DESAFÍOS PROCESALES DE LA DETECCIÓN DE DEEPFAKES Y SU VALORACIÓN EN EL SISTEMA DE JUSTICIA DIGITAL

Redacción derechoartificial.com
Fecha: Marzo de 2026

DERECHO ARTIFICIAL

ÍNDICE

RESUMEN

La irrupción de la inteligencia artificial generativa, específicamente a través de las Redes Adversarias Generativas (GAN), ha posibilitado la creación de contenidos multimedia hiperrealistas conocidos como deepfakes o ultrafalsificaciones. Este fenómeno plantea un desafío sin precedentes para el derecho probatorio contemporáneo, al superar los umbrales de la percepción sensorial humana y cuestionar el paradigma tradicional de "ver para creer". El presente artículo analiza la naturaleza jurídica de los deepfakes como "prueba sintética" y su encaje en el marco normativo español, principalmente como prueba documental digital bajo la Ley de Enjuiciamiento Civil y la Ley de Enjuiciamiento Criminal. Se examinan las herramientas técnicas de vanguardia para su identificación —desde el análisis de metadatos y biometría (señales PPG) hasta el uso de Vision Transformers (ViT)— y se confrontan con los estándares de admisibilidad y valoración judicial. La tesis principal sostiene que la inmediación sensorial del juzgador es hoy insuficiente, deviniendo la pericia técnica y el cumplimiento de protocolos internacionales de gestión de evidencias (ISO/IEC 27037:2012) en requisitos sine qua non para salvaguardar la presunción de inocencia y la integridad del proceso. Finalmente, se evalúan las implicaciones sistémicas de la construcción paralela de investigaciones y las propuestas de lege ferenda, incluyendo el nuevo marco de transparencia del Reglamento de IA de la Unión Europea y la necesidad de una reforma procesal que estandarice la cadena de custodia digital frente al riesgo de estafa procesal.

ABSTRACT

The emergence of generative artificial intelligence, specifically through Generative Adversarial Networks (GANs), has enabled the creation of hyper-realistic multimedia content known as deepfakes. This phenomenon poses an unprecedented challenge to contemporary evidentiary law by surpassing the thresholds of human sensory perception and questioning the traditional "seeing is believing" paradigm. This article analyzes the legal nature of deepfakes as "synthetic evidence" and its placement within the Spanish regulatory framework, primarily as digital documentary evidence under the Law of Civil Procedure and the Law of Criminal Procedure. State-of-the-art technical tools for identification—ranging from metadata and biometric analysis (PPG signals) to the use of

Vision Transformers (ViT)—are examined and contrasted with standards of admissibility and judicial valuation. The main thesis argues that the judge's sensory immediacy is currently insufficient, making technical expert testimony and compliance with international evidence management protocols (ISO/IEC 27037:2012) sine qua non requirements to safeguard the presumption of innocence and the integrity of the legal process. Finally, it evaluates the systemic implications of parallel construction in investigations and proposals for lege ferenda, including the new transparency framework of the European Union AI Act and the need for procedural reform to standardize the digital chain of custody against the risk of procedural fraud.

I. INTRODUCCIÓN

La irrupción de la inteligencia artificial generativa ha marcado un punto de inflexión en la configuración de la prueba digital en el proceso penal y civil contemporáneo. Si bien la digitalización de la sociedad se ha consolidado como la cuarta revolución industrial, la capacidad actual de los algoritmos para generar **«representaciones sintéticas»** o **«ultrafalsificaciones»** (deepfakes)[^1] plantea un desafío estructural para el derecho probatorio. El fenómeno, que inicialmente se asoció a la desinformación política y a la pornografía no consentida, ha trascendido a la esfera jurisdiccional, donde la creación de contenidos multimedia hiperrealistas mediante técnicas de aprendizaje profundo amenaza con socavar los principios de inmediación, contradicción y verdad material.

El paradigma tradicional de la justicia, sintetizado en la máxima «ver para creer», se encuentra hoy en crisis. Los deepfakes, creados fundamentalmente a través de **Redes Adversarias Generativas (GAN)**[^2] —un sistema donde un modelo generador compite contra uno discriminador hasta alcanzar un equilibrio de Nash de indistinguibilidad—, son capaces de superar los umbrales de la percepción sensorial humana. Esta realidad técnica impide que el juzgador, mediante su mera observación directa, pueda discriminar con certeza entre una evidencia auténtica y una manipulada.

La **tesis principal** que sostiene este artículo es que el sistema procesal español, si bien posee flexibilidad interpretativa para integrar el documento electrónico, presenta una brecha normativa y técnica que exige un desplazamiento del modelo de valoración libre hacia un modelo de **verificación técnica obligatoria**. En un contexto donde la apariencia de veracidad puede ser generada algorítmicamente de forma ilimitada, la inmediación sensorial resulta insuficiente si no se acompaña de una pericia informática rigurosa y del cumplimiento estricto de estándares internacionales de gestión de evidencias, singularmente la norma **ISO/IEC 27037:2012**[^3]. La admisibilidad de la prueba sintética no debe depender de la «ausencia de dudas» del juez, sino de la trazabilidad íntegra del dato digital y la solidez científica de las herramientas de detección.

Para fundamentar esta tesis, el presente trabajo se estructura en un mapa de ruta que recorre siete apartados críticos. En la **Parte I**, se delimita el marco fáctico y normativo, analizando la evolución de la prueba electrónica y su encaje como prueba documental. La **Parte II** aborda el marco teórico-doctrinal, definiendo la naturaleza de la prueba sintética y su distinción de las manipulaciones tradicionales o shallowfakes. En la **Parte**

III, se analiza detalladamente el problema jurídico de la autenticidad y la carga de la prueba ante la impugnación de archivos digitales. La **Parte IV** evalúa críticamente las herramientas de detección —desde el análisis de metadatos hasta señales biométricas PPG— y las tensiones que generan en el derecho de defensa. La **Parte V** ofrece un análisis comparado de la respuesta legislativa, con especial atención al Reglamento de IA de la Unión Europea y la Directiva 2024/1385[^4]. Finalmente, las **Partes VI y VII** exponen las implicaciones sistémicas para la práctica judicial, como el riesgo de estafa procesal, y formulan propuestas de lege ferenda para una reforma procesal que garantice la integridad del entorno virtual.

