La Jornada

▲ Las firmas de ciberseguridad en todo el mundo se están enfocando en prevenir cualquier tipo de problema relacionado con la inteligencia artificial, pero se deben tener regulaciones por parte de los gobiernos para prevenir su utilización, considera un especialista. Imágenes de un congreso sobre IA en Santiago, Chile. Fotos Xinhua

PREOCUPA SU USO EN PROCESOS ELECTORALES

Con ayuda de IA, cualquiera puede falsificar identidades

Es prácticamente imposible reconocer la suplantación de una persona en videos editados y utilizados para estafas, advierten expertos

JULIO GUTIÉRREZ

Falsificar identidades por medio de la inteligencia artificial (IA) es menos complejo de lo que se piensa. Está al alcance de cualquier persona con un poco de iniciativa, comentan especialistas. Las últimas dos semanas han sido un ejemplo de un fenómeno que despierta creciente preocupación en entes reguladores, instancias de justicia y en grupos de expertos.

En los pasados 10 días, usuarios mexicanos de Internet han visto videos con la imagen y voz de Claudia Sheinbaum, precandidata de Morena a la Presidencia; de Victoria Rodríguez, gobernadora del Banco de México (BdeM), o del director general de la Bolsa Mexicana de Valores, José Oriol Bosch. En ellos, las imágenes y voces, que reproducen con alta similitud la de los personajes citados, invitan a invertir en plataformas tecnológicas que ofrecen altos rendimientos al destinar como mínimo 4 mil pesos. Tienen en común que todas son fraudes.

Para los ciberdelincuentes, pagar una suscripción en páginas especializadas en editar videos y hacer que parezca que una persona importante de la vida pública nacional invite a hacer inversiones en una plataforma y hacer estafas no es un gasto, es una inversión, y los bajos costos que se tienen hoy en día para acceder a todas las herramientas de inteligencia artificial que permiten falsificar una identidad pueden ser fondeados por cualquier consumidor de medios digitales, incluso para aquellos que nunca los han usado, afirman especialistas.

Los expertos en ciberseguridad consultados por este medio indican que identificar la suplantación de identidad de una persona es, para cualquiera, prácticamente imposible, y el trabajo que hacen las empresas del sector está enfocado actualmente en prevenir cualquier tipo de ataque o fraude que se realice con la IA.

Este tipo de estafas, que en el lenguaje coloquial son conocidas como *deepfake*, han escalado a tal grado que el Foro Económico Mundial (WEF, por sus siglas en inglés) las considera un riesgo. Particularmente, a esta institución le preocupa que puedan alterar las decisiones políticas este año, el cual captará la atención del mundo por las elecciones presidenciales.

Cerca de la mitad de la población vive en países que tendrán elecciones este año, algunas presidenciales, locales o legislativas. Entre las primeras, votarán por presidente en India (el país más poblado del mundo), Estados Unidos, México y Rusia.

En nuestro país, se hicieron virales este tipo de estafas desde el tercer trimestre de 2023, cuando fue suplantada la identidad de Petróleos Mexicanos (Pemex) y se invitó al público a hacer supuestas inversiones en la paraestatal desde 2 mil pesos con atractivos rendimientos.

El hecho llegó a tal grado que los cibercriminales difundieron en las redes sociales videos en los que aparecía la cara y la voz del presidente Andrés Manuel López Obrador, así como algunos conductores de noticieros en televisión abierta en los que se hacía la invitación para invertir en la empresa, algo que es completamente falso y que Pemex tuvo que salir a desmentir en sus medios oficiales.

No paró ahí, en semanas recientes se publicaron videos con la cara de la gobernadora del BdeM en los que supuestamente se ofrecen servicios como créditos e inversiones en una plataforma falsa del organismo.

"El Banco de México advierte al público en general de la difusión en redes sociales de un video falso, presuntamente generado por inteligencia artificial, que usa la imagen y falsea la voz de la gobernadora de este banco central, así como de otras personalidades de la vida pública de México. Este instituto central niega categóricamente la información que se difunde, e insta a la población a ignorar el mencionado video falso para evitar ser víctima de engaños que puedan llevar a operaciones fraudulentas."

