Un arma de destrucción particular: los Deepfakes

Descripción

Los deepfakes son, cada vez más, muy sofisticados y difíciles de detectar. En los últimos años han proliferado aplicaciones para realizar videos falsos o clonar voces. Ahora es más fácil ponerse en la piel de Robert Downey Jr como Iron Man o hablar como el presidente Obama y declarar la guerra a los Asgardianos.

El mundo del cine vive un nuevo episodio creativo que le puede permitir revivir a Peter Cushing en Star Wars.

Incluso puede resultar divertido pasar un rato viendo parodias como la del Equipo-E, pero esta tecnología no está exenta de riesgos.

Durante los últimos meses, con el crecimiento del teletrabajo, ha aumentado el “voice phishing” o “vishing”, como se llama a los ataques que emplean la voz para la suplantación de identidad. A través de este método, los ciberdelincuentes consiguen obtener información sensible de sus víctimas.

La suplantación de la imagen está también provocando la proliferación de vídeos pornográficos con los rostros de artistas en escenas de sexo explícito, algo que puede resultar evidente y denunciable pero que, en el caso de desconocidos, puede derivar en extorsión o incluso en la destrucción de la vida personal y privada de sus víctimas.

Esta tecnología no está exenta de riesgos

Pero hay otras formas más sutiles de aprovechar la tecnología para delinquir. Es el caso que describe Jude Egan en su artículo sobre la manipulación de pruebas mediante deepfakes en el Tribunal de divorcios (ver aquí). Egan explica cómo una mujer, sin necesidad de disponer de una amplia experiencia en tecnología móvil, generó pruebas digitales falsas de mensajes de texto móvil en las que su ex-marido la acosaba y amenazaba y, de esta manera, logró el fallo a su favor para obtener la custodia de sus tres hijos menores de edad.

En este caso, la mujer sólo tuvo que cambiar el nombre de contacto en su agenda del teléfono entrante y escribir, con ese número, mensajes amenazantes para que el registro de su móvil viniera encabezado por el nombre, y no el número. Aunque parece evidente que es fácil contrastarlo, en esta ocasión, el juez no profundizó y falló, inicialmente, a favor de la mujer.

Sin embargo, otros casos resultaron de más elaboración, como el de una mujer que generó falsas imágenes pornográficas de su marido, dejándolas en su Ipad para que su hijo las encontrara y poder denunciar así al marido ante los Servicios de Bienestar Infantil.

Suplantar una identidad de un famoso puede resultar un acto de desprestigio o un intento de ridiculizarlo con un conocimiento y hasta una posible aprobación general del público, pero parece menos probable que tenga un calado mayor. Sin embargo, falsear la vida y acciones de personas desconocidas puede ser más peligroso, abriendo la veda a acosos, extorsiones, venganzas e incluso la exclusión de su colectivo social.

En la sociedad de 144 caracteres de profundidad donde vamos tan acelerados que no tenemos tiempo de profundizar en la verdad, cualquier prueba visual o auditiva que nos llegue, por falsa que sea, puede parecernos una confirmación de un hecho que jamás sucedió pero que puede cambiar la vida de otras personas.

La inteligencia artificial ha sido, incluso, capaz de generar vídeos enteros a partir de una sola fotografía, llagando a dar vida a la mismísima Gioconda de Leonardo de Vinci. La próxima vez, piense el lector qué podrían hacer con sus fotos de Facebook o Instagram antes de compartirlas con todo el mundo.