DEEPFAKES PORNOGRÁFICOS: UN ANÁLISIS NORMATIVO, JURISPRUDENCIAL Y DE GÉNERO

TRABAJO DE FINAL DE GRADO

Doble Titulación en Administración y Dirección de Empresas y Derecho

Autora: Miriam Vera Carmona

Tutora: Carolina Fernández Blanco

Universidad de Girona. Facultad de Derecho.

Curso 2023/2024

Convocatoria: Mayo de 2024

ÍNDICE

INTRODUCCIÓN

Imagina que estás en tu casa, disfrutando de una noche tranquila después de un largo día de trabajo. De golpe, el sonido de tu teléfono interrumpe el silencio, avisándote de que has recibido un mensaje vía Whatsapp: se trata de un compañero de trabajo. Con curiosidad, abres el mensaje, esperando que se trate de algo relacionado con el proyecto en el que estáis trabajando. Sin embargo, lo que ves te deja helada: se trata de un enlace que te dirige a un vídeo en el que apareces tu, completamente desnuda y manteniendo relaciones sexuales. Te invade una sensación de pánico y confusión, sabes que el vídeo no es real, pero ¿cómo es posible que exista un vídeo tan convincente en el que apareces en una situación tan comprometedora cuando sabes que nunca ocurrió?

Aunque parezca extraída de una película de terror, la situación que se acaba de relatar expone la impactante realidad de los *deepfakes* pornográficos, una tecnología que ha desdibujado peligrosamente la línea entre aquello que es real y aquello que es falso en el mundo digital. Se trata de un fenómeno tecnológico que no solo afecta a grandes celebridades como Jennifer Lawrence, Rosalía o Taylor Swift, entre otras, que ya han sido víctimas de este tipo de creaciones, sino también a personas anónimas.

En este sentido, en septiembre de 2023 diversos medios de comunicación se hicieron eco del caso de las jóvenes de Almendralejo, que tuvo lugar en España. Concretamente, Elpais.com publicó el 18 de septiembre de 2023 una noticia titulada "Decenas de menores de Extremadura denuncian que circulan fotos de falsos desnudos suyos creadas por inteligencia artificial: "Me dio un vuelco el corazón""[1]. A una estudiante de derecho, joven, mujer y profundamente conmovida por los derechos de las mujeres, le resultan cuanto menos preocupantes este tipo de situaciones.

El carácter novedoso del fenómeno junto con el destacable auge de casos y el potencial dañino para los derechos fundamentales de las personas, sobretodo de las mujeres, justifica la necesidad de abordar esta temática y sirve de motivación a la presente investigación. De este modo, el presente trabajo surge del profundo interés por los derechos y libertades sexuales de las mujeres y de la preocupación por las nuevas amenazas derivadas de la innovación digital. Sin dejar de

[1] Viejo, M. (18 de septiembre de 2023). Decenas de menores de Exremadura denuncian que circulan fotos de falsos desnudos suyos creadas por inteligencia artificial: "Me dio un vuelco el corazón": La policía identifica a varios de los presuntos autores de los montajes fotográficos después de que varias familias de Almendralejo alertaran de que habían localizado imágenes en las que aparecían sus hijas adolescentes. *El país.*

https://elpais.com/espana/2023-09-18/la-policia-investiga-el-desnudo-integral-de-varias-menores-en-extremadura-con-inteligencia-artificial-me-dio-un-vuelco-el-corazon.html#

lado el papel que ocupa el género en este fenómeno, el presente trabajo consiste en un análisis del actual abordaje que, desde el derecho, se realiza en España en los casos de *deepfakes* no consentidos de carácter sexual.

Se pretende hallar respuestas a las siguientes preguntas: ¿Qué normativa regula actualmente este tipo de contenidos?, ¿Qué propuestas están actualmente en vía de aprobación para la regulación de los *deepfakes*?, ¿Qué dificultades presenta su regulación?, ¿Qué derechos se ven amenazados por este tipo de conductas?, ¿Quiénes son las principales víctimas de estas conductas?, ¿Cómo se abordaría un caso de *deepfake* actualmente en España?

Con tal finalidad, el presente trabajo se estructura en diferentes apartados fundamentales:

En el apartado 2 se lleva a cabo una indagación teórica que busca comprender la naturaleza o esencia de los *deepfakes*, explorando sus características, su origen y evolución.

Posteriormente, en el punto 3 se aborda de manera específica el análisis de los derechos fundamentales que se ven amenazados por esta tecnología.

Seguidamente, en el punto 4 se realiza un análisis detallado de la legislación actual a nivel estatal y europeo, explorando su aplicabilidad potencial en casos de *deepfakes.*

Tras esta revisión normativa, el punto 5 examina las iniciativas actuales que, a día de hoy, están siendo consideradas para hacer frente a la problemática de los *deepfakes.*

Además, el punto 6 de la presente investigación se destina específicamente a atender la importancia de abordar esta problemática desde una perspectiva de género, que ponga en el centro a las víctimas de este tipo de conductas.

Y, por último, en el punto 7 se realiza un análisis jurisprudencial con el propósito de examinar casos relevantes que podrían servir de referencia en el contexto de un posible litigio por *deepfake* en España.

1. MARCO TEÓRICO

El término anglosajón "*deepfake*"[2] se fundamenta etimológicamente en las palabras "*fake*" (o falso en español) y "*deep*" (o profundo), este último deriva del término "*deep learning*" o aprendizaje profundo, que es un método de inteligencia artificial que, a través de algoritmos, permite que un sistema aprenda o mejore de forma automática y autónoma. De este modo, el concepto "*deepfake*" es utilizado para referirse a vídeos, imágenes o incluso archivos de audio que, a pesar de no ser reales, aparentan serlo debido a una manipulación meticulosa.

Generalmente, por *deepfake* nos referimos a un vídeo en el que se muestran imágenes falsas, habitualmente del rostro de una persona, que parecen ser reales y que se han producido utilizando inteligencia artificial. Podría decirse que el *deepfake* se erige como una mentira audiovisual, que puede llegar a los extremos de recreación de lo real de forma que deviene prácticamente imposible para la percepción humana determinar si es veraz o falaz (Cerdán y Padilla, 2019)[3].

Como se ha dicho, este tipo de creaciones son fácilmente posibles gracias a la Inteligencia Artificial. Este tipo de tecnología moderna permite, a través de programas sencillos y gratuitos, que cualquier persona que disponga de un ordenador convencional o teléfono smartphone pueda realizar vídeos o imágenes falsas que parezcan reales.

El mejor ejemplo es el de usar la cara de un personaje famoso para colocarlo en el cuerpo de otra persona. Así ha ocurrido con numerosas celebridades internacionales como Scarlett Johansson, Jennifer Lawrence y Emma Stone, entre otras, cuyos rostros fueron utilizados para superponerlos en el cuerpo de actrices pornográficas para la creación de contenido pornográfico.

Como veremos a continuación, la creación de material pornográfico con el rostro de celebridades fue su uso original, pero los *deepfakes* pueden emplearse para muchos otros fines fraudulentos tales como la difusión de noticias falsas, estafas, coacciones o para generar contenido pornográfico. Aun así, el presente estudio se centrará específicamente en el uso del *deepfake* para la producción de material pornográfico y como método de perpetuación de violencia contra la mujer. Por tanto, de ahora en adelante, con el término *deepfake* nos referiremos exlusivamente a este contexto.

[2] "*Profundamente falso*" o "*Ultrafalso*" serían sus alternativas en español.

[3] Cerdán Martínez, V y Padilla Castillo., G. (2019). Historia del *fake* audiovisual: deepfake y la mujer en un imaginario falsificado y perverso. *Historia y comunicación social, vol.24* (2), 505-520. https://dx.doi.org/10.5209/hics.66293

De esta forma, incidiendo en su uso para la creación de material pornográfico, Douglas Harris (2019)[4] señala que actualmente es posible para cualquier persona con habilidades informáticas rudimentarias crear un *deepfake* pornográfico que retrate a un individuo participando en un acto sexual que en realidad nunca ocurrió. De hecho, insiste, si bien los *deepfakes* pornográficos se crearon inicialmente para producir vídeos de celebridades, ahora se generan para representar a otras personas sin su consentimiento, como una amiga o una compañera de clase.

1.1. ORIGEN Y EVOLUCIÓN DE LOS *DEEPFAKES*

¿Cúando y dónde surge el *deepfake*?, ¿Cómo se desarrolla y cómo evoluciona? Y lo más importante, ¿Para qué? ¿Cual es su finalidad principal? Las respuestas a todas estas cuestiones resultan necesarias para simplificar la comprensión del fenómeno de los *deepfakes* y es por ello que en el presente apartado nos detenemos brevemente en sus orígenes.

Antes de abordar el nacimiento del *deepfake*, resulta fundamental contextualizar previamente el papel elemental desempeñado por la inteligencia artificial. Así pues, la inteligencia artificial nace el año 1956 a raíz del Proyecto de investigación de verano sobre inteligencia artificial de la Universidad de Dartmouth, (*Dartmouth Summer Research Project on Artificial Intelligence*), convocado por John McCarthy en Hannover, Nueva Hampshire, Estados Unidos. El proyecto duró aproximadamente dos meses y se constituyó como el evento fundacional de la inteligencia artificial como campo.

No obstante, en aquel momento la idea de inteligencia artificial (de ahora en adelante, IA) estaba lejos de la idea concebida hoy en día. De hecho, no es hasta alrededor de los años 80 que el paradigma cambia y la IA empieza a trabajar con bases de datos "*Data Science*". Es a partir de este momento que empieza a hablarse de *deep learning*[5] y de la IA como la conocemos hoy en día (Gibert, 2022)[6].

---

[4] Douglas Harris, A. (2018). Deepfakes: False Pornography is here and the law cannot protect you. *Duke Law & Technology Review, vol.17* (1), 99-128.
https://scholarship.law.duke.edu/dltr/vol17/iss1/4

[5] El *deep learning* es un tipo de *machine learning* que permite que un sistema aprenda y mejore de forma autónoma mediante redes neuronales, sin tener que ser programado explícitamente, a través de la ingesta de grandes cantidades de datos.

[6] Gibert, K. (8 de junio de 2022). *Inteligencia artificial. Retos y oportunidades* [Ponencia]. Facultat de Lletres i de Turisme, UdG, Girona, España.

https://diobma.udg.edu/handle/10256.1/6773?show=full.

El avance de la IA ha propiciado una situación actual en la que esta tecnología se encuentra infiltrada en diversos aspectos de nuestra vida cotidiana. Ejemplos palpables de IA de nivel básico como la aspiradora autónoma Roomba (capaz de aprender el mapa de la casa en pocas horas y de diferenciar puertas y escaleras), los sistemas de posicionamiento global (GPS), y asistentes virtuales como Alexa, son omnipresentes en los hogares actuales, ilustrando así su penetración generalizada en la sociedad moderna. Incluso en plataformas como Amazon, Spotify, Netflix y Google, la IA se utiliza para crear perfiles de usuarios y descubrir qué les gusta y qué no les gusta a los consumidores.

Durante su intervención en las *Jornadas de SIG Libre*[7], Gibert (2022) señala que en los últimos años ha aparecido la cara más invasiva de la IA, adquiriendo el ámbito de la ética una creciente preocupación y relevancia.

Así pues, en este contexto de desarrollo y auge de las IA, Cole (2017) señala que el primer *deepfake* fue creado el año 2017 por el usuario de la plataforma Reddit autodenominado como "Deepfakes" (Citado por Cerdán y Padilla, 2019, p. 506). Este usuario seleccionó los rostros de las celebridades Gal Gadot, Maisie Williams y Taylor Swift para incluirlos en el cuerpo de varias actrices de cine para adultos. Para su realización, el usuario Deepfakes utilizó el ordenador de su casa y un algoritmo de *machine learning*[8], que cualquiera puede descargarse de Internet. El resultado fueron varios vídeos de carácter pornográfico que parecían interpretados por las famosas.

De este modo, fue en la plataforma Reddit donde los primeros *deepfakes* se popularizaron y propagaron. En solo dos meses, el usuario Deepfakes contaba con 15.000 suscriptores y fue esta comunidad la que extendió el uso del término *deepfake* (Cerdán y Padilla, 2019). Sin embargo, el contenido de estos vídeos no quedó limitado a esta plataforma, sinó que pronto se popularizó en los principales portales de contenido pornográfico como Pornhub.

[7] Las Jornadas de SIG Libre, Geotech & Spatial Data Science, son una iniciativa del SIGTE, un congreso dedicado al software libre en el campo de las Tecnologías de la Información Geográfica y la Ciencia de Datos Espaciales.
https://www.jornadassiglibre.org/

[8] El *machine learning* es un tipo de inteligencia artificial, una rama concreta de esta tecnología que, de alguna manera, ha aprendido a aprender, es capaz de absorber una gran cantidad de datos, encontrar patrones entre ellos y sacar conclusiones. Según Reyes Muñoz (2023), hay una diferencia clave entre los términos *machine learning* y *deep learning*:

> El *machine learning* aprovecha datos estructurados y etiquetados para hacer predicciones, mientras que los algoritmos de *deep learning* eliminan parte de estas necesidades de preprocesado, ya que pueden trabajar con datos no estructurados y extraer características de forma automatizada (Citado por Ruiz Guevara, 2023, p.7).

De nuevo cabe recalcar que los vídeos o imágenes *deepfake* no solamente afectan a grandes celebridades, sino que cualquier persona puede ser víctima de este tipo de creaciones, aunque mayoritariamente son mujeres. Concretamente, según datos extraídos del informe *The state of deepfakes*[9], en el año 2019 alrededor del 100% del contenido pornográfico *deepfake* estaba protagonizado por mujeres.

1.2. TECNOLOGÍAS Y MÉTODOS UTILIZADOS EN SU CREACIÓN

Tal y como se expone en el anterior apartado, la creación del primer *deepfake* de carácter pornográfico se considera realizada en el año 2017, tan solo un año después del surgimiento de las primeras técnicas de creación de este tipo de contenidos. De hecho, Alonso (2023)[10] señala que estas técnicas surgen en el año 2016 casi como un juego.

La rápidez en el desarrollo de estas tecnologías ha provocado que en la actualidad resulte muy facil suplantar a una persona tanto en la imagen como en la voz. Concretamente, actualmente destacan dos modelos de tecnología de creación de *deepfake*:

- ***Lip Sync***

  Hoy en día la IA permite imitar la voz de cualquier sujeto, de modo que crear un vídeo en el que alguien aparezca diciendo cosas que nunca ha dicho está relativamente al alcance de cualquiera.

