

EL DEEPFAKE COMO RETO PROBATORIO: ANÁLISIS Y PROPUESTA DE REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL ÁMBITO JUDICIAL

*Andrea Isabel Baeza García, Antonio Herrera Robles
Noelia Acero Sánchez, Melibea Riaño Pailos y Julia Gómez Cerezo*

Tutor: *Lorenzo Mateo Bujosa Vadell*

Universidad de Salamanca

Resumen:

La inteligencia artificial (IA) generativa está en auge en los últimos años y su contenido refleja una vulneración de derechos y una necesidad imperativa de regular. El objetivo era proponer un sistema que regule y evalúe los casos de *deepfake* que se dan en la actualidad, asentado así una base legislativa para el futuro. Para ello, se analizó la legislación que se aplica actualmente y las propuestas de ley que regularían esta materia, también se exploró la opinión doctrinal de algunos autores respecto a esta problemática. Aunque algunos preceptos pueden ser interpretados para proteger a las víctimas, el avance de la IA y sus capacidades generan una inseguridad jurídica que precisa de regulación propia. Solo un sistema con unas bases sólidas es factible para el enfrentamiento contra esta nueva tecnología.

Palabras clave: IA, inteligencia artificial generativa, *deepfake*, peritaje.

Abstract

Generative artificial intelligence (AI) has been booming in recent years and its contents reflect an infringement of rights and an imperative need for regulation. The aim was to propose a system to regulate and assess current cases of *deepfake*, thus establishing a legislative

basis for the future. To this end, the legislation currently in force and the proposed laws that would regulate this matter were analysed, as well as the doctrinal opinion of some authors regarding this problem. Although some precepts can be interpreted to protect victims, the progress of AI and its capabilities generate a legal uncertainty that requires its own regulation. Only a system with solid foundations is a feasible measure for confronting this new technology.

Keywords: AI, generative artificial intelligence, deepfake, expertise.

1. Introducción

La inteligencia artificial (o IA, en adelante) ha evolucionado de manera vertiginosa desde sus inicios en la década de 1950, cuando Alan Turing planteó la posibilidad de crear máquinas capaces de pensar. Este concepto, que en sus comienzos parecía un sueño lejano, ha dado lugar a desarrollos impresionantes en múltiples campos, desde la medicina hasta el entretenimiento. Sin embargo, uno de los ámbitos donde la IA está generando un impacto significativo y creciente es el jurídico. A medida que las tecnologías avanzan, también lo hacen las aplicaciones de la IA en la práctica legal, la administración de justicia y la elaboración de leyes. Pero no todo es positivo, pues también se ha usado para cometer delitos que, debido a la complejidad del sistema, son difíciles de identificar, evaluar y juzgar.

En sus primeras etapas, la IA se centró en resolver problemas específicos y realizar tareas concretas, como el juego de ajedrez o la resolución de problemas matemáticos. Con el tiempo, el desarrollo de técnicas más sofisticadas, entre las que se incluyen el aprendizaje automático y el procesamiento del lenguaje natural, ha permitido a la IA asumir roles más complejos, como el análisis de grandes volúmenes de datos y la predicción de resultados. Estos avances han transformado el mundo y han agilizado la práctica legal, facilitando el trabajo de abogados y jueces y mejorando la eficiencia del sistema judicial.

No obstante, el uso de la IA en el ámbito jurídico también plantea importantes desafíos legales y éticos. También ha puesto trabas al correcto funcionamiento de la justicia, pues se han presentado escenarios que no éramos capaces de concebir hace veinte años. La capacidad de la IA para crear y generar contenido de forma autónoma, así como la toma de decisiones, suscitan preocupaciones sobre la transparencia, la responsabilidad y la equidad. ¿Quién es responsable cuando una IA comete un error? ¿Cómo se asegura la protección contra los algoritmos utilizados en la toma de decisiones judiciales? Además, la creciente dependencia de la tecnología en nuestra sociedad plantea preguntas en torno a la protección de datos, la privacidad y otros derechos fundamentales.

En este ensayo, exploraremos la clasificación de la inteligencia artificial y su incidencia en el mundo jurídico, analizando los problemas legales y éticos que genera. Examinaremos casos específicos y las medidas que se están tomando para abordar estos desafíos por parte de los operadores jurídicos, proporcionando una visión comprensiva del impacto de la IA en el ámbito legal contemporáneo y su intento o necesidad de regulación.

2. Inteligencia artificial generativa y redes generativas antagónicas (GAN)

Cuando hablamos de la inteligencia artificial, en general, tratamos un grupo muy amplio de sistemas que funcionan de diferentes maneras y buscan cumplir diferentes objetivos. Debemos entender a la IA como una orquesta, la cual se compone de instrumentos y músicos con diferentes materiales y funciones, los cuales no son contemplados conscientemente por el público, pues este solo presta atención al resultado final¹. De esta manera, aunque la IA no sea más que un conjunto de elementos y sistemas informáticos, hay que mirar más allá y observar el resultado en su conjunto, así como las diferentes funciones que puede cumplir. Solo de esta forma podremos diferenciar los distintos tipos de IA y el cometido de cada una.

Si se busca hacer una clasificación según su capacidad funcional, nos encontramos con la *narrow AI*, la *general AI* y la superinteligencia² (Ferreira, 2021). En primer lugar, la *narrow AI* o IA débil está diseñada para realizar tareas específicas y no se le permite realizar ninguna acción fuera del ámbito programado. Algunos ejemplos son las asistentes virtuales de sistemas operativos o los sistemas de sugerencia en las plataformas de *streaming*. En segundo lugar, la IA general tiene la capacidad de imitar la inteligencia humana y realizar una gran variedad de acciones. Lo interesante de esta clase de inteligencia es su capacidad de analizar los datos que se le proporcionan y la generación de una respuesta acorde a estos como si del pensamiento humano se tratase. Además, poseen la capacidad de aprender y mejorar su desarrollo a medida que avanza su utilización. Por último, tenemos una pretendida superinteligencia, que debemos entender como una IA hipotética que superaría las capacidades humanas, tomando todas sus decisiones de forma consciente y autónoma. Así es como se ha retratado a la IA en las películas futuristas sobre robots y tecnologías en un mundo distópico.

¹ BODEN, M: *AI: Its Nature and Future*. Oxford University Press, Oxford, 2016, p. 4.

² FERREIRA, K. "Tipos de Inteligencia Artificial: conoce cuáles existen y cómo usarlos", en *Rockcontent*, 20 de julio del 2021. Disponible en <https://rockcontent.com/es/blog/tipos-de-inteligencia-artificial/> [Consultado: 30 de junio de 2024].

