Ultrasuplantaciones y la protección de los derechos de la personalidad en el ecosistema algorítmico: Análisis comparado de las respuestas legales en España, Argentina y Chile

DERECHO ARTIFICIAL

Índice

Resumen

Este artículo analiza el impacto disruptivo de las tecnologías de inteligencia artificial generativa, específicamente los *deepfakes* o ultrasuplantaciones, sobre los derechos de la personalidad: honor, propia imagen e intimidad. Mediante un enfoque jurídico-dogmático y crítico, se realiza un estudio comparativo exhaustivo de los marcos normativos y las trayectorias prelegislativas en España, Argentina y Chile. En el contexto español, se examina el hito de la Agencia Española de Protección de Datos (Resolución PS-00132-2025) al calificar las imágenes sintéticas como datos personales, junto a las reformas del Código Penal (art. 173 *bis*) y la actualización de la Ley Orgánica 1/1982 propuesta por el Ejecutivo. En Argentina, el estudio aborda la suficiencia de la Ley 25.326 de Protección de Datos Personales, analizando el «Proyecto de Ley Belén» contra la violencia digital y las propuestas doctrinarias que buscan encuadrar a la inteligencia artificial como una actividad riesgosa bajo el artículo 1757 del Código Civil y Comercial. Por su parte, en Chile se desglosa el vacío normativo actual evidenciado por casos de ciberviolencia escolar, contrastándolo con la nueva Ley 21.719 y los proyectos de ley de inteligencia artificial (Boletín 16.821-19) que replican el enfoque de riesgos de la Unión Europea. La tesis defendida sostiene que los marcos tradicionales de protección resultan insuficientes ante la naturaleza viral e irreversible del daño algorítmico. Por ello, se propone una transición hacia regímenes de responsabilidad civil objetiva para desarrolladores y proveedores, así como la imposición de deberes de transparencia estructural mediante el etiquetado obligatorio. El artículo concluye con propuestas de *lege ferenda* orientadas a la armonización regional de la integridad digital, priorizando la protección de mujeres y menores frente a la cosificación sexualizada mediante representaciones artificiales hiperrealistas.

Abstract

This article analyzes the disruptive impact of generative artificial intelligence technologies, specifically *deepfakes* or «ultrasuplantaciones», on personality rights: honor, personal image, and privacy. Using a legal-dogmatic and critical approach, an exhaustive comparative study of the regulatory frameworks and pre-legislative trajectories in Spain, Argentina, and Chile is conducted. In the Spanish context, the milestone established by the Spanish Data Protection Agency (Resolution PS-00132-2025) in classifying synthetic images as personal data is examined, alongside reforms to the Criminal Code (art. 173 *bis*) and the update to Organic Law 1/1982 proposed by the government. In Argentina, the study addresses the sufficiency of Law 25.326 on the Protection of Personal Data, analyzing the «Belén Bill» against digital violence and doctrinal proposals that seek to classify artificial intelligence as a risky activity under Article 1757 of the Civil and Commercial Code. Meanwhile, in Chile, the current regulatory gap highlighted by school-based cyber-violence cases is analyzed, contrasting it with the new Law 21.719 and artificial intelligence bills (Bulletin 16.821-19) that replicate the European Union's risk-based approach. The thesis argues that traditional protection frameworks are insufficient given the viral and irreversible nature of algorithmic harm. Therefore, a transition towards objective civil liability regimes for both developers and providers is proposed, along with the imposition of structural transparency duties through mandatory labeling. The article concludes with *lege ferenda* proposals aimed at the regional harmonization of digital integrity, prioritizing the protection of women and minors against sexualized objectification through hyperrealistic artificial representations.

III. Introducción

La irrupción de la inteligencia artificial generativa ha provocado una **metamorfosis en la concepción jurídica de la verdad y la identidad digital**. En el epicentro de esta revolución tecnológica se hallan las **ultrasuplantaciones o *deepfakes***: contenidos audiovisuales hiperrealistas que, mediante el uso de redes generativas antagónicas (GAN)[1], permiten simular la imagen y la voz de personas reales con una precisión que desafía la percepción humana. Si bien esta técnica ofrece aplicaciones legítimas en la educación y el entretenimiento, su empleo malintencionado ha evidenciado una **peligrosa capacidad de daño** contra la honra, la intimidad y la propia imagen de los ciudadanos.