  La posibilidad de clonar la voz y de recrear los labios a tiempo real de un sujeto para que el audio corresponda con los mismos, permite la creación de un vídeo en el que una persona diga lo que tu quieras que diga (Alonso, 2023).

[9] Ajder, H.,Patrini, G., Cavalli, F y Cullen, L. (2019). *The State of deepfakes: Landscape, threats, and impact.*
https://regmedia.co.uk/2019/10/08/deepfake_report.pdf

[10] Alonso, J.M. (28 de septiembre de 2023). *Ciberseguridad y Hacking en el mundo de Inteligencia Artificial, Robots y Humanos* [Ponencia magistral]. Larga vida al retail, XIX Congreso Español de Centros y Parques Comerciales, Madrid, España.
https://www.youtube.com/watch?v=gsnFXlLYt9w

Un ejemplo de ello es el vídeo [11] realizado por investigadores de la Universidad de Washington en el año 2017 en el que aparece el expresidente de Estados Unidos, Barack Obama, reproduciendo con su voz cosas que no ha dicho.

- ***Faceswapping***

La técnica del "*face swap*" aplicada en vídeos permite superponer la cara de un sujeto encima de la de otro sujeto. De esta forma, utilizando como base las expresiones del individuo original y super posicionando cada parte de ambos rostros, se logra que cada una de las expresiones se mantengan pero con el rostro de otra persona.

Dicho de otro modo, la aplicación de esta herramienta de inteligencia artificial permite intercambiar el rostro de alguien por el de otro sujeto. Hoy en día se parte de algoritmos preentrenados, de forma que construir una falsificación de un fotograma de una persona es, como ya se ha dicho, bastante sencillo.

Si bien es cierto que la aplicación de estas herramientas tiene numerosas ventajas, como por ejemplo en el ámbito cinematográfico, empresarial o incluso en la medicina, el fácil alcance y uso de las mismas por cualquier persona pone en evidencia el surgimiento de múltiples amenazas y peligros. De hecho, en los últimos años ha crecido de forma exponencial la preocupación por la parte ética de la IA, aunque Gibert (2022) destaca que esta preocupación no es intrínseca de la tecnología en si misma, sinó más bien intrínseca de los usos asociados a la misma.

Para ilustrar esta idea, resulta útil pensar en el ejemplo del cuchillo presentado por Joseph Raz[12]. El autor expone que el hecho de que un cuchillo filoso pueda ser usado para hacer daño no significa que ser filoso no sea una característica que haga buenos los cuchillos. Dicho de otro modo, es innegable que un cuchillo es, hoy en día y desde tiempos históricos, una herramienta valiosa e indispensable, actualmente nadie podría plantearse una civilización sin el uso cotidiano de cuchillos, aunque la misma herramienta también puede ser utilizada como un arma, siendo su uso en este último contexto claramente punible.

En definitiva, resulta urgente y necesario tomar conciencia de los peligros asociados al uso inadecuado de estas técnicas de creación digital, puesto que "si alguien puede ser cualquier persona, imagina qué puede pasar si un hombre mayor se mete en un grupo de niños y

[11] BBC News. (19 de julio de 2017). *Fake Obama created using AI video tool_BBC News*. [Vídeo]. https://www.youtube.com/watch?v=AmUC4m6w1wo

[12] Raz, J. (1983). *The Authority of law: essays on law and morality*. Oxford University Press., p. 281

pretende ser un niño o si alguien suplanta al CEO de una compañía [...] y solicita una transferencia". (Alonso, 2023, 8:45).

Aunque hoy en día ya existen detectores de *deepfakes* y la comunidad de expertos del sector sigue trabajando en el desarrollo de algoritmos y/o herramientas de IA capaces de detectar y desenmascarar vídeos falsos, la necesidad de definir un marco ético y legal con el propósito de regular los *deepfakes* resulta inminente.

2. IMPACTO EN LOS DERECHOS FUNDAMENTALES

El presente apartado tiene como objetivo hacer hincapié en la necesidad urgente de establecer un marco legal que establezca medidas para frenar el auge de este tipo de contenido. Tal necesidad se evidencia al analizar el impacto directo que el uso de la tecnología *deepfake* puede tener en los derechos fundamentales de sus víctimas. Recordemos que el presente trabajo se centra en la pornografia *deepfake* o en *deepfakes* de contenido sexual, motivo que nos lleva a remarcar que estos fotogramas pueden no solo utilizarse para la autogratificación de su creador, sino que también tienen potencial para extorsionar, humillar, acosar y chantajear a las víctimas (Harris, 2018)[13].

Ya se ha mencionado anteriormente el hecho de que las mujeres son las principales afectadas por este tipo de conductas, y aunque lo veremos con mayor detenimiento más adelante, no podemos obviar este hecho al analizar el impacto de los *deepfakes* en los derechos fundamentales debido al importante componente de género subyacente a estas conductas.

Tal y como observa Bello San Juan (2023)[14]:

La elaboración y distribución de contenido pornográfico falso protagonizado por mujeres supone un ataque directo a su integridad psíquica y autonomía, desautorizando a las mujeres y cuestionando, por tanto, su posición como sujeto de derechos tan relevantes como la dignidad o la propia imagen, prerrogativas reconocidas como Derechos Fundamentales en nuestra Constitución de 1978. (p.243)

[13] Douglas Harris, A. (2018). Deepfakes: False Pornography is here and the law cannot protect you. *Duke Law & Technology Review*, *vol.17* (1), 99-128. https://scholarship.law.duke.edu/dltr/vol17/iss1/4

[14] Bello San Juan, P. (2023). La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica. En COLEX (ed.), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI* (p.219-244). https://dialnet.unirioja.es/servlet/libro?codigo=924170

A nivel comunitario, el Consejo de la Unión Europea ha dejado constancia de los múltiples beneficios que las tecnologías digitales, en particular la IA, aportan al conjunto de la sociedad. Sin embargo, también ha reconocido el riesgo que conllevan las mismas para los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales y la consecuente necesidad de desplegar esfuerzos para velar por que quede garantizado el respeto a los mismos. Además, ha hecho hincapié en que el enfoque europeo de la transformación digital, y en particular de la IA, debe estar centrado en el ser humano y garantizar el pleno respeto y la promoción de los derechos fundamentales[15].

A continuación se hace un breve análisis de los principales derechos fundamentales que pueden resultar amenazados por los *deepfakes*.

2.1 DIGNIDAD Y DERECHO A LA INTEGRIDAD MORAL

Los conceptos de dignidad e integridad moral se encuentran tan íntimamente relacionados que en el presente apartado se ha optado por tratar ambos términos de forma conjunta. De este modo, se entiende por dignidad e integridad moral el derecho inherente de toda persona a ser tratada con respeto y dignidad, sin ser humillada o vejada e independientemente de las circunstancias o de las relaciones que tenga con otros sujetos. Puede ser considerada una más de las cualidades de la persona humana que le permiten tomar decisiones que afecten a su comportamiento y, en definitiva, influye en la conducta del individuo, así como en sus creencias y en su forma de interactuar con el entorno.

Así, la dignidad de la persona humana constituye la base misma de los derechos fundamentales. De hecho, la Declaración Universal de Derechos Humanos, 1948 (de ahora en adelante, DUDH)[16] consagra la dignidad humana en su preámbulo, estableciendo el reconocimiento de la misma y de los derechos iguales e inalienables como la base de la libertad, la justicia y la paz en el mundo. Además, en el artículo 1 se reconocen la dignidad y el deber de todos los seres humanos de comportarse fraternalmente los unos con los otros.

[15] Consejo de la Unión Europea. (2020). Conclusiones de la Presidencia sobre La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital (11481/20). https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf

[16] Asamblea General de la ONU. (1948). Declaración Universal de Derechos Humanos.

Por otro lado, a nivel europeo el Art.1 de la Carta de los Derechos Fundamentales de la Unión Europea, 2000 (de ahora en adelante, Carta o CDFUE)[17] establece la inviolabilidad de la dignidad humana, que debe ser respetada y protegida. De igual modo, la FRA[18] reconoce la dignidad de la persona humana no solo como un derecho fundamental, sino como la base de los derechos fundamentales, de lo que se deduce que ninguno de los derechos inscritos en la Carta podrá ser utilizado para atentar contra la dignidad de otras personas y que la misma forma parte de la esencia de los derechos inscritos.

A nivel estatal, la Constitución Española, 1978 (de ahora en adelante, CE)[19] reconoce en su artículo 10.1 la dignidad de la persona, junto a los derechos inviolables que le son inherentes, al libre desarrollo de la personalidad, y al respeto a la ley y a los derechos de los demás, como "fundamento del orden político y de la paz social".

Es evidente que los *deepfakes* en general, y los de contenido sexual en particular, constituyen una amenaza directa para la dignidad e integridad moral de sus víctimas, que pueden sufrir un daño real derivado de la creación de este tipo de contenido. De este modo, el bienestar, la reputación y la sensación de seguridad de la víctima puede quedar gravemente afectada, lo que supone una vulneración de su derecho a la integridad moral, reconocido a nivel estatal en el Art.15 de la CE, y a su vez regulado y protegido por el Art.3 CDFUE.

Concretamente, el Art.15 CE establece textualmente que: *"*Todos tienen derecho a la vida y a la integridad física y moral, sin que, en ningún caso, puedan ser sometidos a tortura ni a penas o tratos inhumanos o degradantes". Pues bien, parece evidente que este tipo de *deepfakes* pornográficos constituyen un trato degradante hacia la víctima o sujeto retratado, menoscabando su integridad moral y con enorme potencial de ocasionarle graves daños psicológicos.

Finalmente, cabe decir que estos riesgos ya han sido observados por la comunidad de expertos y por las instituciones, concretamente el Consejo de la Unión Europea ha reconocido *"*la protección y la promoción de los derechos fundamentales y la idea subyacente de dignidad humana como el eje vertebrador de un enfoque de la IA centrado en el ser humano*"*[20].

[17] Carta de los Derechos Fundamentales de la Unión Europea. Niza, 7 de diciembre del 2000. (BOE [en línea], núm.303, 14-12-2007, pp.1-16). <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2007-70004>.[Consulta: 1 de Marzo de 2024]
[18] European Union Agency For Fundamental Rights.
[19] España. Constitución Española. (BOE [en línea], núm. 311, 29-12-1978, pp. 29313-19424).<https://www.boe.es/eli/es/c/1978/12/27/(1)/con>. [Consulta: 1 de Marzo de 2024]
[20] Carta de los Derechos Fundamentales de la Unión Europea. Niza, 7 de diciembre del 2000. (BOE [en línea], núm.303, 14-12-2007, pp.1-16). <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2007-70004>.[Consulta: 3 de Marzo de 2024]

2.2 DERECHO AL HONOR, INTIMIDAD PERSONAL Y PROPIA IMAGEN

En España, los derechos fundamentales al honor, a la intimidad y a la propia imagen se encuentran reconocidos y regulados en el Art.18. CE y en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (a partir de ahora LO 1/1982). Así mismo, el Art. 12 DUDH dispone que:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Lo que supone un reconocimiento del derecho a la intimidad o vida privada y el derecho al honor o reputación.

La relevancia de estos derechos es tal que la CE los realza hasta el punto de reconocerlos como un límite al ejercicio del derecho a la libertad de expresión, derecho con el mismo carácter de fundamental y previsto en el Art. 20.1 CE. De este modo, la CE los consagra como límites a las diferentes libertades de expresión a través de su Art. 20.4, que dispone textualmente que: "Estas libertades tienen su límite [...], especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y la infancia".

En términos generales, el derecho al honor prohíbe que alguien pueda referirse a otra persona de forma insultante o injuriosa, o atentando contra su reputación, lo que postula directamente la creación y difusión de un *deepfake* personal de carácter pornográfico como una conducta lesiva para el honor del sujeto retratado en el correspondiente fotograma.

Sin embargo, cabe destacar que aunque el derecho al honor constituye un valor de gran alcance en nuestro ordenamiento, su concepto jurídico no está claramente definido. Tal y como señaló el TC en la STC 46/2002, de 25 de Febrero de 2002: "

> Es un concepto jurídico que, aunque expresa de modo inmediato la dignidad constitucional inherente a toda persona, depende, en parte, de las normas, valores e ideas sociales vigentes en cada momento, por lo que comporta un margen de imprecisión que ha de irse reduciendo por la concreción judicial" (FJ.4)[21] .

Por otro lado, junto al derecho a la intimidad personal previsto en la CE y en la DUDH hay que tener en cuenta el Art.8 CEDH y el Art. 7 CDFUE, que reconocen el derecho al respeto a la vida privada y familiar. Además, el derecho a la intimidad personal se encuentra fuertemente ligado al derecho a la protección de la propia imagen. No parece haber discusión en cuanto que la difusión

[21] Sentencia del Tribunal Constitucional 46/2002, de 25 de febrero de 2002.

no consentida de imágenes explícitas de un sujeto manteniendo relaciones sexuales en su esfera privada constituye un ataque directo a su intimidad personal, pero el principal problema que plantean los *deepfakes* en relación al derecho a la intimidad personal y propia imagen es que los hechos reproducidos en los mismos nunca fueron realizados por la víctima, lo que podría plantear dudas en cuanto a su capacidad de lesionar el derecho a la intimidad personal y propia imagen. De hecho, el creador ni siquiera necesita el material sexual de la víctima, sino que basta únicamente una imagen o vídeo del rostro que en la actualidad puede ser fácilmente extraído de una red social como Instagram, LinkedIn, Facebook o Twitter (Oliva, 2022)[22].

Pero aún así, en los *deepfakes* se utiliza el rostro de la víctima para superponerlo en el cuerpo de actrices de contenido para adultos, uso que debería considerarse suficiente para entenderse vulnerado el derecho al honor, la intimidad personal y propia imagen. Y esto debería ser así porque el rostro constituye un elemento esencial para la identidad de la persona, por lo que debería estar protegido.

Según el TEDH, la imagen de una persona "constituye uno de los principales atributos de su personalidad, ya que revela las características de la persona y la distingue de sus iguales" (Citado por Huijstee et al.,2021, p.40). Además, según el estudio realizado por el European Parliamentary Research Service (EPRS), debido a la amplitud de la definición del término "imagen", incluso el simple reconocimiento de la víctima podría ser suficiente para que los derechos de imagen entrasen en juego, lo que implica que, en los ordenamientos donde los derechos de imagen estén protegidos, el uso de una imagen para la creación de un *deepfake* podría ser ilegal[23].