No obstante, la reciente Ley de Inteligencia Artificial aprobada por el Consejo Europeo y el Parlamento Europeo³ propone una clasificación basada en los posibles riesgos que pueda conllevar el uso de la IA, siendo estos el riesgo inaceptable, el alto, el limitado y el mínimo.

Así, el primer grupo —riesgo inaceptable— se caracteriza por una prohibición expresa y absoluta de su uso debido al peligro que puede generar en el bienestar social, hallándose aquí los sistemas de puntuación social, el reconocimiento facial sistemático y la IA manipulativa.

En el grupo de riesgo alto, contamos con inteligencias que precisan de una extensa regulación debido a su impacto en la salud, la seguridad y los derechos fundamentales, siendo este el grupo principal sobre el que versa la ley. En este grupo podemos encontrar diversos sistemas cuya función suple la capacidad de decisión del ser humano, sustituyendo a este en tareas evaluativas y analíticas como la educación, el rendimiento laboral, la atención sanitaria o el sistema judicial.

Al descender al nivel de riesgo limitado, nos encontramos ante las inteligencias que se verán obligadas a proporcionar cierto nivel de transparencia a fin de proteger a los usuarios que están interactuando con ella. Es aquí donde nos encontramos los procesadores de lenguaje o los generadores de contenido audiovisual. En última instancia, se pretende que las personas tengan más facilidad a la hora de discernir entre el contenido generado por una IA y el generado por un ser humano.

Por último, se establece un riesgo mínimo para aquellas inteligencias cuya función tiene un impacto mínimo en las personas y su objetivo es meramente agilizar tareas triviales y repetitivas, como pueden ser los filtros de spam en los correos electrónicos o algunos videojuegos gestionados con dicha tecnología.

No cabe duda de que la IA está en constante evolución y avanza a un ritmo más rápido que el Derecho. Por ello, buscamos analizar como los modelos más modernos de inteligencia artificial pueden llegar a afectarnos y evaluar las opciones a nuestro alcance y la posible necesidad de una reforma en el marco legal de este mundo digital.

De acuerdo con los diferentes productos que pueden ser fruto de la inteligencia artificial, nos encontramos la IA generativa como un tipo de inteligencia

³ UNIÓN EUROPEA. PARLAMENTO EUROPEO, CONSEJO EUROPEO: “Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828”, en *Diario Oficial de la Unión Europea*, 10 de junio de 2024.

artificial que puede crear contenido nuevo y original a partir de datos existentes. Utiliza modelos avanzados de aprendizaje automático para generar texto, imágenes, audio y vídeo que son casi indistinguibles del contenido creado por humanos. En sus primeras etapas, la IA generativa utilizó modelos estadísticos y algoritmos simples para generar texto y patrones básicos. Pero no fue hasta mediados de la década de 2010 que su avance adquirió un ritmo sin igual gracias a la introducción de redes neuronales y el *deep learning*, que no es más que un modelo informático “por capas” que busca simular el cerebro humano y la manera en la que este genera respuestas y contenido.

Según la legislación europea, se precisa concretar si el contenido que visualizamos ha sido producido por una IA o un ser humano, pero esta tarea se ha vuelto más difícil en los últimos años, en los cuales el contenido ha llegado a ser tan sofisticado que sería difícil diferenciar ambos a simple vista. Para ejemplificar el nivel de sofisticación de estas imágenes y vídeos, mostramos a continuación dos imágenes de la célebre cantante española Lola Flores en escenarios televisivos.



Probablemente un lector informado no podría indicar cuál de las dos imágenes es un *deepfake*. En realidad, la de la izquierda fue creada en 2021 para un mensaje publicitario de una conocida marca de cerveza. Para su elaboración, se combinaron más de mil imágenes de la cantante y decenas de horas de vídeo para poder replicar su estructura facial sobre la cara de una modelo. De esta forma, y veintiséis años después de su fallecimiento, los españoles volvieron a ver y oír a una de sus cantantes más famosas. Pero esto solo nos hace plantearnos hasta dónde puede llegar la IA y, en particular, si puede cruzar la línea de lo ético y lo legal.

Si bien este no es el caso, los *deepfakes* pueden ser utilizados para diversos fines ilícitos o ilegales. Entre los usos más preocupantes, ya relativamente frecuentes en el entorno digital, se encuentran, entre otros, la difusión de desinformación y propaganda, donde los *deepfakes* pueden manipular la opinión

pública al falsificar declaraciones de políticos o figuras públicas; la creación de pornografía no consensuada, que constituye una grave invasión de la privacidad y puede resultar en un daño emocional y reputacional a las víctimas; la suplantación de identidad en fraudes financieros, donde los delincuentes pueden engañar a sistemas de seguridad biométrica o realizar fraudes de voz para obtener acceso no autorizado a cuentas bancarias y datos sensibles; la fabricación de pruebas falsas en procesos judiciales, afectando la integridad de la justicia; y la extorsión y el chantaje, donde los *deepfakes* se utilizan para crear contenido comprometedor y coaccionar a las víctimas.

La creciente sofisticación y accesibilidad de la tecnología de *deepfake* hace que estos riesgos sean cada vez más prevalentes y difíciles de mitigar. En la actualidad, los materiales han alcanzado tal nivel de perfeccionamiento que hace imposible discernirlo del no generado por IA, lo cual se ha presentado como un serio problema para los órganos jurisdiccionales. La evaluación de dicho contenido durante el proceso judicial debe seguir unos procedimientos que difieren mucho de los tradicionales, pues hace evidente *prima facie* que no se pueda confiar en el juez para la evaluación autónoma la prueba.

Al ser un campo en constante evolución, es comprensible que no exista una regulación concreta al respecto. Sería interesante, pues, evaluar los caminos que pueden seguirse de acuerdo con la ley, las distintas vías que ha tomado la jurisprudencia y las propuestas doctrinales a este respecto.

3. Entre lo real y lo ficticio: el *deepfake* como reto probatorio

A la hora de abordar la noción de *deepfake*, nos encontramos con que este se configura como una incógnita arraigada dentro de la estructura procesal de todos los ordenamientos jurídicos actuales, debido a la escasa regulación en lo que a inteligencia artificial respecta.

En este tercer punto, vamos a centrar nuestra atención en los tres ejes fundamentales que posicionan al *deepfake* como un verdadero reto probatorio: la colisión entre el mismo y los derechos fundamentales (3.1), su posible configuración como prueba diabólica (3.2) y su influencia en la actual labor pericial (3.3).

