

La prueba *deepfake* como prueba ilícita

Joel Almagro Martín

Universitat Pompeu Fabra - Barcelona School of Management (UPF-BSM)

Fecha de presentación: diciembre 2025

Fecha de aceptación: abril 2026

Fecha de publicación: octubre 2026

Resumen

Los *deepfakes*, conforme a la definición del Reglamento de la Unión Europea en materia de inteligencia artificial, son contenidos audiovisuales generados o manipulados por una inteligencia artificial que se asemejan a personas, objetos, lugares, entidades o sucesos reales y que pueden inducir a una persona a pensar erróneamente que son auténticos o verídicos. Especial atención doctrinal ha merecido la posibilidad de que estos materiales sean aportados como prueba en un proceso judicial. Ahora bien, entre otras cuestiones, debe tenerse en cuenta que en la creación de estas ultrasuplantaciones se vulnera, en ciertas ocasiones, el derecho fundamental a la protección de datos. En este artículo, se analiza en qué supuestos sucede la indicada infracción para, finalmente, vincular estas conclusiones con el concepto de prueba ilícita dispuesto tanto en el artículo 11.1 de la Ley Orgánica del Poder Judicial como en la conocida doctrina del caso Falciani, esto es, la STC 97/2019, de 16 de julio.

Palabras clave

deepfake; prueba ilícita; derecho a la protección de datos; tratamiento de datos personales

Deepfake evidence as illegally obtained evidence

Abstract

Deepfakes, as defined by the EU Artificial Intelligence Act, are audiovisual content generated or manipulated by artificial intelligence that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful. Particular attention has been paid in legal scholarships to the possibility that these materials may be introduced as evidence in judicial proceedings. However, among other things, it should be taken into account that, in the creation of deepfakes, the fundamental right to data protection is violated on certain occasions. In this article, the cases in which such infringement occurs are analysed, and these conclusions are finally linked to the concept of illegally obtained evidence provided for both in Article 11.1 of the Organic Law of the Judiciary and in the doctrine established in the Falciani case, that is, STC 97/2019, of 16 July.

Keywords

deepfake; illegally obtained evidence; right to data protection; processing of personal data

Introducción

En el mundo digital, ver o escuchar no es suficiente para creer.

Uno de los mayores retos que los tribunales van a tener que afrontar en los próximos años es la eventual aportación de *deepfakes*¹ como prueba.² Estas falsificaciones audiovisuales realizadas mediante inteligencia artificial (en adelante, IA) suponen un auténtico punto de inflexión en el *thema probatorio*.

En efecto, en la actualidad, es técnicamente posible que una parte genere íntegramente un contenido audiovisual falso o que manipule artificialmente un material preexistente a partir de la adición, supresión o sustitución de determinados elementos, de tal modo que el contenido resultante refleje aquello que a dicha parte le interese y, posteriormente, lo aporte como prueba.

La realización del *deepfake* de alguien en concreto requiere que la herramienta de generación de *deepfakes* disponga de contenidos audiovisuales de la persona a suplantar, a partir de los cuales pueda recrearla -esto es, pueda simular su morfología, gestos, cambios en la tonalidad de la voz, etc.- y generar así el *deepfake* de conformidad con las instrucciones proporcionadas en el *prompt*. Sin embargo, la imagen o la voz presentes en estos contenidos audiovisuales son datos de carácter personal, cuyo poder de disposición debe permanecer en la esfera de su titular.

Corolario de lo anterior, procede analizar, desde la perspectiva del derecho a la protección de datos, si la generación de *deepfakes* destinados a ser aportados como prueba en un proceso judicial vulnera el derecho fundamental reconocido en el artículo 18.4 de la Constitución

Española (en adelante, CE). En el caso de que la respuesta sea afirmativa, y en función de la concepción de ilicitud probatoria que se adopte, la prueba *deepfake* sería falsa en cuanto a su contenido e ilícita en cuanto a la forma en la que habría sido obtenida (Almagro Martín, 2024).

Para realizar este estudio se ha acudido tanto a la normativa aplicable en España en materia de protección de datos como a todas las resoluciones dictadas por el Tribunal Constitucional español (en adelante, TC) que citan el artículo 18.4 CE hasta el 31 de julio de 2025, que ascienden a un total de 92 -en particular, 82 sentencias y 10 autos-.³

1. Vulneración del derecho fundamental a la protección de datos personales (artículo 18.4 de la CE)

Nuestra *norma normarum* consagró en su artículo 18.4 que «[l]a ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Bajo este precepto ha sido desarrollado el derecho fundamental a la protección de datos personales, tanto por la normativa en protección de datos como por la jurisprudencia del TC.

El concepto «dato personal» engloba toda la información sobre una persona física o identificable, es decir, «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador», y, en concreto, esto abarca -aunque no taxativamente- los «elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha

1. La definición legal del término *deepfake* la encontramos en el artículo 3.60 del Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial, que establece que son «un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos».
2. Problemática que ha suscitado un gran interés doctrinal debido a que los jueces no pueden confiar en su propia percepción para detectar *deepfakes* (Pellicer Ortiz, 2025) y, además, no existe consenso en la comunidad científica respecto a aquellos medios técnicos que permiten probar *deepfakes* (Nieva Fenoll, 2025; Cano Fernández, 2025).
3. Las 92 resoluciones han sido obtenidas mediante el buscador de jurisprudencia constitucional -sistema HJ- del Tribunal Constitucional de España a partir del filtro «Búsqueda por disposiciones citadas», estableciendo el criterio «disposiciones citadas», introduciendo como normativa «Constitución española, de 27 de diciembre de 1978» y seleccionando como artículo específico «Artículo 18.4». Se puede consultar este buscador a partir del siguiente enlace: <https://hj.tribunalconstitucional.es/> [Fecha de consulta: 14 de abril de 2026].

persona».⁴ De este modo, la imagen y la voz de un individuo están protegidas por la legislación en materia de protección de datos al ser consideradas datos de carácter personal, en la medida en que se refieren a una persona física y permiten su identificación.

Según el Reglamento (UE) 2016/679, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), se entiende por «tratamiento»:

«[C]ualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

Cierta parte de la doctrina afirma que entonces un «tratamiento» es «cualquier actividad en la que estén presentes datos de carácter personal» (Salvador Cerqueda, 2025).

