

INTELIGENCIA ARTIFICIAL Y *DEEPFAKES*: LAS ULTRASUPLANTACIONES COMO MEDIO PARA VULNERAR LOS DERECHOS AL HONOR, INTIMIDAD Y PROPIA IMAGEN

ARTIFICIAL INTELLIGENCE AND DEEPFAKES: ULTRASUPLANTATIONS AS A MEANS OF VIOLATION OF THE RIGHTS TO HONOUR, PRIVACY AND SELF-IMAGE

JESÚS DANIEL AYLLÓN GARCÍA

Universidad de Cantabria

Recibido: 25/09/2024

Aceptado: 22/10/2024

DOI: <https://doi.org/10.14679/3897>

Resumen: El presente estudio aborda el impacto de la inteligencia artificial, especialmente de los *deepfakes* o ultrasuplantaciones, en los derechos de la personalidad como el honor, la intimidad y la propia imagen. Las ultrafalsificaciones son contenidos audiovisuales manipulados mediante IA, que simulan a personas realizando acciones que nunca ocurrieron, presentando riesgos significativos para su reputación y privacidad. El estudio examina cómo estas tecnologías pueden ser utilizadas para suplantar identidades, difundir desinformación o incluso para crear contenido pornográfico falso, afectando gravemente a la integridad de las personas. Se analiza la regulación de los *deepfakes* en el contexto del Reglamento Europeo de Inteligencia Artificial y de la legislación española, resaltando la necesidad de un marco legal que proteja los derechos fundamentales ante el uso indebido de estas tecnologías.

Palabras clave: ultrasuplantaciones, inteligencia artificial, derechos de la personalidad, juridificación de la IA.

Abstract: *This study addresses the impact of artificial intelligence, especially deepfakes, on personality rights such as honor, privacy and self-image. Deepfakes are audiovisual content manipulated by AI, which simulate people performing actions that never happened, presenting significant risks to their reputation and privacy. The study examines how these technologies can be used to impersonate identities, spread disinformation or even create fake pornographic content, seriously affecting people's integrity. It analyses the regulation of deepfakes in the context of the European Regulation on Artificial Intelligence and Spanish legislation, highlighting the need for a legal framework that protects fundamental rights against the misuse of these technologies.*

Keywords: *Deepfakes, artificial intelligence, personality rights, regulation of AI.*

SUMARIO: 1. INTRODUCCIÓN. 2. INTELIGENCIA ARTIFICIAL Y DEEPFAKES: CONTEXTO, APROXIMACIONES SEMÁNTICAS Y MODELOS DE APLICACIÓN. 3. VULNERACIÓN DE LOS DERECHOS DE LA PERSONALIDAD A TRAVÉS DE ULTRA-

SUPLANTACIONES O *DEEPFAKES*. 4.REGULACIÓN DE LAS ULTRASUPLANTACIONES O *DEEPFAKES* EN EL MARCO EUROPEO Y ESPAÑOL.5. CONCLUSIONES. 6. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

Resulta innegable que la llegada de la Inteligencia Artificial (IA, en adelante) ha supuesto un impacto en nuestra sociedad reportando beneficios tanto a nivel personal (automatización de luces, termostatos o electrodomésticos en el hogar), como a nivel profesional (reducción de los tiempos empleados en el análisis de datos como, por ejemplo, en la búsqueda de jurisprudencia sobre una cuestión concreta), pero no podemos olvidar que la IA también puede acarrear inconvenientes pudiendo llegar, incluso, a vulnerar Derechos Fundamentales, tales como el honor, la intimidad o la propia imagen, entre otros.

La manipulación de imágenes, videos e, incluso, de la voz de las personas a través de la IA puede llegar a vulnerar los derechos al honor, intimidad y la propia imagen de los individuos¹, en su esfera personal y profesional. Nos estamos refiriendo a las denominadas *deepfakes* o ultrasuplantaciones, que suelen presentarse en forma de videos, imágenes o audios que, habitualmente, representan a una persona realizando una actividad o una manifestación de voluntad que parece real y que, en realidad, se han producido por IA a través de las técnicas de *machine learning* denominadas *Deep learning* o aprendizaje profundo, sobre las que tendremos la oportunidad de detenernos.

Algunos ejemplos recientes podemos encontrarlos dentro de la industria musical. En el último año se han generado algunos temas musicales con voces de cantantes utilizando el *Deep learning* (“Mi burrito sabanero”² interpretada falsamente por Bad Bunny o “NostalgIA”³ cuya autoría se ha asociado al mismo autor en colaboración con Bad Gyal) y que, algunas, superaron en pocas horas el millón de reproducciones⁴. El problema radica en que dichas producciones musicales han utilizado la

¹ Nótese que se está haciendo referencia, tanto en el título de la presente contribución, como aquí y como se hará a lo largo del estudio, a los “derechos” al honor, intimidad y propia imagen, en plural en contra de lo que hace la doctrina tradicional y el propio legislador en la Ley Orgánica 1/1992, de 5 de mayo de protección civil del derecho al honor, a la intimidad y a la propia imagen. Ello se debe, como más adelante se detallará, a que, pese a que el legislador lo ha tratado de manera unánime, es consolidada la jurisprudencia que entiende que cada uno de esos derechos tiene un contenido autónomo. Es por ello que se ha decidido emplear el término “derechos”, en vez de “derecho”, pues con esta redacción más actualizada se podría evitar caer en un error, ya no de forma, sino de fondo.

² Puede escucharse y visualizarse en <https://www.youtube.com/watch?v=n2Mk7Y41OAw> [fecha de consulta: 16/08/2024].

³ Puede escucharse y visualizarse en <https://www.youtube.com/watch?v=1OuSRAIf8rM> [fecha de consulta: 16/08/2024)].

⁴ Para un estudio pormenorizado de la creación de contenidos musicales por medio de herramientas de IA, *Vid.* VÁZQUEZ ALONSO, Víctor Javier, *La libertad del artista: censuras límites y cancelaciones*, Editorial Athenaica, 2023.

voz y la imagen de determinados cantantes sin su consentimiento, vulnerando de este modo algunos de sus derechos de la personalidad, entre otros derechos que no serán objeto de análisis.

De este modo, ante la posibilidad de crear *deepfakes* con unas pocas imágenes de una persona y un pequeño fragmento de audio con su voz, se plantean importantes cuestiones sobre la vulneración de determinados derechos de la personalidad, no circunscribiéndose únicamente a la industria musical, sino a cualquier otro campo, ya sea personal o profesional, pudiendo generar importantes perjuicios a las personas suplantadas por la IA.

En relación con esta cuestión, analizaremos algunas materias del recién publicado Reglamento de Inteligencia Artificial europeo⁵ (RIA, en adelante) que, a diferencia de su proyecto inicial, incide en la protección de los derechos de los ciudadanos europeos, entre ellos, el derecho a la imagen y a la intimidad, expresamente mencionados como de fundamental defensa, habida cuenta la capacidad de las IA generativas para crear imágenes, contextos o producciones audiovisuales capaces de imitar la apariencia, la voz y la figura de las personas. A nivel estatal, haremos alusión a la 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 (LOPDH, en adelante), a la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial; así como al Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales; normativas todas ellas relacionadas con el tema objeto de análisis del presente estudio.

2. INTELIGENCIA ARTIFICIAL Y DEEPFAKES: CONTEXTO, APROXIMACIONES SEMÁNTICAS Y MODELOS DE APLICACIÓN

2.1. Aproximación semántica de Inteligencia Artificial

Antes de adentrarnos en el estudio de lo que entendemos por inteligencia artificial, es conveniente fijar, en primer lugar, qué se entiende por inteligencia, o por inteligencia humana para ser más precisos.

A este respecto, la concepción de inteligencia con mayor aceptación desde el año 2007, es la elaborada por el Prof. DRENTH, quien la define como *el conjunto de las habilidades cognitivas o intelectuales necesarias para obtener conocimientos y utilizar esos conocimientos de forma correcta con el fin de resolver problemas que tengan un objetivo y una meta bien descritos*⁶. BARRIO ANDRÉS, por su parte, en-

⁵ REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828. (DOUE. Serie L, de 12.7.2024).

⁶ DRENTH, Piet, *Intelligence: knowing and measuring*, Editorial Nieuwezijds, Amsterdam, 2007, pp. 22-23.

tiende que, en esta definición, uno de los términos clave es la inteligencia cognitiva, que se refiere a las capacidades relativas al conocimiento. Además, mediante conocimientos empíricos o conocimientos basados en la experiencia y conocimientos científicos, la memoria y la relación entre unos y otros se va nutriendo el aprendizaje de manera que se es capaz de razonar y solucionar los problemas que se presentan en la vida diaria⁷.

Asentado el concepto de inteligencia humana de la manera expuesta y en el que no cabe mucha discusión doctrinal, queremos adelantar que, en relación con el concepto de inteligencia artificial, no existe una definición pacífica. Este término fue empleado por vez primera por McCARTHY⁸, padre del concepto de inteligencia artificial, pero tomando como base la definición empleada por el Diccionario de la Real Academia Española⁹, y siguiendo a LÓPEZ RINCÓN¹⁰ puede definirse como aquella disciplina científica enfocada en la replicación sintética del pensamiento y razonamiento humano a través de programación informática basada en algoritmos. O lo que es lo mismo, pero de una manera extremadamente simplificada, la inteligencia artificial serían máquinas que piensan como humanos imitando su pensamiento.

Por lo tanto, según este prisma, para hablar de inteligencia artificial necesitamos que una máquina sea sensible respecto de su ambiente, es decir, que interactúe con el medio (puesto que hasta ahora no se ha conseguido dotar de sensibilidad o sentimientos a las máquinas) y que, a raíz de esa interacción, sea capaz de “aprender”, de adquirir conocimientos¹¹.

No obstante, como adelantábamos, no es pacífica la doctrina en torno al concepto de inteligencia artificial, pues hay quienes defienden que la misma puede definirse como máquinas actuando como si fuesen inteligentes, mientras que otros la definen como máquinas que realmente piensan y no sólo simulan el pensamiento humano¹². Nosotros, en consonancia con GONZÁLEZ QUIRÓS, nos postulamos por la primera de las definiciones, esto es, que actúan como si fueran inteligentes pero que, realmente, no piensan autónomamente¹³, ya que las máquinas que realmente piensan por sí mismas, entendemos que no es algo que vayamos a presenciar en un lapso

⁷ VELAZQUEZ COBOS, Almudena, “El abogado robot”, en *Legal Tech. La transformación digital de la abogacía*, Edición nº 1, LA LEY, 2019 (LA LEY 7383/2019).

⁸ RUSSEL, Stuart y NORVIG, Peter, *Artificial Intelligence. A Modern Approach*, Third Edition, Pearson, 2016, p. 17.

⁹ La RAE define la inteligencia artificial como la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico.

¹⁰ LÓPEZ RINCÓN, Darío, “Robots y Abogacía”, en *Derecho de los Robots*, BARRIO ANDRÉS, Moisés (Dir.), Wolters Kluwer, Madrid, 2018, p. 192.

¹¹ CHURNIN, Stephen, *Inteligencia Artificial: retos éticos y jurídicos, y la influencia de los Derechos Humanos*, Servicio de Publicaciones de la Universidad Complutense de Madrid, 2011, p. 22.

¹² RUSSELL, Stuart y NORVIG, Peter, *Artificial Intelligence...* cit., p. 1020.