3.1 Una amenaza iusfundamental

La libertad de expresión se configura en muchas ocasiones como el derecho fundamental por excelencia en lo que respecta a la problemática de los *deepfake*. En efecto, cabe preguntarse dónde se encuentra el límite de este derecho en relación con el tema que nos atañe.

El sistema normativo español carece de una regulación precisa en torno a la autorización de difundir alteraciones de imágenes o voces y la forma de perseguir su uso ilícito. En este sentido, la Exposición de Motivos de la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, de 13 de octubre de 2023⁴, pone de manifiesto la necesidad de reforzar la protección de los derechos al honor, la propia imagen y la intimidad.

Estos tres derechos fundamentales, siempre en colisión con la libertad de expresión, se configuran a nuestro entender como los auténticos protagonistas cuando se trata de comprender el peso del *deepfake* en el ámbito procesal. En el caso de España, la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen⁵ se ha quedado atrás en el intento por abordar una regulación sistemática de la vulneración de tales derechos. El momento en que fue dictada y la ausencia de una reforma acorde a los tiempos han impedido la consideración de la inteligencia artificial como una amenaza potencial, lo que ha derivado en una inseguridad legislativa que no hace más que alimentar la incertidumbre general acerca de las garantías de los ciudadanos en el ámbito.

No obstante, los derechos fundamentales previamente mencionados no son los únicos elementos que deben considerarse en la contienda procesal ante la que nos hallamos actualmente, puesto que, en el ámbito criminal, nos encontramos con un dilema a que los procesalistas se enfrentan recurrentemente: ¿y la presunción de inocencia? ¿Qué ocurre, realmente, con los derechos del acusado una vez ha sido investigado e imputado por un delito que alega no haber cometido?

El derecho a la presunción de inocencia es otro claro ejemplo de la contraposición entre el *deepfake* y un derecho fundamental, puesto que, adentrándonos en la última ratio del Derecho penal, nos encontraríamos con que la inteligencia artificial se habría colocado en el epicentro del proceso: la prueba.

⁴ ESPAÑA, CONGRESO DE LOS DIPUTADOS. Proposición de Ley Orgánica (13 de octubre de 2023) de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, en: *Boletín Oficial de las Cortes Generales*, núm. 122/000011, 2023. Disponible en: https://www.congreso.es/public_oficiales/L15/CONG/BOCG/B/BOCG-15-B-23-1.PDF [Consultado: 6 de junio de 2024].

⁵ ESPAÑA, JEFATURA DEL ESTADO. Ley Orgánica 1/1982 (5 de mayo de 1982) de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en: *Boletín Oficial del Estado*, núm. 115, 1982, pp. 1-7. Disponible en: <https://www.boe.es/buscar/pdf/1982/BOE-A-1982-11196-consolidado.pdf> [Consultado: 7 de junio de 2024].

De este modo, podemos observar que la configuración del *deepfake* como fuente de prueba supone una grave amenaza para la integridad de ciertos derechos fundamentales, desde la presunción de inocencia hasta los derechos al honor, a la intimidad y a la propia imagen. En este contexto, ¿qué pueden hacer los órganos jurisdiccionales de los Estados para detectarlo y ponerle freno?

3.2 El *deepfake* y la prueba diabólica

El fenómeno emergente del *deepfake* constituye, como se ha expuesto *ut supra*, una grave amenaza contra los derechos fundamentales del investigado en un proceso judicial, violentando la veracidad de la información que circula en línea⁶.

El *deepfake* es creado a través de la manipulación de producciones audiovisuales mediante el uso de algoritmos de aprendizaje profundo, los cuales poseen la capacidad de reemplazar y superponer rostros, así como de modificar voces, generando así un contenido altamente realista⁷. La distorsión de la percepción de la realidad, junto con la difamación y la manipulación, suponen una problemática que debe ser abordada para poder preservar la presunción de inocencia del investigado en todas las fases del proceso, así como las garantías de la parte acusadora.

Y, es que, el *deepfake* ha alzado el velo de la incertidumbre probatoria tanto en la parte activa como en la parte pasiva del proceso. El escritor Michael Grothaus⁸, en su libro *Trust No One: Inside the World of Deepfakes*, describe cómo solicitó a un *deepfaker* que manipulara un vídeo en el que se estaba cometiendo un robo con una motocicleta para cambiar el rostro del delincuente por el suyo. El autor señala que, para ello, únicamente fue necesario un vídeo con que entrenar al *software*, que terminó por arrojar un material audiovisual realista de Grothaus cometiendo el crimen.

Por el contrario, y siendo conscientes de que entre el 90 y el 95% del contenido *deepfake* que circula en la red es de pornografía no consentida, y que, dentro de

⁶ <https://biblioteca.corteidh.or.cr/tablas/R08047-30.pdf> [Consultado: 10 de junio de 2024].

DAGAR, D.; KUMAR VISHWAKARMA, D.: "A Literature Review and Perspectives in Deepfakes: Generation, Detection, and Applications", en: *International Journal of Multimedia Information Retrieval*, vol. 11, julio de 2022, pp. 219-289. Disponible en: <https://link.springer.com/article/10.1007/s13735-022-00241-w> [Consultado: 7 de junio de 2024].

⁷ GARCÍA-ULL, F. J.: "*Deepfakes*: el próximo reto en la detección de noticias falsas", en: *Anàlisi: Quaderns de comunicació i cultura*, núm. 64, junio de 2021, pp. 103-120. Disponible en: <https://analisi.cat/article/view/v64-garcia> [Consultado: 8 de junio de 2024].

⁸ GROTHAUS, M.: *Trust No One: Inside the World of Deepfakes*. Hachette UK, Londres, 2021.

este, el 90% lo es de mujeres⁹, la configuración del *deepfake* como contraprueba es más que plausible, pudiendo llegar a ser utilizado en casos de denuncia por agresión sexual o cualquier otra cuestión de índole similar para tratar así de convencer al juez del otorgamiento de un consentimiento inexistente por parte de la contraparte procesal.

De este modo, en ambos casos, nos encontramos ante la tan temida “prueba diabólica”, esto es, aquella que reclama la necesidad de probar la inexistencia de unos hechos de los que se acusa a una persona. La prueba diabólica no hace más que trasladar la carga de la prueba penal a la parte acusada, lo cual está constitucionalmente vedado en los ordenamientos jurídicos de nuestro entorno. No obstante, la anuencia a que la inteligencia artificial se configurara como un elemento probatorio más, sin regulación alguna, así como la incorporación inmoderada del *deepfake* como fuente de prueba, conllevarían inevitablemente a aceptar el riesgo de que los hechos introducidos por ella no fuesen ciertos.

