GESTIÓN

El área gris de las denuncias contra el deepfake que también afecta a empresas en Perú

Pese a los desafíos legales por el avance de la Inteligencia Artificial, los expertos instan a las personas a usar los derechos ARCO para proteger y controlar el uso de su información personal ante empresas e instituciones. Aquí los detalles.

Ani Lu Torres

09/07/2025 05H02 - ACTUALIZADO A 09/07/2025 06H25

En un reciente taller de inteligencia artificial para periodistas, varias plataformas de IA generativa llamaron la atención. Herramientas como Lumen5 o Runway permiten doblar videos a otros idiomas o incluso alterar su mensaje 'con naturalidad'. Pero lo que parece un avance importante en la creación de contenido también alerta sobre la facilidad con que hoy, más que nunca, pueden generarse deepfakes - videos e imágenes falsas- sin que el ojo humano los detecte.

Eric Biagioli, director de Ciencia de Datos y Ciencia de la Computación de **UTEC**, afirma que posiblemente "*en un año o dos, generar deepfakes ya no requiera de tanto esfuerzo técnico como todavía se necesita*".

De hecho, es posible que las pocas plataformas que se han lanzado para detectar los deepfakes -como Originality.ai- estén generando el efecto contrario: perfeccionar las nuevas versiones de los **videos e imágenes falsos**. "*Estamos llegando a un punto en que lo que analiza la red neuronal de la IA ya no son visibles al ojo humano, sino, correlaciones o características geométricas del rostro*", explica.

Deloitte ha estimado que las pérdidas económicas relacionadas a la expansión del *deepfake* en el mundo aumentarán de US$ 12,000 millones en 2023 a más de US$ 40,000 millones para el 2027. Por supuesto, varios informes alertan que los **estafadores** están concentrando su esfuerzo de falsificación en directores ejecutivos y en empresas.

En el mundo ya se han reportado **videos manipulados** en los que un supuesto Elon Musk promociona inversiones en criptomonedas (hay víctimas que aún esperan justicia). En Perú, en mayo, el **BCP** tuvo que aclarar mediante un comunicado que un video donde aparecía su CEO, **Gianfranco Ferrari**, recomendando un negocio era completamente falso y había sido creado con inteligencia artificial.

LAS ÁREAS GRISES

En 2024, Kaspersky advirtió que el 75% de peruanos no sabía qué es un *deepfake* y que un 57% no podría identificar este tipo de videos, lo que refleja una alta vulnerabilidad frente a posibles **estafas en línea**. Aunque ya se han reportado varios casos y víctimas en el país, **aún no existe jurisprudencia ni sentencias contra los ciberdelincuentes en este campo.**

Y no es que falten herramientas legales para sancionar estos delitos, tanto en el ámbito administrativo como penal (existen leyes como la **32314** o la **29733**, entre otros) . El problema es que, en la práctica -dicen los expertos-, persisten áreas grises que dificultan la detención de los responsables, especialmente cuando resulta casi imposible identificar al autor.

"*Por ejemplo, para poner una denuncia ante la **Autoridad Nacional de Datos Personales** (la imagen o video es un dato personal), hay que identificar al autor o responsable del deepfake: puede ser al creador del software o quien haya elaborado el video. Pero muchas veces identificarlos es complejo debido al uso de la IA*", explica Julia Loret de Mola, socia de Competencia de Payet, Rey, Cauvi, Pérez Abogados.

Erick Palao, asociado principal de Derecho Penal del mismo estudio de abogados, aclara que no tiene conocimiento si las empresas o ejecutivos peruanos víctimas del *deepfake* han realizado las denuncias ante las instancias correspondientes, pero señala que -como en otros casos- las personas lo piensan dos veces si deben hacer o no la denuncia: "*Muchos desisten de hacerlo por lo engorroso del trámite penal*".

En diálogo con G de Gestión, Bruno Mejía, líder de Competencia y Mercados de **EY Law** señala que, dependiendo del caso, se puede identificar hasta **tres tipos de culpables**: el que crea el contenido; la plataforma que aloja el contenido (que debería tener políticas para que ciertos videos o imágenes no sean alojados en su plataforma), y quien difunde el contenido (vuelve a ser complejo considerando que más del 50% de usuarios en redes sociales usa un nombre falso).