Especial atención merece que la compartición de contenidos audiovisuales con el programa de generación de *deepfakes* conlleva el riesgo de que esos materiales puedan ser almacenados y, posteriormente, utilizados por la herramienta (Jiménez-Castellanos Ballesteros, 2025). Es decir, más allá de la realización de la ultrasuplantación, es posible que estos contenidos acaben siendo empleados por la empresa de generación de *deepfakes* para otras fi-

nalidades.⁵ No en vano, la Agencia Española de Protección de Datos emitió en abril de 2025 un comunicado sobre los riesgos para la protección de datos derivados de subir fotografías a herramientas de IA, en el que destacaba que los datos obtenidos de los archivos compartidos pueden ser almacenados o reutilizados por las empresas desarrolladoras de las aplicaciones o para el entrenamiento de algoritmos (AEPD, 2025). Asimismo, el estudio de Boté Vericad y Váñez (2022) mostró que la mayoría de las aplicaciones mediante las cuales se puede generar un *deepfake* no indican si el proceso de manipulación se realiza en un servidor local o remoto y que gran parte de estas herramientas recogen datos de carácter personal sin señalar si esos materiales son o no conservados.

En consecuencia, la generación de un *deepfake* de un sujeto en particular implica, desde la óptica del RGPD, un tratamiento de datos personales que únicamente puede ser considerado lícito en el caso de haber sido efectuado conforme a alguna de las bases legitimadoras del artículo 6 del RGPD (Trujillo Cabrera, 2024).

A continuación, se realizará una clasificación diferenciando entre cuatro supuestos. Los tres primeros comparten dos características: que el sujeto sobre el que se realiza el *deepfake* es una persona física⁶ y que el creador del *deepfake* es alguien distinto respecto a la persona suplantada.⁷ No obstante, se diferencian entre sí en que los dos primeros casos hacen referencia al creador del *deepfake* -si es una persona jurídica o una persona física-, mientras que en el tercero se analiza el escenario específico en el que los materiales empleados para hacer el *deepfake* sean ac-

4. Artículos 4.1 del Reglamento General de Protección de Datos; 3.1 de la Directiva (UE) 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y 5.1 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
5. La jurisprudencia constitucional ha señalado que «la cesión de datos personales a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, supone una nueva posesión y uso que requiere el consentimiento del interesado, y ello porque si se priva a la persona de las facultades de disposición y control sobre sus datos personales, se la estará también privando del derecho fundamental consagrado en el artículo 18.4 CE» (SSTC 96/2012, de 7 de mayo, y 292/2000, de 30 de noviembre). En este sentido, en aquellos supuestos en los que el material empleado para hacer el *deepfake* acabe siendo finalmente incorporado al sistema, se habrá producido una cesión de datos personales a un tercero -la empresa del *software* de IA-, y de no recaer esta nueva posesión bajo alguna de las bases legitimadoras, se debe entender conculcado el artículo 18.4 de la CE.
6. Al margen de la posibilidad o no de realizar un *deepfake* de una persona jurídica, lo cierto es que no se vulnera el derecho a la protección de datos cuando se realiza un tratamiento de datos respecto de una persona jurídica, ya que la mención a ciudadanos que realiza el artículo 18.4 CE limita el ámbito subjetivo de aplicación de este derecho a las personas físicas (SSTS n.º de recurso 3763/2013, de 14 de noviembre de 2014; y n.º de recurso 732/2003, de 20 de febrero de 2007).
7. No podría considerarse vulnerado el derecho a la protección de datos cuando el sujeto suplantado coincide con el propio autor del *deepfake*, salvo que en ese material aparecieran datos personales de terceros y sobre ellos se hubiera realizado también un tratamiento ilícito.

cesibles públicamente. Por último, en la cuarta categoría, se examina si vulnera el artículo 18.4 de la CE la producción de *deepfakes* en los que no aparezcan exteriorizados datos de carácter personal.

1.1. *Deepfakes* generados por personas jurídicas

La presente categoría engloba aquellos supuestos en los que una persona jurídica disponga de contenidos de imagen o voz de un sujeto -incluso cuando los hubiera obtenido de forma legítima- y los utilice para generar un *deepfake* de una persona física sin su consentimiento para posteriormente aportarlos como prueba en un proceso judicial. Podría suceder, por ejemplo, en el orden laboral, en la realización de un *deepfake* para justificar un despido.

Estos casos quedan dentro del ámbito de aplicación material del RGPD, por un lado, debido a lo estipulado en el artículo 2.1 del RGPD y, por otro lado, porque no recaen en ninguno de los tratamientos de datos personales en los que el Reglamento no es de aplicación (apartados segundo y tercero del artículo 2 del RGPD).

Por ello, para que el tratamiento sea lícito, debe haberse realizado mediante alguna de las bases legitimadoras que expone el artículo 6.1 del RGPD. Ahora bien, la determinación de la licitud de la generación de un *deepfake* de una persona en particular requiere de un análisis en el que se diferencien dos momentos. Primero, el de la licitud de la obtención del material que contiene la imagen o la voz del sujeto respecto al cual se realiza el *deepfake*; y segundo, el de la licitud de la creación del *deepfake* a partir de los materiales previamente obtenidos que contienen la imagen o la voz de un sujeto identificable. En consecuencia, para que la obtención del *deepfake* no vulnere el derecho fundamental a la protección de datos, el tratamiento de datos producido en ambas instancias debe ser lícito.

De lo anterior se infiere que la obtención legítima de materiales que contienen la imagen o la voz de un sujeto no implica que la creación del *deepfake* a partir de estos contenidos quede amparada en el artículo 18.4 de la CE y viceversa.⁸ Esto es debido a que se estaría produciendo un nuevo tratamiento que debe de igual modo quedar bajo alguna de las seis condiciones del artículo 6 del RGPD, cuyo análisis se aborda a continuación.

