



Las redes sociales en pro de la inteligencia artificial

Social networks for artificial intelligence

Por María de Lourdes López García y Luis Ángel Rivera Núñez

Resumen: El uso de las redes sociales incrementa la cantidad de información almacenada en la nube y al mismo tiempo existen técnicas como el *deepfake*, que se alimenta de gran cantidad de datos para generar bases o directorios susceptibles de ser falsificados. Este artículo es una reflexión para generar conciencia sobre qué datos, imágenes, contactos, preferencias y otros indicadores son compartidos en las redes sociales.

Palabras clave: redes sociales, *deepfake*, seguridad de la información.

Abstract: Using of social networks increases the amount of information stored in the cloud and at the same time there are techniques such as *deepfake*, which feeds on a large amount of data to generate databases or directories that can be counterfeited. This article is a reflection to raise awareness about what data, images, contacts, preferences, and other indicators are shared on social networks.

Keywords: social networks, *deepfake*, information security.

Recibido: 09/09/21 • Aprobado: 26/11/21

La **facilidad** con la que un individuo adquiere un dispositivo móvil ha propiciado que el uso de aplicaciones de internet se incremente, así como de los servicios en la nube. Los usuarios optan por las redes sociales como su principal herramienta de comunicación y de información. Entre las aplicaciones más utilizadas se encuentran las de compras, pagos, transferencias bancarias y entretenimiento.

El uso de estas aplicaciones ayuda a perfilar los gustos e intereses de cada persona gracias a técnicas de inteligencia artificial, pues las redes neuronales clasifican la información y desarrollan un perfil basado en el comportamiento del usuario para sugerirle mercancías, páginas web u otro tipo de información específica

que sea de su interés. Ejemplo de ello es cuando recibimos promociones de viajes, ropa o cualquier otro tema que haya sido objeto de nuestra búsqueda en la web.

Estos mecanismos brindan al usuario final la posibilidad de tener al alcance toda clase de servicios y contenidos de manera inmediata las 24 horas del día los 365 días del año. Con el paso del tiempo, la información acumulada a través del comportamiento más lo que se sube a las redes sociales, como fotografías, videos, documentos, etc., abre la posibilidad de que gente malintencionada la utilice en su perjuicio.

Durante los últimos años se ha debatido la forma de operar esta información digital, debido a que

las empresas que se encargan de administrar y proveer los servicios digitales solicitan permiso para utilizar los datos privados; sin embargo, en la mayoría de las ocasiones el consentimiento para instalar determinada aplicación implica el uso de los datos personales para efectos de mercadotecnia. Así se generan grandes bancos de información que son abastecidos, primordialmente, por las redes sociales.

El avance tecnológico también ha facilitado la generación de técnicas aún más especializadas en la rama del entretenimiento como la del *deepfake*, acrónimo del inglés formado por las palabras *fake* (falsificación) y *deep learning* (aprendizaje profundo), la cual tiene como objetivo utilizar



Ilustración: Gustavo Contreras

múltiples capas de algoritmos de aprendizaje automático para extraer progresivamente características de nivel superior de una entrada sin procesar. Lo poderoso de esta técnica es que se han realizado películas y comerciales con personajes rejuvenecidos y, en el caso extremo, de gente fallecida. El resultado es la creación de un personaje ficticio con cara, cuerpo y voz generados con imágenes de gesticulaciones, posturas y discursos del original, esto hace que el público se sorprenda y emocione con los alcances de la tecnología. No obstante, es una herramienta que puede ocasionar graves daños en lo personal y lo social, sobre todo si se utiliza para crear personajes importantes y con gran influencia en la población con mensajes de odio o de pánico.

La manera de combatir estas acciones malintencionadas y de disfrutar las bondades de la tecnología es mantener un margen de confianza en la información difundida a través de una

red social, de tal manera que un individuo esté consciente de la responsabilidad de leer una noticia, darla por cierta y transmitirla sin haber verificado su origen. La incorporación de la *deepfake* demuestra que no todo lo que se observa es cierto y, aunque en la rama del entretenimiento se sabe que el personaje es ficticio, es muy útil tomarse el tiempo para clasificar el resto de la información que circula en internet y que deseamos seguir compartiendo.

En conclusión, para sentirnos seguros en la web debemos aprender a utilizar las herramientas de comunicación más actuales y poner en la balanza el impacto de compartir información privada, por eso es necesario clasificar los mensajes recibidos y, ante todo, verificar y consultar fuentes fidedignas que permitan una convivencia sana en la gran comunidad que está inmersa en las redes sociales. 



María de Lourdes López García es doctora en Ciencias de la Computación, profesora de tiempo completo en el Centro Universitario UAEM Valle de Chalco, sus áreas de investigación son criptografía, seguridad de la información y visión artificial.

Luis Ángel Rivera Núñez es licenciado en Informática Administrativa. Actualmente es estudiante de la Maestría en Ciencias de la Computación en el Centro Universitario UAEM Valle de Chalco. Su proyecto de investigación es sobre la seguridad de la información almacenada en la nube.