¹³ GONZÁLEZ QUIRÓS, José Luis, “La inteligencia artificial y la realidad restringida: las estrecheces metafísicas de la tecnología”, *Naturaleza y Libertad: Revista de Estudios Interdisciplinarios*, Núm. 12: Número especial: *Inteligencia artificial y Antropología filosófica*. ¿Es

breve de tiempo, pese a que algunos autores, como KURZWEIL¹⁴, defiendan que la denominada “singularidad” (comunicación directa entre máquinas y humanos), será una realidad a corto plazo¹⁵. Quizás un acercamiento a esa singularidad, a esa comunicación directa entre máquinas y humanos esté comenzando a vislumbrarse a través de la reciente versión de *GPT 4.Omni* (GPT 4.o), quien está a la vanguardia del PLN (Procesamiento del Lenguaje Natural), donde GPT puede mantener una conversación con un humano y se prevé que, incluso, pueda guiar a una persona invidente en tiempo real haciendo una descripción del entorno.

En todo caso, el término IA implica una importante distinción con respecto a la inteligencia natural (la propia de los seres humanos) y no es otra que el origen de la inteligencia artificial es el resultado de un esfuerzo informático intencionado, en lugar de la inteligencia de una persona¹⁶.

Lo que es innegable es que la inteligencia artificial ya está presente en nuestra sociedad y nuestra vida diaria, tanto en la domótica del hogar, como en el ámbito profesional y en el personal a través de los *smartphones*. De este modo, podemos hablar, a modo ejemplificativo, de Siri, de Alexa o de Bixby, que son unos asistentes personales que utilizan el procesamiento del lenguaje natural (PLN) para prestar sus servicios; de Facebook/Meta, que utiliza el reconocimiento de imagen para sugerir etiquetados en sus fotos; de Instagram que neutraliza o censura determinados comentarios basados en amenazas directas o aquellas publicaciones que vulneran los derechos de autor de la música; o Amazon que nos muestra sugerencias de compras basadas en otros productos que ya hemos comprado o que tenemos en nuestras listas de deseos. Y no podemos olvidarnos de GPT, que como ya se ha señalado con anterioridad se encuentra a la vanguardia del PLN. Estos son algunos ejemplos de inteligencia artificial que nos acompañan cada día y que, básicamente, la llevamos o bien en nuestros bolsillos o muñecas a través de *smartphones* y *smartwatches*, respectivamente; o bien en los ordenadores de nuestro hogar y/o puestos de trabajo.

De todo lo anterior, se puede deducir que, en la actualidad existen dos enfoques básicos para la inteligencia artificial:

- a) La IA basada en el conocimiento, conocida como *knowledge-based AI*, donde sus tecnologías utilizan un conocimiento extraído a partir de expertos humanos o documentos y lo representan de manera explícita y formal, de manera que se crea un algoritmo para razonar y proporcionar solucio-

posible transferir la mente humana a un soporte no biológico?, Estudios, 2019. DOI: <https://doi.org/10.24310/NATyLIB.2019.v0i12.6271> pp. 132-133.

¹⁴ DIEGUEZ LUCENA, Antonio Javier, “La singularidad tecnológica y el desafío posthumano”. *Pasajes: Revista de pensamiento contemporáneo*, núm. 50. 2016, pp. 154-164.

¹⁵ AYLLÓN GARCÍA, Jesús Daniel, “La Inteligencia Artificial como medio de control y difusión de las *Fake News*”, VILLEGAS DELGADO, César y MARTÍN RÍOS, Pilar (Dir.), *El Derecho en la encrucijada tecnológica: estudios sobre Derechos Fundamentales, nuevas tecnologías e Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2022, pp. 218-220.

¹⁶ BARRIO ANDRÉS, Moisés, “Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial”, BARRIO ANDRÉS, Moisés (Dir.) *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, p. 3.

nes a problemas en un ámbito particular, como, por ejemplo, los sistemas de expertos¹⁷.

- b) La IA basada en datos, *data-driven AI* o más conocida como aprendizaje automático (*machine learning*), donde su aprendizaje se centra en ejemplos o en la experiencia del uso del sistema. Los datos presentan información incompleta sobre los acontecimientos y los algoritmos tratan de generalizar esa información para hacer predicciones sobre los sucesos ya conocidos, es decir, no utilizan la causalidad, sino la probabilidad. Estos son viables desde hace relativamente poco tiempo porque requieren enormes cantidades de datos y recursos informáticos para ser eficaces y ha sido Internet quien lo ha hecho posible por la ingente cantidad de datos que almacena¹⁸.

Ambos enfoques tienen sus inconvenientes y sus ventajas: mientras la *data-driven AI* es apropiada para operaciones que precisan la identificación de patrones (reconocimiento del habla, visión artificial, robótica, etc.), la IA basada en conocimiento es más útil para campos específicos donde el conocimiento y el razonamiento pueden estar sistematizados, como la resolución de problemas por expertos¹⁹. Sin embargo, en numerosas ocasiones los sistemas de IA emplean componentes provenientes de ambos enfoques, lo que se conoce como “sistemas multiagente”²⁰.

De todo lo anterior se deduce que la IA, a largo plazo, pretende dotar a las máquinas de cualidades propias del ser humano, tales como la creatividad y la inteligencia interpersonal y, aunque la IA aún no ha conseguido emular la capacidad de los seres humanos de moverse por el mundo y de interactuar con todo el entorno que le rodea, tanto animado como inanimado, puede llegar el momento en el que sí se logre, lo que supone que podamos hacer, nuevamente, una doble distinción, en cuanto a tipos de IA se refiere: la IA “débil” y la IA “fuerte”. La débil sería la IA que existe actualmente, la que todos conocemos, que tiene la capacidad de resolver problemas específicos y delimitados, en un principio, con más agilidad y acierto que el ser humano. Por su parte, la fuerte haría referencia a la IA que se pretende crear en el futuro, esa IA que igualaría o, incluso, superaría la inteligencia humana y que tendría capacidad para razonar, representar conocimiento, planificar, aprender, comunicarse en lenguaje natural e integrar todas esas habilidades hacia un objetivo común²¹.

¹⁷ Vid. a este respecto MARTINO, Antonio Anselmo, *Expert System in law*. Editorial North-Holland, New York, 1992.

¹⁸ Se entiende que el auge del *big data* está ligado al desarrollo actual del aprendizaje automático, tal y como lo entiende BARRIO ANDRÉS. BARRIO ANDRÉS, Moisés, “Objeto, ámbito de aplicación... cit. p.22.

¹⁹ AYLLÓN GARCÍA, Jesús Daniel, “La Inteligencia Artificial como medio para administrar justicia”, BUENO DE MATA, Federico (Dir.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Editorial Comares, 2020, pp. 3-14.

²⁰ BARRIO ANDRÉS. BARRIO ANDRÉS, Moisés, “Objeto, ámbito de aplicación... cit. p.23.

²¹ LLANO ALONSO, Fernando M., *Homo Ex Machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnológica*, Tirant lo Blanch, Valencia, 2024, pp. 223-224.

Una vez señalado el concepto de inteligencia humana y de haber hecho una aproximación al concepto de IA y a sus posibles categorías, es necesario hacer alusión al concepto de “sistemas de inteligencia artificial” que, en este caso, lo encontramos plasmado en el Reglamento de Inteligencia Artificial (RIA) ya mencionado, concretamente en su artículo 3, bajo la rúbrica de “Definiciones”, en su apartado primero, y dispone lo siguiente:

«sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

De este modo, podemos afirmar que el concepto de “sistema de IA” en el RIA se refiere a un sistema automatizado capaz de operar de manera autónoma y adaptativa, utilizando la información recibida para generar resultados como predicciones, recomendaciones o decisiones (lo que se corresponde con lo que antes hemos denominado *data-driven AI*). Estos resultados, dirigidos a cumplir objetivos específicos o implícitos, pueden influir tanto en entornos físicos como virtuales, reflejando la capacidad del sistema para aprender y ajustarse tras su implementación (lo que podemos categorizar dentro de lo que antes hemos denominado IA débil).

2.2. Concepto de *deepfake* o ultrasuplantación

Dado que el presente estudio se centra en el análisis de la inteligencia artificial y su relación con los *deepfakes*, es ahora el momento de abordar el concepto de estos últimos.

Pese a que los *deepfakes* se dice que tienen su origen a finales de 1990, cobraron especial relevancia en el año 2017, a raíz de la publicación de material pornográfico falso a través de la plataforma Reddit²², donde un usuario anónimo utilizó el rostro de actrices famosas para crear dicho contenido ilícito, conocido ahora como pornografía²³ *deepfake* no consentida²⁴.

Como una primera aproximación, podríamos decir que los *deepfakes* constituyen una técnica avanzada de manipulación digital basada en la inteligencia artificial que permite la creación de contenido audiovisual sintético, en el que la apariencia, la voz o los comportamientos de una persona son alterados o falsificados con un

²² <https://www.newtral.es/deepfakes-pornograficos-mujeres-ley-ia-almendralejo/20230920/> [fecha de consulta: 24/08/2024].

²³ Para un estudio pormenorizado del uso de las *deepfakes* vinculado a la pornografía, se considera de obligada lectura VALERO HEREDIA, Ana, *La Libertad de la pornografía*, Editorial Athenaica, Sevilla, 2022.

²⁴ Vid. BAÑUELO CAPISTRÁN, Jacob, “Evolución del *deepfake*: campos semánticos y géneros discursivos (2017-2021), *Icono 14: Revista científica De Comunicación Y Tecnologías Emergentes*, Vol. 20, núm. 1, (Ejemplar dedicado a: Niños y jóvenes ante los dispositivos: Nuevos fenómenos comunicativos y nuevos creadores de producto). 2022, pp. 9-11.

alto grado de realismo. Estas tecnologías se fundamentan en redes neuronales profundas, específicamente, en algoritmos de aprendizaje automático profundo (*Deep learning*), tales como las redes generativas antagónicas (GANs)²⁵.

Dicho en otras palabras, las *deepfakes* consisten en manipular un video, una fotografía o la voz de una persona de tal modo que, los oyentes o videntes crean en la veracidad de lo que ha sido manipulado y consideren que lo que están viendo o escuchando es certero cuando, en realidad, es una falsedad.

Por su parte, y en el mismo sentido ya apuntado, también el Reglamento de Servicios Digitales²⁶, en su art. 35.1.k) aporta un concepto de *deepfake*:

Un elemento de información, ya se trate de imagen, audio o vídeo generado o manipulado que se asemeja notablemente a personas, objetos, lugares u otras entidades o sucesos existentes y que puede inducir erróneamente a una persona a pensar que son auténticos o verídicos.

En cuanto a la capacidad de parecer veraces dependerá del programa informático o sistema de IA que se utilice para su elaboración. Como acabamos de mencionar, los *deepfakes* se originan, entre otros medios, a través del aprendizaje profundo automático, basado en algoritmos sofisticados que son capaces de analizar si un archivo es real o si está alterado y, de esta forma, la inteligencia artificial puede ir mejorando con la práctica y ser más precisa en la labor de falsificar de manera fidedigna, pudiendo llegar a crearse *deepfakes* directamente por softwares especializados sin necesidad, si quiera, de la intervención humana²⁷.