En primer lugar, la letra a) del artículo 6 del RGPD -interpretada a la luz del artículo 4.11 del RGPD- exige el consentimiento libre, específico, informado e inequívoco del interesado para uno o varios fines específicos. Sin embargo, partimos expresamente de que la persona física no ha otorgado consentimiento para la utilización de su imagen, voz o cualesquiera datos biométricos con la finalidad de generar un contenido sintético destinado a su aportación procesal. En consecuencia, la base legitimadora del consentimiento queda descartada.

En segundo lugar, la letra b) contempla que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o la aplicación a petición de este de medidas precontractuales. Ahora bien, no podría ser necesario para la ejecución de un contrato un tratamiento orientado a la fabricación de una prueba falsa.

En tercer lugar, la letra c) estipula la licitud del tratamiento cuando sea necesario para cumplir una obligación legal aplicable al responsable. No obstante, como resulta claro, no existe hoy en día ninguna obligación legal de generar *deepfakes* de otros sujetos y menos si ello se realiza con el fin de aportar una prueba falsa en un procedimiento judicial.

En cuarto lugar, la letra d) permite la realización de aquellos tratamientos necesarios para proteger intereses vitales del interesado o de otra persona física. Esta base legitimadora, que es de aplicación excepcional debido a lo

8. La STC 119/2022, de 29 de septiembre, analizó un supuesto en el que se aportó como prueba las imágenes captadas por una cámara de videovigilancia en la que no se había cumplido con el deber de información. No obstante, el TC acabó concluyendo que no se había producido lesión alguna al artículo 18.4 de la CE en tanto en cuanto la empresa había colocado el correspondiente distintivo en un lugar visible. Ahora bien, ante la ausencia de pronunciamientos específicos por parte del TC en relación con pruebas *deepfake*, imaginemos por un momento un supuesto como este, pero en el que, además, la empresa hubiera utilizado las imágenes captadas para realizar posteriormente un *deepfake* mediante el cual imputar a los trabajadores la comisión de unos hechos en concreto. En este caso, podremos afirmar, del mismo modo, que en la STC 119/2022, de 29 de septiembre, la obtención de las imágenes mediante las cámaras de videovigilancia fue ajustada al derecho de la protección de datos. Sin embargo, su posterior empleo para la realización del *deepfake* habría vulnerado el derecho del artículo 18.4 de la CE, ya que ese tratamiento de datos no queda bajo el amparo de ninguno de los supuestos que establece el artículo 6 del RGPD.

establecido en el considerando 46 del RGPD, no puede ser empleada para justificar el presente tratamiento, debido a que de ningún modo con la aportación de una prueba *deepfake* se está protegiendo el interés vital del interesado o de otra persona física.

En quinto lugar, la letra e) habilita el tratamiento cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. Sin embargo, el interés público en el correcto funcionamiento de la Administración de Justicia exige precisamente la autenticidad de los medios de prueba, no su manipulación.

Por último, la letra f) contempla que el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado. Evidentemente, no puede apreciarse la concurrencia de un interés legítimo preponderante cuando el tratamiento está destinado a la generación de una prueba falsa.

En definitiva, en el supuesto que nos ocupa, puede comprobarse que la generación de *deepfakes* de una persona física realizada por una persona jurídica con el fin de aportar ese contenido como prueba en un proceso judicial vulnera el derecho fundamental a la protección de datos en tanto en cuanto dicho tratamiento no quedaría justificado bajo ninguna de las seis bases legitimadoras del artículo 6.1 del RGPD.

1.2. *Deepfakes* generados por personas físicas

A continuación, analizaremos los supuestos en los que una persona física genere *deepfakes* de otra con el objetivo de aportarlos como prueba. En estos casos, nos encontramos con que el RGPD contempla en el artículo 2.2c) la excepción doméstica que, si bien de su tenor literal podría inferirse que un caso como el presente no queda subsumido -y, por ende, que la legislación en materia de protección de datos es aplicable-, no llegamos a la misma conclusión si lo relacionamos con el considerando 18 del RGPD. Sin embargo, la doctrina emanada por el TC res-

pecto al artículo 18.4 de la CE sí quedaría vulnerada en el presente supuesto, motivo que nos conduce a sostener que también en estos casos se vulnera el derecho fundamental a la protección de datos.

1.2.1. La excepción doméstica

El RGPD ha previsto la denominada *excepción doméstica*, en virtud de la cual queda fuera del ámbito de aplicación del RGPD aquel tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

No obstante, el RGPD no define con precisión qué debe entenderse por «en el ejercicio de actividades exclusivamente personales o domésticas». Al respecto, el considerando 18 del RGPD realiza un matiz que, en nuestro caso, adquiere especial relevancia al vincular el concepto de «actividades exclusivamente personales o domésticas» con la ausencia de cualquier conexión con una actividad profesional o comercial. Sin embargo, son fácilmente imaginables supuestos en los que una persona física realice un tratamiento de los datos de otra que puedan perjudicar a esta última, sin estar habilitada para ello y sin que necesariamente esté conectado este tratamiento con una actividad profesional o comercial. *Verbigracia*, en un procedimiento de divorcio, uno de los cónyuges genera un *deepfake* del otro en el cual aparece actuando de forma agresiva hacia la hija menor común y aporta este material como prueba con el objetivo de obtener la custodia exclusiva de la menor. En este caso, resulta cuestionable si opera o no la excepción doméstica y, por lo tanto, no es diáfano si el tratamiento de datos producido en la realización de la ultrasuplantación debiera evaluarse o no desde la óptica del RGPD.

La jurisprudencia del TJUE⁹ ha interpretado esta excepción de manera restrictiva, haciendo énfasis en que verdaderamente consista en una actividad «exclusivamente» personal o doméstica. Por ello, se ha considerado que solamente opera en actividades que se inscriben dentro del marco de la vida privada o familiar de los particulares,¹⁰ llegando incluso a excluir la actividad de curador a título profesional realizada por una persona física.¹¹

9. SSTJUE C-345/17, C-25/17, C-73/16 y C-212/13.

10. SSTJUE C-25/17, C-73/07 y C-101/01.

11. STJUE C-461/22.

El Tribunal Supremo español¹² ha destacado la conexión de esta excepción con el hogar familiar, refiriendo que en dicho ámbito pueden desarrollarse tratamientos de datos personales debido a la especial protección constitucional que merece el domicilio como espacio de ejercicio de derechos fundamentales, singularmente la intimidad personal y familiar, de modo que esta exclusión solo resulta aplicable cuando el tratamiento permanece íntegramente dentro de esa esfera privada y no trasciende a terceros ni al espacio público.

