Revista Iberoamericana de la Propiedad Intelectual
Cultura digital e inteligencia artificial: retos para la propiedad intelectual en Iberoamérica
Número especial (2026): 445-498

Deepfakes, derecho de imagen y derecho de autor: desafíos jurídicos para artistas e intérpretes ante la inteligencia artificial generativa

* * * *

Lucas Lehtinen[1]
Universidad Austral (Argentina)
lucaslehtinen@gmail.com
https://orcid.org/0000-0003-4771-3238

Recibido: 31 de enero de 2026
Aceptado: 20 de abril de 2026
https://doi.org/10.26422/RIPI.2026.espIA.leh

Resumen
El artículo examina los desafíos jurídicos que plantean los *deepfakes* y la clonación digital para artistas e intérpretes en el contexto de la inteligencia artificial generativa. Se demuestra que el régimen tradicional de derechos de autor y derechos de imagen resulta insuficiente para gobernar réplicas digitales que capturan la esencia performativa del intérprete. Se analizan cuatro familias tecnológicas —texto-a-video, clonación de voz, reanimación facial y transferencia de movimiento— y la fragmentación normativa que obliga a invocar simultáneamente múltiples líneas de protección, generando incertidumbre y asimetrías de poder.
Se desarrollan tres ejes: arquitectura contractual modular para licencias de clones digitales con remedios operativos, visibilidad algorítmica y desplazamiento de *performers* por contenido sintético y gobernanza del legado *post mortem* centrada en regular *inputs* antes que *outputs*. Se examinan desarrollos legislativos recientes

1 Abogado (Universidad Nacional de Córdoba). Maestría en Administración de Empresas (MBA) (Escuela de Graduados de Ciencias Económicas) y en Propiedad Intelectual (Universidad Austral). Se desempeña como director de la Maestría en Propiedad Intelectual y Nuevas Tecnologías (Universidad Austral) y es fundador de la consultora Argeopolis y Líder Global de Educación en GLIPA.

(ELVIS Act, NY § 50-f, California § 3344, propuesta danesa) que convergen en reconocer la "réplica digital" como categoría autónoma y se analiza el "dividendo del mentiroso" en el plano probatorio. Se concluye que la identidad performativa migra hacia un esquema de propiedad intelectual especializada que requiere reconceptualización jurídica profunda, balanceando protección con libertad de expresión y derecho a la información.

Palabras clave: *deepfakes*, clones digitales, inteligencia artificial generativa, derechos de autor, derecho de imagen, *right of publicity*, artistas e intérpretes, gobernanza algorítmica, legado digital *post mortem*, prueba de consentimiento.

Deepfakes, Image Rights and Copyright: Legal Challenges for Artists and Performers in the Age of Generative Artificial Intelligence

Abstract
This article examines the legal challenges posed by deepfake technologies and digital cloning for artists and performers in the context of generative AI. It demonstrates that the traditional copyright and image rights regime is insufficient to govern digital replicas that capture the performative essence of the interpreter. Four technological families are addressed —text-to-video, voice cloning, facial reenactment, and body motion transfer— alongside the normative fragmentation that forces artists to simultaneously invoke multiple protection lines, generating legal uncertainty and power asymmetries.
Three axes are developed: modular contractual architecture for digital clone licenses with operational remedies; algorithmic visibility and performer displacement through synthetic content; and post-mortem digital legacy governance focused on regulating inputs rather than outputs. Recent legislative developments (ELVIS Act, NY § 50-f, California § 3344, Danish proposal) converging in recognizing "digital replica" as an autonomous category are examined, as is the "liar's dividend" on the evidentiary level. It concludes that performative identity is migrating toward a specialized intellectual property scheme requiring profound legal reconceptualization that balances performer protection with freedom of expression and the right to information.

Key words: deepfakes, digital clones, generative artificial intelligence, copyright, image rights, right of publicity, artists and performers, algorithmic governance, post-mortem digital legacy, proof of consent.

Deepfakes, direito de imagem e direito autoral: desafios jurídicos para artistas e intérpretes diante da inteligência artificial generativa

Resumo
O artigo examina os desafios jurídicos colocados pelos deepfakes e a clonagem digital para artistas e intérpretes no contexto da IA generativa. Demonstra-se que o regime tradicional de direitos autorais e de imagem é insuficiente para governar réplicas digitais que capturam a essência performativa do intérprete. Abordam-se quatro famílias tecnológicas —texto-para-vídeo, clonagem de voz, reanimação facial e transferência de movimento— e a fragmentação normativa que obriga a invocar simultaneamente múltiplas linhas de proteção, gerando incerteza e assimetrias de poder.
Desenvolvem-se três eixos: arquitetura contratual modular para licenças de clones digitais com remédios operacionais; visibilidade algorítmica e deslocamento de performers por conteúdo sintético; e governança do legado post-mortem centrada em regular inputs antes que outputs. Examinam-se desenvolvimentos legislativos recentes (ELVIS Act, NY § 50-f, California § 3344, proposta dinamarquesa) que convergem no reconhecimento da "réplica digital" como categoria autônoma, e analisa-se o "dividendo do mentiroso" no plano probatório. Conclui-se que a identidade performativa migra para um esquema de propriedade intelectual especializada que exige reconceituação jurídica profunda, equilibrando proteção com liberdade de expressão e direito à informação.

Palavras-chave: deepfakes, clones digitais, inteligência artificial generativa, direitos autorais, direito de imagem, right of publicity, artistas e intérpretes, governança algorítmica, legado digital post-mortem, prova de consentimento.

1. Introducción: cuando la persona deja de ser necesaria

Hubo un momento —no hace tanto— en que reproducir la voz de un artista requería que ese artista se sentara frente a un micrófono. Copiar su imagen exigía una cámara apuntando hacia él. Esa cadena causal —persona real, obra real— es la que los sistemas jurídicos aprendieron a proteger durante décadas. Esa cadena se ha roto.

Hoy, los modelos generativos sintetizan rostro, voz y movimiento a partir de datos disponibles, sin que la persona participe, consienta ni sepa que existe una réplica de ella. El resultado no es una "copia" en el sentido en que el derecho conocía, es un clon digital que circula a escala global con costos cercanos a cero. Como señalaron Chesney y Citron (2019), la amenaza más insidiosa no es la fabricación de contenido falso, sino la erosión de la confiabilidad de todo contenido. Es la sustitución funcional de la persona en el mercado cultural.

Este desplazamiento expone los límites de los marcos vigentes. El Tratado de Beijing robusteció la tutela del intérprete en el entorno digital, pero sus categorías siguen ancladas en la existencia previa de una fijación real —reproducción, distribución, puesta a disposición— que no capturan la lógica de una síntesis generada por IA (Von Lewinski, 2013). Para defenderse, el artista debe activar simultáneamente líneas heterogéneas de protección —derechos conexos, imagen, datos biométricos, competencia desleal—, cada una con sus requisitos y foros, con costos enormes y asimetrías que se agravan cuando la explotación es transnacional. A eso se suma una tensión que la generación sintética exacerba: la distinción entre autoría y *performance*. En la tradición de derechos conexos, el intérprete se protege incluso cuando su contribución no alcanza obra autoral; pero cuando una IA produce algo indistinguible de una *performance* humana, la pregunta por el estatuto jurídico de la *performance* deja de ser académica (Gervais, 2015).

Este artículo sostiene que el problema no se resuelve con un único derecho rector, sino con una arquitectura de gobernanza que combine: un mapa de solapamiento de los derechos que inciden sobre una réplica digital; gestión contractual granular mediante licencias de clon que regulen objeto, usos, trazabilidad y revocación; estándares probatorios y tecnológicos —*proof of personality*, *proof of consent*— para reducir disputas *ex post*; y un análisis realista del *en-*

forcement, donde los términos de las plataformas funcionan como derecho operativo que puede tanto proteger al intérprete como profundizar su exclusión. Se propone así un marco para entender cómo la identidad performativa migra, de manera irreversible, hacia un esquema híbrido entre propiedad intelectual, derechos de personalidad y protección de datos, con implicancias también para la gestión del legado post mortem.

La tesis central que articula el presente trabajo puede enunciarse en una sola línea: la protección jurídica de artistas e intérpretes frente a la IA generativa requiere migrar de un modelo basado en derechos dispersos aplicados *ex post* hacia una arquitectura integrada de gobernanza *ex ante* que reconozca la réplica digital como categoría autónoma y combine, de modo inseparable, cuatro capas: (i) una arquitectura contractual modular, con especificidad operacional sobre objeto licenciado, entrenamiento de modelos, trazabilidad y remedios; (ii) un régimen de visibilidad algorítmica que corrija el desplazamiento sistémico del intérprete humano por contenido sintético en entornos de distribución algorítmica; (iii) una gobernanza del legado *post mortem* centrada en regular *inputs* antes que *outputs*; y (iv) una infraestructura probatoria transversal que haga operativamente exigibles las tres capas anteriores. Estos cuatro ejes no son compartimentos independientes, sino piezas interdependientes de un mismo régimen: sin infraestructura probatoria, los contratos no son ejecutables; sin contratos modulares, la transparencia algorítmica no produce remedio; sin directivas de identidad en vida, el legado *post mortem* queda a merced del *dividendo del mentiroso*. De esta tesis se sigue una propuesta normativa concreta: el reconocimiento de la réplica digital como objeto jurídico autónomo exige una lógica *copyright-like* —exclusividad fuerte, remedios rápidos, consentimiento verificable y responsabilidad en cadena—, pero calibrada mediante excepciones robustas para parodia, crítica, documental y uso informativo, y con límites temporales *post mortem* razonables. Los apartados siguientes desarrollan cada eje y la conclusión sistematiza las recomendaciones normativas que de ellos derivan.

2. Cuando la máquina suplanta al artista: coordenadas técnicas y jurídicas del problema

Antes de adentrarnos en el análisis jurídico propiamente dicho, conviene delimitar con precisión el objeto de estudio. En términos técnicos, el *deepfake* es una subespecie de *synthetic media*: contenido audiovisual generado o alterado mediante modelos de aprendizaje profundo para producir una representación altamente verosímil de una persona haciendo o diciendo algo que nunca ocurrió (Abbas y Taeihagh, 2024; Chesney y Citron, 2019; Mustak, 2023). Pero desde el punto de vista jurídico-probatorio, lo que importa no es tanto la falsedad como la plausibilidad: a mayor fidelidad perceptiva, mayor riesgo de confusión y más caro resulta desmentir el engaño (Chesney y Citron, 2019). Lo verdaderamente disruptivo no es que alguien pueda fabricar un video falso —eso existe desde los albores de la edición audiovisual—, sino que ahora puede hacerlo a escala, con calidad suficiente para erosionar la confianza en los registros audiovisuales y a un costo que se desploma año tras año (Jayanti, 2019).

Esta erosión no afecta solo contenidos aislados, sino que genera efectos sistémicos sobre la confianza epistémica en los medios digitales (Mustak, 2023). Cuando la distinción entre lo auténtico y lo sintético se vuelve imperceptible para el observador promedio, estamos ante lo que algunos autores llaman una "crisis de la evidencia visual", con repercusiones tanto en el ámbito judicial como en el debate público (Abbas y Taeihagh, 2024). Volveremos sobre esto con detenimiento en el apartado 6, pero conviene tenerlo presente desde ahora: el problema de fondo no es solo que se puedan fabricar mentiras convincentes, sino que la posibilidad misma de fabricarlas contamina la credibilidad de todo lo demás.

Ahora bien, cuando trasladamos el análisis al ámbito específico de artistas e intérpretes, el problema cambia de naturaleza. Los conceptos de "clon digital" o "réplica digital" exceden la mera reproducción estática de una fotografía o una grabación. Lo que estas tecnologías persiguen es algo más ambicioso: una continuidad funcional de la identidad performativa. No solo el rostro o la voz, sino la gestualidad, el *timing*, la prosodia, las microexpresiones y el movimiento corporal, de modo que el resultado pueda efectivamente "actuar" como sustituto del sujeto en un contexto de explotación comercial

(U.S. Copyright Office, 2024). Como señala el informe de la U.S. Copyright Office, la réplica captura la "esencia performativa" del intérprete: ese conjunto de atributos intangibles —control vocal, expresividad, capacidad de transmitir emociones— que constituyen su valor de mercado y que incluyen también componentes más difusos como reputación, trayectoria y capital simbólico acumulado. Esto desplaza la discusión jurídica desde el tradicional "uso de una imagen" hacia el uso de una capacidad personal explotable: la *performance* entendida como atributo económico y reputacional.

Precisamente porque el fenómeno no encaja en un único compartimento normativo, los enfoques contemporáneos más sofisticados proponen una arquitectura regulatoria por capas (U.S. Copyright Office, 2024). En ausencia de ese régimen unificado, los artistas se ven forzados a invocar simultáneamente derechos de autor sobre la interpretación fijada, derechos de imagen, teorías de enriquecimiento injusto y protección de datos personales, cada línea con sus propios requisitos y excepciones. El resultado es incertidumbre jurídica, costos de litigio elevados y, en la práctica, una ventaja estructural para quien tiene más recursos para navegar la complejidad (Chesney y Citron, 2019).

En términos operativos, la IA generativa aplicada a la *performance* puede ordenarse por canal y por tarea. Predominan hoy cuatro familias tecnológicas, cada una con implicaciones jurídicas propias.

Los modelos de texto-a-video sintetizan secuencias audiovisuales a partir de instrucciones textuales, produciendo contenido performativo enteramente sintético sin requerir grabación previa del sujeto (Abbas y Taeihagh, 2024). Lo particularmente inquietante es que la "imagen" en cuestión nunca fue capturada, fue directamente generada a partir de *datasets* de entrenamiento, lo que plantea interrogantes sobre los límites del derecho a la propia imagen cuando no hubo captura alguna que autorizar o prohibir.

Las técnicas de clonación de voz replican timbre, prosodia y estilo de un hablante con apenas unas pocas muestras —en algunos casos, bastan tres segundos de audio—, habilitando lo que podríamos llamar una "suplantación sonora" del intérprete (Arık et al., 2018; Azzuni y El Saddik, 2025). La facilidad de esta clonación ha generado especial preocupación en la industria del entretenimiento, donde actores de doblaje y locutores reportan casos de uso no autorizado

descubiertos recién cuando el contenido ya circula públicamente (U.S. Copyright Office, 2024).