Así, podemos observar cómo, con la posible entrada del *deepfake* como fuente de prueba, la potencial violación de derechos fundamentales va más allá, ya que también nos encontraríamos ante la eventual vulneración de las garantías constitucionales del proceso penal que, como recoge la Corte Interamericana de Derechos Humanos¹⁰, constituyen el último amparo que establecen las constituciones y que debe prestar el Estado para el efectivo reconocimiento y respeto de las libertades y derechos de la persona individual y de los grupos sociales en que se desenvuelve.

Por lo tanto, frente a la inevitable —y no por ello negativa— entrada de la inteligencia artificial en la Administración de Justicia, debemos atender a las vías procesales, particularmente probatorias, con las que contamos para tratar de guiar su ingreso de la manera más adecuada.

3.3 Inteligencia artificial y peritaje: el dilema de la prueba sobre la prueba

La búsqueda de las formas más depuradas de combatir los *deepfakes* y sus consecuencias ha llevado, quizá paradójicamente, al empleo de métodos de inteligencia artificial basados en la capacidad de gestionar información. De esta

⁹ HAO, K.: “Deepfake Porn is Ruining Women’s Lives. Now the Law May Finally Ban It”, en *MIT Technology Review*, 12 de febrero de 2021. Disponible en: <https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/> [Consultado: 9 de junio de 2024].

¹⁰ CARO CORIA, D. C.: “Las garantías constitucionales del proceso penal”, en: *Anuario de Derecho Constitucional Latinoamericano*, 2006, pp. 1028-1045. Disponible en: <https://biblioteca.corteidh.or.cr/tablas/R08047-30.pdf> [Consultado: 10 de junio de 2024].

manera, sistemas como las redes neuronales convolucionales (CNN) —subconjunto de *machine learning* y núcleo de los algoritmos de *deep learning*— han demostrado ser verdaderamente efectivas a la hora de identificar patrones complejos en imágenes y vídeos, permitiendo entradas de imagen, voz o señales de audio¹¹.

En este sentido, en la actualidad existen diferentes técnicas empleadas para la identificación de *deepfakes* que aún se encuentran en proceso de mejora¹²:

Por un lado, las técnicas de procesamiento de textura y color permiten identificar patrones anómalos en tales características, pudiendo así detectar aquellas alteraciones más burdas e inexactas. Asimismo, el análisis de movimiento facial también ha sido de gran ayuda a la hora de detectar *deepfakes*, puesto que su algoritmo, basado en la correlación sincrónica entre los labios y el habla, así como en los gestos faciales desnaturalizados, es capaz de señalar movimientos faciales incoherentes y sin sentido.

Por otro lado, también nos encontramos frente a técnicas basadas en metadatos y huellas digitales, las cuales estudian los metadatos insertados en los archivos multimedia, analizando la ausencia o inconsistencia de los mismos. Igualmente, la detección de artefactos de comprensión, como la distorsión del medio, así como los enfoques de espectros de frecuencia destinados a la búsqueda de patrones de frecuencia atípicos en imágenes y vídeos, se han revelado como herramientas eficaces a la hora de identificar recursos audiovisuales fraudulentos.

Con todo ello, es evidente que no son escasas las técnicas de detección frente al *deepfake* que podrían ser incorporadas en la práctica forense. La verdadera cuestión, sin embargo, atañe a la forma en que debe hacerse.

Existe una posibilidad muy cierta de que toda prueba documental presentada en el proceso —y parte de la prueba pericial— sea falsa y no exista, en ocasiones, manera humana de saberlo, al aparentar ser cierto cuanto vemos, escuchamos o leemos en unos documentos que pueden constituir la prueba reina del proceso penal.

No obstante, los problemas planteados en este trabajo demuestran que es necesaria una configuración que vaya más allá de los conocidos criterios

¹¹ RANA, S. *et al.*: “Deepfake Detection: A Systematic Literature Review”, en: *IEEE Access*, vol. 10, 2022, pp. 25494-25513. Disponible en: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9721302> [Consultado: 11 de junio de 2024].

¹² GUTIÉRREZ SULLCA, E. M.: “Artificial Intelligence Techniques for Detecting Deepfakes and their Impact on the Veracity of Online Content”, en: *International Journal of Systems Engineering*, vol. 4, núm. 2, 2023, pp. 6-9. Disponible en: <https://systemjournal.org/index.php/ijse/article/view/39/26> [Consultado: 12 de junio de 2024].

Daubert, puesto que, de no ser así, nos hallaríamos ante un círculo vicioso de prueba sobre la prueba, en el que todo medio probatorio propuesto por las partes podría ser calificado como fraudulento en un intento de ralentizar el proceso y de entorpecer su cauce, debido a la necesidad de contactar, caso por caso, con peritos informáticos que resolviesen la contienda.

A todo lo mencionado con anterioridad, debemos añadir que los jueces no poseen generalmente los conocimientos suficientes sobre inteligencia artificial y su incorporación al plano legal de forma teórica y práctica¹³, por lo que, de no ofrecerse una solución adecuada, el auge del *deepfake* como elemento probatorio derivará inevitablemente en una marea de contrapruebas periciales que, siendo o no oportunas, resultarán en un entorpecimiento de la Administración de Justicia.

Por ello, es más que evidente la necesidad de un nuevo modelo de garante, sobre el que profundizaremos más adelante, que se superponga a los intereses individuales y se ajuste a las necesidades de todo Estado de Derecho basado en la protección de los derechos fundamentales y de las garantías jurídico-procesales de la sociedad en su conjunto.

4. Del papel a la práctica: preceptos normativos adecuados al *deepfake*

Debido a la carencia de una normativa específica sobre esta materia, los tribunales han tenido que ofrecer ingeniosas respuestas a la hora de interpretar las normas con el fin de proporcionar un mínimo nivel de protección contra los ataques derivados del *deepfake*.

Para los menores de edad, la legislación penal española castiga de forma explícita la creación de material pornográfico infantil. Sin embargo, no existe un equivalente normativo que se refiera a los adultos, que dependen así de la interpretación judicial sobre los delitos contra el honor, la intimidad y la propia imagen.