3. LEGISLACIÓN APLICABLE

Sabemos que la IA es una tecnología relativamente novedosa que en los últimos años está experimentando un desarrollo y auge exponencial y sin precedentes, tanto es así, que la regulación de las constantes innovaciones tecnológicas, que además están en contínuo cambio, se convierte en una tarea especialmente ardua.

[22] Lavanda Oliva, M. Deepfake: Cuando la inteligencia artificial amenaza el Derecho y la Democracia. *Revista de Derecho y Tecnología*, 2022(2), 84-96. https://tinyurl.com/3mmhkxmy

[23] European Parliamentary Research Service. (July, 2021). *Tackling deepfakes in European policy*. (Panel for the Future of Science and Technology). European Parliament. https://doi.org/10.2861/325063 [Consulta: 7 de Marzo de 2024]

Tanto a nivel comunitario como estatal ya se ha reconocido la relevancia del desarrollo tecnológico y del amplio abanico de beneficios económicos y sociales que puede generar la IA, tanto en relación a los ciudadanos, como al desarrollo empresarial o a los servicios de interés público[24] . Sin embargo, los riesgos potenciales de las tecnologías de IA entre los cuales se encuentra la creación y publicación de *deepfakes* de carácter pornográfico y no consentido, demuestran la necesidad de adoptar medidas de forma urgente para lograr que éstas se desarrollen y se apliquen de forma segura.

Lo que ocurre con la problemática de los *deepfakes* es que ésta es tan incipiente que no se encuentra legislada de forma explícita ni a nivel europeo ni estatal. En este sentido, el presente apartado tiene como objetivo recoger y analizar brevemente la posible normativa aplicable a este tipo de casos.

3.1 NORMATIVA ESTATAL

En España, como ya se ha adelantado previamente, no existe normativa destinada explícitamente a la protección de las víctimas de *deepfakes*, por lo que el abordaje de este tipo de casos habría de realizarse atendiendo a otras normas cuyas disposiciones puedan dar cabida a este tipo de conductas, aunque en el momento de su redacción los *deepfakes* pareciesen únicamente posibles en la ciencia ficción.

3.1.1. Constitución

En primer lugar resulta imperativo mencionar de nuevo nuestra Constitución. Ya se ha analizado en un apartado[25] previo que la CE, en calidad de norma suprema de nuestro ordenamiento jurídico, consagra como fundamentales una serie de derechos, entre los cuales cabe destacar el derecho a la dignidad (Art. 10 CE) e integridad moral (Art.15 CE) y el derecho al honor, intimidad y propia imagen (Art. 18 CE).

Aún así, la experiencia histórica pone de manifiesto que la consagración constitucional de los derechos constituye una condición necesaria, pero no suficiente, para garantizar la plena eficacia

[24] Comisión Europea. (2020). *Libro Blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza* [Libro blanco]. https://tinyurl.com/bhsjsh8z [Consulta: 7 de Marzo de 2024]

[25] Véase apartado 2: "Impacto en los derechos fundamentales"

de los derechos fundamentales (Alonso de Antonio, 2005)[26]. En este mismo sentido, García Morillo (2013)[27] señala que "la efectividad de los derechos fundamentales depende tanto de su reconocimiento formal cuanto de la existencia de mecanismos jurídicos susceptibles de garantizar su eficacia real" (p.379). De este modo, deviene necesario que la declaración de derechos se complemente con un sistema de garantías suficientes que asegure la efectividad de su ejercicio y, por cuanto los *deepfakes* constituyen un contenido potencialmente lesivo para los derechos a la dignidad, integridad moral, honor, intimidad personal y propia imagen, su creación y difusión debe poder ser perseguida, regulada y limitada.

3.1.2. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Esta complementación al reconocimiento constitucional del derecho al honor, intimidad y propia imagen se ha llevado a cabo de acuerdo con los Arts. 53 y 81 CE a través de la LO 1/1982. El objetivo de la norma es desarrollar el Art.18.1 CE, previamente analizado en el presente estudio, y el interés principal de este punto reside en evaluar si la mencionada Ley Orgánica tiene capacidad suficiente para garantizar la protección de los derechos de las víctimas de *deepfakes*.

Antes de entrar a analizar el articulado de la norma, conviene destacar algunos aspectos estipulados en el preámbulo. De este modo, cabe señalar que los derechos garantizados por la norma son irrenunciables ya que se encuadran dentro de los derechos de la personalidad y, aunque ello no impide que en determinados supuestos legalmente previstos se pueda autorizar o consentir su renuncia, el Art. 2.3 establece que tal consentimiento será revocable en cualquier momento. Esto nos lleva a afirmar que, aunque un determinado sujeto dé su consentimiento para el uso de su rostro en la creación de material *deepfake* de carácter pornográfico, cualquier conducta de producción o difusión de este contenido posterior a la revocación del consentimiento, constituye una conducta ilícita. Además, la Ley exige que el consentimiento sea expreso, por lo que en ningún caso puede interpretarse que la publicación por parte de la víctima de cualquier tipo de imagen en redes sociales o cualquier medio similar, constituya el consentimiento de la misma para la utilización o manipulación posterior de dichas imágenes.

Tampoco se puede pasar por alto la puntualización que realiza el legislador en relación al ámbito de interpretación de la norma, y es que lo expuesto en el preámbulo de la ley nos lleva a entender que, efectivamente, las disposiciones de la misma pueden ser interpretadas de forma amplia por

[26] Alonso de Antonio, A. y Alonso de Antonio, J. (2005). *Derecho Constitucional Español (7a ed.)*. Universitas.

[27] García Morillo, J. (2013). Las garantías de los derechos fundamentales (II). Las garantías jurisdiccionales. In *Derecho constitucional*. Tirant lo Blanch.

el juzgador puesto que el legislador deja claro que los conceptos de honor, intimidad personal y la esfera del uso de la imagen personal queda determinada de forma decisiva por las ideas presentes en la sociedad y por el concepto que cada persona tenga al respecto. En términos literales, se específica que *"*la cuestión se resuelve en la ley en términos que permiten al juzgador la prudente determinación de la esfera de protección en función de datos variables según los tiempos y las personas*"*, por lo que se entiende que el legislador ha querido permitir la adaptación de la ley a los tiempos. Por ende, no es descabellado pensar que, aunque probablemente la redacción de la ley no se llevó a cabo teniendo en cuenta los casos de *deepfakes*, a día de hoy es lógico pensar que la creación y difusión de un *deepfake* entraría dentro del ámbito de aplicación de la norma, pues en cuanto a los usos sociales es evidente que este tipo de creaciones constituyen una intromisión ilegítima al derecho al honor, intimidad y propia imagen, almenos hasta que estas situaciones dispongan de regulación específica.

Asimismo, el Art.1.1 LO 1/1982 ofrece otro indicio interpretativo en cuanto a la aplicación o no de la LO 1/1982 a los casos de *deepfakes*, estableciendo que: "el derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas". Por consiguiente, debería entenderse que los *deepfakes* constituyen una intromisión ilegítima que da lugar a la aplicación de esta Ley Orgánica, dado que el uso del término "todo género" expone de forma clara la voluntad del legislador de abarcar cualquier intromisión que se considere ilícita o reprochable de acuerdo a los usos sociales del momento, tal y como se observaba en el anterior párrafo.

Por otro lado, el Art.4 LO 1/1982 contiene la regulación relativa a intromisiones ilegítimas al derecho al honor, intimidad o la imagen de personas fallecidas, por lo que el alcance de protección de estos derechos por la norma abarca también los supuestos de fallecimiento del titular del derecho lesionado. De este modo, en el preámbulo de la norma se expone que "aunque la muerte del sujeto de derecho extingue los derechos de la personalidad, la memoria de aquél constitiuye una prolongación de esa última que debe también ser tutelada por el Derecho*"*. Por lo tanto, también estarían protegidos los *deepfakes* elaborados con el rostro de personas fallecidas.

Un precepto especialmente relevante en cuanto al análisis de la presente Ley Orgánica en relación a su aplicación a los casos de *deepfakes* es el Art. 7 LO 1/1982, destinado a delimitar las conductas que tendrán la consideración de intromisión ilegítima a efectos de su aplicación. En este sentido, resultan interesantes los apartados 3, 5 y 7 del precepto, que establecen lo siguiente:

> Artículo séptimo**.**
>
> Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:
>
> [...]
>
> 3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
>
> [...]
>
> 5. 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, salvo los casos previstos en el artículo octavo, dos.
>
> [...]
>
> 7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

El principal problema que se halla en los apartados 3 y 5 es la dificultad para determinar si la inclusión de los casos de *deepfakes* en el ámbito de aplicación de la norma significaría sobrepasar los límites de interpretación amplia del texto normativo esperados por el legislador. Aunque es cierto que el precepto no especifica si el hecho o imagen en cuestión han de referirse a hechos u actos reales, parece innegable que la voluntad de su redactado es la de referirse a la divulgación de hechos o a la captación, reproducción o publicación de imágenes reales, no falsas. Sin embargo, tampoco puede negarse que un *deepfake* de carácter pornográfico consiste en la imagen del rostro de una persona real, y representa a ésta misma en un momento de su vida privada que, aunque no es real, causa un gran perjuicio a la víctima y atenta directamente contra su dignidad y reputación.

Por otro lado, el apartado 7 del mencionado artículo considera intromisión ilegítima la imputación de hechos a través de acciones que de cualquier forma lesionen la dignidad de otra persona. En este sentido, el precepto podría acoger los casos de *deepfakes* como un tipo de intromisión ilegítima al derecho al honor, intimidad y propia imagen en cuanto que a través de un *deepfake*, por su naturaleza, se le imputa la realización de un acto sexual a la víctima que realmente nunca llevó a cabo. Dicho de otra forma, podría entenderse que a través de la creación y difusión de un *deepfake* se le está imputando un hecho (en este caso sexual) a la víctima, por más que este hecho resulte falso y, por lo tanto, la interpretación en términos amplios del Art. 7.7 LO 1/1982 podría servir para extender la aplicación de la norma a este tipo de casos.

Otro precepto destacable en este punto es el Art.9.2 LO 1/1982, que establece que:

> La tutela judicial comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y, en particular, las necesarias para:
>
> > a) El restablecimiento del perjudicado en el pleno disfrute de sus derechos, con la declaración de la intromisión sufrida, el cese inmediato de la misma y la reposición del estado anterior. En caso de intromisión en el derecho al honor, el restablecimiento del derecho violado incluirá [...] la publicación total o parcial de la sentencia condenatoria a costa del condenado con al menos la misma difusión pública que tuvo la intromisión sufrida.
> >
> > b) Prevenir intromisiones inminentes o ulteriores.
> >
> > c) La indemnización de los daños y perjuicios causados.
> >
> > d) La apropiación por el perjudicado del lucro obtenido con la intromisión ilegítima en sus derechos.

Al respecto cabe puntualizar la dificultad que supone en los casos de *deepfake* la aplicación de estas medidas e, incluso siendo posible su aplicación, la dificultad de las mismas para cumplir con su finalidad, que no es otra que poner fin a la intromisión ilegítima y restablecer el derecho de la víctima tras su lesión. Esto se debe a dos aspectos que suponen una especial dificultad en el tratamiento de esta problemática; en primer lugar, la dificultad para conocer el sujeto autor de estos contenidos y, en segundo lugar, la dificultad para detener la difusión de dicho contenido debido a la pérdida de control del mismo una vez ha sido publicado en línea.

En lo referido a la díficil identificación del autor del contenido *deepfake*, cabe señalar que los usuarios en línea fácilmente se esconden tras perfiles falsos o anónimos, y lo mismo sucede con los usuarios que se encargan posteriormente de difundir dicho material. Esto implicaría la pérdida de eficacia de las medidas previstas en el apartado 2 del precepto, puesto que ante la imposibilidad de hallar al responsable de la vulneración de los derechos de la víctima, no existe sujeto contra quien iniciar un procedimiento,

Este hecho provoca que sea especialmente dificultoso para la víctima la obtención de la indemnización contemplada por el apartado c) del precepto por los daños y perjuicios sufridos. Además, disminuye drásticamente la capacidad disuasoria de las medidas, dificultando el objetivo de prevenir intromisiones inminentes o ulteriores previsto en el apartado b).

Por otro lado, en cuanto a la dificultad para poner fin a la difusión de los *deepfakes* una vez éstos han sido publicados en línea, conviene destacar un hecho que supone un desafío a la hora de tratar estos casos, y es que una vez se publica o difunde un vídeo o imagen en Internet, es prácticamente imposible hacerlo desaparecer. Los usuarios en línea inician sus descargas y el material pasa a su

posesión, no importa si el usuario inicial lo elimina, el vídeo o imagen en cuestión ya está a disposición de diferentes usuarios que ahora pueden resubirlo a la red, continuar su difusión por cualquier otra vía o incluso modificarlo de nuevo y volver a publicarlo. Esto supone una grave pérdida de control sobre el *deepfake* original, lo que dificulta y prácticamente imposibilita poner fin a la intromisión ilegítima sufrida por la víctima. El apartado a) que aboga por el restablecimiento del perjuicado en el pleno disfrute de sus derechos y por el cese inmediato de la intromisión sufrida deviene ineficaz frente a estos ataques.

Respecto a estas dificultades conviene mencionar la STEDH, as. DELFI contra Estonia, de 10 de Octubre de 2013[28]. En este caso, la sociedad DELFI AS, titular de un conocido portal de noticias en Estonia, publicó en 2006 un artículo criticando ciertas actuaciones de un empresa de transportes. Esta publicación provocó en la propia web de noticias de DELFI AS numerosos comentarios anónimos, difamatorios y ofensivos contra la empresa de transporte y, en concreto, contra su accionista mayoritario, referido en la sentencia como "L".

La empresa fue condenada por los tribunales nacionales a satisfacer una indemnización a "L" por los daños causados a su derecho al honor y la consideraban responsable de los comentarios difamatorios publicados por los lectores en su portal de noticias de Internet. DELFI AS alegó ante el TEDH que la exigencia de responsabilidad civil por los comentarios constituía una injerencia desproporcionada a su libertad de expresión, vulnerando así el Art.10 del CEDH.

El TEDH reiteró la decisión tomada por los tribunales nacionales y confirmó la responsabilidad de DELFI AS por los comentarios difamatorios publicados por los lectores en su portal de noticias de Internet, afirmando que se trataba de una restricción justificada y proporcionada sobre el derecho a la libertad de expresión de la empresa, negando así la vulneración del art.10 del Convenio.

El argumento principal aportado por el TEDH es que, en este tipo de casos y a efectos de presentar una demanda civil, resulta muy dificil para un individuo establecer la identidad de las personas a demandar. Y establece que, en efecto, "por razones puramente técnicas parecería desproporcionado imponer la responsabilidad de la identificación de los autores de comentarios difamatorios sobre la persona lesionada en un caso como el presente".