La reanimación facial (*face reenactment*) transfiere expresiones y movimientos desde un video de origen hacia la identidad de un sujeto objetivo, preservando la identidad visual mientras se copia la actuación facial (Kligvasser et al., 2025). Esta tecnología resulta particularmente problemática porque separa dos cosas que en el mundo analógico eran inseparables: un actor puede "prestar" su *performance* facial mientras otro "presta" su rostro, generando un híbrido cuya autoría y titularidad resulta difícil de determinar.

La transferencia de movimiento codifica la actuación corporal de un video de referencia para aplicarla a otro sujeto, recreando la *performance* sin presencia física del intérprete (Kansy et al., 2025). Estudios ya han utilizado captura de movimiento de dobles de acción para aplicar esos movimientos a réplicas de actores principales, eliminando la necesidad de contratar al talento original sin reconocimiento ni compensación adicional (U.S. Copyright Office, 2024).

Las consecuencias jurídicas de este repertorio son inmediatas, porque el objeto de apropiación puede ser la identidad, la actuación o ambas simultáneamente, y cada combinación activa regímenes distintos (Chesney y Citron, 2019; U.S. Copyright Office, 2024). Más aún, la combinatoria genera posibilidades exponencialmente complejas: un mismo contenido puede involucrar la voz del artista A, el rostro de B con las expresiones de C y los movimientos de D, desafiando cualquier taxonomía basada en categorías discretas y mutuamente excluyentes.

De ahí que resulte indispensable trazar una matriz de riesgos jurídicos recurrentes. No pretende ser exhaustiva —la evolución tecnológica genera constantemente nuevos vectores—, pero sí identificar los patrones más estables y las vulnerabilidades estructurales que cualquier respuesta regulatoria debería atender.

El primero es el riesgo de confusión de fuente o autenticidad: el *deepfake* puede inducir al público a atribuir declaraciones o *endorsements* al artista cuando nunca existieron (Chesney y Citron, 2019; Mustak, 2023). Lo que Mustak (2023) llama el "sesgo de familiaridad" refuerza esta dinámica: los usuarios tienden a asumir que contenido que luce auténtico probablemente lo sea, y la investigación

empírica sugiere que incluso advertencias explícitas tienen eficacia limitada una vez que el material se viraliza descontextualizado (Abbas y Taeihagh, 2024).

El segundo es la apropiación económica de la *performance*: la réplica permite capturar el valor de mercado del artista —voz, imagen, estilo interpretativo— sin pagar honorarios equivalentes, habilitando tanto sustitución laboral como extracción de renta del capital reputacional acumulado a lo largo de toda una carrera (U.S. Copyright Office, 2024). La asimetría entre el valor capturado y la compensación pagada —frecuentemente, una tarifa única por la sesión de captura— plantea serios cuestionamientos desde la teoría del enriquecimiento injusto.

El tercero es el daño reputacional y moral que surge cuando el clon se inserta en contextos degradantes o contradictorios con la imagen pública del intérprete (Chesney y Citron, 2019). Este daño puede ser particularmente persistente, incluso después del desmentido público, residuos de la información falsa permanecen en memoria colectiva y en algoritmos de recomendación (Belfer Center, 2019). Para artistas cuyo valor depende críticamente de su imagen pública, esto tiene traducción económica directa en pérdida de contratos y erosión de oportunidades.

El cuarto, a escala industrial, es el desplazamiento de mercado y el debilitamiento del poder de negociación. La disponibilidad de réplicas abarata reemplazos y presiona condiciones contractuales (U.S. Copyright Office, 2024). La mera amenaza de sustitución digital disciplina demandas salariales y empuja a los artistas a aceptar cláusulas más amplias de cesión de derechos por temor a quedar fuera del mercado. No estamos hablando solo de casos individuales de sustitución, sino de transformaciones sistémicas de las prácticas contractuales.

El quinto, quizás el más preocupante desde una perspectiva sistémica, es la erosión de la evidencia. Aquí confluyen dos efectos que se retroalimentan: las disputas *ex post* sobre si existió consentimiento y cuál fue su alcance y el "dividendo del mentiroso" (*liar's dividend*) por el cual la mera existencia de *deepfakes* facilita negar evidencia auténtica, elevando el umbral probatorio y debilitando el *enforcement* (Belfer Center, 2019; Chesney y Citron, 2019). Los métodos de detección están envueltos en una carrera armamentística con los

de generación: cada marcador forense identificado es eliminado por nuevos modelos (Abbas y Taeihagh, 2024). Confiar exclusivamente en detección técnica resulta insuficiente; será necesario complementar con autenticación proactiva, cadenas de custodia digital, *watermarking* robusto y reformas procesales que redistribuyan la carga de la prueba (Chesney y Citron, 2019).

El panorama trazado hasta aquí evidencia que la irrupción de la inteligencia artificial (IA) generativa aplicada a la *performance* no es un desafío técnico susceptible de ajustes menores. Estamos ante una transformación estructural que pone en tensión los fundamentos mismos de la protección jurídica de artistas e intérpretes: desde la delimitación del objeto protegido hasta los mecanismos de atribución y prueba, pasando por la configuración de incentivos que determinan quién captura el valor generado por estas tecnologías. Con estas coordenadas en mente, podemos adentrarnos en el análisis de cómo los ordenamientos jurídicos existentes responden —o no— a estos desafíos.

3. ¿Quién es "artista" y quién es "intérprete"? Taxonomías funcionales y la arquitectura del solapamiento normativo

Antes de examinar cómo responden los distintos ordenamientos, conviene precisar qué entendemos por "artista" y qué por "intérprete", porque estas categorías despliegan regímenes de protección muy diferentes. La distinción determina qué derechos se activan, qué pruebas importan y qué estrategias de defensa están disponibles. Un mismo *deepfake* puede activar varios de estos regímenes simultáneamente, de modo que la respuesta jurídica efectiva raramente consiste en elegir un derecho, sino en orquestar varios.

Esta multiplicidad no es un defecto del sistema, sino una característica estructural. Diferentes dimensiones del fenómeno lesionan bienes que fueron protegidos por regímenes especializados —personalidad, prestación artística, obras interpretadas, posición de mercado, datos personales— y el desafío es entender cómo interactúan frente a una tecnología que ignora las fronteras conceptuales de un mundo analógico donde identidad, *performance* y fijación eran inseparables.

Desde una perspectiva funcional, distinguimos cuatro categorías. El artista-creador aporta autoría sobre una obra —guión, música, coreografía— y se protege bajo derecho de autor. Lo crucial es que el valor protegido depende de la originalidad de la obra, no de la recognoscibilidad del creador. El artista-intérprete aporta *performance*. Como explica Gervais (2015), los sistemas jurídicos enfrentaron tempranamente la tensión entre *performance* y obra: ¿es la interpretación de Hamlet por Laurence Olivier una "obra" autoral o una prestación distinta de la obra de Shakespeare? La solución fue crear los derechos conexos, régimen paralelo al derecho de autor. Esta dualidad se vuelve problemática frente a *deepfakes* que generan "nuevas *performances*" sintéticas: ¿estamos ante reproducción de una *performance* fijada o ante creación de una obra derivada?

La distinción entre intérprete principal y secundario parece meramente artística, pero adquiere relevancia jurídica concreta: la centralidad narrativa afecta la magnitud del perjuicio, la recognoscibilidad activa derechos de imagen y *publicity rights*, la aportación creativa determina el alcance de derechos morales y la explotación comercial incide en el daño económico. Las zonas grises —actores de doblaje, extras, músicos de sesión— son especialmente problemáticas porque la tecnología no distingue jerarquías: un sistema de clonación vocal reproduce con igual fidelidad la voz de un actor de doblaje que la de una estrella de Hollywood. Si la protección se gradúa según prominencia, desprotegemos a los más vulnerables.

Von Lewinski (2013) documenta que, durante la negociación del Tratado de Beijing, se entendió que los extras no "interpretan" obras en el sentido del tratado. En la misma línea, Gervais (2015) recuerda que la distinción entre *interprètes* y *exécutants* en la Convención de Roma dejaba fuera a quienes meramente ejecutan instrucciones técnicas. Estas exclusiones generan tensiones evidentes cuando el rostro de un extra o la voz de un músico de sesión son clonados para producciones que nunca consintieron.

El Tratado de Beijing (2012, Art. 2) define a los intérpretes de manera intencionalmente amplia e incorpora expresamente la improvisación, reconociendo que el valor del intérprete no se agota en ejecutar una partitura, sino que incluye su aportación creativa espontánea (Von Lewinski, 2013). Pero esto plantea una pregunta

espinosa: ¿qué es "obra" cuando lo que circula es una réplica sintética que parece *performance* humana, pero nunca fue ejecutada por persona alguna? La disociación entre obra y *performance* —impensable en el mundo analógico— desafía las categorías sobre las que se construyeron los derechos conexos. En cuanto a derechos morales, el Tratado reconoce integridad "tomando debidamente en cuenta la naturaleza de las fijaciones audiovisuales" (Art. 5), flexibilización que resulta problemática cuando la frontera entre edición normal y manipulación lesiva se vuelve borrosa. Respecto de los derechos económicos —reproducción, distribución, alquiler, *making available*—, la pregunta central es si estos derechos, diseñados para la explotación de fijaciones existentes, se extienden a la generación sintética de nuevas *performances*. Un *deepfake* no copia mecánicamente fotogramas; genera contenido usando modelos entrenados con múltiples *performances*. Si no es "reproducción", ¿es adaptación, obra derivada o algo que requiere reforma legislativa?

3.1 Arquitectura del solapamiento: regímenes concurrentes y estrategias de articulación

Un mismo *deepfake* puede activar simultáneamente múltiples regímenes. El de derechos de personalidad constituye la primera línea de defensa, con el consentimiento como llave estructural en tres dimensiones: captación inicial, usos derivados sintéticos (¿el consentimiento para ser filmado implica autorizar el entrenamiento de modelos de IA?) y explotación comercial. Sus ventajas probatorias son considerables —basta probar uso sin consentimiento, el daño moral se presume en muchos ordenamientos—, pero puede no cubrir réplicas sintéticas que técnicamente no son "la imagen" del sujeto.

El régimen de derechos conexos protege la interpretación como prestación artística. Aquí la doctrina está profundamente dividida. Una interpretación amplia diría que hay "reproducción" en sentido económico-funcional, línea consistente con la jurisprudencia europea (Rosati, 2025) y con la posición de la Licensing Executives Society International (2025). Una interpretación estricta diría que no hay reproducción porque no se copian fragmentos identificables; Bracha (2024a, 2024b) sostiene que la apropiación del "estilo" no

constituye infracción porque el estilo es elemento no protegible que se derrama al dominio público. Lo que está en juego es si los derechos conexos protegen solo fijaciones específicas o más ampliamente la capacidad artística del intérprete. El Tratado de Beijing se negoció antes de que los *deepfakes* estuvieran ampliamente disponibles (Gervais, 2015; Von Lewinski, 2013) y sus categorías siguen pensadas para fijaciones existentes.

El derecho de autor presenta múltiples entradas: uso no autorizado de obras preexistentes, creación de obras derivadas y el debate sobre si la *performance* misma cualifica como obra (Gervais, 2015). El régimen de marcas y competencia desleal opera cuando el *deepfake* funciona como señal de origen, con umbral probatorio más bajo y remedios expeditos. El régimen de protección de datos biométricos —GDPR,[2] LGPD,[3] BIPA[4]— exige consentimiento explícito, informado y revocable, con la consecuencia de que modelos de IA entrenados con datos de personas que rescindieron consentimiento podrían volverse ilícitos.

3.2 Mapa integrado: sinergias, tensiones y gobernanza contractual

Las cinco dimensiones del *deepfake* —identidad, *performance*, obras subyacentes, mercado, datos— activan regímenes diferenciados. Como capa transversal, el contrato funciona como mecanismo de gobernanza privada que puede reforzar o erosionar las protecciones legales. En la práctica, como remarca Gervais (2015), esta maraña de derechos raramente se materializa en litigios porque la explotación está contractualmente cubierta. El tratado de Beijing reconoce esta realidad en su Artículo 12, que permite presumir transferencia de derechos al productor una vez consentida la fijación (Von Lewinski, 2013).

Pero esta flexibilidad contractual es precisamente el punto más vulnerable frente a *deepfakes*. Los contratos fueron diseñados para

2 General Data Protection Regulation (Reglamento General de Protección de Datos), Unión Europea, 2016/679.

3 Lei Geral de Proteção de Dados Pessoais, Brasil, Lei n.° 13.709/2018.

4 Biometric Information Privacy Act (Estados Unidos), 740 ILCS 14, 2008.

usos previsibles —reproducción en diferentes formatos, transmisión por diferentes canales—, no para entrenar modelos de IA que generen contenido nuevo sin participación del artista. Estudios argumentarán que cláusulas de "todos los usos presentes y futuros" cubren la IA generativa (Davis Wright Tremaine LLP, 2025). Intérpretes responderán que una interpretación literal vacía de contenido el requisito de consentimiento informado. Este argumento encontró reconocimiento legislativo: AB 2602[5] declaró inaplicable cualquier cláusula que permita réplicas digitales sin descripción específica de usos y sin asesoría jurídica o sindical.[6] La U.S. Copyright Office (2024) recomendó limitar licencias a cinco o diez años. SAG-AFTRA[7]/AMPTP[8] estableció que el consentimiento para réplicas debe negociarse separadamente por proyecto (SAG-AFTRA, 2023).

La asimetría de poder agrava todo esto. La mayoría de los intérpretes están en posición de "tomar o dejar", y la sofisticación técnica que exigen cláusulas sobre datos biométricos o entrenamiento de modelos excede lo razonablemente esperable del intérprete promedio. De ahí que la solución no pueda descansar solo en la gobernanza contractual privada, se requieren pisos mínimos de protección legal —normas imperativas debajo de las cuales los contratos no pueden descender— que corrijan las fallas del mercado: información asimétrica, poder de negociación desigual, externalidades no internalizadas.

