DEEPFAKES EN EL PROCEDIMIENTO PROBATORIO[*]

DEEPFAKES NO PROCEDEMENTO PROBATORIO

DEEPFAKES IN THE EVIDENTIARY PROCEDURE

Rubén Blázquez Moreno[**]
A Coruña

RESUMEN: El desarrollo de aplicaciones con base en inteligencia artificial permite a los usuarios potenciar la eficiencia de sus recursos disponibles a la hora de desarrollar una determinada tarea. No obstante, cualquier herramienta puede utilizarse para fines cuestionables y la inteligencia artificial no es una excepción.

Uno de los fines maliciosos que puede tener el uso de aprendizaje profundo es la creación de deepfakes. A través de las ultrafalsificaciones, al presentar apariencia de realidad, es posible alterar la percepción del destinatario de la misma.

Esta cuestión motiva la realización del trabajo, en el cual se analiza la posibilidad de que una deepfake sea introducida en un procedimiento judicial, cómo se podría evitar y las consecuencias que podría acarrear su aportación.

Palabras claves: *Deepfake*, aprendizaje profundo, inteligencia artificial, prueba.

ABSTRACT: The development of Artificial Intelligence-based applications enables users to save resources that were previously required to perform a specific task. However, any tool can be used for questionable purposes and Artificial Intelligence is no exception.

One malicious purpose of AI is the use of deep learning to create deepfakes, which can alter the recipient´s perception by presenting a seemingly real appearance.

This issue motivates the present work, in which we will analyse the possibility of a deepfake being introduced into a legal proceeding, how it could be prevented, and the consequences that could result from it use.

Keywords: Deepfake, deep learning, Artificial Intelligence, evidence.

* * *

---

[*] El trabajo ha obtenido el Premio Instituto Vasco de Derecho Procesal en su XIII Edición del año 2023.
[**]Rubén Blázquez Moreno. Universidade da Coruña.

KES COMO PRUEBA EN EL PROCESO. 5.1. Delito de estafa procesal. 5.2. Impugnación de sentencias firmes. 6. CONCLUSIONES. 7. BIBLIOGRAFÍA.

1. INTRODUCCIÓN

Múltiples voces consideran que la humanidad se enfrenta a una nueva revolución industrial-digital, en concreto la cuarta revolución industrial o Industria 4.0[1]. Más precisamente, se apunta que actualmente se vive la era de la digitalización[2], digitalización que se consigue mediante la aplicación de tecnologías de la información y comunicación en el ámbito laboral-profesional.

Estas tecnologías proporcionan herramientas que, aplicadas al día a día, permiten facilitar tareas que antes eran más gravosas de realizar o requerían de mayor inversión temporal o de capital humano. No es algo nuevo. Basta con pararse a pensar, por ejemplo, cómo cambió el concepto de oficina tras la introducción de ordenadores y otras tecnologías informáticas en los años sesenta.

Actualmente, se está viviendo otro punto de inflexión. Pero esta revolución no es tan "física" como la vivida años atrás. Gracias al desarrollo de la ciencia informática, surgen nuevas formas en las que la tecnología se integra en las sociedades, resolviendo problemas de los individuos. Y es que las ciencias computacionales han desarrollado una infraestructura mundial que permite la hiperconectividad, la comunicación en tiempo real y el procesamiento masivo de datos[3]. Hecho que, a su vez, ha permitido el desarrollo y consolidación de tecnologías disruptivas como Blockchain, Big Data, Inteligencia artificial (en adelante IA), Tecnología 5G-Internet de las Cosas (IoT), etc.

Precisamente este trabajo pretende abordar el fenómeno de las aplicaciones de IA en un concreto aspecto, el procedimiento de prueba en el ordenamiento jurídico español. Hay que entender a las aplicaciones de IA como instrumento que consigue facilitar el uso de herramientas digitales. Funciones que tradicionalmente requerían de una inversión de recursos significativos para lograr dominarlas, con la inteligencia artificial, puede desarrollarse, en cuestión de minutos, un trabajo de cierta calidad aplicando estos instrumentos[4]. O, a título ilustrativo, cómo pueden automatizar procesos y realizar una tarea en menor tiempo[5], en otras palabras, el potencial ámbito de aplicación de estos instrumentos, es inmensurable.

Concretamente, en este trabajo se pone el foco en la cuestión de la manipulación de imágenes, vídeos y demás contenidos, a través de sistemas de IA generadores de *deepfakes*. Si

---

[1]Múltiples autores hacen referencia a este concepto que fue acuñado por Klaus Schwab en su libro de título homónimo: *La cuarta revolución industrial* (2016).

[2] Hay quienes afirman que vivimos en la "era de la IA". Como máximo referente de esta posición, hay que mencionar a Bill Gates, ya que en su propio Blog GatesNotes, establece este concepto y reflexiona sobre el fenómeno de la Inteligencia Artificial en lo relativo a su impacto en la sociedad actual. Disponible en: https://www.gatesnotes.com/The-Age-of-AI-Has-Begun#ALChapter6 [Consulta 26/03/2023].

[3] ENCINAS GRIJALVA, M. d. S. (2021). *La innovación disruptiva como recurso para la transformación de modelos de negocios en medios de comunicación*. [Tesis] pp. 219-225. Madrid. Disponible en https://eprints.ucm.es/id/eprint/67599/.

[4] Pensemos, por ejemplo, en un programador, puede realizar más rápido su trabajo con la herramienta "Blackbox", obviamente debe de contar con conocimientos en la materia para especificar concretamente qué código necesita. Disponible en: https://www.useblackbox.io/. [Consulta 29/03/2023].

[5] "Copy.ai" permite a un usuario crear contenidos (monetizables) para sus redes sociales simplemente rellenando un formulario. Disponible en: https://www.copy.ai/social-media-managers. [Consulta 29/03/2023].

bien, herramientas y técnicas para manipular esos contenidos existen desde hace años, el uso de aplicaciones de inteligencia artificial hace posible que un usuario promedio, entendido como aquel que no cuenta con la pericia necesaria en el uso de herramientas digitales, pueda manipular estos contenidos[6] logrando resultados de calidad.

La manipulación de contenidos audiovisuales es uno de los métodos de ingeniería social que puede condicionar la realidad social (a título ilustrativo, a través de las *fake news)*. Como ejemplo, a finales de marzo de 2023 circularon una serie de imágenes generadas por IA donde se "detiene" al expresidente de los Estados Unidos, Donald Trump[7]. Este fenómeno, en el que se presenta como protagonista a un personaje influyente puede llegar a ser fuente de un problema de orden público[8].

Las *deepfakes*, incluso, se pueden considerar un arma de las guerras híbridas. Como ejemplo, el "vídeo" de la rendición de Zelenski[9]. Debido a esto, los gobiernos nacionales y organizaciones internacionales, en sus ámbitos de actuación trabajan para mitigar los posibles efectos perjudiciales para el país[10].

Este fenómeno preocupa a nivel mundial, países como China han tomado medidas y desarrollado su propia regulación jurídica de las *deepfakes[11]*, prohibiendo el uso de representaciones sintéticas para difundir noticias falsas o información perjudicial para la economía, la seguridad social o la imagen de China.

A nivel europeo, también preocupa este fenómeno, la propia EUROPOL en uno de sus informes de 2020[12] advierte de los potenciales peligros de las *deepfakes* en relación con la desinformación. En otro extremo, existe una Propuesta de Reglamento de Ley de Inteligencia Artificial, que recientemente ha sido aprobada en primer ciclo por el Parlamento Europeo[13]. Esta propuesta se centra en la clasificación en función del riesgo a los tratamientos de datos con técnicas de inteligencia artificial y prohíbe ciertos tratamientos, como el reconocimiento facial en tiempo real en los espacios públicos. En el caso concreto de las *deepfakes*, la Propuesta de Reglamento indica que son tratamientos de riesgo alto, por lo tanto, los operadores que quieran usar la tecnología de generación de representaciones sintéticas, deben cumplir

---

[6] Un ejemplo de herramienta de manipulación-generación de vídeos o imágenes accesible es "runway". Disponible en: https://runwayml.com/. [Consulta 31/03/2023].

[7] Disponible en: https://www.elmundo.es/internacional/2023/03/23/641c97c921efa034268b45b0.html [Consulta 31/03/2023].

[8] QUIRÓS-FONS, A., & GARCÍA-ULL, F. J. (2022). "La Inteligencia Artificial como herramienta de la desinformación: deepfakes y regulación europea". En E. G.-A. Palacios, Los derechos humanos en la inteligencia artificial: su integración en los ODS de la Agenda 2030, pp. 537-555, p.539. Pamplona: Thomson Reuters Aranzadi.

[9] Disponible en: https://unaaldia.hispasec.com/2022/03/la-rendicion-de-zelenski-el-poder-del-deepfake.html [Consulta 31/03/2023].

[10] En ese sentido, la Secretaría Técnica de la Fiscalía General del Estado en 2021 elaboró un informe sobre el tratamiento penal del fenómeno de la desinformación. Disponible en: https://www.icab.es/export/sites/icab/.galleries/ documents-noticies/ tratamiento-penal-de- las-fake-news- fiscalia-general-del-estado.pdf.

[11] Disponible en: https://www.reasonwhy.es/actualidad/china-regulacion-deepfakes-etiquetado-consentimiento-inteligencia-artificial [Consulta el 14/06/2023].

[12] EUROPOL. (2020). *Malicious Uses and Abuses of Artificial Intelligence.* Disponible en: https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf [Consulta el 14/06/2023].

[13] Disponible en: https://www.businessinsider.es/parlamento-europeo-vota-hoy-reglamento-ia-estas-son-claves-1259232 [Consulta el 15/06/2023].

con una serie de condiciones que se le imponen. Por ejemplo, una de las condiciones que deben cumplir es dejar claro para el usuario que el contenido como no real. Para ello, el archivo será etiquetado como una ultrafalsificación.

En lo que respecta al Estado español, una de las principales preocupaciones del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación es la lucha contra la desinformación[14]. Por tanto, las ultrafalsificaciones son también una preocupación para el legislador español, ya que son una de las nuevas armas de desinformación disponibles.

También pueden ser una amenaza para la privacidad personal, pues diversos estudios han probado que los mecanismos de seguridad basados en reconocimiento facial o, incluso de voz de nuestros dispositivos electrónicos, pueden ser sorteados gracias a un *deepfake* del legítimo usuario del mismo[15].

Por todo ello, es razonable argumentar que se presenta un cambio de paradigma. Si bien, en el pasado, una evidencia proporcionada a través de una imagen o de un vídeo, era una fuente de prueba que podía influir en la formación del juicio de valor en una persona, actualmente, con el aumento exponencial de la utilización de *deepfakes*, pueden darse diversos escenarios de manipulación social: a través de la generación de *fake news*, con la consiguiente pérdida de confianza ante estos contenidos como fuentes de información[16], estafas, suplantaciones de identidad, etc.

2. CONCEPTOS

2.1. Definición *deepfake*:

Etimológicamente "*deepfake*" viene de la combinación de dos vocablos: "deep" y "fake". "Deep" se refiere al proceso de generación vía aprendizaje profundo (o "deep learning"), la cual, a su vez, es un método de aprendizaje automático (o "machine learning"), sistema de IA que se desarrolla en el campo de las ciencias de la informática[17]. Por su parte, "fake" hace alusión a algo que es falso. En su conjunto, como primera noción, podría entenderse por la creación de contenidos falsos a través de técnicas de aprendizaje profundo.

El término en castellano que suele emplear la doctrina para referirse a este fenómeno es "representación sintética"[18] o "ultrafalsificación". Como tal, no existe definición del anglicismo en sí en el diccionario de la Real Academia Española, por lo tanto, acudir a las definiciones de "representación" y "sintético, ca" respectivamente, proporcionará un acercamiento al concepto que maneja la doctrina.

---

[14] Disponible en: https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/LaLuchaContraLaDesinformacion.aspx [Consulta el 14/06/2023].

[15] ESAGE, A. (22 de marzo de 2022). "¿Cómo usar deepfake para engañar a los sistemas biométricos de autenticación FLV?" *Noticias de seguridad informática*. Disponible en: https://noticiassegu ridad.com/seguridad-informatica/como-usar-deepfake-para-enganar-a-los-sistemas-biometricos-de-autenticacion-flv/ [Consulta 02/04/2023].

[16] En este sentido, HODGE D., S. J. (2021). Don't Always Believe What You See: Shallowfake and Deepfake Media Has Altered the Perception of Reality. *Hosfra Law Review*, pp. 51-80, p. 56., recoge el concepto de "apatía por la realidad", haciendo referencia al fenómeno en el que las personas repudien pruebas de vídeo que si muestran la realidad.

[17] Disponible en https://seon.io/es/recursos/glosario/deepfake/ [Consulta el 08/03/2023].

[18] QUIRÓS-FONS, A., & GARCÍA-ULL, F. J. (2022). "La Inteligencia Artificial… Op. cit.

Sobre el vocablo "representación" son de interés para el trabajo las siguientes acepciones: "*1. Acción y efecto de representar." "2. Imagen o idea que sustituye a la realidad." "4. Cosa que representa otra."*

Respecto "sintético, ca", interesa: "*3. Dicho de un producto: Que se obtiene por procedimientos industriales y que reproduce la composición y propiedades de uno natural."*

Por tanto, se entiende como "representación sintética" aquella representación obtenida por un procedimiento informático, que reproduce la composición y propiedades de otra imagen, pretendiendo sustituir la realidad, representando otra cosa que realmente puede no haber ocurrido como se muestra en ese archivo informático.

Aclarados estos aspectos, una aproximación más técnica podría ser la que brinda la Propuesta de Reglamento de Inteligencia Artificial[19], una *deepfake* sería 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.

Las deepfakes, dependiendo de su calidad de desarrollo, pueden llevar a engaño tanto a personas como a algoritmos[20]. Piénsese en un smartphone que puede ser desbloqueado por reconocimiento facial de su legítimo propietario. Cabe adelantar que el uso de una *deepfake* puede soslayar esta medida de seguridad y dar acceso a dicho dispositivo[21]. Esta realidad se desarrollará más adelante.

Hay que destacar que no es algo ajeno a la realidad social, pues en la actualidad, con el uso masivo de redes sociales, estas técnicas de manipulación están muy accesibles a la mano de sus usuarios. Ello a través de la posibilidad de aplicar filtros en sus publicaciones, entre los cuales, uno de realidad aumentada que retoque las facciones de la cara de una persona usuaria para hacerle más estética podría coincidir con la acepción de *deepfake*.