II. MARCO FÁCTICO, NORMATIVO Y PROCEDIMENTAL

El abordaje jurídico de los deepfakes o representaciones sintéticas exige, de manera preliminar, una delimitación de su génesis técnica y del ecosistema normativo que ha intentado, con desigual éxito, aprehender una realidad caracterizada por la inmaterialidad y la ubicuidad. En el sistema procesal español, este fenómeno no ha nacido en un vacío, sino que se ha insertado en la evolución de la prueba electrónica, obligando a una interpretación extensiva de preceptos decimonónicos y a la creación de nuevas salvaguardas tecnológicas.

1. Antecedentes fácticos: De la edición manual a la autonomía algorítmica

La manipulación audiovisual no es un fenómeno reciente; sus raíces se remontan a mediados del siglo XIX con la edición de negativos fotográficos. Sin embargo, la aparición de la tecnología deepfake en 2017, vinculada inicialmente a plataformas de intercambio de contenidos como Reddit, supuso un salto cualitativo disruptivo. A diferencia de las manipulaciones tradicionales o shallowfakes —basadas en la edición manual de fragmentos o montajes rudimentarios—, los deepfakes se fundamentan en el aprendizaje profundo (deep learning).

El núcleo técnico de este fenómeno reside en las **Redes Adversarias Generativas (GAN)**, donde una red generadora crea contenidos y una red discriminadora actúa como control de calidad, compitiendo hasta alcanzar un equilibrio de indistinguibilidad para el ojo humano[^5]. Este realismo ha permitido que la tecnología trascienda su uso inicial en pornografía no consentida para convertirse en una herramienta de desinformación política, fraude mediante suplantación de identidad (como la "estafa del CEO") y, potencialmente, en una fuente de prueba espuria en procesos judiciales.

2. Marco Normativo Sustantivo: El concepto de documento digital

En el ordenamiento español, el anclaje de la prueba sintética comienza en el Derecho Penal. El **Código Penal**, en su artículo 26, ofrece una definición amplia de documento: «todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria»[^6]. La jurisprudencia ha consolidado una interpretación funcional de este precepto, entendiendo que el soporte papel ha sido superado por las nuevas tecnologías y que los datos electromagnéticos o informáticos poseen plena naturaleza documental[^7].

Bajo esta premisa, la creación de un deepfake con fines espurios puede integrar diversas tipicidades:

- **Falsedad documental:** Al mutar la realidad mediante un soporte que incorpora datos incompatibles con la verdad de los hechos.
- **Delitos contra la intimidad:** Conforme al artículo 197 del Código Penal, cuando se utilizan imágenes manipuladas para vulnerar la privacidad o la integridad moral.
- **Estafa procesal:** El artículo 250.1.7º del Código Penal sanciona a quien, en un proceso judicial, manipula pruebas para inducir a error al juzgador y obtener una resolución favorable en perjuicio de tercero[^8].

3. Marco Normativo Procesal: La prueba electrónica en la LEC y la LECrim

El tratamiento procesal de estas evidencias se divide según el orden jurisdiccional, aunque ambos convergen en la necesidad de autenticación técnica.

- **Proceso Civil:** La **Ley de Enjuiciamiento Civil (LEC)**, en su artículo 299, reconoce como medios de prueba los instrumentos que permitan archivar y reproducir palabras, datos o imágenes. El artículo 382 LEC regula específicamente la admisión de grabaciones de sonido e imagen, permitiendo al tribunal valorarlas conforme a las reglas de la sana crítica. Un punto crítico es el artículo 383 LEC, que exige que estos materiales se presenten junto con una transcripción escrita de su contenido, la cual, no obstante, no sustituye a la fuente de prueba intangible.
- **Proceso Penal:** La **Ley de Enjuiciamiento Criminal (LECrim)** sufrió una reforma estructural mediante la **Ley Orgánica 13/2015**, que introdujo medidas de investigación tecnológica (artículos 588 bis a 588 octies)[^9]. Esta reforma colmó lagunas normativas sobre el registro remoto de equipos, la interceptación de comunicaciones telemáticas y el acceso a dispositivos de almacenamiento masivo. La validez de estas medidas está supeditada a los principios de especialidad, idoneidad, necesidad y proporcionalidad.

4. Estándares Técnicos y Normativa Internacional de Referencia

Dada la fragilidad y facilidad de manipulación de la prueba digital, el marco normativo se complementa con estándares técnicos internacionales que, aunque no poseen rango de ley, son esenciales para la valoración judicial:

- **ISO/IEC 27037:2012:** Establece las directrices para la identificación, recogida, adquisición y preservación de evidencias digitales. Su cumplimiento garantiza la **cadena de custodia**, asegurando que el dato analizado es idéntico al incautado[^10]. La norma define al Digital Evidence First Responder (DEFR) como el encargado de asegurar la trazabilidad del dato desde el momento inicial[^11].
- **Reglamento de Inteligencia Artificial de la UE:** Este marco emergente califica a los sistemas de generación y detección de deepfakes como de **alto riesgo**, imponiendo obligaciones de transparencia y etiquetado para evitar la inducción a error del usuario[^12].
- **Reglamento eIDAS:** El Reglamento (UE) 910/2014 consagra la equivalencia entre el documento electrónico y el físico, prohibiendo que se le nieguen efectos jurídicos por su formato digital[^13].

En este escenario, el marco fáctico revela una brecha entre la capacidad técnica de generación de falsedades y la capacidad procesal de detección, lo que sitúa a la pericia informática como el eje vertebrador de la integridad de la prueba sintética.

III. MARCO TEÓRICO-DOCTRINAL Y CONCEPTOS CLAVE

El análisis jurídico de los deepfakes requiere una cimentación teórica que precise su naturaleza ontológica y los conceptos técnicos que informan su tratamiento procesal. La doctrina contemporánea ha acuñado el término **«prueba sintética»** para referirse a aquel soporte digital generado o alterado mediante inteligencia artificial que presenta una apariencia de autenticidad capaz de inducir a error al observador razonable[^14]. Este apartado desglosa la arquitectura conceptual necesaria para comprender el fenómeno desde el derecho probatorio y penal.

1. Ontología de la prueba sintética: El concepto de deepfake

Etimológicamente, el término deepfake es un acrónimo de deep learning (aprendizaje profundo) y fake (falsedad). Desde una perspectiva normativa, el **Reglamento (UE) 2024/1689** (Ley de IA) define los deepfakes como contenidos de imagen, audio o vídeo generados o manipulados mediante sistemas de IA que guardan un parecido apreciable con personas, objetos o eventos reales, y que presentarían falsamente a una persona como auténticos o verídicos[^15].