Así, este argumento podría aplicarse por analogía a los casos de *deepfakes* publicados en determinadas plataformas. En otras palabras, el caso DELFI AS contra Estonia podría servir como un indicio para determinar una posible solución a la dificultad de identificar al sujeto autor del

[28] Sentencia del Tribunal Europeo de Derechos Humanos, asunto DELFI AS contra Estonia, de 10 de Octubre de 2013.

deepfake, que facilitase a las víctimas la obtención de la indemnización prevista en el Art.9.2.c) LO 1/1982, gracias a la posibilidad de exigir cierta responsabilidad a las plataformas o aplicaciones que acogen este tipo de contenidos.

Además, en cuanto a la pérdida de control del contenido una vez publicado en Internet, el TEDH reconoce que *"*la propagación de Internet y la posibilidad -o para algunos propósitos el peligro- de que, una vez hecha pública, la información permanecerá pública y circulará para siempre, llama a la precaución". Este elemento es considerado por el TEDH como un factor importante que justificaría modificar el riesgo de la persona difamada para obtener una indemnización por parte de la empresa, normalmente en una mejor situación económica que el difamador.

Finalmente, cabe destacar que la LO 1/1982 señala que alguno de los derechos regulados por la misma tienen también protección penal, por lo que, en caso de que exista protección penal, ésta será de preferente aplicación. Aún así, el Art.1.2 establece que el carácter delictivo de la intromisión no impedirá la aplicación de la norma, pues en caso de responsabilidad civil derivada de delito, ésta deberá fijarse de acuerdo con los criterios establecidos por la misma.

En este sentido, y con la finalidad de analizar cuál es la protección penal existente a día de hoy en España para los casos de *deepfake*, se ha llevado a cabo una detenida lectura de la Ley Orgánica 1/1995, de 23 de noviembre, del Código Penal (de ahora en adelante, CP) de la que a continuación se destacan los aspectos más relevantes en relación a este tipo de casos.

3.1.3. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Antes de analizar los diferentes delitos en los que podrían encuadrarse los casos de *deepfakes*, cabe destacar que el CP no contempla ningún tipo penal destinado de forma clara a proteger a las víctimas de este tipo de contenido. Por este motivo, en la mayoría de casos, la subsunción de una conducta de este tipo en un il·lícito penal contempado en el CP será resultado de una interpretación amplia del mismo.

Siguiendo la línea de análisis de la protección a los derechos fundamentales al honor, intimidad y propia imagen, se analizan los delitos previstos en los Títulos X (delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio) y XI (delitos contra el honor). Así, en primer lugar conviene detenerse en el Art.197.2 CP que contempla penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses:

> Al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

Estas conductas recibirán mayores penas, de tres a cinco años de prisión, si los datos personales utilizados corresponden a la víctima, conforme al Art. 197.4.b. De este modo, y teniendo en cuenta que el rostro de la víctima constituye un dato de carácter personal que la distingue de cualquier otra, no es ilógico pensar que los *deepfakes* podrían tener cabida en este tipo penal.

Por otro lado, entre los delitos contra el honor (Título XI) se halla el delito de injuria previsto en el Art.208 CP. En él, se define la injuria como *"*la acción o expresión que lesiona la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación*"*. Al respecto, el propio precepto aclara también que no toda conducta de este tipo será constitutiva de delito de injurias, pues únicamente lo serán las injurias "que sean tenidas en el concepto público por graves".

Sin dejar de señalar el carácter indeterminado y ambiguo de estas últimas líneas, cabe advertir también que la imputación de hechos no es considerada grave según el CP. En este sentido, teniendo en cuenta que los *deepfakes,* suponen precisamente la imputación a la víctima de unos hechos o actos de carácter sexual, se podría llegar a la consideración de que la producción y difusión de un *deepfake* no es una conducta constitutiva de un delito de injurias. Sin embargo, el Art.208 prevé que tendrán tal consideración si ésta se ha llevado a cabo "con conocimiento de su falsedad o temerario desprecio hacia la verdad". Resulta evidente que quien crea un *deepfake* tiene pleno conocimiento de que los hechos representados en el fotograma son falsos, pues el sujeto debe llevar a cabo un proceso de modificación de la imagen, actuando de esta forma con temerario desprecio hacia la verdad. En este sentido, parece evidente que los casos de *deepfake* pueden ser adecuadamente subsumidos dentro del delito de injurias.

Especial atención merecen los delitos contra la libertad sexual (Título VIII) debido al enorme componente sexual de los *deepfakes*. En este sentido, resulta especialmente relevante el Art.189 CP que, aunque se refiere únicamente a la protección de víctimas menores de edad o con discapacidad, parece incluir los casos de *deepfakes* de forma menos dudosa. Esto se debe a dos motivos; en primer lugar, a la amplitud de acciones que tienen la consideración de il·lícitas según el Art. 189.1 apartados a) y b). Y, en segundo lugar, a la amplitud del término "pornografía infantil" o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección.

En cuanto al primer motivo, el precepto castiga con penas de prisión de uno a cinco años tanto la "captación*"* como la "utilización" de menores o personas con discapacidad, así como la "producción, venta, distribución, exhibición o facilitación*"* de los mismos por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad, independientemente del origen del material. En términos literales, el Art.189.1 establece que:

1. Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido".

El redactado del precepto evidencia la especial protección de los menores y personas con discapacidad frente a cualquier tipo de conducta que utilice su imagen para usos pornográficos. Parece que la intención del legislador fuese la de evitar que ante posibles situaciones dudosas, éstas quedasen fuera del ámbito de aplicación del tipo penal.

En este mismo sentido, el segundo motivo se conforma alrededor del amplio concepto que el legislador establece respecto a qué se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad. Al respecto, se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad, las siguientes:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada**.**

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

De este modo, resulta evidente que los *deepfakes* de carácter pornográfico en los que se utiliza el rostro de menores o de personas con discapacidad necesitadas de especial protección constituyen una conducta perfectamente subsumible en el tipo penal previsto en el Art.189 CP. El legislador hace referencia de forma clara a cualquier tipo de material que represente a menores o personas

con discapacidad, tanto si esa representación es real como si es simulada. Además, el uso de términos como "toda" o "cualquier" representación, así como de "imágenes realistas", diluyen cualquier posible duda al respecto.

La necesidad de especial protección a menores y personas con discapacidad necesitadas de especial protección resulta indiscutible atendiendo la elevada vulnerabilidad de estos colectivos. Tal es así, que el Art.189 CP no solamente castiga al autor del material o a quién realizase su difusión o facilitase su visualización a terceros, sino que el apartado 5 del precepto establece como punible también su adquisición o posesión para uso propio, incluso el simple acceso a sabiendas a dicho material pornográfico.

El Art.189 CP adquiere relevancia en la presente investigación debido a su mayor claridad interpretativa ante los casos de manipulación digital de imágenes. Parece que, hasta el momento, es el que menos dudas plantea en relación a su aplicación a casos de *deepfakes* y, aunque está únicamente destinado a la protección de menores y personas con discapacidad frente a este tipo de conductas, podría constituir una sugerencia de cómo regular la problemática de los *deepfakes*.

Por otra parte, el Art.189 bis establece que:

> La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar a la comisión de los delitos previstos en este capítulo y en los capítulos II y IV del presente título será castigada con la pena de multa de seis a doce meses o pena de prisión de uno a tres años.

Lo que plantea la cuestión de si determinadas apps como Deepnude, Onlyfakes o Undressai, programadas para generar desnudos realistas a través de imágenes y promocionadas como tal, podrían tener la consideración de contenido específicamente destinado a promover, fomentar o incitar la comisión de este tipo de delitos y, como tal, su distribución o difusión sería punible de acuerdo con el mencionado precepto. En otras palabras, se plantea el interrogante de si sería posible prohibir o bloquear el uso de este tipo de aplicaciones en España.

Al respecto, resulta interesante el Auto del Juzgado Central de Instrucción 89800/2024[29], de 22 de marzo de 2024, mediante el que se ordenó la suspensión de forma cautelar de la aplicación de mensajería instantánea Telegram, debido a un supuesto delito contra los derechos de la propiedad intelectual. Tal medida se consideró justificada al concurrir los principios de necesidad, idoneidad y proporcionalidad, argumentando el tribunal que:

[29] Auto del Juzgado Central de Instrucción 89800/2024 (Sección 5ª), de 22 de marzo de 2024.

No existe otro tipo de medida que pueda detener la reiteración de los hechos denunciados. La medida es idónea porque su ejecución pondría fin a la infracción de los derechos de la propiedad intelectual denunciada al impedir el acceso a través de la red de TELEGRAM a los contenidos de los derechos citados. (FJ. QUINTO)

Así, el razonamiento expuesto por el tribunal nos conduce a sostener que resulta plenamente justificable considerar el bloqueo de aplicaciones de creación de *deepfakes* como una medida potencialmente aplicable en este tipo de situaciones. [30]

Dejando atrás el ámbito de los delitos contra la libertad sexual, existe la posibilidad de que los casos de *deepfakes* pudiesen encuadrarse entre los delitos de odio si son dirigidos contra un mujer. En este sentido, el Art.510.1 CP se encarga de la regulación de este tipo de delitos. De este modo, establece penas de prisión y multa a quiénes realicen determinadas conductas destinadas a promover, fomentar o incitar de forma directa o indirecta el odio, dicriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia a aquel, por diferentes motivos listados en el precepto, entre los que se hallan el sexo y las razones de género.

Es el apartado 2.a) del precepto que establece que serán castigados con pena de prisión de seis meses a dos años y multa de seis a doce meses:

Quienes lesionen la dignidad de las personas mediante acciones que entrañen humillación, menosprecio o descrédito de alguno de los grupos a que se refiere el apartado anterior, o de una parte de los mismos, o de cualquier persona determinada por razón de su pertenencia a ellos por [...] su sexo, [...] por razones de género [...], o produzcan, elaboren, posean con la finalidad de distribuir, faciliten a terceras personas el acceso, distribuyan, difundan o vendan escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos para lesionar la dignidad de las personas por representar una grave humillación, menosprcecio o descrédito de alguno de los grupos mencionados, de una parte de ellos, o de cualquier persona determinada por razón de su pertencencia a los mismos.

Resulta innegable el componente de género en la creación de *deepfakes* de carácter pornográfico. Aunque el presente trabajo dedica más adelante un apartado destinado al papel del género[31] en este tema, conviene señalar que detrás de estas conductas se halla un fuerte desprecio hacia la mujer. Evidencia de ello se encuentra en los estudios que demuestran que son principalmente ellas

[30] Tan solo dos días más tarde, a través del Auto del Juzgado Central de Instrucción 89783/2024, de 25 de marzo de 2024, se dejó sin efecto la orden de bloqueo de Telegram. El juez consideró que se trataba de una medida excesiva debido al claro perjuicio que esta medida supondría para los millones de usuarios que utilizan la aplicación para fines no delictivos (particulares, empresas, funcionarios, trabajadores en general...).

[31] Véase apartado 5: Enfoque de género.

las perjudicadas por este tipo de conductas. En este sentido, si bien los *deepfakes* de carácter no pornográfico analizados en YouTube eran protagonizados en un 61% por hombres, los *deepfakes* de contenido pornográfico son un fenómeno que afecta y daña exclusivamente a las mujeres, ya que en estos supuestos las mujeres representan prácticamente el 100% del total[32].

Resulta evidente entonces que los casos de *deepfakes* pornográficos en los que la víctima sea una mujer pueden encuadrarse dentro del ámbito de aplicación del Art.510.2 CP.

Finalmente, cabe decir que en ocasiones los *deepfakes* son utilizados como mecanismo para amenazar o coaccionar a sus víctimas. En este caso, los *deepfakes* podrían tener cabida en determinados delitos contra la libertad (Título VI), como el delito de amenazas previsto en el Art.169 CP o el delito de coacciones previsto en el Art.172 CP.

En definitiva, el Código Penal no contempla de forma explícita los casos de *deepfakes*. Aunque parece ser que en los casos de *deepfakes* de menores o personas con discapacidad la protección a sus víctimas es más clara y, por lo tanto, más fácilmente aplicable, no ocurre lo mismo con el resto de casos, pues para proteger al resto de víctimas de este tipo de conductas es necesario acudir a otros delitos que, en función del caso concreto, podrán o no entenderse cometidos. Esto plantea un problema de seguridad jurídica que ha de ser abordado cuanto antes.

3.2. NORMATIVA EUROPEA

Aunque a nivel comunitario existe normativa relativa al desarrollo tecnológico que hace mención expresa a la Inteligencia Artificial, no hay ninguna normativa específicamente destinada a abordar la problemática de los *deepfakes* no consentidos de carácter pornográfico. De hecho, el tema del desarrollo tecnológico suele tratarse poniendo en el centro las oportunidades inherentes a dicha tecnología y se pone el énfasis en los beneficios económicos y sociales que tecnologías como la IA pueden aportar. Además, preocupan aspectos como garantizar su acceso a todos los ciudadanos o impulsar la situación competitiva de las empresas y de la indústria europea en un contexto económico cada vez más digitalizado.

Sin embargo, si bien se reconoce la existencia de riesgos asociados a los usos de la IA y se subraya la importancia de abordar estos desafíos de forma urgente y adecuada, hasta la fecha no se han implementado mecanismos suficientes para afrontar dichas problemáticas a nivel europeo. Esto se debe, en gran medida, a la complejidad inherente a los desafíos planteados por la IA y tecnologías afines.

[32] Ajder, H.,Patrini, G., Cavalli, F y Cullen, L. (2019). *The State of deepfakes: Landscape, threats, and impact,* p.2.

Por ejemplo, el Reglamento 2021/694/UE del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital[33], tiene como objetivo reforzar y promover la capacidad de la Unión Europea en el proceso de desarrollo de la tecnología digital. De este modo, trata de impulsar el liderazgo europeo en áreas clave como la informática de alto rendimiento, la inteligencia artificial, la ciberseguridad y confianza, las capacidades digitales avanzadas y el despliegue y mejor uso de la capacidad digital e interoperabilidad.

A través del Reglamento, se establece una dotación financiera para el Programa Europa Digital durante el período 2021-2017, crucial para garantizar la financiación necesaria para llevar a término las acciones previstas en el programa e impulsar la implementación de iniciativas estratégicas.