La doctrina (Megías Quirós, 2021) entiende que la justificación de esta excepción se encuentra en salvaguardar el control sobre los datos de carácter personal y el derecho a la vida privada y familiar de todo ciudadano. En particular, solo sería aplicable esta excepción cuando el mencionado tratamiento de datos sin el consentimiento de su titular incide de manera mínima en la vida privada de este último, es decir, cuando estos datos tratados permanecen en la esfera íntima de las personas unidas por lazos familiares o de amistad.

En este sentido, hay quienes sostienen (Megías Quirós, 2021) que, en el caso de utilizar datos personales con un fin judicial, su utilización quedaría automáticamente sometida a las exigencias establecidas en las normas de protección. Por lo tanto, no se aplicaría la excepción doméstica. Si extrapolamos esta tesis a nuestro supuesto, entonces podría afirmarse que la generación de un *deepfake* para su posterior aportación como prueba vulneraría el derecho fundamental a la protección de datos, sin perjuicio de que el creador del *deepfake* fuera una persona física. Sin embargo, a mi modo de ver, esto no resulta tan diáfano. Es cierto que no parece plausible calificar la generación de un *deepfake* con la finalidad de presentarlo como prueba en un proceso judicial como una «actividad exclusivamente personal o doméstica». Ahora bien, debido a la vinculación que realiza el considerando 18 del RGPD, *a priori* deberíamos analizar, caso por caso, si hay una conexión entre el objeto del litigio, el *deepfake* aportado como prueba y la actividad comercial o profesional de aquel que la aporta.

Todo lo anterior nos conduce a la conclusión de que, en los casos de generación de *deepfakes* de personas físicas

generados por otras personas físicas para su posterior aportación como prueba, podemos encontrarnos ante dos situaciones.

Una en la que la generación de ese *deepfake* sí que esté vinculada con una actividad profesional o comercial -*verbigracia*, el caso de un autónomo que elabore un *deepfake* de voz en el que un sujeto aparezca mostrando (artificialmente) la aceptación a un contrato-. En ese caso, sí que podríamos afirmar la existencia del vínculo que establece el considerando 18 del RGPD y, por ende, no se aplicaría la excepción del artículo 2.2c) del RGPD. Esto nos conduciría a que sí operase tanto el RGPD como la LOPDGDD y entonces se entendiera vulnerado el derecho a la protección de datos personales por los motivos expuestos en el apartado anterior, relativo a los *deepfakes* generados por personas jurídicas, es decir, debido a que el tratamiento de datos no se habría realizado bajo ninguna de las bases que lo legitiman.

Y otra, en la que no exista la indicada vinculación. En tal escenario, en mi opinión, no es claro si operarían el RGPD y la LOPDGDD, en la medida en que podría entenderse que opera la excepción doméstica debido a lo establecido en el considerando 18 del RGPD. Ahora bien, aunque llegáramos a considerar que no son aplicables, como veremos en el siguiente subapartado, sí que debería sostenerse que, bajo la óptica de la doctrina del TC en relación con el artículo 18.4 de la CE, se vulneraría el derecho fundamental a la protección de datos de carácter personal.

1.2.2. La jurisprudencia del Tribunal Constitucional español respecto al artículo 18.4 de la CE

A partir de lo dispuesto en el artículo 18.4 de la CE, el TC ha configurado el derecho fundamental a la protección de datos personales. Este precepto constitucional se ha concebido tanto como un derecho de carácter instrumental, que pretende salvaguardar otros derechos -muy en particular, el derecho al honor y la intimidad-, como, también, un derecho de carácter autónomo cuyo contenido, en términos generales, consiste en el derecho a la libertad frente a potenciales agresiones a la dignidad y

12. STS 692/2022, de 22 de julio.

libertad de una persona provenientes del uso ilegítimo de la informática.¹³

Su objeto es más amplio que el del derecho a la intimidad, puesto que comprende también aquellos datos que sean relevantes para el ejercicio de cualesquiera derechos de la persona, sean o no relativos al honor, la ideología, la intimidad personal y familiar o a cualquier otro bien constitucionalmente amparado.¹⁴ En consecuencia, su ámbito de protección no se circunscribe únicamente a los datos íntimos de la persona, sino que incluye cualquier tipo de dato personal, sea o no íntimo, cuyo empleo o conocimiento por terceros pueda afectar a sus derechos, sean o no fundamentales.¹⁵ En efecto, se ha considerado que la imagen¹⁶ y la voz son datos personales en relación con el artículo 18.4 de la CE.

El derecho de control sobre los datos relativos a la propia persona -la denominada «libertad informática»- implica el derecho a controlar el uso de los datos insertos en un programa informático -*habeas data*- y abarca, entre otras cuestiones, la posibilidad de oposición a que los datos sean empleados con fines distintos a aquel legítimo que justificó su obtención.¹⁷ Por tanto, se pretende garantizar el poder de control del titular de los datos sobre el uso y destino de estos y así impedir su tráfico ilícito y lesivo para la dignidad del afectado.¹⁸ La razón de ello radica en que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo está también de su derecho fundamental a la protección de datos, ya que «se rebasa o se desconoce el contenido esencial cuando

el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificulten más allá de lo razonable o lo despojan de la necesaria protección».¹⁹

Los poderes de disposición y control se concretan jurídicamente en las facultades de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles. Y precisa como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y, por otro lado, el poder oponerse a esa posesión y usos.²⁰

De lo anterior se infiere que la cesión de datos a un tercero para proceder con fines distintos de los que originaron su recogida supone una nueva posesión y uso que requiere el consentimiento del interesado, puesto que de lo contrario se está vulnerando el derecho fundamental del artículo 18.4 de la CE.²¹

En cuanto a los límites de este derecho, por un lado, la Constitución establece expresamente el artículo 105 b)²² y, por otro lado, en virtud del principio de unidad de la CE, también actúan como límite los restantes derechos fundamentales y bienes jurídicos protegidos constitucionalmente.²³ Además, estas limitaciones deben estar justificadas, ser proporcionadas y estar establecidas mediante ley, ya que el derecho fundamental a la protección de datos no admite otros límites.²⁴ Asimismo, en aquellas ocasiones en las que colisione con otro derecho fundamental, uno

13. SSTC 23/2022, de 21 de febrero; 292/2000, de 30 de noviembre; 202/1999, de 8 de noviembre; 143/1994, de 9 de mayo; 11/1998, de 13 de enero, y 254/1993, de 20 de julio.