Para adquirir una noción sólida de *deepfake*, se debe distinguir de las *shallowfakes*. Como se apunta en la introducción, la manipulación de imágenes y videos no es algo novedoso. Las herramientas de inteligencia artificial hacen que la manipulación sea más sofisticada. Pero, antes de su existencia, era posible manipular un contenido audiovisual, mediante su edición[22]: alterando la velocidad de reproducción, cortando partes de la misma, o, simplemente, sacando de contexto dicho contenido, pero sin cambiar el contenido de modo alguno.

En un *shallowfake* no intervienen sistemas de aprendizaje profundo, siendo esta la principal diferencia respecto a sus homólogas, las *deepfakes*. Las *shallowfakes* pueden generarse con un software de edición estándar, lo que inevitablemente significará la inversión de una cantidad ingente de tiempo en el mismo por parte del creador (comparada con el tiempo

[19] Enmienda 203 a la Propuesta de Reglamento por el que se establecen normas armonizadas de inteligencia artificial (Ley de Inteligencia Artificial) y que modifica determinadas actos legislativos de la Unión Europea. Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_ES.html.

[20] HERNANDEZ-ORTEGA, J., FIERREZ, J., MORALES, A., & GALBALLY, J. (2023). Introduction to presentation attack detection in face biometrics and recent advances. *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment*, pp. 203-230.

[21] Investigadores de las universidades de Pensilvania, Zhejiang y Shandong, han desarrollado un marco de ataque denominado "LiveBugger". Atestiguan, en sus conclusiones, que la mayoría de los sistemas de reconocimiento facial en directo son altamente vulnerables a los ataques basados en deepfake. Disponible en: https://arxiv.org/abs/2202.10673.

[22] KOCSIS, E. (2021). Deepfakes, Shallowfakes, and the Need for a Private Right of Action. *Dickinson L. Rev., 126*, p. 621.

invertido generando una representación sintética)[23]. Identificándose como otra de las principales características diferenciadoras de ambos fenómenos: el ahorro del tiempo. Ahorro no solo en la edición, sino también la formación del usuario; inclusive un ahorro económico, pues un usuario que no desee adquirir competencias en una herramienta de edición debería contratar a otra persona, siendo potencialmente más costoso que el uso de un sistema de IA.

2.2. Cómo se crea una *deepfake*:

Las *deepfakes* funcionan gracias a las Redes Adversarias Generativas (en inglés GAN)[24], un tipo de algoritmo que se utiliza en el campo del aprendizaje automático no supervisado (*deep learning*) para el procesamiento de imágenes, visión artificial y generación de imágenes, todo ello con base en la teoría de juegos[25]. En concreto, esta tecnología aplica el marco de juego cooperativo de suma cero. Como su nombre indica, se compone de más de una red neuronal, en concreto de dos: una denominada "generadora" y la otra "red de coste o discriminadora". Un sistema generador de *deepfakes*, se compone, a grandes rasgos, de los siguientes elementos:

La red generadora, se encarga de crear un input para la red de coste. Es decir, genera un contenido a través de la fusión, combinación, reemplazo, superposición, permuta, etc. de imágenes y vídeos. Es así como es posible crear un vídeo "falso", ello debido a que puede ser creado un contenido que en sí nunca hubiera existido, pero con apariencia de realidad[26]. Una vez finalizada su tarea, envía ese archivo a la red de coste para procesarlo.

Por su parte, la *red de coste o discriminadora* es una red neuronal convolucional[27] que se ocupa de decidir si cada instancia de datos que revisa pertenece o no al conjunto de datos de entrenamiento. Se trata de una especie de control de calidad del output de la red generadora, determinando si este es realista o no a los datos de entrenamiento. A tenor del resultado que arroje, la red generadora "aprenderá" de los fallos que ha cometido y no los perpetuará, consiguiendo una reducción gradual de los recursos[28], pues esa resolución pasa a ser parte de los datos de entrenamiento de la red. Y así es como la red aprende por sí misma.

Son "adversarias" puesto que una red compite con la otra. Es decir, la red generadora crea un contenido audiovisual y lo envía a la red discriminadora, la cual determina si su elaboración cumple con los requisitos de realidad que previamente extrajo del conjunto de da-

---

[23] Un ejemplo de herramienta para la creación de *shallowfakes* es *vidyo.ai*. Se trata de una aplicación que permite crear vídeos cortos a partir de secuencias más extensas. La propia herramienta selecciona los momentos más importantes o impactantes del video, los edita y subtitula. Incluso, esta aplicación permite exportar el vídeo a plataformas de consumo de contenidos como YouTube. Disponible en https://vidyo.ai/ [Consulta el 18/03/2023].

[24] QUIRÓS-FONS, A., & GARCÍA-ULL, F. J. (2022). "La Inteligencia Artificial… Op. cit. p. 538.

[25] GOODFELLOW, I. et. al. (Noviembre de 2020). "Generative adversarial networks." *Communications of the AC, 63*(11), pp. 139-144. doi: https://doi.org/10.1145/3422622.

[26] El resultado de esta función depende en gran medida de la calidad de, entre otros, los datos de entrenamiento, del tiempo de entrenamiento, de la arquitectura de diseño de la red neuronal propiamente dicha, su programación, etc. Llegar a un resultado muy perfecto es costoso tanto en el plano económico, como de recursos técnicos, lógicos, energéticos, de tiempo, etc.

[27] O CNN (Convolutional Neural Network), son modelos de aprendizaje profundo que permiten principalmente el reconocimiento de imágenes, permitiendo etiquetar, porcentualmente, una imagen en función de las categorías que correspondan. En este caso: real o no real.

[28] CANZANI, A., & LECUN, Y. (2020). NYU Center for Data Science. Obtenido de NYU Deep Learning Spring 2020. Disponible en: https://cds.nyu.edu/deep-learning/ [Consulta el 08/02/2023].

tos de entrenamiento. En caso de no superar este "juicio", la red generadora recibe esta crítica como un dato que le permite autoajustarse para realizar un nuevo contenido que pueda ser capaz de superar ese estándar. Y, a su vez, la red discriminadora "aprende" de los patrones de creación de la generadora para aumentar el nivel de filtro, consiguiéndose, con este proceso de escalabilidad, mejores resultados. Usando la terminología de la teoría de juegos, cabe indicar que con este proceso se llega a un equilibrio de Nash[29].

En sí, su funcionamiento matemático, se basa en las funciones objetivas que, siendo incompatibles entre sí, deben minimizarse simultáneamente para llegar a un equilibrio entre ambas.

Para generar una representación sintética, el primer paso es que el usuario determine el resultado deseado para crear un conjunto de datos de entrenamiento (imágenes, sonidos, vídeos) que sustenten el resultado potencial deseado. A continuación, se aleatorizarán y se insertarán en la red generadora. La propia red neuronal, extraerá su propio concepto de realidad en base a estos datos de entrenamiento y generará un determinado contenido. Dicho concepto de realidad irá mutando cada vez que ambas redes "se enfrenten".

2.3. Perfil y usos de la tecnología *deepfake*.

El perfil de actores que produce *deepfakes* es muy amplio. Cualquier persona que quiera crear una representación sintética tiene a su alcance innumerables herramientas para ello, muchas de ellas gratuitas. Ahora bien, entre ellos es posible distinguir ciertas categorías de usuarios que generan *deepfakes*: comunidades de aficionados[30], profesionales de la política, delincuentes, actores profesionales, productores audiovisuales, agencias de publicidad, investigadores científicos, etc.

Las representaciones sintéticas, en tanto que herramienta de creación, pueden ser usadas con trasfondos más o menos legales. Todo dependerá de la finalidad que maneje el productor al realizar el contenido. Por una parte, se pueden poner en relieve algunos usos legítimos y, por otra parte, otros cuya legalidad puede estar en entredicho.

Algunos ejemplos de índole positiva:

Para el ámbito del marketing, se pueden realizar campañas publicitarias con personas famosas que ya han fallecido[31] o, incluso de personas que no existen en la realidad. Hay que precisar que, a fecha de mayo de 2023, los comerciales realizados completamente por he-

[29] El equilibrio de Nash, concepto desarrollado por John Nash en 1951, hace referencia a la solución que se da en un juego en el que intervienen dos o más jugadores. Tradicionalmente se explica el equilibrio de Nash haciendo referencia al dilema del prisionero. Es una solución óptima para todos los jugadores pues todas han elegido la mejor estrategia según las que los demás han estado utilizando, es decir, se intenta llegar a una estrategia que maximice el beneficio individual lo mejor posible y, por consiguiente, significa que no hay incentivo alguno para el jugador de cambiar de estrategia pues es conocedor de que no hay mejor opción.

[30] Cualquier persona que pueda acceder a un ordenador y que tenga un mínimo conocimiento de computación, podría realizar una representación sintética por su cuenta. Tarea que se facilita gracias a los repositorios de código, véase: https://github.com/, en concreto su apartado *DeepFaceLab* (https://github.com/iperov/DeepFaceLab) donde se puede encontrar guías y demás recursos creados por la comunidad, para aprender a crear *deepfakes*.

[31] Anuncio de una conocida marca de cervezas que revive a Lola Flores. Disponible en https://sevilla.abc.es/sevilla/sevi-making-hizo-anuncio-cruzcampo-lola-flores-y-tecnica-deepfake-02101211457noticia.html [Consulrta el 20/04/2023].

rramientas de IA[32], no tienen un aspecto depurado. Pero, con la repercusión mediática que genera actualmente el concepto de inteligencia artificial, logran sus fines propagandísticos (en tanto que, usando estas herramientas consiguen que los medios les dediquen atención mediante alguna publicación). Hay que destacar que, de esta manera, una productora evitaría riesgos respecto a posibles infracciones de la normativa relativa al tratamiento de datos personales[33], puesto que se están tratando los datos personales de una persona fallecida, hecho que implica que el tratamiento no esté dentro del ámbito de aplicación de la normativa de protección de datos.

Respecto de la industria cinematográfica, es por todo el mundo conocido que una parte notable de los presupuestos de los largometrajes se destinan a sufragar los gastos en la generación de efectos especiales, hay empresas que se dedican en exclusiva a realizar este cometido[34]. Una labor que es bastante cuantiosa no solo en términos monetarios, si no también temporales, requiriendo invertir muchas horas de personal cualificado. Horas que pueden verse mermadas gracias al uso de herramientas de IA[35] y, como se viene reflejando, el acceso libre a estas tecnologías permite que cualquier usuario pueda llevar a cabo trabajos de alta calidad[36].

En el campo médico existen innumerables aplicaciones de esta tecnología. El hecho de que exista un propio campo de estudio, la ingeniería biomédica, da buena fe de ello. Por poner de relieve una de las posibles aplicaciones de las redes convolucionales es la detección de enfermedades: en la sangre[37], cánceres[38], etc.

El mundo jurídico tampoco escapa de los posibles usos de la IA. Esto puesto que es posible redactar textos legales[39] (con mayor o menor acierto[40]) o, incluso para ayudar a la mo-

---

[32] Caso de la productora londinense "Privateisland.tv", genera un comercial de cerveza, denominado "*Synthetic Summer*" exclusivamente aplicando métodos de inteligencia artificial, RIVERO, T. (3 de mayo de 2023). Disponible en https://hipertextual.com/2023/05/anuncio-cerveza-generado-inteligencia-artificial-una-autentica-pesadilla [Consulta el 05/05/2023].

[33] No entra en ninguno de los ámbitos de aplicación que detalla el artículo segundo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[34] Como curiosidad y a título de ejemplo, la mercantil española Drama FX S.L. se dedica a esta labor.

[35] Disponible en https://www.xataka.com/inteligencia-artificial/animar-will-smith-digital-geminis-ha-costado-millones-hollywood-ve-cercano-uso-masivo-deepfakes-cine#comments-close [Consulta el 15/05/23].

[36] Un ejemplo notorio de esta afirmación es el siguiente audiovisual realizado por un grupo de aficionados, no profesionales del mundo del cine, que consiguen recrear una escena de una conocida serie pero con mayor calidad, aplicando técnicas de manipulación sintética de la imagen. https://www.youtube.com/watch?v=861gfPVmgdc.

[37] PÉREZ GÓMEZ, A. (2020). *Redes Generativas Antagónicas para la estandarización de imágenes de células de sangre periférica.* Barcelona: Universidad Politécnica de Cataluña Barcelonatech. Disponible en https://upcommons.upc.edu/handle/2117/182625 [Consulta el 19/05/2023].

[38] La Sociedad Española de Senología y Patología Mamaria, recoge en una de sus entradas de blog los beneficios de usar el triaje basado en herramientas de IA para reducir la carga de trabajo de los radiólogos, pudiendo este personal experto dedicarse a casos "más complejos". Disponible en https://www.sespm.es/inteligencia-artificial-para-el-diagnostico-de-cancer-de-mama/ [Consulta el 25/05/2023].

[39] Por ejemplo, un reconocido despacho de abogados ha desarrollado, para uso interno, un sistema de IA que redacta textos legales. Disponible en https://www.elconfidencial.com/juridico/2023-02-15/allen-overy-lanza-una-herramienta-de-ia-para-redactar-textos-legales_3576481/ [Consulta el 14/06/2023].

tivación de sentencias judiciales[41]. Todo ello logrado gracias al uso de un sistema de IA generativa, sería, por ejemplo el caso de ChatGPT-3.

Otra posible aplicación relacionada con el derecho sería generar, mediante herramientas de creación de *deepfakes*, contenidos que sirvan para que las autoridades policiales puedan avanzar en sus investigaciones de ciertos tipos de delitos. Por ejemplo, para desarticular una organización criminal que se dedique a pornografía infantil, puede ser necesaria la aplicación de la diligencia de investigación del agente infiltrado. En este concreto caso, sería un agente informático, es decir, no hay exposición física del individuo como sería una infiltración "más tradicional".

Para poder acceder a la red pornográfica, podría llegar a ser necesario aportar contenidos de pornografía de menores[42], ello con el objetivo de ganarse la confianza de los sujetos que integren la organización. Aquí sería útil un sistema programado para generar este contenido[43]. Pues, de esta manera no se atentaría contra los derechos o libertades de ninguna persona ya que quien aparecería en ese contenido no sería una persona real. Por tanto, esta tecnología podría ser de utilidad para la fase de investigación, siempre y cuando, dicho sistema cumpla con el ordenamiento jurídico y la posible regulación policial interna que se le debiera de aplicar.

Sin embargo, esta tecnología también puede servir para fines fraudulentos como para facilitar la vulneración de las interfaces de programación de aplicaciones (Aplication Programming Interfaces o APIs) de reconocimiento facial. Estas aplicaciones se suelen usar para el desbloqueo de dispositivos electrónicos, como mecanismo de seguridad para medios de pagos con estos artilugios (como, por ejemplo, el sistema de pago de Apple, que requiere de verificación facial para realizar el pago). Investigadores de la Universidad de Sungkyunkwan[44] en 2021 lograron superar APIs de reconocimiento facial usando *deepfakes*.

