UAB
Universitat Autònoma
de Barcelona

*Trabajo Final de Grado*

# Delitos susceptibles de ser cometidos a través de la Inteligencia Artificial: *Deepfakes* sexuales

Análisis penal de los nuevos retos en la protección de la intimidad

Grado en Derecho

Curso 2024/2025
Autora: Eva Zambrana Ruiz
Tutora: María José Pifarré de Moner

ÍNDICE

**1. Introducción.....4**

**2. Capítulo I: Marco teórico sobre las nuevas tecnologías..... 6**

2.1 La Inteligencia Artificial: definición, evolución y regulación..... 6

2.2 La nueva tecnología de los *deepfakes*: usos lícitos e ilícitos..... 9

2.2.1 Casos relevantes..... 13

**3. Capítulo II: Marco jurídico sobre los delitos con repercusión sexual en la Era Digital.....15**

3.1 *Deepfakes* sexuales: una nueva forma de violencia digital..... 15

3.2 *Deepfakes* de contenido sexual como medio comisivo: aplicación a distintos tipos penales..... 17

3.2.1 Artículo 186 CP: Delito de exhibicionismo y provocación sexual... 17

3.2.2 Artículo 189 CP: Delito de explotación sexual y corrupción de menores..... 20

3.2.2.1 Propuestas legislativas..... 24

3.2.3 Artículos 197 a 201 CP: Delito de descubrimiento y revelación de secretos.....25

3.2.4 Arts. 205 y ss. CP: Delitos contra el honor..... 31

3.2.5 Artículo 172 ter 5: Delito de coacciones.....36

3.2.6 Análisis del acoso sexual (art. 184 CP): exclusión de los *deepfakes* 37

**4. Capítulo III: Responsabilidad penal y la IA.....40**

4.1 Problemas de imputabilidad: ¿Puede una IA ser sujeto de derecho penal?... 40

4.2 La responsabilidad penal de las personas físicas por los delitos cometidos mediante *deepfakes* sexuales.....43

4.2.1 Especial consideración a menores.....46

4.3 Personas jurídicas: Análisis del artículo 31 bis del Código Penal..... 48

**5. Conclusiones..... 52**

**6. Bibliografía..... 56**

ABREVIATURAS

| | |
|---|---|
| CP | Código Penal |
| IA | Inteligencia Artificial |
| Art.(s) | Artículo(s) |
| ss. | Siguientes |
| CE | Comisión Europea / Constitución Española |
| RIA | Reglamento de Inteligencia Artificial |
| STS | Sentencia del Tribunal Supremo |
| STC | Sentencia del Tribunal Constitucional |
| ATS | Auto del Tribunal Supremo |
| BOE | Boletín Oficial del Estado |
| FGE | Fiscalía General del Estado |
| AEPD | Agencia Española de Protección de Datos |
| LORPM | Ley Orgánica de Responsabilidad Penal de Menores |
| LOPD | Ley Orgánica de Protección de Datos |
| RPPJ | Responsabilidad Penal de las Personas Jurídicas |

## 1. Introducción

¿A qué repercusiones legales debería enfrentarse quien, sin consentimiento, utiliza la imagen de otra persona, la altera digitalmente para mostrarla desnuda y la difunde? ¿Qué tipo de responsabilidad penal debería atribuirse a quien manipula el rostro de una persona conocida para insertarlo en un vídeo para adultos con el fin de satisfacer sus propios deseos? ¿Cómo se sienten las víctimas al descubrir el uso indebido de sus imágenes? ¿En qué medida estos supuestos pueden ser tipificados como delitos en la legislación actual?

Todos estos interrogantes han sido consecuencia de la evolución tecnológica que ha transformado la sociedad, de manera que ha permitido la materialización de nuevas formas de agresión en el ámbito sexual. Estas nuevas manifestaciones externas atentan contra una multitud de derechos de otras personas, y para poder ser sancionadas deben encontrarse tipificadas en el Código Penal.

Actualmente nuestro ordenamiento jurídico no cuenta con una respuesta penal específica para afrontar este tipo de supuestos en su conjunto, pues son relativamente recientes. Sin embargo, el legislador está tomando conciencia del aumento de casos que van surgiendo, de modo que se plantea una posible tipificación para ello.

En este sentido, el Derecho Penal se enfrenta al reto de adaptarse a una realidad en la que los delitos han trascendido el ámbito físico para manifestarse en el entorno digital. Entre los ilícitos más comunes destacan los *deepfakes*; vídeos, imágenes o audios generados por Inteligencia Artificial (en adelante "IA") que imitan con precisión la apariencia y la voz de una persona, hasta el punto de poder engañar tanto a los individuos como a los propios algoritmos.

De hecho, según el estudio "*State of deepfakes 2023*" realizado por *Home Security Heroes*, entre 2022 y 2023 la cantidad de pornografía *deepfake* generada aumentó

un 464%, es decir, pasó de haber 3.725 vídeos en 2022 a 21.019 en 2023[1], datos que preocupan socialmente.

Es por ello que decido abordar este trabajo, ya que es sumamente importante regular los nuevos delitos susceptibles de ser cometidos a través de la IA para dar una respuesta judicial efectiva y así brindar seguridad jurídica en la sociedad. La ausencia de una tipificación específica para estos nuevos supuestos impedirá la evolución del Derecho Penal en el entorno digital, además de aumentar la incertidumbre de las propias víctimas.

Por lo tanto, en el desarrollo del presente trabajo, se analizará cómo el Derecho Penal aborda estos supuestos delitos, qué herramientas ofrece para perseguirlos, cómo se deberá determinar la presunta responsabilidad y hasta qué punto es efectiva su regulación. Sin embargo, también será importante identificar las posibles lagunas legislativas y los problemas que surgen en la práctica, ya que muchas veces el Derecho no avanza al mismo ritmo que la tecnología, y tiende a quedarse atrás, lo que produce problemas en su aplicación y protección para las víctimas.

Por ende, la metodología utilizada para este trabajo ha consistido en realizar una lectura exhaustiva de una variedad de fuentes tanto de datos como de doctrina. Además, se proveen al menos 15 sentencias en relación con esta materia o análogas, y análisis de algunos casos prácticos.

[1] Security Hero. (2023). *2023 State of Deepfakes: Realities, Threats and Impact.* https://www.securityhero.io/state-of-deepfakes/

## 2. Capítulo I: Marco teórico sobre las nuevas tecnologías

### 2.1 La Inteligencia Artificial: definición, evolución y regulación

Todos hemos oído hablar últimamente de la Inteligencia Artificial, ¿pero realmente sabemos qué es y desde cuándo existe?

La Inteligencia Artificial es la habilidad de una máquina de presentar algunas capacidades de los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear[2]. O al menos así es como lo define el Parlamento Europeo. Esta expresión también es definida por la Fundación del Español Urgente (FundéuRAE), promovida por la EFE y la Real Academia Española como una "*disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico*", que además la escogieron como palabra del año en 2022.

Aunque la IA no sea capaz de sustituir a un humano completamente, su impacto en diversas áreas es innegable, especialmente en la automatización de tareas y el procesamiento de *big data*. Sin embargo, en ámbitos donde la empatía y el juicio humano son esenciales, como la psicología, la medicina o el derecho, la IA debe ser vista como una herramienta complementaria en lugar de un reemplazo absoluto.

Aunque muchos de nosotros pensemos que la IA es una herramienta novedosa y actual, este término nació durante la conferencia de Dartmouth en 1956, cuando se reunieron los mejores científicos de la época para debatir sobre una posible creación de una máquina que fuera capaz de pensar como un ser humano[3]. Sin embargo, los inicios se remontan en el siglo XX cuando los matemáticos más

[2] Parlamento Europeo. (2020, 8 de septiembre). *¿Qué es la inteligencia artificial y cómo se usa?*. https://www.europarl.europa.eu/topics/es/article/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa.

[3] Gobierno de España. (2023, 19 de abril). *Qué es la Inteligencia Artificial*. Plan de Recuperación, Transformación y Resiliencia. https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr.

prestigiosos de la época trabajaban en las teorías de los sistemas y de la computación, lo cual hizo que se asentaran las bases para la IA. De este modo, John McCarthy, frecuentemente denominado «padre de la inteligencia artificial», acuñó una definición para la IA como "*la ciencia y la ingeniería de hacer máquinas inteligentes, especialmente programas de computadora inteligentes*".
Es curioso poner de relieve que la ciencia ficción fue un elemento clave para inspirar su creación, pues ya en la década de los años 20 se hizo protagonistas de sus historias a los robots y a máquinas inteligentes, creando así entre el público una cultura popular enfocada al nacimiento de posibles nuevas tecnologías.

Lo que ha sucedido en estos últimos años ha sido algo insólito; aunque algunas tecnologías con inteligencia ya formaban parte de nuestras vidas desde hace más de 50 años, los nuevos algoritmos y la capacidad de computación han sido los causantes del gran progreso en esta área, hecho que justifica que a día de hoy tengamos una herramienta tan potente como la IA generativa, capaz de ayudarnos en casi todos los ámbitos de nuestra vida.

Es por este motivo que no resulta extraño ver a nuestro alrededor el uso de la Inteligencia Artificial en sectores tan cotidianos como en la medicina, donde se emplea para la detección temprana de tumores y el desarrollo de tratamientos personalizados; el deporte, optimizando el rendimiento de los atletas mediante el análisis de estadísticas captadas por cámaras de alta precisión; o las plataformas digitales, donde los sistemas de recomendación personalizan el contenido según los intereses de cada usuario. Incluso en nuestro campo, el Derecho, tenemos una plataforma legal que reúne la mayor base de datos de legislación y jurisprudencia, vLex, que recientemente ha incorporado también la IA con la creación de *Vincent AI*, un asistente informático que analiza distintos documentos, responde a preguntas jurídicas y automatiza la redacción de textos legales.

Si bien todo lo expuesto hasta ahora hace pensar que la Inteligencia Artificial es una herramienta muy positiva y que ha llegado para quedarse, ello no implica que esté exenta de riesgos o consecuencias negativas que deban ser reguladas.

La protección de datos y la privacidad del individuo son esenciales para la salvaguarda de los derechos fundamentales, por lo que el entrenamiento de la IA debe estar en manos de personas que garanticen el respeto a esos valores. Por ello, resulta imprescindible establecer una regulación adecuada y específica que asegure un uso responsable de ésta, con tal de proteger tanto el interés público como los derechos de los ciudadanos.

El Parlamento Europeo y el Consejo han sido pioneros en crear unas normas armonizadoras en materia de Inteligencia Artificial para todos los países de la Unión Europea. De esta manera, pretenden "*impulsar el desarrollo, la utilización y la adopción en el mercado interior de la IA y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad y la protección de los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, reconocidos y protegidos por el Derecho de la Unión*[4]".

Es así como ha surgido el Reglamento (UE) 2024/1689, de 13 de junio de 2024[5], de Inteligencia Artificial. En dicho texto se regulan aspectos tan esenciales como su aplicabilidad a los individuos y entes, las prácticas que se consideran prohibidas (art. 5), los sistemas de IA calificados de "alto riesgo" (art. 6), etc. Pero además impone la obligación de la transparencia a los responsables y proveedores de determinados sistemas de IA (art. 50), ya que todo el mundo tiene derecho a saber que lo que está viendo no es real, sino un producto generado por la inteligencia artificial.

Además, a través del desarrollo del Reglamento 2024/1689, se prevé la creación de instituciones encargadas de supervisar y controlar las prácticas y los sistemas que tienen implementada la IA, como la Oficina Europea de Inteligencia Artificial, el Consejo Europeo de IA (art. 65), así como la formación de un grupo de expertos científicos que asesorarán a dichas instituciones (art. 68).

---

[4] *VLex*. (s. f.). https://justis.vlex.com/vid/1043286588

[5] por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828.

En relación con las disposiciones reguladas del Reglamento, debemos tomar en especial consideración el artículo 5, referente a las "Prácticas de IA prohibidas". En este, como bien indica su título, se regulan aquellas prácticas de IA que deben estar prohibidas, como "*la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, [...], con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona [...] de un modo que provoque, [...], perjuicios considerables a esa persona o a otra* (b)".

En dicho artículo se regulan distintos comportamientos en torno a sistemas de IA, pero no contiene ninguna mención expresa a otros delitos de diversa naturaleza que pueden cometerse a través de esta herramienta. Así, conductas relacionadas con la utilización de la inteligencia artificial para la comisión de delitos contra la libertad sexual, la intimidad o el honor, no se encuentran específicamente contempladas en el texto, por lo que tampoco se aborda cómo debe responder el Derecho Penal ante estos nuevos riesgos, especialmente ante fenómenos como la generación y difusión de contenido íntimo no consentido mediante IA o la manipulación de datos privados con fines delictivos, dejando un vacío preocupante en la protección de las víctimas. No obstante, aunque no se regulen de manera explícita, algunas de estas conductas podrían subsumirse en tipos penales ya existentes.

La falta de normativa específica, plantea muchas dudas: ¿son suficientes las normas actuales para perseguir estos delitos?, ¿cómo se protege a quienes sufren estas nuevas formas de violencia digital? La tecnología avanza rápido, pero la ley parece ir un paso por detrás.

### 2.2 La nueva tecnología de los *deepfakes*: usos lícitos e ilícitos

Desde hace unos años, ha surgido un tipo de "ciberviolencia" que sigue siendo noticia a día de hoy y que, a pesar de su gravedad, no parece preocuparnos lo suficiente la manera en que se aborda. Estamos hablando de los *deepfakes*, un tipo de contenido que ha sido creado mediante el uso de tecnología de procesamiento

de gráficos y técnicas avanzadas de aprendizaje profundo (*deep learning*) con el objetivo de generar vídeos o audios que parecen reales pero que en realidad son completamente falsos[6], de modo que se haga creer a los usuarios que están viendo a una persona determinada realizando acciones o declaraciones que nunca ocurrieron[7]. De hecho, su traducción literal significa "falsedades profundas", por lo que aunque el *deepfake* no se cree necesariamente para engañar, es fácil hacerlo cuando no se advierte de que se trata efectivamente de un contenido manipulado.

Si bien producir este contenido desde cero es complejo, la existencia de programas de código abierto (*open source*) ha facilitado su acceso, permitiendo que cualquier persona pueda utilizar estas herramientas para mejorar el realismo de las fotos y vídeos creados.

Es por ello que la tecnología de los *deepfakes* se puede encontrar en múltiples contextos de nuestra vida cotidiana. Un ejemplo de ello es el entretenimiento, donde es capaz de crear vídeos y películas, simulando tanto la imagen como la voz[8], tal y como se ve en la película *The Irishman* (2019), en la que se usó esta herramienta para rejuvenecer al actor Robert de Niro y así simular distintas etapas de su vida. También se usan los *deepfakes* en el marketing o la publicidad, donde se da la oportunidad de revivir a celebridades ya fallecidas para que aparezcan en sus campañas, tal y como sucedió con Audrey Hepburn, que protagonizó falsamente una campaña de los chocolates *Galaxy* en 2013. Otro caso que tuvo una gran trascendencia entre los jóvenes ocurrió en 2023, cuando la voz del artista puertorriqueño Bad Bunny fue clonada por el usuario anónimo "*FlowGPT*" para crear una canción que fue mundialmente conocida (Nostalgia), y que muchos de sus seguidores creyeron auténtica de dicho autor.

