FERNANDEZADVOCATS

DIFUSIÓN DE IMÁGENES ÍNTIMAS Y DEEPFAKES SEXUALES

La difusión no consentida de imágenes íntimas es una de las formas más graves de violencia digital. El daño no depende únicamente de que el archivo llegue a miles de personas: un solo reenvío puede quebrar la confianza de quien compartió un contenido en un contexto privado y provocar una afectación intensa de su intimidad.

La expansión de herramientas de inteligencia artificial ha añadido un problema nuevo: los deepfakes sexuales, es decir, imágenes o vídeos manipulados o generados para mostrar a una persona en una situación sexual que no existió. Aunque el Derecho penal español ofrece respuestas relevantes, no todos los supuestos tienen el mismo encaje jurídico[1].

1. El artículo 197.7 del CP: La difusión íntima no consentida

El art. 197.7 del CP sanciona, en lo más esencial, la difusión, revelación o cesión a terceros de imágenes o grabaciones audiovisuales de otra persona que se hubieran obtenido con su anuencia (consentimiento) en un domicilio o en otro lugar fuera del alcance de la mirada de terceros, cuando se divulgan sin autorización y se produce un grave menoscabo de su intimidad.

Ese precepto se dirige a una realidad muy reconocible: una persona puede consentir hacerse una fotografía íntima, grabarse o compartir ese contenido con alguien de confianza, pero ese consentimiento no autoriza por sí mismo a difundirlo.

La STS 70/2020, de 24 de febrero, destaca que el núcleo de esta modalidad está en la difusión incontenida, no en la obtención de la imagen. También confirma que la obtención puede producirse porque la propia persona afectada remita voluntariamente el contenido a quien después lo divulga.

1.1 Elementos que conviene distinguir

[1] Este artículo ofrece información general sobre el Derecho Penal español. La calificación concreta depende de cómo se obtuvo el contenido, cómo se alteró, a quién se difundió y qué prueba existía.

Para valorar la posible aplicación del art. 197.7 CP, no basta con constatar que se ha compartido una imagen. Habitualmente, deben analizarse estos elementos:

1) Contenido de las imágenes afectadas: el tipo no se limita, literalmente a imágenes sexuales; lo decisivo es que la difusión afecte gravemente a la intimidad personal.
2) Obtención con anuencia: puede existir consentimiento para la captura o para la remisión privada del archivo.
3) Ámbito reservado: la norma contempla imágenes obtenidas en un domicilio o lugar fuera de la mirada de terceros.
4) Falta de autorización para difundir: consentir la toma o el envío privado no equivale a consentir una publicación o un reenvío.
5) Grave menoscabo de la intimidad: la gravedad se valora según el contenido, el contexto, los destinatarios, el modo de difusión y el impacto en la esfera personal.

Por eso, no debe afirmarse que toda publicación incontenida en internet sea automáticamente delito ni que solo sea relevante la difusión masiva. La valoración tiene que ser necesariamente individualizada.

2. Un reenvío puede ser suficiente

No se exige que el contenido se haga viral. La jurisprudencia ha señalado que la difusión a una sola persona puede bastar para integrar la conducta, porque el menoscabo de la intimidad puede producirse desde el primer quebrantamiento de la reserva.

Además, la reforma introducida por la LO 10/2022 amplió expresamente la respuesta penal frente a la redifusión por terceros receptores. La STS 767/2023, de 3 de octubre, resulta especialmente relevante para explicar este cambio: hoy debe distinguirse entre quien recibió la imagen directamente de la persona afectada y quien, habiéndola recibido, decide reenviarla sin autorización.

La ley prevé agravación, entre otros supuestos, cuando el autor es o ha sido cónyuge o persona ligada por una relación afectiva análoga, cuando la víctima es menor de edad o persona con discapacidad necesitada de especial protección, o cuando existe finalidad lucrativa.

3. Consentir una videollamada no es consentir una grabación

Las comunicaciones digitales obligan a separar actos que con frecuencia se confunden. Aceptar una videollamada de contenido sexual o mostrar una imagen de forma efímera no implica necesariamente consentir su grabación, almacenamiento, descarga, edición o reenvío.

Cuando la captación fue clandestina o no consentida, el supuesto no puede encajar en el art. 197.7 CP, que parte de una obtención con anuencia. En estos casos, pueden entrar en consideración otros apartados de los delitos contra la intimidad. La STS 928/2023, de 14 de diciembre, es una referencia importante para diferenciar la difusión de contenido inicialmente consentido de los supuestos en que la captación en sí misma ya vulneró la intimidad.

4. Deepfakes sexuales: una realidad tecnológica con límites penales aun discutidos

Un deepfake sexual puede consistir en alterar una imagen o vídeo real para simular una conducta sexual, o en generar un contenido hiperrealista que atribuye falsamente a una persona una apariencia o actividad íntima. El perjuicio reputacional, emocional y relacional puede ser muy grave, pero el encaje penal no debe presentarse como automático.

El art. 197.7 del CP está construido sobre imágenes o grabaciones de la propia persona afectada, obtenidas con su anuencia en un entorno reservado. Por ello, el análisis cambia según el origen del material.

Si existen imágenes íntimas reales de la persona, obtenidas o remitidas con consentimiento en un ámbito privado, y se manipulan o difunden después sin autorización, puede haber base para examinar el art. 197.7 CP.

Si se crea un montaje sexual completamente sintético a partir de fotografías públicas, no íntimas, o de material generado desde cero, el encaje directo en ese artículo es discutible pues pueden faltar elementos esenciales del tipo.

Si la persona afectada es menor de edad, pueden cobrar especial relevancia los tipos vinculados a pornografía infantil, incluida la problemática de imágenes manipuladas o virtuales.

La conclusión prudente es que un deepfake sexual puede tener relevancia penal, pero la calificación dependerá de su creación, contenido, difusión, víctima y contexto. No existe una fórmula única aplicable a cualquier imagen falsa creada con inteligencia artificial.

5. Prueba digital: conservar antes de que desaparezca

La prueba electrónica es volátil. Los mensajes pueden borrarse, los perfiles modificarse y los enlaces dejar de funcionar. Por ello, ante una posible difusión no consentida resulta útil conservar:

- Archivo recibido o publicado, evitando su modificación
- Capturas que incluyan el perfil, la hora, URL y destinatarios (siempre que sea posible)
- Mensaje, correos, enlaces, nombres de usuario y datos de las cuentas implicadas
- Comunicaciones donde se reconozca la autoría o se amenace con difundir
- Datos de personas que hayan recibido el contenido o puedan acreditar el reenvío.

Las capturas pueden ser relevantes, pero la atribución de autoría exige normalmente corroboración. Es aconsejable evitar borrar conversaciones o restablecer el dispositivo antes de documentar la evidencia.

6. Conclusiones

La normativa penal española protege la intimidad frente a la difusión no autorizada de imágenes obtenidas o compartidas en un contexto reservado. El consentimiento para crear o remitir contenido no equivale a autorizar su circulación posterior, y un único reenvío puede tener relevancia penal si se cumplen los requisitos legales.

Los deepfakes sexuales plantean un reto adicional: su impacto puede ser profundo, pero su encaje jurídico exige estudiar el origen de las imágenes, el tipo de manipulación, la edad de la persona afectada y la forma de difusión. Un enfoque jurídicamente responsable evita prometer una respuesta única y pone el acento en la preservación de la prueba y en el análisis concreto del caso.

**El presente artículo es meramente divulgativo y no supone asesoramiento ni compromiso de actualización.*

Para más información o asesoramiento, contacte con info@fernandezadvocats.es.