Jurisprudencialmente, la prueba sintética se distingue de la evidencia analógica por su **intangibilidad**, **replicabilidad** y **volatilidad**[^16]. Mientras que la prueba tradicional se manifiesta a través de los sentidos de forma directa, el dato sintético es una representación binaria que requiere de una «traducción» informática para ser inteligible por el juzgador. Esta característica impone la distinción fundamental entre:

- **Evidencia digital:** La información o archivo almacenado en un soporte electrónico antes de ser procesado judicialmente.
- **Prueba digital:** El resultado de la evidencia tratada e incorporada al proceso bajo garantías de autenticidad e integridad.

2. Taxonomía de la falsificación: Deepfakes frente a Shallowfakes

Para una correcta calificación jurídica, la doctrina diferencia entre las ultrafalsificaciones y las manipulaciones convencionales o **shallowfakes**[^17]. En estas últimas, no intervienen sistemas de aprendizaje profundo; se trata de ediciones manuales —como la alteración de la velocidad de reproducción, el corte de fotogramas o la descontextualización— realizadas con software de edición estándar.

La diferencia no es solo técnica, sino de eficiencia y realismo. El shallowfake requiere una inversión significativa de tiempo y pericia manual, mientras que el deepfake permite a un usuario sin conocimientos avanzados generar resultados de alta calidad en cuestión de minutos gracias a la automatización algorítmica. Esta capacidad de «democratizar» la falsificación hiperrealista es lo que sitúa a la prueba sintética en un umbral de riesgo superior para la seguridad jurídica.

3. La arquitectura técnica: Redes Adversarias Generativas (GAN)

El núcleo doctrinal del fenómeno reside en las **Redes Adversarias Generativas (GAN)**. Este modelo arquitectónico de la IA se basa en la competencia de dos redes neuronales:

1. **El Generador:** Entrenado para crear datos falsos que incorporen las características del conjunto de entrenamiento.
2. **El Discriminador:** Actúa como un clasificador que intenta distinguir entre los datos reales y los sintéticos.

Este proceso competitivo continúa hasta que el discriminador es incapaz de diferenciar entre lo real y lo artificial, alcanzando el denominado **Equilibrio de Nash**[^18]. Para el derecho probatorio, esto implica que el deepfake no es un mero error de edición, sino un producto diseñado específicamente para eludir el control de calidad, lo que invalida la observación superficial como método de autenticación.

4. Abuso sexual basado en imágenes (IBSA) y derecho a la propia imagen

En el marco teórico penal, la doctrina internacional y la **Directiva (UE) 2024/1385** integran los deepfakes pornográficos bajo el concepto de **Abuso Sexual Basado en Imágenes (IBSA)**[^19]. Se define como la creación o distribución no consentida de imágenes íntimas, subrayando que el daño reside en la violación de la **autonomía sexual** y la dignidad de la víctima, independientemente de si la imagen es una grabación real o una representación sintética.

Desde la vertiente civil, la identidad digital se configura como una extensión del derecho a la propia imagen (art. 18.1 CE), donde la construcción de una narrativa falsa mediante IA atenta contra el derecho del individuo a redefinirse y controlar su representación en el entorno virtual[^20].

IV. ANÁLISIS DETALLADO DEL PROBLEMA JURÍDICO PRINCIPAL

El núcleo de la problemática jurídica que plantean los deepfakes reside en la quiebra de la confianza epistémica sobre la que se asienta el proceso probatorio tradicional. La capacidad de la inteligencia artificial para generar contenidos que superan el umbral de detección sensorial humana sitúa al juzgador ante una paradoja: el mantenimiento del principio de libre valoración de la prueba frente a la insuficiencia de la inmediación física. Este apartado analiza la metamorfosis del concepto de autenticidad, las reglas de distribución de la carga de la prueba tras la impugnación y el riesgo de fraude procesal.

1. La crisis de la inmediación y la suficiencia de la «sana crítica»

El modelo probatorio español se fundamenta en la libre apreciación de la prueba conforme a las reglas de la sana crítica (art. 348 LEC y art. 717 LECrim). Sin embargo, la irrupción de la «prueba sintética» —contenidos multimedia cuya apariencia de veracidad es generada algorítmicamente— impide que la mera observación directa por parte del tribunal constituya una garantía suficiente de autenticidad.

La jurisprudencia reciente, señaladamente la **Sentencia del Tribunal Supremo 692/2023, de 27 de septiembre**[^21], ha subrayado que el juicio crítico del tribunal debe prevalecer, siendo la pericia técnica un instrumento facultativo pero relevante para fundamentar dicho juicio. No obstante, la doctrina advierte que la sofisticación de las

ultrafalsificaciones obliga a poner en duda la capacidad de un juez no asistido técnicamente para detectarlas, lo que podría erosionar la presunción de inocencia (art. 24.2 CE) al inducir error sobre hechos esenciales[^22].

2. La impugnación de la prueba digital y el desplazamiento del onus probandi

Uno de los puntos más críticos en la praxis procesal es la determinación de quién debe probar la autenticidad una vez que se alega la existencia de una manipulación. La **Sentencia del Tribunal Supremo 300/2015, de 19 de mayo**[^23], marcó un hito al establecer que, ante la impugnación de la autenticidad de conversaciones en redes sociales o mensajería instantánea, la carga de la prueba se desplaza hacia quien pretende aprovechar su idoneidad probatoria.

Este desplazamiento del onus probandi exige la práctica de una pericial informática que identifique:

- El verdadero origen de la comunicación.
- La identidad indubitada de los interlocutores.
- La integridad del contenido (ausencia de alteraciones bit a bit).

Dicha carga probatoria ha sido calificada por parte de la doctrina como un requisito de «prueba sobre prueba», donde el proponente debe garantizar la fiabilidad del contenido inmaterial frente a la mera posibilidad de manipulación, la cual «forma parte de la realidad de las cosas»[^24].

3. Autenticidad, integridad y trazabilidad: Los pilares de la cadena de custodia

Para que un archivo digital sea admisible, debe acreditarse su **autenticidad** (que no ha sido alterado desde su captura) y su **integridad** (que es idéntico al original). En este contexto, la **cadena de custodia** digital adquiere una dimensión crítica, pues no basta con asegurar el soporte físico (el hardware), sino que debe demostrarse la integridad lógica de la información.