Hasta ahora hemos venido haciendo referencia a estas prácticas con el término anglosajón *deepfakes*. No obstante, en el ordenamiento jurídico español sería más conveniente denominarlas “ultrasuplantaciones”²⁸, ya que es un término que ha sido introducido recientemente en nuestro sistema jurídico a través del Reglamento de Inteligencia

²⁵ Para un estudio pormenorizado de las redes generativas antagónicas (GANs), consúltase la siguiente Tesis Doctoral: CALCAGNI, Laura Randa, *Redes generativas antagónicas y sus aplicaciones*, Tesis Doctoral, RONCHETTI, Franco (Dir.), Universidad Nacional de la Plata, Argentina, 2020. Disponible en <http://sedici.unlp.edu.ar/handle/10915/101507> [fecha de consulta: 25/08/2024].

²⁶ Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). DOUE núm. 277, de 27 de octubre de 2022, páginas 1 a 102.

²⁷ ENDARA-CHAMORRO, Ronald Estiven; ESPINOZA-JIMÉNEZ, Juan Sebastián; LÓPEZ-FUEL, Eder Ronaldo y SANTANDER-MORENO, Jessica Johanna, “Análisis Jurídico del deepfake en relación con la suplantación de identidad, Ecuador”, *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas*, Año IX, Vol. IX, Núm. 1. Edición Especial, 2024, p. 242. <https://doi.org/10.35381/racj.v9i1.3530>.

²⁸ Conviene advertir que el término que empleaba el RIA hasta su última revisión hace unos escasos meses, no era el de “ultrasuplantaciones”, sino el de “ultrafalsificaciones”. Sin embargo, en su última revisión fue modificado, entendemos, simple y llanamente, por cuestiones de traducción. Por ello, no sería extraño encontrar referencias en otros artículos doctrinales al término ultrafalsificaciones y, en realidad, se estaría refiriendo a las ultrasuplantaciones o *deepfakes*.

Artificial europeo al que ya hemos hecho referencia. Por vez primera, una norma ha regulado el concepto y el régimen jurídico de los *deepfakes*. No obstante, por el momento, únicamente vamos a señalar qué es lo que ha entendido el RIA que son las ultrasuplantaciones, puesto que de su régimen jurídico nos encargaremos posteriormente.

De este modo, al igual que sucedía con el concepto de “sistemas de IA”, el RIA contempla, igualmente en su artículo 3 (donde recoge otras 67 definiciones), el concepto de “ultrasuplantación” en los siguientes términos, concretamente en su apartado 60:

«ultrasuplantación»: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos²⁹;

Dentro del concepto de ultrasuplantación o de *deepfake*, debemos distinguir, aunque el RIA no lo haya hecho, entre dos conceptos o dos realidades que se han venido confundiendo y denominando de forma común bajo el término de *deepfake* y que comparten algunas características, pero, como veremos, no son exactamente lo mismo, y que son, por un lado, lo que acabamos de señalar que son las ultrasuplantaciones o *deepfakes* en sentido estricto, donde realmente se ven representadas personas en determinadas situaciones y, por otro lado, lo que se viene denominando, también con un anglicismo, como *fake news* o noticias falsas, es decir, lo que se viene conociendo como los bulos o la desinformación, que también son susceptibles de generar en el público en general, la confianza de que dichas noticias son veraces sin serlo, lo que ha supuesto que ahora existan los verificadores de la verdad o verificadores de noticias³⁰, es decir, personas, organizaciones o programas informáticos que se encargan de analizar si una noticia es real o si se trata de un bulo que pueda afectar a la opinión pública manipulándola.

De este modo, se podría decir que las *deepfakes* y las *fake news* son formas de desinformación digital que, aunque comparten el objetivo de engañar o manipular a la audiencia, difieren tanto en su naturaleza, como en su metodología. Mientras que las *fake news* se refieren a la difusión de información falsa o engañosa a través de textos, titulares

²⁹ En una versión anterior el concepto de ultrasuplantación iba a denominarse ultrafalsificación en el RIA en los siguientes términos: *un contenido de sonido, imagen o vídeo manipulado o sintético que puede inducir erróneamente a pensar que es auténtico o verídico, y que muestra representaciones de personas que parecen decir o hacer cosas que no han dicho ni hecho, producido utilizando técnicas de IA, incluido el aprendizaje automático y el aprendizaje profundo.*

³⁰ Las principales organizaciones, en España, que se encargan de verificar la veracidad de las noticias, actualmente, son Maldita.es, Newtral y Efe Verifica, quienes se encargan de comprobar que los datos que se difunden tanto en medios de comunicación como a través de las redes sociales y aplicaciones de mensajería sean ciertos con el objetivo de combatir los bulos y la desinformación que pueden afectar a la opinión pública. Tan solo estas tres organizaciones en España son las que están adscritas y certificadas a y por la *International Fact Checking Network* (IFCN). <https://www.ttandem.com/blog/contenidos-asi-funcionan-los-verificadores-de-noticias/> [fecha de consulta: 29/08/2024].

o noticias, que se presentan como si fueran hechos verídicos con el fin de influir en la opinión pública o generar confusión³¹, las *deepfakes*, por su lado y como hemos tenido ocasión de señalar, son contenidos audiovisuales manipulados mediante IA que alteran de manera realista la apariencia, voz o acciones de una persona, creando situaciones que nunca ocurrieron. Así, mientras que las *fake news* se centran en distorsionar la realidad a través de palabras, las *deepfakes* lo hacen mediante imágenes y sonidos mediante IA, aumentando así su capacidad de persuasión y el desafío para su detección y control.

2.2.1. Uso de los *deepfakes*

Una vez hemos definido lo que son los *deepfakes* o ultrasuplantaciones y su distinción con las *fake news*, es conveniente hacer una breve revisión de los tipos o modelos de *ultrasuplantaciones* más empleados por los sistemas de IA, no sin antes hacer una alusión a los actores que intervienen en un *deepfake* a lo largo de su ciclo de vida³². En este sentido, durante ese ciclo de vida, intervienen seis actores: a) la víctima, cuya imagen física o voz es empleada para generar el contenido falso; b) el autor o productor del *deepfake*; c) la audiencia o los destinatarios del contenido falso, que podrían ser engañados o manipulados por diversas finalidades; d) el proveedor de la tecnología, es decir, el desarrollador responsable del software o servicio prestado que ha hecho posible la creación del *deepfake*; e) la plataforma en línea que proporciona el medio o soporte empleado por sus usuarios para alojar y difundir los *deepfakes*; y f) los propios usuarios de la plataforma en línea³³.

En relación con los tipos de *deepfakes*, ultrasuplantaciones y sistemas de IA que se emplean para la creación de aquellos, existen cientos de modelos y softwares, pero, en lo que nos atañe en el presente estudio, nos gustaría señalar las siguientes:

Face Swapping: es una técnica de manipulación digital que permite intercambiar el rostro de una persona en una imagen o video con el rostro de otra persona. Utilizando algoritmos avanzados de inteligencia artificial (GANs), esta técnica logra que el nuevo rostro se integre de manera realista con las expresiones faciales, movimientos y características del cuerpo de la persona original. Muchas redes sociales, como *TikTok* o *Instagram*, ya utilizan estos filtros. Además, ya existen numerosas aplicaciones que permiten emplear estos sistemas de IA³⁴.

³¹ AYLLÓN GARCÍA, Jesús Daniel, “La Inteligencia Artificial como medio... cit., p. 221.

³² Con ciclo de vida de un *deepfake* nos referimos a tres etapas concretas: la creación, el uso y la difusión de la ultrafalsificación. WESTERLUND, Mika, “The Emergence of Deepfake Technology: A Review”, *Technology Innovation Management Review*, vol. 9, issue 11, Carleton University, 2019, p. 41.

³³ GUTIÉRREZ GARCÍA, Elisa, *Inteligencia artificial y Derechos Fundamentales. Hacia una convivencia en la era digital*, Colex, A Coruña, 2024, pp. 153-154.

³⁴ Una de las aplicaciones más utilizadas, a nivel de usuario, para hacer *face swapping* es “Vidnoz Face Swapping”, que permite hacer intercambio de caras tanto en fotos, como en videos consiguiendo, en algunas ocasiones, muy buenos resultados. <https://es.vidnoz.com/face-swap.html> [fecha de consulta: 02/09/2024].

Voice Cloning: permite replicar la voz de una persona con un alto grado de precisión. A través de un pequeño fragmento de la voz original que se quiere replicar, utilizando algoritmos de aprendizaje automático, se pueden capturar las características distintivas de la voz, como el tono, la entonación y el ritmo. Una vez procesada la voz, este sistema de IA permite generar nuevas grabaciones en las que la persona parece decir cosas que nunca ha dicho, con un timbre y estilo prácticamente idénticos al original³⁵.

Lip-Sync Deepfakes: este tipo de *deepfake* manipula los movimientos labiales de una persona en un video para que coincidan con una pista de audio diferente, generando la ilusión de que está pronunciando palabras que nunca dijo³⁶.

Full-body Deepfakes: este modelo de *deepfake* implica la manipulación no sólo del rostro y la voz, como hacen los anteriores tipos de *deepfakes*, sino también de los movimientos corporales completos, creando la ilusión de que una persona está realizando acciones que nunca llevó a cabo³⁷. Esto quiere decir que, si se combinan todos los modelos anteriores, es decir, si se utilizan imágenes, videos y la voz de una persona, se pueden recrear situaciones que nunca han ocurrido al mismo tiempo que se pueden representar en lugares que nunca han estado, diciendo cosas que nunca han dicho.

Estos tipos de *deepfakes* subrayan la complejidad y el potencial de daño que tales tecnologías pueden generar en el contexto jurídico, obligando a repensar las normativas y medidas de protección ante estas formas de manipulación digital. Si tenemos en cuenta lo dicho hasta ahora sobre estas tecnologías parece que, únicamente, pueden tener usos negativos. Sin embargo, las ultrasuplantaciones, entendidas como un sistema de IA, pueden tener aplicaciones positivas y negativas que destacan tanto su potencial, como sus riesgos. Entre los usos beneficiosos, las *deepfakes* pueden emplearse en la industria del entretenimiento para recrear actores fallecidos en películas o en la publicidad, como se hizo con Lola Flores³⁸, o bien para personalizar contenidos dirigidos a distintos públicos. También pueden ser útiles en la educación y la formación, creando simulaciones realistas para entrenar a profesionales en situaciones complejas³⁹. Pero los *deepfakes* también tienen un lado oscuro, como su uso

³⁵ Un ejemplo de este sistema de IA es el ofertado por la empresa de IA *ElevenLabs*, quien ha recreado la voz de Judy Garland para leer el audiolibro de “El mago de Oz” en su nueva aplicación *Reader*. <https://cnnespanol.cnn.com/2024/07/03/ia-resucita-voces-actores-fallecidos-leer-audiolibros-trax> [fecha de consulta: 02/09/2024].

³⁶ Los ciberdelincuentes están utilizando el *Lip-Sync Deepfakes* para que famosos y famosas parezca que están promocionando productos o aplicaciones móviles. Así lo han hecho con Taylor Swift, Leo Messi o Tom Hanks. <https://www.lavanguardia.com/andro4all/tecnologia/deepfakes-de-famosos-desde-taylor-swift-sortear-sartenes-a-leo-messi-pidiendo-que-descargues-su-app> [fecha de consulta: 02/09/2024].

³⁷ Información más detallada sobre esta cuestión, puede consultarse en: <https://www.unite.ai/es/creating-full-body-deepfakes-by-combining-multiple-nerfs/> [fecha de consulta: 02/09/2024].

³⁸ Puede visionarse el anuncio de Cruzcampo donde sale Lola Flores después de muerte, recreada por IA en el siguiente enlace: <https://www.youtube.com/watch?v=Yewm6TjLZ3Q> [fecha de consulta: 02/09/2024].