4.1 Posición normativa actual

Los artículos 189.1.b) y 189 *bis* del Código Penal español tipifican delitos de pornografía infantil y pueden ser aplicados a resultados de un proceso relacionado con un *deepfake* que implique la creación y distribución de contenido pornográfico falsificado de menores de edad.

¹³ SIMÓ SOLER, E.: “Retos jurídicos derivados de la Inteligencia Artificial Generativa: *deepfakes* y violencia contra las mujeres como supuesto de hecho”, en: *InDret Criminología: Revista para el Análisis del Derecho*, núm. 2, 2024, pp. 493-515. Disponible en: <https://indret.com/wp-content/uploads/2023/04/1767.pdf> [Consultado: 14 de junio de 2024].

El mencionado artículo 189.1.b) se refiere a la producción, distribución, difusión o exhibición de material pornográfico que involucre a menores de edad. Aunque no se haga mención explícita a ello, el precepto puede interpretarse de manera que queden cubiertos los supuestos de falsificación de imágenes o vídeos pornográficos de menores a través de inteligencia artificial, incluso si los menores no participaron directamente en la creación del material. Más concretamente, el apartado d) castiga las conductas referidas sobre contenidos en imágenes realistas de un menor participando en conductas sexuales, lo cual podría dar a entender que distintos contenidos como la animación o el generado por IA, podría caer en esta categoría.

El artículo 189 *bis* del Código Penal se centra en la conducta relacionada con el acceso a material pornográfico infantil y la utilización de medios tecnológicos para dicho fin. Este artículo puede aplicarse en casos donde se demuestre que se han utilizado inteligencias artificiales para acceder, crear o distribuir este tipo de pornografía infantil. El uso de tecnología avanzada para estos fines puede ser interpretado como un agravante, dada la intención de crear contenido ilícito y potencialmente distribuirlo a nivel masivo, lo cual aumenta el alcance y el daño causado por estas acciones.

En lo que respecta a los mayores de edad, debemos explorar la posibilidad de usar los tipos penales de los delitos contra el honor y la intimidad para proteger a las víctimas. Aquí surge un problema debido al carácter restrictivo de la ley, pues en lo que se refiere a la imagen íntima, no podría aplicarse el 197.1 del Código Penal debido a que este solo protege frente a determinados ataques y se refiere a la imagen fiel o verídica de la persona.

Para escapar de la interpretación pacata del texto legal, una opción posible sería argumentar que se comete un delito contra el honor tipificado en el art. 208 CP, con el agravante del art. 209 CP si existe una posterior difusión. Se puede argumentar que el hecho de crear una imagen artificial de la víctima con el objetivo de burlarse de esta y ridiculizarla concuerda con el *animus injuriandi* de este tipo penal. De este modo podría pensarse el atentado contra el honor, pero sería solo con una multa. Este desvalor, en comparación con la distribución de pornografía sin consentimiento de la víctima, plantea dudas sobre la correcta protección de las personas ante este nuevo escenario.

Estas preocupaciones no son exclusivas de nuestro lado del charco, sino que también ha sido materia de debate en diversos países de Latinoamérica. Como bien indica Rodrigo López¹⁴, la creación de contenido *deepfake* sobrepasa las

¹⁴ RODRIGO LÓPEZ, J. F.: “Tragic Realism: How to Regulate Deepfakes in Colombia?”, en: *Latin American Law Review*, núm. 8, 2022, pp. 125-145. Disponible en <https://doi.org/10.29263/lar08.2022.08>. [Consultado: 30 de junio de 2024].

capacidades humanas y las de la propia IA. Se realizó una evaluación sobre el impacto de la regulación y, aunque la mayoría de los colombianos estaba de acuerdo con que los *deepfakes* eran un problema, también estaban preocupados de que el modelo regulatorio que surgiera pudiera afectar de algún modo a su libertad de expresión. Se defiende que debieran introducirse sistemas de autorregulación dentro de las propias redes sociales y de difusión para frenar la proliferación de este tipo de contenidos, así como criminalizar los *deepfakes* que se creen con fines ilícitos.

4.2 Opinión doctrinal

A diferencia de lo que ocurre en otras materias más asentadas en Derecho, la novedad que supone la Inteligencia Artificial, especialmente en su vertiente derivada en el *deepfake*, hace muy difícil encontrar a día de hoy jurisprudencia consolidada en relación a su impacto y a la configuración normativa que derivaría de los tribunales, por lo que es la doctrina, también escasa, la que ha intentado encauzar el rumbo de su encuadre legislativo y las posibles reformas normativas que podrían llevarse a cabo, abriendo así un tedioso camino por el que inevitablemente, tarde o temprano, tendrán que pasar los jueces y magistrados.

En este sentido, la doctrina española mantiene una postura firme al desechar la idea de que la regulación de los *deepfakes* se agote en la simple subsunción en los tipos penales previstos el artículo 197 del Código Penal, puesto que dicho precepto excluye todo contenido que sea fruto de la manipulación¹⁵. Por ello, consideramos que no debe cerrarse la puerta a una posible subcategoría de dicho artículo a través de la adición de un nuevo apartado relativo al modo de generación del contenido audiovisual¹⁶.

Esta posición es la también mantenida por la jurisprudencia del Tribunal Constitucional español, para el cual, en relación con el artículo 18 de la Constitución, el derecho al honor, a la intimidad personal y familiar y a la propia imagen deben dirigirse únicamente a las imágenes que reflejen una vida íntima de existencia real, puesto que la intimidad es un derecho personalísimo que no cabe extender de manera externa y artificial a la propia persona. La Sentencia 81/2001, de 26 de marzo (FJ 2.º), destaca lo siguiente:

¹⁵ JAREÑO LEAL, Á.: “El derecho a la imagen íntima y el Código Penal: la calificación de los casos de elaboración y difusión del *deepfake*”, en: *Revista Electrónica de Ciencia Penal y Criminología*, núm. 26, 2024, pp. 1-37. Disponible en: <http://criminet.ugr.es/recpc/26/recpc26-09.pdf> [Consultado: 12 de junio de 2024].

¹⁶ SIMÓ SOLER, E.: *op. cit.*

“A pesar de la creciente patrimonialización de la imagen y de la necesaria protección del derecho a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma [...], el derecho garantizado en el art. 18.1 CE, por su carácter ‘personalísimo’ [...] limita su protección a la imagen como elemento de la esfera personal del sujeto, en cuanto factor imprescindible para su propio reconocimiento como individuo”.