La jurisprudencia (p. ej., **STS 455/2021**[^25]) establece que cualquier deficiencia en la trazabilidad del dato digital no genera automáticamente la nulidad, pero sí impone al juez una carga argumentativa reforzada para motivar su fiabilidad. El uso de herramientas técnicas como algoritmos hash, sellado de tiempo y firmas electrónicas se vuelve indispensable para construir esta garantía de origen.

4. El riesgo de estafa procesal y falsedad documental

La introducción deliberada de un deepfake en un juicio no es solo un problema de admisibilidad, sino que puede integrar tipos penales graves. La doctrina distingue tres conductas:

- **Manipulación:** Alteración activa del archivo para inducir a error al tribunal.
- **Falsedad documental:** Conforme al artículo 26 del Código Penal, el soporte informático es un documento; su alteración puede constituir falsedad material o ideológica.

- **Estafa procesal:** Recogida en el artículo 250.1.7º CP, se consuma cuando la prueba manipulada induce a una resolución judicial injusta que provoca un perjuicio patrimonial[^26].

Incluso si se dicta sentencia firme basada en una ultrafalsificación, el sistema ofrece el **recurso de revisión** (art. 510 LEC y art. 954 LECrim), permitiendo rescindir resoluciones fundadas en documentos declarados falsos con posterioridad[^27].

V. EVALUACIÓN CRÍTICA: FORTALEZAS, DEBILIDADES, CONTRADICCIONES Y TENSIONES

El análisis de la prueba sintética no puede limitarse a su encaje procedimental; requiere una evaluación crítica de las herramientas técnicas de detección y las tensiones que su aplicación genera en el núcleo de las garantías procesales. La literatura científica y los informes de organismos de seguridad revelan una "carrera armamentista" tecnológica donde la eficacia de la detección se ve constantemente desafiada por la evolución de las Redes Adversarias Generativas (GAN).

1. Fortalezas y debilidades de las herramientas de detección técnica

La vanguardia en detección se divide actualmente en dos grandes enfoques, cada uno con fortalezas específicas y vulnerabilidades críticas:

- **Detección basada en artefactos y aprendizaje profundo:** El uso de Vision Transformers (ViT) ha demostrado una precisión superior (hasta el 96%) en comparación con las Redes Neuronales Convolucionales (CNN) tradicionales[^28]. Su fortaleza radica en la capacidad de capturar relaciones espaciales globales y dependencias de largo alcance en la imagen, detectando inconsistencias sutiles que las CNN, centradas en patrones locales, suelen obviar. No obstante, su debilidad principal es el **elevado costo computacional** y el riesgo de **sobreajuste** (overfitting), lo que limita su escalabilidad en laboratorios forenses con recursos limitados.
- **Análisis de señales biológicas (PPG):** Una de las fortalezas más robustas es la extracción de señales de fotopletismografía remota (rPPG)[^29]. Esta técnica detecta las variaciones imperceptibles en el color de la piel causadas por el flujo sanguíneo. Dado que las GAN suelen generar imágenes fotograma a fotograma, a menudo no logran replicar la coherencia temporal de los latidos cardíacos, creando una "huella biológica" de falsedad. Sin embargo, esta técnica es altamente sensible a la **compresión de vídeo** y a las condiciones de iluminación, lo que puede generar falsos negativos en pruebas obtenidas de fuentes de baja calidad como redes sociales.
- **Fragilidad de los metadatos y ELA:** El Análisis de Nivel de Error (ELA) permite identificar inconsistencias en la compresión JPEG. Es una herramienta rápida pero limitada: su debilidad estructural reside en que los metadatos son **fácilmente eliminables** mediante capturas de pantalla o procesos de resalvado, lo que los convierte en una prueba de integridad frágil en entornos hostiles[^30].

2. La carrera armamentista: El bucle de retroalimentación de las GAN

Una debilidad sistémica identificada es el funcionamiento intrínseco de las GAN. El modelo discriminador de una GAN actúa, de facto, como un detector. Cuando los

investigadores publican nuevas técnicas de detección (como el parpadeo ausente o reflejos oculares inconsistentes), los desarrolladores de IA integran estos criterios en el entrenamiento de nuevos modelos. Esto crea un ciclo donde el éxito de la detección impulsa la perfección de la falsificación, alcanzando un **Equilibrio de Nash** donde el fraude se vuelve indistinguible incluso para algoritmos avanzados[^31].

3. Tensiones procesales: La erosión de la inmediación y la prueba ilícita

La introducción de estas herramientas genera tres tensiones jurídicas fundamentales:

1. **Inmediación vs. Pericia:** Existe una contradicción entre la jurisprudencia que insiste en la autonomía del juez para valorar la prueba conforme a la "sana crítica" (STS 692/2023) y la realidad técnica que demuestra que el ojo humano es incapaz de detectar ultrafalsificaciones sofisticadas. La tensión radica en si la pericia técnica debe dejar de ser un auxilio facultativo para convertirse en un **presupuesto de admisibilidad**[^32].
2. **Derecho a la no autoincriminación:** Surge una tensión crítica cuando se requiere que un investigado proporcione muestras de su voz o imagen para realizar un cotejo con un posible deepfake. La negativa a colaborar está amparada por el derecho a no declarar contra sí mismo (art. 24.2 CE), lo que puede dejar al tribunal en una situación de **indefensión epistémica** ante la imposibilidad de verificar la autenticidad de la prueba[^33].
3. **Construcción paralela e integridad:** El informe de Europol advierte sobre el riesgo de "limpiar" pruebas obtenidas de forma ilícita mediante la creación de narrativas alternativas, fenómeno conocido como **construcción paralela** (parallel construction)[^34]. Esto genera una tensión entre la eficacia en la persecución del ciberdelito y el respeto al derecho de defensa, ya que la opacidad del algoritmo puede ocultar vulneraciones de derechos fundamentales en la fase de obtención.

VI. ANÁLISIS COMPARADO: PRECEDENTES, DERECHO COMPARADO Y EVOLUCIÓN NORMATIVA

El tratamiento jurídico de las representaciones sintéticas revela una respuesta global asimétrica, caracterizada por la transición de marcos analógicos hacia normativas específicas que intentan capturar la sofisticación de la IA. Mientras que algunos sistemas optan por adaptar tipos penales clásicos (honor, intimidad, falsedad), otros, liderados por la Unión Europea, han iniciado un proceso de armonización que tipifica de forma autónoma el abuso de imágenes basadas en IA.