³⁹ En relación con los beneficios que pueden predicarse de los sistemas de IA, es interesante consultar HUERGO LORA, Alejandro, “La Inteligencia Artificial: una aproximación jurídica

para la difusión de desinformación, la suplantación de identidad en fraudes financieros, o la creación de contenido pornográfico no consensuado⁴⁰. Estos malos usos pueden causar graves daños a la reputación, la honra, la privacidad, la protección de datos y la seguridad de las personas, entre otros Derechos Fundamentales.

3. VULNERACIÓN DE LOS DERECHOS DE LA PERSONALIDAD A TRAVÉS DE ULTRASUPLANTACIONES O *DEEPFAKES*

En atención a lo expuesto hasta ahora, podemos afirmar que el uso o la creación de imágenes, audios y/o vídeos *deepfake* plantea serios desafíos legales y éticos, ya que, como hemos señalado, pueden ser utilizados para la difusión de información engañosa, suplantación de identidad, o incluso para cometer actos delictivos, afectando a derechos fundamentales como la privacidad, la honra, y la imagen de las personas⁴¹, poniendo en riesgo, por tanto, la tutela de determinados derechos tradicionalmente englobados dentro de la categoría de los derechos de la personalidad.

Además, la opacidad de la IA hace que los sistemas algorítmicos sean difíciles de auditar y responsabilizar. Los sistemas de IA también incentivan la vigilancia y la recopilación desmesurada de datos porque necesitan enormes conjuntos de información para el entrenamiento y el funcionamiento de los modelos subyacentes. Esto favorece prácticas que invaden la intimidad y erosionan las normas de protección de datos. Por último, los sistemas de IA tienen sesgos⁴²; operan sobre la base del *corpus* de datos en el que han sido programados y, por lo tanto, los datos que están sesgados en origen, por ejemplo, según la raza, la nacionalidad, el sexo o las brechas socioeconómicas, conducirán a resultados discriminatorios en las decisiones de IA⁴³.

Por ello, ahora sí, nos vamos a detener en la manera en la que una ultrasuplantación puede afectar a determinados derechos de la personalidad, concretamente, a aquellos que afectan a la esfera más íntima y personal de las personas.

no catastrófica”, *Revista española de control externo*, núm. Extra 74-75, (Ejemplar dedicado a: *Inteligencia artificial. Gestión y control público*), pp. 119-120.

⁴⁰ AZUAJE-PIRELA, Michelle, “Deepfakes, distorsión de la realidad y desafíos jurídicos”, *Telos: Cuadernos de comunicación e innovación*, Núm. 122 (Junio), 2023 (Ejemplar dedicado a: Posverdad), pp. 126-129.

⁴¹ GARCÍA-ULL, Francisco José, “Deepfakes: el próximo reto en la detección de noticias falsas”, *Anàlisi: Quaderns de comunicació i cultura*, Núm. 64, 2021, págs. 103-120. <https://doi.org/10.5565/rev/analisi.3378>.

⁴² Para un estudio completo sobre los sesgos y la IA, consúltese: SAN MIGUEL CASO, Cristina, “Inteligencia artificial y algoritmos: La controvertida evolución de la tutela judicial efectiva en el proceso penal”, *Estudios penales y criminológicos*, núm. extra 44 (*Inteligencia artificial y sistema penal*), 2023, DOI: <https://doi.org/10.15304/epc.44.8859>; y SAN MIGUEL CASO, Cristina, “Reflexiones sobre la prevención y mitigación de los sesgos en los sistemas inteligentes”, ARRABAL PLATERO, Paloma y CARO CATALÁN, José (Coord.), *Más allá de la Justicia: nuevos horizontes del derecho procesal*, Tirant lo Blanch, Valencia, 2024, pp. 229-242.

⁴³ MOISÉS BARRIO, Andrés, “Objeto, ámbito de aplicación y... cit., p. 26.

3.1. El derecho a la privacidad

Antes de hacer una referencia expresa a los derechos al honor, intimidad y propia imagen recogidos en el art. 18 CE conviene detenerse, brevemente, en el denominado “Derecho a la privacidad”, un término que es más propio de las esferas internacionales que de nuestro ordenamiento jurídico.

El derecho a la privacidad es el derecho “a ser dejado en paz”⁴⁴. Lo que viene a proteger este derecho es la existencia de una esfera privada a la que terceros no van a poder acceder sin el consentimiento de la persona titular del derecho. Este derecho genérico integra a otros derechos autónomos como son el derecho al honor, el derecho a la intimidad, el derecho a la propia imagen o el derecho a la protección de datos; y, su fundamento no es otro que la dignidad de la persona⁴⁵.

Este derecho, debido a su generalidad, queda contemplado bajo diferentes formas de expresión y extensión de su contenido, en textos internacionales y nacionales. De este modo, el art. 8 CEDH⁴⁶ establece que *toda persona tiene el derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*⁴⁷; por su parte, el art. 12 DUDH⁴⁸ 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*. El PIDCP⁴⁹ en su art. 17 afirma que *nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o reputación*. Finalmente, la CDFUE⁵⁰ establece en su art. 7 que *toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*, reconociendo, seguida-

⁴⁴ *To be let alone*, según LOUIS BRANDIES. SERRANO MAILLO, María Isabel, “Derecho al honor, intimidad, propia imagen y otros derechos colindantes”, SÁNCHEZ GONZÁLEZ, Santiago (Coord.), *Derechos y Libertades*, Universitas, 2021, pp. 301-303.

⁴⁵ DE ESTEBAN ALONSO, Jorge y GONZÁLEZ TREVIJANO SÁNCHEZ, Pedro José, *Tratado de Derecho constitucional*, Servicio de Publicaciones, Universidad Complutense de Madrid, Madrid, 2004, p. 110.

⁴⁶ Convenio para la protección de los derechos humanos y las libertades fundamentales, de 4 de noviembre de 1950. BOE núm. 243, de 10 de octubre de 1979.

⁴⁷ Sobre los posibles límites difusos entre la vida privada y familiar que contempla el convenio, puede consultarse la Tesis Doctoral de la profesora Lara Redondo, donde, en sus conclusiones presenta unas conclusiones muy interesantes de lo expuesto en el cuerpo de su reciente premiado trabajo de investigación. REDONDO SACEDA, Lara, *El derecho a la vida familiar. Del Convenio Europeo de Derechos Humanos a la Constitución Española*, Tesis Doctoral, GARCÍA ROCA, Francisco Javier (Dir.); CARMONA CUENCA, Encarnación del Rosario (Codir.), Alcalá de Henares, 2023.

⁴⁸ Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948. <https://www.un.org/es/about-us/universal-declaration-of-human-rights> [fecha de consulta: 07/09/2024].

⁴⁹ Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966. <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> [fecha de consulta: 07/09/2024].

⁵⁰ Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000. DOUE 2010/C 83/02.

mente, a toda persona *el derecho a la protección de los datos de carácter personal que la conciernan* en su art. 8.

A pesar, como acabamos de apuntar, del amplio significado de este derecho, el término de privacidad en el ámbito de la IA suele hacer referencia, principalmente, a la protección de datos personales⁵¹, puesto que gran parte de los datos con los que los sistemas de IA se alimentan son generados por los seres humanos⁵². En España, existe una estrecha interrelación entre el derecho a la protección de datos y los derechos al honor, la intimidad y la propia imagen, todos ellos amparados por la CE. Estos derechos están destinados a salvaguardar la privacidad de las personas, tanto en el ámbito personal como digital, evitando la divulgación indebida de información personal que pueda vulnerar la dignidad o reputación de los individuos. Por tanto, la protección de datos actúa como un mecanismo esencial para garantizar el respeto de estos derechos fundamentales.

En suma, si atendemos a este concepto amplio de Derecho a la privacidad, podemos concluir que el uso de sistemas de IA puede vulnerar no sólo el derecho a la protección de datos, sino también otros derechos fundamentales conexos como el honor, la intimidad y la propia imagen. Es por ello por lo que, a continuación, vamos a señalar cómo estos derechos fundamentales pueden verse afectados por el uso de la inteligencia artificial, particularmente, en el contexto de los *deepfakes* o las ultrasuplantaciones.

3.2. Especial referencia a los derechos al honor, intimidad y propia imagen

Aunque los derechos al honor, a la intimidad y a la propia imagen son, rigurosamente hablando, derechos distintos, la unificación de su tratamiento normativo en la LOPDH⁵³ y en art. 18 CE puede considerarse aceptable en la medida en que existen entre ellos numerosos nexos que hacen muy difícil diferenciar, en muchas ocasiones, los unos de los otros. En otras palabras y, según el Tribunal Constitucional⁵⁴, se puede decir que estos derechos tienen cada uno de ellos un contenido autónomo y diferenciado de los demás, pese a que exista una fuerte conexión entre los mismos. Por ejemplo, la publicación de un texto o de unas imágenes en un medio de comu-

⁵¹ FERRIOLS I SOLÁ, Antoni y FERNÁNDEZ-ALLER, Celia, “El derecho a la protección de datos de carácter personal: disposición adicional quinta de la Constitución española”, LÓPEZ GARRIDO, Diego (Coord.), *Los nuevos derechos sociales fundamentales: una propuesta de reforma constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2023, p. 153.

⁵² En este sentido el “Libro Blanco sobre la inteligencia artificial de la Unión Europea. Un enfoque europeo orientado a la excelencia y a la confianza”, destaca los riesgos que la IA puede acarrear para la protección de datos personales y a la privacidad, dentro de los derechos fundamentales.

⁵³ 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. Permalink ELI: <https://www.boe.es/eli/es/lo/1982/05/05/1/con>

⁵⁴ En este sentido STC 81/2001, de 26 de marzo, FJ 2; STC 156/2001, de 2 de julio, FJ 3; STC 46/2002, de 25 de febrero, FJ 4; STC 14/2003, de 30 de enero, FJ 4 y STC 127/2003, de 30 de junio, FJ 6.

nicación o en una red social puede lesionar al mismo tiempo el honor, la intimidad y el derecho a la propia imagen de una determinada persona o grupo de personas⁵⁵ e, incluso, podría, también al mismo tiempo, vulnerar el derecho a la protección de datos⁵⁶.

En relación con el derecho al honor⁵⁷, el mismo puede verse comprometido cuando la buena fama y la propia estima de una persona esté en entredicho. Tradicionalmente la vulneración de este derecho se revelaba a través de la manifestación de juicios de valor, ya fuese de manera oral o escrita, o por la difusión de imágenes en medios de comunicación o redes sociales hecha por una persona que pudiese menoscabar su honra. En la actualidad, el derecho al honor puede verse comprometido también cuando los sistemas de IA generen ultrasuplantaciones, manipulando imágenes, videos o audios de una persona, creando contenido que pueda dañar su reputación. Tal y como hemos expuesto anteriormente, un *deepfake* puede representar a una persona diciendo o haciendo cosas que nunca ha dicho o hecho, incluso después de su muerte, lo que puede ser altamente difamatorio atendiendo al contenido de la ultrasuplantación, pues no siempre que exista una ultrasuplantación se tiene que vulnerar el derecho al honor⁵⁸. Al tergiversar la realidad, estas tecnologías no sólo afectan a la imagen pública de una persona, sino que también pueden impactar en su dignidad y percepción ante terceros y, por ello precisamente, es por lo que se dice que se estaría vulnerando su derecho al honor, íntimamente ligado con las cualidades de dignidad y estima de terceros.