4. El mapa no es el territorio: regulación comparada en la frontera del clon digital

La tendencia regulatoria más visible del período 2024-2026 es un desplazamiento conceptual: el movimiento desde el *right of publicity* hacia modelos que tratan ciertos rasgos identitarios con lógica *copyright-like* —exclusividad fuerte, remedios rápidos, foco en

5 Assembly Bill 2602, proyecto de ley de la Asamblea del Estado de California (luego promulgado como ley).

6 Cfr. Cal. Lab. Code § 927, 2024.

7 Screen Actors Guild/American Federation of Television and Radio Artists.

8 Alliance of Motion Picture and Television Producers.

consentimiento verificable y responsabilidad a lo largo de toda la cadena—. El punto de llegada de este apartado no es inventariar normas, sino mostrar que tres líneas regulatorias aparentemente dispares convergen en un mismo problema no resuelto: cómo verificar que el consentimiento fue efectivamente otorgado y cómo atribuir responsabilidad cuando no lo fue.

4.1 Estados Unidos: el mosaico estatal y la carrera hacia la ley federal

En Estados Unidos, el punto de partida sigue siendo estatal. La estructura típica opera con un *trigger* (uso no autorizado con fines comerciales), un daño y remedios que incluyen *injunction* y daños. El ejemplo canónico es California § 3344; Nueva York incorporó en 2024 la Civil Rights Law § 50-f, primera legislación del estado en abordar la clonación de voz mediante IA (Kapilian, 2025). En mayo de 2025, el presidente Donald Trump firmó la TAKE IT DOWN Act, que criminaliza imágenes *deepfake* no consentidas y encomienda al FTC[9] un régimen de *notice-and-removal* (U.S. Congress, S. 146, 2025). A la fecha, 46 estados tienen alguna legislación sobre *deepfakes* (Jones Walker LLP, 2026), y la U.S. Copyright Office (2024) le recomendó al Congreso crear un nuevo derecho federal específico.

Esa recomendación impulsó la NO FAKES Act, que propone un derecho federal de propiedad sobre voz y *likeness* con *takedown* modelado sobre el DMCA,[10] protección durante la vida más hasta 70 años *post mortem* y registro renovable ante la Copyright Office (U.S. Congress, S. 1367, 2025). Como observó Rothman (2025), en lugar de crear un verdadero *right of publicity* federal, añade otra capa al *identity thicket*: una maraña de derechos superpuestos sin armonización real. Lo que estos regímenes no resuelven es cómo determinar, en la práctica, si una réplica digital concreta es "la persona" u "otra cosa". Es la fractura epistemológica que se examina en los apartados siguientes.

9 Federal Trade Commission (Comisión Federal de Comercio de los Estados Unidos).

10 Digital Millennium Copyright Act (17 U.S.C. §§ 512 y ss., 1998), ley federal estadounidense que establece el régimen de notificación y remoción (*notice-and-take-*

4.2 ELVIS Act: cuando la responsabilidad aprende a seguir la cadena

La ELVIS Act (Tennessee, vigente desde julio de 2024) es la legislación más relevante del período no por lo que prohíbe, sino por cómo estructura la responsabilidad. Fue el primer estatuto estadounidense en proteger explícitamente contra usos de IA sobre la propia voz, con una definición deliberadamente amplia que incluye *simulation* (State of Tennessee, 2024), cerrando la laguna de los *sound-alikes* generados por IA. Como señaló Morrison Foerster (2025), la definición podría alcanzar incluso imitaciones analógicas. El catalizador fue Fake Drake, generada en 2023 mediante clonación de voz, que se viralizó en TikTok antes de ser retirada (Kohel y Klukosky, 2024).

Pero el aporte central es la creación de responsabilidad secundaria más allá del usuario final. La primera categoría recae sobre quien publica o distribuye voz o *likeness* "with knowledge that use was not authorized", alcanzando potencialmente a plataformas y servicios de *streaming* (Latham y Watkins, 2024, p. 2). La segunda recae sobre quien pone a disposición herramientas cuyo propósito principal sea producir réplicas no autorizadas —apuntando a proveedores de clonación y desarrolladores de modelos generativos. Es la primera norma que intenta distribuir responsabilidad a lo largo de la cadena tecnológica.

La pregunta que no responde es: la responsabilidad secundaria requiere *knowledge*, pero en un ecosistema sin infraestructura estándar de verificación, ¿cómo demuestra un distribuidor que "no sabía"? La ELVIS Act crea el marco normativo de la responsabilidad en cadena, no crea el mecanismo por el cual esa cadena pueda ser verificada.

4.3 Dinamarca: cuando la herramienta que funciona no es la que deberías usar

Si la ELVIS Act se mueve dentro de la lógica del *right of publicity*, la propuesta danesa representa algo cualitativamente diferente: reencuadrar la identidad personal como objeto de protección intelectual. En junio de 2025, Dinamarca anunció una enmienda a su

down) para infracciones de derechos de autor en línea.

Copyright Act, otorgando derechos sobre cuerpo, rasgos faciales y voz como si fueran obras protegidas (Schjødt, 2025; *Denmark to tackle deepfakes…*, 2025). Lo que importa no es la calidad del derecho creado sino el problema que pretende resolver. Thomas Heldrup, de la Danish Rights Alliance, lo identificó con franqueza: el problema ha sido que las plataformas no responden a reclamos basados en derechos de personalidad como responden a DMCA *takedowns* (como se citó en Tech Policy Press, 2025). Dinamarca está usando la herramienta que funciona —*copyright*— para resolver un problema que aquellas que *deberían* funcionar no resuelven en la práctica. Es un movimiento pragmático, y, en ese sentido, está tanto su fuerza como su vulnerabilidad: *copyright* trae supuestos sobre transferibilidad que no encuadran naturalmente con la identidad personal.

El caso *Jack Nicklaus* lo ilustra con brutalidad: en 2007, vendió sus intereses comerciales por USD 145 millones, incluyendo nombre, imagen y *likeness*; años después, la empresa autorizó una réplica hecha por IA sin su consentimiento, y recién en marzo de 2025 un juez de Nueva York determinó que nunca había cedido autorización exclusiva sobre su propia identidad (McCann, 2025). La U.S. Copyright Office (2024) subrayó el punto: la capacidad de mantener control sobre la propia identidad no debe poder cederse permanentemente mediante contrato.

4.4 El eje común: tres tradiciones, un mismo desafío

De la lectura comparada emergen tres pilares convergentes. Primero, consentimiento verificable: no abstracto, sino acreditable en alcance y uso específico. Segundo, *notice-and-takedown* reforzado: Dinamarca introduce sanciones severas (*Denmark to tackle deepfakes…*, 2025); la ELVIS Act crea responsabilidad del distribuidor con conocimiento; la TAKE IT DOWN Act impone remoción en 48 horas (U.S. Congress, S. 146, 2025); la EU AI Act exigirá marcado obligatorio de contenido sintético desde agosto de 2026 (European Parliament & Council, 2024). Tercero, deberes operativos para plataformas: reconceptualizarlas como actores con obligaciones positivas, no meros intermediarios pasivos. Estos tres pilares confluyen en una pregunta que ninguna legislación responde satisfactoriamente: ¿cuál es la in-

fraestructura que permite que estos mandatos sean operativos? Es lo que se aborda en los apartados siguientes.

5. La gobernanza que los tribunales no ven: plataformas, T&C y la invención del "derecho operativo"

Gran parte del cumplimiento cotidiano en el espacio de réplicas digitales no se decide en tribunales ni en leyes estatales, se decide en los términos y condiciones y políticas de moderación de las plataformas que generan, distribuyen y monetizan contenido. Estas políticas funcionan como lo que en este apartado se denomina *derecho operativo*: no tienen autoridad formal de ley, pero definen en la práctica qué conductas son permitidas, cuál es el estándar de consentimiento exigido y cuáles son las consecuencias por violación. La distancia entre esta gobernanza privada y los mandatos legislativos examinados en el apartado 4 es, paradójicamente, uno de los indicadores más claros de que los regímenes sustantivos necesitan una capa de infraestructura que los conecte con la realidad operativa.

5.1 El patrón que se repite: declaración sin verificación

Las políticas de uso de la mayoría de las plataformas comparten una estructura reconocible: obligación del usuario de tener derechos o consentimiento sobre la identidad que pretende representar, prohibición explícita de suplantación y usos no consentidos y mecanismo de *enforcement* que incluye remoción, suspensión y terminación de cuenta. El problema evidente es que la obligación recae sobre el usuario, pero la plataforma no tiene un mecanismo para verificar que este efectivamente tiene el consentimiento que declara poseer. Es un sistema de declaración unilateral, no de verificación.

El alcance de lo que está en juego cuando ese sistema falla no es académico. En enero de 2024, la firma de ingeniería Arup perdió 25 millones de dólares cuando un empleado participó en una videollamada con un *deepfake* del CFO[11] y varios colegas artificialmente generados que autorizaron quince transferencias bancarias antes de ser detectado.

11 Chief Finance Officer (gerente de finanzas).

Pindrop Security encontró que más de un tercio de 300 perfiles de candidatos analizados estaban completamente fabricados, con resúmenes generados por IA y video *deepfake* en entrevistas en tiempo real (Jones Walker LLP, 2026). El *gap* entre obligación declarativa y capacidad real de verificación no es un problema teórico, es un vector de daño activo.

5.2 HeyGen: cuando la réplica digital se convierte en datos biométricos

HeyGen es, entre las plataformas comerciales de video sintético, una de las pocas que explicita de manera clara la exigencia de consentimiento expresado para crear avatares personalizados, con sanciones que incluyen remoción, suspensión y terminación (HeyGen, s.f.-a). Lo interesante no es solo la existencia de esta regla, sino también su Biometric Privacy Notice, que reconoce explícitamente que el proceso involucra tratamiento de datos biométricos (HeyGen, s.f.-b). Esta es una conexión que pocas plataformas hacen de manera transparente: crear una réplica digital no es solo generar contenido, es también procesar datos biométricos de una persona real, sujeto a regulación adicional (GDPR, Art. 9 en Europa; BIPA en Illinois; normas equivalentes en otras jurisdicciones).

En la práctica, esta conexión genera un segundo canal de *enforcement*: si el tratamiento de datos biométricos sin consentimiento es ilegal independientemente de si el contenido generado resulta perjudicial, la plataforma tiene un incentivo propio —no solo contractual, sino también legal— para verificar que el consentimiento fue efectivamente otorgado antes de procesar los datos.

5.3 OpenAI y Sora: el consentimiento como evento diseñado

El enfoque de OpenAI en el lanzamiento de Sora es relevante no por ser el más restrictivo, sino por ser quizás el más explícito en diseñar el consentimiento como evento tecnológicamente registrable. OpenAI (2025) describe un sistema de *consent-based likeness*, mediante el cual el usuario puede controlar quién usa su representación digital, puede revocar ese consentimiento y recibirá notificación cuando su *likeness* sea utilizada. Junto a este mecanismo, OpenAI (2025) señala medidas

de prevención: *watermark* visible, señales invisibles, metadata C2PA embebida y herramientas internas de trazabilidad. La combinación de estas dos capas —consentimiento registrable y prevención de contenido— es la aproximación más cercana que una plataforma comercial ha mostrado, a lo que en el apartado 6 se denominará "infraestructura de prueba integrada". La limitación inherente es que todo esto opera dentro del ecosistema de OpenAI. Un contenido generado por otra herramienta, o generado por Sora, pero exportado sin sus credenciales, escapa enteramente de esta arquitectura.

5.4 El estándar que las plataformas están inventando sin saberlo

Sin que sea ley formal ni estándar interoperable, la práctica emergente de las plataformas más grandes tiende a construir —de manera convergente, pero no coordinada— un estándar de "consentimiento suficiente" con tres propiedades que el consentimiento contractual tradicional no tenía. Primero, es expreso y atribuible: debe existir registro de que la persona representada activamente lo otorgó. Segundo, es revocable con control de accesos: el sujeto puede retirar la habilitación y la plataforma debe tener un mecanismo para que esa revocación surta efecto. Tercero, tiene auditabilidad mínima: *logs*, metadata y *provenance* permiten reconstruir el historial del contenido y sostener decisiones de moderación con evidencia técnica.

Este patrón es, sin que las plataformas lo formulen así, la respuesta privada al problema que en el apartado 4 se identificó como no resuelto: cómo hacer que el consentimiento sea verificable. Pero la respuesta tiene dos limitaciones (que se examinarán en el apartado 6): la primera es que es fragmentada: cada plataforma construye su estándar independientemente, sin interoperabilidad; la segunda es que funciona solo hacia adentro, en el ecosistema de cada plataforma, pero no en la cadena completa desde la creación hasta la distribución final.

6. Cuando ver ya no es creer: la infraestructura de prueba que los derechos necesitan para poder existir

6.1 El supuesto que se derrumba: normas correctas sobre hechos imposibles de establecer

Todo el arco analítico recorrido hasta aquí —derechos de personalidad, derechos conexos, derecho de autor, competencia desleal, protección de datos, gobernanza contractual, regulación comparada— descansa en un supuesto epistemológico que la tecnología ha comenzado a disolver: que es posible determinar, con certeza razonable, si un contenido audiovisual es auténtico o sintético y si la identidad representada corresponde a una persona real que consintió o no. Los regímenes examinados son normativamente correctos, pero prescribir que el uso no consentido de una réplica digital es ilícito carece de valor operativo si la víctima no puede demostrar que la réplica existe, que es suya y que no fue consentida.

Las normas analizadas —AB 2602, ELVIS Act, NO FAKES Act (U.S. Congress, S. 1367, 2025), la propuesta danesa— presuponen que los hechos relevantes pueden ser establecidos. Se trata de un problema estructuralmente diferente al que abordó el derecho antes de la generación sintética: no es una cuestión de interpretación jurídica, sino de capacidad epistemológica. Como señalaron Chesney y Citron (2019) al identificar el *dividendo del mentiroso* (*liar's dividend*), la amenaza más insidiosa de los *deepfakes* no es la fabricación de contenido falso, sino la erosión de la confiabilidad de todo contenido audiovisual: cuanto más se difunde la conciencia pública sobre *deepfakes*, más fácil resulta desestimar como fabricado cualquier contenido inconveniente.