1. El Sistema Europeo: Hacia la armonización del Abuso Sexual Basado en Imágenes (IBSA)

La Unión Europea se sitúa a la vanguardia normativa con un enfoque dual que combina la regulación técnica (Reglamento de IA) y la penal (Directivas de género).

- **Directiva (UE) 2024/1385:** Representa un hito al obligar a los Estados miembros a criminalizar el intercambio no consentido de material íntimo o manipulado[^35]. El artículo 5 de esta Directiva exige sancionar la producción, alteración y posterior difusión pública de contenidos que simulen actividades sexuales de otra persona sin su

consentimiento. Es relevante destacar que la Directiva no exige que el daño se materialice, sino que la conducta sea «idónea» para causar un perjuicio grave.

- **El Modelo de Benelux (Bélgica y Países Bajos):** Estos países han evolucionado desde el concepto de «porno de venganza» hacia el de Abuso Sexual Basado en Imágenes (IBSA)[^36]. En los Países Bajos, el artículo 254ba del Código Penal (DCC) criminaliza tanto la producción como la posesión y distribución de imágenes sexuales no consentidas, incluyendo expresamente las ultrafalsificaciones. Por su parte, la jurisprudencia belga ha extendido el tipo penal del **voyeurismo** para cubrir la creación de deepfakes de personas reales, argumentando que se vulnera la integridad sexual independientemente de la autenticidad de la grabación[^37].

2. Divergencias en la Tradición Continental: Alemania y Turquía

El análisis comparado entre Alemania y Turquía permite observar cómo la falta de una norma específica genera lagunas de impunidad o aplicaciones fragmentadas:

- **Alemania (StGB):** El sistema alemán intenta aprehender los deepfakes a través de la protección del honor (§ 185 et seq. StGB) y el acoso o stalking (§ 238 StGB), reformado en 2021 para incluir el ciberacoso mediante imágenes. No obstante, la doctrina advierte que el bien jurídico protegido —el honor— no refleja adecuadamente la injusticia del deepfake sexual, que atenta contra la **autodeterminación sexual**[^38].
- **Turquía (TCK):** La legislación turca se centra en la protección de la moral pública (§ 226 TCK) y los datos personales (§ 136 TCK). Sin embargo, si la víctima es adulta y la imagen no es estrictamente privada (por haber sido capturada de redes sociales públicas), el artículo 134 sobre violación de la intimidad resulta a menudo inaplicable, dejando un vacío que la propuesta del nuevo artículo 105/A pretende colmar tipificando específicamente la creación y difusión de deepfakes[^39].

3. El Modelo de Common Law**: Estados Unidos y la Teoría del «Testigo Silencioso»**

En los Estados Unidos, el desafío se ha centrado en la admisibilidad procesal más que en la tipificación penal federal sustantiva, condicionada por la Primera Enmienda.

- **La Teoría del Testigo Silencioso (**Silent Witness Theory**):** Esta doctrina permite que una imagen o vídeo hable por sí mismo y sea admitido como prueba sin necesidad de un testigo que verifique su exactitud, siempre que se demuestre la fiabilidad del proceso de obtención[^40]. Esta presunción de fiabilidad se ve hoy amenazada por las GAN, que operan precisamente para engañar al sistema.
- **Reglas Federales de Evidencia (FRE):** Las enmiendas de 2017 a las reglas FRE 902(13) y 902(14) introdujeron la **autenticación automática** (self-authentication) para registros digitales certificados por una persona cualificada. Esto permite introducir datos de GPS o mensajes sin testigos presenciales, una facilidad procesal que los perpetradores de deepfakes pueden explotar si no se exige una pericia técnica que desvirtúe la apariencia de veracidad[^41].

4. Evolución Histórica: Del montaje analógico al «Equilibrio de Nash»

Históricamente, el derecho probatorio ha lidiado con la falsificación documental desde el siglo XIX. Sin embargo, la evolución técnica muestra un salto cualitativo:

1. **Era Analógica/Digital Temprana (**Shallowfakes**):** Manipulaciones manuales (edición de negativos, Photoshop) que dejan rastros perceptibles o artefactos de compresión JPEG detectables mediante análisis de nivel de error (ELA).
2. **Era de la IA Generativa (**Deepfakes**):** Uso de GANs que alcanzan el **Equilibrio de Nash**, donde el fraude es indistinguible para el ojo humano y para detectores algorítmicos estándar, obligando al derecho a desplazarse desde la confianza en la percepción sensorial hacia la confianza en la trazabilidad bit a bit (ISO/IEC 27037)[^42].

VII. IMPLICACIONES SISTÉMICAS Y PARA LA PRÁCTICA JURÍDICA / POLÍTICA PÚBLICA

La propagación de la prueba sintética no constituye meramente un reto técnico-procesal, sino una amenaza estructural que impacta en los pilares de la seguridad nacional, la confianza en las instituciones y la integridad del Estado de Derecho. La transición hacia una «era de la digitalización» ha convertido a los deepfakes en instrumentos de desestabilización que trascienden el proceso penal para afectar la cohesión social y el funcionamiento de la democracia.

1. La erosión de la confianza institucional y la «apocalipsis de la información»

El primer impacto sistémico identificado por organismos como Europol es la quiebra de la confianza pública en los contenidos audiovisuales, fenómeno denominado como «apocalipsis de la información» o «apatía de la realidad»[^43]. En un entorno donde la percepción humana ya no es un guía fiable, se produce una erosión de la autoridad de los hechos oficiales. Para la práctica jurídica, esto implica que la máxima «ver para creer» ha muerto, obligando a los tribunales a operar bajo una presunción de duda sistemática sobre cualquier evidencia digital.

Esta pérdida de confianza se proyecta también sobre las fuerzas de seguridad. El uso de ultrafalsificaciones para retratar falsamente a agentes cometiendo transgresiones puede ser utilizado para desacreditar a la policía, incitar a la violencia y manipular la opinión pública, especialmente cuando se combina con prácticas de doxxing.