14. SSTC 96/2012, de 7 de mayo, y 292/2000, de 30 de noviembre.

15. SSTC 89/2022, de 29 de junio; 17/2013, de 31 de enero; 96/2012, de 7 de mayo, y 292/2000, de 30 de noviembre.

16. SSTC 119/2022, de 29 de septiembre; 39/2016, de 3 de marzo; 29/2013, de 11 de febrero, y 14/2003, de 28 de enero.

17. SSTC 23/2022, de 21 de febrero; 96/2012, de 7 de mayo; 44/2009, de 12 de febrero; 292/2000, de 30 de noviembre; 202/1999, de 8 de noviembre; 44/1999, de 22 de marzo; 94/1998, de 4 de mayo; 254/1993, de 20 de julio, y 11/1998, de 13 de enero. A esta última se remiten enteramente doce sentencias más.

18. SSTC 119/2022, de 29 de septiembre; 23/2022, de 21 de febrero; 39/2016, de 3 de marzo; 29/2013, de 11 de febrero; 17/2013, de 31 de enero; 96/2012, de 7 de mayo; 44/2009, de 12 de febrero; 110/2007, de 10 de mayo; 85/2003, de 8 de mayo, y 292/2000, de 30 de noviembre.

19. SSTC 292/2000, de 30 de noviembre, y 11/1981, de 8 de abril.

20. SSTC 119/2022, de 29 de septiembre; 23/2022, de 21 de febrero; 39/2016, de 3 de marzo; 96/2012, de 7 de mayo, y 292/2000, de 30 de noviembre.

21. SSTC 96/2012, de 7 de mayo, y 292/2000, de 30 de noviembre.

22. «Artículo 105. La ley regulará: b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas».

23. SSTC 23/2022, de 21 de febrero; 39/2016, de 3 de marzo; 17/2013, de 31 de enero; 292/2000, de 30 de noviembre; 196/1987, de 11 de diciembre; 110/1984, de 21 de diciembre, y 11/1981, de 8 de abril.

24. STC 96/2012, de 7 de mayo.

de ellos deberá ser considerado prevalente para ese caso en concreto. Mas el derecho preterido no queda vacío de contenido, sino que solo debe ser sacrificado en la medida estrictamente necesaria para salvaguardar la efectividad del prevaleciente.²⁵ La razón que subyace es la inexistencia de una jerarquía entre derechos fundamentales, de manera que la determinación de la prevalencia de uno u otro derecho depende de las circunstancias de cada caso en concreto.²⁶

Expuesto lo que antecede, la generación de *deepfakes* de una persona física sin su consentimiento con el fin de aportar dichos contenidos como prueba en un proceso judicial vulnera el derecho fundamental a la protección de datos en tanto en cuanto el sujeto sobre el que se realiza la ultrasuplantación estará perdiendo el poder de disposición sobre sus datos personales -la imagen y/o la voz-. Asimismo, la doctrina del TC no limita expresamente el ámbito subjetivo del artículo 18.4 de la CE, exigiendo que el sujeto infractor necesariamente sea una persona jurídica, ni que, aun siendo una persona física, la infracción deba haberse producido en el marco de una actividad comercial o profesional.

A mayor abundamiento, tampoco podría entrar un caso como el presente bajo alguno de los límites constitucionales del artículo 18.4 de la CE. Es decir, ni el artículo 105 b) de la CE es aplicable, puesto que se refiere al derecho de acceso de los ciudadanos a los archivos y registros administrativos, ni tampoco el principio de unidad de la CE podría justificar la presente injerencia, en tanto en cuanto las pruebas *deepfake* no quedan bajo el amparo conferido por ningún otro derecho o libertad fundamental.

Además, el artículo 10.2 de la CE estipula que los derechos fundamentales deben ser interpretados conforme a los tratados y acuerdos internacionales ratificados.²⁷ Precisamente, la Carta de los Derechos Fundamentales de la Unión Europea establece en su artículo octavo el

derecho a la protección de datos. Este precepto, al igual que la jurisprudencia del TC, configura el mencionado derecho sin limitar su ámbito subjetivo de aplicación a aquellos tratamientos realizados por personas jurídicas o personas físicas en el marco de una actividad comercial o profesional. En este sentido, señala que los datos deben tratarse de un modo leal, para fines concretos y sobre la base del consentimiento u otro fundamento legítimo. Ahora bien, en un supuesto como el aquí analizado, no es plausible afirmar que los datos hayan sido tratados de un modo leal ni tampoco que hayan sido generados bajo un fundamento que legitime su tratamiento, ya que con ellos se pretende generar artificialmente una prueba falsa.

En definitiva, aun si considerásemos que no son aplicables el RGPD y la LOPDGDD por efecto de la excepción doméstica, debería sostenerse que en aquellos casos en los que una persona física realiza el *deepfake* de otra con el fin de aportarlo como prueba en un proceso judicial, se ha producido una vulneración del derecho fundamental a la protección de datos en atención a la doctrina del TC en relación con el artículo 18.4 de la CE.

1.3. *Deepfakes* generados a partir de contenidos audiovisuales accesibles públicamente

Internet y las redes sociales han configurado un auténtico ecosistema digital en el que circulan masivamente datos de carácter personal. Dicha información puede consistir en fotografías, audios o vídeos relativos a determinadas personas físicas que, en ocasiones, son publicados por estas mismas y en otras son compartidos por terceros. A partir de estos materiales publicados, es posible crear *deepfakes*, y en estos casos es cuestionable la vulneración del derecho a la protección de datos debido a que los contenidos empleados son accesibles públicamente y, por consiguiente, pudiese llegar a considerarse que, en el acto de la publicación del material, el usuario estuviese desistiendo de la protección conferida a estos datos.