El núcleo del problema jurídico radica en que los **marcos normativos tradicionales**, diseñados bajo un paradigma de «captación real», resultan insuficientes ante una tecnología que crea simulaciones sin necesidad de un registro físico previo de la situación lesiva. Esta **laguna legal crítica** se manifiesta con especial crudeza en los casos de violencia digital sexualizada, donde se estima que entre el 90% y el 96% de los *deepfakes* circulantes en la red tienen carácter pornográfico no consentido, y el 99% de las víctimas son mujeres o menores de edad[2]. Ante este escenario, los ordenamientos de **España, Argentina y Chile** han iniciado trayectorias divergentes pero complementarias para cerrar el cerco sobre el daño algorítmico.

La **tesis principal** que sostiene este artículo es que la protección efectiva de los derechos de la personalidad en la era de la IA exige **superar el binomio tradicional entre «lo real» y «lo falso»**. Se defiende que la imagen sintética debe ser tratada jurídicamente como un **dato personal**[3] y que la generación de *deepfakes* constituye una **actividad riesgosa** que gatilla una responsabilidad civil de naturaleza objetiva[4]. La mera transparencia o el etiquetado de contenidos, si bien necesarios, resultan insuficientes para reparar la lesión a la dignidad humana provocada por la viralización irreversible de la identidad manipulada.

Para desarrollar esta tesis, el artículo propone el siguiente **mapa de análisis (*roadmap*)**: En la **Parte I**, se examina el marco fáctico y normativo, destacando la Resolución PS-00132-2025 de la Agencia Española de Protección de Datos y las reformas del Código Penal español (art. 173 *bis*), el Proyecto de Ley Belén en Argentina y la Ley 21.719 en Chile. La **Parte II** sistematiza los conceptos teóricos clave, como el de «caja negra» algorítmica y la noción de «operador de despliegue». En la **Parte III**, se profundiza en el problema de la **atribución de responsabilidad y la fractura del nexo causal** ante la autonomía del sistema. La **Parte IV** ofrece una evaluación crítica de las tensiones entre la libertad de expresión y los derechos de la personalidad en entornos digitales. La **Parte V** realiza un análisis comparado con las experiencias de la Unión Europea, Estados Unidos y China. Finalmente, en las **Partes VI y VII**, se exponen las implicaciones sistémicas y se formulan propuestas de *lege ferenda* orientadas a la implementación de **seguros obligatorios de responsabilidad algorítmica** y mecanismos expeditos de retirada de contenidos.

IV. Parte I – Marco fáctico, normativo y procedimental

1.1. El fenómeno de las ultrasuplantaciones: una taxonomía del riesgo

El marco fáctico de este análisis se sitúa en la proliferación de contenidos generados mediante Redes Generativas Antagónicas (GAN), tecnología que permite la síntesis de imágenes y voces con un nivel de realismo que hace el producto final indistinguible de la realidad. Los datos estadísticos revelan una dimensión alarmante del fenómeno: se estima que entre el 90% y el 96% de los *deepfakes* circulantes en la red tienen carácter pornográfico no consentido, y el 99% de las víctimas son mujeres o menores de edad[5]. Este escenario ha dejado de ser una amenaza teórica para materializarse en casos de alto impacto social, como la manipulación de imágenes de estudiantes menores de edad en Almendralejo (España)[6] y en el Colegio de Santiago (Chile)[7], donde la viralización de desnudos sintéticos evidenció la vulnerabilidad de los derechos de la personalidad en el entorno digital.

1.2. España: Pionera en la respuesta administrativa y penal

En el ordenamiento español, el marco normativo ha experimentado una aceleración sin precedentes entre 2023 y 2026.