2. Riesgos para la integridad del sistema penal: condenas erróneas e impunidad

La admisión de pruebas sintéticas sin protocolos de validación rigurosos plantea consecuencias devastadoras para la administración de justicia:

- **Errores judiciales graves:** Un deepfake hiperrealista puede incriminar a un inocente colocándolo en la escena de un crimen o fabricando una confesión falsa. Esto daña irreversiblemente la vida de los implicados y socava la legitimidad del sistema penal.
- **Ambiente de impunidad:** Recíprocamente, la facilidad con la que se alega una manipulación digital puede ser explotada por criminales reales para impugnar pruebas legítimas, generando una «defensa deepfake» que dificulta la obtención de condenas[^44].
- **Desigualdad de armas:** La capacidad de detectar o producir pruebas sintéticas depende de recursos tecnológicos y periciales costosos. Esto genera una brecha entre las partes, donde la justicia podría basarse en la capacidad de manipular o verificar tecnología y no en la verdad material de los hechos.

3. El peligro de la «construcción paralela» y la opacidad algorítmica

Una implicación sistémica crítica es el riesgo de la **construcción paralela** (parallel construction)[^45]. Esta práctica consiste en la creación de una narrativa alternativa para ocultar el origen real —y potencialmente ilícito— de una prueba obtenida mediante tecnologías avanzadas de vigilancia o inteligencia.

La falta de regulación específica en este ámbito permite que pruebas que vulneran derechos fundamentales sean «blanqueadas» mediante una explicación ficticia sobre su origen, lo que mina el principio de transparencia y el derecho a un proceso con todas las garantías. La opacidad de los algoritmos de detección, a menudo protegidos por secretos comerciales, añade una capa de indefensión para la defensa, que no puede controvertir eficazmente los sesgos o errores del sistema detector[^46].

4. Impacto en la operatividad y gestión del sistema judicial

Desde una perspectiva de política pública, el sistema de justicia digital se enfrenta a un incremento insostenible de la carga de trabajo. La necesidad de peritajes informáticos para cada archivo digital impugnado choca con el principio de economía procesal.

- **Costes y Tiempos:** Un informe pericial forense es oneroso y requiere tiempos que dilatan indebidamente los procesos, amenazando el derecho a un proceso sin dilaciones indebidas.
- **Necesidad de Capacitación:** Existe una brecha formativa alarmante entre los operadores jurídicos[^47]. La práctica actual delega de facto la valoración de la prueba en los peritos informáticos, desplazando la función jurisdiccional hacia profesionales técnicos que carecen de las garantías jurídicas del juez.

En conclusión, el impacto de las pruebas sintéticas exige una respuesta coordinada que no se limite a la técnica forense, sino que incluya una reforma de los marcos de transparencia algorítmica y un refuerzo de la integridad de la cadena de custodia digital como pilar de la confianza ciudadana en la justicia.

VIII. PROPUESTAS NORMATIVAS, INTERPRETATIVAS O DE LEGE FERENDA

La insuficiencia del marco procesal y sustantivo actual frente a la sofisticación de la prueba sintética exige una respuesta holística que trascienda la mera aplicación analógica de normas decimonónicas. Las propuestas que se articulan a continuación buscan armonizar la eficacia en la persecución del ilícito digital con la salvaguarda de las garantías constitucionales, desplazando el eje de la convicción judicial desde la percepción sensorial hacia la verificación técnica certificada.

1. Eje Procesal: Hacia un modelo de verificación técnica obligatoria

El sistema de libre valoración de la prueba, fundamentado en la sana crítica, resulta inoperante cuando el objeto de valoración es indistinguible de la realidad para el ojo humano. Por ello, se proponen las siguientes reformas:

- **Institucionalización de la Pericia Informática Judicial:** Es imperativa la incorporación de peritos informáticos adscritos de manera permanente a los juzgados.

Estos especialistas deben actuar como auxiliares jurisdiccionales encargados de realizar un triaje técnico inicial de cualquier evidencia audiovisual impugnada, garantizando que el tribunal cuente con una base científica antes de formar su convicción[^48].

- **Reforma de las normas de admisión (LEC y LECrim):** Se propone que, ante la impugnación razonable de la autenticidad de un archivo digital, la carga de la prueba no solo se desplace al proponente (conforme a la STS 300/2015), sino que la práctica de una pericial técnica sea un requisito previo de admisibilidad para que el archivo sea valorado como prueba documental.
- **Protocolo Unificado de Validación de Pruebas Digitales:** El sistema judicial debe adoptar un protocolo obligatorio basado en estándares internacionales, específicamente la norma **ISO/IEC 27037:2012**. Este protocolo debe exigir el análisis forense de metadatos y la verificación de la integridad bit a bit mediante algoritmos hash desde el momento de la incautación[^49].

2. Eje Penal: Tipificación autónoma y protección de la integridad digital

La fragmentación de los tipos penales actuales (honor, intimidad, falsedad) deja lagunas de impunidad en los casos de representaciones sintéticas que no encajan en el concepto tradicional de "grabación real".

- **Creación del delito de Abuso de Imágenes Basado en IA:** Siguiendo el modelo de la **Directiva (UE) 2024/1385**, se propone tipificar como delito autónomo la producción, alteración y difusión no consentida de contenidos sintéticos que simulen actividades de naturaleza sexual. El injusto debe centrarse en la violación de la **autonomía sexual** y no meramente en el daño al honor[^50].
- **Ampliación de la Estafa Procesal:** Se propone una reforma del artículo 250.1.7º CP para incluir expresamente el uso de tecnologías de inteligencia artificial generativa como un medio de "engaño bastante" cualificado para inducir a error al juzgador.
- **Criminalización de la Posesión de Herramientas de Falsificación:** Al igual que en los delitos de intrusión informática, se debe considerar la penalización de la posesión intencional de software diseñado específicamente para la creación de deepfakes con fines delictivos, siempre que se acredite la intención de causar daño a terceros[^51].

3. Eje Institucional y Tecnológico: Transparencia y Gobernanza

- **Registro Nacional de Pruebas Audiovisuales Verificadas:** Se propone la creación de una base de datos centralizada donde se almacenen las evidencias digitales que hayan superado un proceso de autenticación forense. Esto evitaría la duplicidad de peritajes y facilitaría el contraste en investigaciones transfronterizas o complejas.
- **Implementación del Etiquetado de IA (Watermarking):** En línea con el Reglamento de IA de la UE, se debe exigir a los proveedores de sistemas de IA que implementen marcas de agua digitales imperceptibles y metadatos C2PA que permitan rastrear el origen sintético del contenido[^52]. La ausencia de este etiquetado en archivos generados artificialmente debería operar como una presunción iuris tantum de manipulación maliciosa en el proceso judicial.
- **Plan de Capacitación Transversal:** Es urgente la formación obligatoria de jueces, fiscales y abogados en el manejo de evidencias tecnológicas y la detección de sesgos

algorítmicos. La justicia digital no puede depender de una fe ciega en el experto informático, sino de una comprensión crítica de las limitaciones de la técnica[^53].