Parece ser que la norma no ignora los riesgos asociados al desarrollo tecnológico, pues en el párrafo 36 de la misma se destaca la necesidad de aumentar la sensibilización en materia de ciberseguridad y la importancia de desarrollar un enfoque común europeo en este sentido. Sin embargo, no se hace referencia alguna a los riesgos que suponen los *deepfakes*.

Por otro lado, la Decisión 2481/2022/UE del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030[34], parece poner más énfasi en la necesidad de proteger los derechos fundamentales y la inclusión de los ciudadanos europeos. En este sentido, el Art.3.1.a) fija como uno de los objetivos generales del programa estratégico de la Década Digital para 2030:

> Promover un entorno digital centrado en el ser humano, basado en los derechos fundamentales, inclusivo, transparente y abierto en el que las tecnologías y servicios digitales seguros e interoperables respeten y refuercen los principios, derechos y valores de la Unión y sean accesibles a todos y en toda la Unión.

Esta necesidad de garantizar un entorno digital basado en los derechos fundamentales obliga a tener en cuenta la problemática de los *deepfakes* por el ataque directo que estos materiales suponen a los derechos fundamentales reconocidos en la CDFUE. Aún así, se observa que lo

[33] Reglamento (UE) nº 694/2021 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240. (DOUE L, nº 166, 11-05-2021, p. 1-34). < https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80609>. [Consulta: 12 de marzo 2024].

[34] Decisión 2481/2022/UE del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030. https://eur-lex.europa.eu/eli/dec/2022/2481/oj [Consulta: 12 de marzo de 2024]

establecido en la normativa europea es insuficiente para hacer frente a este tipo de situaciones, y no se ha desarrollado aún legislación directamente destinada a abordar este tipo de casos.

Finalmente, conviene destacar el Libro Blanco de la Comisión Europea sobre la inteligencia artificial[35], que aunque carece de fuerza legal obligatoria, ofrece ciertas recomendaciones y directrices para la consecución de una IA fiable y hace algo más de hincapié en los riesgos potenciales que acarrea este tipo de tecnología. En este sentido, se reconoce que determinadas características de la IA, como la opacidad, pueden dificultar la aplicación y ejecución de la legislación. Por este motivo, se establece que "resulta necesario analizar si la legislación actual puede hacer frente a los riesgos de la IA y si su observancia es factible o si, por el contrario, es necesario adaptarla o se requiere nueva legislación".

A lo largo del documento se hace especial mención a los resultados nocivos que puede acarrear una regulación insuficiente de la IA. Aunque es cierto que tampoco se habla explícitamente de *deepfakes*, se expone la dificultad en la aplicación de las normas diseñadas para proteger los derechos fundamentales como uno de los principales riesgos relacionados con el uso de la IA. Se habla explícitamente de la posible afectación de esta tecnología a la dignidad humana, a la protección de datos personales y de la vida privada y de discriminación por razón de sexo.

Además, se hace hincapié en la necesidad de establecer un marco común europeo que incluya nueva legislación específica sobre IA. Y, en este sentido, la Comisión defiende un enfoque basado en el riesgo a fin de garantizar una intervención reguladora proporcionada.

La idea consistiría en establecer criterios claros que permitan diferenciar entre las distintas aplicaciones de IA, clasificándolas en función de si suponen un riesgo elevado o no. Esta clasificación dependerá de "lo que esté en juego" (p.21), y de la consideración tanto de si el sector como el uso previsto de la IA suponen riesgos significativos, en especial desde la perspectiva de la protección de aspectos como la seguridad, los derechos de los consumidores y los derechos fundamentales.

De este modo, se propone el establecimiento de una serie de requisitos legales obligatorios a los que deberán atenerse las aplicaciones de IA que entrañen un riesgo elevado. Estos requisitos deberían diseñarse a partir de las directrices de un grupo de expertos de alto nivel y podrían contar con las siguientes características:

[35] Comisión Europea. (2020). *Libro blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza* [Libro blanco].
https://tinyurl.com/3cmvmsj6

1. Datos de entrenamiento.
2. Datos y registros de datos.
3. Información que debe facilitarse.
4. Solidez y exactitud.
5. Supervisión humana.
6. Requisitos específicos en el caso de determinadas aplicaciones de IA, como las empleadas para la identificación biométrica remota.

4. PROPUESTAS LEGISLATIVAS

Tal y como se ha expuesto anteriormente, los *deepfakes* no son algo nuevo. La tecnología lleva años permitiendo la manipulación de imágenes. Sin embargo, el nacimiento de la inteligencia artificial generativa ha provocado un incremento sin frenos en su creación y difusión, generando una situación realmente preocupante. Especialmente alarmante es su empleo con fines maliciosos, como en el caso de la producción y difusión de imágenes o vídeos de carácter pornográfico y no consentido con los rostros de personas reales.

A lo largo del presente Trabajo de Final de Grado, se enfatiza el potencial dañino de tales contenidos para los derechos fundamentales de sus víctimas, que pueden sufrir daños morales y reputacionales de naturaleza incuantificable. En los últimos años se han hecho públicos diversos casos en España como el de las jóvenes de Almendralejo, en el que se difundieron imágenes de falsos desnudos de decenas de menores, todas ellas niñas. O casos de figuras públicas como Laura Escanes o Rosalía, quienes denunciaron a través de sus redes sociales la existencia de imágenes suyas falsas en las que aparecían desnudas. Estos casos, entre muchos otros más, ponen de relieve cómo el avance de los sistemas de inteligencia artificial ha facilitado el acceso a la creación de *deepfakes* y como el resultado de los mismos es cada vez más realista.

Tampoco puede obviarse que las principales afectadas por este tipo de conductas son las mujeres, lo que podría llevar a considerar este tipo de contenido como una nueva forma de violencia sexual. Por ello, resulta imperativo el desarrollo de normativa adecuada destinada a aplacar este tipo de ataques a los derechos fundamentales de las mujeres y, aunque no se ignora el gran desafío que ello supone, la necesidad y urgencia de medidas protectoras lo hacen impostergable.

A continuación, se analizan dos propuestas legislativas en vías de aprobación; por un lado, a nivel europeo destaca la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se

establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (de ahora en adelante Propuesta de Reglamento) y, por otro lado, a nivel estatal destaca la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial (de ahora en adelante Proposición de Ley Orgánica).

4.1. PROPUESTA DE REGLAMENTO EUROPEO

En vista de la voluntad de la UE para mantener su posición de líder tecnológico y de los riesgos inherentes al desarrollo de los sistemas de IA, la Propuesta de Reglamento de Inteligencia Artificial pretende establecer un marco jurídico coherente, efectivo y proporcionado destinado a la consecución de una IA fiable. En este sentido, tiene como objetivo final garantizar el desarrollo y aplicación de la IA de modo que se respeten los derechos de los ciudadanos. Tal y como establece el propio texto en su exposición de motivos, las normas relativas a la IA "deben estar centradas en las personas, a fin de que la población tenga la seguridad de que la tecnología se usa de modo seguro y en consonancia con la ley, lo que también implica respetar los derechos fundamentales".

La importancia de disponer de un marco jurídico europeo que regule esta materia no radica únicamente en la amenaza de la IA para los derechos fundamentales de los ciudadanos, sino también en el hecho de que la ausencia de una regulación armonizada podría llevar a los Estados Miembros a adoptar normas nacionales destinadas a garantizar el desarrollo y uso seguro de la IA. En este sentido, el texto reconoce que "la existencia de distintas normas nacionales puede dar lugar a la fragmentación del mercado interior y reducir la seguridad jurídica de los operadores que desarrollan o utilizan sistemas de IA".

Por lo tanto, la adopción de un marco jurídico europeo en esta materia respondería a la necesidad de establecer un marco jurídico uniforme en toda la Unión que evite las divergencias normativas entre estados y que ofrezca una protección uniforme de los derechos de los ciudadanos europeos.

Por otro lado, es inconcebible ignorar que nos encontramos ante un gran desafío a nivel jurídico. La labor de legislar sobre algo tan innovador y cambiante como la Inteligencia Artificial, con un impacto directo en los derechos fundamentales, es sumamente compleja. En este sentido, la Propuesta de Reglamento debe, por un lado, redactarse de forma que pueda resistir al paso del tiempo, y ello pasa por establecer un marco jurídico que incluya mecanismos flexibles que le permitan adaptarse de forma dinámica a nuevas situaciones preocupantes que puedan surgir a causa de la evolución tecnológica. Por otro lado, su regulación debe ser proporcionada y limitarse a establecer los requisitos mínimos necesarios para alcanzar el objetivo de una IA fiable y segura, que respete los derechos fundamentales. Todo esto sin obstaculizar ni impedir de forma indebida

el desarrollo tecnológico, pues de lo contrario podrían vulnerarse otros derechos fundamentales como por ejemplo el derecho a la libertad de expresión si, por ejemplo, se estableciese la medida desproporcionada de prohibir los sistemas de IA de generación o edición de vídeo o imagen.

Así las cosas, la propuesta plantea la adopción de normas armonizadas para el desarrollo, introducción en el mercado y para el uso de sistemas de IA en la Unión partiendo de un enfoque proporcionado basado en los riesgos. Esta propuesta basada en los riesgos, distingue entre los usos de la IA que generan un riesgo inaceptable, los sistemas de alto riesgo y finalmente los usos o sistemas de IA de riesgo bajo o limitado. Partiendo de tal clasificación, el texto prohíbe en su Art.5 las prácticas que comportan un riesgo inaceptable y recomienda, pero no obliga, a seguir códigos de conducta a los usos o sistemas de riesgo bajo o limitado. En cuanto a los sistemas de IA de alto riesgo (Arts. 6 a 29), la Propuesta de Reglamento dedica gran parte de su articulado a establecer requisitos específicos para su introducción en el mercado y obligaciones para los operadores de dichos sistemas. Podría decirse que los sistemas de alto riesgo son los protagonistas de la propuesta debido al potencial lesivo para la salud y la seguridad o los derechos fundamentales de los ciudadanos y de los valores de la Unión y por ello estarían sujetos al cumplimiento de requisitos específicos que garanticen la adecuación y respeto de los mismos a los derechos fundamentales. Estos sistemas de alto riesgo no estarían prohibidos en el mercado europeo siempre y cuando cumpliesen con los requisitos específicos exigidos y siempre que hubiesen sido sometidos a una evaluación de conformidad ex ante.

Partiendo de la base que existen numerosos sistemas de IA, veamos como trata la propuesta de Reglamento los sistemas de creación de *deepfakes* y si la misma contempla herramientas eficaces para la protección de sus víctimas. Así, el primer y más importante aspecto a destacar, es que a ojos de la propuesta la tecnología de generación de desnudos o de creación de *deepfakes* no se encuadraría ni en las aplicaciones prohibidas del Art.5 ni tampoco en los sistemas de alto riesgo previstos en los Arts. 6 y 7 del texto. Por tanto, estaríamos según la propuesta ante un sistema de riesgo limitado, que no estaría sujeto a los requisitos específicos ni al control de conformidad ex ante de obligado cumplimiento para los sistemas de alto riesgo.

Sin embargo, aunque la tecnología de creación de desnudos no estaría prohibida ni sujeta a los requisitos que se le exigirían a los sistemas de alto riesgo, la propuesta establece obligaciones de transparencia a las aplicaciones de creación de *deepfakes*. De este modo, el Art. 52.3 se refiere expresamente a este tipo de sistemas estableciendo que:

> Los usuarios de un sistema de IA que genere o manipule contenido de imagen, sonido o vídeo que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes, y que pueda inducir erróneamente a una persona a pensar que son auténticos o verídicos

(ultrafalsificación), harán público que el contenido ha sido generado de forma artificial o manipulado.

Así, el Art. 52.3 constituiría un avance en cuanto a la legislación aplicable hasta la fecha en los casos de *deepfake*, imponiendo la obligación al usuario de este tipo de aplicaciones de informar de la falsedad del contenido a cualquier sujeto que pudiese visualizarlo. Esto podría conllevar la imposición de potenciales sanciones por incumplimiento, también previstas en la propuesta y, por lo tanto, ofrecería mayor protección a las víctimas de la que existe actualmente.

Sin embargo, conviene puntualizar un aspecto que pone en duda la suficiencia de esta medida de transparencia en cuanto a la protección de los derechos de la víctima. En este sentido, el Art.3.4) de la propia propuesta define el término usuario como "toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se emmarque en una actividad personal de carácter no profesional". Esta definición excluye del término usuario a todo áquel que use estas aplicaciones a título personal no profesional y, por lo tanto, no sería aplicable a los casos en que, por ejemplo, un sujeto desde el ordenador de su casa usase el rostro de una compañera de clase para crear un video pornográfico y difundirlo en Internet. Conviene recordar que en la mayoría de los casos así es como ocurre, quienes cometen este tipo de ataques contra los derechos fundamentales a la dignidad, honor, intimidad y propia imagen de las víctimas de *deepfakes* son sujetos desde el ordenador de su casa y sin fines profesionales, por lo que a mi parecer, esta medida de transparencia es insuficiente para garantizar la protección de las víctimas de estos contenidos.

Otro aspecto destacable es que el propio Art.52.3 exime de la obligación de informar de la falsedad del contenido *deepfake* en caso de que el sistema de IA correspondiente resulte necesario para el ejercicio del derecho a la libertad de expresión y el derecho a la libertad de las artes, ambos garantizados por la CDFUE. Por tanto, un usuario malicioso podría alegar en su defensa que el contenido *deepfake* fue creado por razones artísticas o mera libertad de expresión, lo que podría comportar que, en la práctica, existiesen numerosos *deepfakes* eximidos del deber de transparencia y provocar un escenario potencialmente litigioso en cuanto a la necesidad de determinar si debe aplicarse o no la obligación de etiquetar este tipo de contenido (Álvarez y Eguiluz, 2023)[36].

