LA VOZ SINTÉTICA EN UN MUNDO DE MENTIRAS

NOTI 347 – Marzo de 2024

Conceptos

- **Deep Fake:** Pueden ser archivos de video, imagen o voz que son manipulados y generados mediante el uso de Inteligencia Artificial, con el fin de que parezcan reales. Su intención de uso puede variar desde fines de entretenimiento hasta ser utilizados para generar confusión y engaños.

- **Fake News:** Contenido difundido a través de portales de noticias, prensa, radio, televisión, redes sociales y cualquier medio de difusión, que tiene por objetivo desinformar a un público en específico.

Imagen tomada de: https://icloudseven.com/como-implementar-la-inteligencia-artificial-en-una-empresa-en-8-pasos/

La IA, o Inteligencia Artificial, es el tema del momento que mueve a la economía mundial y que acapara todos los titulares de la prensa. Sólo debemos dar un vistazo rápido a los periódicos y redes sociales para entender los alcances de esta tecnología en nuestra realidad. Vemos como NVIDIA, una compañía que se dedica a producir chips gráficos de computador, gracias a la IA se convirtió, en poco más de un año, en una de las empresas más valiosas del mundo; notamos con preocupación la realidad de los despidos masivos en E.E.U.U., por cuenta de las automatizaciones que se derivan del uso de esta tecnología; y ni qué decir de los riesgos asociados de las fake news, cuya creación y divulgación se facilita con la IA.

Para el ciudadano común, la IA puede representar riesgos que ya hemos venido identificando en ediciones pasadas de nuestro Boletín mensual. Uno de estos riesgos tiene que ver con el uso del Deep Fake de voz, donde criminales podrían utilizar nuestra voz para cometer fraudes bancarios, engañar a nuestros parientes; e incluso, engañar a nuestros compañeros de trabajo, todo con el fin de realizar actos fraudulentos con nuestra identidad y/o autoridad.

La IA se combate con IA pero cada uno debe procurar conservar los niveles de seguridad apropiados, de acuerdo a su nivel de riesgo, para disminuir la posibilidad de ser suplantado y convertirse en víctima.

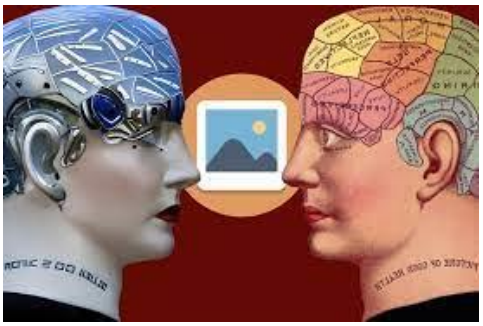

Imagen tomada de:
https://www.genbeta.com/actualidad/emular-sentido-comun-inteligencia-artificial-a-hora-generar-imagenes-video-eso-que-promete-meta-i-jepa

Por: Santiago Duque
ASR S.A.S.

Medellín, Colombia
+573103923352 - 3233453366
asr@asr.com.co
http://www.asr.com.co/

Estos riesgos presentan, entonces, retos de cómo enfrentarlos y cómo protegernos ante estas eventualidades. La respuesta, probablemente, la encontremos también en el mundo tecnológico, donde la IA se debe combatir con otra IA que la contrarreste. Otro método que siempre estará con nosotros debe ser el sentido común o la, coloquialmente, llamada "malicia indígena"; donde la desconfianza prime sobre la urgencia que se nos presenta cuando los delincuentes desean utilizarnos para su propio beneficio.

Es por este motivo que las empresas más expuestas frente al riesgo de fraude por voz, como lo son los Call Centers y las Instituciones Financieras, deben acudir a técnicas y soluciones tecnológicas que les ayuden a identificar el posible uso de voces sintéticas de parte de clientes ficticios; y de esta manera analizar el espectro de las señales que genera una llamada telefónica en tiempo real. Estas nuevas tecnologías buscarán características en el sonido ambiente de la llamada, en el tono y cadencia de la voz, con el fin de determinar patrones asociados a una voz natural frente a una artificialmente generada.

La buena noticia, por el momento, es que para poder clonar la voz de una persona y efectivamente utilizarla en tiempo real, se requiere de una alta sofisticación tecnológica que no se encuentra aún al alcance de cualquier persona. Llegar a tal grado de perfección requiere entrenar modelos de IA con data confiable, algo que resulta difícil y dispendioso de conseguir.

Si bien aún estamos un poco lejos de que clonen nuestra voz para fines fraudulentos, sí debemos estar a la vanguardia de estas nuevas técnicas de fraude que se van asentando en nuestra vida diaria gracias a los avances monumentales de la tecnología. Conocer los riesgos a los que nos enfrentamos en el futuro, nos permitirá prepararnos en el presente para protegernos cuando lleguen.

asr@asr.com.co