Para realizar suplantaciones de identidad con las cuales realizar estafas. Un claro ejemplo es la integración en la "estafa del CEO" de técnicas de ultrafalsificaciones para lograr que este tipo de *phishing* consiga engañar a la víctima de este fraude[45]. Hay que remarcar que esta práctica es extrapolable a otros ámbitos, no solo al mundo empresarial. Ya es una reali-

---

[40] En relación a ello, un abogado utilizó Chat GPT para fundamentar uno de sus escritos y el sistema inventó legislación. Disponible en https://www.xataka.com/legislacion-y-derechos/abogado-uso-chatgpt-juicio-ahora-quien-debe-dar-explicaciones-a-juez-incluir-citas-falsas [Consulta el 14/06/2023].

[41] En Colombia, el juez presidente del Juzgado Primero del Circuito de Cartagena Juan Manuel Padilla García apoyó la motivación de una de sus sentencias en base a respuestas generadas por ChatGPT. Disponible en: https://elcierredigital.com/salud-y-bienestar/998940193/chat-gpt-ya-utilizado-dictar-sentencias-judiciales-analizamos-pros-contras.html [Consulta el 14/06/2023].

[42] Posibilidad que brinda el artículo 282 bis 6 LECrim: "*El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.*".

[43] BLANCO, H. (2021). El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre. *InDret, 1*, pp. 431-501. p. 474.

[44] Citado por SEON, en su glosario, disponible en: https://seon.io/es/recursos/glosario/deepfake/ [Consulta el 08/03/2023].

[45] STUPP, C. (30 de agosto de 2019). Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The wall street journal*. Disponible en: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 [Consulta el 25/05/2023].

dad usar técnicas de IA para realizar estafas más "personales" aprovechando vínculos familiares o sentimentales, para chantajear a cualquier persona[46].

También es posible su uso para producir manipulación del mercado. Crear una *deepfake* de una persona relevante en una concreta mercantil cotizada, puede hacer que la tendencia del mercado mute. Una ultrafalisificación puede generar una suerte de situaciones irreales de posición privilegiada, que hipotéticos inversores aprovecharían y perderían el capital invertido en dicha posición. En el mundo de los criptoactivos, ha ocurrido[47], nuevamente, no es descabellado pensar que la práctica se lleve a terrenos de activos más tradicionales.

Todas estas y más utilidades negativas son los retos a los que se debe enfrentar el legislador. Cuestión que debe ser atendida con prioridad en todos los ordenamientos jurídicos de cada Estado, siendo una situación a la que se le debe dar una respuesta homogénea. Por ello, hay que destacar el papel de la Unión Europea en su labor de estandarización legal de este fenómeno en todos los estados miembros de la misma. Modelo que, desde Bruselas, se busca que sirva como referencia legal a nivel mundial[48].

2.4. Marco legal.

El marco regulatorio general de las representaciones sintéticas, conforme al punto de vista del presente trabajo, vendría conformado por las siguientes normas:

En primer lugar, la Propuesta de Reglamento por el que se establecen normas armonizadas de inteligencia artificial (Ley de Inteligencia artificial) y que modifica determinados actos legislativos de la Unión Europea[49]. Esta propuesta de regulación no prohíbe el uso de tecnologías como las *deepfakes*, sino que impone ciertas acciones a aquellas personas que utilicen esta tecnología.

Estas obligaciones, además de garantizar que las tecnologías de la información y de la comunicación se adecuen al ordenamiento jurídico de la Unión y de sus estados miembros buscan garantizar la transparencia.

La principal garantía de transparencia consiste en la obligación de hacer público que un determinado contenido ha sido generado de forma artificial o que han sido manipulados[50]. El objetivo es tratar de minimizar al máximo posible el riesgo de inducción a error a cualquier

---

[46] VÁZQUEZ, D. (6 de marzo de 2023). Los estafadores están clonando voces con IA para hacerse pasar por familiares que piden ayuda económica. *Business insider*. Disponible en: https://www.businessinsider.es/estafadores-ya-suplantan-voz-ia-hacerse-pasar-familiares-1210564. [Consulta el 04/06/2023].

[47] DI SALVO, M. (25 de mayo de 2022). Deepfake Video of Elon Musk Promoting Crypto Scam Goes Viral. *Decrypt*. Disponible en https://decrypt.co/101365/deepfake-video-elon-musk-crypto-scam-goes-viral [Consulta el 04/06/2023].

[48] A ello se hace referencia expresa en "Un enfoque europeo de la inteligencia artificial". Disponible en; https://digital-strategy.ec.europa.eu/es/policies/european-approach-artificial-intelligence [Consulta el 04/06/2023].

[49] COMISIÓN EUROPEA. (2021). Propuesta de Reglamento por el que se establecen normas armonizadas de inteligencia artificial (Ley de Inteligencia Artificial) y que modifica determinadas actos legislativos de la Unión Europea. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206.

[50] Es de interés mencionar que esta solución se plantea en el punto 178 de la "Resolución del Parlamento Europeo del 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica" (2018/2088(INI)). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019IP0081&from=EN.

persona. Dicha precisión está contenida en el artículo 52.3 de la mencionada Propuesta de Reglamento.

Además, la Propuesta clasifica los distintos tipos de sistemas de inteligencia artificial según su riesgo para con los derechos y libertades individuales. Atendiendo al caso, de acuerdo con el artículo 6º de la norma y su anexo III, los sistemas de generación de ultrafalsificaciones son considerados como sistemas de alto riesgo. Estas mismas obligaciones se aplican a los sistemas de detección de ultrafalsificaciones, pues también son considerados sistemas de alto riesgo (Considerando 38 de la Propuesta de Reglamento). La razón, un sistema opaco de detección de ultrafalsificaciones puede estar diseñado para conseguir el objetivo contrario. Calificar a archivos audiovisuales reales como ultrafalsificaciones, desvirtuando una posible aportación como prueba en un proceso a dicho archivo.

Entonces, para operar en el mercado europeo, será necesario contar con los elementos que refleja el artículo 16 de la Propuesta de Reglamento. Un sistema de gestión de riesgos, documentación técnica accesible y actualizada sobre la herramienta y su funcionamiento, sometimiento a una evaluación de conformidad previa a su introducción en el mercado, conservación de los archivos de registro generados, el proveedor o, en su caso, su representante deben inscribirse, antes de la puesta en servicio del sistema, en la base de datos de la Unión Europea para sistemas de IA de alto riesgo, medidas correctoras en caso de funcionamiento deficiente, información a las autoridades nacionales competentes del estado miembro donde opere el sistema. Además, y en todo momento, los operadores que utilicen en el tráfico jurídico estos sistemas deben poder acreditar frente a las autoridades nacionales competentes el cumplimiento de los requisitos que impone la Propuesta de Reglamento.

También resulta relevante para determinar el marco legal de las ultrafalsificaciones el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en adelante RGPD. Además de su ampliación y desarrollo por el legislador español en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPDGDD en adelante.

El uso de la imagen de una persona física para generar contenidos[51] supone, per se, el tratamiento de sus datos personales. Esto significa que dicha actividad queda comprendida por el ámbito de aplicación de la normativa relativa a la protección de datos.

Esto no impediría la generación de estos vídeos, pues podría ampararse en alguna base de legitimación de la normativa de protección de datos (véase el interés legítimo[52]). máxime cuando son de personas notoriamente públicas, pues entran en colisión derechos fundamentales de ambas partes (derecho de acceso a la información-libertad de expresión versus

[51] Entendiendo como contenido aquel archivo en el que se reproduzca la voz, la imagen o la sucesión de imágenes con o sin audio.

[52] Piénsese en la utilización de técnicas de *deepfake* para generar un contenido didáctico en el que el protagonista sea una persona pública reconocida que ha fallecido. No sería de aplicación la normativa de protección de datos, puesto que no es una persona viva. Tampoco los posibles derechos de propiedad intelectual o de imagen que pudieran ostentar los herederos, quedarían relegados por los límites para finalidades educativas que recoge el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia y el límite de personaje público de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

derecho al honor, a la intimidad personal y familiar y a la propia imagen). Por lo tanto, es necesario realizar un análisis de proporcionalidad para cada caso, hecho que daría lugar a numerosos estudios, no siendo este el objeto del presente.

También resulta relevante, para atender el caso de las ultrafalsificaciones como prueba en el proceso la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, LEC en adelante y Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, en adelante LECrim.

El propio artículo cuarto de la LEC establece el carácter supletorio de la LEC, es decir, se aplicará en todo proceso que carezca de disposiciones regulatorias. O que, en un proceso reglado por normativa procesal propia, un concreto acto que no se contemple en la misma, quedará bajo el ámbito de aplicación de la LEC. Conclusión que puede ser extraída de su artículo cuarto.

Por tanto, se debe atender, en este cuerpo general, a la regulación del procedimiento probatorio general, que se contiene en el Libro II, Título I, Capítulos V y VI. Interesa, para la presente investigación, el artículo 299 LEC[53], en concreto sus apartados segundo y tercero, desarrollados con más detenimiento en la Sección 8ª del Capítulo VI.

Es esta, por tanto, la vía de entrada de archivos audiovisuales como fuente de prueba al proceso civil. Y como tal, es también la vía de entrada de las representaciones sintéticas, pues atendiendo a su formato, serán archivos digitales que contengan estos contenidos. Por tanto, será esta la plausible forma de acceso de una *deepfake*, como fuente de prueba documental derivada de una prueba electrónica, en un procedimiento jurisdiccional[54].

Con respecto al ámbito del proceso penal, la localización de la normativa a manejar se presenta en la Sección 4ª, del Capítulo III, Titulo III, del Libro III de la LECrim. Pero, es necesaria una interpretación extensiva de lo contenido en el artículo 726 del mismo cuerpo legal. Por todos es conocido que la normativa regulatoria del proceso penal en el ordenamiento jurídico español tiene más de un siglo de vida. Si bien, se ha venido modificando el lenguaje empleado en alguno de los preceptos, resulta necesario que se lleven a cabo interpretaciones para adaptar la norma a la nueva realidad digital.

En este punto, es menester referirse al concepto de prueba electrónica. En palabras del profesor Bueno de Mata, la prueba digital sería aquel "*medio electrónico, ya sea físico o electrónico, que permite autenticar hechos significativos en el proceso, y consta de dos elementos necesarios para su existencia, lo que define la peculiaridad de la prueba electrónica*

---

[53] El artículo 299 de la LEC, dice así: "*1. Los medios de prueba de que se podrá hacer uso en juicio son:*

1.º Interrogatorio de las partes.

2.º Documentos públicos.

3.º Documentos privados.

4.º Dictamen de peritos.

5.º Reconocimiento judicial.

6.º Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias".

[54] Si bien, esta cuestión, se verá más pormenorizadamente en el siguiente capítulo del trabajo.

frente a las demás pruebas: elementos técnicos o hardware (un sistema de administración informático) y elementos lógicos o software (el soporte donde se archiva la información)".

Esta modalidad de prueba se caracteriza[55] por ser intangible, es decir, no es apreciable a través de los sentidos, siendo necesarios procesos informáticos complejos para que se puedan percibir. Por su replicabilidad, es posible copiar o replicar tantas veces como se desee. Aunque hay que precisar que esta acción podría dar lugar a otro archivo digital distinto. Es decir, otra de sus características es la volatilidad. También la debilidad es apuntada como una de sus cualidades, entendiendo que esta prueba puede ser fácilmente destruida, sin necesidad de destrucción del soporte físico que la contiene[56]. Por último, la doctrina suele apuntar a la parcialidad como otra de sus cualidades, entendida como la posibilidad de que la prueba se integre por múltiples ficheros informáticos repartidos por distintas localizaciones y en distintos formatos digitales[57].

Anejo a este marco regulatorio, es imperioso apuntar la normativa técnica que han de manejar los peritos informáticos en su labor de creación del informe pericial informático de la prueba digital. Se trata de la normativa contenida en la UNE (acrónimo de Una Norma Española, antes denominada como AENOR, Asociación Española de Normalización) que, a su vez deriva de la normativa internacional de la ISO (en inglés, International Organization for Standardization), entre otras[58].

3. NATURALEZA JURÍDICA DE LAS *DEEPFAKES*: LA PRUEBA DOCUMENTAL DIGITAL.

3.1. Consideración como documento digital.

Una *deepfake* puede manifestarse de las siguientes formas: en formato audiovisual, visual o solo de audio. Es decir, el archivo digital que contiene una ultrafalsificación puede ser un vídeo, una imagen o un archivo de audio. El medio de prueba por el cual se introducen los archivos audiovisuales, de los que recoge el artículo 299 Ley de Enjuiciamiento Civil, es vía prueba documental[59]. Para comprender el motivo por el cual un contenido audiovisual se considera como medio de prueba documental, hay que remitirse a la definición que el ordenamiento jurídico otorga a la palabra documento:

Se puede encontrar una definición de documento en el artículo 26 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, el cual define al documento de la siguiente forma: "*(…) se considera documento todo soporte material que exprese o incorpore datos,*

[55] DE LA TORRE RORÍGUEZ, P. J. (s.f.). *La Prueba Digital en el Proceso Judicial*. Obtenido de https://indalics.com/ [Consulta el 19/06/2023].

[56] De ahí la importancia de seguir unas reglas para la manipulación de las mismas, en otras palabras, aplicar procesos que son regulados en los estándares aplicables para los forenses informáticos.

[57] VADELL BUJOSA, L., BUSTAMANTE RÚA, M., & TORO GARZÓN, L. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal, 7*(2), pp. 1347-1384, p. 1366.

[58] Se detallará con mayor precisión, infra, en el apartado cuarto.

[59] ABEL, L. X., PICÓ i JUNOY, J., GINÉS CASTELLET, N., & ARBOS i LLOBET, R. (2011). *La prueba electrónica.* Barcelona: Bosch, pp. 70-74.

hechos o narraciones con eficacia probatoria (…)". Por lo tanto, es posible una interpretación amplia de dicho concepto[60].

También la posición jurisprudencial mayoritaria es considerar a la prueba digital como documental[61]. Así se pronuncia la Sentencia 2925/2020, de 23 de julio de 2020, de la Sala Cuarta de lo Social del Tribunal Supremo[62].

Es precisamente la expresión "todo soporte material" del artículo 26 CP la que permite interpretar que un documento electrónico puede ser entendido como un documento a los efectos normativos. Y ello porque la forma de contener la información de un documento no necesariamente ha de ser escrito, permitiéndose cualquier soporte que posibilite perpetuar una información[63], en un soporte duradero (entrando aquí su versión informática). En esta línea la Sentencia del Tribunal Supremo, de la Sala Segunda de lo Penal, de 2 de diciembre del 2000[64], fundamento de derecho segundo: *"Se argumenta principalmente que las falsedades (…) no puede ser tales en cuanto no se efectuaron sobre documentos (…) lo único que hizo fue manipular apuntes informáticos (…) Si bien es cierto que ese concepto de documento ha sido clarificado en el artículo 26 del vigente Código Penal, no lo es menos durante la vigencia del anterior, también se consideró que los soportes informáticos podían ser objeto de falsedad penal (…)"*. Por lo tanto, un soporte informático es un documento a la luz del ordenamiento jurídico y, como tal, una *deepfake* en tanto en cuanto es un soporte informático, es un documento.