Al parecer, la Propuesta de Reglamento supone un avance en materia de regulación de la inteligencia artificial a nivel comunitario y contempla por primera vez los *deepfakes* de forma

[36] Álvarez, P., Eguiluz, J. (23 de Marzo de 2024). El Reglamento de IA ante los deepfakes de desnudos. *Blog de Propiedad Intelectual y Tecnologías*. https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/el-reglamento-de-ia-ante-los-deepfakes-de-desnudos

expresa, estableciendo una definición para los mismos y ofreciendo una medida de transparencia para mitigar sus riesgos. No obstante, desde mi punto de vista, esta iniciativa sigue siendo insuficiente. Aunque se hace referencia a los *deepfakes* en términos generales, es importante recordar que no todos son de contenido sexual, por lo que a mi parecer, la propuesta pasa por alto la cuestión de los *deepfakes* de naturaleza pornográfica y el impacto que estos tienen en los derechos de sus víctimas, mayoritariamente mujeres. En este sentido, la Comisión Europea aborda el tema de los *deepfakes* en su investigación *Tackling deepfakes in European policy*, ya citado anteriormente en el presente trabajo. En este informe se proponen otras medidas que aún no se han incorporado en la Propuesta de Reglamento y que cabrá ver si finalmente se acogen en el texto final o en una posible futura normativa de desarrollo. Alguna de estas medidas son:

1. Establecer la tecnología *deepfake* como de alto riesgo.

   La propia Propuesta de Reglamento establece en su exposición de motivos que "los riesgos deben calcularse teniendo en cuenta su repercusión para los derechos y la seguridad", lo que nos lleva a remarcar que resulta totalmente lógico y coherente deducir que los *deepfakes*, sobretodo los de carácter pornográfico no consentido, tienen una repercusión indiscutible para los derechos de las víctimas. Por lo tanto, a mi parecer, esta medida es totalmente proporcional a sus riesgos, pues implicaría más obligaciones y requisitos específicos a los proveedores de los sistemas de IA generativa de *deepfakes*, reforzando así la protección de las víctimas de este tipo de contenido.

2. Ampliar el marco jurídico actual en materia de delitos.

   El informe también propone, entre otras medidas, modificar los Códigos Penales de los estados miembros. En este sentido, establecer un delito específico que tipifique y castigue la creación y difusión de *deepfakes* de carácter pornográfico no consentido podría devenir una posible solución a la dificultad de subsumir este tipo de conductas en los delitos previstos actualmente en la legislación penal.

3. Establecer etiquetas y obligar a las plataformas de difusión a detectar y prohibir determinados contenidos identificados como *deepfakes* o imágenes generadas por inteligencia artificial.

4.2. PROPOSICIÓN DE LEY ORGÁNICA

A nivel estatal se halla la propuesta de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, destinada específicamente a mitigar los riesgos asociados a las técnicas de recreación de imágenes y voces de personas a través de la inteligencia artificial.

La propuesta utiliza de forma expresa el término "*deepfake*", a diferencia de los textos normativos analizados previamente. Además, ofrece una definición para el mismo a la vez que alerta textualmente de que:

> El resultado de estos avances técnicos difumina 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.

Así, en la exposición de motivos el texto expone de nuevo la necesidad urgente de reforzar la protección de los derechos al honor, intimidad personal y familiar y propia imagen, y a su vez advierte del significativo sesgo de género que existe en estos contenidos señalando que el 90 por cierto de este tipo de vídeos suplantan la identidad de mujeres. El texto incide en que los *deepfakes* pornográficos, más allá de la clara vulneración de derechos que suponen en sí mismos, aumentan el riesgo de incidencia de los casos de acoso y otras formas de violencia sobre la mujer, reconociendo este tipo de contenido como una nueva y peligrosa forma de violencia sexual.

Por otro lado, aunque la propuesta señala que la libertad de expresión recogida en el Art.20.1 CE ampara el uso de la inteligencia artificial, advierte que los posibles conflictos que los *deepfakes* pueden ocasionar entre el derecho a la libertad de expresión y el derecho al honor, además de las posibles lesiones al derecho a recibir una información veraz y al resto de derechos fundamentales, hace necesaria una actualización de la normativa española. A mi parecer, la ponderación de derechos fundamentales es una cuestión sumamente delicada que requiere ser abordada con gran cautela. Sin embargo, resulta innegable que los *deepfakes* pornográficos no consentidos atentan de forma agresiva y directa contra el honor, la intimidad y el derecho a la propia imagen de las víctimas, lo que constituye motivo suficiente para considerar la limitación del derecho a la libertad de expresión.

Considerando lo anterior, el texto propone una reformulación normativa basada en la introducción de nuevos artículos o la modificación de preceptos ya existentes, así como la creación del Consejo de Participación Ciudadana para la supervisión y evaluación de la IA y del Consejo Consultivo sobre el uso de la IA. A continuación se exponen los puntos más relevantes de la propuesta.

En primer lugar, el texto propone en su Art.2 una modificación de la actual LO 1/1982, analizada previamente en el apartado 3.1.2 de la presente investigación. En este sentido, si al analizar la LO 1/1982 se apreciaba cierta dificultad para incluir los *deepfakes* entre el listado de intromisiones ilegítimas contenido en el Art.7 de la LO 1/1982, la propuesta que ahora se analiza propone añadir un apartado 9 al mencionado precepto que contemple explícitamente como intromisión ilegítima al derecho al honor, intimidad y propia imagen:

> La difusión y utilización de imágenes y vídeos de personas o audios generados a través de sistemas automatizados, software, algoritmos o mecanismos de IA sin la previa autorización o consentimiento expreso de la persona o personas afectadas, excepto que incluyan de forma clara y sobresaliente una advertencia de su condición de imagen o audio de voz generado artificialmente por IA.

En consecuencia, y partiendo de la base que los *deepfakes* que ocupan la presente investigación nunca serán consentidos, no solo la producción, sinó también la difusión de estos materiales constituiría una de las intromisiones ilegítimas previstas en la LO 1/1982 pudiendo dar lugar a las medidas necesarias para poner fin a dicha intromisión previstas en el Art.9 de la misma Ley Orgánica, lo que facilitaría su aplicación y por ello supondría un avance que ofrecería mayor garantía de protección a las víctimas. Sin embargo, la propuesta prevé una excepción y establece que no tendrá tal consideración de intromisión ilegítima la difusión o producción de *deepfakes* cuando estos incluyan una advertencia clara de su falsedad, lo que a mi parecer resulta cuestionable.

Aunque parezca evidente que los daños reputacionales de la víctima pueden verse reducidos si el *deepfake* va acompañado de una advertencia que elimine cualquier duda respecto a la realización por parte de la víctima de los actos sexuales recreados, no parece que esta medida brinde una protección suficiente a los derechos fundamentales de las víctimas. Y esto se debe a que, aún teniendo conocimiento de la falsedad de las imágenes, cualquiera que pueda visualizar el contenido en el que aparece la víctima practicando sexo, tiene a su disposición contenido hiperrealista de la misma que la recrea en una situación de absoluta y extrema intimidad y vulnerabilidad, que jamás debiese haber podido estar a disposición de un tercero sin el consentimiento expreso de la víctima.

En segundo lugar, el texto propone en su Art.3 la modificación del Código Penal, creando un nuevo artículo 208 bis y modificando el art.211 ya presente en la norma. Así, el nuevo artículo 208 bis, relativo al delito de injuria, despejaría cualquier posible duda respecto a la subsunción de los de *deepfake* en el tipo penal del delito, estableciendo explícitamente que tendrá la consideración de injuria:

> La acción que, sin autorización y con ánimo de menoscabar el honor, fama, dignidad o la 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.

Cuando se analiza el Art.208 CP en el apartado 3.1.3 del presente Trabajo de Final de Grado, se observa que la actual redacción del delito de injuria ya permitiría la subsunción de los casos de *deepfakes* en el tipo penal, por lo que a primera vista podría entenderse que la incorporación del

Art.208 bis planteada por la propuesta de LO es inecesaria. Sin embargo, a mi parecer la incorporación del Art.208 bis es relevante por dos motivos; en primer lugar, porque agiliza y simplifica la tarea interpretativa del juzgador y, en segundo lugar, porque más allá de la función reguladora de las normas, éstas sirven para promover y postular los valores de la sociedad. Así, en estos tiempos de digitalización en que parece que lo que ocurre tras una pantalla es irrelevante y que carece de consecuencias, me parece importante usar palabras textuales y claras que expongan socialmente que ciertas conductas han de ser inaceptables.

Por otro lado, el Art.211 CP prevé una pena mayor para las injurias hechas con publicidad. En este sentido, la propuesta plantea la inclusión de un segundo párrafo en el precepto que considere los *deepfakes* como injurias hechas con publicidad, lo que implicaría un agravante del delito de injuria.

Finalmente, se plantea la inclusión de un nuevo apartado 12.º al Art.727 de la LEC, relativo a las medidas cautelares específicas que pueden acordarse en el proceso judicial. Así, el texto propone establecer la posibilidad de acordar como medida cautelar *"*La retirada de las simulaciones de imágenes, vídeos o voces de personas, generadas por sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial a petición de la persona afectada o sus representantes*"*. Aún así, sería conveniente valorar la efectividad de esta medida y los desafíos que podría conllevar su aplicación, puesto que una vez que el material ha sido publicado y difundido en Internet, la rápidez de propagación y la diversidad de plataformas digitales dificultan la eliminación efectiva del contenido, lo que en la mayoría de casos resulta en una falta de control sobre el uso y la disponibilidad del material en la red.

5. ENFOQUE DE GÉNERO

Hasta el momento, se ha identificado la necesidad de abordar el fenómeno de los *deepfakes* pornográficos debido a la gravedad íntrinseca de estos contenidos. La creación y difusión de *deepfakes* pornográficos no consentidos constituye un grave ataque a los derechos fundamentales y la libertad sexual de las víctimas, independientemente de su edad, nacionalidad o profesión. Sin embargo, resulta imperativo destacar que el género puede ser un factor determinante que condicione la probabilidad de ser víctima de este tipo de manipulación digital. En este sentido, eludir que los *deepfakes* pornográficos suponen un problema que atenta de forma casi exclusiva contra las mujeres equivaldría a ignorar que se trata de un nuevo tipo de violencia sexual por razón de género.

Los patrones de desigualdad y los roles de género tradicionalmente establecidos en la sociedad evolucionan con el paso del tiempo; no desaparecen, sino que se adaptan a los nuevos tiempos con el fin de perdurar, encontrando nuevas formas de manifestarse en la era digital. Así, la producción y difusión de contenido sexual con el rostro de mujeres con el fin de denigrarlas y ridiculizarlas, causándoles graves daños personales o sociales, constituye una nueva forma de cosificación y reducción de las mismas a objetos sexuales. Por ello, el fenómeno de los *deepfakes* debe ser entendido como una nueva forma de violencia sexual, y no como un simple efecto negativo de las nuevas tecnologías.

En este sentido, conviene citar de nuevo el estudio realizado por la empresa Deeptrace en el año 2019[37], que determinó que, mientras que los *deepfakes* de carácter no pornográfico eran protagonizados en un 61% por hombres, la tendencia se invertía cuando se analizaba únicamente material pornográfico, ya que en estos casos las mujeres protagonizaban prácticamente el 100% del total. Y ello en un contexto en que el 96% de los vídeos *deepfakes* online eran de carácter pornográfico. Así, el estudio retrata la pornografía *deepfake* como un fenómeno que perjudica casi exclusivamente a las mujeres.

Una evidencia de esta cuestión de género en la producción de pornografía *deepfake* es el funcionamiento de determinadas aplicaciones como DeepNude, lanzada en 2019, que permitía a los usuarios "desnudar" artificialmente fotografías de personas. Sin embargo, esta aplicación únicamente funcionaba si quienes aparecían en las imágenes eran mujeres, ya que utilizaba algoritmos que habían sido ajustados para eliminar la ropa de imágenes de mujeres y generar partes desnudas de su cuerpo que en la fotografía original estaban cubiertas. Estos algoritmos no tenían capacidad para generar imágenes de hombres desnudos puesto que habían sido únicamente entrenados con imágenes de cuerpos de mujeres, por lo que solo ellas podían ser víctimas de esta aplicación.

Aunque esta app fue retirada, su software se ha ido distribuyendo de forma independiente. Desde el momento en que la aplicación estuvo disponible para su descarga, quedó fuera del control de su creador, y actualmente resulta muy complicado eliminar la circulación de dicho software. Este, continuará esparciéndose y mutando como un virus, deviniendo una herramienta popular para crear pornografía *deepfake* no consentida de mujeres, fácilmente accesible y dificilmente controlable (Adjer, H., Patrini, G., Cavalli, F. y Cullen, F., 2019).

[37] Ajder, H.,Patrini, G., Cavalli, F y Cullen, L. (2019). *The State of deepfakes: Landscape, threats, and impact.*

Por otro lado, Hamilton (2020) señaló que 680.000 mujeres fueron víctimas de estas conductas solo en el año 2020 (Citado por Bello San Juan, 2023, p.241)[38]. Lo que en este caso evidencia la dimensión de la problemática de los *deepfakes* es que las fotografías utilizadas para la producción del contenido pornográfico que posteriormente fue subido a Telegram, fueron extraídas a través de IA de las redes sociales de las víctimas, pero no únicamente de perfiles públicos, sinó también de conversaciones privadas (Bello San Juan, 2023).

Se ha comprobado que resulta insoslayable el componente de género que subyace tras las conductas de creación y difusión de *deepfakes*, pues son las mujeres las principales afectadas por este tipo de contenidos. Además, tal y como se ha expuesto previamente en el presente trabajo, no solamente debe ser motivo de preocupación el evidente daño reputacional y al honor de las víctimas, sinó también la instrumentalización de los *deepfakes* como herramientas de extorsión a las mismas, amenazándolas con la difusión del contenido. Así, en el contexto actual resulta imposible no calificar estas conductas como un tipo de violencia sexual en tanto que se persigue socavar la autonomía de las mujeres humillándolas, controlándolas e intimidándolas.

6. ANÀLISIS JURISPRUDENCIAL

Ante la falta de jurisprudencia relativa a casos de *deepfakes* debido el carácter novedoso de este fenómeno, en el presente apartado se realiza un análisis de casos que pueden resultar análogos o similares con el fin de examinar cuál es el pronunciamiento de los tribunales al respecto y determinar cuál podría ser la decisión de los mismos ante un posible caso de *deepfake* no consentido de carácter pornográfico.

No resulta en absoluto sorprendente afirmar, tras el analisis jurisprudencial realizado, que quien realiza las conductas que motivan el presente trabajo, es decir, quien produce y difunde contenido falso, de carácter pornográfico y sin el consentimiento de la víctima a partir de imágenes del rostro de la misma, comete una intromisión ilegítima a los derechos fundamentales al honor y a la propia imagen recogidos en el Art.18 CE y desarrollados y amparados en la LO 1/1982. Casos ejemplificadores de ello son tres sentencias del Tribunal Supremo: la STS núm. 185/2006, de 7

[38] Bello San Juan, P. (2023). La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica. En COLEX (ed.), *La justicia en la sociedad 4.0: nuevos retos para el siglo XXI* (p.219-244).
https://dialnet.unirioja.es/servlet/libro?codigo=924170

de marzo de 2006[39], la STS núm. 588/2011, de 20 de julio de 2011[40] y la STS núm. 592/2011, de 12 de septiembre de 2011[41].