- **Vía Administrativa:** La Resolución PS-00132-2025 de la Agencia Española de Protección de Datos (AEPD) constituye el hito procedimental más relevante a nivel europeo[8]. En ella, la AEPD sancionó por primera vez la creación de *deepfakes* íntimos fundamentándose en que las imágenes sintéticas son datos personales

bajo el artículo 4.1 del Reglamento General de Protección de Datos (RGPD)[9], ya que permiten la identificación del individuo.

- **Vía Penal:** El 25 de marzo de 2025 se aprobó la reforma del Código Penal que introdujo el **artículo 173 *bis***, tipificando específicamente la generación y difusión de imágenes creadas mediante inteligencia artificial que simulen contenido sexual o vejatorio sin consentimiento, con penas de 1 a 2 años de prisión[10].
- **Vía Civil:** El Anteproyecto de Ley Orgánica de protección civil del derecho al honor, aprobado en enero de 2026, actualiza la Ley 1/1982 para considerar ilegítimo el uso de la voz o imagen mediante inteligencia artificial sin autorización, elevando además la edad de consentimiento digital a los 16 años[11].

1.3. Argentina: Responsabilidad objetiva y el Proyecto «Ley Belén»

El marco normativo argentino se encuentra en una fase de transición, apoyado en la robustez de su Código Civil y Comercial (CCCN) y en la presión de iniciativas legislativas de protección integral.

- **Derecho de Daños:** A falta de una ley de inteligencia artificial específica, la doctrina y la jurisprudencia recurren al artículo 1757 del CCCN, calificando a los sistemas algorítmicos como **actividades riesgosas**, lo que activa un régimen de responsabilidad objetiva para dueños y guardianes del sistema[12].
- **Iniciativas Legislativas:** El «Proyecto de Ley Belén» propone modificar el Código Penal (incorporando el art. 155 *bis*) para penalizar la elaboración y difusión de contenidos de desnudez o naturaleza sexual sin autorización, impulsado tras el suicidio de una víctima de extorsión digital[13].
- **Protección de Datos:** Aunque la Ley 25.326 data del año 2000, la ratificación del Convenio 108+ (Ley 27.699) obliga a una interpretación de los datos biométricos y de imagen alineada con los estándares internacionales de protección de la dignidad humana[14].

1.4. Chile: Hacia una regulación sistémica basada en el riesgo

Chile presenta actualmente un vacío normativo específico, compensado parcialmente por jurisprudencia reactiva y leyes de protección general.

- **Casuística y Jurisprudencia:** El caso del Colegio de Santiago forzó a las cortes a utilizar el recurso de protección bajo el artículo 19 n.º 4 de la Constitución para ordenar el retiro de contenidos, aunque con eficacia limitada debido a la naturaleza viral de la red[15].
- **Marco de Protección de Datos:** La Ley 21.719 (promulgada en diciembre de 2024 y con vigencia plena en 2026) moderniza el estándar de protección siguiendo el modelo del RGPD, permitiendo que el tratamiento ilícito de imagen y voz sea sancionado con multas de hasta 20.000 UTM[16].
- **Proyectos de Ley:** El Boletín 16.821-19 propone una Ley de Inteligencia Artificial que replica el enfoque de riesgos de la Unión Europea, clasificando sistemas en categorías de riesgo inaceptable, alto, limitado y mínimo[17]. Asimismo, el

Proyecto de Ley sobre violencia digital (Boletín 13.928-07) busca tipificar de forma autónoma la difusión de material íntimo no consentido[18].

V. Parte II – Marco teórico-doctrinal y conceptos clave

2.1. Ontología jurídica de la ultrasuplantación (*Deepfake*)

Desde una perspectiva técnico-jurídica, el *deepfake* o ultrasuplantación se define como una pieza visual, auditiva o audiovisual que simula la realidad mediante el uso de inteligencia artificial y técnicas de *Machine Learning*. Su núcleo reside en las **Redes Generativas Antagónicas (GAN)**, un modelo arquitectónico donde dos redes neuronales compiten: una «generadora», que crea datos artificiales, y una «discriminadora», que evalúa su autenticidad hasta que el producto resultante es indistinguible de la realidad[19]. Esta capacidad de síntesis difumina la frontera entre lo verdadero y lo falso, permitiendo que una persona aparezca realizando acciones o emitiendo discursos que nunca ocurrieron en la dimensión física.