IX. CONCLUSIONES

La investigación desarrollada permite concluir que el sistema de justicia se enfrenta a una **metamorfosis estructural del concepto de prueba** provocada por la democratización de la inteligencia artificial generativa. La transición de la evidencia analógica a la «prueba sintética» no representa un cambio meramente formal, sino la ruptura de la confianza epistémica que ha sustentado el proceso judicial durante siglos. El axioma de la inmediación sensorial, fundamentado en la capacidad del juzgador para discernir la verdad mediante la observación directa, ha devenido en una ficción jurídica ante la sofisticación de las **Redes Adversarias Generativas (GAN)**.

En primer lugar, se constata que las representaciones sintéticas han alcanzado un **equilibrio de Nash** donde el fraude es indistinguible para el ojo humano y para los detectores algorítmicos convencionales[^54]. Esta realidad técnica invalida la suficiencia de la «sana crítica» aplicada de forma aislada. La jurisprudencia, señaladamente la **STS 692/2023**, si bien insiste en la autonomía del tribunal, reconoce implícitamente que la pericia informática ya no es un auxilio facultativo, sino un presupuesto de fiabilidad ante la impugnación de la integridad del dato digital.

En segundo lugar, la eficacia del sistema penal frente a la **estafa procesal** y la falsedad documental depende hoy de la estandarización de los protocolos forenses. El cumplimiento de la norma **ISO/IEC 27037:2012** se erige como la única garantía de trazabilidad bit a bit, asegurando que la evidencia digital no ha sido contaminada desde su incautación. La adopción de este estándar no solo reduce los tiempos de trabajo y mejora la extracción de datos, sino que blinda el proceso frente a la «defensa deepfake», impidiendo que los infractores utilicen la duda tecnológica como una patente de impunidad.

En tercer lugar, el marco normativo europeo —liderado por el **Reglamento de IA** y la **Directiva 2024/1385**— marca el camino hacia una tipificación autónoma del **Abuso Sexual Basado en Imágenes (IBSA)**. La protección de la autonomía sexual y del entorno virtual propio debe prevalecer sobre la veracidad material del contenido; el daño a la dignidad de la víctima se consuma con la creación de la representación sintética no consentida, independientemente de si el observador sabe que la imagen es artificial.

Finalmente, este artículo sostiene que la respuesta institucional ante el «apocalipsis de la información» no debe ser el repliegue analógico, sino la **tecnificación garantista**. El riesgo de la **construcción paralela** y la opacidad de los algoritmos de detección exigen un compromiso con la transparencia algorítmica y la formación transversal de los operadores jurídicos. La integridad del Estado de Derecho en la era de la digitalización no se preserva prohibiendo la técnica, sino sometiéndola al control jurisdiccional estricto y a una cadena de custodia inexpugnable, garantizando que la justicia siga siendo una búsqueda de la verdad y no una validación de simulacros.

X. BIBLIOGRAFÍA Y REFERENCIAS CITADAS

1. Organismos Internacionales e Institucionales

- EUROPOL (2022/2024). Facing reality? Law enforcement and the challenge of deepfakes, Observatory Report from the Europol Innovation Lab. Publications Office of the European Union, Luxemburgo.
- EUROPOL (2025). European Union Serious and Organised Crime Threat Assessment (EU-SOCTA) – The changing DNA of serious and organised crime. Publications Office of the European Union, Luxemburgo.
- National Institute of Standards and Technology (NIST) (2020/2021). 2018 Media Forensics Challenges (MFC18): Summary and Results. NISTIR 8324.
- National Institute of Standards and Technology (NIST) (2006). Guide to Integrating Forensic Techniques into Incident Response. Special Publication 800-86.
- Unión Europea (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de IA)*, DO L, 12 de julio de 2024.
- Unión Europea (2024). *Directiva (UE) 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*, de 15 de mayo de 2024, DO L, 2024.

2. Monografías y Artículos Académicos

- ALDAY LÓPEZ-CABELLO, F. (2025). Tratamiento procesal de las pruebas electrónicas en el proceso penal español. Colección Estudios Procesales Nº 1, Editorial Colex, A Coruña.
- ALTUNCU, E., FRANQUEIRA, V. N. L., & LI, S. (2024). «Deepfake: definitions, performance metrics and standards, datasets, and a meta-review». Frontiers in Big Data, Vol. 7.
- BLÁZQUEZ MORENO, R. (2023). «Deepfakes en el procedimiento probatorio». Revista Vasca de Derecho Procesal y Arbitraje, III Edición Premios IVADP.
- CELEBI, N., LIU, Q., & KARATOPRAK, M. (2022). «A Survey of Deep Fake Detection for Trial Courts». Computer Science & Information Technology (CS & IT), pp. 227-238.
- EISELE, J., & DUMAN, I. (2025). «Criminal Liability of Deepfake Pornography under Turkish and German Criminal Law». Zeitschrift für Internationale Strafrechtswissenschaft (ZfIStw), 1/2025.
- FARFAN CHIUN, J. E. (2024). ISO 27037:2012 para mejorar el análisis informático forense en la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú. Tesis de Maestría, Universidad Nacional Federico Villarreal, Lima.
- MARTÍNEZ GALINDO, G. (2022). «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales». Revista Electrónica de Ciencia Penal y Criminología (RECPC), 24-23, pp. 1-38.
- ROYER, S., OERLEMANS, J. J., & VAN WEGBERG, R. (2024). «An empirical and legal analysis of sexual deepfakes in the EU, Belgium and the Netherlands». Revue Internationale de Droit Pénal, pp. 459-482.

3. Informes Técnicos y Literatura de Especialidad (arXiv / Forense)

● Forvis Mazars España (2025). «La Inteligencia Artificial y el Riesgo de Pruebas Digitales Falsas en el Sistema Judicial: Análisis y Propuestas de Reforma». Creando soluciones de valor, 28/01/2025.
● GOYAL, H., et al. (2025). «State-of-the-art AI-based Learning Approaches for Deepfake Generation and Detection». arXiv:2501.01029.
● MUJAWAR, S., et al. (2025). «Exploring AI/ML Techniques for Deepfake Detection: A Comprehensive Review». International Journal on Science and Technology (IJSAT), Vol. 16, Issue 2.
● NGUYEN, H. H., et al. (2024). «Vision Transformers need registers for Deepfake Detection». arXiv:2405.00355v2.
● YANG, J., et al. (2022/2024). «Exposing Deepfake with Pixel-wise Autoregressive and PPG Correlation from Faint Signals». arXiv.