Por su parte, el derecho a la intimidad ha sido históricamente concebido como un derecho fundamental que protege la esfera privada de las personas frente a intrusiones externas⁵⁹, especialmente en un contexto social cada vez más interconectado. Tradicionalmente, la protección de este derecho era más flexible, y no siempre se

⁵⁵ DIEZ PICAZO, Luis y GULLÓN, Antonio, *Sistema de Derecho Civil, Vol. 1*, Tecnos, Madrid, 2010, p. 345.

⁵⁶ Los sistemas de IA, especialmente aquellos que dependen de grandes volúmenes de datos personales (como los *data-driven AI* a los que antes hicimos referencia), pueden vulnerar el derecho a la protección de datos personales recogido en normativas como el Reglamento General de Protección de Datos (RGPD) o la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). Concretamente, los datos biométricos y de comportamiento utilizados por los sistemas de IA (como los que permiten identificar a una persona a través de su rostro, voz o gestos), son especialmente sensibles. Estos datos, si no se gestionan con cuidado, pueden ser utilizados sin el consentimiento de las personas, lo que supone una clara vulneración de su derecho a la protección de datos de carácter personal.

⁵⁷ La vulneración del derecho al honor se puede alcanzar con manifestaciones orales o escritas sobre una persona, pero también a raíz de la divulgación de su imagen en un contexto que suponga el desmerecimiento de la consideración ajena. Así lo afirma el Tribunal Constitucional en las siguientes resoluciones: STC 223/1992, de 14 de diciembre, FJ 3; STC 170/1994, de 7 de junio, FJ 3; STC 14/2003, de 28 de enero.

⁵⁸ VEGA GARCÍA, Paula, “Protección y comercialización del derecho a la propia imagen del difunto ante la inteligencia artificial”, ARRÉBOLA BLANCO, Adrián (Dir.), *Retos del Derecho de Sucesiones del Siglo XXI. Volumen II*, Reus, Madrid, 2023, pp. 1003-1004.

⁵⁹ DIEZ PICAZO, Luis y GULLÓN, Antonio, *Sistema de Derecho... cit.* pp. 344-345.

valoraba la gravedad de las posibles injerencias, pero con el avance de la tecnología, el uso masivo de las redes sociales y la creciente exposición en los medios de comunicación y de la información, la intimidad se ha visto continuamente amenazada, lo que ha obligado a una reinterpretación más rigurosa por parte de jueces y tribunales del contenido de este derecho. Hoy en día, se concede una mayor relevancia a la necesidad de proteger la privacidad de las personas ante la exposición constante de datos personales y situaciones íntimas⁶⁰. La evolución ha estado marcada por un cambio en la postura de los tribunales, que han pasado de una interpretación más permisiva a una estricta defensa del derecho a la intimidad. Esta transformación ha sido impulsada en gran medida por la influencia de los organismos europeos, como el Tribunal Europeo de Derechos Humanos, que ha subrayado la importancia de salvaguardar la privacidad en un entorno digital⁶¹. En consecuencia, el derecho a la intimidad ha adquirido una mayor protección y es tratado con un respeto mucho más riguroso que en épocas anteriores.

Teniendo ello en cuenta, y en relación con la IA, podemos afirmar que, actualmente, los sistemas de IA que utilizan tecnologías de reconocimiento facial, monitoreo de comportamientos o análisis biométricos pueden invadir la esfera privada de una persona siempre, claro está, que recaben y/o utilicen esos datos, imágenes, voces, etc. sin el consentimiento de sus titulares. El derecho a la intimidad protege, por tanto, la vida privada y personal de los individuos y, cualquier intrusión por parte de la inteligencia artificial en este ámbito, como la recopilación no autorizada de datos personales en redes sociales, cámaras en espacios públicos (con las salvedades previstas en la ley) o incluso en el hogar, puede resultar una grave violación de este derecho. Si bien es cierto esto que se acaba de mencionar, entendemos que, en este caso concreto, el uso de un sistema de IA, mientras no haya difusión de las posibles ultrasuplantaciones que se generen, no estaría afectando tanto al derecho a la intimidad según está configurado en el art. 18 CE, sino más bien al derecho al honor en los términos que hemos señalado y al derecho a la propia imagen, en los términos que vamos a señalar ahora.

En cuanto al último derecho que nos queda de mencionar, pero no menos importante por ello, es decir, el derecho a la propia imagen, el mismo protege a las personas contra el uso no autorizado de su imagen, su voz⁶² o su nombre con fines co-

⁶⁰ GARCÍA MARCOS, Julián, “Hacia una exclusiva reserva jurisdiccional en la protección del derecho a la intimidad”, *Actualidad Civil*, núm. 4, LA LEY, 2024 (LALEY 15717/2024).

⁶¹ Sentencia del Tribunal Europeo de Derechos Humanos Marper c. Reino Unido, de 4 de diciembre de 2008; y Sentencia del Tribunal Europeo de Derechos Humanos, caso G.B.S c. Suiza, de 22 de diciembre de 2015; entre otras.

⁶² Si bien el derecho a la imagen está claramente delimitado y considerador como un derecho autónomo de la personalidad, la consideración de la voz como un derecho autónomo es más debatida en la doctrina, aunque recientes desarrollos jurisprudenciales y doctrinales han reconocido su importancia dentro de los derechos de la personalidad. AMMERMAN YEBRA, Julia, *El derecho a la propia voz como derecho de la personalidad*, Colex, A Coruña, 2021, p. 236; En el mismo sentido, la Sentencia del Tribunal Constitucional núm. 117/1994, de 25 de abril (RTC 1994/117).

merciales o análogas de otro tipo⁶³. El uso de las ultrasuplantaciones también plantea serios problemas respecto a este derecho, al igual que sucede con los anteriormente tratados. Este derecho es, por tanto, vulnerable ante las manipulaciones tecnológicas. Ya hemos señalado como los *deepfakes* permiten la alteración o creación de imágenes y voces de una persona sin su consentimiento, generando representaciones falsas, pero extremadamente realistas, lo que puede llevar a una intromisión ilegítima de este derecho siempre que la imagen, la voz o el nombre no se utilicen con el correspondiente consentimiento preceptivo. Esto puede suceder en contextos como publicidad, medios de comunicación o entretenimiento, donde el rostro o cuerpo de una persona es utilizado sin autorización, afectando su control sobre cómo se representa públicamente su figura o sobre cómo se utiliza su voz.

En este contexto y tal y como hemos ido señalando, el uso de las ultrasuplantaciones puede suponer no sólo una violación del derecho a la imagen y la voz, sino también una afectación indirecta al derecho al honor, al asociar a una persona con acciones o declaraciones que nunca realizó.

Pero ¿dónde están reguladas estas intromisiones ilegítimas al derecho al honor, a la intimidad y a la propia imagen? Dichas intromisiones están recogidas en los artículos 7 y 8 LOPDH, donde se recogen una serie de supuestos que se consideran intromisiones ilegítimas. La cuestión es si se pueden considerar intromisiones ilegítimas cuando los supuestos contemplados en dichos preceptos son fruto de una creación hecha por un sistema de IA, es decir, cuando la vulneración del derecho en cuestión se hace a través de una ultrasuplantación o *deepfake*.

La respuesta ha de ser afirmativa en tanto en cuando la norma, adelantándose a los posibles avances tecnológicos, utiliza expresiones tales como “o de cualquier otro medio” (arts. 7.1 y 2); y “o cualquier otro procedimiento”; expresiones que abarcan, si hacemos uso del criterio hermenéutico de la interpretación sociológica, el uso de sistemas de IA. De este modo, si la manifestación de juicios de valor que lesionen la dignidad de la persona, o el uso de imágenes o de la voz de una persona, o la revelación de datos privados de una persona, se hace a través de una ultrasuplantación, se considerará intromisión ilegítima, ya que dichas expresiones (“o de cualquier otro medio” y “o cualquier otro procedimiento”) hacen que los casos contemplados en la norma no sean taxativos, sino *numerus apertus*. Sin embargo, no podemos olvidar que la normativa reguladora de estos derechos de la personalidad data del año 1982 y que sería necesaria una actualización de la misma. Por ello, podemos afirmar que el régimen jurídico actual, aunque avanzado, debe seguir desarrollándose para abordar de manera efectiva estas nuevas vulneraciones en el entorno digital; cuestión que, como se apuntará en el siguiente apartado, está siendo abordada por los legisladores tanto internacionales como nacionales.

En suma, podemos concluir este apartado afirmando que la IA, si bien es una herramienta poderosa y puede ser muy beneficiosa en muchos ámbitos, plantea desafíos significativos en términos de protección de los derechos fundamentales, con-

⁶³ DIEZ PICAZO, Luis y GULLÓN, Antonio, *Sistema de Derecho... cit.* p. 345.

cretamente, como hemos visto, en materia de algunos derechos de la personalidad. Para mitigar estos riesgos, es esencial que los marcos regulatorios se adapten y promuevan una transparencia, control humano y supervisión adecuada, garantizando que estas tecnologías no se utilicen de manera que puedan vulnerar los derechos al honor, la intimidad, la imagen y la protección de datos de las personas y, precisamente, sobre estas cuestiones, son las que nos vamos a detener a continuación, tratando de dilucidar si la normativa actual garantiza suficientemente la protección de estos derechos ante la llegada de la IA a nuestras vidas.

4. REGULACIÓN DE LAS ULTRASUPLANTACIONES O DEEPFAKES EN EL MARCO EUROPEO Y ESPAÑOL

Hasta ahora hemos señalado que los sistemas de IA pueden traer importantes inconvenientes en la esfera más íntima de las personas: hemos señalado como pueden afectar a la normativa de protección de datos (la privacidad), así como a otros derechos fundamentales (honor, intimidad o propia imagen). Es por ello, por lo que la doctrina, en todos los sistemas jurídicos, se está encargando de juridificar la inteligencia artificial y establecer garantías en sus herramientas, especialmente cuando atentan o menoscaban los derechos fundamentales.

A continuación, vamos a analizar la normativa aplicable en esta materia en nuestro ordenamiento jurídico; tanto la que viene de instancias supranacionales como aquellas normas de carácter nacional que se están tramitando para tratar de, como señalábamos, juridificar la IA.

4.1. Reglamento de Inteligencia Artificial

Desde el ámbito supranacional, la normativa en relación con los ultrasuplantaciones nos viene impuesta por la Unión Europea, concretamente por el Reglamento de Inteligencia Artificial (RIA), conocido coloquialmente como “Ley de Inteligencia Artificial”.

Es importante señalar (únicamente con el propósito de contextualizar dicha normativa puesto que el denominado “paquete sobre la Ley de Servicios Digitales” al que se va a hacer referencia ahora se extralimita del objeto de este estudio), que el RIA forma parte de un marco jurídico más amplio en el que han sido aprobados recientemente otros instrumentos jurídicos que caminan en la misma dirección. Nos referimos al RGPD, que entró en vigor en un primer momento y que fue seguido de la Ley de Servicios Digitales⁶⁴ (DSA) y la Ley de Mercados Digitales⁶⁵ (DMA)⁶⁶. Es

⁶⁴ Reglamento de Ejecución (UE) 2023/1201 de la Comisión de 21 de junio de 2023 relativo a las disposiciones detalladas para la tramitación de determinados procedimientos por parte de la Comisión con arreglo al Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo.

⁶⁵ Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828.