25. Esto es respaldado por el TC (SSTC 58/2018, de 4 de junio; 121/2002, de 20 de mayo, y 171/1990, de 12 de noviembre), por el TJUE (STJUE C-73/07, C-92/09 y C-93/09) y por el TEDH (STEDH *Mouvement raëlien Suisse c. Suiza*).

26. ATC 155/2009, de 18 de mayo.

27. Como ha establecido la jurisprudencia del TC, este precepto no trata de crear *ex novo* derechos fundamentales, sino de concretar el contenido de los presentes en la Constitución. Esto último puede conducir a la incorporación de facultades, garantías o posiciones jurídicas no explicitadas en el texto constitucional, pero que derivan de un derecho fundamental (STC 150/2011, de 29 de septiembre).

No obstante, esta interpretación es errónea. El TC²⁸ ha expresado que los datos personales públicos no escapan del poder de disposición del afectado que confiere el derecho a la protección de datos. Por esta razón, se sostiene, en relación con la compartición de imágenes, que el hecho de que circulen datos privados en internet no significa que lo privado se haya tornado público, ni tampoco que, debido a ello, los ciudadanos hayan perdido o renunciado a los derechos del artículo 18.4 de la CE.²⁹

Desde la óptica del RGPD, el carácter público de un dato personal no implica su desprotección, puesto que los tratamientos realizados a partir de estos deben igualmente realizarse bajo alguna de las condiciones habilitadoras del artículo 6.1 del RGPD, resultando, conforme a lo expuesto en los apartados anteriores, que ninguna de ellas justifica la realización de *deepfakes* para su posterior aportación como prueba.³⁰

Especialmente esclarecedora es la tesis sostenida por ciertos autores alemanes (Orrù, 2024) que parten de una diferenciación entre los términos *dato* e *información*. Así, los datos son signos que, por sí mismos, no necesariamente tienen un significado propio, y la información son datos interpretados dentro de un contexto. En consecuencia, cuando una persona publica un material audiovisual, -por ejemplo, una imagen en una red social- está difundiendo datos -entre otros, los píxeles de la imagen compartida-, pero en realidad su intención es transmitir una información específica dentro de un contexto -*verbigracia*, la imagen de perfil de un usuario en una red social pretende mostrar una primera impresión de sí mismo al resto-. De esta manera, puede afirmarse que el usuario, a partir de la publicación de dicha fotografía, no habrá pretendido compartir, entre otros, sus datos biométricos, a pesar de que estos puedan ser extraídos de la imagen publicada. El

foco, entonces, está en las características de la información y, por lo tanto, existirá vulneración cuando los datos hayan sido tratados en un contexto diferente respecto a aquel inicial en el que fueron publicados.

En definitiva, la existencia de contenidos audiovisuales accesibles públicamente no implica que el interesado haya desistido de la protección conferida por el artículo 18.4 de la CE, incluso cuando él mismo haya publicado dichos materiales. El dato personal, aunque público, sigue estando protegido por la normativa en protección de datos y deberá analizarse el posterior tratamiento con el fin de determinar su licitud.³¹ Ahora bien, en el caso de la creación de *deepfakes* con el objetivo de aportarlos posteriormente como prueba, tal y como ha sido expuesto con anterioridad, ninguna base legitimadora justifica dicho tratamiento y, por lo tanto, debemos concluir que en estos casos también se habrá vulnerado el derecho fundamental a la protección de datos.

1.4. *Deepfakes* en los que no aparecen datos de carácter personal

El derecho a la protección de datos no engloba todo dato, sino únicamente aquellos que tienen la consideración de carácter personal. Por tanto, pudiera pensarse que en aquellos *deepfakes* en los que no aparezcan datos de carácter personal, no se ha vulnerado el derecho a la protección de datos. Sin embargo, esta rápida conclusión no es acertada.

Es preciso distinguir los casos en los que para la generación del *deepfake* no se hayan utilizado datos de carácter personal -respecto a los cuales no se debería considerar vulnerado el derecho a la protección de datos- de aquellos en los que sí se hayan tratado datos de carácter personal,

28. STC 96/2012, de 7 de mayo; STC 292/2000, de 30 de noviembre, y el voto particular de María Luisa Balaguer Callejón en la STC 33/2023, de 18 de abril.

29. Voto particular de María Luisa Balaguer Callejón en la STC 33/2023, de 18 de abril.

30. Tampoco nos debe conducir a error lo estipulado en el artículo 9.2 e) del RGPD, que establece como excepción a la prohibición del tratamiento de datos biométricos los casos en los que «el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos», puesto que en virtud del considerando 51 del RGPD, dicha excepción debe interpretarse a la luz del artículo 6 del RGPD, de manera que los tratamientos de datos biométricos que el interesado ha hecho manifiestamente públicos no están prohibidos, pero deben realizarse con base en las condiciones habilitadoras que establece el RGPD.

31. Recordemos, además, el matiz introducido en los apartados anteriores, a saber: desde la perspectiva del derecho a la protección de datos, la legitimidad de la realización de un *deepfake* requiere analizar tanto la licitud de la obtención de los datos empleados como la del posterior tratamiento realizado a partir de estos. En consecuencia, aun cuando la obtención de dichos contenidos pudiera considerarse legítima, por ser accesibles públicamente, su uso para generar la ultrasuplantación requiere un examen específico que, en el presente caso, conduce a sostener su ilicitud.

pero estos no aparezcan exteriorizados en el *deepfake* -en los que sí se habría vulnerado igualmente este derecho fundamental-.