A su vez, la sentencia referida en el párrafo anterior se apoya en otras anteriores del Alto Tribunal, las cuales siguen esta misma corriente doctrino-jurisprudencial. Es decir, la corriente mayoritaria es considerar que el documento electrónico queda incardinado en el concepto de documento del Código Penal.

Incluso, en este punto se deben tener presentes también las consideraciones que la normativa europea atribuye al documento electrónico, pues le es otorgada la equivalencia con un documento físico. Es decir, un documento electrónico es lo mismo que un documento en papel. Por lo tanto, no se les pueden negar efectos jurídicos, ni de admisibilidad como prueba

---

[60] Interpretación que sustenta el Alto Tribunal, en el fundamento cuarto, párrafos tercero y cuarto de la Sentencia 2925/2020, de 23 de julio de 2020, de la Sala Cuarta de lo Social del Tribunal Supremo. ECLI: ES:TS:2020:2925.
Disponible en: https://www.poderjudicial.es/search/openDocument/a300242c85b950d9 [Consulta el 06/06/2023].

[61] MARTÍNEZ MOYA, J. (2020). El correo electrónico como medio probatorio: su naturaleza de prueba documental a los efectos de los recursos de casación y suplicación. *REVISTA DE JURISPRUDENCIA LABORAL*, pp. 1-10. Disponible en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2020-00000001081 [Consulta el 06/06/2023].

[62] Fundamento de derecho cuarto, párrafo quinto: "*El avance tecnológico ha hecho que muchos documentos se materialicen y presenten a juicio a través de los nuevos soportes electrónicos, lo que no debe excluir su naturaleza de prueba documental (…). Si no se postula un concepto amplio de prueba documental, llegará un momento en que la revisión fáctica casacional quedará vaciada de contenido si se limita a los documentos escritos, cuyo uso será exiguo*".

[63] CORCOY BIDASOLO, M., & MIR PUIG, S. (2015). *Cometarios al código penal.* Valencia: Tirant lo Blanch. pp. 148-149.

[64] ECLI: ES:TS:2000:8867 Disponible en https://vlex.es/vid/falsedad-documento-mercantil-estafa-17726041 [Consulta el 05/06/2023].

en procedimientos judiciales por el mero hecho de estar en formato electrónico[65]. Esta consideración está contenida en distintos artículos de la LEC[66].

También hay que tener en cuenta que un documento puede tener naturaleza pública o privada y como tal, la diferencia entre ambos es la distinta fuerza probatoria que el legislador otorga a cada clase de documento. Un documento público, en virtud del artículo 319 LEC tiene mayor poder probatorio, pues goza de fe pública registral, lo que significa que sus posibilidades de impugnación son más limitadas. Por otro lado, el documento privado, de acuerdo con el artículo 326 LEC, tendría la misma fuerza probatoria que un documento público, es decir, haría prueba plena en caso de que no se cuestione su autenticidad.

Por ejemplo, en el caso de un contenido de una web que interese a una de las partes, puede acudir ante un notario a que levante acta sobre el contenido de dicha web. Sin embargo, el acta notarial no demuestra que sea un contenido no manipulado, solo se daría fe de lo que en ese momento percibe el notario[67], pudiéndose cuestionar la autenticidad del contenido en sí, pese a que sea documento público. Por tanto, extrapolándolo al caso de una *deepfake* en la que, por ejemplo aparezca un individuo que aparentemente reconoce una deuda. En caso de que se transcriba ese contenido y se eleve a acta pública, y sea aportada como un documento público, podría ser impugnada vía reconocimiento del propio tribunal del contenido y vía informe pericial.

A pesar de que en base a la jurisprudencia analizada, la aportación de un archivo audiovisual en el que se contenga una ultrafalsificación encajaría sin mayores problemas en el medio de prueba documental. Para el caso de que se aportase en algún tipo de soporte o de forma que escapase del concepto de documento, siempre quedaría como último recurso el artículo 299.3 LEC. Pues este artículo faculta al tribunal, y siempre a instancia de parte, a adoptar "*otro medio de prueba no expresamente previsto en los apartados anteriores siempre que pudiera obtenerse certeza sobre hechos relevantes*". Eso sí, sin perder de vista la adopción de medidas que en cada caso resultaran necesarias en pro de la cadena de custodia, integridad, etc.

3.2. Consideraciones acerca de la admisibilidad de las pruebas digitales.

Una prueba electrónica es toda información con potencial valor probatorio que se contiene en un medio electrónico o que se transfiere a través del mismo.

Por lo tanto, lo primero que hay que distinguir es desde donde se produce la extracción de la prueba digital y la propia prueba en sí. Es decir, diferenciar el continente del contenido. Ello, puesto que se pueden aportar ambas como prueba, pero se le aplicarán una serie de precisiones respecto a su admisión en un proceso. El legislador en la LEC separa "instrumen-

---

[65] Así versa el artículo 46 en desarrollo del considerando 63 del REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Disponible en: https://www.boe.es/doue/2014/257/L00073-00114.pdf [Consulta el 05/06/2023].

[66] En concreto, los artículos 326.3, 327, 333 y 812.1.1º Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[67] CANUT ZAZURCA, P. J. (2016). Validez y eficacia procesal de la prueba electrónica. En R. OLIVA LEÓN, & S. VALERO BARCERLÓ, *La prueba electrónica validez y eficacia procesal.* (págs. 152-156). Z: Juristas con futuro. Disponible en https://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16 PruebaElectronicagran-final.pdf [Consulta el 12/06/2023].

tos, grabaciones y semejantes", de "instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso" (artículos 382 y 384 respectivamente).

Esto supone que la prueba digital puede ser el soporte físico dónde se generó, y/o dónde está contenida (artículo 384 LEC). En otros términos, para acceder a la misma, hay que registrar los datos almacenados en el *hardware*, en el dispositivo computacional físico en sí. Lo que implicaría que sería necesario aportar el dispositivo físico en sí al procedimiento.

O también puede ser el propio archivo, en otras palabras, el producto de la aplicación de las herramientas lógicas que contiene ese dispositivo computacional (artículo 382 LEC). En este caso, se trataría del resultado de la aplicación de algún tipo de *software* o distintos procesos informáticos que trabajen en colaboración para generar ese archivo.

Esto supondría la aportación al proceso del archivo intangible, en virtud del artículo 383 LEC, que el archivo quedará custodiado por el Letrado de la Administración de Justicia. La custodia por parte del Letrado garantiza la cadena de custodia de la prueba propuesta[68]. También, por mandato del mismo artículo, que el archivo ha de ser presentado junto con la transcripción de su contenido en un soporte duradero. Esto permite manejar de mejor manera la prueba. Pero, en ningún momento la transcripción será la fuente de prueba, simplemente es accesoria a la prueba, facilita su estudio por parte de los tribunales y de las partes del proceso.

Por tanto, una *deepfake* puede ser aportada al proceso junto con el dispositivo de almacenaje en el que se encuentre, es decir, la prueba se practicará sobre el *hardware*. O puede ser aportada en formato intangible, es decir, el producto resultante del sistema de generación de ultrafalsificaciones, debiéndose aportar su archivo al LAJ y transcribir su contenido en un soporte duradero, para que se maneje su contenido con mayor facilidad.

La jurisprudencia, aprecia desde un primer momento la posibilidad de manipulación de los contenidos audiovisuales. Es el caso de la Sentencia 190/1992, de 16 de noviembre del Tribunal Constitucional[69] la cual contiene el siguiente razonamiento: "(…) *Con carácter general, debe reconocerse que toda grabación magnetofónica presenta una posibilidad cierta de manipulación, trucaje y distorsión del contexto global en el que tuvieron lugar las manifestaciones reproducidas (...) para evitar la proliferación de "pruebas" artificiosamente conseguidas se recomiende proceder con suma cautela a la hora de admitir como tales las manifestaciones contenidas en uno de estos soportes, y otra bien contraria es que deba negárseles radicalmente toda eficacia probatoria.*" (F.J. 3º).

Por ello, distintos pronunciamientos del Tribunal Supremo y del Tribunal Constitucional han venido perfilado ciertas cautelas a la hora de la admisión de pruebas digitales. Algunas de estas sentencias son anteriores al contenido que regula el fenómeno de la prueba digital en la normativa procesal, por lo tanto, brindaron cierta seguridad al tráfico jurídico:

Resulta relevante destacar la Sentencia del Tribunal Supremo Nº. 1140/2010, de 29 de diciembre de 2010[70], que establece cómo valorar las grabaciones. De acuerdo con esta resolución "*1) Corresponde a los jueces determinar la legitimidad de este medio (...) el trucaje, la manipulación o la distorsión de las cintas grabadas se evitará no solo por medio de la técnica más depurada, sino también si la prueba se práctica, a través de lo que las partes hayan*

[68] Acto que es tendente a minimizar el riesgo de que la contraparte impugne la autenticidad por vulneración de la cadena de custodia.

[69] ECLI: ES:TC:1992:190.
Disponible en: https://vlex.es/vid/-252334458.
Disponible en: https://hj.tribunalconstitucional.es/en/Resolucion/Show/2077 [Consulta el 05/06/2023].

[70] ECLI: ES:TS:2010:7184.

solicitado, en el juicio oral con publicidad e inmediación, incluso con la visualización y audición de las mismas y la intervención pericial oportuna en los casos en que sea necesario (…). Cualquier medio, en tanto en el proceso penal no rige el sistema de prueba tasada será válido si se respetan los derechos de las partes y sirve para algo tan esencial como es en la investigación criminal (…)".

De acuerdo con esta sentencia, la prueba consistente en un contenido audiovisual puede haber sido manipulada, correspondiéndole al juzgador determinar si admite o no una prueba de estas características. Para evitar la manipulación de pruebas, una basada en un contenido audiovisual ha de ser practicada en el juicio oral, para que la misma pueda ser cuestionada por las partes. Además, esta sentencia recoge la idea que se contiene en el artículo 382 LEC, el cual faculta a la parte que propone el contenido inmaterial como prueba a acompañar a la misma con otros medios de prueba para reforzar su autenticidad. Es decir, acompañar a la prueba con otras pruebas, es una medida que puede reforzar la posible convicción del órgano jurisdiccional sobre la existencia o inexistencia de los hechos invocados.

En relación a la aportación de otros instrumentos para potenciar el poder de convicción, cabe reseñar que algunos autores[71], siguen de manera deficiente la corriente creada por la Sentencia del Tribunal Supremo Nº. 300/2015[72]. Esta, en un caso de conversaciones mantenidas por una red social, rezaba lo siguiente ante la impugnación de la autenticidad de las mismas: "*(…) la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.*"

Pero la argumentación de esta sentencia no terminaba ahí. El Tribunal Supremo continuaba señalando que "*(…) dos razones son las que excluyen cualquier duda. La primera, el hecho de que fuera la propia víctima la que pusiera a disposición del Juez de instrucción su contraseña con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial. La segunda, el hecho de que el interlocutor con el que se relacionaba XXX fuera propuesto como testigo y acudiera al plenario. Allí pudo ser interrogado por las acusaciones y defensas acerca del contexto y los términos en que la víctima mantuvieron aquel diálogo*". Por tanto, en este caso se observa cómo se puede potenciar la convicción del tribunal vía otros medios de prueba, mediante el reconocimiento judicial e interrogatorio de partes.

En estos mismos términos, para dejar clara esta posición, se pronuncia la Sentencia del Tribunal Supremo 375/2018, de 19 de julio de 2018[73]: "*(…) no es posible entender, (…) que estas resoluciones establezcan una presunción iuris tantum de falsedad de estas modalidades de mensajería, que debe ser destruida mediante prueba pericial que ratifique su autenticidad y que se debe practicar en todo caso; si no que, en el caso de una impugnación de su autenticidad se debe realizar tal pericia (…) tal pericia no será precisa cuando no exista du-*

[71] Olmos García, Mercedes, en https://repositorio.comillas.edu/rest/bitstreams/88302/retrieve [Consulta el 06/06/2023].
García Gómez, José Luis, en https://www.institutopascualmadoz.es/wp-content/uploads/2016/06/TFM-Jos%C3%A9-Luis-Garc%C3%ADa-G%C3%B3mez.pdf [Consulta el 06/06/2023].
[72] Disponible en: https://vlex.es/vid/571257698 [Consulta el 08/06/2023].
[73] ECLI: ES:TS:2018:2949. Disponible en: https://vlex.es/vid/736117133 [Consulta el 06/06/2023].

da al respecto mediante la valoración de otros elementos de la causa o la práctica de otros medios de prueba".

Por tanto, de ambas sentencias se pueden extraer dos conclusiones. La primera es que en caso de impugnarse la autenticidad de la prueba, en el momento procesal oportuno[74], quien ha de demostrar la autenticidad de la misma es quien se quiere aprovechar de su potencial probatorio. Es decir, la parte que aporta esa prueba debe acreditar que esa evidencia es auténtica. La segunda, como detallan ambas sentencias, la parte que pretende valerse de la potencial fuerza probatoria del contenido cuestionado, puede utilizar otros medios probatorios para garantizar la autenticidad de la misma. En otras palabras, no es obligatorio acudir a la pericial[75].

A su vez, para completar la cuestión de una posible impugnación a mala fe, se prevé específicamente en el segundo párrafo del cuarto apartado del artículo 326 LEC, la imposición de costas, gastos y derechos que origine la comprobación a cargo de quien formula la impugnación. Además, si el tribunal estima que la impugnación ha sido temeraria, puede ser impuesta una multa de 300 a 1200 euros.

De las anteriores resoluciones analizadas se pueden extraer las siguientes conclusiones: el órgano juzgador es quien debe decidir acerca de la admisión o no como prueba a una prueba digital debido a la posibilidad de su manipulación. Para evitar una posible inadmisión, las partes pueden potenciar la apariencia de legitimidad de sus pruebas digitales aportando otros medios probatorios que potencien a dicha prueba en cuestión. En caso de impugnación de una prueba digital, la carga de la prueba recae sobre quien pretenda hacer valer la prueba, en este sentido es posible aportar también otros medios de prueba para certificar la autenticidad de la prueba, no siendo de obligado cumplimiento aportar pericial informática.