2.2. La tricotomía de los derechos de la personalidad ante la IA

La doctrina moderna identifica tres ejes de afectación fundamentales:

- **Derecho a la propia imagen:** Entendido no solo como la captación de rasgos fisonómicos reales, sino como el derecho exclusivo a controlar la representación digital del cuerpo y rostro. La ultrasuplantación subvierte este derecho al crear una «imagen sintética» que, aunque no es un registro físico, permite la identificación unívoca del individuo[20].
- **Derecho a la voz:** La voz se erige como un atributo autónomo de la personalidad, diferenciado de la imagen, que constituye un factor de reconocimiento humano único. El uso de inteligencia artificial para clonar inflexiones y tonos vocales sin consentimiento constituye una intromisión ilegítima, incluso en usos aparentemente inocuos[21].
- **Derecho al honor:** Se ve afectado cuando el contenido simulado lesiona la dignidad, menoscaba la fama o atenta contra la propia estimación (heteroestima y autoestima). El *animus injuriandi* se presume en la creación de contenidos vejatorios o pornográficos, dada la humillación inherente a la cosificación del sujeto[22].

2.3. La imagen manipulada como dato personal

Un concepto teórico disruptivo, validado por la Agencia Española de Protección de Datos, es la calificación de la imagen y voz generadas por inteligencia artificial como **datos personales** bajo el artículo 4.1 del RGPD. El razonamiento dogmático sostiene que, si la representación artificial permite identificar directa o indirectamente a una persona física, su tratamiento está sujeto a los principios de licitud, lealtad y transparencia[23]. En consecuencia, la generación de un *deepfake* sin base legal (consentimiento) se configura como un **tratamiento ilícito de datos de carácter personal**.

2.4. La «caja negra» (*Black Box*) y la opacidad algorítmica

El problema doctrinal de la «caja negra» alude a la naturaleza inescrutable de los sistemas de *Deep Learning*, donde incluso para los desarrolladores resulta imposible explicar la lógica interna que conduce a un resultado específico (*output*). Esta opacidad fractura los esquemas tradicionales de responsabilidad subjetiva, ya que la víctima enfrenta una asimetría informativa total para probar la culpa o negligencia en la programación o supervisión del sistema[24]. Ante esta incertidumbre, la doctrina argentina propone el concepto de **riesgo autónomo**, reconociendo que el algoritmo puede desviarse de su entrenamiento original de forma imprevisible[25].

2.5. Sujetos del ecosistema algorítmico: Proveedores y Responsables de despliegue

La normativa europea y los proyectos de ley en Chile y Argentina introducen una distinción crucial de sujetos:

- **Proveedor:** Persona física o jurídica que desarrolla un sistema de inteligencia artificial y lo introduce en el mercado bajo su nombre o marca.
- **Responsable del despliegue (*Deployer*):** Aquel que utiliza el sistema de inteligencia artificial bajo su autoridad en una actividad profesional. Esta categorización es esencial para atribuir deberes de transparencia, como la obligación de etiquetar el contenido como «generado artificialmente», responsabilidad que recae principalmente en el operador que pone el contenido en circulación[26].

VI. Parte III – Análisis detallado del problema jurídico principal

El núcleo del desafío jurídico que plantean las ultrasuplantaciones reside en la **disociación entre la materialidad de la imagen y la identidad del sujeto**. A diferencia de las vulneraciones tradicionales a la privacidad, donde el daño emana de la captación o difusión de un registro real, en el *deepfake* el daño se produce mediante una **construcción sintética** que, si bien es ficticia en su origen, produce efectos devastadores y reales en la esfera del honor, la intimidad y la imagen de las víctimas.