También es cierto que el uso consentido de la IA a través de los *deepfakes* puede dar como resultado aplicaciones con un impacto positivo en la vida de las

---

[6] Simó Soler, E. (2023). *Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho*. InDret 2.2023 ,pp. 493-515.

[7] INCIBE. *Deepfakes*. (s.f.). https://www.incibe.es/aprendeciberseguridad/deepfakes.

[8] Un problema cada vez más presente en el sector de los locutores quedó en evidencia en 2023, cuando la Asociación Española de Locutores emitió un comunicado alertando sobre el impacto de la inteligencia artificial en su profesión

personas, entre ellas la clonación de voz en pacientes con trastornos neurodegenerativos, como la esclerosis lateral amiotrófica (ELA)[9]. En estos casos, la tecnología puede ayudar a estas personas a comunicarse con sus seres queridos de una manera más auténtica y recuperar su identidad vocal.

Aunque estos usos sean innovadores y además permitan que las empresas optimicen el rendimiento de su trabajo a cambio de ahorrar en costes, también plantean dilemas éticos y posibles riesgos, como la posibilidad de engañar al público[10] o utilizar los datos de las personas representadas sin su consentimiento. De hecho, fue Danielle Citron en 2014 quien también compartió esta idea en su obra "*Hate Crimes in Cyberspace*", donde destacó que los *deepfakes* no sólo se empleaban con fines de entretenimiento, sino que también podían ser utilizados con propósitos maliciosos, incluidos para cometer delitos que atentan contra la libertad sexual.

Es en este punto donde radica el problema principal; aunque se trata de imágenes falsas, se generan a partir de datos reales extraídos de redes sociales u otras fuentes sin el consentimiento de la persona involucrada. Esto, de un modo u otro, amenaza su privacidad y protección de datos, ya que la imagen es utilizada sin la correspondiente autorización para crear contenido manipulado, y posteriormente, la mayoría de casos también es difundido.
A pesar de la evidente invasión a la privacidad, actualmente no parecen existir suficientes soluciones jurídicas que frenen el uso indebido de estos datos personales.

El conflicto se agrava cuando, además de vulnerar la privacidad de sus datos, la víctima sufre daños a su reputación, traumas psicológicos, ansiedad, depresión y otros problemas de salud mental[11]. Estas secuelas suelen intensificarse en el

---

[9] Chesney, B; Citron, D. (Diciembre del 2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* — California Law Review. California Law Review. https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security.

[10] Es el caso de un estafador para engañar a una mujer francesa y estafarle cerca de un millón de euros creyendo que mantenía una relación con Brad Pitt desde hacía un año y medio.

[11] Laffier, J.; Rehman, A. (2023, 24 de junio). *Deepfakes and Harm to Women*. https://doi.org/10.51357/jdll.v3i1.218

contexto de los *deepfakes* sexuales, en los que se generan imágenes y vídeos falsos de índole sexual que simulan situaciones íntimas sin el consentimiento de la persona, convirtiéndose en una poderosa herramienta de abuso, extorsión y humillación. Este acontecimiento no sólo constituye una grave vulneración a la intimidad, sino que también podría ser considerada una forma de abuso sexual, ya que provoca a la víctima una "*situación objetiva y gravemente intimidatoria, hostil o humillante*", tal y como lo describe el artículo 184 del Código Penal.

La cuestión que nos lleva hasta aquí es que, ante la creación y difusión de los *deepfakes* sexuales, son varios derechos los que se ven afectados y que, por precaución y protección hacia las víctimas, debería existir una respuesta jurídica capaz de identificar y sancionar quienes se benefician del uso indebido de datos personales y los utilizan para humillar a las víctimas o satisfacer sus deseos sexuales, sin tener en cuenta la repercusión que puede tener dicho contenido.

Desde la perspectiva del Derecho Penal, como los *deepfakes* sexuales atentan contra una serie de bienes jurídicos que se ven vulnerados, de alguna manera podrían corresponderse con delitos que ya están tipificados en el Código Penal, simplemente variando el instrumento mediante el cual se comete. Por lo tanto, lo ideal sería ampliar la tipificación de los delitos ya existentes en el texto penal para cubrir todas las formas en que estos hechos pueden realizarse. No dudemos que el uso de sistemas de IA en la comisión de delitos representa una evolución de la ciberdelincuencia tradicional.

Antes de analizar qué delitos pueden ser cometidos a través de la IA y considerar su posible tipificación, debemos establecer un marco general que nos permita saber cuándo una inteligencia artificial ha sido clave para llegar a cometer un ilícito penal. En este caso debemos tener en cuenta diferentes cuestiones.

En primer lugar, la cuestión que es imprescindible abordar es si cabe atribuir personalidad jurídica a la IA a efectos del Derecho Penal, de acuerdo con los artículos 27 y 28 del CP[12]. La mayoría de juristas se decantan por no reconocer

[12] Cabrales Acosta, J.M. (2024, 26 de marzo). *La inteligencia artificial y la nueva delincuencia*. Lefebvre. ELDERECHO. https://elderecho.com/la-inteligencia-artificial-y-la-nueva-delincuencia.

personalidad jurídica a la IA al carecer de autonomía personal, entre otras cualidades que son inherentes a la persona física. Es así como debemos entender este aspecto; al considerar que en el Derecho Penal se requiere dolo o imprudencia en el sujeto activo del delito, es ontológicamente imposible dotar de responsabilidad a la IA, puesto que no tiene personalidad física ni jurídica.

Es por ello que, con la regulación que disponemos a día de hoy, lo único que podemos interpretar desprendiéndose del art. 28 es que sólo podría imputarse la autoría del hecho al sujeto que efectivamente realiza el hecho. Por lo tanto, la IA podría ser la herramienta a través de la cual se comete el delito, pero esta tecnología no puede considerarse como autora, de momento.

Este escenario no supone una variación del sistema de atribución de responsabilidad penal que existe legalmente, puesto que quien ejecute la acción típica, deberá responder como autor de los hechos delictivos.

Existen otras posibles situaciones sobre la atribución de responsabilidad penal en el uso ilícito de sistemas de IA, pero su análisis se abordará en un capítulo posterior *(véase Capítulo III)*.

### 2.2.1 Casos relevantes

A pesar de que existen numerosos casos diarios que reflejan la importancia y preocupación de esta nueva tecnología, uno de los más mediáticos en España fue el caso de Almendralejo (Badajoz), donde varios estudiantes menores de edad utilizaron Inteligencia Artificial para generar imágenes falsas de sus compañeras de clase de contenido sexualmente explícito y posteriormente difundirlas mediante redes sociales y plataformas de mensajería móvil.

La Fiscalía de Menores de Extremadura recogió los hechos y, con ayuda de la Policía Nacional, identificaron a algunos de los menores que habían cometido y participado en la creación y difusión de dichas imágenes. Un Fiscal Superior de la Comunidad Autónoma de Extremadura describió el caso como “alarmante”,

puesto que "se suplantan identidades mediante la manipulación fotográfica, cosa que atenta contra la intimidad y honor de las víctimas"[13].

Casi un año más tarde, el Juzgado de Menores de Badajoz declaró a 15 menores de edad responsables por veinte delitos de pornografía infantil y otros veinte delitos contra la integridad moral. La condena impuso a cada uno de ellos la medida de libertad vigilada durante un año, especialmente orientada a recibir formación afectivo sexual sobre el uso responsable de las tecnologías de la información, la comunicación, y sensibilización en materia de igualdad y género[14].

Aunque este caso concluyó con una resolución judicial efectiva, la condena se basó en tipos penales existentes que no estaban diseñados específicamente para los *deepfakes* sexuales.

Mientras de la legislación vigente no acaben de proporcionarse respuestas más claras, son los tribunales los que tienen que ir adaptando las normas existentes a situaciones que hace unos años no se contemplaban, evidenciando la necesidad de una regulación específica.

---

[13] Redacció. (2023, 19 de septiembre). *Alumnes d'institut denuncien la difusió de fotos seves despullades creades amb IA a Badajoz*. 3Cat. https://www.3cat.cat/324/alumnes-dinstitut-denuncien-la-difusio-de-fotos-seves-despullades-creades-amb-ia-a-badajoz/noticia/3250408/

[14] Comunicación Poder Judicial. (2024, 9 de julio). *Imponen la medida de libertad vigilada durante un año a los 15 menores acusados de manipular y difundir imágenes de menores desnudas en Badajoz*. Consejo General del Poder Judicial. Noticias Judiciales. https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/Imponen-la-medida-de-libertad-vigilada-durante-un-ano-a-los-15-menores-acusados-de-manipular-y-difundir-imagenes-de-menores-desnudas-en-Badajoz.

## 3. Capítulo II: Marco jurídico sobre los delitos con repercusión sexual en la Era Digital

### 3.1 *Deepfakes* sexuales: una nueva forma de violencia digital

Como ya hemos estado comentando, los *deepfakes* sexuales no son algo novedoso, sino que lleva existiendo desde hace varios años. No por eso se debería normalizar, ya que supone una nueva forma de violencia sexual especialmente hacia las mujeres, que son la mayor parte de las personas afectadas[15]. Este comportamiento se basa en la ausencia de consentimiento[16], es decir, el hecho de que se publiquen libremente las fotos en Internet, ¿da permiso a que un tercero se apodere de ellas y las manipule creando contenido sexual para su posterior difusión? En este caso, ¿cuáles son las herramientas eficaces para frenar este contenido?

Cecilia Barba Arteaga, periodista e investigadora en comunicación, explica en su artículo "*Deepfakes sexuales: impacto, prevención y perspectivas de género en el entorno digital*"[17] que durante su investigación concluyó que los deepfakes sexuales estaban clasificados dentro de la categoría de Abuso Sexual Basado en Imágenes (ASBI), lo cual implica la producción, difusión o amenaza de material sexual explícito sin el consentimiento de la persona afectada. Este concepto fue

[15] Flynn, A., Powell, A., Scott, A., Cama, E. (2021, 3 de diciembre). *Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse.* The British Journal of Criminology, Volume 62, Issue 6, November 2022, Pages 1341–1358, https://doi.org/10.1093/bjc/azab111.

[16] La STC 27/2020, de 24 de febrero (ECLI:ES:TC:2020:27) estableció la necesidad del consentimiento expreso del titular para la publicación de cualquier fotografía extraída de redes sociales. El Tribunal Constitucional concluyó que el titular del derecho fundamental debe autorizar cada acto concreto de utilización de su imagen, así como los fines para los que lo otorga, ya que el consentimiento prestado para la captación de la imagen no se extiende a otros posteriores, como por ejemplo su publicación o difusión. Asimismo también señaló que dicho consentimiento no puede reputarse como indefinido y vinculante con respecto a aquél que se prestó inicialmente para una ocasión o con una finalidad determinada.

[17] Barba Arteaga, C. (2024). *Deepfakes Sexuales: impacto, prevención y perspectivas de género en el entorno digital*. Miguel Hernández Communication Journal, 15, 229-244. https://doi.org/10.21134/zt4eht31. Fecha de consulta 22 de febrero de 2025.

acuñado por la jurista norteamericana JARVIS COOPER[18], y aunque en este contexto permite englobar una amplia variedad de conductas, no deja de tratarse de una concepto jurídico estadounidense, con escasa o nula relevancia en nuestro ordenamiento.

De todas maneras, esta forma de abuso digital supone una grave vulneración de la privacidad y la dignidad de la persona, y a diferencia de la sextorsión o la pornovenganza, para crear los *deepfakes* ya no es necesario poseer previamente imágenes íntimas de la víctima, lo que implica que cualquier mujer puede ver su rostro utilizado en contenido pornográfico, lo cual constituye una realidad alarmante. También es importante destacar que la principal finalidad de los *deepfakes* sexuales es la de ridiculizar y vejar a la víctima, con lo cual constituyen herramientas especialmente poderosas, ya que son capaces de convertirse en un instrumento de control sobre las víctimas de este abuso, además de generar un entorno degradante y ofensivo en cualquier ámbito.

Antes de entrar a analizar los delitos que pueden cometerse a través de los *deepfakes* sexuales, es fundamental señalar que la intimidad personal abarca inseparablemente la esfera de la sexualidad. Es por ello que la sexualidad no constituye una dimensión aislada, sino que es una parte esencial de la intimidad de cada individuo. Por este motivo, cualquier vulneración de la intimidad a través de los *deepfakes* que pueda tener connotación sexual, no solamente afecta a la privacidad de la persona, sino que también impacta de manera directa en su dignidad, propia imagen y honor, lo que justifica la necesidad de una respuesta penal adecuada para combatir estos nuevos delitos.

[18] Jarvis Cooper, L. (2023, 17 de abril). *Sexual Privacy and Persecution*. UCLA Law Review. SSRN. https://www.uclalawreview.org/sexual-privacy-and-persecution/.

### 3.2 *Deepfakes* de contenido sexual como medio comisivo: aplicación a distintos tipos penales

En este apartado se abordará el análisis de los delitos con repercusión sexual que pueden ser cometidos a través de la IA, en especial mediante el uso de *deepfakes*, así como su posible inclusión en el Código Penal.

Antes de proceder con el análisis, conviene destacar que dicho contenido audiovisual de naturaleza sexual debe ser falso aunque realista al haber sido alterado mediante IA, pero la parte utilizada de la imagen de la víctima debe ser verdadera. BOLAÑOS GARCÍA también define a los *deepfakes* de contenido sexual como aquellos "contenidos creados con el ánimo de parecer reales y de un alto grado de realismo, para vejar a personas individuales y que parezca que están teniendo comportamientos vejatorios o actividades de naturaleza sexual"[19].

Cabe señalar que la imagen de la víctima que ha sido manipulada, normalmente se hace sin el consentimiento de ésta, de modo que se crea un *deepfake* de naturaleza sexual o pornográfica con la que se pretende, con su posterior difusión, vejar y humillar a la víctima.

#### 3.2.1 Artículo 186 CP: Delito de exhibicionismo y provocación sexual

El delito de provocación sexual regulado en el artículo 186 CP contiene 4 elementos típicos acumulativos que deben darse para encontrarnos dentro de esta tipología delictiva:

1) Por cualquier medio directo;
2) Vender, difundir o exhibir;
3) Material pornográfico;
4) Entre menores de edad o personas con discapacidad necesitadas de especial protección.

[19] Consejo de Ministros. (2025, 25 de marzo). *Rueda de prensa tras el Consejo de Ministros: Félix Bolaños, Pilar Alegría y Sira Rego.* La Moncloa. https://www.lamoncloa.gob.es/multimedia/videos/consejoministros/Paginas/2025/250325-rueda-de-prensa-ministros.aspx

Para poder determinar si este delito puede ser cometido mediante *deepfakes* sexuales, debemos analizar si en alguno de estos puntos puede tener cabida su realización mediante esta nueva tecnología.

Al encontrarnos dentro de la categoría de delitos sexuales, el bien jurídico que se busca proteger es la libertad sexual, concretamente en este caso la de los menores y personas discapacitadas. Esto es importante ya que son personas necesitadas de especial protección que pueden sufrir daños en su proceso educativo y en la formación y desarrollo de su personalidad y sexualidad[20]. Es por ello que esta tipología delictiva sólo tiene este carácter si los sujetos pasivos afectados son menores o personas con discapacidad.

