TÉCNICAS DE ANONIMIZACIÓN

A raíz de un problema con una imagen publicada en un artículo científico de un miembro de la AEP, esta Asociación ha comprobado que se producen errores o fallos a la hora de aplicar técnicas de anonimización de datos personales.

Debemos recordar que en trabajos académicos aplicar máscaras o filtros de privacidad en imágenes no es opcional, sino que es una obligación legal que pesa tanto sobre el autor/a del trabajo, como sobre la entidad que edita o publica el trabajo.

Resumidamente, esta obligación se deriva del Reglamento General de Protección de Datos (RGPD), de la Ley Orgánica de Protección de Datos (LOPDGDD), de la Ley Orgánica 1/1982, de protección a la propia imagen, intimidad, etc.

De todas esas normas se extrae que el autor/editor debe garantizar la confidencialidad de la información que publica y aplicar las medidas técnicas necesarias sobre la imagen que eviten la identificación directa o indirecta de la persona física que aparezca en esa imagen. Estas son las denominadas técnicas de anonimización o seudonimización que derivan del Principio de Minimización de Datos.

Además, al tratarse habitualmente de imágenes o documentos relacionados con la práctica de una especialidad médica correspondientes, estaríamos hablando de datos de salud lo que eleva el riesgo. Y si añadimos que la imagen o documento se refiere a un menor, se convierte en un riesgo inasumible, por las consecuencias de una mala práxis.

Específicamente desde el punto de vista científico, el autor tiene, por Ley, el Deber de Secreto y Confidencialidad que es especialmente intenso cuando se publican datos de investigación que afectan a personas identificadas o identificables, aunque sea en entornos educativos o científicos. Aunque se tenga el consentimiento de la persona afectada para publicar determinadas imágenes, este consentimiento se suele referir a finalidades científicas, pero no a un uso comercial, de promoción personal del médico o para su publicación en redes sociales. Hay que tener en cuenta que una vez aparece la publicación en redes sociales, el autor y el editor suelen perder el control de la publicación, de las imágenes o de los documentos contenidos en el mismo, de su repercusión o de las veces que se comparta, etc., incluso del uso que los motores de búsqueda o herramientas de inteligencia artificial pueden hacer de la misma.

Por todo ello, la no aplicación de estas técnicas de anonimización puede, no solo dar lugar a sanciones legales, sino también pueden derivar en daños indemnizables a las personas implicadas.

En definitiva, si una persona puede ser identificada en una imagen y no es imprescindible para ese trabajo conocerla o identificarla, es obligatorio anonimizar la imagen.

Para evitar esos riesgos, hemos elaborado las siguientes recomendaciones que pueden ayudar a realizar esos trabajos con un menor riesgo:

Aplicar **filtros de privacidad en imágenes** o documentos consiste en ocultar o eliminar información sensible (caras, documentos, etc.) antes de publicarlas o compartirlas. Esto se denomina anonimizar o pseudonanimizar.

Existen diversas formas de aplicarlas, en función del tipo de datos o la protección que sea necesaria. La aplicación concreta de una máscara o filtro de privacidad se debe utilizar, preferiblemente, **ANTES de incorporar la imagen o documento al trabajo/artículo/etc**., dado que, si no se hace de esta manera, se podrían utilizar técnicas que permitan la reversión de la anonimización.

Entre ellas, podemos destacar:

1. Pixelado.

Consiste en convertir zonas de una imagen en bloques grandes. Se suele utilizar para anonimizar imágenes o datos visibles.

Es un método difícil de revertir si se realizar adecuadamente.

* Ejemplo de herramientas gratuitas: Facepixelizer, Paint de Windows o GIMP.

2. Desenfocado (blur)

Es una técnica que realizar un desenfoque de la imagen. Aunque afecta menos a la imagen, es menos seguro que pixelar si el desenfoque no es fuerte.

* Ejemplos de herramientas gratuitas: GIMP, Photopea o CANVA o Google Photos.

3. Tapado o censura.

Consiste en cubrir con rectángulos negros o de color partes de la imagen o de los documentos, siendo una de las técnicas más seguras si se hace correctamente.

* Ejemplos de herramientas: Acrobat pdf, ilovepdf.GIMP, Photopea, Paint.

4. Recortado.

Lleva a cabo una eliminación directa de la parte sensible. Al impedir la recuperación, es la técnica más segura cuando se puede aplicar.

* Cualquier herramienta de edición permite llevarlo a cabo.

5. Eliminación de metadatos

Como las imágenes y los documentos contienen información oculta (ubicación GPS, fecha, dispositivo) se deben comprobar tanto los metadatos (EXIF), como la posible información de autor, ubicación, etc., que puede aparecer en las propiedades de los documentos.

** Herramientas: Windows (propiedades → quitar información personal) ó GIMP (gratuita) o Photoshop → exportar sin metadatos ó Exiftool.*

Desde un punto de vista práctico, antes de publicar una imagen de una persona en un artículo o trabajo, se debe contestar a la pregunta: *"¿Alguien podría identificar a una persona o acceder a información sensible con esta imagen?"*

- ✓ *Si la respuesta es afirmativa, se debe aplicar un filtro de privacidad.*
- ❖ *Si es negativa, la imagen sería publicable.*

AMENAZA	CHECK LIST	ACCIÓN A REALIZAR
Imágenes de rostros identificables	☐ ¿Se ve la cara claramente? ☐ ¿Se puede reconocer por rasgos, ropa o contexto? ☐ ¿Hay menores de edad?	Pixelar, Desenfocar o Censurar
Datos Personales visibles	☐ DNI, pasaporte o tarjetas ☐ Nombres y apellidos ☐ Correos electrónicos ☐ Números de teléfono ☐ Firmas	Censurar
Documentos o pantallas	☐ Informes médicos, académicos o laborales ☐ Pantallas de ordenador/móvil ☐ Formularios, bases de datos	Recortar o Cubrir completamente
Información identificativa indirecta	☐ Matrículas de vehículos ☐ Uniformes, logotipos, credenciales ☐ Ubicación del trabajo o centro educativo	Pixelar o Eliminar zonas de la imagen.
Ubicaciones	☐ Direcciones, calles, portales ☐ Lugares fácilmente reconocibles ☐ Coordenadas o mapas en pantalla	Ocultar detalles o Recortar imagen
Datos sensibles	☐ Datos especialmente protegidos (hospitales, domicilios) ☐ Información que pueda causar daño reputacional ☐ Imágenes en contextos confidenciales	NO PUBLICAR
Metadatos de la imagen	☐ GPS (ubicación exacta) ☐ Fecha y hora ☐ Dispositivo o autor	Eliminar metadatos antes de compartir
Consentimiento	☐ ¿Tengo permiso de las personas que aparecen? ☐ ¿Saben para qué se usará la imagen?	Obtener consentimiento explícito para las finalidades necesarias.
Uso y finalidad	☐ La imagen es necesaria o se puede sustituir? ☐ ¿Cumple con la normativa aplicable?	minimizar datos (usar solo lo necesario)
En investigación / académico	☐ ¿Los participantes están anonimizados? ☐ ¿Se han eliminado identificadores directos e indirectos?	anonimización completa