Para el caso de la deslegitimación de un contenido como una ultrafalsificación, puede ser lo idóneo aportar un informe pericial, pero, hay que poner en relieve el principio de economía procesal, el derecho a un debido proceso, etc. Puesto que, un informe informático-pericial de un archivo digital es oneroso no solo en términos económicos sino también temporales, pudiendo dar lugar a dilaciones indebidas del proceso.

En resumen, una representación sintética, siendo un archivo audiovisual, desde un punto de vista jurídico es un documento digital. Por tal consideración, podría ser aportada en un proceso como prueba documental, la cual podría ser discutida por las partes y derivar en la aportación de otros medios de prueba para potenciar el poder de convicción y su autenticidad. Pero nunca será obligatorio un informe pericial, cuando se cuestione una prueba digital. Si bien, aparentemente, puede ser la opción más garantista en términos formales, en términos de respeto al debido proceso puede que existan, siempre dependiendo del caso en concreto, opciones más favorables que impulsen la capacidad de convencimiento de una prueba digital, tales como el reconocimiento judicial e interrogatorio de partes[76].

---

[74] Artículo 427 Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[75] Artículo 326, apartado segundo, Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. "*Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto".*

[76] Como fue el caso en la Sentencia del Tribunal Supremo Nº. 300/2015 Op. cit. En dicho procedimiento, se despejaron las dudas sobre la autenticidad de un documento electrónico permitiendo el acceso al dispositivo por parte del juzgador. Este hecho es posible extrapolarlo al caso de las ultrafalsificaciones, en el sentido de, permitir el acceso al dispositivo donde se generó el archivo o, permitir el visionado de los metadatos donde se refleje la manipulación de los contenidos.

En paralelo a ello, la introducción de una ultrafalsificación, podría ser equivalente a la introducción de una prueba falsa. Hecho que podría conllevar consecuencias penales, pues esta acción podría enmarcarse dentro del delito de estafa procesal[77].

4. LA PERICIAL INFORMÁTICA Y PRINCIPALES HERRAMIENTAS DE ANÁLISIS.

4.1. Formación del perito y elaboración del informe pericial.

El informe pericial tiene una doble implicación en los procedimientos jurisdiccionales. Pueden ser por sí mismos una fuente de prueba aislada, propuestas como prueba en el momento procesal oportuno, o pueden potenciar la autenticidad de otra prueba, como prevé el artículo 382 LEC.

Se corresponde con la figura del perito aquella persona física o jurídica, ajena al proceso judicial, que es llamada por iniciativa de las partes o por el juez debido a que es poseedor de un conocimiento especializado que permite valorar hechos o circunstancias relevantes en un proceso[78]. Su interpretación en el proceso es de utilidad debido a que puede aportar información, vía informe pericial o a través de la contestación de preguntas formuladas durante su comparecencia en el procedimiento, sobre determinados puntos técnicos de un litigio. Con ello, facilita al órgano jurisdiccional poseer un criterio con el cual poder tomar una decisión final informada[79].

Un informe pericial informático, debe ser realizado por una persona experta en informática forense[80], la cual aplicará una serie de herramientas tendentes a la generación de un informe pericial. Informe que garantizará la validez científica del proceso a través de la recogida, procesado y examinado de las pruebas de manera estandarizada. Y, sobre todo, de manera en que el resultado o conclusión a la que llegue ese perito quede pormenorizado en su informe. Es decir, para garantizar que la prueba pueda ser discutida y valorada, en su caso, por parte de la contraparte e incluso por el propio órgano juzgador[81]. Es decir, puede ser cuestionada a través de otra pericial[82], en atención al derecho al debido proceso y al principio de igualdad de medios de defensa (artículo 24 de la Constitución Española). Incluso, si tras las intervenciones de los peritos de ambas partes, existe discrepancia entre los informes periciales y no queda clara una realidad consistente de los hechos, las partes o el órgano jurisdiccional pueden nombrar un tercer perito, el perito dirimente. Este será designado para resolver definitoriamente la cuestión.

---

[77] Esta cuestión se detallará con mayor amplitud en el quinto punto del trabajo.

[78] BARAZA SÁNCHEZ, X., & BLANCO MARTÍONEZ, J. F. (2022). *El Perito Técnico en Prevención de Riesgos Laborales.* Barcelona: Editorial UOC. p. 13.

[79] Así lo estipula el artículo 335 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[80] LÁZARO DOMINGUEZ, F. (2014). *Introducción a la informática forense.* Madrid: RA-MA Editorial. p.18.

Define a la informática forense como *"el empleo de métodos científicos comprobables para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidencias digitales procedentes de fuentes digitales, con el propósito de hacer posible la reconstrucción de los hechos.*"

[81] Artículo 348 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[82] Incluso, si tras las intervenciones de los peritos de ambas partes, existe discrepancia entre los informes pericial y no queda clara una realidad consistente de los hechos, las partes o el órgano jurisdiccional pueden nombrar un tercer perito, el perito dirimente, para que resuelva (artículo 339 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil).

La homogeneidad que crean las normas de estandarización son de importancia ya que es vital que se garantice la integridad y conservación de las evidencias[83]. Esto retroalimenta la importancia de la cadena de custodia, la necesidad de generar documentación detallada sobre el proceso seguido, para que sea reproducible esa investigación. De lo contrario, es decir, de no preservarse no podría ser revisado ese informe pericial, aplicando las reglas de la sana crítica. Esta es pues la base de la ciencia, es decir, la autocrítica genera conocimiento y el revisionismo del mismo, ello en aras de no caer en el dogmatismo.

En concreto, la normativa técnica de estandarización que los peritos suelen manejar, entre otras, a la hora de realizar su labor es la siguiente[84]. Norma UNE 197001/2015 relativa a las Normas Generales para la elaboración de informes y dictámenes periciales sobre TIC. Esta normativa general sirve para unificar los requisitos formales que debe contener un informe pericial en el ámbito de las tecnologías de la información. Es una normativa estructural, no de contenido, pues nada se establece acerca de los procedimientos o métodos específicos para desarrollar una pericial informática.

La norma UNE 71505/2013, subdividida en tres bloques, establece los atributos que debe cumplir una evidencia informática para que pueda ser considerada confiable y el ciclo de gestión que ha de seguirse durante el ciclo de vida de la misma para que no pierda tal condición. Estas, para el caso de una *deepfake* por su naturaleza documental, son complementadas con la norma UNE 71506/2013 la cual define el proceso concreto del análisis forense de estas evidencias[85]. Dicho proceso se compone de varias fases. La primera es la fase de preservación, la cual es la que se ocupa de mantener en todo momento la validez y confiabilidad de las evidencias originales. Implica utilizar soportes informáticos adecuados, llevar indumentaria apropiada y el almacenamiento idóneo de la prueba.

La siguiente fase sería la de adquisición, en la cual se realiza la copia del archivo, pero siguiendo un procedimiento por el cual no se modifican los metadatos de la evidencia, garantizando así la identidad del archivo a la hora del análisis. A continuación, se realizaría la etapa de la documentación, que supone plasmar todo el procedimiento de análisis, así como herramientas aplicadas, de manera cronológica en aras de facilitar el examen de la cadena de custodia de la evidencia.

La penúltima etapa es la del análisis, aquí es donde el perito aplica las herramientas, metodologías y procesos para dar respuestas a las cuestiones que motivan el desarrollo de la pericial. En el caso de una representación sintética, aplicarán una serie de herramientas[86], para

---

[83] Por ello, en este campo del peritaje, es muy útil recurrir a las técnicas de duplicado forense. Es decir, realizar una copia espejo de los datos del archivo original, que quedará tendrá bajo custodia el Letrado de la Administración de Justicia, pudiendo trabajar en esos datos sin la posibilidad de hacer desaparecer la prueba original en sí.

[84]RUBIO ALAMILLO, J. (5 de noviembre de 2016). *Estándares nacionales e internacionales que puede seguir un perito informático para realizar el análisis forense de una evidencia y para la elaboración de un peritaje informático*. Obtenido de Javier Rubio Alamillo Perito Informático: https://peritoinformaticocolegiado.es/blog/estandares-nacionales-e-internacionales-que-puede-seguir-un-perito-informatico-para-realizar-el-analisis-forense-de-una-evidencia-y-para-la-elaboracion-de-un-peritaje-informatico/ [Consulta el 05/06/2023].

[85] GlobátiKa. (2023). *ISO 71506/2013. Metodología para el análisis forense de las evidencias electrónicas.* Obtenido de Normativas Aplicables por el Perito Informático.: https://peritosinformaticos.es/iso-71506-2013-perito-informatico/ [Consulta el 14/06/2023].

[86] Que se verán a continuación, en el punto 4.2.

que el perito concluya si ese archivo ha sido generado artificialmente o, si, por el contrario, es un contenido sin manipulaciones informáticas[87].

La pericial informática concluye con la fase de la presentación del informe pericial propiamente dicho. Esto supone trasladar a un lenguaje inteligible todas las conclusiones a las que llega durante el análisis de la prueba. Informe que será trasladado al proceso como fuente de prueba. Prueba que no escapará de su posible discusión, ya que puede ser cuestionada por la parte contraria en la fase de la práctica de la misma[88].

4.2. Herramientas para el análisis forense informático.

Existen en el mercado diversas aplicaciones que facilitan la labor de los peritos informáticos. Por ejemplo, un recurso a tener en cuenta para la gestión de evidencias digitales son los denominados "contenedores forenses", que se puede definir como almacén lógico donde se custodian, conservan y procesan las evidencias digitales, respetando los estándares aplicados en la informática forense. Un ejemplo de contenedor forense de uso reconocido es el Contenedor AFF (Advanced Forensics Format o Formato Forense Avanzado): de formato abierto, sirve para el almacenamiento de imágenes de datos[89] y metadatos.

Para el desarrollo del análisis forense[90], alguna de las herramientas que se pueden aplicar son, por ejemplo, WinHex[91] con funcionalidades de edición e inspección avanzada de todo tipo de archivos. Permite recuperar archivos eliminados, datos perdidos o corruptos de dispositivos de almacenamiento. Para el caso que nos ocupa, esta herramienta podría ser de utilidad, al poder ser usada para recuperar los datos de entrenamiento borrados que se aplicaron en el sistema de generación de ultrafalsificaciones, aportando así un indicio de manipulación.

Otra cuestión que deben atender los peritos forenses a la hora de manipular pruebas digitales, es garantizar la identidad de la prueba con el archivo analizado. Es decir, garantizar que no muten los metadatos del archivo por no ser manipulados correctamente. Por eso FTK imager[92] es de interés ya que se trata de una herramienta para la obtención de imágenes de datos, útil para adquirir evidencia forense mediante la creación de copias de datos sin alterar la prueba original, es decir, no se alterarían los metadatos del archivo. Por apuntar, si se atendiera un caso en el cual han de ser tratados con premura una cantidad considerable de datos, po-

[87] Hay que tener en cuenta que esto no verifica que no haya sido manipulado. Como se apuntó a la hora de definir a las *shallowfakes* pueden aplicarse técnicas de edición audiovisual que puedan alterar también el contenido. Ahí entrará el criterio del juez, el cual, a la luz de todas las pruebas practicadas en el proceso, resolverá conforme a su criterio, siempre respetando el ordenamiento jurídico.

[88] Ello en virtud del artículo 24 de la Constitución española, pues no poder cuestionar una prueba iría en detrimento de la tutela judicial efectiva.

[89] Una imagen de datos es una copia exacta de un dispositivo de almacenamiento, es decir, se trata de una copia bit a bit de todo dato contenido en un dispositivo. Dicha copia se basa en el duplicado en otro dispositivo diferente, desde el cuál se realizarán las acciones necesarias para la búsqueda y obtención de datos de relevantes que pudieran haber sido eliminados u ocultados.

[90] ESPINOZA MINA, M. A. (2019). Informática forense: una revisión sistemática de la literatura. *Rehuso, 4(2)*, pp. 112-128. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7047153 [Consulta el 07/06/2023].

[91] Disponible en: http://www.winhex.com/winhex/hex-editor.html [Consulta el 07/06/2023].

[92] Disponible en: https://www.exterro.com/ftk-imager [Consulta el 07/06/2023].

dría utilizarse EnCase Enterprise V4[93] que serviría para realizar copias instantáneas de grandes volúmenes de datos, sin alterar los metadatos.

Una herramienta de verificación forense de firma biométrica[94] también podría ser interesante para el caso de una posible deepfake. Es decir, ante un hipotético caso de una ultrafalsificación en la que una persona quede vinculada a una relación contractual por la misma y esta sea causa sea judicializada, aplicar esta herramienta podría ser útil para deslegitimar esa prueba documental.

4.3. Técnicas de detección de *deepfakes*.

En este apartado, se pretende apuntar una serie de técnicas que se suelen emplear en informática forense para detectar representaciones sintéticas. Si bien, con antelación hay que dejar constancia de que la continua sofisticación de las técnicas de generación de *deepfakes*, complican la detección de las manipulaciones[95]. Estas técnicas y herramientas debieran ser actualizadas al son de la evolución de los métodos de generación de deepfakes.

Hay que destacar que existen métodos de detección de ultrafalsificaciones que aplican métodos de inteligencia artificial similares a aquellos que se utilizan para crear representaciones sintéticas. Por otro lado, también hay otros métodos que, si bien aplican algún tipo de método informático, no son propiamente aplicaciones basadas en técnicas de aprendizaje profundo.

Como último apunte, la comunidad de investigación de análisis digital forense se muestra favorable a aplicar la misma tecnología que se utiliza para generar a las *deepfakes*. Es decir, aplicar las redes neuronales generativas adversariales. Aunque también se reconoce que otras técnicas que se han venido depurando, como el análisis de compresión del vídeo, cada vez logran resultados más precisos[96]. Luego, no es disparatado pensar que una combinación de ambos métodos podría generar un análisis sólido.

Para proceder al análisis de los metadatos del archivo, entendidos como los datos del archivo que sirven para suministrar información sobre los datos producidos. Es decir, los metadatos proporcionan información sobre edición del contenido, por ejemplo. Para analizarlos son útiles herramientas como ExifTool[97], MediaInfo[98] o File Viewer[99] pues permiten realizar análisis de metadatos sobre ficheros multimedia y ofimáticos. Aunque, si bien, en ningún caso deberían ser considerados como una prueba de cargo[100], debido a que los metadatos también pueden ser manipulados para mostrar, por ejemplo, que un cambio se realizó en otra fecha distinta de en la que efectivamente se produjo la manipulación. Por ello, los metadatos,

---

[93] Disponible en: https://www.ondata.es/recuperar/encase_forensic.htm [Consulta el 07/06/2023].

[94] Es el caso de la herramienta que usa Docuten, como prestador cualificado de servicios de confianza en el tráfico jurídico. Más información disponible en: https://docuten.com/es/blog/firma-biometrica-en-docuten-sencilla-segura-confidencial-y-legal/#:~:text=Para%20reforzar%20la%20seguridad%20legal,vez%20estas%20han%20sido%20descifradas. [Consulta el 12/06/2023].