Tal y como defiende Lloría García¹⁷, “no siempre los instrumentos tradicionales del Derecho penal son válidos para resolver las cuestiones que surgen a propósito de las lesiones a bienes jurídicos nuevos o la afectación de los tradicionalmente tutelados con una mayor intensidad”, por lo que quizás sea necesario reinterpretar el bien jurídico “intimidad” para así poder prever las potencialidades lesivas respecto de los ya mencionados derechos fundamentales que genera el entorno virtual y la eventual afectación a múltiples bienes dignos de tutela jurídico-penal.

No obstante, una parte de la doctrina española navega a favor de la inclusión del *deepfake* como un delito de injurias graves de los artículos 208 y 209 del Código Penal, siempre que se dé el *animus injuriandi*, como hemos mencionado anteriormente. Esto ocurre, especialmente, en aquellos casos de difusión de imágenes simuladas de naturaleza sexual, en los que la víctima es objeto de mofa o venganza, entre otros¹⁸.

Asimismo, siguiendo a Jareño Leal, la autora sostiene la posibilidad de incluir el *deepfake* como un delito de amenazas básicas y condicionales de los apartados 1 y 2 del artículo 169 del Código Penal, o bien como un delito de acoso del apartado 5 del artículo 172 *ter* y, en caso de menores de edad, su subsunción dentro del artículo 189.1 b) del mismo cuerpo normativo.

Este último artículo —ya mencionado anteriormente— es especialmente relevante en materia de Inteligencia Artificial y de *deepfake*, puesto que nos encontramos ante una expresa referencia a imágenes simuladas, pero realistas, de un menor de edad. La Circular 2/2015 de la Fiscalía General del Estado ha matizado que esta conducta no tiene cabida como “toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales” (subapartado b) ya que “no se utiliza realmente al menor o incapaz, sino que se abusa de su imagen o voz

¹⁷ LLORÍA GARCÍA, P.: “Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral (especial referencia al ‘sexting’)”, en *La ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, núm. 105, 2013, pp. 215-232.

¹⁸ JAREÑO LEAL, Á.: *op. cit.*

manipulándola con artificios técnicos”, concluyendo así que no se lesiona el bien jurídico propio de estos delitos¹⁹.

No obstante, la Circular mantiene que tales conductas deberán castigarse como “pornografía infantil virtual o técnica” (subapartados c y d), ya que “si se tipifican estas subespecies de pornografía, que no representan a menores reales, con más razón cabrá poder reaccionar contra la (p)seudopornografía infantil, en la que se abusa de la imagen de un menor real”. Y es que, la creación de *deep-fakes* pornográficos que utilicen imágenes de menores, aunque no sean reales, podría ser considerada una forma de explotación y abuso sexual, dada la naturaleza lesiva y la potencial distribución de dicho contenido.

La doctrina española, al enfrentar la interpretación de dicho artículo 189.1 b) del Código Penal, ha calificado la subsunción del *deepfake* en tal precepto de “innegablemente desproporcionada”, tal y como manifiesta Jareño Leal, al ubicar dicha conducta dentro de un tipo básico de delitos de explotación sexual y corrupción de menores, careciendo de sentido reconocer con el mismo desvalor la elaboración de pornografía que involucra a menores que aquella que es simulada²⁰.

Ahora, en lo que respecta a la doctrina colombiana, Rodrigo López²¹ destaca la relevancia del artículo 20 de la Constitución Colombiana en relación al derecho de recibir información veraz e imparcial contrapuesto a la libertad de creación de contenido audiovisual.

No obstante, la doctrina de la Corte Constitucional de Colombia, con base en la jurisprudencia emanada de la Sentencia T-391/07, sostiene que la libertad de expresión no es absoluta:

“La libertad de expresión, a semejanza de los demás derechos, no es un derecho absoluto, en ninguna de sus manifestaciones específicas (libertad de expresión *stricto sensu*, libertad de información o libertad de prensa); puede eventualmente estar sujeta a limitaciones, adoptadas legalmente para preservar otros derechos, valores e intereses constitucionalmente protegidos con los cuales puede llegar a entrar en conflicto. Sin embargo, como se ha enfatizado en los apartes precedentes, el carácter privilegiado

¹⁹ ESPAÑA. FISCALÍA GENERAL DEL ESTADO: “Circular 2/2015 (19 de junio de 2015) sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015”, en: *Boletín Oficial del Estado*, ref. FIS-C-2015-00002, 2015. Disponible en: https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2015-00002.pdf [Consultado: 15 de junio de 2024].

²⁰ JAREÑO LEAL, Á.: *op. cit.*

²¹ RODRIGO LÓPEZ, J. F.: *op. cit.*

de la libertad de expresión tiene como efecto directo la generación de una serie de presunciones constitucionales – la presunción de cobertura de toda expresión por el ámbito de protección constitucional, la sospecha de inconstitucionalidad de toda limitación de la libertad de expresión, la presunción de primacía de la libertad de expresión sobre otros derechos, valores o intereses constitucionales con los cuales pueda llegar a entrar en conflicto y la presunción de que los controles al contenido de las expresiones constituyen censura”.

Asimismo, esta misma Corte, en su Sentencia T-244/18, dio pie a la formación de una nueva opinión jurisprudencial en el país americano:

“Este mandato constitucional –libertad de expresión-, ha sido considerado por la Corte como un derecho fundamental de doble vía porque involucra tanto al emisor como al receptor de actos comunicativos, agrupa un conjunto de garantías y libertades diferenciables en su contenido y alcance, tales como la libertad de expresar pensamientos y opiniones, la libertad de informar y recibir información veraz e imparcial, la libertad de fundar medios masivos de comunicación y el derecho de rectificación. Y aunque se prohíbe la censura, también se integran las prohibiciones de realizar propaganda de la guerra, de apología al odio, de pornografía infantil, y de instigación pública y directa al genocidio”.

De este modo, podemos observar cómo en Colombia el auge del *deepfake* también ha supuesto una nueva problemática relacionada, especialmente, con el ya mencionado artículo 20 de su Constitución y con el artículo 21 de la misma, relativa al derecho a la honra; sin que haya, actualmente, ningún precepto normativo que remedie dicho rompecabezas.

En este sentido, debemos tomar en consideración que, a diferencia del caso español, la legislación penal colombiana no hace referencia expresa a la divulgación de contenido íntimo, si bien puede establecerse una relación analógica con el artículo 220 de su Código penal, relativo a imputaciones honrosas. Por ello, al tratar de ofrecer soluciones, siquiera temporales, en relación con cláusulas análogas, no encontramos en el Código Penal colombiano la variedad de preceptos normativos favorables a una subsunción del *deepfake* como en el caso del Código Penal español.