Para delimitar el significado del concepto "material pornográfico" nos acogemos a la definición que nos proporciona la jurisprudencia señalada en el texto de QUINTERO OLIVARES[21]: "*toda obra gráfica, literaria, fílmica con miras exclusivamente libidinosas, carente de todo valor artístico, cultural, literario, científico, pedagógico o informativo*". Aún así, la Real Academia Española también define este concepto como: "*toda aquella representación explícita de actos sexuales que busca producir excitación*". Es por ello que el material pornográfico debe tener como objetivo la excitación o estimulación sexual de quien lo consume.

En cuanto a la tipología de actividad que debe realizar la persona activa para ser culpable, ésta debe «vender, difundir o exhibir». Si atendemos a la primera conducta, a cambio de la venta del material pornográfico debe darse un beneficio económico en forma de ánimo de lucro.
Por "difundir" se entiende la divulgación de dicho material, ya sea a través de internet o medios de comunicación, siempre y cuando sea entre menores de edad o personas con discapacidad.

---

[20] Vidal. G. (2024, 20 de junio). *Los delitos de exhibicionismo y provocación sexual en el Código Penal*. Gerson Vidal. https://www.gersonvidal.com/blog/delitos-exhibicionismo-provocacion-sexual/.

[21] Quintero Olivares, G. (2011). *Esquemas de la parte especial del derecho penal* (Vol. 32). Tirant lo Blanch.

Al mismo tiempo, dicha acción también puede consistir en "exhibir"[22], lo que comporta el hecho de mostrar el material pornográfico entre aquellos grupos que el artículo describe[23]. Es decir, dentro de esta definición se incluyen aquellas situaciones en las que dicho contenido se exhibe físicamente o se muestra digitalmente a través de pantallas[24].

Por último, debe tenerse en cuenta que el delito debe realizarse "*por cualquier medio directo*", esto es, la necesidad de una relación directa entre el sujeto activo y el sujeto pasivo del delito, carente de intermediarios entre actor y destinatario[25]. Es por ello que GÓMEZ TOMILLO exige que la acción suponga un contacto físico entre el autor y la víctima. Sin embargo, explica que la *difusión* no puede ser realizada mediante una presencia física entre ambos sujetos, sino que solamente puede llevarse a cabo mediante Internet. Por este motivo no cabe una interpretación estricta de este elemento en particular, ya que se estaría vaciando de contenido dicha modalidad delictiva prevista en la ley.

Una vez llegados a este punto, podemos considerar que el material pornográfico, como uno de los elementos principales de este precepto, no contiene ninguna restricción en su creación, es decir, podría tener cierta cabida el uso de los *deepfakes* sexuales para cometer el delito del 186 CP. Aunque se tratase de imágenes generadas artificialmente, el contenido de estas reproduce actos sexuales de forma explícita y suele estar destinado al consumo con fines de excitación, cumpliendo así la finalidad de la pornografía. De hecho, Jacobsen, B.

---

[22] Gómez Tomillo, Manuel (2010). *Comentarios al Código Penal.* Valladolid. Lex Nova. Página 740.

[23] Cabe destacar que, tal y como expone Morales Prats en "*Comentarios al Código Penal*" de Gómez Tomillo, "*no toda exhibición circunstancial que por efectuarse genéricamente pueda ser percibida por menores o incapaces, resultara relevante penalmente, ya que el quiosquero que tiene expuestas revistas con contenido pornográfico, en cuanto las vean menores que van a comprar, no podría constituirse el tipo delictivo del art. 186, pues no se considera forma directa, ya que no había una intención estricta de que los menores contamplaren las revistas".*

[24] Código Penal Online. (s.f.). *Artículo 186 del Código Penal explicado* (2024). https://codigopenal.online/articulo-186/.

[25] Op. Cit.

N., y Simpson, J.[26] señalan que los *deepfakes* se identificaron por primera vez en el ámbito de la pornografía. Añaden que, aunque no todo *deepfake* tiene una naturaleza pornográfica, VAN DER NAGEL[27] citó un estudio en el que determinó que el 96% de las imágenes *deepfake* de carácter sexual corresponden a pornografía no consensuada en su difusión.
Además no hemos de olvidar lo que se ha dicho *supra*[28]*:* casi todo el contenido pornográfico realizado mediante *deepfakes* tiene como protagonistas mujeres, tal y como lo confirma el informe *State of deepfake 2023*[29].

Una vez dicho lo anterior, debemos considerar una posible ampliación en el tipo penal existente, de modo que entren a regularse también los *deepfakes* sexuales como una nueva modalidad de cometer el delito relativo a la provocación sexual.

### 3.2.2 Artículo 189 CP: Delito de explotación sexual y corrupción de menores

Otro tipo penal susceptible de ser cometido mediante *deepfakes* sería la conducta de pornografía infantil, establecida en el art. 189 CP, en la que también se busca proteger la libertad o indemnidad sexual de los menores o personas con discapacidad necesitadas de especial protección, además de la dignidad (individual o de la infancia) y la integridad física[30].
Este delito prevé principalmente dos conductas punibles. La primera se refiere a aquella persona que capte o utilice a menores de edad o a personas con discapacidad con fines o en espectáculos exhibicionistas o pornográficos, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financie cualquiera de estas actividades o se lucre de ellas.

---

[26] Jacobsen, B. N., & Simpson, J. (2023). *The tensions of deepfakes.* Information, Communication & Society, *27*(6), 1095–1109. https://doi.org/10.1080/1369118X.2023.2234980.

[27] Van der Nagel, E. (2020, 2 de junio). *Verifying images: deepfakes, control, and consent*. Porn Studies, 7(4), 424–429. https://doi.org/10.1080/23268743.2020.1741434.

[28] Pág. 4

[29] Op.Cit.

[30] Exposición de motivos de la Ley Orgánica 11/1999, de 30 de abril.

El segundo comportamiento ilícito hace referencia a aquél que produzca, venda, distribuya, exhiba, ofrezca o facilite la producción, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad, o lo poseyera para estos fines.

Ambas conductas comparten como elemento común el contenido pornográfico que muestre menores de edad[31], término que el propio Código Penal define a través de varias disposiciones. En esencia, se considera como tal cualquier material que represente visualmente a un menor o una persona con discapacidad necesitada de especial protección, participando en una conducta sexualmente explícita, ya sea real o simulada[32].

Para profundizar en los elementos de este delito, tomaremos como referencia la Circular 2/2015, de 19 de junio, de la Fiscalía General del Estado[33], que aunque no sea una norma jurídica –sino más bien una opinión autorizada–, proporciona criterios clave para su análisis.

En cuanto a la definición de la letra *a)* que acabamos de ver, la Fiscalía General del Estado ordena a sus miembros que excluyan totalmente de esta interpretación el material pornográfico escrito y el mero desnudo[34], tal y como recoge la STS nº1342/203, de 20 de octubre, en la que se consideró que la imagen de un desnudo no puede ser considerada objetivamente material pornográfico, con independencia del uso que de las fotografías pueda posteriormente hacerse. Sin embargo, el desnudo con connotaciones sexuales sí puede ser considerado como tal, ya que así lo dispone el ATS nº 521/2013, de 21 de febrero.
Además, en opinión de la FGE existiría una limitación respecto al material

[31] La STS nº 271/2012, de 26 de marzo ha definido la pornografía infantil como cualquier material audiovisual que utiliza a niños en un contexto sexual, aunque es necesario que el material visual se centre en un comportamiento sexual de un menor o bien en sus órganos sexuales.

[32] Art. 189.1 apt. 2 a) CP

[33] Madrigal Martínez-Pereda, C. (2015, 19 de junio). *Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015*. Fiscalía General del Estado. https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2015-00002.pdf.

[34] STS nº 376/2006, de 8 de marzo; STS nº 803/2010, de 30 de septiembre; STS nº 264/2012, de 3 de abril.

audible, ya que, en términos generales, el audio por sí solo no es suficiente para ser considerado pornografía, dado que ésta requiere representaciones visuales. No obstante, en ciertos casos, el contenido sonoro puede ser relevante para determinar la naturaleza pornográfica o no de un vídeo[35].

Por otro lado, es importante destacar que el Código Penal contempla tanto el material pornográfico real como el simulado[36], lo que permite incluir lo que se conoce como «pornografía virtual». Esta categoría, definida por la doctrina de la FGE, abarca aquellas representaciones en las que la imagen del menor es una creación artificial pero realista, generada mediante ordenador u otros medios.
Para el enfoque de este trabajo, este aspecto resulta fundamental, ya que esta interpretación implica la inclusión en el concepto de material pornográfico el *deepfake* de contenido sexual, dejando claro el alcance del delito y sus posibles manifestaciones en el entorno digital. Para ello, ha bastado una aclaración fruto de la normal tarea interpretativa prevista en la ley para asegurarse de que los *deepfakes* entran en el viejo concepto.

En relación con lo anterior, el art. 189.1.d) también define la pornografía infantil como aquellas "*imágenes realistas de un menor participando en una conducta sexualmente explicita [...] con fines principalmente sexuales*". Que una imagen sea realista implica, según la RAE, que trate de ajustarse a la realidad, es decir, que no sea auténtica pero que lo parezca, entendiéndose también por la FGE[37] que *"no deberán entender incluidos dibujos animados, manga o representaciones similares, pues no serían propiamente "imágenes realistas", en tanto no perseguirían ese acercamiento a la realidad.*"

Esta definición podría aplicarse al concepto fundamental de este trabajo, los "*deepfakes* sexuales"; imágenes manipuladas –mediante IA– con fines sexuales que representan a personas reales, en el caso concreto de este tipo penal, menores.

[35] Op. Cit. Pág. 3

[36] Art. 189.1 par. 2 letra c)

[37] Circular 2/2015, de 19 de junio, de la FGE.

Para acabar de perfilar este concepto, el CP también nos proporciona una última definición que hace referencia al "*material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada [...], salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes*". Es a esto a lo que la FGE llama «pornografía técnica»[38], es decir, aquellas representaciones en las que aparecen personas presentadas como menores en un contexto sexual.

La Fiscalía solicitó que, para que pudiera tener relevancia penal, debía atenderse al aspecto físico de la persona (facciones, vestimenta, etc.), ya que mediante sus rasgos pueden aparentar ser menores de edad (rasgos aniñados, peinados…). No obstante, esta apariencia no determina automáticamente su relevancia penal, sino que debe analizarse cada caso concreto. Es decir, si las investigaciones correspondientes pueden determinar la minoría de edad de la persona representada en la fecha en que se produjo el material, la calificación habrá de referirse al material pornográfico infantil común[39]. En cambio, si se comprueba posteriormente que el protagonista de dicha escena tenía en realidad 18 o más años cuando se produjo el material, habría de excluirse la responsabilidad penal de la conducta, al menos de este delito en concreto.

Sin embargo, si no puede determinarse con exactitud si la persona representada es menor o mayor de edad pero el material la "presenta" como menor, la Fiscalía entiende que deberá realizarse una interpretación amplia considerando el material como pornografía infantil, y viceversa; si el material no presenta a dicha persona como menor de edad, no podrá imputarse delito alguno. Por lo tanto, los dos elementos claves en el tipo penal bajo examen son, pues:

a) Si los protagonistas del material son menores, y/o
b) Si a estas personas se las presenta como menores.

[38] Art. 189.1 par. 2 letra c)

[39] Circular 2/2015, de 19 de junio, de la FGE., apt. 2.4.

Además de los elementos principales del delito de pornografía infantil previstos en el artículo 189 CP, los apartados 4, 5 y 6 del mismo precepto tipifican otras conductas igualmente punibles. De ellas, sólo la del apartado 5 podría cometerse mediante el uso de *deepfakes*, ya que se refiere a la posesión de la pornografía infantil, un concepto que ya hemos definido y que puede abarcar tanto el material real como el simulado.

Así lo entiende la FGE, según la cual a partir de la reforma 1/2015, este apartado supone una "ampliación del radio de las conductas típicas relacionadas con la posesión, pues será delito adquirir o poseer material pornográfico virtual o técnico".

#### 3.2.2.1 Propuestas legislativas

Todavía cabe señalar que nuestro actual Gobierno ha aprobado recientemente la tipificación de los delitos *deepfakes* de contenido sexual así como el *grooming*. El Ministro de la Presidencia, Justicia y Relaciones con las Cortes, Félix Bolaños, y la ministra de Juventud e infancia, Sira Rego, presentaron el día 25 de marzo de este mismo 2025 las bases del Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, que se aprobó el mismo día por el Consejo de Ministros y que se remitirá al Congreso de los Diputados para su ulterior aprobación[40]. El ministro explicó que el Gobierno "protege de manera muy especial a los menores y a las víctimas de violencia sexual en el ámbito digital, de tal manera que les reconocen el derecho a ser reconocidos como víctimas de estas violencias [...]", además de precisar que hay una falta de adaptación de la normativa vigente hacia los nuevos avances tecnológicos, por lo cual deberá comportar una modificación del Código Penal así como de la Ley de Protección de Datos Personales.

En la redacción del nuevo texto –insiste– se incorporarán modificaciones en los delitos actualmente previstos, como en el artículo 186, relativo al exhibicionismo

[40] Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. (2025, 25 de marzo). *El Gobierno aprueba tipificar como delito los deepfakes de contenido sexual y el grooming*. Secretaría de Estado de Justicia. https://www.mjusticia.gob.es/es/institucional/gabinete-comunicacion/noticias-ministerio/Proteccion-menores-entorno-digital.

y a la provocación sexual (ver *supra*), en el que se establecerá como delito la puesta a disposición de material pornográfico a menores "de manera indiscriminada", aunque ya se concretará la manera de hacerlo.

También se prevé la introducción de un nuevo artículo, el 173 bis, que sancionaría "a quienes, sin autorización de la persona afectada y con ánimo de menoscabar su integridad moral, difundan, exhiban o cedan su imagen corporal o audio de voz generada, modificada o recreada mediante sistemas automatizados, software, algoritmos, inteligencia artificial o cualquier otra tecnología, de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorias".

Esta tipificación implica que los *deepfakes* de contenido sexual o «gravemente vejatorios», como precisa el Ministro Bolaños, serán delito "cuando por su grado de realismo pretendan vejar a una persona en concreto", independientemente de que la víctima sea mayor o menor de edad. Es por ello que no solamente estarán tipificados dentro de los delitos contra la libertad e indemnidad sexual, sino que también se incluirán en la regulación de los delitos contra la integridad moral[41].

### 3.2.3 Artículos 197 a 201 CP: Delito de descubrimiento y revelación de secretos

El tipo penal que nos disponemos a analizar protege la intimidad personal, derecho fundamental regulado en el art. 18.4 CE. Este aspecto abarca, como explica QUINTERO OLIVARES, todos aquellos ámbitos en los que ésta puede proyectarse, con independencia del sustrato en el que se plasme (correo electrónico, comunicaciones telefónicas, fotografías, documentos, etc.). Asimismo, la protección de este derecho depende en exclusiva de la voluntad del titular de mantener la reserva respecto de determinados ámbitos personales. Es decir, el consentimiento del sujeto activo reviste especial importancia a la hora de determinar la punibilidad de la conducta.