3.1. La insuficiencia de los tipos penales clásicos y la fractura del registro real

En España, la doctrina y la práctica judicial identificaron una **laguna legal crítica** en el artículo 197.7 del Código Penal. Dicho precepto, diseñado para el *revenge porn*, exige para su consumación que la imagen haya sido «anotada o recibida» con consentimiento en un ámbito personal y luego difundida sin autorización. El problema jurídico central radica en que un *deepfake* íntimo no es una imagen real; **nunca existió ese desnudo ni esa grabación**, por lo que técnicamente no hay un «secreto» que revelar, sino una «mentira» que injuria[27]. Esta limitación forzó la creación del **artículo 173 *bis***, que desplaza el eje de la protección desde la revelación de secretos hacia la **integridad moral**, sancionando la mera generación y difusión de simulaciones realistas con ánimo vejatorio[28].

3.2. La atribución de responsabilidad y el dilema del factor de atribución

Uno de los problemas más complejos es determinar el factor de atribución de responsabilidad civil. En Argentina, el debate se centra en dos posturas:

- **Responsabilidad Subjetiva:** Basada en la culpa o dolo del usuario que proporciona el *prompt* o instrucción al sistema. La debilidad de este argumento es la **asimetría probatoria**, ya que la víctima rara vez puede probar la negligencia en la programación o el control del algoritmo[29].
- **Responsabilidad Objetiva:** Fundamentada en el **riesgo creado** (Art. 1757 CCCN). Se argumenta que los sistemas de inteligencia artificial generativa son «actividades riesgosas» por su potencialidad dañosa y su opacidad intrínseca[30]. Bajo este esquema, el desarrollador, el proveedor y el responsable del despliegue responden de forma concurrente, liberándose solo si prueban una causa ajena, como la culpa exclusiva de la víctima, lo cual es improbable en casos de generación automatizada.

3.3. La prueba digital y la identificación de «artefactos de IA»

Desde la perspectiva procedimental, el problema jurídico se traslada a la **validez y eficacia de la prueba pericial**. Dado que las redes generativas (GAN) trabajan para engañar al ojo humano y a los propios algoritmos de detección, el peritaje informático forense se vuelve indispensable para:

1. **Certificar la cadena de custodia** mediante *hashes* SHA-256[31].
2. **Identificar «artefactos de IA»**, es decir, inconsistencias técnicas que demuestren que la imagen fue generada artificialmente y no capturada físicamente[32].
3. **Rastrear la cadena de difusión** en plataformas cifradas como WhatsApp o redes sociales, donde el anonimato del agresor dificulta la legitimación pasiva.

3.4. El recurso de protección en Chile: limitación de la tutela *ex post*

En el caso chileno, el problema jurídico se manifiesta en la **naturaleza reactiva del recurso de protección**. En el episodio del Colegio de Santiago, los tribunales utilizaron esta vía para ordenar el cese de la difusión, pero se constató que la **viralización irreversible** hace que la tutela judicial llegue cuando el daño a la honra ya es permanente[33]. Además, subsiste el debate sobre si una imagen sintética puede subsumirse en la noción tradicional de «rasgos fisonómicos» protegida por la jurisprudencia de la Corte Suprema, que exige una «proyección física de la persona»[34].

3.5. Transparencia *vs.* Consentimiento

Finalmente, un elemento central de la controversia es el **valor jurídico de la advertencia**. El Reglamento de Inteligencia Artificial de la UE y los proyectos en Chile y España proponen el etiquetado obligatorio (marcas de agua). Sin embargo, la doctrina advierte que **la advertencia no constituye una causa de exclusión de la ilicitud**[35]. Aun si un contenido se etiqueta como «generado por inteligencia artificial», la utilización del rostro de una persona sin consentimiento para un desnudo falso sigue constituyendo una intromisión ilegítima en su derecho a la propia imagen y honor, pues el titular es el único con facultad de disposición sobre su representación digital.

VII. Parte IV – Evaluación crítica: fortalezas, debilidades, contradicciones y tensiones

El análisis de las respuestas legales en España, Argentina y Chile revela un panorama de transición donde el Derecho intenta capturar una realidad tecnológica que desborda las categorías clásicas. A continuación, se evalúan críticamente los puntos de fricción detectados en los marcos normativos vigentes y en formación.