⁶⁶ La Ley de Servicios Digitales y la Ley del Mercado Digital constituyen un conjunto único de normas que se aplican en toda la UE y tienen dos objetivos principales: a) Crear un espacio digital

por ello que, aunque en este estudio nos vayamos a centrar en el RIA, no podemos olvidarnos de la existencia de estas normas y de la interrelación que existe entre las mismas. Sin embargo, para el análisis objeto de este estudio no es necesario profundizar en las mismas, por lo que nos vamos a circunscribir a lo previsto en el RIA en relación con los Derechos Fundamentales.

4.1.1. Los derechos fundamentales en el RIA

En este apartado no vamos a analizar en profundidad el RIA, pues no es el objetivo de este estudio, sino que nos centraremos en cómo ha abordado la protección de los derechos sobre los que nos hemos detenido con anterioridad y, sobre todo, en cómo regula las ultrasuplantaciones. No obstante, sí que es necesario hacer una brevísimas referencia de cuál ha sido, a nuestro parecer, el objetivo del RIA.

Se podría decir que su objetivo principal es establecer un marco jurídico uniforme para el desarrollo, comercialización y uso de sistemas de IA en la Unión Europea, promoviendo una IA respetuosa con el ser humano y con sus derechos fundamentales⁶⁷. De este modo, el legislador europeo trata, con esta norma, de garantizar un alto nivel de protección de los derechos fundamentales, sobre todo de aquellos a los que hemos podido hacer referencia en las páginas precedentes, como, por ejemplo, la privacidad o la intimidad, la propia imagen, la protección de datos, así como otros derechos fundamentales tales como la no discriminación, la salud y la seguridad pública.

El RIA, para ello, adopta un enfoque basado en riesgos⁶⁸, imponiendo obligaciones más estrictas a los sistemas de IA que ha denominado de alto riesgo (art. 6 RIA y su Anexo III), prohibiendo ciertas prácticas consideradas como inaceptables (art. 5 RIA y Anexo II RIA)⁶⁹, y estableciendo mecanismos de transparencia (art. 13 y 50.4 RIA) y supervisión (art. 14 RIA). Además, promueve la innovación (art. 53 RIA), apoyando el desarrollo de tecnologías de IA en consonancia con los valores de la UE. Por último, también hace referencia a un régimen sancionador donde contempla un catálogo de

más seguro en el que se protejan los derechos fundamentales de todos los usuarios de servicios digitales; y b) Establecer unas condiciones de competencia equitativas para fomentar la innovación, el crecimiento y la competitividad, tanto en el mercado único europeo como a escala mundial.

⁶⁷ Sobre el tratamiento humano de la IA y la necesidad de un control sensible de la IA *Vid.* PONCE SOLÉ, Juli, “Reserva de humanidad y supervisión humana de la Inteligencia artificial”, *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, (Ejemplar dedicado a: *Inteligencia artificial y derecho*), 2022, pp. 58-67.

⁶⁸ El marco regulatorio del RIA sigue un enfoque basado en riesgos, lo que significa que se establecen diferentes niveles de obligaciones y requisitos en función del riesgo que un sistema de IA represente para los derechos fundamentales.

⁶⁹ Se establecen prohibiciones claras para el uso de ciertos sistemas de IA que, por su naturaleza, son considerados inaceptables. Por ejemplo, se prohíben los sistemas de IA que manipulen el comportamiento humano de manera que puedan causar perjuicios significativos, así como aquellos que permitan la categorización biométrica basada en datos sensibles como la raza, la orientación sexual o las creencias religiosas. MIGUEZ MACHO, Luis y TORRES CARLOS, Marcos, “Sistemas de IA prohibidos y sistemas de IA de alto riesgo”, BARRIO ANDRÉS, Moisés (Dir.) *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 49-86.

sanciones divididas en tres categorías: muy graves, graves y leves⁷⁰, dejando parte de la regulación de dichas sanciones en manos de los legisladores estatales.

En suma, el propósito del RIA es proporcionar seguridad jurídica mediante un marco unificado *ex ante* aplicable a todos los sistemas de IA puestos en el mercado de la UE y lo hace en atención al grado de riesgo que presenta cada sistema para la salud, la seguridad y los derechos fundamentales de los ciudadanos⁷¹.

Ahora sí, una vez determinado cuál es el objetivo que perseguía el legislador europeo con la elaboración del RIA, es el momento de determinar cómo aborda la protección de algunos de los derechos fundamentales que hemos analizado anteriormente en relación con las ultraplantaciones.

Lo primero que debe señalarse es que el RIA no hace una referencia expresa al derecho al honor tal y como sí hace con el derecho a la intimidad y protección de datos y con el derecho a la propia imagen. Lo que sí hace, como ya hemos tenido ocasión de señalar, es referirse de manera general a la protección de los derechos fundamentales y a las vías de recurso para las personas cuyos derechos, incluyendo según entendemos el derecho al honor, puedan verse afectados por el uso de sistemas de inteligencia artificial. En particular, en el considerando 171 menciona que las personas deben tener derecho a obtener una explicación cuando una decisión basada en sistemas de IA de alto riesgo produzca efectos significativos en su salud, seguridad o derechos fundamentales, lo que entendemos que implica un reconocimiento de la protección contra posibles daños a la dignidad y reputación de las personas y, por ende, al derecho al honor.

Por el contrario, a quien sí dedica una mención expresa es al derecho a la intimidad y al derecho a la protección de datos, cuya tutela la considera como esencial en el contexto de la IA, concretamente en sus considerados 69 y 70, respectivamente. De este modo, en el considerando 69 se apunta que el derecho a la intimidad y a la protección de datos personales debe garantizarse durante todo el ciclo de vida de los sistemas de IA⁷² y, para ello, se deben aplicar principios como el de la minimización de datos y la protección de datos desde el diseño y por defecto, conforme al Derecho de la UE en materia de protección de datos⁷³. Por su parte, el considerando 70 dispo-

⁷⁰ El régimen sancionador del RIA se recoge en tres preceptos: a) el art. 99 RIA regula un régimen sancionador general; b) el art. 100 RIA hace referencia a un régimen sancionador específico para la propia Administración de la UE cuya competencia se atribuye al Supervisor Europeo de Protección de Datos (SEPD); y, c) el art. 101 RIA se refiere a un régimen sancionador específico para los proveedores de modelos de IA de uso general cuya competencia se atribuye a la Comisión Europea. DELGADO MARTÍN, Joaquín, “Régimen sancionador”, BARRIO ANDRÉS, Moisés (Dir.), *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 201-217.

⁷¹ BARRIO ANDRÉS, Moisés, “Objeto, ámbito de aplicación... cit. p. 30.

⁷² CASTILLA BAREA, Margarita, “Vigilancia postcomercialización, códigos de conducta y directrices”, BARRIO ANDRÉS, Moisés (Dir.), *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 139-200.

⁷³ Las medidas para garantizar estos principios pueden, según el considerando 69 RIA, incluir la anonimización, el cifrado y el uso de tecnologías que permitan entrenar sistemas de IA sin necesidad de transmitir datos brutos.

ne que los proveedores de sistemas de IA de alto riesgo podrán tratar datos personales sensibles, siempre que sea estrictamente necesario para detectar y corregir sesgos en los sistemas, y se cumplan las garantías adecuadas para proteger los derechos y libertades fundamentales atendiendo a la normativa europea en la materia, especialmente al RGPD.

Por último, también hace mención expresa de la protección del derecho a la imagen como derecho fundamental de las personas, cuyo análisis abordaremos a continuación y de forma separada por ser el que está más relacionado con el uso de las ultrasuplantaciones.

4.1.2. Las ultrasuplantaciones en el RIA

Como ya apuntamos cuando analizamos el concepto de ultrasuplantación, el RIA introduce dicho término en el art 3, apartado 60 en los siguientes términos:

«ultrasuplantación»: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos.

Además de su concepto, también prevé en su considerando 134 y en su artículo 50.4 algunas directrices sobre transparencia para los proveedores de sistemas de IA cuando creen ultrasuplantaciones, estableciendo que los proveedores y los responsables del despliegue de sistemas de IA que generen o manipulen contenido audiovisual deberán garantizar que el público general sea consciente de que dicho contenido ha sido generado o manipulado por sistemas de IA, es decir, que deberá de constar de manera clara que la ultrasuplantación es una imagen, video o voz (o combinación de todas ellas) manipulada por un sistema de IA⁷⁴. Esta transparencia es esencial para proteger el derecho a la imagen de las personas, evitando que sean representadas de manera falsa o manipulada sin su consentimiento⁷⁵. De hecho, ya Instagram, por ejemplo, cuando se publica una foto o una *storie* presenta la opción (que no debería de ser una opción sino algo automático y preceptivo) de marcar que ha sido creada por un sistema de IA⁷⁶, dando así cumplimiento a esta normativa.

⁷⁴ El RIA en su art. 50.4 establece que *esta obligación no se aplicará cuando la ley autorice su uso para detectar, prevenir, investigar o enjuiciar delitos*. Además, prosigue afirmando que *cundo el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos, las obligaciones de transparencia establecidas en el presente apartado se limitarán a la obligación de hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra*.

⁷⁵ Por tanto, podría decirse que los sistemas de IA deben ser diseñados y utilizados de manera que respeten la autonomía humana, lo que incluiría la necesidad de obtener el consentimiento expreso de las personas antes de usar sistemas de IA que puedan afectar su imagen o intimidad.

⁷⁶ <https://comsentido.es/etiquetar-contenido-con-ia-en-instagram/> [fecha de consulta: 21/09/2024].

En suma, el RIA regula el derecho a la propia imagen principalmente en relación con la manipulación de contenido audiovisual generado por IA, esto es, en relación con las ultrasuplantaciones.

Se establecen en este sentido, y tal y como se acaba de apuntar, obligaciones de transparencia para los responsables que utilicen sistemas de IA para crear o modificar imágenes, audio o video de manera que se asemejen a personas reales. Específicamente, hemos señalado que deben informar clara e inequívocamente que el contenido ha sido creado o manipulado artificialmente para evitar confusión sobre su autenticidad y proteger así el derecho a la propia imagen de las personas afectadas.

Por lo tanto, se puede concluir este apartado con la siguiente premisa: el RIA busca garantizar que la utilización de sistemas de IA en la sociedad no comprometa los derechos fundamentales, estableciendo un equilibrio entre la innovación tecnológica y la protección de los derechos fundamentales, especialmente en relación con el derecho a la protección de datos, a la intimidad y a la imagen de las personas. O lo que es lo mismo y en palabras de PLAZA PENADÉS, *el diseño técnico y jurídico de los sistemas de inteligencia artificial debe tener en cuenta que los derechos fundamentales prevalecen sobre la tecnología*⁷⁷.

4.2. Normativa en tramitación en el ordenamiento jurídico español

Con origen estatal, aparte de la LOPDH a la que antes se hizo referencia y sobre la que concluimos que tenían cabida las ultrasuplantaciones como una posible intromisión ilegítima de los derechos al honor, intimidad y propia imagen en los términos que ya han sido señalados, no disponemos de una normativa en vigor que regule las ultrasuplantaciones (aparte del RIA).

No obstante, se están tramitando dos normas que hacen alusión a las ultrasuplantaciones o *deepfakes* sobre las que nos vamos a detener, muy brevemente, a continuación.