En todas ellas, los hechos versan sobre la difusión pública de imágenes falsas o fotomontajes en los que la demandante aparece falsamente desnuda o semidesnuda. Así, en la primera de ellas, una revista denominada "Noticias del Mundo", realizó un reportaje titulado "la doble de Chabeli desnuda", en la que aparecía una composición fotográfica integrada por la fotografía de la cabeza verdadera de la afectada y otra del cuerpo desnudo de otra mujer hasta la parte superior de los muslos, cubierta con un taparrabos y exhibiendo unos pechos protuberantes. En la segunda sentencia, varias revistas publicaron un fotomontaje en el que se unía la cabeza de la afectada al cuerpo de una modelo desconocida únicamente cubierto por una braga levemente bajada con las manos para enseñar un tatuaje, encontrándose el pecho parcialmente descubierto. En cuanto a la tercera sentencia, el antiguo programa de televisión "Aquí hay tomate" de Telecinco, emitió en 2004 un reportaje titulado "El desnudo del año". En él, aparecían algunas imágenes manipuladas, en las que se había hecho desaparecer el bañador de dos piezas que la afectada llevaba cuando se realizaron las fotografías originales para que ésta quedase aparentemente sin ropa. En otras palabras, las fotografías que aparecían en el reportaje habían sido trucadas y eran falsos desnudos.

Las similitudes entre estos casos y un supuesto caso de *deepfake* son más que evidentes. Por un lado, en todos ellos se ha llevado a cabo una manipulación fotográfica del rostro del sujeto afectado con la finalidad de recrear contenido en el que éste aparezca desnudo o semidesnudo y, posteriormente, se ha procedido a la difusión de dicho material. Por otro lado, en todos ellos tanto la obtención, como la alteración y la difusión de las imágenes se ha llevado a cabo sin el consentimiento de la víctima.

En cuanto a las diferencias, cabe destacar que en las tres sentencias analizadas la persona afectada tiene la consideración de personaje público, mientras que por casos de *deepfakes*, a lo largo del presente Trabajo de Final de Grado se ha pretendido hacer referencia no solamente a *deepfakes* que afecten o puedan afectar a personajes públicos, sinó también, y sobretodo, a aquellos casos en que la víctima es una persona sin exposición pública.

Aún así, que en los tres casos analizados la víctima fuese un personaje público no elimina el poder ejemplificador y/o esclarecedor de estas sentencias, pues como a continuación se expone en las líneas que siguen, la condición de personaje público es precisamente un elemento alegado por la

[39] Sentencia del Tribunal Supremo 185/2006 (Sala de lo Civil, Sección 1ª), de 7 de marzo de 2006.
[40] Sentencia del Tribunal Supremo 588/2011 (Sala de lo Civil, Sección 1ª), de 20 de julio de 2011, (recurso 1745/2009).
[41] Sentencia del Tribunal Supremo 592/2011 (Sala de lo Civil, Sección 1ª), de 12 de septiembre de 2011, (recurso 941/2007).

defensa en los tres casos para negar la intromisión ilegítima a los derechos del honor y la propia imagen. Por lo tanto, si aún siendo las víctimas personajes públicos el Tribunal Supremo ha estimado que las conductas llevadas a cabo por la parte demandada eran vulneradoras de los derechos al honor y la propia imagen, más evidente resulta tal vulneración cuando la víctima es una persona anónima, y a esta conclusión es a la que se llega aplicando el argumento para llenar lagunas conocido como "a fortiori" en su versión "a minore ad maius", pues quien tiene prohibido lo más tiene prohibido lo menos (si está prohibido subir al tren con un gato, mucho más lo estará con un tigre y, si está prohibido entrometerse en la intimidad de una persona pública mucho más lo estará hacerlo respecto de una persona sin relevancia pública).

Así, en los tres casos ha sido pretendido por la defensa que el Tribunal estimase justificado el ataque al honor y a la propia imagen de las demandantes aludiendo a la prevalencia del derecho a la libertad de expresión por tratarse las víctimas de personajes públicos. En este sentido, en todos los casos los demandados se amparan en el Art.8.2 LO 1/1982, que establece que no se considerarán intromisiones ilegítimas al derecho a la propia imagen cuando el sujeto afectado ejerza un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público, o cuando se utilicen caricaturas de dichas personas de acuerdo con el uso social.

En este sentido, la defensa insiste en el interés público de los reportajes debido a la condición de personajes públicos de sus protagonistas, así como en el carácter humorístico, irónico, satírico o sarcástico de los mismos, tratando en un intento fallido que el tribunal considere encuadrables en el concepto de caricatura acorde con los usos sociales las imágenes publicadas, y así queden amparadas por el Art. 8.2 LO 1/1982. Sin embargo, el TS niega en primer lugar que las imágenes puedan ser consideradas una caricatura y, en segundo lugar, destaca que aún de ser así, no todas las caricaturas merecen la protección del Art. 8.2 LO 1/82. En el primer sentido porque aunque el tribunal reconoce la evolución de las caricaturas, entendiendo que éstas ya no se refieren solamente a dibujos sino que las nuevas tecnologías permiten la alteración de imágenes originales, también determina que "para no perder su esencia de creación irónica debe basarse en la reelaboración de la fisonomía del modelo con un contenido injerente de exageración y distorsión de la realidad" (STS 588/2011 FJ.4), características que no se dan en ninguno de los casos analizados. Más bien todo lo contrario:

> En el fotomontaje publicado el rostro era el de la demandante sin deformación alguna, es decir, sus facciones, el elemento por el que más identificable es una persona, y el cuerpo semidesnudo era el de otra mujer, por ende tampoco deformado ni ridiculizado sino, lejos de ello, conjuntado con el rostro de la demandante de un modo tan perfecto que los dos elementos de la composición parecían pertenecer a una misma persona" (STS 185/2006 FJ.4).

En síntesis, el TS considera en los tres casos analizados que ha habido una intromisión ilegítima en el derecho al honor y a la propia imagen de las demandantes, que en ninguno de los casos se entiende justificada en beneficio del derecho a la libertad de expresión. Cabe recordar que, ante la colisión del derecho a la libertad de expresión y los derechos de la personalidad como el derecho al honor, intimidad o propia imagen, debe realizarse una ponderación constitucional de tales derechos que necesaria y lógicamente resultará más compleja cuando el titular de los derechos de la personalidad sea un personaje público. En este sentido, ante un eventual caso de *deepfake* en el que la defensa alegue libertad de expresión, las reglas de la lógica nos permiten afirmar que si ante los casos analizados el TS ha determinado la prevalencia de los derechos al honor y propia imagen, entendiendo la existencia de una clara vulneración a tales derechos, aún más evidente resultará la vulneración de tales derechos cuando la víctima del *deepfake* sea un personaje anónimo.

Se incide en que en todos los casos el TS ha apreciado una intromisión ilegítima al derecho al honor y a la propia imagen de las afectadas. Por tanto, ateniendo al analisis jurisprudencial de las tres sentencias analizadas, se afirma que ante un hipotético caso de *deepfake* los tribunales constatarían la existencia de una vulneración a los derechos al honor y propia imagen, pues tal y como determina el TS en la STS 185/2006, respecto a la propia imagen:

> Se aprovechaba el rostro de aquélla para, en definitiva, ofrecerla públicamente de un modo habitualmente preservado por la demandante a la curiosidad ajena; en suma, de un modo que no está de acuerdo con el uso social (art. 8.2.b, y también art. 2.1, ambos de la LO 1/82). De ahí que no esté de más recordar la jurisprudencia de esta Sala que, en materia de protección del derecho fundamental a la propia imagen, se caracteriza por su rigor al considerar ilegítima la publicación inconsentida de la imagen de una persona desnuda o semidesnuda incluso cuando se trate de un personaje público y aun cuando sí hubiera mediado consentimiento para la mera captación de la imagen, pues el pudor sigue siendo un sentimiento socialmente estimable.

Por otro lado, en cuanto al honor, la STS 588/2011 establece que:

> La fotocomposición vulnera también el derecho al honor de la actora, puesto que, tal y como se ha dicho, al no existir deformación o distorsión alguna, y ser el rostro de la actora, se produce una identificación plena de su imagen que se presenta semidesnuda, y, esto, al no ser consentido, atenta contra su honorabilidad, tanto en la esfera personal y social, como en la profesional.

Mayores dudas suscita la cuestión de si en los casos de *deepfakes* se produce una intromisión ilegítima al derecho a la intimidad personal, puesto que lo cierto es que los hechos representados en las imágenes nunca ocurrieron, no son reales y, por tanto, podría resultar dudosa la lesión que estas conductas pueden provocar en la esfera íntima de las víctimas. Sin embargo, esta cuestión parece quedar resuelta por el TS en la última de las tres sentencias analizadas, esto es, la STS

592/2011, en la que, a parte de la vulneración al honor y propia imagen de la demandante, el tribunal también estimó que había habido una intromisión ilegítima al derecho a la intimidad. Aunque la defensa de la parte demandada insistía en que no podía haber habido una violación del derecho a la intimidad alegando que "por ser hechos falsos, los mismos no pueden gozar de la protección de la que disfrutan los hechos íntimos o privados de la vida de las personas", el TS no aceptó tal argumento puesto que:

> Una cosa es que la veracidad de la información no excluya la intromisión ilegítima en la intimidad [...] y otra muy distinta que la falta de veracidad excluya la intromisión ilegítima en el derecho a la intimidad. Antes bien, la intromisión en la intimidad puede resultar agravada precisamente por la falta de veracidad de la información si esta falta de veracidad contribuye a presentar, como en este caso, una situación de los demandantes aún más reservada o sustraída a los ojos de los demás que la situación real (FJ.8 9ª).

En definitiva, la postura adoptada por el TS en los tres casos examinados podría resultar ejemplificadora de cómo se abordaría un posible caso de *deepfake* en España, pues los argumentos empleados por el tribunal para determinar la violación de los derechos al honor, intimidad y propia imagen de las personas afectadas por los materiales gráficos difundidos son perfectamente aplicables por analogía a un caso de *deepfake,* ya sea que la víctima sea un individuo sin repercusión pública o una figura pública. Esto confirma la alta probabilidad de aplicar la LO 1/1982 en un hipotético caso de *deepfake*, y la resolución del asunto a través de los arts. 2.1, 7.3, 7.5. 7.7 y 8.2 de dicha norma. Además, tal y como sucede en las tres sentencias analizadas, se vislumbra la posibilidad de aplicar las medidas contempladas en el art.9.2 LO 1/1982, lo que implica que el responsable podría ser condenado al pago de una indemnización por los daños y perjuicios causados a la víctima.

Una vez confirmado que los *deepfakes* constituyen en España un ílicito civil, se procede a analizar si este tipo de casos también podrían tener recorrido por la via penal, es decir, si también podrían ser considerados como delitos penales. Sin embargo, la falta de casos suficientemente similares constituye la primera dificultad en este análisis.

En primer lugar, se plantean como posibles casos similares los supuestos de *sexting*[42], en los que la víctima consintió la obtención por un tercero de un vídeo o imagen íntimo y éste, sin el

[42] El sexting se incluye entre los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y, en concreto, en el delito de descubrimiento y revelación de secretos. Dicho delito engloba aquellas conductas de remisión y envío a través de internet o de cualquier terminal teléfonico de mensajes de contenido sexual producidos y protagonizados por el emisor del mensaje, en que la persona afectada otorga o ha otorgado el consentimiento en el ámbito íntimo de la pareja, si bien con posterioridad una de las partes difunde a terceros sin el consentimiento de la otra parte, atentando contra la dignidad de la persona e intimidad de la misma". (SAP Málaga 279/2019, de 26 de abril de 2019, FJ.4)

consentimiento de la misma, difundió dicho material. Algunas sentencias ejemplificadoras son la STS 492/2020, de 24 de febrero de 2020[43] o la STS 767/202, de 3 de octubre de 2023[44]. En el primer caso, D.Constantino envió desde su teléfono móvil a D.Federico, en esa época compañero sentimental de Joaquina, una fotografía en la que ésta aparecía desnuda sin el consentimiento de la misma y que previamente Joaquina le había enviado a Constantino. En el segundo caso, D.Romualdo, pareja sentimental de Teodoro, remitió por Whatssap a un amigo una fotografía de Teodoro en la que éste aparecía con el torso descubierto y con un pene erecto junto a su cara. La fotografía había sido tomada con la anuencia de la víctima, aunque la remisión por Whatsapp no había sido consentida.

En ambos casos el tribunal determina que la conducta llevada a cabo por los denunciados constituye un delito de revelación de secretos, concretamente el previsto en el Art. 197.7 CP, que establece que:

> Será castigado [...] el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

Sin embargo, se observa que ninguno de estos casos se asemeja suficientemente a los casos de *deepfakes*, principalmente porque el Art.197.7 CP que regula los casos de *sexting* hace referencia expresa a imágenes obtenidas con la anuencia de la víctima y en los casos de *deepfakes* no existe tal anuencia o consentimiento. Por tanto, se descarta que un supuesto caso de *deepfake* pudiese ser perseguido penalmente por vía del Art. 197.7 CP.

En segundo lugar, se examinan dos casos en que los denunciados consiguen captar imágenes de las víctimas desnudas a través de la instalación oculta de mecanismos de grabación en espacios privados. Con el análisis de estos casos lo que se espera es obtener supuestos más similares a los casos de *deepfakes* que los casos de *sexting*, puesto que en estos casos, las imágenes son obtenidas sin el consentimiento de la víctima, igual que ocurre en los supuestos de *deepfakes.*

Las sentencias analizadas son la SAP 90156/2021, de 25 de mayo de 2021 [45] y la SJP 20/2022, de 16 de mayo de 2022 [46]. En el primer caso, el denunciado D.Juan Francisco, sin el

[43] Sentencia del Tribunal Supremo 492/2020 (Sala de lo Penal), de 24 de febrero de 2020 (recurso 3335/2018).
[44] Sentencia del Tribunal Supremo 767/2023 (Sala de lo Penal, Sección 1ª), de 3 de octubre de 2023 (recurso 5039/2021).
[45] Sentencia de la Audiencia Provincial de Vizcaya 90156/2021 (Sección 2ª), de 25 de mayo de 2021 (recurso 51/2021).
[46] Sentencia del Juzgado de lo Penal de Vitoria-Gasteiz 20/2022 (Sección 2ª), de 16 de mayo de 2022 (recurso 36/2022).

consentimiento de Dña.Azucena, a quien tenía subarrendada una habitación en un domicilio compartido, colocó una cámara oculta en la habitación de la víctima, efectuando grabaciones en que Dña.Azucena aparecía desnuda. En el segundo, D.Tomás colocó en múltiples ocasiones un teléfono en los vestuarios de un complejo deportivo, enfocando hacia el espacio de las duchas comunes o las bancadas del vestuario, de forma que conseguía captar las imágenes de hombres desnudos, saliendo de la ducha o secándose el cuerpo y cambiándose de ropa. Posteriormente, D.Tomás compartió alguno de los vídeos con otro sujeto, a través de una plataforma de mensajería.