[95] QUIRÓS-FONS, A., & GARCÍA-ULL, F. J. (2022). "La Inteligencia Artificial… op.cit. pp. 537-555.

[96] QUIRÓS-FONS, A., & GARCÍA-ULL, F. J. (2022). "La Inteligencia Artificial… op.cit. p. 539.

[97] Disponible en: https://exiftool.org/ [Consulta el 12/06/2023].

[98] Disponible en: https://mediaarea.net/es/MediaInfo [Consulta el 12/06/2023].

[99] De la empresa OSForensics, disponible en https://www.osforensics.com/file-viewer.html [Consulta el 12/06/2023].

[100] LIFe. (2022). *¿Realmente sirven los metadatos como prueba forense?* Obtenido de LIFe. Laboratorio de informática forense: https://www.laboratoriodeinformaticaforense.com/realmente-sirven-los-meta datos-como-prueba-forense/ [Consulta el 12/06/2023].

han de ser tenidos en cuenta con el conjunto de otras evidencias digitales por parte del profesional informático encargado de la pericia. También, por parte de los juzgadores han de valorarlos en relación con los demás hechos. Por ejemplo, los datos de posicionamiento GPS, pueden ayudar a desmontar o potenciar una declaración, pero nunca por sí mismo, podrán ser una prueba de cargo que justifique la condena de una persona.

Esto debido a que no es muy laborioso realizar una manipulación de esta clase de datos[101]; o en otro sentido, es fácil alterar un archivo, haciendo que muten esos metadatos (de ahí que la doctrina presente la volatilidad como una de las características de la prueba digital[102]), realizando una acción que pudiera parecer cotidiana. Por ejemplo, en el caso de los metadatos de geolocalización, habría que demostrar claramente la posesión en ese momento del dispositivo que se ha triangulado.

En caso de que los metadatos muten, se ha de apuntar que el archivo en sí será diferente. Es decir, cada archivo digital tiene datos sobre sus datos, que son propiamente los metadatos: quién accede al archivo, en qué fecha y hora, última edición, etc. cualquier cambio, hará mutar dichos datos. Por ejemplo, no es lo mismo, un archivo que se encuentre en una determinada carpeta de un dispositivo de almacenamiento, que ese mismo archivo, enviado a través de algún proceso de comunicación vía Internet. A ese archivo se le aplicarán una serie de protocolos para que pueda enviarse a través de Internet. Por lo tanto, el archivo que visualiza el usuario destinatario del mismo, es distinto, debido a que el contenido de los metadatos ya no sería igual al contenido en ese dispositivo de almacenamiento, aunque el contenido en sí es el mismo. Es decir, un mismo contenido, metadatos dispares. De ahí la importancia de que el perito vigile la identidad del archivo a estudiar, pues de lo contrario, no quedará garantizado que el archivo objeto de litigio sea el mismo que el analizado.

Otra técnica relevante es el análisis de la matriz de filtrado de color[103]. Técnica de análisis fotográfico que se basa en el estudio del patrón de ruido[104] del sensor fotográfico de una cámara digital. Con ello se puede identificar a una concreta cámara, o el empleo de varias, que podría ser un indicio de manipulación del contenido.

Otras técnicas para la detección de ultrafalsificaciones más informales son el análisis del número de parpadeos, análisis del cuerpo en escena (es más costoso generar *deepfakes* de todo el cuerpo humano, la mayoría se centran en el rostro y ello supone incongruencias en las proporciones físicas de la persona, sombras, movimientos, etc.), coordinación del sonido con los labios, etc.

A continuación, se apuntan técnicas que aplican métodos de inteligencia artificial para detectar contenidos generados artificialmente. El análisis de los parámetros de compre-

[101] En esta página web, por ejemplo, se indica cómo se puede alterar la fecha y hora de un fichero utilizando el programa informático File Date Changer. Disponible en: https://indalics.com/blog/metadatos-investigacion-forense [Consulta el 12/06/2023].

[102] VADELL BUJOSA, L., BUSTAMANTE RÚA, M., & TORO GARZÓN, L. (2021). La prueba digital… Op. Cit p. 1366.

[103] MUÑOZ-BERMÚDEZ, C., & CORTES-OSOIO, J. A. (2021). Identificación de Cámara Fuente a partir del Patrón de Ruido del Sensor extraído mediante Transformada Wavelet no Diezmada. *Scientia et Technica, 26*(4), pp. 474-485. Disponible en: https://dialnet.unirioja.es/buscar/documentos?querysDismax.DOCUMENTAL_TODO=Identificaci%C3%B3n+de+C%C3%A1mara+Fuente+a+partir+del+Patr%C3%B3n+de+Ruido+del+Sensor+extra%C3%ADdo+mediante+Transformada+Wavelet+no+Diezmada [Consulta el 12/06/2023].

[104] El ruido de una fotografía es la cantidad de píxeles que no tienen color o luminosidad correcta debido a una exposición deficiente.

sión de la imagen[105]es un método en el que se aplican técnicas de aprendizaje automático para detectar la doble compresión JPEG de las imágenes. Es decir, se detecta si hay superposición de imágenes, aplicando una serie de cálculos matemáticos que realiza el sistema autónomamente. Esta técnica, según sus creadores, ofrece un 95% de efectividad en la detección de contenidos manipulados.

Un método que emplea redes neuronales siamesas[106], entrenadas casi en exclusiva con vídeos falsos, es FakeTalkerDetect[107]. Aun teniendo un escaso entrenamiento con imágenes reales, esta herramienta, según su explicación, es efectiva en un 98.81% de los casos planteados. Es decir, se trata de un clasificador basado en redes neuronales generativas, que discrimina si un contenido ha sido generado aplicando técnicas propias de una *deepfake*. Sería aplicar otra red discriminadora, hipotéticamente mejor entrenada que la usada para la creación, que detecte esos patrones indiciarios de contenido manipulado.

Uno de los métodos que mayor aprobación académica ha obtenido es la aplicación de las redes convolucionales para la detección universal de manipulación de imágenes[108]. Es decir, aplica las CNN para que el sistema aprenda automáticamente a detectar diferentes manipulaciones de imágenes. Lo curioso es que, con este método, la herramienta no "se fija" en las características de la imagen, es más obvia a la imagen en sí. En su lugar, pone el foco en aprender las características de la manipulación, lo cual hace que este método autónomo. En el sentido de que no es necesario fijar características predeterminadas indiciarias de manipulación, como en otros casos. Los autores[109], tras experimentar con el modelo, indican un 99,1% de efectividad.

Para finalizar, uno de los métodos más recientes y más enfocados para la detección de representaciones sintéticas es una aplicación de distintas técnicas de aprendizaje profundo para la detección de *deepfakes* y *shallowfakes*[110].

La mecánica de trabajo de esta técnica comienza con la introducción el archivo que se quiera analizar. Se le aplican un conjunto de filtros que sirvan para extraer la distribución del ruido de las imágenes. Posteriormente se aplican en paralelo dos redes neuronales convolucionales cuya misión es extraer las características del archivo.

Los resultados de ambas redes son fusionados e introducidos en otra red convolucional, la cual se dedica a la segmentación semántica las imágenes[111], que en este caso es una

---

[105] YANG, P., NI, R., & ZHAO, Y. (2018). Double JPEG Compression Detection by Exploring the Correlations in DCT Domain. *sia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 728-732. doi:10.23919/APSIPA.2018.8659485.

[106] Es un tipo de arquitectura de red neuronal, en concreto las redes siamesas son el germen de desarrollo de las GAN, pues el planteamiento teórico de estas tiene de base una red siamesa.

[107] JEON, H., BANG, Y., & WOO, S. S. (2019). FakeTalkerDetect: Effective and Practical Realistic Neural Talking Head Detection with a Highly Unbalanced Dataset. *IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)*, 1285-1287. doi:10.1109/ICCVW.2019.00163. [Consulta 04/03/2023].

[108] BAYAS, B., & STAMM, M. (2016). A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security.* doi: https://dl.acm.org/doi/pdf/10.1145/2909827.2930786.

[109] BAYAS, B., & STAMM, M. (2016). A Deep Learning Approach… Op. cit..

[110] ZHANG, G., TOHIDYPOUR, Y., & NASIOPOULOS, P. (2023). Shallow- and Deep- fake Image Manipulation Localization Using Deep Learning,. *2023 International Conference on Computing, Networking and Communications (ICNC)*, 468-472. doi:10.1109/ICNC57223.2023.10074246.

[111] Una red discriminadora que clasifica la imagen en real o falsa.

de las mejores redes de estas características disponibles en el mercado actualmente. Esta última es la que discrimina si el contenido es una ultrafalsificación o una *shallowfake*. Sus ideadores, apuntan un 75% de efectividad en los experimentos de localización de *deep o shallowfakes*.

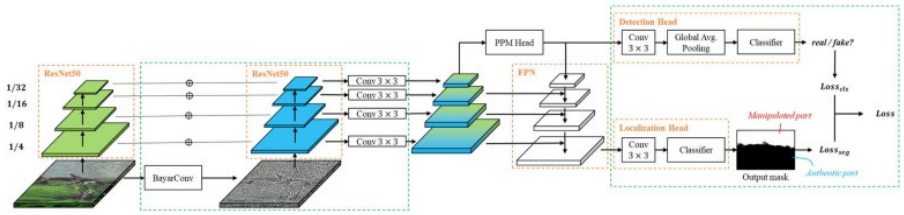

Ilustración 1. Estructura de funcionamiento de la red de detección de deepfakes y shallowfakes. Fuente: Shallow- and Deep- fake Image Manipulation Localization Using Deep Learning,. *2023 International Conference on Computing, Networking and Communications (ICNC)*, 468-472. doi:10.1109/ICNC57223.2023.10074246-

Para recapitular, estas técnicas pueden ser utilizadas por los profesionales forenses informáticos para realizar su juicio de valor acerca de la autenticidad de un archivo digital que pueda ser presentado en un procedimiento judicial. Ahora bien, las técnicas y sistemas referenciados no suponen un listado taxativo de estas. Los peritos, en virtud de su posición de experto, pueden utilizar los métodos que estimen más convenientes para realizar la pericial.

No se puede perder de vista que estas técnicas y herramientas son consideradas, a la luz de la propuesta, como sistemas de alto riesgo por ser sistemas de detección de *deepfakes*. Un sistema de detección que esté configurado maliciosamente puede dictaminar que un archivo real sea etiquetado como falso. Por lo tanto, deben de contar con las obligaciones que se les impone a las herramientas de generación de *deepfakes* (apuntadas en el punto 2.4 de este trabajo[112]), por parte de la Propuesta de reglamento.

5. IMPLICACIONES PENALES Y PROCESALES DE LA INTRODUCCIÓN DE *DEEPFAKES* COMO PRUEBA EN EL PROCESO.

5.1. Delito de estafa procesal

La introducción de una prueba manipulada en un procedimiento judicial es una de las tipologías del delito de estafa. La estafa es un ilícito consistente en mediante engaño sufi-

[112] Es necesario que cuenten con: un sistema de gestión de riesgos, documentación técnica accesible y actualizada sobre la herramienta y su funcionamiento, sometimiento a una evaluación de conformidad previa a su introducción en el mercado, conservación de los archivos de registro generados, el proveedor o, en su caso, su representante deben inscribirse, antes de la puesta en servicio del sistema, en la base de datos de la Unión Europea para sistemas de IA de alto riesgo, medidas correctoras en caso de funcionamiento deficiente, información a las autoridades nacionales competentes del estado miembro donde opere el sistema. Además, y en todo momento, los operadores que utilicen en el tráfico jurídico estos sistemas deben poder acreditar frente a las autoridades nacionales competentes el cumplimiento de los requisitos que impone la Propuesta de Reglamento.

ciente, conseguir inducir a error a otra persona para que realice un acto de disposición en perjuicio propio o ajeno, siempre que exista ánimo de lucro [113].

La estafa procesal es una modalidad agravada de la estafa, puesto que además de atentar contra la víctima, se produce un desvalor en la Administración de Justicia. Está tipificada en el artículo 250 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en concreto: *1. El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando: (...) 7.º Se cometa estafa procesal. Incurren en la misma los que, en un procedimiento judicial de cualquier clase, manipularen las pruebas en que pretendieran fundar sus alegaciones o emplearen otro fraude procesal análogo, provocando error en el juez o tribunal y llevándole a dictar una resolución que perjudique los intereses económicos de la otra parte o de un tercero*.

Para que se produzca el ilícito es necesario que concurran las siguientes condiciones[114]: existir engaño bastante, engaño con finalidad de producir error en el juez o tribunal que conoce del asunto para que dicte una determinada resolución favorable a sus intereses y que implique la producción de un perjuicio ilícito a un tercero. Es decir, el sujeto activo del delito persigue obtener un beneficio ilícito o el reconocimiento de un derecho que no tiene.

Hay que precisar que este delito cabe en su forma de tentativa, es decir, para que se entienda consumado el delito es necesario obtener resolución judicial que resuelva el fondo del litigio, perjudicando a la contraparte. No siendo necesaria la ejecución de la sentencia para que se consuma el delito. En cambio, si no se llega a dictar sentencia, debido a que, por ejemplo, el tribunal se percata del engaño, estaríamos ante un caso de tentativa, puesto que se cumplen los elementos necesarios para ello: existencia de decisión de cometer el delito y la transformación de la decisión en una acción que suponga el comienzo de la ejecución del delito[115].

Por tanto, la acción de aportar una ultrafalsificación a un proceso entraría dentro del tipo penal, pues sería una manipulación de una prueba documental. Como se ha establecido en el presente trabajo, una *deepfake* también puede ser un archivo de audio. Si se diera el caso de una aportación de un audio manipulado en el que la contraparte reconoce una supuesta deuda, se estaría ante un supuesto claro de estafa procesal. Habría que atender al caso, pues si hubiera sentencia, sería un delito consumado de estafa procesal. Sin embargo, si se demostrara que el contenido es falso, antes de llegar a dictarse sentencia, estaríamos ante una tentativa de delito de estafa procesal.

Podría pensarse que, en caso de aportación de una ultrafalsificación, pudiéramos estar ante un caso de concurso ideal o medial entre el delito de estafa procesal y fraude documental de los artículos 250.1. 7º, 395 y 396 respectivamente del CP. Pero esta no es la realidad. La mayor parte de la jurisprudencia considera que si se aporta una falsificación de un documento privado, se está ante un caso de concurso de leyes[116] que se resuelve en virtud del principio de consunción. También, en función de la cuantía, condiciones de la cosa o entidad

---

[113] Artículo 248 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[114] PÁRAMO DE SANTIAGO, C. (2013). Estafa procesal. Falsedad documental: Comentario a la STS, Sala de lo Penal, de 16 de julio de 2013. *CEFLegal. Revista práctica De Derecho, 154*, 193-200. Disponible en: https://revistas.cef.udima.es/index.php/ceflegal/article/view/11839 [Consulta el 15/06/2023].