Para apreciarlo con mayor claridad, expondremos un ejemplo. Imaginemos el supuesto en el que una empresa pretende acreditar en un procedimiento laboral que un trabajador no se encontraba en su puesto de trabajo en un determinado momento, a efectos de justificar una sanción disciplinaria que ha sido recurrida ante los tribunales. Sin embargo, existe una grabación original de las cámaras de seguridad en la que el trabajador aparece en el centro de trabajo en la hora controvertida. Acto seguido, la empresa modifica artificialmente la grabación eliminando la presencia física del trabajador, de tal modo que el vídeo final refleja el centro de trabajo sin el trabajador en dicho momento y sin otros datos que nos pudieran permitir identificarlo. Como podemos comprobar, en el contenido sintético resultante es posible que no aparezcan datos de carácter personal, pero estos sí han sido tratados en el proceso de obtención del *deepfake*. En consecuencia, que en un *deepfake* no aparezcan exteriorizados datos de carácter personal no implica la ausencia de un tratamiento ilegítimo de los mismos en el proceso de obtención de la ultrasuplantación. Cuestión distinta -que no va a ser abordada en este artículo- es cómo probar que, en un *deepfake* en el que no aparezcan datos de carácter personal, se han empleado contenidos audiovisuales que sí disponían de estos.

2. La prueba *deepfake* como prueba ilícita

Una vez hemos determinado aquellos supuestos en los que la generación de *deepfakes* con el fin de su aportación como prueba vulnera el derecho fundamental a la protección de datos, analizamos a continuación la calificación de la prueba *deepfake* como prueba ilícita en España.

El derecho fundamental a la prueba no es absoluto ni ilimitado en tanto en cuanto está sujeto a límites intrínsecos y

extrínsecos. Los primeros derivan de la propia naturaleza de la actividad probatoria -estos son la pertinencia y la utilidad-, mientras que los segundos, en cambio, hacen referencia a las formalidades y los cauces procesales necesarios para el ejercicio válido de este derecho fundamental (Picó i Junoy, 2021).

La ilicitud probatoria es un límite extrínseco del derecho constitucional a la prueba vinculado al proceso de obtención de la prueba que implica, siguiendo a la expresiva terminología italiana, la *inutilizzabilità* de dicho elemento.³² Ahora bien, de la consideración de que no toda prueba vale en función de cómo ha sido lograda, subyace el problema del alcance. Es decir, el de la determinación del criterio que permita decidir cuáles valen y cuáles no, cuestión que no es pacífica.

De este modo, como ha sido expuesto en un estudio de derecho comparado sobre las distintas concepciones de la prueba ilícita, podemos apreciar que ciertos Estados adoptan conceptos muy amplios -como Francia, que excluye la prueba lograda con vulneración del principio de lealtad-, mientras que otros abogan por conceptos mucho más restrictivos -como Estados Unidos, donde la jurisprudencia de su Corte Suprema relaciona el alcance de la prueba ilícita con la vulneración realizada por un agente público de cualquier derecho contenido en las enmiendas IV, V, VI o XIV de su *Bill of Rights*- (Picó i Junoy, 2025).

En España, el artículo 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ),³³ instauró la definición de prueba ilícita mayoritariamente acogida por la doctrina al vincular el concepto de ilicitud probatoria con la vulneración de un derecho fundamental en el proceso de obtención del elemento probatorio.³⁴ No obstante, el panorama ha tornado a oscurecerse tras la STC 97/2019, de 16 de julio -comúnmente conocida como caso *Falciani*-, que estableció que la vulneración de un derecho fundamental en la obtención de una prueba no es suficiente para determinar la ilicitud de esta última, sino que, además, el elemento probatorio debe haberse obtenido con la intención de perjudicar el derecho de defensa de

32. En concreto, en España se vincula a la vulneración de derechos o libertades fundamentales, sea debido a que la fuente probatoria está contaminada por la indicada vulneración o porque el medio probatorio ha sido practicado con idéntica infracción (Picó i Junoy, 2021).

33. Del *iter* parlamentario de esta norma se elucida que recoge el concepto de prueba ilícita expuesto por la STC 114/1984, de 29 de noviembre (Picó i Junoy, 1996).

34. Sea debido a que la fuente probatoria está contaminada por la vulneración de un derecho fundamental o porque el medio probatorio ha sido practicado con idéntica infracción (Picó i Junoy, 2021).

la parte contraria. Esta limitación del alcance de la prueba ilícita se debe a la necesidad de proteger al máximo el derecho a la prueba (Picó i Junoy, 2020).

Bajo el enfoque de la doctrina Falciani, el análisis de la ilicitud de una prueba debe abordarse tanto desde una perspectiva interna como externa.

El control interno requiere la apreciación de que la vulneración del derecho fundamental ha estado instrumentalmente orientada a la obtención de pruebas al margen del canon constitucional exigible, comprometiéndose con ello la integridad del proceso en curso y la igualdad entre las partes, salvo en aquellos casos en los que la vulneración, a pesar de carecer de dicho carácter instrumental, sea de tal intensidad que afecte al núcleo axiológico de nuestro orden de derechos fundamentales. Adicionalmente, el control externo determina que debe evaluarse si existen necesidades generales de prevención o disuasión de la vulneración consumada.

Conforme a lo planteado en el apartado primero, en determinados supuestos, en la obtención del *deepfake* de un sujeto en particular, se vulnera el derecho a la protección de datos, que es un derecho fundamental. En consecuencia, resulta claro que, si nos acogemos a la concepción de prueba ilícita prevista en el artículo 11.1 de la LOPJ, las pruebas *deepfake* obtenidas a partir de la indicada vulneración del artículo 18.4 de la CE son pruebas ilícitas. En cambio, si adoptamos la doctrina del caso *Falciani*, deberíamos realizar un análisis caso por caso para determinar si, desde una perspectiva interna y externa, dicho elemento se ha obtenido con la finalidad de perjudicar el derecho de defensa de la parte contraria.

Conclusiones

Los *deepfakes* introducen al proceso un conjunto de aspectos problemáticos que deben ser debidamente analizados con el objetivo de adaptar el derecho procesal a los nuevos desafíos tecnológicos. En determinados casos, según la concepción de prueba ilícita vigente en el ordenamiento jurídico español, la prueba *deepfake* reúne las características de ser falsa en cuanto a su contenido e ilícita en cuanto a la forma en la que esta ha sido obtenida. Ahora bien, la demostración de que el material aportado como prueba es un *deepfake* es condición necesaria para su apreciación como prueba tanto falsa como ilícita. En

efecto, la detección de estos contenidos audiovisuales hiperrealistas es uno de los grandes retos que tanto juristas como expertos de otras disciplinas debemos afrontar para preservar, entre otras cuestiones, las garantías del proceso.