No hay que olvidar que la "intimidad" como bien jurídico también se encuentra protegida en la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor,

[41] Op. Cit.

a la intimidad personal y familiar y a la propia imagen, además de en la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[42].

El delito de descubrimiento y revelación de secretos que estamos analizando cuenta con varias conductas punibles, aunque solo los apartados 2, 3 y 5 son de interés para nuestro objeto de estudio.

En primer lugar, la conducta prevista en el art. 197.2 castiga a quien, «*sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal [...] que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. [...]*».

En este apartado se contempla una conducta punible atribuible al sujeto pasivo, que puede consistir en apoderarse, utilizar o modificar determinados datos. El Tribunal Supremo define estos términos en la sentencia nº 771/2023, de 18 de octubre: por "apoderarse" entiende la traslación de datos a otro soporte con el fin de poseerlos, mientras que por "utilizar" se refiere a "hacer uso de los datos, emplearlos o aprovecharse de los mismos, lo que no comporta necesariamente su aprehensión física".

Asimismo, el artículo 197 también hace referencia a los "datos reservados de carácter personal", cuya interpretación debe realizarse conforme a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que los define como cualquier información sobre una persona física que pueda ser identificada e identificable.

En base a lo anterior, puede afirmarse que los *deepfakes* encajan en el tipo previsto en el art. 197.2 CP. Esto se debe a que constituyen datos reservados de carácter personal, al referirse a información sobre una persona física "identificada e identificable", y además, este material suele encontrarse registrado en soportes informáticos o en archivos, tanto públicos como privados. Así, se reúnen las dos

[42] La LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, fue modificada por la actual LOPDPGDD (3/2018, de 5 de diciembre.

condiciones necesarias para que este tipo de conductas puedan ser penalmente relevantes.

En segundo lugar, en el apartado tercero se sanciona la conducta consistente en difundir, revelar o ceder a terceros los datos, hechos o imágenes obtenidas de forma ilícita, aunque además castiga a quien realice dicha conducta sin conocimiento de su origen ilícito y sin haber sido parte en su descubrimiento.

El primer párrafo de este apartado, como señala JORGE BARREIRO, recoge el tipo agravado de «revelación», lo que implica una mayor gravedad en el ataque hacia la intimidad de la persona, en cuanto lleva consigo la difusión, revelación o cesión de los datos, hechos descubiertos o imágenes captadas[43]. Esto resulta especialmente relevante, ya que, como se ha indicado, el bien jurídico protegido en este delito es la intimidad, y, en este contexto, lo verdaderamente grave no es tanto el descubrimiento de los "secretos", sino su revelación, especialmente cuando se lleva a cabo mediante su difusión, ya que tiene un mayor impacto sobre la víctima.

Además, conviene señalar que, conforme el artículo 7.5 de la LO de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, se consideran "intromisiones ilegítimas" en el ámbito de protección al honor, la intimidad y la propia imagen, "*la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos [...]*". Esta previsión refuerza la idea de que la difusión de imágenes sin el consentimiento del titular, como sucede en la mayoría de casos de *deepfakes* sexuales, puede suponer una vulneración directa hacia la intimidad personal.

Por último, en el apartado 5 del artículo 197 se agravan las penas previstas en los apartados anteriores en los casos en que los datos descubiertos tengan carácter especialmente sensible, de modo que "*revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o persona*

[43] Barreiro, J. (2016, 25 de agosto). *El delito de descubrimiento y revelación de secretos en el Código Penal de 1995. Un análisis del artículo 197 del CP*. Revista Jurídica Universidad Autónoma De Madrid, (6). Pág. 31. https://revistas.uam.es/revistajuridica/article/view/6240.

*con discapacidad necesitada de especial protección*". Tal y como indica JORGE BARREIRO, este precepto exige la previa comisión de alguna de las conductas descritas en los apartados anteriores y que dichas conductas afecten a lo que se conoce como el "núcleo duro" de la intimidad: ideología, religión, salud o vida sexual, ámbitos especialmente protegidos tanto por la Constitución como por el Derecho Internacional y la legislación en materia de protección de datos (LOPD). Asimismo, se extiende esta protección a los casos en los que la víctima sea menor de edad o persona con discapacidad necesitada de especial protección. Por tanto, si como consecuencia de la realización de alguna de las conductas previstas en los apartados 1 a 4 se revelara este tipo de información personal, estaríamos ante un supuesto encuadrable en este tipo agravado, al entenderse que se vulnera gravemente la intimidad personal, bien jurídico que debe preservarse en todo caso.

A la luz de lo analizado hasta ahora, podría deducirse que la creación de *deepfakes* y su posterior difusión es una conducta plenamente punible a través de los preceptos analizados del artículo 197 CP, ya que implican un apoderamiento o utilización de datos reservados de carácter personal que, en la mayoría de casos, se encuentran registrados en soportes informáticos o archivos, y cuya divulgación supone una intromisión en la intimidad del sujeto afectado. Además, este mismo precepto contempla expresamente como conducta delictiva la difusión de dicha información, lo que refuerza la posibilidad de encuadrar estas prácticas en su ámbito de aplicación.

No obstante, también existen posturas contrarias a estas ideas. Así, JAREÑO LEAL sostiene que en un *deepfake* sexual la persona afectada no puede reconocer como suyo el cuerpo al que se ha adherido su rostro, siendo precisamente el primero el que constituye en estos casos el recipiente de la imagen íntima protegida en el Código Penal, por lo que el hecho de que dicho cuerpo no se corresponda con la identidad real es lo que también impide hablar de vulneración

de la intimidad[44]. Sin embargo, la autora explica que "es indudable que el mero hecho de utilizar, manipular y difundir el rostro de una persona sin su consentimiento vulnera, como mínimo, la facultad de disposición de su imagen, aunque tal conducta no reúne los parámetros necesarios para entrar en el tipo penal señalado; aunque sí para merecer la protección civil que ofrece la Ley 1/1982 (art. 7.5)".

Aún así, también existen diversas investigaciones que sugieren que la intimidad podría verse afectada en el ámbito de la inteligencia artificial, como en el estudio "*Deepfake*"[45] realizado en 2025 por la empresa de software iProov, la cual registró que únicamente el 0.1% de los participantes[46] fueron capaces de identificar correctamente todos los contenidos reales y manipulados (tanto imágenes como vídeos). Además, más del 60% de los encuestados confiaban en sus capacidades de detección de *deepfakes*, lo que demuestra un peligroso exceso de confianza.

La investigación "*Unmasking Illusions: Understanding Human Perception of Audiovisual Deepfakes*"[47] realizada por Hashmi et al. (2024), también reveló que los participantes acertaron solamente en el 65,64% de los casos al enfrentarse a *deepfakes* audiovisuales. A su vez se observó que, incluso cuando percibían que un vídeo era falso, tenían dificultades para identificar con precisión en qué consistía la manipulación. Estos hechos demuestran que el nivel de confianza declarado por los participantes era superior a su verdadera capacidad de detección.

---

[44] Jareño Leal, Á. (2024). *El derecho a la imagen íntima y el Código penal La calificación de los casos de elaboración y difusión del deepfake sexual*. Revista electrónica de ciencia penal y criminología, 26(1). Págs. 15 y ss.

[45] iProov. (2023, 26 de agosto). *Estadísticas y soluciones sobre deepfakes; Cómo protegerse de los deepfakes.* https://www.iproov.com/es/blog/deepfakes-statistics-solutions-biometric-protection.

[46] iProov encuestó a 2.000 consumidores de Reino Unido y Estados Unidos, exponiéndolos a una serie de contenidos reales y *deepfakes*.

[47] Hashmi, A., Shahzad, S. A., Lin, C. W., Tsao, Y., & Wang, H. M. (2024). *Unmasking illusions: Understanding human perception of audiovisual deepfakes*. Recuperado a partir de https://arxiv.org/pdf/2405.04097

Por último, el estudio llevado a cabo por Klaire Somoray y Dan J. Miller[48] mostró que la precisión media en la categorización de los *deepfakes* fue del 60,7%, y que las distintas estrategias de detección empleadas no influyeron ni en la eficacia ni en la confianza de los participantes.

Estas investigaciones han demostrado que la impresión de quien recibe este tipo de imágenes es que son reales, lo que lleva a asociar a la persona representada en el *deepfake* con un desnudo real. Esto se debe a que, aunque se trate de una simulación, la reacción de quienes lo visualizan es prácticamente la misma que tendrían ante una situación real, generando así un perjuicio que se asemeja mucho al causado por una intromisión directa en la intimidad.
Sin embargo, al tratarse de un contenido falso que genera un error en quien lo ve, el daño no sólo afecta a la imagen de la persona manipulada, sino también a su intimidad. Precisamente por parecer verídico, el impacto va más allá de una simple vulneración de imagen, por lo que puede sostenerse que los *deepfakes* sexuales tienen un carácter pluriofensivo, ya que lesionan tanto la imagen personal como la intimidad de la víctima.

Para poder abordar estos supuestos dentro del artículo 197 CP, sería necesaria una reformulación del mismo, ya que, aunque la conducta encaja en el tipo, el principal problema reside en la determinación del bien jurídico protegido; su inclusión o no depende en gran medida de la interpretación que se adopte.
Por lo tanto, si prescindimos de una interpretación estrictamente sistemática, puede entenderse que lo relevante es la percepción de quienes reciben el contenido, ya que creen estar ante una vulneración real de la intimidad de esa persona, aunque se trate de una simulación. Por ello, se puede considerar que, actualmente, los *deepfakes* se encuentran en una especie de "limbo" entre la protección de la intimidad y la de la propia imagen.

[48] Somoray, K., & Miller, D. J. (Agosto del 2023). *Providing detection strategies to improve human detection of deepfakes: An experimental study*. Computers in Human Behavior, *149*, 107917. Researchgate. https://www.researchgate.net/publication/373258736_Providing_detection_strategies_to_improve_human_detection_of_deepfakes_An_experimental_study

En definitiva, el hecho de que los *deepfakes* no encajaran inicialmente en un bien jurídico tradicional no implica que no pueden ser comprendidos bajo una nueva interpretación. Una nueva realidad social genera un nuevo contexto que exige respuestas jurídicas actualizadas, y es precisamente el Derecho el que debe adaptarse a la sociedad, no a la inversa.

### 3.2.4 Arts. 205 y ss. CP: Delitos contra el honor

Como hemos estado analizando en el apartado anterior, los *deepfakes* sexuales vulneran, sobre todo, el honor, derecho recogido en el Título XI del Código Penal, donde se recogen figuras como la injuria y la calumnia. En nuestro caso afecta mayoritariamente a la primera (art. 208 CP), que es definida como una acción o expresión que lesiona la dignidad de otra persona, de manera que menoscaba su fama o atenta contra su propia estimación, y que únicamente se perfeccionará cuando sea puesta en el tráfico jurídico, tal y como añade ZAMARRO BALLESTEROS[49].

El bien jurídico protegido es el honor, y en cuanto a su interpretación debemos atender a dos planteamientos[50]:

1) Clásico, en el que se vincula el honor a la buena fama, a la autoestima o a la propia estimación.
2) Actual, que vincula el honor a la definición que ofrece la Constitución (art. 18.1 CE), esto es, el honor, la intimidad personal y familiar y la propia imagen.

RODRÍGUEZ PUERTA añade que el honor, en cuanto al derecho constitucional, encuentra su fundamento en la dignidad humana y el libre desarrollo de la personalidad (art. 10.1 CE). Así, podría resumirse que el honor abarca la dignidad, la intimidad personal y la propia imagen, es decir, cómo se ve a una persona públicamente y cómo se valora su reputación, o como lo describe VIVES ANTÓN, "el juicio que la comunidad proyecta sobre el individuo".

[49] Zamarro Ballesteros, R. (19 de mayo de 2023). *Deepfakes: análisis de esta nueva tecnología*. SEPIN Editorial Jurídica. https://blog.sepin.es/deepfakes-analisis-nueva-tecnologia.

[50] Op. Cit. Pág 218.

Siguiendo la explicación de esta autora, la injuria cuenta con una conducta típica en la que los *deepfakes* sexuales podrían ser los protagonistas, y se trata de:

A) Emitir expresiones o realizar acciones que lesionen la dignidad humana, a través de:
    a) el menoscabo de la fama
    b) el atentado contra la propia estimación

Es importante destacar que al amparo del art. 208 CP, sólo constituyen delito de injurias aquellas que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves[51].
Asimismo, las injurias que consistan en la imputación de hechos tendrán la consideración de "grave" solamente cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad.

En el contexto de los *deepfakes* sexuales, es evidente que la realización de estas imágenes manipuladas supone un menoscabo significativo de la fama y de la reputación de la víctima. La manipulación, aunque sea artificial, es percibida como auténtica por gran parte de la sociedad, lo que provoca un desprestigio de su imagen pública y un daño a su dignidad, al asociar a la persona representada con un acto sexual que nunca ha ocurrido. Es más, lo que va en contra de la dignidad de la persona no es tanto la creación de un *deepfake* sino su posterior difusión[52], conducta también amparada en los arts. 209 y 211 CP. Esto es así ya que amplía de forma sustancial el daño causado, de manera que se pierde el control sobre su propagación y sobre la permanencia del material en Internet, prolongando el efecto lesivo sobre la víctima ya que trata de humillar y degradarla frente a terceros. Además, cabe destacar que en el artículo 211 se describe que la

[51] Y en todo caso se dejará en manos de la propia víctima, quien tendrá la facultad de interponer querella para penar la calumnia o la injuria, según lo establecido en el art. 215 CP.

[52] No podemos olvidar que el artículo 7.5 de la Ley 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen describe como "intromisión ilegítima" «*la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos [...]*», y que el TC ha considerado que la reproducción de una imagen de carácter neutro extraída de las RRSS, sin consentimiento del titular, ha sido declarada ilícita (STC 27/2020, de 24 de febrero).

publicidad de la calumnia y de la injuria se reputará hecha «*cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante*». El último medio podría amparar la publicidad realizada mediante Internet, ya sea redes sociales, plataformas de vídeo o cualquier otro canal digital que permita una difusión masiva.
Toda esta situación podría considerarse un atentado contra la dignidad humana, encajando así en la conducta descrita.

El tercer apartado del art. 208 CP añade la consideración de «grave» a las injurias que consistan en la imputación de hechos sólo cuando se lleven a cabo con conocimiento de su falsedad o desprecio hacia la verdad. En este sentido, el contenido *deepfake* que es creado y compartido posteriormente en redes sociales o plataformas de mensajería móvil, suele tener una apariencia real de la persona representada, de modo que, aunque no se trate de hechos verídicos, los efectos generados por la difusión de este contenido son equiparables a los que produciría la divulgación de una imagen sexual auténtica, reforzando la percepción de veracidad del contenido. Todo ello contribuye a considerar este tipo de injurias como graves, dado que tanto el creador como el difusor actúan con conocimiento de su falsedad. Así lo explica JAREÑO LEAL en la Revista Electrónica de Ciencia Penal y Criminología[53], donde describe que el hecho de que la imagen se elabore y se difunda con el simple ánimo de ridiculizar a la persona afectada o por mero divertimento o consumo de terceros, corrobora la presencia del elemento subjetivo del delito contra el honor, este es, el *animus injuriandi*, y es por ello que considera que se está ante un delito de injurias graves del art. 208 CP (y art. 209 CP cuando hay difusión).