Y hay otro punto adicional: muchos de estos **delitos cibernéticos** son transfronterizos. Es decir, pueden suplantar la imagen de un gerente peruano y divulgar un video falso en territorio nacional, pero el IP está en Tanzania, por poner un ejemplo; o la cuenta por donde recauda el dinero de las víctimas es de otro país.

"*Creo que todavía no tenemos peritos capacitados para llegar al trasfondo del delito. Se pueden iniciar las investigaciones, a veces hasta tienes la trazabilidad de las cuentas, pero cuando los IP están en otro país, se vuelve complicado*", añade el abogado Erick Palao.

¿JUZGADO ESPECIALIZADO EN DELITOS CON IA?

Si bien en Perú ya existen **fiscalías especializadas en ciberdelincuencia**, inicialmente en Lima y aún en proceso de descentralización, todavía existe la necesidad de entrenar a los fiscales en estas nuevas modalidades de delito, menciona Palao.

Actualmente, si se presentan casos de difamación o estafa usando **IA generativa**, estos se derivan a fiscalías y juzgados comunes, pues no existen juzgados específicos para este tipo de delitos. "*Sin embargo, ante el reciente aumento de estos casos, creería que debería evaluarse si se requiere la creación de fiscalías y jueces especializados en delitos vinculados al uso de **inteligencia artificial***", agrega.

Los expertos para este artículo han explicado que, ante un hecho de ***deepfake***, la **vía formal** más cercana para realizar la denuncia es ante la Policía Nacional del Perú o una Fiscalía especializada. Y en el caso de la vía administrativa (por uso de imagen, etc): a la Autoridad Nacional de Protección de Datos, y al Indecopi (por temas de derecho de autor). Y, no menos importante, hoy más que nunca las personas pueden invocar sus **derechos ARCO** (Ley N° 29733): el cual permite a los ciudadanos tener control sobre su información personal y cómo es utilizada por empresas o instituciones.

Las sanciones administrativas para quienes incurran en la infracción del deepfake pueden alcanzar las 100 UIT gracias a las nuevas leyes y reglamentos. **La sanción penal**, cuando involucra una difamación, puede llegar a los tres años de pena privativa de la libertad; si es una estafa, la condena podría ser de hasta ocho años de cárcel.

Los especialistas también señalan que, en algún momento, los videos y **contenido generado con IA** deberían llevar una etiqueta que informe a los usuarios y consumidores sobre cómo ha sido generado el material audiovisual.

RECOMENDACIONES CLAVE ANTE EL *DEEPFAKE*

Carmen Gardier, South Latam Marketing Solutions Senior Director en **LLYC**, comparte **algunas recomendaciones** a los empresarios y ejecutivos para prevenir y reducir la posibilidad de ser víctimas del ***deepfake***.

- Monitoreo activo: Utilizar herramientas de monitoreo digital para detectar rápidamente usos indebidos de su imagen o voz, y actuar de inmediato con comunicados oficiales.
- Verificar y Desmentir Información Falsa Rápidamente. Para eso es importante contar con una presencia digital fuerte que sustente cualquier tipo de respuesta desmintiendo la información.
- Invertir en Tecnologías de Prevención. Uso de IA para la detección de deepfakes.

- Registro de imagen y voz: Es recomendable que los empresarios o influenciadores registren su voz, imagen o representaciones públicas, con la finalidad de contar con pruebas legales en caso de que se utilicen de manera no autorizada.

Gardier también comparte un método para detectar o identificar si un video o imagen fue manipulado o no:

- Revisar la fuente: Confirmar si el contenido viene de una fuente confiable y reconocida. Si la fuente es desconocida o poco clara, hay que ser más cauteloso.
- Analizar el audio: Identificar desincronización entre el audio y los movimientos de la boca, o tonos de voz que suenen artificiales.
- Observar detalles extraños: Identificar señales visuales o textuales poco naturales, como errores en imágenes, frases repetitivas o inconsistencias en el estilo.
- Contrastar la información: Verificar si el contenido está presente en otros medios confiables y si coincide con hechos conocidos.