La dinámica ya es observable en la práctica judicial. En Estados Unidos, la defensa en un proceso contra Tesla intentó desestimar declaraciones videograbadas de Elon Musk argumentando que podrían ser *deepfakes*; un juez federal de Washington rechazó el argumento, advirtiendo que aceptar dicha defensa sin estándares adicionales haría que "la evidencia se vuelva carente de sentido" (como se citó en Dixon, 2024, párr. 12). En septiembre de 2025, un tribunal en el condado de Alameda descartó un caso civil completo tras determinar que un testimonio videograbado era un *deepfake* deliberadamente presentado como prueba (University of Colorado Boulder, 2025).

La tesis de este apartado es que la protección jurídica efectiva requiere, como condición de aplicabilidad, una infraestructura de prueba que permita verificar tres cosas interrelacionadas: (i) que un contenido es sintético o auténtico (*proof of provenance*); (ii) que la identidad de una persona está representada en ese contenido (*proof of personality*); y (iii) que el consentimiento fue o no otorgado, en qué alcance y por quién (*proof of consent*). Sin esta infraestructura, los regímenes sustantivos permanecen como derecho que no puede ser ejercido.

6.2 El dividendo del mentiroso opera en dos direcciones

En el contexto de los derechos del intérprete, el dividendo del mentiroso opera bidireccionalmente. En la primera dirección, el productor o plataforma que distribuyó una réplica no consentida puede argumentar que el contenido es obra original y no réplica de ningún individuo real. En la segunda —menos analizada—, el mismo intérprete puede ver socavada su posibilidad de ejercer derechos legítimos si la otra parte cuestiona la autenticidad de la evidencia que aporta. El dividendo del mentiroso amenaza la eficacia del sistema de prueba en el espacio privado: contratos, litigios comerciales, negociaciones sindicales. Como observó el análisis parlamentario californiano al fundamentar AB 2602, si incluso las partes que firmaron los contratos no anticiparon el alcance tecnológico, con mayor razón no anticiparon la necesidad de infraestructura probatoria (California Assembly Privacy and Consumer Protection Committee, 2024). La propuesta de Louisiana de reforma al Code of Civil Procedure —que les exigiría a los abogados verificar la autenticidad de la evidencia antes de ofrecerla, con sanción de *contempt of court*— representa uno de los primeros intentos de imponer una obligación de *gatekeeping* del que el sistema actual carece (Jones Walker LLP, 2026).

6.3 C2PA y sus límites estructurales

La respuesta tecnológica más desarrollada al problema de *provenance* es el estándar C2PA (Coalition for Content Provenance and Authenticity), que opera mediante *Content Credentials*: metadatos fir-

mados digitalmente que registran acciones, actores e ingredientes en cada punto de la vida de un *asset* digital (Coalition for Content Provenance and Authenticity, 2025). El NIST[12] lo identificó como el mecanismo más prometedor para *provenance data tracking*, pero subrayó que ninguna técnica es solución autónoma: requiere una combinación de *provenance*, detección, educación y política (Chandra et al., 2024).

El problema fundamental es que el C2PA es un sistema *opt-in*: funciona cuando los actores cooperan con el estándar. La evaluación empírica de Rijsbosch et al. (2025) —que examinó cincuenta sistemas de generación sintética— encontró que la mayoría no implementa *watermarking* invisible verificable y los que lo hacen frecuentemente no comparten algoritmos de detección. El C2PA puede certificar que un contenido es auténtico, pero no puede demostrar que un contenido sin credenciales es necesariamente sintético. Como advirtió el U.S. Department of Defense (2025), "la ausencia de una etiqueta C2PA no significa automáticamente que el contenido sea un *deepfake*" (p. 6). Según las proyecciones de Europol (como se citó en Jones Walker LLP, 2026), hasta el 90% del contenido en línea podría ser generado sintéticamente para 2026.

6.4 EU AI Act Art. 50 y la primera obligación de transparencia *multilayer*

El marco regulatorio más avanzado es la EU AI Act (Regulation (EU) 2024/1689), cuyo Artículo 50, vinculante desde agosto de 2026, exige que los proveedores de sistemas de IA que generen contenido sintético aseguren que los *outputs* estén "marcados en formato legible por máquinas y sean detectables como artificialmente generados o manipulados", con soluciones "efectivas, interoperables, robustas y confiables" (European Parliament & Council, 2024). El Art. 50(4) impone revelar que un contenido *deepfake* ha sido artificialmente ge-

12 National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología), agencia federal estadounidense dependiente del Departamento de Comercio responsable, entre otras funciones, del desarrollo de estándares técnicos en ciberseguridad e inteligencia artificial.

nerado, sin condición de comercialidad. El borrador del Código de Prácticas de diciembre de 2025 rechazó la idea de una única técnica y promovió un enfoque *multilayer*: (a) metadata con firmas digitales; (b) *watermarking* imperceptible; y (c) herramientas de detección accesibles a terceros (European Commission, 2025). Es la primera norma que se acerca a exigir lo que denominamos "infraestructura de prueba".

China ya implementó *watermarking* obligatorio sobre contenido de *deep synthesis*, mientras que India está desarrollando marcos propios tras la orden del Delhi High Court en 2024 de conformar un comité regulatorio específico (CyberPeace Foundation, 2025). Sin embargo, el Art. 50 tiene dos limitaciones: su alcance territorial (aplica a sistemas en el mercado europeo, no a contenido generado desde jurisdicciones externas) y que sus obligaciones recaen sobre proveedores e implementadores de IA, no sobre usuarios que generan *deepfakes* con herramientas *open-source* fuera de ecosistemas regulados.

6.5 La transformación conceptual del consentimiento

Una contribución central de la infraestructura de prueba consiste en transformar el consentimiento: pasarlo de ser un *permiso abstracto* (disposición general al momento de contratar) a ser un *evento verificable* (acto con fecha, contenido específico y auditabilidad). La práctica de las plataformas ya apunta en esta dirección. OpenAI describió un enfoque de *consent-based likeness* con credenciales de *provenance* embebidas (OpenAI, 2025). HeyGen (s.f.-b) exige consentimiento de la persona representada conectado a su Biometric Privacy Notice. Lo que estas políticas construyen es un consentimiento con tres propiedades que el contractual tradicional no tenía: expreso y atribuible, revocable con control de accesos y auditable mediante *logs*, metadata y *provenance*.

Este modelo converge con lo que la AB 2602 exige normativamente al requerir "descripción razonablemente específica de los usos previstos" (Cal. Lab. Code § 927, 2024). La NO FAKES Act reconoce parcialmente esta necesidad al proponer licencias en escritura, firmadas y con duración limitada a diez años (U.S. Congress,

S. 1367, 2025), pero el mecanismo de verificación tecnológica en tiempo real permanece sin definir. El *gap* actual es que la conexión entre requisito normativo y mecanismo técnico verificable aún no está estandarizada fuera de cada plataforma individual.

6.6 La trampa de la cooperación: por qué la prueba no puede depender solo de la buena voluntad

La debilidad más profunda de cualquier sistema basado en trazabilidad y consentimiento verificable es que asume un ecosistema donde los actores cooperan. Esto es razonable para plataformas reguladas y ecosistemas comerciales formales, no para quienes generan *deepfakes* fuera de ellos. El NIST fue explícito: los actores maliciosos no usarán *watermarking* o metadata de la manera prevista (Chandra et al., 2024).

La infraestructura de prueba puede resolver el problema de *verificación* (demostrar que un contenido es auténtico y que un consentimiento fue otorgado), pero no puede por sí sola resolver el de *detección* (identificar *deepfakes* no consentidos). La prueba debe operar en dos niveles: uno *preventivo* (trazabilidad y consentimiento registrado) y uno *reactivo* (detección y atribución cuando el daño ya ocurrió). El segundo requiere herramientas más sofisticadas que las de creación —una carrera armamentística que, según el NIST, actualmente está ganando el lado de la creación—.

Ningún régimen puede descansar exclusivamente en la obligación del intérprete de demostrar la violación: en muchos casos, será técnicamente imposible o prohibitivamente costosa. La contratación de expertos en *digital forensics* puede costar miles de dólares por proyecto, y esa carga cae desproporcionadamente sobre quienes menos pueden asumirla (Dixon, 2024). La propuesta de Delfino (2023, 2025) de reformar la Federal Rule of Evidence 901 mediante *burden-shifting* —donde, una vez presentada evidencia suficiente de fabricación por IA, la carga pasa al proponente de demostrar autenticidad con estándar más alto— aborda esta asimetría desde el lado procesal. Pero no resuelve la pregunta más fundamental: ¿cómo se comporta un sistema de prueba cuando la herramienta misma de detección no es confiable? En *USA v. Khalilian*, cuando la defensa impugnó grabaciones de voz como posibles *deepfakes*, el tribunal

respondió que la familiaridad del testigo con la voz sería suficiente, estándar inadecuado cuando la clonación vocal es comercialmente accesible (Jones Walker LLP, 2026).

6.7 Hacia una arquitectura completa: los cuatro componentes que ninguno tiene solo

La protección efectiva requiere una arquitectura de prueba que integre al menos cuatro componentes que actualmente operan en silos.

Primero, verificación de identidad biométrica vinculada al consentimiento: un mecanismo que asocie persona real (verificada mediante KYC o equivalente) con un perfil digital desde el cual los consentimientos puedan otorgarse, registrarse y revocarse.

Segundo, trazabilidad de origen certificada: un sistema como C2PA que registre el historial del contenido desde su creación, indicando si fue generado por IA, qué modelo fue utilizado y qué *inputs* proporcionados.

Tercero, trazabilidad de la cadena de distribución: un mecanismo que permita reconstruir cómo un contenido se movió desde su creación hasta su distribución o monetización, incluyendo plataformas intermediarias.

Cuarto, admisibilidad procesal de la evidencia técnica: estándares sobre cómo *logs*, *hashes*, *timestamps*, metadata C2PA y resultados de detección deben tratarse como evidencia en contextos litigiosos, incluyendo reglas de cadena de custodia digital y valor probatorio.

Ninguno existe en forma completa y sistematizada a nivel global. El C2PA cubre parcialmente el segundo. La EU AI Act, Art. 50, comienza a mandatar el segundo y parte del tercero. Las políticas de plataformas como OpenAI y HeyGen esbozan el primero. Lo que falta es la integración: un marco que reconozca que estos elementos no funcionan aislados. La analogía más precisa es la cadena de custodia en evidencia forense tradicional: nadie asume que una sola huella dactilar resuelve un caso. Para *deepfakes* y réplicas digitales, esa cadena aún no existe como sistema, solo como piezas dispersas que los actores más grandes van ensamblando individualmente.

7. La gobernanza económica del clon en la era digital: contratos, visibilidad algorítmica y legado *post mortem* en la inteligencia artificial generativa

Como ya se dijo, la irrupción de sistemas de inteligencia artificial generativa ha desestabilizado los presupuestos fundamentales del derecho de la personalidad tal como fue concebido en el siglo XX. Cuando pensamos en la capacidad técnica actual de producir réplicas sintéticas indistinguibles de *performances* humanas —no solo el rostro o la voz, sino la gestualidad completa, el estilo interpretativo, los matices que definen a un artista— nos enfrentamos a una transformación que va mucho más allá de lo que los redactores de códigos civiles pudieron imaginar. El *likeness* ha dejado de ser un atributo limitado por la materialidad de su reproducción para convertirse en un activo infinitamente replicable, modificable y comercializable (Preminger y Kugler, 2024). Esta mutación tecnológica exige algo más que ajustes normativos menores; requiere una reconceptualización jurídica profunda del problema mismo que intentamos resolver.

Ya no se trata simplemente de determinar quién puede usar la imagen de una persona, pregunta relativamente sencilla en un mundo donde las fotografías eran objetos físicos y las películas requerían costosas producciones. El problema contemporáneo es mucho más complejo: quién controla la capacidad generativa misma, quién gobierna los *datasets* que permiten la síntesis, quién determina las condiciones de visibilidad y monetización en ecosistemas algorítmicos donde la distribución obedece a lógicas opacas. El régimen clásico —fundamentado en la distinción entre derechos morales y patrimoniales, con remedios dispersos entre derecho civil, penal y constitucional—operaba bajo el supuesto implícito de que los usos no autorizados de la imagen son identificables, aislados y remediables *ex post* mediante indemnización. Pero cuando un modelo de IA puede generar infinitas variaciones de una *performance* a partir de un conjunto limitado de materiales fuente, y cuando esas generaciones circulan en plataformas cuya visibilidad se determina algorítmicamente, tres problemas estructurales emergen simultáneamente y se condicionan entre sí.

7.1 La arquitectura contractual como infraestructura de gobernanza

7.1.1 El desajuste entre texto y tecnología

Cualquier abogado que haya revisado contratos de imagen de la década de 1990 o incluso de principios de los 2000 habrá encontrado cláusulas del tipo "se autoriza el uso de imagen en todos los medios presentes y futuros, conocidos o por conocerse". En su momento, estas fórmulas amplias parecían razonables: protegían al productor contra la obsolescencia tecnológica sin exponer excesivamente al titular. Después de todo, con el material filmado se podía hacer "solo hasta cierto punto". La materialidad misma de la producción audiovisual —los costos de rodaje, edición, distribución— imponía restricciones fácticas a la explotación. Había un límite natural entre autorizar el uso de una imagen en una película y autorizar su transformación en algo completamente distinto.

Ese límite ha desaparecido. Con IA generativa y clones digitales, el mismo conjunto de materiales —quizás apenas unas horas de grabación de voz, algunos escaneos faciales, captura de movimientos de gestos característicos— puede alimentar réplicas prácticamente infinitas. No estamos hablando solo de usar la misma imagen en distintos formatos (del cine al *streaming*, de la televisión a las redes sociales), sino de generar *performances* completamente nuevas que el artista nunca ejecutó, en contextos que nunca imaginó, para propósitos que pueden ir desde el homenaje respetuoso hasta la manipulación política o el fraude comercial. Preminger y Kugler (2024) sostienen convincentemente que esto exige nuevos cánones interpretativos y un rediseño contractual profundo. La alternativa es que licencias redactadas para otra era se conviertan en habilitaciones de facto para *deepfakes* sin que el titular pueda invocar vicios del consentimiento basándose en la imprevisibilidad del uso concreto.

