

Fraude de identidad y deepfakes: suenan las alarmas

21/12/2023



El ámbito del fraude de identidad tuvo recientemente un giro dramático al incorporarse los deepfakes a las herramientas utilizadas para vulnerar la identidad de usuarios en todo el mundo. Este término proviene del acrónimo inglés formado por las palabras fake (falsificación) y deep learning (aprendizaje profundo). Asistido muchas veces por la inteligencia artificial, se trata de una falsificación que es prácticamente indistinguible a simple vista.

El Informe de Fraude de Identidad 2023 de la empresa Sumsu confirma este nuevo peligro y señala que los deepfakes a nivel global tuvieron un aumento exponencial (más de 10 veces) de 2022 a 2023.

El panorama que pinta Sumsu es preocupante, ya que el reporte brinda detalles de un aumento sorprendente de incidentes con deepfakes en varias regiones del mundo. En América del Norte y Centroamérica, por ejemplo, se observa un aumento del 1740%, en el Asia-Pacífico del 1530%; en Europa (incluido el Reino

Unido) del 780%; en Oriente Medio y África del 450%; y en América Latina, la última región, del 410%.

¿Qué se puede falsificar con esta nueva tecnología? Aunque el informe señala que el pasaporte de los Emiratos Árabes Unidos fue el documento más falsificado a nivel global, la expansión del uso de deepfakes en distintos ámbitos de la sociedad es un problema que requiere atención inmediata. Las tarjetas de identificación siguen siendo un objetivo principal, como lo demuestra que constituyan casi el 75% de todas las actividades fraudulentas registradas por Sumsb que tienen que ver con documentación personal.

Ante este problema, la IA parece ser, como en otros casos que analizamos, un arma de doble filo. Su influencia en este problema es evidente. Por ejemplo, los incidentes de deepfakes que involucran IA y criptomonedas constituyeron el 88% de los casos detectados, seguidas muy de lejos por las fintech (8%). En cuanto a las industrias donde estos eventos tuvieron lugar, el informe señala que los medios online han experimentado un sorprendente aumento del 274% en las tasas de fraude de identidad entre 2022 y 2023. Es que sus audiencias multitudinarias, junto con la falta de regulación, son terreno fértil para actividades fraudulentas, como la proliferación de cuentas falsas y campañas de desinformación. Lo paradójico es que muchos de estos casos que involucraron el uso de inteligencia artificial fueron resueltos también gracias a ella, lo cual refleja acertadamente su doble naturaleza de recurso poderoso tanto para impedir un fraude, como para cometerlo.

Para Sumsb, el problema que se viene tiene que ver con la regulación. A medida que nos acercamos al próximo año, se hace cada vez más evidente la necesidad de regulaciones estrictas sobre inteligencia artificial. El informe destaca los esfuerzos pioneros de China en la regulación de deepfakes, lo que ofrece un posible modelo para otros países y territorios, como la UE, el Reino Unido o los Estados Unidos. Reconocer la

seguridad de la IA como parte integral de las actividades operativas se vuelve imperativo para las empresas que navegan este paisaje de amenazas en constante evolución.

Mirando hacia adelante, el informe de Sumsb prevé un aumento de esquemas de "toma de control" de cuentas y «money muling» (lavado de dinero), lo que hará necesaria una serie de contramedidas sólidas vinculadas especialmente a la regulación. Pero un enfoque puesto en métodos de verificación no documental y la adopción de enfoques alternativos de validación de identidad parece ser, actualmente, la herramienta más a mano para remodelar la dinámica de las interacciones en línea y los posibles fraudes por deepfake.