Por otro lado, cabe señalar que el 13 de octubre de 2023 se publicó en el BOE la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la Inteligencia Artificial. Como indica su propio título, esta iniciativa busca abordar el uso de las técnicas de recreación de imágenes y voces humanas mediante IA, comúnmente conocidas como *deepfakes*. Este texto legislativo surge como respuesta al avance de las nuevas

[53] Página 16

tecnologías y a los desafíos legales que plantean, tal y como explican OYARZABAL y PÉREZ TEROL[54].

Sin embargo, la Proposición de Ley Orgánica no llegó a prosperar, ya que el 15 de marzo de 2024 se acordó su retirada. No obstante, resulta relevante destacar el valor de esta iniciativa como un primer intento de adaptar el marco jurídico a los desafíos que plantea la IA, así como la posibilidad de que en un futuro se retome esta línea normativa. De todos modos, es conveniente citar algunas de las modificaciones que pretendían dar forma a una nueva regulación sobre IA.

En primer lugar, en la Exposición de Motivos se destaca que estas tecnologías "*difuminan la barrera entre lo que es verdadero y lo que es falso; entre lo que son acciones realmente realizadas por una persona y lo que son simulaciones generadas por terceros de manera totalmente artificial*", y que "*el sistema normativo español carece de una regulación en lo que respecta a la forma de autorizar la difusión de las alteraciones de imágenes o voces y sobre la persecución de su utilización ilícita*".

En vista de lo anterior, la Proposición de LO buscaba dar respuesta a los nuevos conflictos derivados del uso de los *deepfakes*, proponiendo la actualización de varios preceptos normativos, entre los que se encuentran la Ley 13/2022 General de Comunicación Audiovisual, la LO 1/1982, la Ley de Enjuiciamiento Civil y el Código Penal. En lo que aquí nos concierne, se propuso la incorporación de un nuevo artículo en el CP, el 208 bis[55], cuya redacción sería la siguiente:

*"Artículo 208 bis.*

> *Igualmente tendrá la consideración de injuria la acción que, sin autorización y con ánimo de menoscabar el honor, fama, dignidad o la*

[54] Oyarzabal, N; Pérez Terol, R. (2023, 18 de octubre). *Deepfake vs. Derecho al honor, intimidad y propia imagen*. CUATRECASES. https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/deepfake-derecho-honor-intimidad-propia-imagen.

[55] Congreso de los Diputados. *Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial*. (2023, 13 de octubre). Presentada por el Grupo Parlamentario Plurinacional SUMAR. https://www.congreso.es/public_oficiales/L15/CONG/BOCG/B/BOCG-15-B-23-1.PDF

*propia estimación de una persona, recrease mediante sistemas automatizados, software, algoritmos o inteligencia artificial para la pública difusión su imagen corporal o audio de voz."*

De la misma manera se planteó añadir en el art. 211 del mismo texto un nuevo párrafo, que quedaría redactado de la siguiente forma:

*"Artículo 211.*

*La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.*
*Salvo previa autorización expresa de la persona o personas afectadas, las simulaciones de imágenes, vídeos o audios de voz de estas generados a través de sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial que fueran difundidos a través de redes sociales serán consideradas como injurias hechas con publicidad."*

Aunque la Proposición de LO no llegara a aprobarse, ha abierto la puerta a que pueda volver a retomarse en el futuro, dada la necesidad de un marco normativo que contemple el nuevo contexto social derivado del uso de la inteligencia artificial.

Así pues, en vista de lo anterior cabe afirmar que los *deepfakes* sexuales también constituyen una nueva forma de lesionar el honor, y es por ello que también debería tenerse en cuenta su capacidad lesiva hacia la dignidad de la persona.

Por último, conviene destacar la relevancia del conflicto entre el derecho al honor y los derechos fundamentales a la libertad de expresión y de información, recogidos en el artículo 20 de la Constitución Española, siguiendo el análisis de RODRÍGUEZ PUERTA. En determinados casos, la conducta típica del delito de injurias puede quedar amparada por la aplicación del art. 20.7 CP, que contempla el ejercicio legítimo de un derecho como causa de justificación.

La autora explica que, para poder aplicar esta eximente deben cumplirse dos requisitos:

1) Si se trata de ideas, opiniones o juicios de valor, no deben utilizarse insultos para expresar dicho pensamiento, tal y como establecen las SSTC 101/2003, de 2 de junio y 39/2005, de 28 de febrero.

2) Si se trata de informaciones sobre hechos que puedan tener relevancia pública, estas deben ser veraces, y si no lo fueran, debe haberse actuado con la debida diligencia en su verificación y haber contrastado la información antes de su difusión, conforme a lo indicado en la STC 21/2000, de 31 de enero.

### 3.2.5 Artículo 172 ter 5: Delito de coacciones

La última conducta que podría llevarse a cabo mediante el uso de *deepfakes* sexuales es la recogida en el apartado 5 del artículo 172 ter del Código Penal, que se refiere a quien, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios, crear perfiles falsos en redes sociales o en cualquier otro medio de difusión pública, generando con ello una situación de acoso, hostigamiento o humillación.

Partiendo de esta descripción, es importante analizar los elementos clave que configuran este delito. En primer lugar, el bien jurídico protegido es la libertad de las personas, concretamente su libertad de obrar, entendida como la capacidad de decidir libremente sobre sus propias acciones y no ser privado de ellas (es decir, coaccionado).

En segundo lugar, es esencial que la conducta descrita se realice sin el consentimiento del titular de la imagen, es decir, si la persona en cuestión prestara su consentimiento de manera consciente, el tipo penal dejaría de aplicarse. Aquí cobra especial relevancia la STC 27/2020, de 24 de febrero, ya citada anteriormente, que establece que el titular del derecho fundamental debe autorizar de forma expresa cada acto concreto de utilización de su imagen. Además, subraya que la mera reproducción sin consentimiento ya es considerada ilícita, pues sólo el titular tiene la facultad de decidir quién puede usar su imagen y de qué forma. Es importante destacar que el precepto se refiere en todo momento a "la imagen de una persona", y aunque en el caso de los *deepfakes* sexuales no

estemos ante imágenes auténticas, sí prestan una apariencia realista y una gran verosimilitud con la persona representada, lo que conlleva una misma lesividad.

En tercer lugar, este delito se caracteriza porque debe causar a la víctima una situación de acoso, hostigamiento o humillación. Este último término, tal y como señala JAREÑO LEAL, está relacionado con otro bien jurídico distinto, como es el honor, mientras que las demás consecuencias sí que afectan directamente a la libertad. En todo caso, la conducta debe consistir en la utilización de la imagen del titular con el fin de crear perfiles falsos en redes sociales *"o en cualquier otro medio de difusión pública"*[56], lo que incluye no solo estas plataformas, sino también páginas web, foros o aplicaciones de mensajería móvil.

La misma autora añade que, dado que la imagen de una persona puede comprender desde una parte de su cuerpo, como el rostro o hasta la figura corporal completa, las imágenes generadas con IA podrían encajar dentro del tipo penal, siempre que partamos de la premisa de que el bien jurídico protegido en este delito es la libertad de obrar, y no la imagen íntima como tal. Esta interpretación, que personalmente comparto, se justifica en el hecho de que el legislador ha incluido esta figura entre los delitos contra la libertad, centrando su atención en el aspecto coactivo de la conducta del autor, quien obliga al sujeto pasivo a soportar múltiples intentos de contacto. Así, podrá usarse tanto una imagen real como un *deepfake* como instrumento para lograr el propósito final, que no es otro que crear las situaciones que describe el precepto.

#### 3.2.6 Análisis del acoso sexual (art. 184 CP): exclusión de los *deepfakes*

Tras el análisis de los delitos en los que no hay duda de que puedan cometerse mediante *deepfakes* sexuales, seguidamente se explicará de manera breve el delito de acoso sexual, en el que no está clara su aplicación mediante esta nueva tecnología.

[56] Art. 172 ter 5 CP

En primer lugar, el delito de acoso sexual, que tiene por objeto la protección de la libertad sexual de la persona, cuenta con 3 características fundamentales que son acumulativas entre ellas:

1) *"Solicitar favores de naturaleza sexual, para sí o para un tercero"*. Es decir, esta conducta ha de pretender la solicitud y la obtención de este tipo de favores de naturaleza sexual, con lo cual dicha acción consiste en pedir y obtener.

2) Esta conducta solamente debe manifestarse *"en el ámbito de una relación laboral, docente, de prestación de servicios o análoga"*, pero además impone una temporalidad determinada, ya que debe ser *"continuada o habitual"*, es decir, no basta con que se realice una vez. Este artículo acota los entornos en los cuales se puede manifestar el comportamiento, con lo cual, si no se está dentro de ninguno de ellos, no podrá ser punible.

3) Por último, este comportamiento debe provocar a la víctima *"una situación objetiva, y gravemente intimidatoria, hostil o humillante"*.

A diferencia de los *deepfakes*, que pueden ser creados y difundidos sin que el agresor tenga interacción ninguna con la víctima, este tipo penal requiere tradicionalmente una acción directa hacia la víctima. Esta diferencia plantea ya, de entrada, una dificultad relevante a la hora de integrar esta nueva tipología delictiva en las categorías tradicionales, pues el elemento clave del acoso sexual es la "solicitud de favores de naturaleza sexual". Es decir, se exige una conducta concreta en la que el autor pida y obtenga dichos favores, con el objetivo de obtener un beneficio de carácter sexual.
La dificultad radica, precisamente, en cómo puede llegarse a realizar esta solicitud a través del uso de los *deepfakes*.

Si bien es cierto que el uso de este tipo de contenidos puede generar en la víctima una situación «objetiva y gravemente intimidatoria, hostil o humillante», tal y como describe el artículo 184 CP, esto no resulta suficiente para que se configure el tipo penal.

Para comprender el alcance de estas consecuencias, nos acogemos a la definición que proporciona la RAE: lo "intimidatorio" es entendido como la causación de miedo o temor hacia la víctima; lo "hostil" hace referencia a que se debe provocar una situación enemiga u opuesta hacia la víctima, de modo que le provoque un ambiente desfavorable o adverso; y lo "humillante" implica una situación de menoscabo de la dignidad personal.

Aunque los *deepfakes* sexuales pueden fácilmente provocar estas situaciones en la víctima, de manera que se cumplan con dos de los tres elementos mencionados, el elemento esencial –la solicitud de favores sexuales– no puede materializarse en estos casos, pues el contenido en sí no constituye una petición, sino una representación artificial usada como instrumento.

Por todo ello, se concluye que el delito de acoso sexual presenta grandes dificultades para ser cometido a través del uso de los *deepfakes*, ya que, tras analizar los elementos típicos del precepto, no se cumple con el requisito principal, esto es, la solicitud directa de favores de naturaleza sexual.

## 4. Capítulo III: Responsabilidad penal y la IA

### 4.1 Problemas de imputabilidad: ¿Puede una IA ser sujeto de derecho penal?

Una vez analizados los delitos que podrían cometerse mediante el uso de *deepfakes* sexuales, también es necesario abordar la regulación de la responsabilidad penal derivada de dichos actos. En particular, trataremos de determinar sobre quién recae dicha responsabilidad en los casos en los que la Inteligencia Artificial ha intervenido en la comisión del delito, y, además, cómo se plantea todo ello cuando los sujetos activos son menores o personas jurídicas.

Para empezar a determinar si una inteligencia artificial puede ser penalmente responsable, primero debemos considerar que el Derecho Penal se rige por el principio de culpabilidad (*nullum crimen sine culpa*), que implica que no habrá responsabilidad penal sin dolo o imprudencia (art. 5 CP). Así lo expone SÁNCHEZ DAFAUCE[57], quien considera que la culpabilidad es el factor que, añadido al injusto, permite la aparición de la pena.

Sin embargo, como para la atribución de responsabilidad penal por dolo es necesaria la conciencia de los elementos del tipo así como la voluntad, una inteligencia artificial, por sí sola, no podrá ser penalmente responsable, pues no es capaz de formar su propia voluntad al no tener libertad de decisión.

BAGNAT argumenta que el principio de culpabilidad "presupone lógicamente la libertad de decisión del hombre, pues sólo si existe básicamente la capacidad de actuar de otra forma podrá hacerse responsable al autor de haber llegado al hecho antijurídico en lugar de dominar los impulsos criminales"[58]. Es decir, sólo puede ser penalmente responsable quien actúa con conciencia y voluntad, y como una IA

[57] Sánchez Dafauce, M. (2018). *Elementos de la culpabilidad penal*. Biblioteca Jurídica BOE. Pág 2. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-2018-10021300237.

[58] Bagnat, M. (2020). *El principio de culpabilidad en el Derecho Penal y los límites en el poder punitivo estatal*. Revista Pensamiento Penal, 4. https://www.pensamientopenal.com.ar/system/files/2021/03/doctrina88940.pdf.

no tiene capacidad para decidir libremente, de momento no puede considerarse culpable jurídicamente.

No obstante, dado el creciente número de delitos cometidos mediante inteligencia artificial y la actual ausencia de una regulación penal específica para ello, se plantea la necesidad de regular dichos comportamientos y así someterlos a los juicios de tipicidad correspondientes, de modo que se responda adecuadamente al principio de legalidad.

Así pues, cada vez son más los autores que plantean posibles vías para determinar una reforma de la responsabilidad penal que incluya a la IA en el debate jurídico. Un ejemplo de ello es ROMEO CASABONA, quien expone dos sistemas de determinación de la responsabilidad criminal[59]. El primero de ellos es considerar que el sistema inteligente autónomo es responsable por los crímenes cometidos por sus actos. Ello implica una dificultad, porque como ya se ha dicho, una IA no puede tener intención ni voluntad sin emanar de un humano previamente, por lo que se debe dejar en el aire sobre si, en un futuro, la máquina podría tener la misma intención como la tiene una persona. Si esto fuera una realidad, el autor concluye que habría la necesidad de modificar el actual sistema de responsabilidad penal para adaptarlo a los entes autónomos, con un alto precio para el sistema penal que tenemos en la actualidad.

El segundo método que ROMEO CASABONA propone es una responsabilidad penal centrada en la imprudencia por actos inintencionales u omisivos derivados de un diseño defectuoso del mismo[60]. Esta forma es confusa, ya que una IA no es capaz de entender autónomamente qué es una "obligación de cuidado", porque no tiene la misma capacidad de valorar las normas como un humano. Es por ello que ésta no puede valorar si está actuando conforme una norma, lo cual es necesario para poder aplicar la responsabilidad penal por imprudencia. De la misma manera, en este contexto es igualmente difícil determinar quién asume la responsabilidad por la comisión de delitos negligentes causados por errores en la programación de

[59] Romeo Casabona, C. M. (2020). *Criminal responsibility of robots and autonomous artificial intelligent systems?*. ULP Law Review. REVISTA DE DIREITO DA ULP.