Con todo esto, podemos observar que a nivel doctrinal tampoco existe una postura firme en relación con la adecuación del *deepfake* en alguno de los preceptos normativos existentes, lo que, sumado a la falta de regulación normativa a nivel estatal, europeo o global, suscita nuevamente la persistente incertidumbre acerca de la protección frente al *deepfake*.

5. Conclusiones

A pesar de la proliferación de la inteligencia artificial como una herramienta de uso frecuente en las sociedades contemporáneas, podemos afirmar que los órganos jurisdiccionales no cuentan con las herramientas adecuadas para interpretar los riesgos que tales herramientas puedan generar.

El *deepfake*, como lado oscuro de la inteligencia artificial, no ha hecho más que resaltar las carencias procesales que padecen los sistemas judiciales actuales. La acuciante regulación normativa, todavía pendiente, revela la lentitud o incapacidad de los Estados a la hora de salvaguardar los derechos de sus ciudadanos.

Por ello, el *deepfake* ha logrado introducirse en la médula de la justicia, con una elevada capacidad lesiva para los derechos fundamentales que, a pesar de gozar de una posición privilegiada en nuestros ordenamientos jurídicos, no son inmunes a los avances tecnológicos. Las herramientas de inteligencia artificial generativa han logrado, además, inmiscuirse en las más férreas garantías jurídico-procesales, lo cual puede resultar en una quiebra de la confianza ciudadana en los órganos llamados a impartir Justicia.

A lo largo del trabajo, hemos expuesto que la injerencia del *deepfake* en el proceso penal ha supuesto un verdadero reto probatorio, especialmente al ser configurado como contraprueba, debido a que el sistema jurisdiccional carece por lo general de los medios necesarios para poder detectar de una manera eficiente los recursos audiovisuales fraudulentos presentados por las partes.

En este mismo sentido, la forma habitual de proceder ante la plausible utilización del *deepfake* como elemento probatorio ha sido la asistencia de peritos informáticos caso a caso, lo cual, por motivos obvios, ralentiza el curso del proceso y vulnera sistemáticamente los principios de Derecho procesal que lo rigen.

En lo que respecta a la regulación normativa del *deepfake*, el caso español es un claro ejemplo de la versatilidad del tipo penal, cuya ambigüedad permite encajar, no sin controversias, el concepto novedoso sobre el que hemos centrado nuestro análisis. Sin embargo, se trata de una solución provisional que bien merecería una profunda reflexión sobre la necesidad de una reforma legislativa, que pudiera colmar las lagunas que una flexibilidad interpretativa no pudiera satisfacer de manera conveniente. A este respecto, consideramos que, a pesar de ser múltiples los preceptos penales en los que podría incluirse analógicamente la utilización ilícita de *deepfakes*, debería acometerse una reforma de la legislación para despejar las dudas que el avance tecnológico pudiera despertar.

Por todo ello, podemos concluir que es necesario un cambio en los mecanismos jurisdiccionales, en el sentido que esbozaremos en el siguiente apartado, de manera que los ciudadanos cuenten con suficientes garantías para enfrentar los riesgos derivados del *deepfake* en el foro judicial.

6. Propuesta

Una vez analizada la problemática que suscita el auge del *deepfake* como consecuencia de la proliferación de la Inteligencia Artificial y de lo accesible que esta resulta para el ciudadano corriente, consideramos que es necesario atajar dos problemáticas principales. La primera es resolver las lagunas legales para proporcionar una mayor seguridad jurídica ante estos nuevos escenarios; la segunda sería instaurar un mecanismo u organismo que vele por el cumplimiento de las medidas legislativas propuestas. Así, nos dirigimos no solo a la esfera teórica contenida en las leyes, sino también al ámbito de la aplicación práctica y el cumplimiento de estas.

En primer lugar, es esencial acometer una reforma legislativa que regule la utilización de las imágenes de terceras personas para la creación de contenido audiovisual mediante herramientas de Inteligencia Artificial, sobre todo cuando dicho contenido es, en su mayoría, de carácter sexual. La utilización IA generativa con fines ilícitos es una práctica cada vez más extendida para la cual el Derecho carece de mecanismos óptimos de defensa.

Por eso, el Grupo Parlamentario SUMAR defiende la Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de inteligencia artificial, presentada el 13 de octubre de 2023 ante el Congreso de los Diputados español. En su propuesta se incluye un nuevo art. 208 *bis* del Código Penal, que tipifica las conductas que analizamos de la siguiente manera: “Igualmente tendrá la consideración de injuria la acción que, sin autorización y con ánimo de menoscabar el honor, fama, dignidad o la propia estimación de una persona, recrease mediante sistemas automatizados, software, algoritmos o inteligencia artificial para la pública difusión su imagen corporal o audio de voz”. Junto a este artículo, también se modificaría el 211 CP para añadir un párrafo segundo que incluyera la agravante de publicidad en estos casos.

No obstante, algunos autores como Jareño Leal consideran que esta propuesta queda incompleta, al sugerir la propia ley que dichos contenidos pueden no ser penados o gravados con responsabilidad civil si “se incluye de forma clara y sobresaliente que el contenido ha sido generado por inteligencia artificial”. Esto se contrapone al derecho de la propia imagen y el principio de disposición, bajo el que cada individuo es quien tiene la capacidad de decidir cuándo y quién puede disponer de su imagen para reproducirla.

De esta manera, de elaborarse una ley orgánica sobre la materia, esta debiera prever ambos supuestos: tanto la posibilidad de crear *deepfakes* con el objetivo de hacer un daño moral y psíquico, como la posibilidad de crearlos con otros

finés no injuriosos pero igualmente vulneradores de derechos fundamentales, como el de la propia imagen.

Dicha legislación no solo serviría para proteger a las víctimas y perseguir a los actores de estas prácticas, cada vez más frecuentes, sino que también sentarían las bases de una posible regulación futura. Es una realidad innegable que la IA avanza a un ritmo que el Derecho actual es incapaz de alcanzar, por lo que solo nos queda esperar y legislar sobre los casos que se dan. Pero, ¿hasta dónde llegará? Esa es una cuestión para la cual no hay respuesta todavía, pero quizá por esa misma incertidumbre resulta necesario asentar unas bases que ofrezcan un cierto nivel de protección actual y permitan un desarrollo normativo en un futuro con más conocimiento y experiencia.