En primer lugar, hay que mencionar la Proposición de Ley Orgánica 122/000073, de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, de 22 de marzo de 2024, presentada por el Grupo Parlamentario Plurinacional SUMAR⁷⁸. En dicha Proposición se plantea reformar, entre otras normativas, la LOPDH en su apartado 7, donde se contienen las intromisiones ilegítimas para incluir de manera expresa una referencia a las intromisiones ilegítimas que tienen su origen en lo que hemos venido denominado ultrasuplantaciones, aunque en dicha Proposición en la exposición de motivos, se sigue aludiendo

⁷⁷ PLAZA PENADÉS, Javier, “Claves del futuro Reglamento (Ley) de Inteligencia Artificial de la UE”, *Dossier: Las claves de la futura Ley de Inteligencia Artificial Europea*, Aranzadi La Ley, 2023, pp. 8-18. Disponible su descarga en <https://www.aranzadilaley.es/dossier/claves-futura-ley-inteligencia-artificial-europea.html> [fecha de consulta: 20/09/2024].

⁷⁸ Dicha proposición de Ley Orgánica tiene su origen en la Proposición de Ley Orgánica 122/000011, de 13 de octubre de 2023, con el mismo nombre que la 122/000073 y propuesta por el mismo Grupo Parlamentario que fue retomada en 2024.

a esta realidad como *deepfakes* o *videos hiperrealistas*⁷⁹. El pretendido apartado 9 de ese artículo 7 LOPDH dispondría lo siguiente:

9. La difusión y utilización de imágenes y vídeos de personas o audios de voz generados a través de sistemas automatizados, software, algoritmos o mecanismos de inteligencia artificial 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 inteligencia artificial. La advertencia deberá figurar sobreimpresa y legible en la propia imagen. Para el caso de los audios de voz deberá realizarse una advertencia audible antes y después de su difusión.

A este respecto, nos gustaría hacer una puntualización. Si bien consideramos acertado que se pretenda dicha modificación para reconocer de manera expresa el uso de la tecnología *deepfake* como una forma de intromisión ilegítima y que no sea necesario acudir a una interpretación forzada de la norma, también consideramos que presenta algunas deficiencias. De este modo, parece considerar que la intromisión dejará de ser ilegítima si consta que la imagen o la voz han sido generadas por un sistema de IA, lo que supondría que la propia imagen y la voz no son merecedoras de tutela *per se*⁸⁰. ¿A caso si consta que mi imagen o mi voz han sido manipuladas por un sistema de IA y yo no he prestado mi consentimiento para su uso no se está vulnerando mi derecho a la propia imagen? Es simplemente una cuestión que habría que revisar si la tramitación de esta norma sigue adelante, pues está claro que sí es una vulneración del derecho a la propia imagen en tanto en cuando se está utilizando mi imagen, sea manipulada o no y conste o no dicha manipulación, sin mi consentimiento.

En segundo lugar, otra norma también en proceso de tramitación embrionario sería el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales⁸¹ que, en este caso, hace referencia a las “ultrafalsificaciones”⁸² en el ámbito penal, proponiendo un art. 173 bis con el siguiente contenido:

Se impondrá la pena de prisión de uno a dos años a quienes, sin autorización de la persona afectada y con ánimo de menoscabar su integridad moral, difundan, exhiban o cedan su imagen corporal o audio de voz generada, modificada o

⁷⁹ Se define en la Exposición de Motivos a los *deepfakes* como *piezas visuales, auditivas o audiovisuales que simulan la realidad y que consiguen generar falsas imágenes y/o voces de personas. Es una tecnología que se basa en la inteligencia artificial y el Machine Learning que logra, con una apariencia hiperrealista, simular acciones realizadas por parte de dichas personas.*

⁸⁰ En el mismo sentido, TRUJILLO CABRERA, Carlos, “El derecho a la propia imagen (y la voz) frente a la inteligencia artificial, *InDret*, 1, 2024, p. 95.

⁸¹ Puede consultarse el texto íntegro en <https://www.mpr.gob.es/servicios/participacion/audienciapublica/Paginas/TAIP%202024/anteproyecto-de-ley-org-nica-para-la-proteccion-de.aspx> [fecha de consulta: 21/09/2024].

⁸² Se entiende que se hace referencia a los *deepfakes* con el término ultrafalsificaciones porque así lo contemplaba el RIA antes de su última modificación cuando, finalmente, se optó por el término ultrasuplantaciones, por lo que, en una versión posterior, este Anteproyecto de Ley Orgánica, debiera hacer referencia a los *deepfakes* como ultrasuplantaciones.

recreada mediante sistemas automatizados, software, algoritmos, inteligencia artificial o cualquier otra tecnología, de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorias.

Se aplicará la pena en su mitad superior si dicho material ultrafalsificado se difunde a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías, de modo que aquel se hiciera accesible a un elevado número de personas en el espacio virtual.

En el Anteproyecto, por tanto, se contempla específicamente el tratamiento penal de las ultrafalsificaciones (las denominadas ultrasuplantaciones por el RIA) a través de la introducción de ese nuevo artículo 173 bis, en el Código Penal. Dado que estas ultrasuplantaciones se difunden habitualmente en el entorno digital, lo que implica una persistencia potencial del contenido, se incrementa su peligrosidad en comparación con otras formas de intromisión, debido a la gran dificultad de distinguir entre el contenido auténtico y el manipulado. Desde un punto de vista técnico, se ha optado por sancionar la difusión de *deepfakes* pornográficos o especialmente degradantes en el marco de los delitos contra la integridad moral. Esto se justifica por la afectación no sólo a la autoestima y la percepción externa de la persona, sino también por la cosificación e instrumentalización de la víctima, que en la mayoría de los casos son mujeres, niñas, niños y jóvenes, quienes son tratados como meros objetos de consumo.

Otra de las medidas que propone este Anteproyecto para paliar los efectos de las ultrasuplantaciones es la eliminación de los contenidos que puedan vulnerar los derechos fundamentales de las personas en atención lo dispuesto en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Los responsables de las plataformas, se prevé, tendrán que retirar o eliminar los ultrasuplantaciones que vulneren cualquier tipo de derecho.

4.3. Tutela de los derechos al honor, intimidad y propia imagen vulnerados mediante ia en el ordenamiento jurídico español

Para la protección judicial de los derechos al honor, intimidad y propia imagen vulnerados mediante ultrasuplantaciones en España, existen varios mecanismos.

En primer lugar, el RIA impone obligaciones de transparencia a los sistemas de IA de alto riesgo, como los *deepfakes*, y exige que estos contenidos lleven advertencias claras sobre su naturaleza artificial, lo cual sirve de complemento a la tutela judicial en casos de afectación de derechos fundamentales como la imagen o el honor.

En segundo lugar, está el siempre presente procedimiento preferente y sumario del artículo 53.2 CE que es un mecanismo procesal diseñado para proteger de forma ágil y eficaz los derechos fundamentales y libertades públicas reconocidos en los artículos 14 a 29 CE, entre ellos los derechos al honor, intimidad y propia imagen. Este procedimiento se caracteriza por su rapidez y preferencia en los tribunales, lo que permite reducir plazos procesales y priorizar el caso frente a otros asuntos, bus-

cando evitar que una resolución judicial tardía agrave la vulneración del derecho en cuestión⁸³.

En tercer lugar, la ya citada LOPDH, pese a no hacer alusión expresa a los sistemas de IA, ya señalamos que emplea la expresión “o de cualquier otro medio” y “o cualquier otro procedimiento”, por lo que también en estos supuestos permite a las personas afectadas solicitar medidas civiles para la cesación de la intromisión ilegítima y la indemnización por daños y perjuicios causados. Los procedimientos judiciales para ejercer esta tutela pueden ser preventivos o reactivos. De ese modo, la persona afectada puede interponer una acción de cesación (art. 9 LOPDH) para frenar la difusión de un *deepfake* y prevenir nuevos actos que perjudiquen sus derechos. También puede solicitar la remoción del contenido de plataformas o redes sociales mediante un procedimiento de medidas cautelares, lo cual es particularmente útil en el entorno digital por la rapidez que se requiere.

Por último, además de la acción civil, en el ámbito penal se contempla la posibilidad de denunciar estos actos como delitos de injurias o calumnias (art. 208 y 205 CP, respectivamente)⁸⁴. Estos procedimientos están respaldados por la pretendida reforma del Código Penal que tipifica la difusión de contenido falso no consentido, proporcionando protección específica a las víctimas de *deepfakes*.

En conjunto, estas normativas y procedimientos facilitan una protección amplia y articulada en el ámbito judicial, garantizando el resguardo efectivo de los derechos de la personalidad ante vulneraciones por ultrasuplantaciones.

5. CONCLUSIONES

El desarrollo de la IA, y en particular de los *deepfakes* o ultrasuplantaciones, plantea retos significativos para la protección de los derechos de la personalidad, especialmente el honor, la intimidad y la propia imagen, así como el derecho a la protección de datos. La capacidad de estas tecnologías para manipular de manera hiperrealista la apariencia, el comportamiento y la voz de las personas genera graves riesgos para la dignidad y la reputación de los individuos afectados. Tras la realización de este estudio se ha llegado a las conclusiones que se exponen a continuación.

En primer lugar, el estudio ha demostrado que la normativa vigente, tanto a nivel comunitario como nacional, es insuficiente para abordar la complejidad y el impacto de los *deepfakes*. Aunque el Reglamento Europeo de Inteligencia Artificial y las propuestas legislativas en España avanzan en la regulación de estas prácticas, todavía es necesario profundizar más en esta regulación y, sobre todo, llevar a térmi-

⁸³ CONGRESO DE LOS DIPUTADOS, *Sinopsis del artículo 53 de la Constitución española*. Disponible en https://app.congreso.es/consti/constitucion/indice/imprimir/sinopsis_pr.jsp?art=53&tipo=2 (fecha de consulta: 20/10/2024).

⁸⁴ LOZANO SEDEÑO, Antonio, *Delito de injurias y calumnias: protección y regulación legal en España*, 2024. Disponible en <https://www.jlabogados.es/delito-injurias-calumnias/#:~:text=El%20delito%20de%20injurias%20consiste,temerario%20desprecio%20hacia%20la%20verdad.> (fecha de consulta: 22/10/2024).

no la normativa nacional que está en tramitación al mismo tiempo que han de homogeneizarse los términos empleados en ambos ámbitos (comunitario y nacional) y así unificar conceptos y cuestiones terminológicas.

En segundo lugar, resulta imperativo cumplir con las obligaciones específicas de transparencia y consentimiento previstas en el RIA en el uso de tecnologías que generen o manipulen contenido audiovisual. Es fundamental que cualquier uso de estas tecnologías se realice con el consentimiento explícito de las personas afectadas y que se implementen mecanismos de información claros para evitar la confusión o engaño del público, es decir, que cada vez que se genere una imagen, video o voz mediante un sistema de IA quede suficientemente claro que así se ha hecho. En este sentido, entiendo que las plataformas digitales deben asumir una mayor responsabilidad en la detección y eliminación de contenido *deepfake* que vulnere los derechos de la personalidad, en la línea que parece indicar que se desarrollará en nuestro ordenamiento jurídico según el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. Hasta que esa normativa nacional llegue a término, no obstante, no podemos negar que la tutela judicial de la vulneración de los derechos al honor, la intimidad y la propia imagen por ultrasuplantaciones queda amparada por los mecanismos vigentes en el ordenamiento jurídico español, ya sea por el procedimiento sumario previsto en el art. 53.2 CE para la tutela de los derechos fundamentales, ya sea a través de las medidas específicas previstas en la LOPDH que, como ya se ha mencionado, contempla las ultrasuplantaciones como un medio para cometer conductas ilegítimas, ya sea a través de la acción penal, cuando sea pertinente.