[115] En virtud de la Sentencia del Tribunal Supremo Nº. 2954/2019 ECLI:ES:TS:2019:2954.Fundamento de derecho tercero. Disponible en: https://www.poderjudicial.es/search/AN/openCDocument/cac2ec927df2ac2484b8072b28c6b92a5f7922b14f48b336.

[116] Artículo 8.3 y 8.4 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

del fraude, se resolverá por el principio de alternatividad[117]. Por tanto, la estafa procesal quedaría subsumida en el tipo de la falsedad documental[118].

Por el contrario, en caso de estar ante un caso de falsedad de documento público, la jurisprudencia considera que se aplica un concurso medial de delitos[119].

5.2. Impugnación de sentencias firmes.

Por último, se debe apuntar que, en el caso de que se llegue a consumar la estafa procesal. Es decir, que se hubiera dictado sentencia firme con base en una ultra falsificación, existe la posibilidad de acudir a la figura de la revisión[120] de sentencia firme[121], contenida en los artículos 509 a 516 LEC[122]. Revisión que se recoge en cada uno de los órdenes jurisdiccionales[123]. Este medio de impugnación, que en el caso de las *deepfakes* sería una revisión por falsedad documental, está concebido para la situación en la que se conozca la circunstancia posteriormente y, por plazo, no es posible interponer recurso ordinario.

En concreto, para el orden civil habrá de consultarse el artículo 510 de la Ley de Enjuiciamiento Civil, el cual establece los motivos de revisión de sentencia firme. En concreto, interesa para el caso de la aportación de una ultrafalsificación, el apartado 1. 2º de este artículo: "*Si hubiere recaído en virtud de documentos que al tiempo de dictarse ignoraba una de las partes haber sido declarados falsos en un proceso penal, o cuya falsedad declarare después penalmente.*". Esto quiere decir que, tras la sentencia del proceso penal por falsedad documental, se podrá instar la revisión de la sentencia dictada en fraude procesal.

Para el orden penal, hay que acudir al artículo 954 de la Ley de Enjuiciamiento Criminal, el cual indica las causas de revisión de sentencia firme de condena. Para el caso de

---

[117] CURRA SANTOMÉ, C. (2018). El delito de estafa. Especial referencia a las circunstancias calificadoras del artículo 250 CP. Disponible en: https://minerva.usc.es/xmlui/handle/10347/18466 [Consulta el 15/06/2023].

[118] ROJI ABOGADOS. (s.f.). *DERECHO PENAL: FALSEDAD DOCUMENTAL Y ESTAFA PROCESAL*. Obtenido de ROJI ABOGADOS: https://rojiabogados.com/es/derecho-penal-falsedad-documental-y-estafa-procesal/ [Consulta el 16/06/2023].

[119] CURRA SANTOMÉ, C. (2018). El delito de estafa… Op. cit.

[120] DOMÈNECH ADAN, F. (2018). De la revisión de sentencias firmes. En F. DOMÈNECH ADAN, *La LEC práctica en fichas*). Barcelona: Editorial Bosch. p. 183.

[121] El cual, a su vez, tiene sus propios plazos. El general es el que brinda la LEC en su artículo 512, es decir, es posible solicitar la revisión hasta cinco años desde la fecha de publicación de la sentencia, pasados esos cinco años, no ha lugar el recurso. La excepción es la revisión procesal, la cual no cuenta con plazo alguno. Esto es debido a que el fin último de la justicia es castigar al verdadero culpable. Por lo tanto, a una persona que es inocente se le debe permitir demostrar su inocencia, atendiendo a las nuevas circunstancias, en cualquier momento. Inclusive, conforme al artículo 955 LECrim, sus ascendientes, descendientes, cónyuge o quien haya convivido con el penado, pueden promover e interponer este recuso.

[122] El artículo 510 LEC establece los motivos que legitiman una revisión de sentencia firme. Para el caso de las *deepfakes* interesa el motivo 1. 2º, pues sería el caso de la aportación de un documento que, posteriormente, se descubre su falsedad. Por lo tanto, el condenado estaría en posición de invocar la revisión de la sentencia firme. Eso sí, el afectado debe cumplir el plazo de interposición del artículo 512 LEC, es decir, cinco años desde la fecha de publicación de la sentencia.

[123] Recurso cuya competencia se reconoce, según la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, a cada Sala del Tribunal Supremo en su orden jurisdiccional, artículos 56 y ss. Y, también a la Sala de lo Civil y Penal del Tribunal Superior de Justicia de la Comunidad Autónoma correspondiente, contra sentencias que establezca la ley, en virtud artículo 73 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

la introducción de una representación sintética, interesa el apartado 1. a): "*Cuando haya sido condenada una persona en sentencia penal firme que haya valorado como prueba un documento o testimonio declarados después falsos, (...) siempre que tales extremos resulten declarados por sentencia firme en procedimiento penal seguido al efecto. No será exigible la sentencia condenatoria cuando el proceso penal iniciado a tal fin sea archivado por prescripción, rebeldía, fallecimiento del encausado u otra causa que no suponga una valoración de fondo.*". Luego también en un caso de sentencia firme de un proceso penal, es necesario instar otro proceso que declare la falsedad de la prueba documental.

En el caso del orden social, el artículo 236 de la Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social se remite al cauce que establece la Ley de Enjuiciamiento Civil sobre los motivos y plazos de ejercicio del recurso de revisión. Y, también se remite al artículo 86.3 de la Ley 36/2011, el cual indica que no se suspenderá el procedimiento social a menos que el juez o tribunal, al final del juicio, considere que el documento puede ser decisivo para resolver sobre el fondo. De ser el caso, supondría la suspensión del procedimiento hasta que se dictase sentencia o auto de sobreseimiento en la causa criminal.

En la jurisdicción contencioso-administrativa, es menester acudir al artículo 102 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. El referido artículo, recoge expresamente los motivos indicados en la Ley de Enjuiciamiento Civil y, posteriormente, se remite directamente a esa misma norma para lo relativo a legitimación, plazos, procedimientos y efectos de las sentencias.

Por todo lo expuesto, para el caso en que sea consumado el delito de estafa procesal (subsumido en el tipo de falsedad documental) por la introducción al proceso de una *deepfake*, existe remedio consistente en el recurso de revisión en cada una de las jurisdicciones, que permite paliar la situación de injusticia.

6. CONCLUSIONES

PRIMERA. Las imágenes y demás contenidos audiovisuales desempeñan un papel importante en nuestra vida cotidiana, ya que son portadoras de mucha información. Además, cumplen una función social. Es decir, con el uso generalizado de las redes sociales, en muchos casos, las personas desarrollan actividades sociales a través de imágenes en sus perfiles de estas redes. En ciertos casos pueden llegar a ser el diario de la vida de una persona o, incluso obtener rendimientos económicos de la explotación de su imagen. Las imágenes pueden ser un método de realizar una obra artística, un modo de expresión, un pasatiempo, etc. Incluso pueden ser parte del desarrollo de la personalidad del individuo.

Por ello, las manipulaciones de los contenidos con el objetivo de crear rumores y fraudes pueden afectar negativamente a la sociedad en general. Especialmente cuando se difunden a gran velocidad y a gran escala por Internet. El fenómeno de la manipulación digital de contenidos audiovisuales, a través de técnicas de inteligencia artificial, facilita en gran medida este fenómeno, terminando de consolidar la idea de que no es posible aceptar como veraz un archivo multimedia, sin antes razonar críticamente.

Existen, y cada día el número crece, múltiples herramientas que posibilitan, aplicando distintas técnicas, manipular un contenido. Es por ello por lo que, cada vez con más frecuencia, aparecen *fake news* sobre personas de interés (de cualquier clase), realizando actos u otra escena cualquiera imaginable, que atente contra el honor y la propia imagen de dicha persona. O, por el contrario, una ultrafalsificación en la que se muestre un contenido que glorifique a una persona por actos que nunca realizó. De esta manera, utilizando las representa-

ciones sintéticas se puede llegar al fin último por el que se generan: manipular a la opinión pública.

SEGUNDA. La manipulación de audiovisuales no es un fenómeno nuevo, ya que la manipulación y edición de fotos se remonta a mediados del siglo XIX[124]. Pero, la aparición de herramientas de creación de ultrafalsificaciones, supone un salto cualitativo en el fenómeno de la edición de contenidos audiovisuales.

Aunque, se debe tener en cuenta que el resultado de estas herramientas no implica necesariamente que sea genere un contenido de tal calidad que pueda engañar a cualquier persona. Pues también requiere de ciertas habilidades y recursos no al alcance de cualquier persona, para poder conseguir un resultado que burle hasta a las personas más expertas[125]. Pero como se viene apuntando en el presente trabajo, estas técnicas evolucionan con rapidez, siendo cada vez más sencillo, barato y rápido conseguir generar estos contenidos con una calidad "aceptable". Por lo tanto, aparecerán con más frecuencia noticias falsas, debiéndose potenciar la promoción de adquisición, desde los organismos públicos hacia la ciudadanía, de habilidades que les permitan ser más críticos para cuestionar la autenticidad de los contenidos multimedia. Además, las autoridades deben vigilar el cumplimiento de las condiciones que la Propuesta de Reglamento de IA les impondrá a los operadores que aplican técnicas de creación de ultrafalsificaciones.

TERCERA. Es cierto que las representaciones sintéticas suponen un desafío para la sociedad. Pero no se debe perder de vista el punto de que se trata del producto de una herramienta. Las técnicas de creación de *deepfakes*, como herramienta que son, estrictamente no son algo negativo, dependerá de las intenciones con las que las use su operador. Pueden ser muy beneficiosas, por ejemplo, para las autoridades policiales. Por ejemplo, una vez que es aprobada la diligencia de investigación del agente informático encubierto, este podría generar contenidos de apariencia real que no atenten contra los derechos y libertades de personas reales, lo cual sería un acierto para la investigación de organizaciones criminales que se dediquen a la explotación de menores con fines pornográficos. De esta forma, se pueden evitar riesgos de revictimización de la víctima.

CUARTA. El estado normativo del ordenamiento jurídico actual permite la introducción de contenidos digitales como fuente de prueba documental en los procesos jurisdiccionales. Por tanto, parece que queda "abierta" la puerta a posibles contenidos manipulados. Frente a esta posibilidad existen ciertas condiciones o precisiones que se aplican a la prueba digital. Es decir, debido a la posibilidad de manipulación, los organismos jurisdiccionales son más cautelosos a la hora de admitir una prueba electrónica para que se practique. Es por ello por lo que la normativa recoge expresamente que, en estos casos, es conveniente acompañar

---

[124] Una de las primeras técnicas de edición fotográfica fue "Colodión húmedo" atribuida a Oscar Gustav Rejlander en 1851. Más información disponible en: https://josealvarezfotografia.com/rejlander-los-dos-caminos-de-la-vida-2/ [Consulta el 12/06/2023].

[125] En este sentido, conviene apreciar la calidad de la representación sintética del actor Morgan Freeman realizando una reflexión sobre la realidad y las *deepfakes* realizada por Bob de Jong en 2021. Disponible en: https://www.youtube.com/watch?v=oxXpB9pSETo. Si bien, como se apuntaba, no se recrea todo el cuerpo de la persona, lo cual puede ser uno de los indicios que nos haga sospechar, tanto la luz, sombras, como movimientos de la cara están realizados con una técnica precisa, que podría llevar a engaño a una persona.

A su vez, podemos apuntar que este vídeo está cumpliendo con la regulación que propone la Propuesta de Reglamento de IA, pues está claramente etiquetado como *deepfake*.

la fuente de prueba con otras que puedan potenciar el poder de convicción de la figura jurisdiccional, acerca de su autenticidad. Un ejemplo podría ser la aportación del dispositivo donde se almacene la prueba digital objeto de litigio.

QUINTA. La Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, recientemente aprobada por el Parlamento Europeo (14/06/2023). Regulación que supondrá a todas luces una mejora en torno al fenómeno de las ultrafalsificaciones, pues como se ha apuntado, se imponen una serie de condiciones para los agentes que quieran utilizar esta tecnología, tendentes a luchar contra la desinformación. Es decir, medidas como el etiquetado de los contenidos generados artificialmente como no reales, las medidas específicas para los operadores que utilicen *deepfakes* en su tráfico jurídico (sistema de gestión de riesgos, documentación técnica accesible, evaluación de conformidad previa, etc.) y la vigilancia del cumplimiento de dichas medidas, pretenden limitar lo máximo posible la posibilidad de inducir a error a una persona con una *deepfake*.

SEXTA. Cierto sector doctrinal interpreta que, ante un caso de impugnación de autenticidad de un documento electrónico, es imperioso aportar informe pericial que certifique la autenticidad del archivo. Esto no es así, el Tribunal Supremo se plantea la posibilidad de que una prueba electrónica puede ser manipulada. Pero existen otras vías para certificar la autenticidad de la prueba aportada en cuestión. Es decir, ante la impugnación de la autenticidad de una prueba digital, no es obligatorio practicar una pericial informática, se puede acudir, por ejemplo, a la declaración de las partes para aclarar la autenticidad del archivo. Es decir, existen otros cauces para acreditar la autenticidad de una prueba digital, puesto que realizar un informe pericial, en su caso, puede ir en detrimento de la tutela judicial efectiva. En este sentido, hay que tener en cuenta que, para realizar una pericial se debe seguir un método específico por una persona experta, la cual necesita cierto tiempo para elaborar un informe pericial y que, dependiendo de la complejidad del caso, puede dilatar indebidamente un proceso. Todo esto supondría el menoscabo de la tutela judicial efectiva recogida en el artículo 24 CE.

SÉPTIMA. Para el caso en que sea conveniente practicar un informe pericial, los profesionales del análisis forense informático, cuentan con normativa unificadora de esta actividad. Esto supone una mejora para con la seguridad jurídica. Puesto que, una de las precisiones más importantes de esta normativa es que, para la redacción del informe con las conclusiones del perito, se debe utilizar un lenguaje comprensible para cualquier persona. Esto supone que el órgano jurisdiccional cuente con la información de calidad y suficiente para resolver de fondo el asunto.

Los forenses informáticos, tienen a su disposición herramientas que facilitan la realización de sus periciales. En concreto, para detectar ultrafalsificaciones, existen distintas técnicas, entre ellas, hay que destacar que el empleo de técnicas de inteligencia artificial, en concreto aplicar las GAN, son las que mayor aceptación tienen entre los profesionales de la pericial informática.