Esta desconexión entre texto contractual y capacidad técnica genera un doble problema que va más allá de lo puramente jurídico. Por un lado, crea inseguridad para ambas partes: el licenciatario no sabe hasta dónde puede llegar sin exponerse a litigio, y el titular descubre tardíamente que autorizó mucho más de lo que creía. Por otro lado, y quizás más importante, transforma cada licencia amplia en una bomba de tiempo litigiosa. La ausencia de especificación

granular sobre qué rasgos se licencian, para qué finalidades, con qué nivel de fidelidad y bajo qué controles creativos no solo complica la interpretación judicial *ex post*, también frustra la posibilidad misma de una gestión eficiente *ex ante*. El problema, entonces, no reside únicamente en el derecho sustantivo aplicable —aunque ese sea relevante—, sino además en la arquitectura misma de las licencias. Necesitamos contratos que operen como sistemas de gobernanza preventiva, no como documentos que meramente registran una transferencia de derechos cuyo alcance real solo se descubre en el litigio.

7.1.2 De la autorización global al control granular

La propuesta de licencias modulares no es un refinamiento estilístico ni un ejercicio de pedantería contractual, responde a la necesidad práctica de crear puntos de control verificables a lo largo de la cadena de valor generativa. Cuando Samuelson (2025) analiza la factibilidad de licenciamiento colectivo para *training data* en IA, identifica que el problema central no es de derecho sustantivo, sino de transacción, trazabilidad y diseño institucional. Esa misma lógica se aplica con mayor razón al *likeness*, donde el control no es solo patrimonial, sino también moral y reputacional. Un contrato defendible para imagen, voz y *performance* en contexto de IA debe estructurarse como sistema modular, donde cada módulo posee su propia lógica jurídica y sus propios remedios.

Empecemos por lo más básico: la definición del objeto licenciado. No basta la fórmula genérica "imagen y voz", que podría significar casi cualquier cosa. Se requiere especificar con precisión operacional los rasgos que se autorizan a reproducir sintéticamente: rasgos faciales estáticos y dinámicos (incluyendo expresiones características), timbre vocal y patrones prosódicos, nombre artístico o seudónimo y características performativas dinámicas como gestos, rasgos, tiempos interpretativos. Para intérpretes profesionales que puedan invocar derechos conexos, la *performance* misma debe tratarse como objeto autónomo. La clave metodológica consiste en abandonar definiciones "románticas" del tipo "se autoriza el uso de imagen" y pasar a definiciones operacionales: "se autoriza la generación de *outputs*

sintéticos que reproduzcan los siguientes rasgos específicos con el siguiente nivel de fidelidad técnica medible".

Esta especificidad no es capricho formalista. Determina *ex post* si un uso concreto está dentro o fuera del perímetro autorizado, lo cual es crucial cuando el titular quiere ejercer *takedown* o cuando el licenciatario necesita defender su actuación como legítima. Más importante aún, permite escalonar permisos y precios: baja fidelidad versus alta fidelidad, usos internos versus públicos, aplicaciones comerciales versus archivo histórico. Sin esa granularidad, toda discusión sobre modelos de negocio más sofisticados —*revenue share*, *fee* por minuto de *output* generado, licencias limitadas temporalmente— queda bloqueada desde el inicio.

El segundo módulo debe diferenciarse claramente entre licencia de imagen tradicional (uso "estático" o de representación) y licencia de clon digital (uso "generativo" con continuidad de identidad performativa). En el caso de clones digitales, aparecen necesidades de control que simplemente no existían antes. El derecho de aprobación sobre categorías sensibles —política partidaria, contenido sexual, contextos difamatorios, fraude— ya no puede ser una declaración aspiracional que se menciona de paso en una cláusula, debe explicitarse: quién aprueba, en qué plazo, bajo qué estándar, qué sucede si hay desacuerdo. Los límites de contexto deben redactarse como *hard stops* técnicos cuando sea posible, no como meras intenciones que luego resultan imposibles de hacer cumplir. Y las restricciones de aval —prohibición de sugerir patrocinio o aval comercial no autorizado— conectan directamente con remedios de *passing off* y competencia desleal que pueden resultar más eficaces que las acciones tradicionales de derecho de la personalidad.

Pero quizás el aspecto más descuidado en la práctica contractual actual es el tratamiento del entrenamiento de modelos. El error típico consiste en tratarlo como un apéndice de "medios de explotación", cuando en realidad constituye un uso autónomo con implicaciones económicas y de control enormes. La literatura sobre AI *training data* insiste en especificar: finalidad del entrenamiento (¿para qué modelo específico?), quién entrena (¿el licenciatario directo o terceros subcontratados?), si hay *fine-tuning* posterior, si hay reutilización del modelo para beneficio de terceros no contemplados

originalmente y qué sucede con el modelo si se revoca o termina el vínculo contractual. En ausencia de estas especificaciones, el licenciatario puede argumentar —y tribunales han aceptado en otros contextos de IA— que el entrenamiento quedó autorizado implícitamente bajo cláusulas amplias y que el modelo resultante es de su propiedad exclusiva, incluso tras la terminación del contrato.

Esta cuestión adquiere relevancia crítica en casos de clones digitales de artistas fallecidos, tema que se retomará más adelante. Por ahora basta señalar que, si no puede demostrar que el entrenamiento del modelo original fue limitado en alcance y duración, enfrentará dificultades probatorias enormes para atacar usos generativos perpetuos basados en modelos "heredados" por el licenciatario. Por ello, el contrato debe incluir cláusulas sobre modelos entrenados, obligaciones de destrucción verificables y parámetros mediante procesos auditables y mecanismos de auditoría técnica periódica que no dependan de la buena voluntad del licenciatario.

Esto conecta directamente con desarrollos recientes en *proof of consent*, el contrato debe crear infraestructura de trazabilidad. Si el consentimiento no es auditable, se convierte inevitablemente en una discusión probatoria *ex post* que será cara, incierta y probablemente inútil para el titular. *Logs* y metadata mínimos sobre cada uso generativo, obligación de preservación de evidencia, *hashes* criptográficos o *timestamps* cuando se produzcan *outputs* y *flow-down terms* a subcontratistas y plataformas de distribución no son lujos técnicos, son condiciones mínimas para que el sistema funcione. El contrato debe especificar qué prueba es suficiente para acreditar autorización, en lugar de dejar esta cuestión a "políticas" unilaterales y cambiantes del licenciatario (Preminger y Kugler, 2024). Además, debe prever mecanismos de *takedown* rápido con *service level agreements* específicos: el licenciatario se obliga a retirar cualquier *output* no autorizado dentro de X horas de recibir notificación y a realizar esfuerzos razonables para eliminar copias en sistemas espejos y plataformas de terceros. Este tipo de cláusulas operativas no garantiza cumplimiento perfecto, pero crea responsabilidad contractual verificable y facilita *enforcement* posterior.

En síntesis, una arquitectura contractual modular para licencias de clon digital debe contemplar, como mínimo, seis módulos arti-

culados: (i) definición operacional del objeto licenciado, especificando rasgos faciales, vocales, prosódicos y performativos con niveles medibles de fidelidad; (ii) diferenciación explícita entre licencia de imagen tradicional y licencia de clon generativo, con derechos de aprobación sobre categorías sensibles y límites contextuales como *hard stops* técnicos cuando sea posible; (iii) régimen autónomo del entrenamiento de modelos, con finalidad, subcontratación, *fine-tuning*, reutilización y destino del modelo tras la terminación del contrato; (iv) infraestructura de trazabilidad y *proof of consent*, con *logs*, metadata, *hashes*, *timestamps* y *flow-down terms* a subcontratistas y plataformas; (v) remedios operativos rápidos mediante SLA de *take-down*, con plazos tasados y deberes de colaboración activa; y (vi) cláusulas de decaimiento temporal y renovación expresa que eviten la conversión silenciosa de una licencia específica en una habilitación perpetua.

7.1.3 La licencia de clon como objeto económico distinto

Vale la pena detenerse en la economía política de los clones digitales, porque ahí reside uno de los *insights* más importantes para entender por qué las licencias tradicionales no funcionan. Una licencia de clon digital no es simplemente una licencia de imagen más amplia, es un objeto contractual cualitativamente distinto con su propia lógica económica. Su especificidad deriva de que no solo licencia rasgos estáticos (rostro, voz), sino también *performance style* (ritmo interpretativo, entonación, gestualidad), lo que genera continuidad de identidad performativa sintética. El control creativo no se ejerce únicamente sobre el video final, sino sobre *prompt families* o familias de instrucciones generativas que definen el espacio de generación posible. Y la estructura económica migra desde *fee* por sesión —modelo que funcionaba cuando cada uso requería nueva contratación del artista— hacia *revenue share*, *fee* por minuto de *output*, o licencias escalonadas según fidelidad y tipo de uso.

El punto económico central es brutal en su simplicidad: si la licencia de clon es barata y amplia, el intérprete está financiando su propia sustitución. Una vez que el licenciatario posee un clon de alta fidelidad sin restricciones temporales ni contextuales, el incentivo

económico de contratar nuevamente al intérprete original desaparece por completo. ¿Para qué pagar las tarifas actuales de un actor conocido, con todas las complejidades logísticas que implica (agenda, equipo, locaciones), cuando se pueden generar *performances* sintéticas indistinguibles a costo marginal prácticamente cero? Este no es un escenario hipotético de ciencia ficción; ya está sucediendo en doblaje, en ciertas formas de publicidad. La licencia de clon, entonces, debe estructurarse entendiendo que lo que se está licenciando no es solo un derecho de uso, sino también potencialmente la capacidad del artista de seguir generando ingresos futuros en su campo.

Esto nos lleva a una pregunta más amplia sobre gestión individual versus colectiva. No todos los aspectos del *likeness* convienen ser colectivizados, y aquí hay que ser finos en el análisis. La identidad fuerte —clon digital, alto riesgo moral y reputacional— tiende a requerir gestión individual: control creativo personalizado, límites contextuales específicos, revocación rápida, auditoría directa. En cambio, usos masivos y fragmentados (ciertos usos secundarios, remuneraciones de gran escala derivadas de *streaming*) pueden justificar mecanismos colectivos de licenciamiento. Samuelson (2025) muestra que en el contexto de *training data*, el problema central no es de derecho sustantivo, sino de transacción, trazabilidad y diseño institucional. Esa lógica es trasladable al mundo del intérprete para usos masivos, aunque con ajustes importantes. Pero el clon y la identidad "fuerte" probablemente deben quedar fuera del esquema colectivo, precisamente porque requieren decisiones caso por caso sobre contextos sensibles —política, sexualidad, entre otros— que no admiten estandarización sin riesgo de sobreinclusión o subinclusión.

Por último, los remedios. En casos de *deepfakes* y clones no autorizados, el remedio monetario tradicional suele llegar tarde: cuando el daño reputacional ya se consumó, cuando la confusión en el mercado ya se instaló, cuando el video viral ya circuló por millones de dispositivos. Por eso, un contrato bien diseñado prioriza remedios operativos que puedan ejecutarse rápidamente.

8. La paradoja de la visibilidad algorítmica

8.1 Cuando tener derechos no es suficiente

La literatura inicial —señalada en este artículo— sobre *deepfakes* comprensiblemente se concentró en el problema más evidente: la suplantación, un video falso que se hace pasar por auténtico, generando daño reputacional directo o posibilitando fraude. Las discusiones jurídicas y los proyectos legislativos se enfocaron en crear remedios contra estos usos maliciosos, lo cual era necesario, pero insuficiente. Porque en ecosistemas de plataformas con distribución algorítmica emerge un problema estructuralmente distinto que a menudo pasa desapercibido: incluso cuando el artista posee derechos formalmente intactos y los clones están debidamente identificados como sintéticos —cumpliendo con eventuales obligaciones de transparencia—, el intérprete original puede ser desplazado por pura lógica de distribución.

Este desplazamiento no deriva de una violación de derechos en sentido tradicional. No hay apropiación indebida ni uso no autorizado. Hay algo más sutil y quizás más peligroso: una dinámica de mercado mediada por algoritmos de recomendación que sistemáticamente favorece cierto tipo de contenido sobre otro, independientemente de su origen humano o sintético (Gozalbez y Lehtinen, 2025). Para entender esto, necesitamos alejarnos de narrativas conspirativas sobre algoritmos diseñados maliciosamente para perjudicar a artistas humanos y observar tres mecanismos empíricamente identificables que operan sin necesidad de intención maliciosa.

El primero es la saturación y dilución de atención. Los clones aumentan la oferta de contenido que compite por la misma audiencia, reduciendo matemáticamente las tasas de descubrimiento del intérprete original. Si un usuario busca "*performances* de [artista X]", el algoritmo puede *rankear* contenido sintético por encima del auténtico basándose en métricas de *engagement* reciente, sin considerar autenticidad como factor relevante. Desde la perspectiva del algoritmo, ambos son simplemente contenido relacionado con la *query*; el que tiene mejor *performance* en retención o *click-through rate* sube en el *ranking*. Esto no requiere sesgo antihumano, es simplemente optimización ciega sobre métricas.

El segundo mecanismo es la optimización de métricas. El contenido sintético puede ajustarse iterativamente para maximizar re-

tención, *click-through rate* o tiempo de visualización de modo más eficiente que una producción humana orgánica. Los modelos generativos pueden iterar rápidamente sobre variaciones —diferentes reproducciones en los primeros cinco segundos, diferentes duraciones, diferentes estilos de edición— y converger hacia la combinación que mejor *performance* tiene según las métricas que la plataforma prioriza. El intérprete humano, en cambio, está limitado por costos de producción, tiempo disponible y, quizás más importante, por el hecho de que su *performance* refleja decisiones artísticas que no necesariamente coinciden con lo que maximiza el *engagement* medido en segundos de atención.

El tercer mecanismo es la gestión de visibilidad. Horten (2022) ha estudiado empíricamente este fenómeno y lo conceptualiza como una forma de supresión de distribución con impacto relevante en libertad de expresión y garantías procedimentales. Aunque estos mecanismos suelen asociarse con moderación de contenido político o desinformación, pueden aplicarse también a intérpretes humanos cuyos contenidos se categorizan algorítmicamente como "menos relevantes" comparados con *outputs* sintéticos optimizados. La característica distintiva de estas sanciones es que son invisibles o semivisibles: reducen alcance sin remover contenido, sin notificación explícita, sin posibilidad real de apelación. El artista puede tener todos sus derechos intactos, pero si su contenido simplemente no llega a audiencias porque el algoritmo lo ha categorizado en un rango inferior de distribución, esos derechos pierden gran parte de su valor práctico.

