

Tecnología

# Deepfakes: un drama que revoluciona las redes y preocupa a los expertos

En la era de las aplicaciones y las redes sociales, nuevas tecnologías presentan nuevos desafíos desde el punto de vista de la ciberseguridad.

MARIANA MALEK  
Jueves, 25 Marzo 2021 04:00

Compartir esta noticia



Deepfakes. Foto: Shutterstock

En octubre de 2020, la estadounidense **Kim Kardashian** cumplió 40 años y su entonces marido, **Kanye West**, revivió a su padre para que le enviara un saludo. En febrero de 2021, unos supuestos videos del actor **Tom Cruise** haciendo tonterías aparecieron en las redes: se trataba del trabajo de un artista digital. Todos estos son ejemplos de lo que se conoce como **deepfake** o **ultrafalso**.

“La palabra *deepfake* alude a los sistemas informáticos que permiten, mediante técnicas de inteligencia artificial, desarrollar videos manipulados extremadamente realistas, aunque también es frecuente que se aplique a los videos así creados. El realismo es tal que puede ser imposible saber qué ha sido falseado, lo que puede emplearse, por ejemplo, para propagar **noticias falsas** y como **porno venganza**”, explica la organización Fundéu RAE en su web.

Este tipo de desarrollo existe hace varios años. Sin embargo, gracias al avance de dispositivos y nuevas aplicaciones, su uso es cada vez más masivo y más riesgoso para los usuarios.

Herramientas como **FaceApp** o **Reface**, que se popularizaron en el último año, crean pequeños *deepfakes* solo con la información que les proporciona una foto. Así, los usuarios se arriesgan sin notarlo.



El catedrático de Ciberseguridad de la Facultad de Ingeniería de la Universidad ORT y encargado de ciberseguridad de MAPFRE, **Roberto Ambrosoni**, explicó a El País que uno de los grandes problemas del presente es que el avance de la tecnología hará que accedamos cada vez más rápido y masivamente a nuevas tecnologías. “Las medidas de seguridad caerán en manos de los usuarios por la rapidez a la cual accedemos y el volumen”, remarcó.

Y agregó: “Estamos absolutamente desinformados, sabemos cómo se usa una aplicación pero ni siquiera miramos las medidas de seguridad”.

## Los deepfakes que conmocionan al 2021

**Chris Ume**, artista de efectos visuales belga, creó los videos de Tom Cruise que inundaron las redes sociales en el mes de febrero. Ume dijo al *New York Times* que para realizarlos requirió experiencia y tiempo. Para lograr un efecto tan realista, utilizó a Miles Fisher, un imitador del actor australiano y, por lo tanto, conoce los gestos y la voz de Cruise. Luego, con ayuda de la tecnología, cambió el rostro del imitador por el del verdadero **Tom Cruise**.

Durante dos meses, Ume usó machine learning para que el modelo de su computadora creara las expresiones faciales del actor de la saga *Misión Imposible*. Cada video de un minuto llevó 24 horas de producción.

Por su parte, el sitio de genealogía *MyHeritage*, lanzó una herramienta llamada **Deep Nostalgia**, que según el *New York Times* permitió que se subieran 26 millones de imágenes en los primeros días después de su lanzamiento. Sin embargo, la animación de esas imágenes puso sobre la mesa un nuevo concepto: el sitio planteaba que para trabajar sobre las imágenes se necesita tener consentimiento de las personas que aparecen retratadas. Pero también propone usar fotos de personas fallecidas por lo que el consentimiento se dificultaría en este caso.



## Ni buena ni mala.

La tecnología, en sí misma, no tiene bondad ni maldad; no obstante, sus usos pueden variar.

Por ejemplo, en 2016, cuando murió la actriz **Carrie Fischer**, quien interpretaba a la princesa Leia en la saga de **Star Wars**, fue sustituida por la colega noruega Ingvild Deila. Mediante programación se reemplazó su rostro por el de la fallecida. En ese caso, el *deepfake* se convirtió en una herramienta útil.

“Los *deepfakes* pueden ser creados con fines recreativos por personas comunes a través de una app en la que, por ejemplo, a partir de una foto podemos hacer un video de esa persona cantando. También encontramos grandes producciones como la que se hizo para hacer un discurso falso pero bastante creíble del expresidente **Barack Obama** con el fin de mostrar los peligros asociados a los *deepfakes*”, explicó a El País **Ignacio Lagomarsino**, docente de Maestría de Ciberseguridad y del programa de desarrollo profesional en seguridad de Universidad ORT.

Por su parte, **Hugo Köncke**, consultor en seguridad de la información de Datasec, advirtió que “no es necesario forzar demasiado la imaginación para darse cuenta de las implicaciones que el mal uso de esta forma de tecnología encierra en muchos órdenes de nuestras vidas. Sin ir mucho más lejos, su uso para la política sucia, para montar campañas difamatorias, puede llegar a ser devastador”.

## Conocer las herramientas al alcance de los usuarios

Para el experto en ciberseguridad Roberto Ambrosoni tienen que existir políticas para prevenir los riesgos de la red.

“Tenemos una oficina de delitos informáticos en Uruguay, que seguramente la mayoría no tiene idea de que existe. Todos los días somos atacados cibernéticamente”, indicó el especialista y docente de la Universidad ORT.

Y agregó: “Nos creemos que no pasa nada, pero al pagar las cuentas por internet ya hacemos un uso importante. Tener una cultura de seguridad cibernética no es solo necesario para las empresas, sino es clave para cualquiera que usa estas herramientas”.

## Medidas de prevención

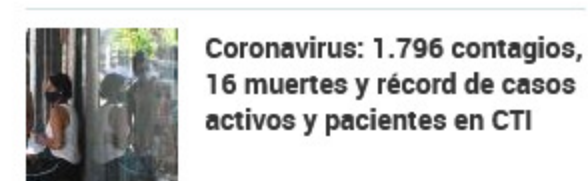
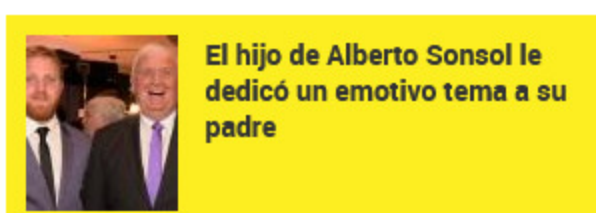
Los expertos coinciden en que a diario los usuarios de internet se enfrentan a engaños y estafas, por lo que la educación y el conocimiento son claves. Para Ambrosoni, por ahora, los usuarios tienen cierta ventaja porque para crear *deepfakes* realistas se necesitan ciertos conocimientos técnicos y equipamiento que hace que no sea rentable el esfuerzo.

Sin embargo, advirtió que hay otros como los *shallowfakes* –videos editados para que cuadren en determinadas situaciones– que también suponen una amenaza latente.

“¿Dudaremos de la veracidad de un video que nos llegue por WhatsApp de nuestros propios hijos pidiéndonos dinero o información? ¿No hablamos de la transacción financiera que nos pidió nuestro jefe en una videollamada? Da para pensarlo”, reflexionó Lagomarsino.

Köncke sumó: “Vivimos un momento de hiperconsumismo multimedia, con un desmedido uso de cualquier cosa digital vinculada a animaciones que se ponga a nuestro alcance, simplemente porque está ahí”.

## LAS MÁS VISTAS



## Nuestra Comunidad



**2,940**

Comentarios publicados en El País semanalmente

Comentar