OCTAVA. El ordenamiento penal español recoge a la estafa procesal como un delito. Por lo tanto, una aportación de una representación sintética como prueba documental en un proceso se tratará como falsedad documental, en el caso de tener la condición de documento privado. Y, para el caso de un documento público, como un concurso real de delitos de falsedad documental y fraude procesal.

Es muy importante destacar que, con la existencia de la revisión de sentencias firmes, se pueden limitar los posibles perjuicios derivados de la introducción de una *deepfake*.

Puesto que, aunque se logre cumplir una estafa procesal, existe un remedio procesal. Es decir, con las herramientas que se contienen en la normativa procesal hay suficientes métodos de actuación para que no se produzcan situaciones injustas derivadas de la aportación de una ultrafalsificación.

7. BIBLIOGRAFÍA

ABEL, L. X., PICÓ i JUNOY, J., GINÉS CASTELLET, N., & ARBOS i LLOBET, R. (2011). *La prueba electrónica.* Barcelona: Bosch, pp. 70-74.

BARAZA SÁNCHEZ, X., & BLANCO MARTÍONEZ, J. F. (2022). *El Perito Técnico en Prevención de Riesgos Laborales.* Barcelona: Editorial UOC.

BAYAS, B., & STAMM, M. (2016). A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security.* doi:https://dl.acm.org/doi/pdf/10.1145/2909827.2930786.

BLACKBOX. (2022). *BLACKBOX*. Recuperado el 29 de Marzo de 2023, de https://www.useblackbox.io/.

BLANCO, H. (2021). El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre. *InDret, 1*, 431-501.

BRANDNER, R., & INTERCOMPONENT, A. G. (2007). *Long-Term provides information for the Internet community. It does not specify as Internet standard of any mind. Distribution of this memo is unlimited.* Obtenido de https://www.rfc-editor.org/rfc/rfc4810 [Consulta el 04/06/2023].

BREZINSKI, D., & KILLALEA, T. (2002). *Guidelines For Evidence Collection and Archiving.* Obtenido de https://dl.acm.org/doi/pdf/10.17487/RFC3227 [Consulta el 08/05/2023].

BUENO DE MATA, F. (2019). *Las diligencias de investigación penal en la cuarta revolución industrial.* Navarra: Aranzandi.

CANUT ZAZURCA, P. J. (2016). Validez y eficacia procesal de la prueba electrónica. En R. OLIVA LEÓN, & S. VALERO BARCERLÓ, *La prueba electrónica validez y eficacia procesal.* (págs. 152-156). Juristas con futuro. Obtenido de https://ecija.com/wp-content/uploads/2016/09/EBOOK-Sept16PruebaElectronicagran-final.pdf [Consulta el 12/06/2023].

CANZANI, A., & LECUN, Y. (2020). *NYU Center for Data Science*. Obtenido de NYU Deep Learning Spring 2020: https://cds.nyu.edu/deep-learning/.

COMISIÓN EUROPEA. (2021). Propuesta de Reglamento por el que se establecen normas armonizadas de inteligencia artificial (Ley de Inteligencia Artificial) y que modifica determinadas actos legislativos de la Unión Europea. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206.

COMISIÓN EUROPEA. (s.f.). *Comisión Europea*. Obtenido de https://digital-strategy.ec.europa.eu/es/policies/european-approach-artificial-intelligence [Consulta el 04/06/2023].

COPY.AI. (2022). *copy.ai*. Recuperado el 29 de marzo de 2023, de https://www.copy.ai/.

CORCOY BIDASOLO, M., & MIR PUIG, S. (2015). *Cometarios al código penal.* Valencia: Tirant lo blanch.

CREW, C. (24 de enero de 2021). We Made a Better CGi Luke Skywalker. Estados Unidos. Obtenido de https://www.youtube.com/watch?v=861gfPVmgdc [Consulta el 29/04/2023].

CURRA SANTOMÉ, C. (2018). El delito de estafa. Especial referencia a las circunstancias cualificadoras del artículo 250 CP. Obtenido de https://minerva.usc.es/xmlui/handle/10347/18466 [Consulta el 15/06/2023].

DAVIES, C. (31 de marzo de 2023). "No, Donald Trump no ha sido detenido, son imágenes de inteligencia artificial.". *EL MUNDO*. Recuperado el 31 de marzo de 2023, de https://www.elmundo.es/internacional/2023/03/23/641c97c921efa034268b45b0.html.

DE LA TORRE RORÍGUEZ, P. J. (s.f.). *La Prueba Digital en el Proceso Judicial*. Obtenido de https://indalics.com/ [Consulta el 19/06/2023].

DI SALVO, M. (25 de mayo de 2022). Deepfake Video of Elon Musk Promoting Crypto Scam Goes Viral. *Decrypt*. Obtenido de https://decrypt.co/101365/deepfake-video-elon-musk-crypto-scam-goes-viral [Consula el 04/06/2023].

DOMÈNECH ADAN, F. (2018). De la revisión de sentencias firmes. En F. DOMÈNECH ADAN, *La LEC práctica en fichas* (págs. 183-189). Barcelona: Editorial Bosch.

ENCINAS GRIJALVA, M. D. (2021). *La innovación disruptiva como recurso para la transformación de modelos de negocios en medios de comunicación. [Tesis].* Madrid. Obtenido de https://eprints.ucm.es/id/eprint/67599/.

ESAGE, A. (22 de marzo de 2022). ¿CÓMO USAR DEEPFAKE PARA ENGAÑAR A LOS SISTEMAS BIOMÉTRICOS DE AUTENTICACIÓN FLV? *Noticias de seguridad informática*. Recuperado el 2 de abril de 2023, de https://noticiasseguridad.com/seguridad-informatica/como-usar-deepfake-para-enganar-a-los-sistemas-biometricos-de-autenticacion-flv/.

ESPINOZA MINA, M. A. (2019). Informática forense: una revisión sistemática de la literatura. *Rehuso, 4(2)*, pp. 112-128. doi:https://dialnet.unirioja.es/servlet/articulo?codigo=7047153.

EUROPOL. (2020). *Malicious Uses and Abuses of Artificial Intelligence.* Obtenido de https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf.

GATES, B. (21 de Marzo de 2023). *GatesNotes*. Recuperado el 26 de Marzo de 2023, de The blog of Bill Gates: https://www.gatesnotes.com/The-Age-of-AI-Has-Begun.

GlobátiKa. (2023). *ISO 71506/2013. Metodología para el análisis forense de las evidencias electrónicas.* Obtenido de Normativas Aplicables por el Perito Informático.: https://peritosinformaticos.es/iso-71506-2013-perito-informatico/ [Consulta el 14/06/2023].

GONDROM, T., BRANDNER, R., & PORDESCH, U. (2007). *Evidence Record Syntax (ERS).* Obtenido de https://dl.acm.org/doi/abs/10.17487/RFC4998 [Consulta el 04/06/2023].

GOODFELLOW, I., & et.al. (Noviembre de 2020). Generative adversarial networks. *Communications of the AC, 63*(11), pp. 139-144. doi:https://doi.org/10.1145/3422622.

HERNÁNDEZ-ORTEGA, J., FIERREZ, J., MORALES, A., & GALBALLY, J. (2023). "Introduction to Presentation Attack Detection in Face Biometrics and Recent Advances". En S. MARCEL, J. FIERREZ, & N. EVANS, *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment* (págs. 203-230). Singapur: Springer. doi:https://doi.org/10.1007/978-981-19-5288-3.

HODGE D., S. J. (2021). Don't Always Believe What You See: Shallowfake and Deepfake Media Has Altered the Perception of Reality. *Hosfra Law Review*, pp. 51-80.

JEON, H., BANG, Y., & WOO, S. S. (2019). FakeTalkerDetect: Effective and Practical Realistic Neural Talking Head Detection with a Highly Unbalanced Dataset. *IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)*, 1285-1287. doi:10.1109/ICCVW.2019.00163. [Consulta 04/03/2023].

JERMAN BLAZIC, A., SALJIZ, S., & GONDROM, T. (2011). *Extensible Markup Language Evidence Record Syntax (XMLERS).* Obtenido de https://dl.acm.org/doi/abs/10.17487/RFC6283 [Consulta el 04/06/2023].

KOCSIS, E. (2021). Deepfakes, Shallowfakes, and the Need for a Private Right of Action. *Dickinson L. Rev., 126*, p. 621.

LÁZARO DOMÍNGUEZ, F. (2014). *Introducción a la informática forense.* Madrid: RA-MA Editorial.

LI, C., WANG, L., JI, S., ZHANG, X., XI, Z., GUO, S., & WANG, T. (2022). Seeing is Living? Rethinking in the Security of Facial Liveness Verification in the Deepfake Area. *31sr USENIX Security Symposium (USENIX Security 22)*, 2673-2690. doi:arXiv:2202.10673.

LIFe. (2022). *¿Realmente sirven los metadatos como prueba forense?* Obtenido de LIFe. Laboratorio de informática forense: https://www.laboratoriodeinformaticaforense.com/realmente-sirven-los-metadatos-como-prueba-forense/ [Consulta el 12/06/2023].

LORA, M. (21 de enero de 2021). Making of: Así se hizo el anuncio de Cruzcampo con Lola Flores y la técnica del «deepfake». *ABC de Sevilla*. Recuperado el 20 de 04 de 2023, de https://sevilla.abc.es/sevilla/sevi-making-hizo-anuncio-cruzcampo-lola-flores-y-tecnica-deepfake-202101211457_noticia.html.

MARTÍNEZ MOYA, J. (2020). El correo electrónico como medio probatorio: su naturaleza de prueba documental a los efectos de los recursos de casación y suplicación. *REVISTA DE JURISPRUDENCIA LABORAL*, 1-10. Obtenido de https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2020-00000001081.

MERINO, M. (2019). Animar el Will Smith digital de 'Géminis' ha costado millones, pero Hollywood ve cercano el uso masivo de los deepfakes en el cine. *Xataka*. Obtenido de https://www.xataka.com/inteligencia-artificial/animar-will-smith-digital-geminis-ha-costado-millones-hollywood-ve-cercano-uso-masivo-deepfakes-cine#comments-close [Consulta el 15/05/23]

MISTERWH1T3. (20 de marzo de 2022). "La rendición de Zelenski, el poder del «deepfake»". *Una al dia*. Recuperado el 31 de marzo de 2023, de https://unaaldia.hispasec.com/2022/03/la-rendicion-de-zelenski-el-poder-del-deepfake.html

MUÑOZ-BERMÚDEZ, C., & CORTES-OSOIO, J. A. (2021). Identificación de Cámara Fuente a partir del Patrón de Ruido del Sensor extraído mediante Transformada Wavelet no Diezmada. *Scientia et Technica, 26*(4), 474-485. Obtenido de https://dialnet.unirioja.es/buscar/documentos?querysDismax.DOCUMENTAL_TODO=Identificaci%C3%B3n+de+C%C3%A1mara+Fuente+a+partir+del+Patr%C3%B3n+de+Ruido+del+Sensor+extra%C3%ADdo+mediante+Transformada+Wavelet+no+Diezmada [Consulta el 12/06/2023]

PÁRAMO DE SANTIAGO, C. (2013). Estafa procesal. Falsedad documental: Comentario a la STS, Sala de lo Penal, de 16 de julio de 2013. *CEFLegal. Revista práctica De Derecho, 154*, 193-200. Obtenido de https://revistas.cef.udima.es/index.php/ceflegal/article/view/11839 [Consulta el 15/06/2023]

PÉREZ GÓMEZ, A. (2020). *Redes Generativas Antagónicas para la estandarización de imágenes de células de sangre periférica.* Barcelona: Universidad Politécnica de Catanluña Barcelonatech. Obtenido de https://upcommons.upc.edu/handle/2117/182625 [Consulta el 19/05/2023].

QUIRÓS-FONS, A., & GARCÍA-ULL, F. J. (2022). "La Inteligencia Artificial como herramienta de la desinformación: deepfakes y regulación europea". En E. G.-A. Palacios, *Los derechos humanos en la inteligencia artificial: su integración en los ODS de la Agenda 2030* (págs. 537-555). Pamplona: Thomson Reuters Aranzadi.

RIVERO, T. (3 de mayo de 2023). Este anuncio se ha generado usando exclusivamente inteligencia artificial y es una auténtica pesadilla. *Hipertextual*. Recuperado el 5 de mayo de 2023, de https://hipertextual.com/2023/05/anuncio-cerveza-generado-inteligencia-artificial-una-autentica-pesadilla.

ROJI ABOGADOS. (s.f.). *DERECHO PENAL: FALSEDAD DOCUMENTAL Y ESTAFA PROCESAL*. Obtenido de ROJI ABOGADOS: https://rojiabogados.com/es/derecho-penal-falsedad-documental-y-estafa-procesal/ [Consulta el 16/06/2023].

RUBIO ALAMILLO, J. (5 de noviembre de 2016). *Estándares nacionales e internacionales que puede seguir un perito informático para realizar el análisis forense de una evidencia y para la elaboración de un peritaje informático*. Obtenido de Javier Rubio Alamillo Perito Informático: https://peritoinformaticocolegiado.es/blog/estandares-nacionales-e-internacionales-que-puede-seguir-un-perito-informatico-para-realizar-el-analisis-forense-de-una-evidencia-y-para-la-elaboracion-de-un-peritaje-informatico/ [Consulta el 05/06/2023].

RUNWAY. (2022). *runway*. Recuperado el 31 de marzo de 2023, de https://runwayml.com/.

SCHWAB, K. (2016). *La cuarta revolución industrial.* Barcelona: Debate.

SEON. (22 de Febrero de 2022). *SEON*. Recuperado el 8 de Marzo de 2023, de SEON: https://seon.io/es/recursos/glosario/deepfake/.

STUPP, C. (30 de agosto de 2019). Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The wall street journal*. Obtenido de https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 [Consulta el 25/05/2023].

VADELL BUJOSA, L., BUSTAMANTE RÚA, M., & TORO GARZÓN, L. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal, 7*(2), pp. 1347-1384.

VÁZQUEZ, D. (6 de marzo de 2023). Los estafadores están clonando voces con IA para hacerse pasar por familiares que piden ayuda económica. *Business insider*. Obtenido de https://www.businessinsider.es/estafadores-ya-suplantan-voz-ia-hacerse-pasar-familiares-1210564 [Consulta el 04/06/2023].

YANG, P., NI, R., & ZHAO, Y. (2018). Double JPEG Compression Detection by Exploring the Correlations in DCT Domain. *sia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 728-732. doi:10.23919/APSIPA.2018.8659485.

ZHANG, G., TOHIDYPOUR, Y., & NASIOPOULOS, P. (2023). Shallow- and Deep- fake Image Manipulation Localization Using Deep Learning,. *2023 International Conference on Computing, Networking and Communications (ICNC)*, 468-472. doi:10.1109/ICNC57223.2023.10074246.