[60] ROMEO CASABONA, 2020, p. 172.

un sistema de IA y cómo se aborda todo ello. Un ejemplo de ello podría ser el vehículo autónomo que atropella a un peatón al no haber interpretado correctamente la presencia de dicha persona en un paso de cebra. Este gran error puede deberse a una mala programación del código o simplemente que el modelo predictivo no esté bien entrenado en días de niebla. En este supuesto, ¿quién respondería penalmente; el diseñador del software o la empresa que fabricó el coche? Muchos autores sostienen que deberían aquellos que tengan la obligación de supervisar y actualizar los sistemas de IA las personas que podrían enfrentarse a la responsabilidad penal por dichos actos delictivos, aunque no hay nada fijado por el momento.

De todos modos, GIANNINI y KWIK[61] explican que atribuir la culpa es realmente difícil, puesto que ni el diseñador ni el operador pueden predecir cómo reaccionará una IA, ya que ésta aprende de la experiencia y actúa en función de su entorno.

Por último, cabe mencionar otro sistema, centrado en la responsabilidad penal de quien comete un delito utilizando la inteligencia artificial como instrumento o medio para ello. En este sentido, resultan especialmente relevantes los artículos 27 y 28 del Código Penal, que atribuyen responsabilidad criminal a quien realiza el hecho por sí solo, conjuntamente o por medio de otro del que se sirve. Así, el usuario que crea un *deepfake* de una persona menor de edad y que posteriormente lo difunde, o el informático que ha desarrollado la herramienta para ello, deben ser considerados autores mediatos del delito. En este último caso, aunque el informático no lleve a cabo directamente la acción delictiva, mantiene el dominio sobre el instrumento que ha creado –el sistema generador de *deepfakes*–, sabiendo de manera consciente que puede ser utilizado por terceros incluso con imágenes de menores, lo cual se correspondería con el delito de pornografía infantil. Es por ello que nos encontramos ante una nueva modalidad de delincuencia, en la que se cometen delitos ya previstos en el CP pero usando sistemas de inteligencia artificial como medio para cometerlos. En este sentido, CABRALES ACOSTA

[61] Giannini, A.; Kwik, J. (2023, 12 de enero). *Negligence Failures and Negligence Fixes. A Comparative Analysis of Criminal Regulation of AI and Autonomous Vehicles*. Springer Nature Link. Crim Law Forum 34, 43–85. https://doi.org/10.1007/s10609-023-09451-1.

señala que, ante el auge de esta tecnología, la IA puede convertirse en un instrumento idóneo para la comisión de estos delitos mediante la producción o facilitación a terceros de herramientas o claves de acceso a sistemas[62].
De este modo, para atribuir responsabilidad penal a quien haya programado una IA deliberadamente para cometer un delito, resulta esencial demostrar su dolo e intencionalidad de dirigir la conducta de la IA hacia la realización del hecho delictivo, o, al menos probar que dicho delito –como la creación de un *deepfake* sexual– se ha ejecutado utilizando un programa de IA.

Este es precisamente el supuesto que aquí nos ocupa, ya que los *deepfakes* sexuales son, básicamente, un instrumento para cometer un delito, y no pueden generarse ni difundirse por sí solos.

### 4.2 La responsabilidad penal de las personas físicas por los delitos cometidos mediante *deepfakes* sexuales

Siguiendo con lo anterior, debemos atender a las conductas presuntamente delictivas realizadas por personas físicas, con el fin de clasificar la posible responsabilidad penal en función del grado de participación de cada una.

En este sentido, hay 2 figuras especialmente relevantes en cuanto a los delitos cometidos mediante *deepfakes*: (I) la persona que crea el contenido *deepfake* sexual, y (II) quien lo difunde a sabiendas de su falsedad, que nada impide que sean la misma persona. Estas figuras son esenciales, sin perjuicio de otras aplicables según su grado de intervención, como el cooperador necesario o el encubridor, que deberán atender a las mismas reglas que en un delito tradicional.

En primer lugar, debemos considerar que actualmente no existe una regulación específica para sancionar a quienes crean y difunden un contenido *deepfake* sexual, aunque con los medios existentes se propone una posible vía de responsabilidad. Es decir, teniendo en cuenta que para atribuir responsabilidad penal en Derecho Penal es necesario analizar si la conducta es típica, antijurídica,

[62] Cabrales Acosta, J.M. (2024, 26 de marzo). *La inteligencia artificial y la nueva delincuencia*. Lefebvre. ELDERECHO. https://elderecho.com/la-inteligencia-artificial-y-la-nueva-delincuencia.

culpable y punible, debe considerarse que quien realmente está detrás del delito es una persona (física o jurídica) y no una inteligencia artificial, lo cual permite atribuirle su correspondiente culpabilidad[63]. Así, la persona dispone de los elementos necesarios para ser penalmente responsable: la culpa (ya sea dolo o imprudencia) y la imputabilidad, entendida como la capacidad para comprender que ha realizado un acto ilícito susceptible de generar consecuencias jurídicas. Por el contrario, si quien estuviera detrás del hecho delictivo fuera únicamente una máquina y no hubiera intervención humana, no sería posible atribuirle responsabilidad penal, ya que no contaría con los elementos necesarios para ello.

En cuanto a la primera figura (I), JAREÑO LEAL defiende que la intención de quien crea un *deepfake* sexual es la de humillar o ridiculizar a la víctima del contenido falso, incluso de deshonrarla, afectando principalmente a su honor, aunque también vulnerando el derecho fundamental a la propia imagen. Para la elaboración de este tipo de contenido, sin embargo, no se exige una pericia o habilidad específica en inteligencia artificial, ya que actualmente existen aplicaciones de uso público y gratuito (open source) que permiten generarlos fácilmente. Así, en realidad, cualquiera puede generar un *deepfake* sexual.
Ahora bien, para poder atribuir responsabilidad por dicha conducta, es necesario que el sujeto activo sea consciente del carácter ilícito de su conducta, esto es, debe saber que está manipulando imágenes de una persona para crear contenido de naturaleza sexual sin su consentimiento. No obstante, en el caso de los menores –que analizaremos más adelante–, no siempre existe una intención directa de lesionar bienes jurídicos, pues estos en muchas ocasiones actúan por diversión o por el deseo de ser aceptados socialmente.

Por otro lado, la persona que difunde el contenido *deepfake* sexual –en muchos casos la misma que lo ha creado–, también pretende humillar a la víctima, dejándola en una posición vulnerable y degradante, atentando contra su dignidad personal. De hecho, el verdadero impacto lesivo es la propia difusión del

[63] Asimismo lo explica FERNÁNDEZ CARRASQUILLA en "Culpabilidad y libertad de voluntad" (Pág. 13), quien considera que "*para ser responsable por culpabilidad, a tono con la teoría normativa, se requiere que el sujeto sea imputable, actúe con dolo o imprudencia y posea en el momento libertad de decisión al estar ausentes en su actuar circunstancias legales de exclusión de la imputabilidad y de la culpabilidad*".

*deepfake*[64], pues a pesar de que el sujeto activo sea plenamente consciente de su falsedad, aún así decide compartirlo, evidenciando así su desprecio y malicia hacia la propia víctima.

De este modo, tanto en la creación como en la difusión del *deepfake* sexual se manifiesta la presencia de dolo y una clara intencionalidad dirigida a causar un daño específico en la esfera personal e íntima de la víctima, lo cual constituye la base para atribuir responsabilidad criminal al culpable.

Por ello, independientemente del bien jurídico protegido, si del análisis del Capítulo II (*véase supra*) se concluye que los hechos pueden ser constitutivos de un delito de pornografía infantil (p.e.), deberán ser considerados autores tanto quienes hayan creado como quienes hayan difundido el *deepfake* sexual, siempre que existan pruebas suficientes que lo acrediten.

Asimismo lo expone ZAMARRO BALLESTEROS[65], quien afirma que como la inteligencia artificial no es un sujeto de derecho, ni se le reconoce, de momento, personalidad jurídica, la responsabilidad penal por las infracciones cometidas utilizándola se imputaría a las personas físicas que utilizaran esta tecnología, o que la programaran para delinquir.

En este sentido, la responsabilidad penal debe equipararse a la que correspondería por la comisión del delito en su modalidad tradicional, pues esa es precisamente la dirección que ha tomado el Gobierno[66], ya que pretende abordar los nuevos desafíos tecnológicos equiparando las conductas realizadas mediante inteligencia artificial a las ya tipificadas en el Código Penal.

---

[64] Es posible solicitar su retirada a la Agencia Española de Protección de Datos, recabando todas las pruebas posibles y denunciarlo ante la Policía.

[65] Zamarro Ballesteros, R. (10 de octubre de 2023). *Culpable, la IA*. Abogacía Española. Consejo General. https://www.abogacia.es/actualidad/opinion-y-analisis/culpable-la-ia/.

[66] Consejo de Ministros. (2025, 25 de marzo). *El Gobierno refuerza la protección de los menores en los entornos digitales.* La Moncloa. https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/250325-rueda-de-prensa-ministros.aspx.

### 4.2.1 Especial consideración a menores

La manera en cómo crecen los menores hoy en día ha cambiado drásticamente con la llegada de Internet, y no es difícil observar que tienen acceso a la tecnología y a las redes sociales cada vez más pronto. La amplia accesibilidad que estos disponen de los medios telemáticos implica que pueden usar la tecnología en cualquier momento y de cualquier forma. Esto supone que, por ejemplo, pueden generar imágenes falsas mediante inteligencia artificial –pues como ya se ha señalado son aplicaciones abiertas al público y fácilmente accesibles– sin tener en cuenta sus consecuencias, tal y como ha pasado en una multitud de ocasiones. De la misma manera lo dispone Graciela Padilla[67], directora de Investigaciones Feministas en la Universidad Complutense, que establece que "*estas tecnologías son demasiado accesibles y su gratuidad y su accesibilidad, por desgracia, son parte de su naturaleza*".

En el caso de que un menor cometa un delito mediante *deepfakes* sexuales deberá atenderse a la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores (LORPM), aplicable a las personas mayores de catorce años y menores de dieciocho, tal y como lo dispone su artículo primero. De este modo, las personas menores de catorce años son inimputables penalmente[68], así que no se les exigirá ningún tipo de responsabilidad vinculada a la LORPM, sino que, tal y como establece el art. 3 de dicho texto "*se aplicará lo dispuesto en las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes*". Así, estas personas deberán ser valoradas conforme a su situación personal, de manera que se tomen las medidas de protección adecuadas conforme a la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

---

[67] Ocaña, J. (2023, 21 de septiembre). *El caso de Almendralejo: ¿Por qué los menores crean contenidos falsos de carácter sexual con la IA?*. Efeverifica. https://verifica.efe.com/almendralejo-inteligencia-artiificial-machismo-menores.

[68] BLANCO BAREA explica en su artículo "*Responsabilidad penal del menor: principios y medidas judiciales aplicables en el derecho penal español*" de la Revista de Estudios Jurídicos que "*el legislador entiende que los menores de catorce años carecen de discernimiento suficiente como para asumir ante el Estado una responsabilidad de índole penal por la comisión de sus actos.*"

Como el objetivo primordial de la responsabilidad penal de los menores no es el castigo de estos sino su reeducación, resocialización y prevención de futuras conductas delictivas, protegiendo así el interés superior del menor, no se les imponen penas, sino medidas de seguridad, reguladas en el artículo 7 y ss. del Código Penal. Estas medidas pueden consistir en el internamiento (cerrado, semiabierto o abierto) en un centro, la asistencia a centros de día, la libertad vigilada o la realización de tareas socioeducativas, de modo que se les prohíbe la aplicación de las penas privativas de libertad aplicables a las personas mayores de edad.

Centrando el análisis en un suceso concreto, tomaremos como referencia el caso "Almendralejo" u (*véase supra*), en el que el Juzgado de Menores de Badajoz declaró responsables a 15 menores de edad por una veintena de delitos de pornografía infantil y otros veinte contra la integridad moral[69], imponiéndoles la medida de libertad vigilada durante un año así como formaciones afectivo-sexuales. Como ya se ha señalado, la mayor accesibilidad a las tecnologías así como la falta de educación digital y emocional de los menores pudo propiciar este hecho delictivo especialmente grave, en el que un grupo de menores crearon imágenes falsas de sus compañeras de clase usando inteligencia artificial, haciéndolas aparecer desnudas, y difundieron este contenido por el colegio así como por grupos de mensajería móvil.

Este caso constata que cualquier persona, incluso un menor, puede ser autor de la creación y difusión de *deepfakes* sexuales. No obstante, en los menores no tiende a existir un ánimo sexual directo ni una intención de lesionar bienes jurídicos fundamentales, sino que suelen actuar impulsados por su entorno, desconociendo el daño causado y las consecuencias jurídicas que conllevan, ya que lo ven como un juego pero no son conscientes ni de las consecuencias graves que puede tener ni que ello puede constituir un delito.

De todas formas, supone una gran dificultad valorar si un menor es consciente plenamente del daño causado así como de la ilicitud de la conducta, pues aún se encuentran en fase de desarrollo, aunque esto puede depender de la madurez

[69] Op. Cit.

personal de cada uno. En este sentido, NAVARRO OLIVAS alerta de que un mal uso de la inteligencia artificial abre nuevas vías al acoso escolar[70], lo que refuerza la necesidad de abordar el problema no solo jurídicamente sino también a través de la educación.

En definitiva, la implicación de menores en la creación y la difusión de *deepfakes* sexuales plantea diversos retos jurídicos en cuanto a su regulación, la cual también exige una respuesta adecuada. Si bien es cierto que el ordenamiento jurídico español ofrece mecanismos de responsabilidad penal a los menores de entre catorce y dieciocho años conforme a criterios reeducativos y preventivos, con la llegada de la IA los usos que derivan de ella se hacen cada vez más alarmantes, por lo que se insiste en una educación digital hacia los menores en edades tempranas para evitar futuras conductas delictivas y así respetar los derechos fundamentales de los demás.

### 4.3 Personas jurídicas: Análisis del artículo 31 bis del Código Penal

Las personas jurídicas también han experimentado la llegada de la inteligencia artificial como algo novedoso, útil y transformador. Sin embargo, algunas empresas han aprovechado el potencial de esta tecnología para llevar a cabo conductas delictivas mediante su uso, dada la gran facilidad con la que puede emplearse. La ausencia de regulación penal específica frente a este tipo de delitos exige una respuesta adecuada y eficiente para determinar la responsabilidad penal de las personas jurídicas en el contexto de la inteligencia artificial.

Con la llegada de la LO 5/2010, de 22 de junio, "*se introdujo en nuestro ordenamiento jurídico la responsabilidad penal de las personas jurídicas, dada la incesante necesidad de dar una respuesta más eficaz al avance de la criminalidad empresarial*", declara la Circular 1/2016, de 22 de enero, de la FGE[71]. Asimismo, XAVIER JANUÁRIO explica que antes de dejar atrás el dogma *societas*

[70] Op. Cit.

[71] Madrigal Martínez-Pereda, C. (2016, 22 de enero). *Circular 1/2016, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por la Ley Orgánica 1/2015*. Fiscalía General del Estado. https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2016-00001.pdf.