En síntesis, tres mecanismos acumulativos producen el desplazamiento del intérprete humano sin que exista violación tradicional de derechos: (i) saturación y dilución de atención, por multiplicación matemática de la oferta sintética que compite por la misma audiencia; (ii) optimización iterativa de métricas por contenido sintético, que converge más rápido hacia lo que maximiza *engagement* que una producción humana orgánica; y (iii) gestión invisible de visibilidad, donde el contenido humano es silenciosamente degradado en el *ranking* sin notificación ni apelación. El daño resultante no es apropiación del *likeness*, sino exclusión del mercado de atención y, por ello, reclama instrumentos jurídicos distintos de los tradicionalmente disponibles para el derecho de la personalidad.

8.2 *Fairness* algorítmica y los límites del derecho antidiscriminatorio

¿Cómo articular jurídicamente este problema? La tentación inmediata es recurrir al lenguaje de *fairness* algorítmica y discriminación, pero aquí debemos ser cuidadosos. Nachbar (2021) propone entender *algorithmic fairness* dentro del marco del derecho antidiscriminatorio, pero advierte crucialmente que funciona como *side constraint* —límite mínimo de lo intolerable— y no como utopía de justicia total. Keswani y Celis (2024) profundizan esta idea mostrando que principios antidiscriminatorios pueden operar como marco normativo para auditoría y remedios, aunque no resuelvan todos los problemas de equidad algorítmica. Por su parte, Wachter et al. (2020) agregan el punto quizás más importante para nuestro análisis: no todo lo "injusto" es automatizable como "discriminación" en sentido jurídico estricto, porque el derecho —especialmente en Europa— es contextual, basado en categorías protegidas específicas, y no siempre traducible a métricas fijas que un sistema automatizado pueda implementar.

La traducción operativa para artistas e intérpretes es que el daño por exclusión algorítmica muchas veces no podrá probarse como "discriminación" en sentido estricto. "Intérprete humano" no es categoría protegida bajo leyes antidiscriminatorias tradicionales, y demostrar que un algoritmo discrimina sistemáticamente contra contenido auténtico en favor de sintético requeriría acceso a datos internos que las plataformas no proporcionan voluntariamente. Sin embargo, el daño puede articularse jurídicamente por otras vías que merecen exploración seria.

Primero, incumplimiento de deberes de transparencia y procedimiento según regímenes aplicables. La Digital Services Act (DSA) en la Unión Europea, por ejemplo, impone obligaciones específicas de transparencia sobre sistemas de recomendación para plataformas de muy gran tamaño. Si una plataforma no divulga adecuadamente cómo funciona su *ranking* o si los parámetros principales de recomendación son deliberadamente opacos, puede haber base para reclamación por incumplimiento regulatorio independientemente de si existe "discriminación" en sentido técnico.

Segundo, competencia desleal o *passing off* si hay confusión comercial entre intérprete auténtico y clones. Esto requiere probar

que consumidores razonables se confunden sobre el origen del contenido, lo cual puede ser difícil si hay *disclosure* adecuado, pero no imposible si la *disclosure* es insuficiente o está enterrada en lugares donde usuarios no la ven.

Tercero, abuso de poder de intermediación si la plataforma posee posición dominante o actúa como *gatekeeper* en el sentido de la Digital Markets Act. Si puede demostrarse que la plataforma favorece sistemáticamente contenido sintético de ciertos proveedores comerciales sobre intérpretes independientes, puede haber base para reclamación por abuso de posición dominante o por violación de obligaciones de *gatekeeper*.

Cuarto, quizás el más interesante desde perspectiva teórica, violación de un "derecho a ser oído" (*right to be heard*) como dimensión infraestructural de participación cultural. Szkalej (2025) conceptualiza este derecho en el contexto de sistemas de recomendación musical, argumentando que el acceso a mercado cultural no es solo cuestión de monetización, sino también de participación en el espacio público cultural. Un artista que produce contenido de alta calidad, pero sistemáticamente es invisible en plataformas porque algoritmos favorecen contenido sintético optimizado, no solo pierde ingresos, pierde además la capacidad de participar efectivamente en el discurso cultural de su tiempo.

8.3 El problema de la transparencia cosmética

Todo esto choca con una realidad incómoda y que Bassan (2025) ha documentado cuidadosamente: incluso cuando hay reportes de transparencia sobre sistemas de recomendación, estos pueden convertirse en "teatro de *accountability*". *Data-dumping* selectivo que inunda con información genérica sin valor práctico. Divulgación de métricas diseñadas para cumplir formalmente con obligaciones legales sin permitir auditabilidad efectiva. Documentación técnica tan compleja que solo puede ser interpretada por especialistas que las plataformas contratan a precios prohibitivos. El problema no es ausencia de transparencia en sentido formal, es ausencia de transparencia accionable, transparencia que les permita a los afectados realmente entender qué está pasando y tomar decisiones informadas.

Esto refuerza el argumento desarrollado en el apartado anterior sobre los contratos: las cláusulas de auditoría deben ser específicas sobre qué datos tiene que preservar el licenciatario o la plataforma, en qué formato, con qué nivel de granularidad, quién tiene acceso y qué consecuencias se derivan del incumplimiento. Sin esta especificidad, la obligación de "transparencia" se vacía de contenido operativo y se convierte en una mera declaración de buenas intenciones. Los intérpretes necesitan poder auditar no solo si su contenido está siendo usado conforme a la licencia, sino también cómo está siendo distribuido, qué métricas determinan su visibilidad y si están siendo sistemáticamente desfavorecidos frente a contenido sintético competidor.

En términos prácticos, esto implica negociar contratos que incluyan no solo derechos de auditoría sobre el uso (¿se está usando mi *likeness* conforme a lo autorizado?), sino también sobre la distribución (¿cómo se está distribuyendo el contenido que usa mi *likeness*?, ¿qué *ranking* tiene?, ¿qué factores determinan ese *ranking*?). Y cuando hablamos de plataformas que operan como intermediarios necesarios para alcanzar audiencias —caso frecuente en música, video, ciertos segmentos de entretenimiento—, el poder de negociación individual del artista puede ser insuficiente. De ahí la importancia de una regulación que establezca pisos mínimos de transparencia algorítmica y auditabilidad, no como favor, sino como condición de operación en mercados culturales.

9. La muerte como punto de inflexión: legado digital y resurrección sintética

9.1 Regular los *inputs* antes que los *outputs*

El control del legado digital plantea preguntas que van más allá de la mera sucesión patrimonial. No se trata solo de determinar quién hereda derechos sobre obras preexistentes —problema relativamente resuelto—, sino también de gobernar los *inputs* que permiten reconstruir sintéticamente a la persona fallecida. *Datasets*, escaneos 3D, grabaciones de voz separadas por fonema, captura de movimientos característicos: estos materiales no son simplemente "obras" en sentido tradicional, son la materia prima que alimenta la posibi-

lidad misma de "resurrección" digital, de continuidad performativa *post mortem*.

Haneman (2024) ha propuesto la idea provocativa del *digital right to be dead*, ubicando el núcleo del conflicto en el uso de datos personales para recrear a alguien con apariencia, voz, emoción y hasta memoria sintética. Su argumento desplaza la discusión desde "¿qué derechos sobreviven a la muerte?" hacia "¿quién controla los materiales que posibilitan la continuidad digital de una identidad?". Esta perspectiva conecta con el concepto de *digital disinterment* —exhumación digital— que Cohen (2023) desarrolla: la IA generativa permite exhumar digitalmente a los muertos mediante síntesis de su identidad performativa a partir de materiales archivados.

Cohen (2023) argumenta convincentemente que el derecho existente puede quedar corto porque opera bajo el presupuesto de que los muertos no tienen intereses jurídicamente protegibles. Pero la "resurrección" digital afecta también a los vivos: herederos con interés legítimo en preservar la memoria, familiares que sufren daño emocional por usos indignos del *likeness*, comunidades de fans cuya relación con el artista incluye dimensiones de identidad colectiva. Y quizás más importante desde la perspectiva de incentivos es que afecta al propio artista en vida, cuyas decisiones sobre qué proyectos aceptar y qué materiales producir están inevitablemente influidas por expectativas sobre el control *post mortem*. Ya hay casos documentados de artistas que deliberadamente limitan la creación de ciertos registros digitales por preocupación sobre usos futuros. Desde una perspectiva de eficiencia económica y cultural, esto puede ser subóptimo: estamos potencialmente perdiendo obras y registros valiosos porque el régimen jurídico no ofrece garantías suficientes.

9.2 ¿Qué sobrevive y bajo qué reglas?

Sin entrar al detalle de cada jurisdicción, podemos establecer una taxonomía funcional. Los derechos patrimoniales tradicionales suelen ser transmisibles durante plazos que siguen la lógica de *copyright*. Los derechos morales presentan mayor heterogeneidad: en la tradición continental europea, tienden a subsistir perpetuamente; en el *common law*, pueden no transmitirse en absoluto o con limitaciones temporales importantes.

Pero para clones digitales *post mortem*, el vehículo jurídico más útil resulta ser el *right of publicity*. P'ng (2024) examina remedios frente a *deepfakes* póstumos y muestra por qué la apropiación indebida de *publicity* puede ser particularmente funcional: está orientada hacia el control de identidad comercial, no requiere demostrar daño moral (complicado cuando el afectado está muerto) y en varias jurisdicciones se extiende *post mortem* con plazos de hasta 70 o 100 años.

Tres desarrollos legislativos recientes ilustran esta tendencia. La Tennessee ELVIS Act (2024) amplía la protección del *right of publicity* para incluir expresamente voz, imagen y *likeness*, con énfasis en protección *post mortem* y remedios contra réplicas digitales no autorizadas —la elección del nombre no es casual: Tennessee es sede de la industria country y del legado Elvis Presley—. La New York Civil Rights Law § 50-f incluye definiciones de *digital replica* y reglas sobre uso comercial de identidad de personas vivas o fallecidas. Por su parte, el California Civil Code § 3344, aunque anterior a la ola reciente de *deepfakes*, sigue siendo referencia central con jurisprudencia que ha interpretado extensivamente sus disposiciones para cubrir usos digitales.

Particularmente interesante es el modelo danés, analizado por el European Parliamentary Research Service (2026), que propone tratar voz, imagen y cuerpo bajo una lógica análoga al *copyright*: derechos exclusivos, licencias transferibles y activación de mecanismos de moderación bajo la DSA. Este enfoque tiene tres ventajas estructurales: reduce fragmentación entre regímenes tradicionalmente separados; al asimilar *likeness* a *copyright*, activa infraestructura ya existente (*notice-and-takedown*, registros, cadenas de título); y facilita interoperabilidad con la DSA, permitiendo *enforcement* mediante obligaciones que las plataformas ya tienen.

9.3 El paquete de legado: herramientas concretas

Teoría jurídica aparte, ¿qué debería hacer concretamente un artista que quiere asegurar el control sobre su identidad digital *post mortem*? Un paquete mínimamente serio requiere varios instrumentos integrados.

Primero, una directiva de identidad o testamento digital que especifique con claridad: *opt-in* condicionado u *opt-out* total frente a

usos generativos *post mortem*, límites de contexto específicos (política partidaria, contenido sexual, *endorsement* comercial no autorizado en vida), categorías de uso permitido (homenaje, archivo histórico, documental educativo) y estándar probatorio para invocar excepciones de *fair use*. Este documento debe redactarse con lenguaje jurídicamente vinculante, no como una carta de intenciones, e integrarse formalmente al testamento o *trust* principal.

Segundo, un mandatario de identidad (*identity executor*). Puede ser una persona física o un comité, con poder específico de aprobación sobre usos del *likeness post mortem*, facultad de ejercer *takedown*, acceso a *logs* y metadata de explotación, y facultad para contratar auditores técnicos independientes. En ausencia de designación expresa, la ley suele asignarle estos poderes al cónyuge o herederos según orden sucesorio, pero esa asignación por defecto puede generar conflictos serios —piénsese en hijos de distintos matrimonios o herederos que priorizan la preservación artística frente a quienes buscan maximizar ingresos a corto plazo—. La designación expresa con criterios claros previene litigios que terminan dilapidando el valor mismo que intentan proteger.

Tercero, un anexo contractual sobre clones *post mortem* en todos los contratos de licencia relevantes firmados en vida: ¿las licencias terminan automáticamente al fallecimiento?, ¿continúan por un plazo determinado?, ¿se renegocian con el heredero?, ¿qué usos de homenaje o de archivo se permiten sin autorización previa del *estate* y bajo qué estándar probatorio? Sin esta especificidad, cada uso *post mortem* genera un litigio interpretativo costoso donde nadie gana, excepto los abogados.

Cuarto, quizás el más práctico, pero frecuentemente descuidado: inventario exhaustivo de materiales fuente. Lista completa de *assets* digitales —escaneos faciales 3D, grabaciones de voz, *motion captures*, fotografías, video en bruto— con información sobre dónde está almacenado cada activo, quién tiene acceso, cómo puede usarse legítimamente, cómo se audita su uso y qué obligaciones de destrucción existen tras la finalización de licencias. La ausencia de inventario convierte el *enforcement post mortem* en un ejercicio especulativo: el *estate* no sabe qué materiales existen, quién los posee ni cómo probar que un clon específico deriva de ellos. Un licenciatario ines-

crupuloso puede simplemente negar que está usando materiales del artista fallecido, y sin inventario detallado más pruebas de *fingerprinting* o *watermarking*, demostrar lo contrario puede ser imposible. El inventario no es un formalismo administrativo, es infraestructura probatoria esencial que debe actualizarse periódicamente mientras el artista está vivo.