Reconocimientos

Agradezco enormemente las continuas orientaciones y los comentarios críticos del profesor Joan Picó i Junoy.

Referencias bibliográficas

- Agencia Española de Protección de Datos (2025). «Riesgos para la protección de datos al utilizar servicios que convierten fotografías a formato Ghibli o similares». *AEPD* [en línea]. Disponible en: <https://www.aepd.es/prensa-y-comunicacion/blog/riesgos-utilizar-servicios-convierten-fotografias-formato-ghibli> [Fecha de consulta: 15 de febrero de 2026]
- ALMAGRO MARTÍN, J. (2024). «Tratamiento procesal de la prueba del *deepfake*». *Derecho Digital e Innovación*, n.º 21 (julio-septiembre).
- BOTÉ VERICAD, J. J.; VÁLLEZ, M. (2022). «Aplicaciones de deepfakes. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad». *Documentación de las Ciencias de Información*, n.º 45, págs. 25-32. DOI: <https://doi.org/10.5209/dcin.77256>
- CANO FERNÁNDEZ, S. (2025). «¿Cómo se prueba un *deepfake*? la lucha contra la mentira». En: PICÓ i JUNOY, J.; MIRANDA VÁZQUEZ, C. (dirs.). *Nuevos retos del derecho probatorio*. Barcelona: J. M. Bosch Editor, págs. 149-162. DOI: <https://doi.org/10.2307/jj.39224090.10>
- JIMÉNEZ-CASTELLANOS BALLESTEROS, I. (2025). «La difícil convivencia entre la inteligencia artificial y los derechos fundamentales: La tecnología *deepfake*». En: FEBLES POZO, N.; NIETO ROJAS, P. (dirs.). *Inteligencia artificial y protección de datos: desafíos en la era digital*. A Coruña: Editorial Colex, págs. 151-178. DOI: <https://doi.org/10.69592/979-13-7011-111-3-CAP-5>
- MEGÍAS QUIRÓS, J. J. (2021). «Actividades personales y domésticas excluidas del ámbito de aplicación (Comentario al artículo 2.2c) RGPD y al artículo 2.2ª) LOPDGGD)». En: TRONCOSO REIGADA, A. (ed.). *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*. Thomson Reuters Aranzadi, págs. 355-375.
- NIEVA FENOLL, J. (2025). «La prueba de los deepfakes pornográficos: I. A. sobre I. A.». En: PICÓ i JUNOY, J.; MIRANDA VÁZQUEZ, C. (dirs.). *Nuevos retos del derecho probatorio*. Barcelona: J. M. Bosch Editor, págs. 133-148. DOI: <https://doi.org/10.2307/jj.39224090.9>
- ORRÚ, E. (2024). «Are publicly available (personal) data “up for grabs”? Three privacy arguments». En: DE HERT, P.; MATSUMI, H.; HALLINAN, D.; DIMITROVA, D.; KOSTA, E. *Data Protection and Privacy: Ideas that drive our digital world*, vol. 16. London: Hart Publishing, págs. 105-123. DOI: <https://doi.org/10.5040/9781509975976.ch-004>
- PELLICER ORTIZ, B. (2025). «Los “deepfakes” y su aportación como prueba en los procesos judiciales». En: MUNNÉ CATARINA, F.; MIRANDA VÁZQUEZ, C. (dirs.). *Desafíos de la probática y del derecho probatorio*. Barcelona: J. M. Bosch Editor, págs. 159-179. DOI: <https://doi.org/10.2307/jj.35139448.7>
- PICÓ i JUNOY, J. (1996). *El derecho a la prueba en el proceso civil*. Barcelona: J. M. Bosch Editor. 441 págs.
- PICÓ i JUNOY, J. (2020). «La prueba ilícita: un concepto todavía por definir». *La Ley Probática*, n.º 1.
- PICÓ i JUNOY, J. (2021). «El derecho a la prueba». En: PICÓ i JUNOY, J.; MENDOZA DÍAZ, J.; MANTECÓN RAMOS, A. (dirs.). *La prueba a debate: diálogos hispano-cubanos*. Barcelona: J. M. Bosch Editor, págs. 19-60. DOI: <https://doi.org/10.2307/jj.ctv1tqcwvs.4>
- PICÓ i JUNOY, J. (2025). «La prueba ilícita: una mirada desde el derecho comparado». En: ANDINO LÓPEZ, J. A.; PICÓ i JUNOY, J. (dirs.). *Prueba y derecho. Algunas reflexiones críticas*. Barcelona: J. M. Bosch Editor, págs. 55-68.
- SALVADOR CERQUEDA, A. (2025). «Principales conceptos». En: SALVADOR CERQUEDA, A. (coord.). *Tratado de Protección de Datos Personales*. Barcelona: Atelier, págs. 61-70.
- TRUJILLO CABRERA, C. (2024). «El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial». *InDret*, n.º 1, págs. 74-113. DOI: <https://doi.org/10.31009/InDret.2024.il.02>

Cita recomendada

ALMAGRO MARTÍN, Joel (2026). «La prueba *deepfake* como prueba ilícita». *IDP. Revista de Internet, Derecho y Política*, núm. 45. UOC [Fecha de consulta: dd/mm/aa]. DOI: <http://dx.doi.org/10.7238/idp.v0i45.980000005516>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Sobre el autor

Joel Almagro Martín

Universitat Pompeu Fabra - Barcelona School of Management (UPF-BSM)

joelalma@gmail.com

Graduado en Derecho en la Universidad Pompeu Fabra y máster universitario de Acceso a la Abogacía y Procura en la UPF-BSM. Presta sus servicios en el área de procesal de Duran-Sindreu, Asesores Legales y Tributarios, SLP. Además, combina su actividad profesional con el desarrollo de su labor investigadora en relación con los aspectos procesales de los *deepfakes*. Fruto de ello, ha participado en diversas ponencias y ha publicado los estudios «*The liar's dividend: Deepfakes* y el uso perverso de su alegación procesal», en *Justicia: Revista de Derecho Procesal* (2025, n.º 1, págs. 371-428), y «Tratamiento Procesal de la Prueba del *Deepfake*», en *Derecho Digital e Innovación* (2024, n.º 21, julio-septiembre).