Una vez conseguida una base normativa sólida, surge la nueva preocupación de garantizar el cumplimiento de esta y su efectiva aplicación en los procesos judiciales. El análisis del material generado con inteligencia artificial es una tarea más ardua de lo que pueda parecer, precisando en ocasiones de expertos que evalúen la veracidad de las pruebas. Delegar esta responsabilidad en los jueces sería inviable, no solo por su inexperiencia y falta de conocimientos técnicos digitales.

Como sucede con otros materiales probatorios, quizá podrían derivarse a una institución externa pero dependiente de los ministerios de justicia, que velase por el correcto uso de las inteligencias artificiales y sirviera de perito corporativo sistemático. ¿Pero esto significaría hacer un sistema pericial masivo con cada prueba digital que pasara por la administración? No tendría por qué. Se podría implantar algún sistema de detección en las pruebas digitales, sistemas que ya se usan en el sector privado para la detección de los *deepfakes*. Dicho mecanismo no es una idea descabellada, pues los sistemas de cribado o filtro llevan años implantados en el ámbito educativo y universitario para evitar plagios. Una institución gubernamental que se dedicara a gestionar dicho sistema y a la cual podría acudir en caso de peritaje adicional sería la encargada de velar por el cumplimiento de las normas, al igual que hacen otras instituciones como la Agencia Española de Protección de Datos. Y es que el único remedio frente a la demonización de la inteligencia artificial es su uso respetuoso con los cauces jurídicos.

Referencias bibliográficas

- BODEN, M: *AI: Its Nature and Future*. Oxford University Press, Oxford, 2016.
- CARO CORIA, D. C.: “Las garantías constitucionales del proceso penal”, en: *Anuario de Derecho Constitucional Latinoamericano*, 2006, pp. 1028-

1045. Disponible en: <https://biblioteca.corteidh.or.cr/tablas/R08047-30.pdf> [Consultado: 10 de junio de 2024].
- DAGAR, D.; KUMAR VISHWAKARMA, D.: “A Literature Review and Perspectives in Deepfakes: Generation, Detection, and Applications”, en: *International Journal of Multimedia Information Retrieval*, vol. 11, julio de 2022, pp. 219-289. Disponible en: <https://link.springer.com/article/10.1007/s13735-022-00241-w> [Consultado: 7 de junio de 2024].
- ESPAÑA, JEFATURA DEL ESTADO. Ley Orgánica 1/1982 (5 de mayo de 1982) de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en: *Boletín Oficial del Estado*, núm. 115, 1982, pp. 1-7. Disponible en: <https://www.boe.es/buscar/pdf/1982/BOE-A-1982-11196-consolidado.pdf> [Consultado: 7 de junio de 2024].
- ESPAÑA, CONGRESO DE LOS DIPUTADOS. Proposición de Ley Orgánica (13 de octubre de 2023) de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, en: *Boletín Oficial de las Cortes Generales*, núm. 122/000011, 2023. Disponible en: https://www.congreso.es/public_oficiales/L15/CONG/BOCG/B/BOCG-15-B-23-1.PDF [Consultado: 6 de junio de 2024].
- ESPAÑA. FISCALÍA GENERAL DEL ESTADO: “Circular 2/2015 (19 de junio de 2015) sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015”, en: *Boletín Oficial del Estado*, ref. FIS-C-2015-00002, 2015. Disponible en: https://www.boe.es/buscar/abrir_fiscalia.php?id=-FIS-C-2015-00002.pdf [Consultado: 15 de junio de 2024].
- FERREIRA, K. “Tipos de Inteligencia Artificial: conoce cuáles existen y cómo usarlos”, en *Rockcontent*, 20 de julio del 2021. Disponible en <https://rockcontent.com/es/blog/tipos-de-inteligencia-artificial/> [Consultado: 30 de junio de 2024].
- GARCÍA-ULL, F. J.: “Deepfakes: el próximo reto en la detección de noticias falsas”, en: *Anàlisi: Quaderns de comunicació i cultura*, núm. 64, junio de 2021, pp. 103-120. Disponible en: <https://analisi.cat/article/view/v64-garcia> [Consultado: 8 de junio de 2024].
- GROTHAUS, M.: *Trust No One: Inside the World of Deepfakes*. Hachette UK, Londres, 2021.
- GUTIÉRREZ SULLCA, E. M.: “Artificial Intelligence Techniques for Detecting Deepfakes and their Impact on the Veracity of Online Content”, en: *International Journal of Systems Engineering*, vol. 4, núm. 2, 2023, pp. 6-9. Disponible en: <https://systemjournal.org/index.php/ijse/article/view/39/26> [Consultado: 12 de junio de 2024].

- HAO, K.: “Deepfake Porn is Ruining Women’s Lives. Now the Law May Finally Ban It”, en *MIT Technology Review*, 12 de febrero de 2021. Disponible en: <https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/> [Consultado: 9 de junio de 2024].
- JAREÑO LEAL, Á.: “El derecho a la imagen íntima y el Código Penal: la calificación de los casos de elaboración y difusión del *deepfake*”, en: *Revista Electrónica de Ciencia Penal y Criminología*, núm. 26, 2024, pp. 1-37. Disponible en: <http://criminnet.ugr.es/recpc/26/recpc26-09.pdf> [Consultado: 12 de junio de 2024].
- LLORÍA GARCÍA, P.: “Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral (especial referencia al ‘sexting’)”, en *La ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, núm. 105, 2013, pp. 215-232.
- RANA, S. *et al.*: “Deepfake Detection: A Systematic Literature Review”, en: *IEEE Access*, vol. 10, 2022, pp. 25494-25513. Disponible en: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9721302> [Consultado: 11 de junio de 2024].
- RODRIGO LÓPEZ, J. F.: “Tragic Realism: How to Regulate Deepfakes in Colombia?”, en: *Latin American Law Review*, núm. 8, 2022, pp. 125-145. Disponible en <https://doi.org/10.29263/lar08.2022.08>. [Consultado: 30 de junio de 2024].
- SIMÓ SOLER, E.: “Retos jurídicos derivados de la Inteligencia Artificial Generativa: *deepfakes* y violencia contra las mujeres como supuesto de hecho”, en: *InDret Criminología: Revista para el Análisis del Derecho*, núm. 2, 2024, pp. 493-515. Disponible en: <https://indret.com/wp-content/uploads/2023/04/1767.pdf> [Consultado: 14 de junio de 2024].
- UNIÓN EUROPEA. PARLAMENTO EUROPEO, CONSEJO EUROPEO: “Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828”, en *Diario Oficial de la Unión Europea*, 10 de junio de 2024.