10. La tensión con libertad de expresión, parodia y derecho a la información

El arco argumental recorrido hasta aquí —régimen sustantivo insuficiente, arquitectura contractual como gobernanza, visibilidad algorítmica, legado *post mortem* e infraestructura probatoria— converge en una propuesta que, al trasladar la lógica del *copyright* al terreno de la identidad personal, es particularmente vulnerable en un punto: su colisión con la libertad de expresión, la parodia y el derecho a la información. En este apartado se desarrolla ese punto con la misma profundidad que los ejes anteriores, porque de su resolución depende que la propuesta sea viable como política pública y no un instrumento de censura privada sobre figuras públicas. Tres preguntas estructuran el análisis: cómo distinguir la parodia legítima del *deepfake* ilícito, quién determina cuándo un clon es homenaje y cuándo es apropiación y cuáles son las consecuencias de proteger por plazos muy largos la identidad de los intérpretes. La respuesta a estas tres preguntas se articula, respectivamente, en un test sustantivo de cuatro factores, un sistema escalonado de filtros institucionales y un régimen de plazos decrecientes. La Figura 1 sintetiza gráficamente cómo operan juntos los tres elementos.

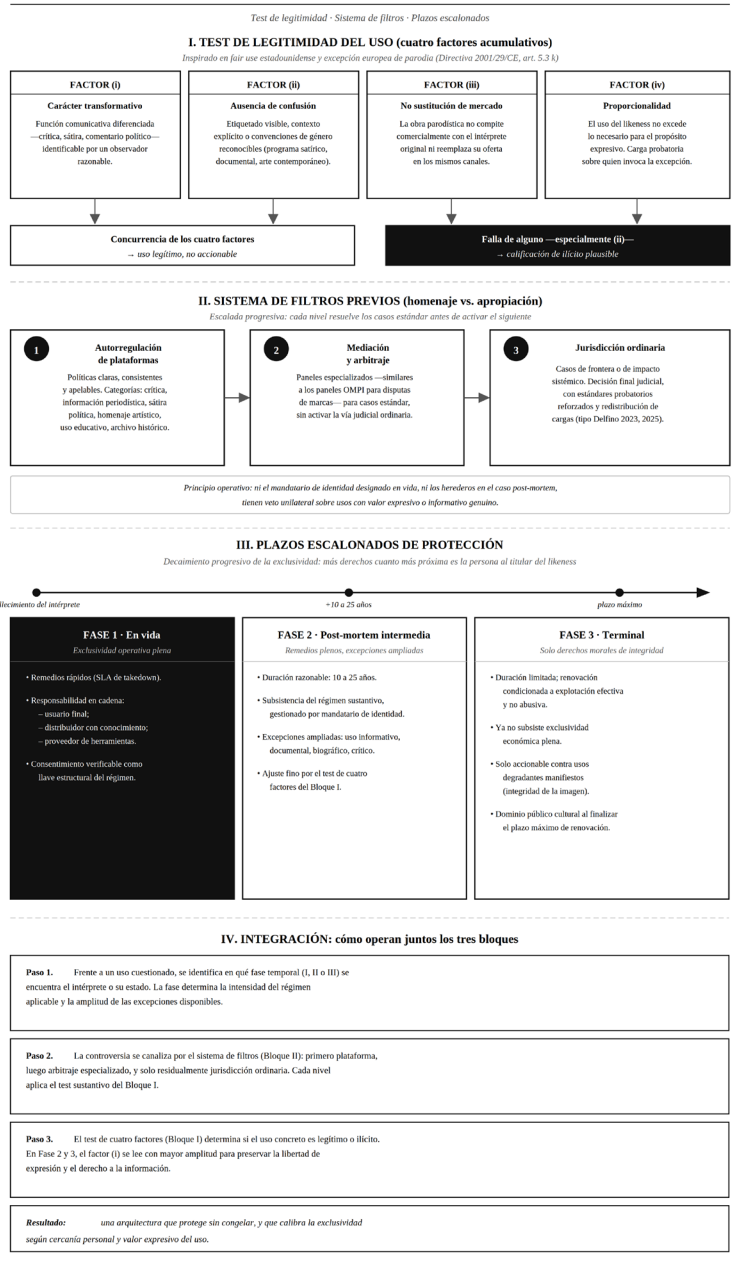

Figura 1. Arquitectura integrada del régimen de réplicas digitales: test de legitimidad, sistema de filtros y plazos escalonados. Fuente: elaboración propia.

10.1 Test sustantivo: cuatro factores para distinguir parodia legítima de *deepfake* ilícito

La doctrina del *fair use* estadounidense y la excepción europea de parodia (Directiva 2001/29/CE, art. 5.3.k) aportan criterios que, con ajustes, pueden trasladarse al clon digital. Cuatro factores resultan especialmente operativos y deben concurrir de modo acumulativo para que el uso sea legítimo. El primero es el carácter transformativo, entendido como función comunicativa diferenciada —crítica, sátira, comentario político— claramente identificable por un observador razonable. El segundo es la ausencia de confusión de fuente, verificable mediante etiquetado visible, contexto explícito o convenciones de género (un programa satírico, un documental, una obra de arte contemporánea). El tercero es la no sustitución de mercado, es decir, que la parodia no compita comercialmente con el intérprete original ni reemplace su oferta en los mismos canales. Y el cuarto es la proporcionalidad, en el sentido de que el uso del *likeness* no exceda lo necesario para el propósito expresivo.

Cuando los cuatro factores concurren, el *deepfake* no debería ser accionable aun bajo un régimen exclusivo. Cuando alguno falla —especialmente el segundo, confusión de fuente—, la calificación de ilícito se vuelve plausible. La carga de la prueba sobre el carácter paródico debe recaer sobre quien invoca la excepción, pero bajo un estándar razonable que no exija condiciones imposibles de cumplir. El test no pretende mecanizar lo que en última instancia es una ponderación contextual, pretende ofrecerle al juzgador —sea plataforma, árbitro o tribunal— un marco consistente para ordenar la discusión y reducir la imprevisibilidad que el estándar contextual puro genera.

10.2 Sistema de filtros: tres niveles institucionales entre homenaje y apropiación

La decisión final sobre si un clon es homenaje o apropiación es necesariamente judicial, pero el sistema no puede descansar exclusivamente en el litigio caso por caso sin colapsar. Tres niveles de filtro previo resultan indispensables y operan en escalada: cada uno resuelve los casos estándar antes de activar el siguiente, y sólo los casos de frontera llegan hasta el último.

En el primer nivel, la autorregulación de plataformas mediante políticas claras, consistentes y apelables que distingan categorías de uso: crítica e información periodística, sátira política, homenaje artístico declarado, uso educativo o archivo histórico. Estas políticas son el filtro cotidiano y masivo: deciden millones de casos al día sin intervención externa. Su legitimidad depende de que sean transparentes, coherentes en el tiempo y susceptibles de apelación efectiva ante un órgano interno cualificado.

En el segundo nivel, mecanismos de mediación y arbitraje especializado —similares a los paneles de la Organización Mundial de la Propiedad Intelectual (OMPI) para disputas de marcas— que resuelvan casos estándar sin activar la vía judicial ordinaria. Este nivel absorbe los casos en que la decisión de plataforma es cuestionada pero no involucra una controversia jurídica de fondo novedosa. Su ventaja es doble: celeridad y especialización técnica, dos condiciones que la justicia ordinaria difícilmente reúne en materia de réplicas digitales.

En el tercer nivel, jurisdicción ordinaria para los casos de frontera o de impacto sistémico, con estándares probatorios reforzados y redistribución de cargas en la línea de las propuestas de Delfino (2023, 2025). Aquí se deciden las cuestiones que crean doctrina, que fijan criterios para los niveles inferiores y que involucran derechos constitucionales en tensión.

Un principio operativo atraviesa los tres niveles: ni el mandatario de identidad designado en vida ni los herederos en el caso *post mortem* tienen veto unilateral sobre usos con valor expresivo o informativo genuino. La lógica del *copyright* trae consigo el riesgo de una censura privada sobre figuras públicas, y el derecho a la información exige que la decisión final no quede enteramente en manos del titular del derecho exclusivo. Sin este principio, el régimen propuesto degeneraría en una herramienta de silenciamiento selectivo.

10.3 Plazos escalonados: decaimiento progresivo de la exclusividad

Proteger la identidad de los intérpretes por plazos muy largos, a imagen del *copyright* (hasta setenta o cien años *post mortem* en algunas

propuestas), conlleva riesgos reales y conocidos: congelamiento del discurso público sobre figuras históricas, encarecimiento del trabajo documental y biográfico, consolidación de rentas en manos de *estates* sin conexión real con la persona fallecida y extensión del *chilling effect* sobre expresiones legítimas por temor a litigio. Estos riesgos son los mismos que el debate sobre la extensión del *copyright* ha documentado durante décadas y no hay razón para creer que se comportarán mejor en el terreno de la identidad personal.

La propuesta razonable es un régimen de plazos escalonados, no uniforme, con tres fases claramente diferenciadas. La primera, durante la vida del intérprete, con exclusividad operativa plena: remedios rápidos mediante SLA[13] de *takedown*, responsabilidad en cadena (usuario final, distribuidor con conocimiento, proveedor de herramientas) y consentimiento verificable como llave estructural del régimen. La segunda fase, intermedia *post mortem*, de duración razonable —entre diez y veinticinco años— con subsistencia del régimen sustantivo gestionado por el mandatario de identidad designado en vida (o, en su defecto, por los herederos bajo reglas supletorias), pero con excepciones ampliadas para uso informativo, documental, biográfico y crítico. Y una tercera fase, terminal, de duración limitada y con renovación condicionada a explotación efectiva y no abusiva, en la que sólo subsistan derechos morales de integridad contra usos degradantes manifiestos, cediendo la exclusividad económica al dominio público cultural.

Este diseño imita la lógica de decaimiento progresivo que el propio *copyright* ha adoptado —aunque con plazos demasiado largos— y corrige sus principales desviaciones aplicadas al terreno de la identidad personal. El riesgo de sobreprotección es real, pero también lo es el de subprotección: un régimen que no logre proteger a los intérpretes vivos frente a la suplantación sistemática equivale, en la práctica, a legalizar la apropiación. El equilibrio no se alcanza me-

13 Service Level Agreement (Acuerdo de Nivel de Servicio): contrato o cláusula contractual que establece los estándares de desempeño exigibles a un prestador de servicios, incluyendo plazos máximos de respuesta o cumplimiento. En el contexto de regímenes de *takedown*, un SLA fija el tiempo máximo dentro del cual la plataforma o el proveedor debe retirar el contenido notificado.

diante una regla única, sino a través de la combinación de remedios rápidos contra usos claramente ilícitos, excepciones robustas y previsibles para usos expresivos legítimos y plazos *post mortem* razonables que eviten la perpetuación indefinida del control privado sobre figuras que ya pertenecen a la historia cultural colectiva.

10.4 Integración gráfica de los tres elementos

La Figura 1 sintetiza la arquitectura propuesta. El test sustantivo de cuatro factores (bloque I) opera como criterio material de legitimidad del uso concreto. El sistema de filtros (bloque II) define quién aplica ese criterio y en qué orden escalonado. Los plazos escalonados (bloque III) calibran la intensidad del régimen según la proximidad temporal entre el uso cuestionado y la persona titular del *likeness*. El bloque de integración (IV) describe cómo funcionan juntos los tres elementos: frente a un uso cuestionado, se identifica primero la fase temporal aplicable, se canaliza la controversia por el sistema de filtros y, en cada nivel, se aplica el test sustantivo con la amplitud que la fase temporal autoriza. El resultado es una arquitectura que protege sin congelar y que calibra la exclusividad según la cercanía personal y el valor expresivo del uso.

11. Conclusión

El análisis desarrollado a lo largo de este trabajo permite concluir que hay una transformación estructural en la protección de la identidad performativa, no susceptible de ajustes menores. La tesis central que articula el artículo se confirma: la protección jurídica de artistas e intérpretes frente a la IA generativa requiere migrar de un modelo basado en derechos dispersos aplicados *ex post* hacia una arquitectura integrada de gobernanza *ex ante* que reconozca la réplica digital como categoría autónoma y combine, de modo inseparable, cuatro capas —arquitectura contractual modular, régimen de visibilidad algorítmica, gobernanza del legado *post mortem* e infraestructura probatoria transversal—, calibrada mediante un test sustantivo, un sistema de filtros y plazos escalonados que resuelven la tensión con libertad de expresión y derecho a la información.

De este marco integrado se derivan, de modo sistemático, ocho recomendaciones normativas y prácticas que articulan la propuesta regulatoria. Las tres primeras corresponden al plano legislativo sustantivo: primero, reconocer legislativamente la réplica digital como categoría jurídica autónoma, con una definición tecnológicamente neutra que abarque voz, rasgos faciales, gestualidad y patrones performativos y que no dependa de que haya existido captura previa del sujeto; segundo, adoptar plazos escalonados de protección —vida del intérprete con exclusividad operativa, fase intermedia *post mortem* corta (entre diez y veinticinco años) con remedios plenos y excepciones ampliadas y fase terminal con sólo derechos morales de integridad— junto con excepciones robustas para parodia, crítica, documental, archivo histórico y uso informativo, con carga probatoria razonable sobre quien invoca la excepción; tercero, establecer responsabilidad en cadena que alcance no sólo al usuario final, sino también a distribuidores con conocimiento y a proveedores de herramientas cuyo propósito principal sea producir réplicas no autorizadas, siguiendo la arquitectura de la ELVIS Act, pero corrigiendo su laguna probatoria mediante estándares técnicos de verificación.

Las tres siguientes corresponden a la arquitectura contractual y de gobernanza: cuarto, consagrar pisos mínimos imperativos en los contratos de licencia de clon —descripción específica de usos autorizados, duración limitada con renovación expresa, cláusulas separadas sobre entrenamiento de modelos con obligaciones de destrucción verificables, asistencia jurídica o sindical obligatoria para el intérprete y prohibición de cláusulas genéricas del tipo "todos los usos presentes y futuros" aplicadas a réplicas digitales—; quinto, imponerles a las plataformas de muy gran tamaño deberes operativos de transparencia algorítmica accionable —no meramente formal— sobre los parámetros que determinan la visibilidad del contenido de intérpretes humanos frente a contenido sintético, con mecanismos de auditoría externa y derechos procedimentales de apelación para artistas afectados; sexto, integrar al ordenamiento sucesorio la directiva de identidad digital como figura típica, con designación de mandatario de identidad, un inventario obligatorio de materiales fuente en el caso de intérpretes con explotación comercial significativa, y reglas supletorias razonables para los supuestos en que no haya disposición expresa.