Al alcance de todos

Claudia Sheinbaum, esta misma semana fue sujeto de fraude, pues en Internet se difundió un video en el cual se presume una entrevista donde se indica que una plataforma, que requiere de inversiones de 4 mil pesos, genera rendimientos de 43 mil pesos anuales.

"Los resultados de las primeras personas muestran que estamos en el camino correcto. En sólo tres meses aumentaremos los ingresos de la población al menos tres veces y todo esto se logra a través de nuestra riqueza nacional del petróleo", dice una voz falsa de Sheinbaum en el video, en el que incluso asegura que "hay que apurarse", pues la plataforma tiene "pocos lugares disponibles y se cerrará el acceso". Supuestamente, los recursos son invertidos en temas relacionados con el petróleo.

Esto provocó que la precandidata de Morena, en sus canales oficiales, difundiera un video en el cual indica que todo lo anterior es falso y fueron cibercriminales quienes falsificaron su voz e imagen. Si uno presta atención al video apócrifo, la voz no coincide con la imagen, pero suena completamente similar.

Miguel Hernández y López, director de ciberseguridad e ingeniería en Check Point México, firma especializada en estos temas, indicó que estas herramientas están al alcance de cualquier persona, incluso, sin ser expertos en temas de computación, es sencillo hacer un video falso.

En entrevista, comentó que todo comenzó cuando fue lanzada abiertamente la plataforma Chat GPT, en la cual se pide a una IA hacer textos, misma que incluso aprobó un examen de maestría en Estados Unidos. Después surgieron las páginas de Internet que ofrecen servicios de edición de video, y en un principio era una broma, pero hoy son utilizadas para realizar estafas.

"Realmente no requieres ser un experto en informática para encontrar dónde hacer el video y la voz, son herramientas enfocadas en los usuarios, si se agrega el conocimiento de quienes saben (*hackers*) se puede obtener de un video (auténtico) el audio y la imagen y hacer el video falso, es la IA la que saca las facciones y la voz y te entrega la imagen de un video de una persona para fines de suplantación.

"Cualquier persona puede hacer el fraude, entras a redes sociales y está la publicidad de este tipo de aplicaciones, lo que hacen las compañías es eso, que el usuario lo descargue, hay pruebas gratis de una semana para hacer los videos, quitar la marca de agua o el nombre de la compañía, pero son precios bajos que cualquier persona puede hacerlo hoy en día", mencionó el experto.

El WEF publicó su reporte de riesgos 2024, en el cual especifica que los temas relacionados con la inteligencia artificial y los *deepfakes* son "una preocupación particular en aquellos países que se enfrentan a próximas elecciones, donde se podría dar una ofensiva contra la interferencia extranjera real o percibida para consolidar el control existente, particularmente en democracias defectuosas o regímenes híbridos".

Destaca que en enero del año pasado, X (antes Twitter) y YouTube acordaron eliminar enlaces a un documental de la BBC en India relacionado con estos temas; sin embargo, precisa, "en México, la sociedad civil ha estado preocupada por el enfoque del gobierno hacia las noticias falsas y sus implicaciones para la libertad y seguridad de la prensa.

"Las interfaces fáciles de usar para modelos de inteligencia artificial a gran escala, que ya no requieren un conjunto de habilidades específicas, ya han permitido una explosión de información falsificada y contenido llamado sintético, desde sofisticadas clonaciones de voz hasta sitios web falsificados", dice el WEF.

Difícil de detectar

Hernández y López comentó que las empresas especializadas en temas de ciberseguridad hoy día analizan y se encargan de detectar cualquier tipo de ataque, amenaza o fraude que pueda ser realizado por medio de la IA, y si bien no es imposible hacerlo, es complicado a la vista del ojo humano.

"Hay formas de detectarlos, claro que sí, a simple vista se ve cuando la imagen está montada, aunque debe verse a detalle. Existen sistemas que detectan si hay alguna anomalía en la voz o la imagen, sí las hay, aunque como usuario normal es una herramienta que cuesta, un celular no lo detecta de forma inmediata, es difícil por ese medio, difícil, pero no imposible."

Precisó que "las compañías de ciberseguridad en todo el mundo se están enfocando en prevenir cualquier problema relacionado con la inteligencia artificial, pero se deben tener regulaciones por parte de los gobiernos para prevenir y su uso".