4. Jurisprudencia Citada

● Tribunal Supremo (Sala Segunda): STS 300/2015, de 19 de mayo; STS 492/2016, de 8 de junio; STS 287/2017, de 19 de abril; STS 507/2020, de 14 de octubre; STS 455/2021, de 19 de mayo; STS 205/2022, de 2 de marzo; STS 692/2023, de 27 de septiembre.
● Tribunal Supremo (Sala Cuarta): STS 2925/2020, de 23 de julio.
● Tribunal Constitucional: STC 190/1992, de 16 de noviembre; STC 170/2003, de 29 de septiembre; STC 145/2014, de 11 de septiembre; STC 172/2020, de 19 de noviembre.
● Jurisprudencia Comparada: Rb. Amsterdam, ECLI:NL:RBAMS:2023:6923; United States v. Miller, 425 US 435 (1976); Katz v. United States, 389 US 347 (1967); Barbulescu v. Rumanía, TEDH, 2017.

5. Estándares Técnicos

● ISO/IEC 27037:2012: Directrices para la identificación, recogida, adquisición y preservación de evidencias digitales.
● UNE 71506:2013: Metodología para el análisis forense de las evidencias electrónicas.

NOTAS AL PIE

[^1]: El término *deepfake* es un acrónimo de *deep learning* y *fake*. Sobre las Redes Adversarias Generativas (GAN), véase GOODFELLOW, Ian et al., "Generative Adversarial Networks", *arXiv:1406.2661*, 2014.
[^2]: GOODFELLOW, op. cit.
[^3]: ISO/IEC 27037:2012, *Directrices para la identificación, recogida, adquisición y preservación de evidencias digitales*.
[^4]: Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 15 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, DO L, 2024.
[^5]: AHIRWAR, *Generative Adversarial Networks Projects*, 2018; ROYER et al., "An empirical and legal analysis of sexual deepfakes in the EU, Belgium and the Netherlands", *Revue Internationale de Droit Pénal*, 2024, pp. 459-482.
[^6]: Artículo 26 del Código Penal español.

[^7]: STS 507/2020, de 14 de octubre (caso Gürtel).
[^8]: Artículo 250.1.7º del Código Penal.
[^9]: Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.
[^10]: ISO/IEC 27037:2012.
[^11]: Ibid.
[^12]: Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de IA), DO L, 12 de julio de 2024, considerando 38.
[^13]: Reglamento (UE) n.º 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 (eIDAS), art. 46.
[^14]: BLÁZQUEZ MORENO, R., "Deepfakes en el procedimiento probatorio", *Revista Vasca de Derecho Procesal y Arbitraje*, 2023.
[^15]: Reglamento (UE) 2024/1689, art. 3(1) y considerando 50.
[^16]: MARTÍNEZ GALINDO, G., "Problemática jurídica de la prueba digital y sus implicaciones en los principios penales", *RECPC*, 24-23, 2022, pp. 1-38.
[^17]: KOCSIS, 2021; HODGE, 2021, citados en ROYER et al., op. cit.
[^18]: GOODFELLOW et al., op. cit.; AHIRWAR, op. cit.
[^19]: MCGLYNN/RACKLEY, "Image-Based Sexual Abuse", 2017; ROYER et al., op. cit.
[^20]: STS 287/2017, de 19 de abril, sobre el derecho al entorno virtual propio.
[^21]: STS 692/2023, de 27 de septiembre.
[^22]: Véase MARTÍNEZ GALINDO, op. cit.
[^23]: STS 300/2015, de 19 de mayo.
[^24]: ALDAY LÓPEZ-CABELLO, F., *Tratamiento procesal de las pruebas electrónicas*, 2025, p. 123.
[^25]: STS 455/2021, de 19 de mayo.
[^26]: Sobre la estafa procesal, véase STS 205/2022, de 2 de marzo.
[^27]: Arts. 510 LEC y 954 LECrim.
[^28]: NGUYEN, H. H. et al., "Vision Transformers need registers for Deepfake Detection", *arXiv:2405.00355v2*, 2024.
[^29]: CIFTCI et al., 2020; MAO/YANG, 2022, citados en YANG, J. et al., "Exposing Deepfake with Pixel-wise Autoregressive and PPG Correlation", *arXiv*, 2024.
[^30]: NIST, *Guide to Integrating Forensic Techniques into Incident Response*, 2006.
[^31]: Reglamento de IA, considerando 38.
[^32]: STS 692/2023.
[^33]: STC 172/2020, de 19 de noviembre.
[^34]: EUROPOL, *Facing reality?*, 2024, p. 15.
[^35]: Directiva (UE) 2024/1385, art. 5.
[^36]: ROYER et al., op. cit.
[^37]: Rb. Amsterdam, ECLI:NL:RBAMS:2023:6923.
[^38]: EISELE & DUMAN, "Criminal Liability of Deepfake Pornography under Turkish and German Criminal Law", *ZfIStw*, 2025.
[^39]: Ibid.

[^40]: CELEBI et al., "A Survey of Deep Fake Detection for Trial Courts", 2022.
[^41]: FRE 902(13) y (14).
[^42]: ISO/IEC 27037:2012.
[^43]: EUROPOL, *EU-SOCTA*, 2025.
[^44]: Forvis Mazars España, "La Inteligencia Artificial y el Riesgo de Pruebas Digitales Falsas", 2025.
[^45]: EUROPOL, *Facing reality?*, 2024.
[^46]: Véase STC 145/2014, de 11 de septiembre, sobre transparencia.
[^47]: ALDAY, op. cit.
[^48]: FARFAN CHIUN, *ISO 27037:2012 para mejorar el análisis informático forense*, 2024.
[^49]: ISO/IEC 27037:2012.
[^50]: Directiva 2024/1385, considerando 19.
[^51]: Propuesta inspirada en el § 105/A TCK turco, según EISELE & DUMAN.
[^52]: Reglamento de IA, art. 50.
[^53]: MARTÍNEZ GALINDO, op. cit.
[^54]: GOODFELLOW et al., op. cit.