Las dos últimas corresponden a la infraestructura probatoria y de *enforcement*: séptimo, mandatar estándares técnicos interoperables de *provenance* y consentimiento verificable (tipo C2PA), con integración jurídica de la metadata firmada como medio de prueba admisible y reglas claras de cadena de custodia digital que redistribuyan la carga probatoria cuando existan indicios razonables de fabricación sintética; octavo, complementar el régimen sustantivo con mecanismos institucionales de resolución de controversias —paneles de mediación y arbitraje especializado, autoridades administrativas con facultades de remoción expeditiva bajo estándares tasados— que aligeren la carga del intérprete individual y eviten que el ejercicio efectivo del derecho quede condicionado a la capacidad económica de litigar.

La migración hacia una *copyright-like personality* no es moda académica, sino una respuesta pragmática al vacío que la fragmentación normativa deja cubierto sólo a medias. Requiere desarrollo normativo coordinado, jurisprudencia que refine principios y soluciones técnicas de *proof of consent* sin costos prohibitivos. El camino no será sencillo: las tecnologías evolucionan más rápido que los ciclos legislativos y los intereses generan conflictos distributivos genuinos. Pero cada día sin marcos adecuados, más artistas firman contratos que no entienden, más clones circulan sin consentimiento, más valor se captura sin compensación justa. La ventana se está cerrando.

Bibliografía

Abbas, F. y Taeihagh, A. (2024). Unmasking deepfakes: A systematic review of deepfake detection and generation techniques using artificial intelligence. *Expert Systems with Applications, 252*, 124260. https://doi.org/10.1016/j.eswa.2024.124260 https://linkinghub.elsevier.com/retrieve/pii/S0957417424011266

Arık, S. Ö., Chen, J., Peng, K., Ping, W. y Zhou, Y. (2018). N*eural voice cloning with a few samples*. Proceedings of the 32nd Conference on Neural Information Processing Systems (NeurIPS 2018). https://arxiv.org/abs/1802.06006

Azzuni, H. y El Saddik, A. (2025). Voice cloning: Comprehensive survey. *arXiv.* https://arxiv.org/abs/2505.00579

Bassan, S. (2025). *Transparency ≠ accountability? Rethinking voluntary vs. mandatory content moderation reports*. SSRN. https://ssrn.com/abstract=5143075

Bracha, O. (2024a). Generating derivatives: AI and copyright's most troublesome right. *North Carolina Journal of Law & Technology*, *25*(3), 345-398. https://scholarship.law.unc.edu/ncjolt/vol25/iss3/2

Bracha, O. (2024b). The work of copyright in the age of machine production. *Harvard Journal of Law & Technology*, *38*(1), 171-226. https://jolt.law.harvard.edu/assets/articlePDFs/v38/4-Bracha.pdf

California Assembly Privacy and Consumer Protection Committee. (2024*). AB 2602, Kalra. Contracts against public policy: personal or professional services: digital replicas*. California State Legislature. https://apcp.assembly.ca.gov/system/files/2024-04/ab-2602-kalra-apcp-analysis.pdf

Chandra, B., Dunietz, J. y Roberts, K. (2024). *Reducing risks posed by synthetic content: An overview of technical approaches to digital content transparency (NIST AI 100-4)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-4

Chesney, R. y Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753-1820. https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security

Coalition for Content Provenance and Authenticity. (2025). *C2PA specifications (v2.3)*. https://c2pa.org/specifications/specifications/2.3/index.html

Cohen, G. (2023). Digital purgatory and the rights of the dead: Protecting against digital disinterment in the age of artificial intelligence. *Cardozo Law Review De Novo, 121*. SSRN. https://ssrn.com/abstract=4620092

CyberPeace Foundation. (22 de julio de 2025). *Watermarking standards and policy for AI-generated media*. https://cyberpeace.org/resources/blogs/watermarking-standards-and-policy-for-ai-generated-media

Davis Wright Tremaine LLP. (2025). *Lights, camera, legislation: Are your entertainment contracts ready for the spotlight?* Inside Tech Law. https://www.dwt.com/insights/2025/03/state-laws-regulating-ai-in-entertainment-industry

Delfino, R. A. (2023). Deepfakes on trial: A call to expand the trial judge's gatekeeping role to protect legal proceedings from technological fakery. *UC Hastings Law Journal, 74*(2), 313-381.

Delfino, R. A. (2025). *Deepfakes on trial 2.0: A revised proposal for a new federal rule of evidence to mitigate deepfake deceptions in court*. Loyola Law School Legal Studies Research Paper No. 2025-10. https://ssrn.com/abstract=5188767

Denmark to tackle deepfakes by giving people copyright to their own features. (27 de junio de 2025). The Guardian. https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence

Dixon, H. B., Jr. (2024). The "deepfake defense": An evidentiary conundrum. *Judges' Journal, 63*(2). https://www.americanbar.org/groups/judicial/resources/judges-journal/2024-spring/deepfake-defense-evidentiary-conundrum/

European Commission. (17 de diciembre de 2025). *First draft: Code of Practice on transparency of AI-generated content*. EU AI Office. https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content

European Parliament & Council. (2024). Regulation (EU) 2024/1689 on artificial intelligence (AI Act), Article 50. Official Journal of the European Union, L 2024/1689. https://artificialintelligenceact.eu/article/50/

European Parliamentary Research Service. (2026). The Danish approach to copyright and deepfakes: A model for the EU? https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA%282026%29782611

Gervais, D. (2015). *The protection of performers under U.S. law in comparative perspective*. *IP Theory, 5*(1), Article 8. https://ssrn.com/abstract=2700919

Gozalbez, R. J. y Lehtinen, L. M. (2025). *Revolución digital y propiedad intelectual: El desafío del derecho de autor en la era de la puesta a disposición*. Tirant lo Blanch

Haneman, V. J. (2024). *The law of digital resurrection*. *B.C. L. Rev. __ (forthcoming 2025)*. https://ssrn.com/abstract=4899324

HeyGen. (s.f.-a). *AI and ethics: Responsible AI video creation*. https://www.heygen.com/ethics

HeyGen. (s.f.-b). *HeyGen Biometric information privacy notice*. https://www.heygen.com/biometric-privacy-notice

Horten, M. (2022). *Algorithms patrolling content: Where's the harm?* SSRN. https://ssrn.com/abstract=3792097

Jayanti, A. (2020). *Deepfakes*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/2024-09/Deepfakes-2.pdf

Jones Walker LLP. (2026). Deepfakes-as-a-service meets state laws: Governing synthetic media in a fragmented legal landscape. *National Law Review*. https://natlawreview.com/article/deepfakes-service-meets-state-laws-governing-synthetic-media-fragmented-legal

Kansy, M., Naruniec, J., Schroers, C., Gross, M. y Weber, R. M. (2025). *Reenact anything: Semantic video motion transfer using motion-textual inversion*. *ACM SIGGRAPH 2025 Conference Papers.* https://doi.org/10.1145/3721238.3730668

Kapilian, A. (2025). New York's Digital Replicas Law: An evaluation of new protections for performing artists. *Cornell Journal of Law & Public Policy*. https://publications.lawschool.cornell.edu/jlpp/2025/02/11/the-digital-replica-contracts-act-an-evaluation-of-new-yorks-new-protections-for-performing-artists

Keswani, V. y Celis, L. E. (2024). *Algorithmic fairness from the perspective of legal anti-discrimination principles*. SSRN. https://ssrn.com/abstract=4116835

Kligvasser, I., Cohen, R., Leifman, G., Rivlin, E. y Elad, M. (2025). *Anchored diffusion for video face reenactment.* Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV 2025). https://doi.org/10.1109/WACV61041.2025.00402

Kohel, M. D. y Klukosky, F. M. P. (2024). *The ELVIS Act: Tennessee law addresses AI's impact on the music industry*. Maryland State Bar Association. https://www.

msba.org/site/site/content/News-and-Publications/News/General-News/ELVIS-Act.aspx

Latham & Watkins. (2024). *The ELVIS Act: Tennessee shakes up its right of publicity law and takes on generative AI*. https://www.lw.com/admin/upload/SiteAttachments/The-ELVIS-Act-Tennessee-Shakes-Up-Its-Right-of-Publicity-Law-and-Takes-On-Generative-AI.pdf

Licensing Executives Society International. (2025). *From performance to replica: Navigating consent, ownership and licensing in the age of generative AI*. https://lesi.org/article-of-the-month/from-performance-to-replica-navigating-consent-ownership-and-licensing-in-the-age-of-generative-ai/

McCann, M. (2025). *Jack Nicklaus wins licensing case as judge says he can use own NIL*. Sportico. https://www.sportico.com/law/analysis/2025/jack-nicklaus-wins-nil-case-1234844880/

Morrison Foerster. (2025). *Digital avatars deep dive series: Navigating the legal and regulatory landscape in 2025*. https://www.mofo.com/resources/insights/250922-digital-avatars-deep-dive-series-navigating

Mustak, M. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research, 154*, 113368. https://doi.org/10.1016/j.jbusres.2022.113368

Nachbar, T. B. (2021). Algorithmic fairness, algorithmic discrimination. *Florida State University Law Review, 48*, 509-558. https://ssrn.com/abstract=3530053

OpenAI. (30 de septiembre de 2025). *Launching Sora responsibly*. https://openai.com/index/launching-sora-responsibly/

P'ng, J. (2024). The resurrection will not be televised: Legal remedies for posthumous deepfakes. *Georgetown Law Technology Review, 8*(2), 338-370. https://ssrn.com/abstract=4900895

Preminger, A. y Kugler, M. B. (2024). The right of publicity can save actors from deepfake armageddon. *Berkeley Technology Law Journal (forthcoming)*. SSRN. https://ssrn.com/abstract=4563774

Rijsbosch, B., Van Dijck, G. y Kollnig, K. (2025). Adoption of watermarking for generative AI systems in practice and implications under the new EU AI Act. *arXiv*. https://arxiv.org/abs/2503.18156

Rosati, E. (2025). Infringing AI: Liability for AI-generated outputs under international, EU, and UK copyright law. *European Journal of Risk Regulation*, *16*(2), 603-627. https://doi.org/10.1017/err.2024.72

Rothman, J. E. (2025). *Revised No FAKES Act still poses danger of our losing control of our digital selves*. Rothman's Roadmap to the Right of Publicity. https://rightofpublicityroadmap.com/news_commentary/revised-no-fakes-act-still-poses-danger-of-our-losing-control-of-our-digital-selves/

SAG-AFTRA. (2023). *Artificial intelligence resources*. https://www.sagaftra.org/contracts-industry-resources/contracts/2023-tvtheatrical-contracts/artificial-intelligence-resources

Samuelson, P. (2025). *Assessing the feasibility of collective licensing of in-copyright*

works as training data for generative AI systems. SSRN. https://ssrn.com/abstract=6051014

Schjødt. (2025). Owning the self: Denmark's copyright turn against deepfakes. https://schjodt.com/news/owning-the-self-denmarks-copyright-turn-against-deepfakes

State of Tennessee, 113th General Assembly. (2024). HB 2091 / Public Chapter 588 (Ensuring Likeness, Voice, and Image Security Act of 2024 — "ELVIS Act"). https://wapp.capitol.tn.gov/apps/Billinfo/default.aspx?BillNumber=HB2091&ga=113

Szkalej, K. (2025). Music recommender systems and the copyright blind spot: Conceptualising the right to be heard. SSRN. https://ssrn.com/abstract=5967014

Tech Policy Press. (2025). *Denmark leads EU push to copyright faces in fight against deepfakes*. https://www.techpolicy.press/denmark-leads-eu-push-to-copyright-faces-in-fight-against-deepfakes/

U.S. Copyright Office. (2024). *Copyright and artificial intelligence: Part 1—Digital replicas* (Report of the Register of Copyrights). https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf

U.S. Department of Defense, Cybersecurity Information Sheet. (2025). *Content credentials: Enhancing trust and transparency in digital content*. https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF

University of Colorado Boulder. (17 de noviembre de 2025). *Deepfakes and AI in the courtroom: Report calls for legal reforms to address a troubling trend*. CU Boulder Today. https://www.colorado.edu/today/2025/11/17/deepfakes-and-ai-courtroom-report-calls-legal-reforms-address-troubling-trend

Von Lewinski, S. (2013). *The Beijing Treaty on Audiovisual Performances*. Max Planck Institute for Intellectual Property and Competition Law Research Paper No. 13-08. https://ssrn.com/abstract=2239109

Wachter, S., Mittelstadt, B. y Russell, C. (2020). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review, 41*(2021), 105567. https://ssrn.com/abstract=3547922

World Intellectual Property Organization. (s.f.). *Beijing Treaty on Audiovisual Performances: Summary*. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_228-accessible1.pdf

World Intellectual Property Organization. (1961). *International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention)*. WIPO Lex. https://www.wipo.int/wipolex/en/text/289757

World Intellectual Property Organization. (1996). *WIPO Performances and Phonograms Treaty (WPPT)*. WIPO Lex. https://www.wipo.int/wipolex/en/text/295578

World Intellectual Property Organization. (2012). *Beijing Treaty on Audiovisual Performances*. WIPO Lex. https://www.wipo.int/wipolex/en/text/295837

Legislación citada

California Civil Code § 3344 (2025). https://law.justia.com/codes/california/code-civ/division-4/part-1/title-2/chapter-2/article-3/section-3344/

California Labor Code § 927. (2024). *Contracts against public policy: personal or professional services: digital replicas* (AB 2602). California State Legislature. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2602

New York Civil Rights Law § 50-f. https://www.nysenate.gov/legislation/laws/CVR/50-F

New York State Senate. (s.f.). Civil Rights Law § 50-f: Right of publicity. https://www.nysenate.gov/legislation/laws/CVR/50-F

Tennessee House Bill 2091, Pub. Ch. 588 (2024) (ELVIS Act). https://publications.tnsosfiles.com/acts/113/pub/pc0588.pdf

* * * *

Roles de autoría y conflicto de intereses

El autor manifiesta que cumplió todos los roles de autoría del presente artículo y declara no poseer conflicto de interés alguno.