*delinquere non potest*, y así establecer los primeros modelos de responsabilidad penal de las personas jurídicas (RPPJ), muchos países entendían que "la persona jurídica sería incapaz de existir, actuar y expresar una voluntad independiente de los individuos que la componen, por lo que su responsabilidad autónoma sería inadecuada[72]".

Por ello, el artículo 31 bis del Código Penal rompió con todos los esquemas frente a la imposibilidad de que una persona jurídica no pudiera tener responsabilidad penal. Lo que dispone este precepto es, principalmente, que las personas jurídicas responderán penalmente:

a) cuando hayan cometido un delito en nombre o por cuenta de ésta, y en su beneficio, por personas que tienen el poder de organización, dirección o de control de la misma.
b) cuando hayan cometido delitos, en el ejercicio de actividades sociales y por cuenta y en beneficio de las mismas, por haberse incumplido gravemente los deberes de supervisión, vigilancia y control de su actividad[73].

En cualquier caso, se establecieron también una serie de eximentes de responsabilidad penal para las personas jurídicas cuando estas hayan implantado eficazmente modelos de organización y gestión orientados a la prevención del delito (programas de *Compliance*), siempre que se cumplan ciertos requisitos y condiciones. Esto evidencia que ante la irrupción de las nuevas tecnologías y los riesgos delictivos que conllevan, ya se exige a las personas jurídicas la adopción de parámetros de cumplimiento normativo y la realización de revisiones periódicas sobre su situación interna.

En lo que respecta a los *deepfakes* sexuales, si bien es cierto que las empresas no suelen ser las creadoras directas de este tipo de contenido, sí pueden desarrollar

[72] Xavier Januário, T. F. (2023). *Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales*. Estudios Penales Y Criminológicos, 44 (Ext.), 1-39. Pág. 12. https://doi.org/10.15304/epc.44.8902.

[73] Artículo 31.1 bis CP.

softwares cuya finalidad inicial sea legítima, pero que acabe siendo desviado para la creación de *deepfakes* sexuales[74]. Aún así, no puede descartarse la posibilidad de que existan empresas cuyo modelo de negocio se base en el desarrollo de herramientas destinadas específicamente a la generación de *deepfakes* sexuales[75], lo que supondría un supuesto mucho más grave. Por este motivo, resulta especialmente importante ejercer una debida diligencia en las actividades desarrolladas dentro de la empresa, así como la implantación de programas de *Compliance* adecuados que contribuyan a controlar las medidas exigidas y asegurar su cumplimiento.

En esta línea, y ante el aumento de sistemas automatizados susceptibles de ser aplicados por las empresas, el Parlamento Europeo aprobó el 16 de febrero de 2017 una Resolución sobre normas de derecho civil de la robótica[76]. En su apartado 59 f), se instó a la Comisión Europea a que, al elaborar su futuro instrumento legislativo, "*explore, analice y considere las implicaciones de todas las posibles soluciones jurídicas*", entre ellas, la creación de una personalidad jurídica específica para los robots. Esta propuesta pretende reconocer una "*e-personalidad*" o "personalidad electrónica" para los robots, lo que permitiría dotar a estos sistemas de una responsabilidad propia, especialmente diseñada para reparar los posibles daños que estos puedan causar de manera autónoma. Sin embargo, como de momento no hay regulación específica al respecto, ZAMARRO BALLESTEROS piensa que quizá la mejor solución es considerar a la IA como una persona jurídica[77], aplicando la doctrina de las STS 514/2015, de

[74] Si *ChatGPT* no se hubiera programado adecuadamente y dejara a los usuarios la libertad para crear imágenes racistas, homófobas y sexuales (*deepfakes*), la responsabilidad penal si se cometiera un ilícito también recaería sobre la empresa OpenAI.

[75] Aunque no se trate específicamente de *deepfakes* sexuales, la empresa londinense "Synthesia" se dedica a la IA generativa, de modo que ofrece a sus clientes una variedad de creaciones *deepfake* con la que pueden realizar imágenes y vídeos hiperrealistas. Osornio, A. (2023, 9 de agosto). *Synthesia, la empresa de IA que vende deepfakes*. Wired UK. https://es.wired.com/articulos/synthesia-empresa-de-ia-que-vende-deepfakes.

[76] Parlamento Europeo. (2017, 16 de febrero). *Normas de Derecho civil sobre robótica. Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017IP0051&from=EN.

[77] Op. Cit.

2 de septiembre, y 234/2019, de 8 de mayo, las cuales establecen que para atribuir responsabilidad penal a una empresa:

a) Es exigible un juicio de culpabilidad específico sobre la actuación de la persona jurídica, basado en el principio de autorresponsabilidad;
b) El fundamento de la responsabilidad penal no es objetiva, sino que ha de tener su soporte en la propia conducta de la persona jurídica;
c) El principio de presunción de inocencia se aplica a la persona jurídica y es autónomo respecto del de la persona física;
d) La persona jurídica actúa sin disponer un sistema de control de sus administradores y empleados dirigidos a controlar la observancia de la norma, del ordenamiento jurídico o no controla las fuentes de peligro de la actividad a la que se dedica.

También conviene destacar que, de entre los delitos analizados en el Capítulo II, muchas veces es el propio Código Penal el que prevé un tratamiento particular para el delito concreto cuando se comete en el seno de una persona jurídica, como es el caso del delito de pornografía infantil (art. 186 CP), en el que la regulación correspondiente para las personas jurídicas está prevista en el artículo 189 ter, la cual dispone una responsabilidad particular para estos sujetos, consistente en multas sobre el beneficio obtenido, así como la posible disolución de la persona jurídica en cuestión.

Es por ello que, si dichos ilícitos penales pueden ser ejecutados mediante IA, y teniendo en cuenta que sigue pendiente la aprobación definitiva para incorporar una regulación específica para los *deepfakes* en el texto penal, resulta evidente que la atribución de responsabilidad penal a las empresas debe estar igualmente contemplada, y más aún si consideramos que este tipo de conductas pueden ser llevadas a cabo por cualquier sujeto, ya sea persona física o jurídica, siempre y cuando tenga a su disposición la tecnología necesaria para ello.

## 5. Conclusiones

A lo largo del presente trabajo se ha expuesto la evolución de la Inteligencia Artificial, así como los usos legítimos e ilegítimos que ésta puede presentar, centrándonos especialmente en los *deepfakes* y su repercusión jurídica. Este fenómeno, que consiste en la manipulación de imágenes y vídeos reales mediante herramientas de IA con el objetivo de hacer creer a los usuarios que ese contenido es real, puede ser usado para fines lícitos como el cine, la publicidad o la música, pero también puede utilizarse con finalidades lesivas para la dignidad, la intimidad o el honor de las personas. En este sentido, como los sistemas de IA aplicados a la comisión de delitos representan una evolución de la ciberdelincuencia tradicional, se plantean retos jurídicos en su tratamiento actual así como en su futura regulación.

En particular, se han analizado sobre todo las tipologías delictivas que podrían derivarse de los *deepfakes* sexuales; es decir, cuando a partir de un contenido manipulado se hace creer que una persona aparece desnuda y posteriormente esa imagen se difunde, ¿Qué delitos pueden ser aplicables en este caso? ¿Sobre quién recae la responsabilidad penal?

Del análisis efectuado se desprende que, actualmente, nuestro ordenamiento jurídico no recoge expresamente esta conducta como un tipo penal autónomo, lo que genera una sensación de desprotección a las víctimas. Sin embargo, no estamos muy lejos de una regulación específica para los *deepfakes*, ya que en Marzo de 2025 el Gobierno aprobó tipificar como delito los *deepfakes* de contenido sexual y el grooming[78].

Asimismo se ha analizado cómo este contenido puede ser constitutivo de una variedad de delitos regulados en el Código Penal, pues afecta a una multitud de bienes jurídicos distintos, entre ellos, la libertad sexual, la intimidad, la propia imagen y el honor.

[78] Op. Cit.

En primer lugar, se ha llegado a la conclusión de que el contenido *deepfake* de carácter sexual puede ser constitutivo del delito de exhibicionismo y provocación sexual contemplado en el art. 186 de Código Penal, pues se trata de vender, difundir o exhibir material pornográfico entre menores de edad o personas con discapacidad necesitadas de especial protección. En este sentido, dado que el precepto no establece una definición limitada de lo que debe entenderse por «material pornográfico», y considerando que los *deepfakes* sexuales reproducen de forma explícita actos de índole sexual simulando ser reales, estos podrían estar subsumidos en este tipo penal.

En segundo lugar, también se ha concluido que dicho contenido puede encajar en el delito previsto en el art. 189 CP, relativo a la explotación sexual y a la corrupción de menores. El propio precepto contempla expresamente tanto el material pornográfico real como el simulado, lo que permite incluir la denominada «pornografía virtual». Este aspecto resulta clave para considerar también el contenido *deepfake* sexual como pornografía infantil, ya que el material generado mediante inteligencia artificial puede representar escenas de carácter sexual sin que estas hayan ocurrido realmente. De hecho, es el propio Gobierno quien, al querer una tipificación específica para los *deepfakes* de carácter sexual, pretende que estos sean tratados como formas de pornografía infantil.

En tercer lugar, los *deepfakes* sexuales también podrían encuadrarse en el delito de descubrimiento y revelación de secretos, regulado en los arts. 197 a 201 CP. Esto se debe a que la conducta típica sancionable consiste en apoderarse o utilizar, sin consentimiento, datos reservados de carácter personal, que normalmente suelen estar registrados en soportes informáticos. De este modo, el contenido *deepfake* sexual podría considerarse como "datos reservados", al tratarse de información que afecta directamente a la intimidad personal de una persona física "identificada e identificable". Además, el propio precepto contempla expresamente la sanción de su posterior difusión, lo que refuerza el carácter intrusivo de la conducta al constituir una grave intromisión hacia la intimidad de la víctima.

De lo anterior también se ha concluido que a pesar del daño psicológico hacia la

víctima que produce la creación del *deepfake* sexual, lo que es verdaderamente perjudicial es su posterior difusión, ya que se expone al mundo exterior una realidad falsa con la intención de avergonzarla y humillarla ante una multitud de personas que han visualizado el contenido.

Los delitos contra el honor, previstos en los arts. 205 y ss CP, también podrían abarcar los daños causados por el contenido *deepfake* sexual, ya que constituyen una injuria hacia la víctima, al tratarse de acciones o expresiones que lesionan su dignidad personal, menoscabando su fama o atentando contra su propia estimación. Así, sólo podrán sancionarse aquellas conductas realizadas con conocimiento de su falsedad o con temerario desprecio hacia la verdad. De esta manera, al tratarse de un contenido falso manipulado mediante IA, pese a no ser reales, pueden provocar un daño equiparable al de una imagen auténtica de contenido sexual, provocando un gran desprestigio hacia la dignidad e imagen pública de la persona afectada.

Por último, y en lo que respecta a la tipificación de los *deepfakes* sexuales, también se ha concluido que estos podrían estar comprendidos en el delito previsto en el artículo 172 ter .5 CP, ya que la conducta típica consiste en utilizar la imagen de una persona, sin su consentimiento, para realizar anuncios o crear perfiles en cualquier medio de difusión pública, generando una situación de acoso, hostigamiento o humillación. En este caso, aunque los *deepfakes* sexuales no constituyan una imagen auténtica, sí prestan una apariencia realista, por lo que esta tipología delictiva también debería contemplarse, al cumplirse con todos los elementos del tipo penal, tal y como se ha analizado previamente.

Asimismo, se ha abordado la responsabilidad penal de los distintos sujetos que pueden intervenir en este tipo de conductas, desde las personas físicas –incluyendo la regulación de los menores de edad– hasta las personas jurídicas. De esta manera, se ha concluido que, si bien una inteligencia artificial no puede ser considerada penalmente responsable ya que no tiene capacidad de decisión sobre sus actos ni voluntad propia, sí deben responder penalmente tanto aquellas personas que hayan creado el *deepfake* sexual así como quienes lo hayan difundido. Esto es así porque sólo las personas físicas pueden reunir los elementos

exigidos para ser penalmente responsables, esto son, la culpabilidad y la imputabilidad.

El caso de Almendralejo ha servido como ejemplo de cómo incluso menores de edad pueden convertirse en los autores de este tipo de conductas, muchas veces por diversión y por desconocimiento de su alcance. De este modo, el Juzgado de Menores de Badajoz declaró responsables a 15 menores de edad por una veintena de delitos de pornografía infantil y otros veinte contra la integridad moral.
Este supuesto, que sirve de precedente para conductas similares, demuestra que el legislador está empezando a reaccionar ante estos nuevos delitos, y aunque es evidente la urgencia de una reforma legislativa que reconozca expresamente los *deepfakes* sexuales como una modalidad delictiva autónoma, no queda mucho para que veamos una respuesta efectiva que proteja a las víctimas y ofrezca seguridad jurídica frente a estas nuevas formas de delincuencia digital.

## 6. Bibliografía


Álvarez, N. (2024, 26 de diciembre). *Responsabilidad penal de la IA: ¿Quién comete realmente el delito?*. ECIJA. https://ecija.com/sala-de-prensa/responsabilidad-penal-de-la-ia-quien-comete-realmente-el-delito/. Fecha de consulta 6 de mayo de 2025.

Bagnat, M. (2020). *El principio de culpabilidad en el Derecho Penal y los límites en el poder punitivo estatal*. Revista Pensamiento Penal, 4. https://www.pensamientopenal.com.ar/system/files/2021/03/doctrina88940.pdf. Fecha de consulta 6 de mayo de 2025.

Barba Arteaga, C. (2024). *Deepfakes Sexuales: impacto, prevención y perspectivas de género en el entorno digital.* Miguel Hernández Communication Journal, 15, 229-244. https://doi.org/10.21134/zt4eht31. Fecha de consulta 22 de febrero de 2025.

Barreiro, J. (2002). *El delito de descubrimiento y revelación de secretos en el Código Penal de 1995. Un análisis del artículo 197 del CP*. Revista Jurídica Universidad Autónoma De Madrid, (6). https://revistas.uam.es/revistajuridica/article/view/6240. Fecha de consulta 6 de mayo de 2025.

Bigas Formatjé, N. (2023, 11 febrero). *'Deepfakes' pornográficos: Cuando la IA desnuda tu intimidad y vulnera tus derechos*. UOC. https://www.uoc.edu/es/news/2023/265-deepfakes-pornograficos-cuando-IA-desnuda-tu-intimidad-vulnera-tus-derechos. Fecha de consulta 18 de febrero de 2025.

Blanco Barea, J. Á. (2008). *Responsabilidad penal del menor: principios y medidas judiciales aplicables en el derecho penal español*. Revista Estudios Jurídicos. Segunda Época, (8). https://revistaselectronicas.ujaen.es/index.php/rej/article/view/9. Fecha de consulta 6 de mayo de 2025.

Cabrales Acosta, J.M. (2024, 26 de marzo). *La inteligencia artificial y la nueva delincuencia*. Lefebvre. ELDERECHO. https://elderecho.com/la-inteligencia-artificial-y-la-nueva-delincuencia. Fecha de consulta 6 de mayo de 2025.

Citron, D. (2014). Notes. In *Hate Crimes in Cyberspace* (pp. 257-328). Cambridge, MA and London, England: Harvard University Press. https://doi.org/10.4159/harvard.9780674735613.c13. Fecha de consulta 18 de febrero de 2025.