En tercer lugar, es imprescindible también reforzar la protección penal frente al uso indebido de *deepfakes*, especialmente en contextos que involucren la suplantación de identidad con fines delictivos o la creación de contenido pornográfico no consentido. La introducción de sanciones específicas para estas conductas en el ordenamiento jurídico español, como se propone en el Anteproyecto de Ley Orgánica, representa un paso positivo, pero debe complementarse con una mayor concienciación social y formación en materia de ciberseguridad y protección de datos.

Otro aspecto que se considera relevante es, precisamente, la necesidad de fomentar una cultura de responsabilidad digital y protección de datos. La sociedad debe ser consciente de los riesgos asociados al uso indebido de estas tecnologías y conocer sus derechos y mecanismos de defensa ante posibles vulneraciones. En este sentido, es fundamental promover programas de educación y sensibilización que orienten a los ciudadanos sobre el correcto uso de las herramientas digitales y los peligros de los *deepfakes*.

Finalmente, es necesario avanzar hacia una regulación coordinada a nivel europeo e internacional. La naturaleza global de estas tecnologías requiere una cooperación estrecha entre Estados y organizaciones para establecer estándares mínimos de protección y sanciones efectivas contra el uso indebido de los *deepfakes* y no dejar parte de la regulación de las sanciones en manos de cada Estado, creando así una disparidad de medidas sancionadoras dependiendo del territorio donde se generen o

difundan las ultrasuplantaciones. Solo mediante un esfuerzo conjunto y la adopción de medidas legales, tecnológicas y educativas se podrá garantizar una protección adecuada de los derechos de la personalidad en el entorno digital.

En suma, es fundamental que los desarrollos normativos se adapten rápidamente a las innovaciones tecnológicas, asegurando que los avances en IA se integren en la sociedad de manera ética y respetuosa con los derechos fundamentales de todas las personas, tal y como entendemos que predica el RIA.

6. BIBLIOGRAFÍA

- AMMERMAN YEBRA, Julia, *El derecho a la propia voz como derecho de la personalidad*, Colex, A Coruña, 2021.
- AYLLÓN GARCÍA, Jesús Daniel, “La Inteligencia Artificial como medio de control y difusión de las *Fake News*”, VILLEGAS DELGADO, César y MARTÍN RÍOS, Pilar (Dir.), *El Derecho en la encrucijada tecnológica: estudios sobre Derechos Fundamentales, nuevas tecnologías e Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2022, pp. 217-239.
- AYLLÓN GARCÍA, Jesús Daniel, “La Inteligencia Artificial como medio para administrar justicia”, BUENO DE MATA, Federico (Dir.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Editorial Comares, 2020, pp. 3-14.
- AZUAJE-PIRELA, Michelle, “Deepfakes, distorsión de la realidad y desafíos jurídicos”, *Telos: Cuadernos de comunicación e innovación*, Núm. 122 (Junio), 2023 (Ejemplar dedicado a: Posverdad), pp. 126-129.
- BAÑUELO CAPISTRÁN, Jacob, “Evolución del deepfake: campos semánticos y géneros discursivos (2017-2021)”, *Icono 14: Revista científica De Comunicación Y Tecnologías Emergentes*, Vol. 20, núm. 1, (Ejemplar dedicado a: Niños y jóvenes ante los dispositivos: Nuevos fenómenos comunicativos y nuevos creadores de producto), 2022. <https://doi.org/10.7195/ri14.v20i1.1773>.
- CALCAGNI, Laura Randa, *Redes generativas antagónicas y sus aplicaciones*, Tesis Doctoral, RONCHETTI, Franco (Dir.), Universidad Nacional de la Plata, Argentina, 2020. Disponible en <http://sedici.unlp.edu.ar/handle/10915/101507> [fecha de consulta: 25/08/2024].
- CASTILLA BAREA, Margarita, “Vigilancia postcomercialización, códigos de conducta y directrices”, BARRIO ANDRÉS, Moisés (Dir.), *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 139-200.
- CHURNIN, Stephen, *Inteligencia Artificial: retos éticos y jurídicos, y la influencia de los Derechos Humanos*, Servicio de Publicaciones de la Universidad Complutense de Madrid, 2011.
- DE ESTEBAN ALONSO, Jorge y GONZÁLEZ TREVIJANO SÁNCHEZ, Pedro José, *Tratado de Derecho constitucional*, Servicio de Publicaciones, Universidad Complutense de Madrid, Madrid, 2004.

- DELGADO MARTÍN, Joaquín, “Régimen sancionador”, BARRIO ANDRÉS, Moisés (Dir.), *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 201-217.
- DIEGUEZ LUCENA, Antonio Javier, “La singularidad tecnológica y el desafío posthumano”. *Pasajes: Revista de pensamiento contemporáneo*, núm. 50. 2016, pp. 154-164.
- DIEZ PICAZO, Luis y GULLÓN, Antonio, *Sistema de Derecho Civil*, Vol. 1, Tecnos, Madrid, 2010.
- DRENTH, Piet, *Intelligence: knowing and measuring*, Editorial Nieuwezijds, Amsterdam, 2007.
- ENDARA-CHAMORRO, Ronald Estiven; ESPINOZA-JIMÉNEZ, Juan Sebastián; LÓPEZ-FUEL, Eder Ronaldo y SANTANDER-MORENO, Jessica Johanna, “Análisis Jurídico del deepfake en relación con la suplantación de identidad, Ecuador”, *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas*, Año IX, Vol. IX, Núm. 1. Edición Especial, 2024, pp. 240-250. [https://doi.org/10.35381\(racji.v9i1.3530](https://doi.org/10.35381(racji.v9i1.3530).
- FERRIOLS I SOLÁ, Antoni y FERNÁNDEZ-ALLER, Celia, “El derecho a la protección de datos de carácter personal: disposición adicional quinta de la Constitución española”, LÓPEZ GARRIDO, Diego (Coord.), *Los nuevos derechos sociales fundamentales: una propuesta de reforma constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2023, pp. 147-173.
- GARCÍA MARCOS, Julián, “Hacia una exclusiva reserva jurisdiccional en la protección del derecho a la intimidad”, *Actualidad Civil*, núm. 4, LA LEY, 2024 (LALEY 15717/2024).
- GARCÍA-ULL, Francisco José, “Deepfakes: el próximo reto en la detección de noticias falsas”, *Anàlisi: Quaderns de comunicació i cultura*, Núm. 64, 2021, págs. 103-120. DOI: <https://doi.org/10.5565/rev/analisi.3378>.
- GONZÁLEZ QUIRÓS, José Luis, “La inteligencia artificial y la realidad restringida: las estrecheces metafísicas de la tecnología”, *Naturaleza y Libertad: Revista de Estudios Interdisciplinarios*, Núm. 12: Número especial: *Inteligencia artificial y Antropología filosófica. ¿Es posible transferir la mente humana a un soporte no biológico?*, Estudios, 2019. DOI: <https://doi.org/10.24310/NATyLIB.2019.v0i12.6271>
- GUTIÉRREZ GARCÍA, Elisa, *Inteligencia artificial y Derechos Fundamentales. Hacia una convivencia en la era digital*, Colex, A Coruña, 2024.
- HUERGO LORA, Alejandro, “La Inteligencia Artificial: una aproximación jurídica no catastrófica”, *Revista española de control externo*, núm. Extra 74-75, (Ejemplar dedicado a: *Inteligencia artificial. Gestión y control público*), pp. 110-129.
- LLANO ALONSO, Fernando M., *Homo Ex Machina. Ética de la inteligencia artificial y Derecho digital ante el horizonte de la singularidad tecnológica*, Tirant lo Blanch, Valencia, 2024.

- LÓPEZ RINCÓN, Darío, “Robots y Abogacía”, en *Derecho de los Robots*, BARRIO ANDRÉS, Moisés (Dir.), Wolters Kluwer, Madrid, 2018, p. 192.
- LOZANO SEDEÑO, Antonio, *Delito de injurias y calumnias: protección y regulación legal en España*, 2024.
- MARTINO, Antonio Anselmo, *Expert System in law*. Editorial North-Holland, New York, 1992.
- MIGUEZ MACHO, Luis y TORRES CARLOS, Marcos, “Sistemas de IA prohibidos y sistemas de IA de alto riesgo”, BARRIO ANDRÉS, Moisés (Dir.) *El Reglamento Europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 49-86.
- PLAZA PENADÉS, Javier, “Claves del futuro Reglamento (Ley) de Inteligencia Artificial de la UE”, *Dossier. Las claves de la futura Ley de Inteligencia Artificial Europea*, Aranzadi La Ley, 2023, pp. 8-18.
- PONCE SOLÉ, Juli, “Reserva de humanidad y supervisión humana de la Inteligencia artificial”, *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, (Ejemplar dedicado a: *Inteligencia artificial y derecho*), 2022, pp. 58-67.
- REDONDO SACEDA, Lara, *El derecho a la vida familiar. Del Convenio Europeo de Derechos Humanos a la Constitución Española*, Tesis Doctoral, GARCÍA ROCA, Francisco Javier (Dir.); CARMONA CUENCA, Encarnación del Rosario (Codir.), Alcalá de Henares, 2023.
- RUSSEL, Stuart y NORVIG, Peter, *Artificial Intelligence. A Modern Approach*, Third Edition, Pearson, 2016.
- SAN MIGUEL CASO, Cristina, “Inteligencia artificial y algoritmos: La controvertida evolución de la tutela judicial efectiva en el proceso penal”, *Estudios penales y criminológicos*, núm. extra 44 (*Inteligencia artificial y sistema penal*), 2023, DOI: <https://doi.org/10.15304/epc.44.8859>.
- SAN MIGUEL CASO, Cristina, “Reflexiones sobre la prevención y mitigación de los sesgos en los sistemas inteligentes”, ARRABAL PLATERO, Paloma y CARO CATALÁN, José (Coord.), *Más allá de la Justicia: nuevos horizontes del derecho procesal*, Tirant lo Blanch, Valencia, 2024, pp. 229-242.
- SERRANO MAILLO, María Isabel, “Derecho al honor, intimidad, propia imagen y otros derechos colindantes”, SÁNCHEZ GONZÁLEZ, Santiago (Coord.), *Derechos y Libertades*, Universitas, 2021, pp. 301-342.
- TRUJILLO CABRERA, Carlos, “El derecho a la propia imagen (y la voz) frente a la inteligencia artificial”, *InDret*, 1, 2024, pp.74-113.
- VALERO HEREDIA, Ana, *La Libertad de la pornografía*, Editorial Athenaica, Sevilla, 2022.
- VEGA GARCÍA, Paula, “Protección y comercialización del derecho a la propia imagen del difunto ante la inteligencia artificial”, ARRÉBOLA BLANCO, Adrián (Dir.), *Retos del Derecho de Sucesiones del Siglo XXI. Volumen II*, Reus, Madrid, 2023, pp. 999-1042.

- VELAZQUEZ COBOS, Almudena, “El abogado robot”, en *Legal Tech. La transformación digital de la abogacía*, Edición nº 1, LA LEY, 2019 (LA LEY 7383/2019).
- VÁZQUEZ ALONSO, Víctor Javier, *La libertad del artista: censuras límites y cancelaciones*, Editorial Athenaica, 2023.
- WESTERLUND, Mika, “The Emergence of Deepfake Technology: A Review”, *Technology Innovation Management Review*, vol. 9, issue 11, Carleton University, 2019, pp. 39-52.