En ambos casos los acusados fueron condenados como autores responsables del delito de descubrimiento y revelación de secretos del art. 197.1 CP. Sin embargo, de nuevo no puede extenderse el posicionamiento de los tribunales a un posible caso de *deepfake* puesto que el redactado del precepto aplicado para la resolución de estos casos no permite el encuadre de los casos de *deepfakes* en el mismo. En este sentido, el Art. 197.1 CP establece que:

> El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Aunque una interpretación amplia del mismo podría llegar a permitir la aplicación del precepto a los casos de *deepfakes* por entender que estos se llevan a cabo mediante un artificio técnico de reproducción de imágenes, a mi parecer hay una clara diferencia entre reproducir y producir. El Art. 197.1 CP hace referencia específicamente a la reproducción o transmisión, y ambas conductas requieren la existencia previa del contenido que se reproduce o transmite. La gran diferencia es que, en el caso de los *deepfakes*, se está creando un contenido nuevo, previamente inexistente.

En definitiva, tras el análisis jurisprudencial realizado se advierte que, a día de hoy, un eventual caso de *deepfake* constituiría un ílicito civil que podría ser resuelto por los tribunales a través de la aplicación de la actual LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y que podría dar lugar a la adopción de las medidas previstas en el art. 9.2 de la norma, entre las cuales se prevé el pago de una indemnización por daños y perjuicios a la víctima afectada. En cuanto a la via penal, el análisis realizado no permite afirmar el acceso a esta vía en un supuesto caso de *deepfake*, por lo menos en lo que respecta a la normativa aplicada en las sentencias analizadas.

Aún así, no se descarta la posibilidad de que un supuesto caso de *deepfake* pueda encuadrarse en el Art.197.2 CP, que establece que incurrirá en un delito de descubrimiento y revelación de secretos:

> El que sin estar autorizado, [...] modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero"

O en el delito de injurias, previsto en el Art. 208 CP. Pero, en todo caso, no hay aún jurisprudencia sobre la aplicación de estos delitos a casos que puedan resultar análogos a los casos de *deepfakes*, por lo que no puede hacerse ninguna afirmación al respecto.

7. CONCLUSIONES

El presente apartado tiene por objetivo ofrecer una visión global de las principales reflexiones y hallazgos realizados sobre la problemática de los *deepfakes* en el contexto social y legal actual.

De este modo, las conclusiones que a continuación se presentan derivan de un análisis riguroso bassado en Derecho, que se espera que pueda contribuir al conocimiento existente sobre la materia y que no sirvan solamente para responder a las preguntas planteadas al inicio del trabajo, sinó que también puedan abrir nuevas línias de investigación y reflexión dentro del ámbito legal. Así, se pretende que estas conclusiones no tan solo culminen el presente Trabajo de Final de Grado, sinó que marquen también el inicio de un debate más amplio y enriquecedor sobre la necesidad y el modo de abordar los *deepfakes*.

Así pues, las principales conclusiones que se extraen del análisis realizado son las siguientes:

- Se detecta, actualmente, la ausencia de normativa destinada a abordar de forma específica los casos de *deepfakes.* Esta carencia de regulación se evidencia tanto a nivel estatal como comunitario, a pesar de que se observa la existencia de una marcada preocupación por parte de las instituciones en relación a los riesgos asociados a la tecnología de Inteligencia Artificial.

- Del análisis de las dos propuestas normativas examinadas, se observa que, a diferencia de lo que ocurre con la normativa vigente, se enfatizan por primera vez los *deepfakes* y se proponen medidas específicamente dirigidas a abordar esta problemática. Sin embargo, a pesar de que

las medidas propuestas suponen un paso más hacia la solución, se estiman insuficientes para hacer frente al ataque que estos contenidos suponen para los derechos fundamentales al honor, intimidad y propia imagen de las posibles víctimas. Concretamente, respecto a la propueta de reglamento europeo, si bien plantea la instauración de obligaciones de transparencia para los *deepfakes*, no llega a categorizarlos como contenidos de alto riesgo, lo que limitaría enormemente la protección de las víctimas.

- La complejidad que envuelve el fénomeno *deepfake* y que, por tanto, dificulta enormemente su abordaje reside, en primer lugar, en el carácter innovador y reciente de esta tecnología: la IA generativa experimenta cambios rápidos y constantes, que permiten su evolución a un ritmo vertiginoso. En este sentido, la dificultad del derecho para adaptarse ágilmente a esta dinámica supone el primer obstáculo para la regulación efectiva de la problemática *deepfake.* La segunda dificultad reside en la necesaria ponderación de derechos fundamentales que requiere la regulación de esta materia, específicamente la ponderación del derecho al honor, a la intimidad y a la propia imagen frente al derecho a la libertad de expresión. La limitación de derechos fundamentales requiere, y así debe ser, un alto grado de rigor, hecho que dificulta enormemente esta cuestión y posiblemente empuje a los tribunales a analizar caso por caso.

- Se observa el género como un factor determinante en la probabilidad de ser víctima de este tipo de conductas, siendo las mujeres las principales víctimas de *deepfakes* no consentidos de carácter sexual. En este sentido, se incide en la necesidad de abordar esta problemática con perspectiva de género, poniendo en el centro a la víctima y ateniendo los casos de *deepfake* como una nueva forma de violencia sexual.

- Ante la falta de jurisprudencia referente a casos de *deepfake* en España, se ha realizado un análisis de casos similares con el fin de inferir cuál sería la posible posición de los tribunales ante este tipo de conducta. Al respecto, cabe deducir que actualmente la producción y difusión de un *deepfake* pornográfico realizado a partir de la imagen del rostro de un tercero, constituye en España un ílicito civil por intromisión ilegítima al derecho al honor, intimidad y propia imagen de la víctima, previsto y regulado en el la LO 1/1982.

- Se detecta una especial dificultad para encuadrar de forma clara la creación y difusión de *deepfakes* en alguno de los delitos previstos en el Código Penal. En este sentido, resulta imprescindible considerar una posible modificación del mismo con el fin de incluir un delito destinado a perseguir estas prácticas ilícitas, tal y como ocurrió con los delitos de *sexting* en la reforma del Código Penal del año 2015.

8. REFERENCIAS BIBLIOGRÁFICAS

8.1. BIBLIOGRAFÍA

Ajder, H.,Patrini, G., Cavalli, F y Cullen, L. (2019). *The State of deepfakes: Landscape, threats, and impact.* https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/

Alonso de Antonio, A. y Alonso de Antonio, J. (2005). *Derecho Constitucional Español (7a ed.)*. Universitas.

Alonso, J.M. (28 de septiembre de 2023). *Ciberseguridad y Hacking en el mundo de Inteligencia Artificial, Robots y Humanos* [Ponencia magistral]. Larga vida al retail, XIX Congreso Español de Centros y Parques Comerciales, Madrid, España. https://www.youtube.com/watch?v=gsnFXlLYt9w

Álvarez, P., Eguiluz, J. (23 de Marzo de 2024). El Reglamento de IA ante los deepfakes de desnudos. *Blog de Propiedad Intelectual y Tecnologías*. https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/el-reglamento-de-ia-ante-los-deepfakes-de-desnudos

BBC News. (19 de julio de 2017). *Fake Obama created using AI video tool_BBC News*. [Vídeo]. https://www.youtube.com/watch?v=AmUC4m6w1wo

Bello San Juan, P. (2023). La inteligencia artificial al servicio del crimen: La revolución del deepfake desde una perspectiva criminológica. En COLEX (ed.), *La justicia en la*

sociedad 4.0: nuevos retos para el siglo XXI (p.219-244). https://dialnet.unirioja.es/servlet/libro?codigo=924170

Cerdán Martínez, V y Padilla Castillo., G. (2019). Historia del *fake* audiovisual: deepfake y la mujer en un imaginario falsificado y perverso. *Historia y comunicación social, vol.24* (2), 505-520. https://dx.doi.org/10.5209/hics.66293

Douglas Harris, A. (2018). Deepfakes: False Pornography is here and the law cannot protect you. *Duke Law & Technology Review, vol.17* (1), 99-128. https://scholarship.law.duke.edu/dltr/vol17/iss1/4

García Morillo, J. (2013). Las garantías de los derechos fundamentales (II). Las garantías jurisdiccionales. In *Derecho constitucional*. Tirant lo Blanch.

Gibert, K. (8 de junio de 2022). *Inteligencia artificial. Retos y oportunidades* [Ponencia]. Facultat de Lletres i de Turisme, UdG, Girona, España. https://diobma.udg.edu/handle/10256.1/6773?show=full.

Lavanda Oliva, M. Deepfake: Cuando la inteligencia artificial amenaza el Derecho y la Democracia. *Revista de Derecho y Tecnología*, 2022(2), 84-96. https://tinyurl.com/3mmhkxmy

Raz, J. (1983). *The Authority of law: essays on law and morality.* Oxford University Press.

Ruiz Guevara, P. (2023). El aprendizaje de las máquinas: El "Machine learning", una rama de la inteligencia artificial en auge. *Alfa*, (55), 6-11. https://www.csn.es/en/csn/revista-alfa/55

Universitat de Girona. *Servei de Sistemes d'Informació geogràfica i Teledetecció.* https://www.jornadassiglibre.org/

Viejo, M. (18 de septiembre de 2023). Decenas de menores de Exremadura denuncian que circulan fotos de falsos desnudos suyos creadas por inteligencia artificial: "Me dio un vuelco el corazón": La policía identifica a varios de los presuntos autores de los montajes fotográficos después de que varias familias de Almendralejo alertaran de que habían localizado imágenes en las que aparecían sus hijas adolescentes. *El país.* https://elpais.com/espana/2023-09-18/la-policia-investiga-el-desnudo-integral-de-varias-menores-en-extremadura-con-inteligencia-artificial-me-dio-un-vuelco-el-corazon.html#

8.2 LEGISLACIÓN

Asamblea General de la ONU. (1948). Declaración Universal de Derechos Humanos. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Carta de los Derechos Fundamentales de la Unión Europea. Niza, 7 de diciembre del 2000. (BOE [en línea], núm.303, 14-12-2007, pp.1-16). <https://www.boe.es/buscar/doc.php?id=DOUE-Z-2007-70004>.[Consulta: 1 de Marzo de 2024]

Comisión Europea. (2020). *Libro Blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza* [Libro blanco]. https://tinyurl.com/bhsjsh8z [Consulta: 7 de Marzo de 2024]

Comisión Europea. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM/2021/206 final).

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206

Congreso de los diputados. (2023). Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial (122/000011).

https://tinyurl.com/yjvr4zp4 [Consulta: 7 de marzo 2024]

Consejo de la Unión Europea. (2020). Conclusiones de la Presidencia sobre La Carta de los Derechos Fundamentales en el contexto de la inteligencia artificial y el cambio digital (11481/20).

https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/es/pdf

Decisión 2481/2022/UE del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, por la que se establece el programa estratégico de la Década Digital para 2030.

https://eur-lex.europa.eu/eli/dec/2022/2481/oj [Consulta: 12 de marzo de 2024]

España. Constitución Española. (BOE [en línea], núm. 311, 29-12-1978, pp. 29313-19424).<https://www.boe.es/eli/es/c/1978/12/27/(1)/con>. [Consulta: 1 de Marzo de 2024]

España. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (BOE [en línea], nº 115, 14-05-1982). < https://www.boe.es/eli/es/lo/1982/05/05/1/con>. [Consulta: 15 de marzo 2024].

España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (BOE [en línea], nº. 281, 24-11-1995, p. 33987-34058). <https://www.boe.es/eli/es/lo/1995/11/23/10/con>. [Consulta: 18 de marzo 2024].

European Parliamentary Research Service. (July, 2021). *Tackling deepfakes in European policy*. (Panel for the Future of Science and Technology). European Parliament.

https://doi.org/10.2861/325063 [Consulta: 7 de Marzo de 2024]

Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. Roma, 4 de noviembre de 1950. (BOE [en línea] nº. 243, 10-10-1979, p. 23564-23570).

< https://www.boe.es/eli/es/ai/1950/11/04/(1)>. [Consulta 3 de Marzo]

Reglamento (UE) nº 694/2021 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240. (DOUE L, nº 166, 11-05-2021, p. 1-34). < https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80609>. [Consulta: 12 de marzo 2024].

Unión Europea. (2000). Carta de los Derechos Fundamentales de la Unión Europea.

https://www.europarl.europa.eu/charter/pdf/text_es.pdf [Consulta 25 de febrero].

8.3. JURISPRUDENCIA

Sentencia del Tribunal Europeo de Derechos Humanos, asunto DELFI AS contra Estonia, de 10 de Octubre de 2013.

Sentencia del Tribunal Supremo 185/2006 (Sala de lo Civil, Sección 1ª), de 7 de marzo de 2006.

Sentencia del Tribunal Supremo 592/2011 (Sala de lo Civil, Sección 1ª), de 12 de septiembre de 2011, (recurso 941/2007).

Sentencia del Tribunal Supremo 588/2011 (Sala de lo Civil, Sección 1ª), de 20 de julio de 2011, (recurso 1745/2009).

Sentencia del Tribunal Supremo 492/2020 (Sala de lo Penal), de 24 de febrero de 2020 (recurso 3335/2018).

Sentencia del Tribunal Supremo 767/2023 (Sala de lo Penal, Sección 1ª), de 3 de octubre de 2023 (recurso 5039/2021).

Sentencia del Tribunal Constitucional 46/2002, de 25 de febrero de 2002.

Sentencia de la Audiencia Provincial de Málaga 279/2019 (Sección 8ª), de 26 de abril de 2019 (recurso 45/2019).

Sentencia de la Audiencia Provincial de Vizcaya 90156/2021 (Sección 2ª), de 25 de mayo de 2021 (recurso 51/2021).

Sentencia del Juzgado de lo Penal de Vitoria-Gasteiz 20/2022 (Sección 2ª), de 16 de mayo de 2022 (recurso 36/2022).

Auto del Juzgado Central de Instrucción 89800/2024 (Sección 5ª), de 22 de marzo de 2024.

Auto del Juzgado Central de Instrucción 89783/2024 (Sección 5ª), de 25 de marzo de 2024.