Chesney, B; Citron, D. (Diciembre del 2019). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* — California Law Review. California Law Review. https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security. Fecha de consulta 18 de febrero de 2025.

Cuatrecasas Monforte, C. (2023). *LA INTELIGENCIA ARTIFICIAL Y LA INVESTIGACIÓN DE DELITOS*. Logos Guardia Civil, Revista Científica Del Centro Universitario De La Guardia Civil, (1), 61–84. Recuperado a partir de https://revistacugc.es/article/view/5912. Fecha de consulta 19 de febrero de 2025.

Fernández Carrasquilla, J. (2013). *Culpabilidad y libertad de voluntad*. Anuario De Derecho Penal Y Ciencias Penales, 66(1), 89–157. https://revistas.mjusticia.gob.es/index.php/ADPCP/article/view/1179. Fecha de consulta 6 de mayo de 2025.

Fernández Sánchez, D. (2024, 22 de mayo). *¿Qué es un deepfake y qué consecuencias legales tiene?*. Pactio Legal. https://www.pactiolegal.es/derecho-penal/que-es-un-deepfake-y-que-consecuencias-legales-tiene/. Fecha de consulta 6 de mayo de 2025.

Flynn, A., Powell, A., Scott, A., Cama, E. (2021, 3 de diciembre). *Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse*. The British Journal of Criminology, Volume 62, Issue 6, November 2022, Pages 1341–1358, https://doi.org/10.1093/bjc/azab111. Fecha de consulta 15 de marzo de 2025.

Giannini, A.; Kwik, J. (2023, 12 de enero). *Negligence Failures and Negligence Fixes. A Comparative Analysis of Criminal Regulation of AI and Autonomous Vehicles*. Springer Nature Link. Crim Law Forum 34, 43–85. https://doi.org/10.1007/s10609-023-09451-1. Fecha de consulta 6 de mayo de 2025.

Gómez Tomillo, M. (2010). *Comentarios al Código Penal*. Valladolid. Lex Nova. Página 740. Fecha de consulta 15 de marzo de 2025.

González Pulido, I. (2023). *El uso de la inteligencia artificial generativa en la investigación de la ciberdelincuencia de género: ante el auge de los deepfakes*. IUS ET SCIENTIA, 9(2), 157-180. https://doi.org/10.12795/IESTSCIENTIA.2023.i02.08. Fecha de consulta 19 de febrero de 2025.

Hashmi, A., Shahzad, S. A., Lin, C. W., Tsao, Y., & Wang, H. M. (2024). *Unmasking illusions: Understanding human perception of audiovisual deepfakes*.

Recuperado a partir de https://arxiv.org/pdf/2405.04097. Fecha de consulta 14 de abril de 2025.

Herrera De Las Heras, R. (2022). *Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil.* Fecha de consulta 19 de febrero de 2025.

Jacobsen, B. N., & Simpson, J. (2023). *The tensions of deepfakes.* Information, Communication & Society, *27*(6), 1095–1109. https://doi.org/10.1080/1369118X.2023.2234980. Fecha de consulta 15 de marzo de 2025.

Jareño Leal, Á. (2024). *El derecho a la imagen íntima y el Código penal La calificación de los casos de elaboración y difusión del deepfake sexual*. Revista electrónica de ciencia penal y criminología, 26(1). Fecha de consulta 22 de febrero de 2025.

Jarvis Cooper, L. (2023, 17 de abril). *Sexual Privacy and Persecution*. UCLA Law Review. SSRN. https://www.uclalawreview.org/sexual-privacy-and-persecution/. Fecha de consulta 6 de mayo de 2025.

Laffier, J.; Rehman, A. (2023, 24 de junio). *Deepfakes and Harm to Women*. https://doi.org/10.51357/jdll.v3i1.218. Fecha de consulta 4 de febrero de 2025.

Madrigal Martínez-Pereda, C. (2015, 19 de junio). *Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015.* Fiscalía General del Estado. https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2015-00002.pdf. Fecha de consulta 14 de abril de 2025.

Madrigal Martínez-Pereda, C. (2016, 22 de enero). *Circular 1/2016, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por la Ley Orgánica 1/2015.* Fiscalía General del Estado. https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2016-00001.pdf. Fecha de consulta 14 de abril de 2025.

Meskys, E., Kalpokiene, J., Jurcys, P., Liaudanskas, A. (2019, 2 de diciembre). *Regulating Deep Fakes: Legal and Ethical Consideration*. Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020, Pages 24–31., Available at SSRN: https://ssrn.com/abstract=3497144. Fecha de consulta 18 de febrero de 2025.

Miró Llinares, F. (2020). *INTELIGENCIA ARTIFICIAL Y JUSTICIA PENAL: MÁS ALLÁ DE LOS RESULTADOS LESIVOS CAUSADOS POR ROBOTS*. Revista de Derecho Penal y Criminología, (20), 87–130. https://doi.org/10.5944/rdpc.20.2018.26446. Fecha de consulta 19 de febrero de 2025.

Morón Lerma, E. (2003). *Derecho Penal y nuevas tecnologías: panorama actual y perspectivas futuras*. In Internet y pluralismo jurídico: formas emergentes de regulación (pp. 93-120). Comares. Fecha de consulta 24 de enero de 2025.

Ocaña, J. (2023, 21 de septiembre). *El caso de Almendralejo: ¿Por qué los menores crean contenidos falsos de carácter sexual con la IA?*. Efeverifica. https://verifica.efe.com/almendralejo-inteligencia-artiificial-machismo-menores. Fecha de consulta 6 de mayo de 2025.

Osornio, A. (2023, 9 de agosto). *Synthesia, la empresa de IA que vende deepfakes*. Wired UK. https://es.wired.com/articulos/synthesia-empresa-de-ia-que-vende-deepfakes.

Oyarzabal, N; Pérez Terol, R. (2023, 18 de octubre). *Deepfake vs. Derecho al honor, intimidad y propia imagen*. CUATRECASES. https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/deepfake-derecho-honor-intimidad-propia-imagen. Fecha de consulta 15 de abril de 2025.

Palomo, J. (2025, 26 de marzo). *El Gobierno cuela en su ley de protección de menores un nuevo delito para las falsificaciones «vejatorias» con IA*. Diario ABC. https://www.abc.es/tecnologia/gobierno-cuela-ley-proteccion-menores-nuevo-delito-20250325142844-nt.html?ref=https%3A%2F%2Fwww.google.com%2F. Fecha de consulta 15 de marzo de 2025.

Quintero Olivares, G. (2011). *Esquemas de la parte especial del derecho penal* (Vol. 32). Tirant lo Blanch. Fecha de consulta 15 de marzo de 2025.

Romeo Casabona, C. M. (2023). *La atribución de responsabilidad penal por los hechos cometidos por sistemas autónomos inteligentes, robótica y tecnologías conexas*. ULP Law Review. Fecha de consulta 6 de mayo de 2025.

Romeo Casabona, C. M. (2020). *Criminal responsibility of robots and autonomous artificial intelligent systems?*. ULP Law Review. REVISTA DE DIREITO DA ULP. Fecha de consulta 6 de mayo de 2025.

Rousay, V. (2023). *Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms*. Master's thesis, Harvard University Division of Continuing Education.

https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374909. Fecha de consulta 15 de marzo de 2025.

Sahuquillo, M. R. (2024, 5 de febrero). *Bruselas penalizará material generado por IA y las 'deepfake' sexuales de menores como pornografía infantil*. El País. https://elpais.com/sociedad/2024-02-05/bruselas-penalizara-material-generado-por-ai-y-las-deepfake-sexuales-de-menores-como-pornografia-infantil.html. Fecha de consulta 6 de mayo de 2025.

Sánchez Dafauce, M. (2018). *Elementos de la culpabilidad penal*. Biblioteca Jurídica BOE. Pág 2. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-2018-10021300237. Fecha de consulta 6 de mayo de 2025.

San Segundo Fernández, E. *Profundizando en los deepfakes:¿qué hace humana a una voz?*. Acción Cultural Española. Anuario AC/E 2024 de Cultura Digital, pp. 28-41.https://www.accioncultural.es/media/2024/Doc/Anuario24/2-Deepfakes-anuario-2024.pdf. Fecha de consulta 19 de febrero de 2025.

Simó Soler, E. (2023). *Retos jurídicos derivados de la Inteligencia Artificial Generativa. Deepfakes y violencia contra las mujeres como supuesto de hecho*. InDret 2.2023 ,pp. 493-515. Fecha de consulta 4 de febrero de 2025.

Somoray, K., & Miller, D. J. (Agosto del 2023). *Providing detection strategies to improve human detection of deepfakes: An experimental study*. Computers in Human Behavior, *149*, 107917. Researchgate. https://www.researchgate.net/publication/373258736_Providing_detection_strategies_to_improve_human_detection_of_deepfakes_An_experimental_study . Fecha de consulta 14 de abril de 2025.

Van der Nagel, E. (2020, 2 de junio). *Verifying images: deepfakes, control, and consent*. Porn Studies, 7(4), 424–429. https://doi.org/10.1080/23268743.2020.1741434. Fecha de consulta 6 de mayo de 2025.

Valls Prieto, J. (2022). *Sobre la responsabilidad penal por la utilización de sistemas inteligentes*. Revista electrónica de ciencia penal y criminología, 24. http://criminet.ugr.es/recpc/24/recpc24-27.pdf. Fecha de consulta 6 de mayo de 2025.

Vidal. G. (2024, 20 de junio). *Los delitos de exhibicionismo y provocación sexual en el Código Penal*. Gerson Vidal. https://www.gersonvidal.com/blog/delitos-exhibicionismo-provocacion-sexual/. Fecha de consulta 15 de marzo de 2025.

Vives Antón, T. S. (1999). Derecho penal : parte especial / T.S. Vives Antón ... [et al.] (3a ed., rev.actualizada). Tirant lo Blanch. Págs. 308-325. Fecha de consulta 6 de mayo de 2025.

Xavier Januário, T. F. (2023). *Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales*. Estudios Penales Y Criminológicos, 44 (Ext.), 1-39. Pág. 12. https://doi.org/10.15304/epc.44.8902. Fecha de consulta 6 de mayo de 2025.

Zamarro Ballesteros, R. (19 de mayo de 2023). *Deepfakes: análisis de esta nueva tecnología*. SEPIN Editorial Jurídica. https://blog.sepin.es/deepfakes-analisis-nueva-tecnologia. Fecha de consulta 15 de marzo de 2025.

Zamarro Ballesteros, R. (10 de octubre de 2023). *Culpable, la IA*. Abogacía Española. Consejo General. https://www.abogacia.es/actualidad/opinion-y-analisis/culpable-la-ia/. Fecha de consulta 19 de febrero de 2025.

Amnistía Internacional. *UE: La Ley de Inteligencia Artificial debe prohibir las tecnologías peligrosas basadas en la inteligencia artificial.* (s.f.). https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/ley-de-inteligencia-artificial-ue-prohibir-las-tecnologias-discriminatorias/. Fecha de consulta 4 de febrero de 2025.

BOE. *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial*. Reglamento de Inteligencia Artificial (s.f.). https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079. Fecha de consulta 31 de enero de 2025.

Código Penal Online. (s.f.). *Artículo 186 del Código Penal explicado* (2024). https://codigopenal.online/articulo-186/. Fecha de consulta 15 de marzo de 2025.

Comunicación Poder Judicial. (2024, 9 de julio). *Imponen la medida de libertad vigilada durante un año a los 15 menores acusados de manipular y difundir imágenes de menores desnudas en Badajoz*. Consejo General del Poder Judicial. Noticias Judiciales. https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/Imponen-la-medida-de-libertad-vigilada-durante-un-ano-a-los-15-menores-acusados-de-manipular-y-difundir-imagenes-de-menores-desnudas-en-Badajoz. Fecha de consulta 6 de mayo de 2025.

Congreso de los Diputados. *Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la*

*inteligencia artificial.* (2023, 13 de octubre). Presentada por el Grupo Parlamentario Plurinacional SUMAR. https://www.congreso.es/public_oficiales/L15/CONG/BOCG/B/BOCG-15-B-23-1.PDF. Fecha de consulta 15 de abril de 2025.

Consejo de Ministros. (2025, 25 de marzo). *El Gobierno refuerza la protección de los menores en los entornos digitales.* La Moncloa. https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/250325-rueda-de-prensa-ministros.aspx. Fecha de consulta 1 de mayo de 2025.

Fundéu RAE. *«Inteligencia Artificial» es la expresión del 2022 para la FundéuRAE*.(s.f.).https://www.fundeu.es/recomendacion/inteligencia-artificial-es-la-expresion-del-2022-para-la-fundeurae/. Fecha de consulta 4 de febrero de 2025.

Gobierno de España. (2023, 19 de abril). *Qué es la Inteligencia Artificial*. Plan de Recuperación, Transformación y Resiliencia. https://planderecuperacion.gob.es/noticias/que-es-inteligencia-artificial-ia-prtr. Fecha de consulta 4 de febrero de 2025.

Google Cloud. *¿Qué es la inteligencia artificial o IA?*. (s. f.). https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419. Fecha de consulta 4 de febrero de 2025.

INCIBE. *Deepfakes*. (s.f.). https://www.incibe.es/aprendeciberseguridad/deepfakes. Fecha de consulta 4 de febrero de 2025.

iProov. (2023, 26 de agosto). *Estadísticas y soluciones sobre deepfakes; Cómo protegerse de los deepfakes.* https://www.iproov.com/es/blog/deepfakes-statistics-solutions-biometric-protection. Fecha de consulta 6 de mayo de 2025.

LISA Institute. (s.f). *Deepfakes: Qué es, tipos, riesgos y amenazas*. https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas?srsltid=AfmBOopqC44BojB-gwW5xRfcSuUkulf1RgSQe-wYnFdfo_7pqWqFOz5H. Fecha de consulta 15 de marzo de 2025.

Maldita.es. (2023, 19 de septiembre). *Inteligencia artificial y pornografía infantil: cómo se está usando la IA para crear contenidos sexuales de menores y qué dice la ley*. Maldita Tecnología. https://maldita.es/malditatecnologia/20230919/pornografia-infantil-inteligencia-artificial/. Fecha de consulta 6 de mayo de 2025.

Parlamento Europeo. (2017, 16 de febrero). *Normas de Derecho civil sobre robótica. Resolución del Parlamento Europeo, de 16 de febrero de 2017, con*

*recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017IP0051&from=EN. Fecha de consulta 1 de mayo de 2025.

Parlamento Europeo. (2020, 8 de septiembre). *¿Qué es la inteligencia artificial y cómo se usa?*. https://www.europarl.europa.eu/topics/es/article/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa. Fecha de consulta 4 de febrero de 2025.

Security Hero. (2023). *2023 State of Deepfakes: Realities, Threats and Impact.* https://www.securityhero.io/state-of-deepfakes/. Fecha de consulta 22 de febrero de 2025.

Universidad de Alicante (s. f.). *Fake news y deep fakes*. https://moodle2024-25.ua.es/moodle/pluginfile.php/151851/mod_resource/content/23/deep_fakes.html. Fecha de consulta 18 de febrero de 2025.