中国政法大学副教授朱巍谈道,现在看到的一些编辑的人脸,包括声音在内,按照《中华人民共和国民法典》规定,都属于当事人、权利人自己的人格权利,未经允许任何人不得侵害。不仅不能直接用,也不能使用当事人的人脸信息、声音

信息进行深度合成,这属于伪造信息,按照《中华人民共和国网络安全法》的规定,属于违法信息。

今年9月1日,国家网信办等四部门联合发布的《人工智能生成合成内容标识办法》正式施行,该办法明确所有AI生成的文字、图片、视频等内容都要“亮明身份”,需要添加标识和隐式标识。

其中明确,平台在服务提供者的内容上架或上线时要进行审核,核验生成合成内容标识,对未标识或疑似生成内容要添加风险提示,力求在传播端阻断虚假信息的扩散。

AI技术滥用破坏市场秩序,打假迫在眉睫

调查中记者发现,当前,各大网络平台普遍升级AI内容识别系统,要求对AI生成作品添加标注,但仍有一些人采用多种手段绕过审核。比如,通过数据篡改、转换编码等形式,处理后上传,平台就难以判定为AI生成内容。

事实上,AI技术滥用引发的问题复杂多变,法律法规的完善仅是底线要求。

截至目前,我国生成式人工智能产品的用户规模已达2.3亿人。随着AI技术的迅猛发展和生成式人工智能的快速迭代,各种纷杂的人工智能生成信息让人眼花缭乱,有时难辨真假,这也给监管部门和平台治理提出了新的挑战。

令人担忧的是,技术上的迭代升级也让这些仿冒内容的防范难度更大。

在过去,需要一定技术门槛和

成本投入的深度伪造,在AI大模型的助力下,不再需要长时间的深度学习和数据训练,就能在几分钟内生成仿冒的内容,逼真程度更是惊人。

在一家技术公司的办公室,技术人员现场给记者拍摄了一张照片,短短几分钟的时间,便通过AI大模型将这张照片生成一段直播带货视频。

同时,记者手里的矿泉水变成了红酒;身上穿的T恤衫变成了西服,还实现了纯正的英文带货推销。

揪出AI“李鬼”,将仿冒者打回原形,还需搭建多方协同的“立体防线”。平台应当扛起责任,进一步升级AI识别技术,用数字水印、区块链存证等手段增强鉴别追溯能力,避免AI仿冒虚假信息进入传播平台。

法律法规也需细化,进一步明确标识规范、回溯机制,追责机制。

而对于技术开发者和使用者的,更应该守住“科技向善”的底线,不把商业利益凌驾于社会责任之上。

AI仿冒带货不仅侵犯了被仿冒人士和品牌的权利,也存在欺诈嫌疑,更触动了数字社会赖以存续的信任根基。AI“李鬼”越来越像真的,作为消费者,我们自己当然要尽可能擦亮眼睛去甄别,对所谓“倾情奉献”的“明星代言”,保持理性判断,避免掉进消费陷阱,但是靠普通消费者的识别能力来防伪是远远不够的,更需要平台和相关监管部门担负起把关的责任,通过技术手段和治理能力的提升,用系统性力量,守好“真”的边界。唯有全社会形成共同抵制AI欺诈的合力,才能以“科技”之笔,绘就“向善”未来。

现代快报+ 新媒体品牌矩阵展播

江苏文脉
文质彬彬 含情脉脉

扫码关注江苏文脉