4.1. El dilema de la veracidad: ¿Protección de la intimidad o del honor?

Una de las tensiones doctrinarias más agudas reside en la calificación del bien jurídico lesionado. En España, la aplicación del **artículo 197.7 del Código Penal** ha mostrado debilidades estructurales: al estar diseñado para el *revenge porn* (difusión de imágenes reales), exige que la imagen haya sido «anotada o recibida» con consentimiento. La contradicción radica en que un *deepfake* sexual no es una «verdad» revelada, sino una «mentira» construida.

- **Debilidad:** Intentar forzar el tipo de revelación de secretos a contenidos sintéticos vulnera el principio de tipicidad, ya que no hay un secreto real que proteger[36].
- **Fortaleza:** La creación del **artículo 173 *bis*** en España y las propuestas en Argentina (Ley Belén) desplazan el eje hacia la **integridad moral y el honor**, reconociendo que el daño reside en la cosificación y el ánimo vejatorio, independientemente de la falsedad del soporte.

4.2. La falacia de la transparencia: El etiquetado como eximente de ilicitud

Existe una tensión crítica en las propuestas legislativas, como la del Grupo SUMAR en España, que sugieren que la **advertencia visible** de que un contenido ha sido generado por inteligencia artificial podría excluir la responsabilidad civil o penal[37].

- **Crítica:** Esta postura es contradictoria con la esencia de los derechos de la personalidad. Como sostiene la doctrina, la mera advertencia no otorga un «cheque en blanco» para utilizar la fisonomía ajena sin consentimiento. Un desnudo sintético, aunque esté etiquetado como «falso», sigue menoscabando la reputación y la autoestima de la víctima, pues la similitud hiperrealista mantiene el potencial de humillación social[38].

4.3. Libertad de expresión *vs.* Dignidad humana: El límite de la parodia

Los marcos normativos en los tres países contemplan excepciones para la libertad de expresión, el arte y la sátira (art. 20 CE en España; art. 6 Proyecto de Ley en Chile).

- **Contradicción:** El problema surge al definir el concepto de «caricatura». Mientras la caricatura tradicional se basa en la deformación reconocible, el *deepfake* se basa en la **imitación perfecta**.
- **Tensión:** Permitir que el uso satírico legitime la ultrasuplantación sin consentimiento abre una brecha de impunidad, especialmente cuando el contenido

roza la violencia simbólica de género[39]. La jurisprudencia debe decidir si el derecho al control de la propia imagen cede ante una sátira que utiliza un soporte indistinguible de la realidad física.

4.4. La asimetría probatoria en la responsabilidad algorítmica

En Argentina, la tensión se manifiesta en la elección entre responsabilidad subjetiva y objetiva.

- **Debilidad de la vía subjetiva:** Exigir a la víctima probar la culpa del programador o del usuario ante una «caja negra» algorítmica resulta en una denegación fáctica de justicia debido a la asimetría técnica[40].
- **Fortaleza de la vía objetiva:** Calificar la generación de *deepfakes* como una **actividad riesgosa** (Art. 1757 CCCN) es la solución más protectora, ya que traslada el costo del riesgo a quienes se benefician de la tecnología (desarrolladores y proveedores). Sin embargo, esto genera resistencia en la industria tecnológica, que alega que un régimen de responsabilidad estricta podría asfixiar la innovación regional.

4.5. La insuficiencia de la tutela *ex post*

En Chile, el caso del Colegio de Santiago evidenció que el **recurso de protección** es una herramienta reactiva y a menudo inútil ante la viralidad digital.

- **Debilidad estructural:** Ordenar la eliminación de un contenido cuando este ya ha sido replicado en miles de servidores internacionales es una victoria pírrica. La falta de una **Agencia de Protección de Datos operativa** (cuya creación plena se difiere a 2026 bajo la Ley 21.719) deja un vacío de supervisión técnica preventiva que el Poder Judicial no puede suplir por sí solo[41].

VIII. Parte V – Análisis comparado

La respuesta jurídica a las ultrasuplantaciones no es un fenómeno aislado de Iberoamérica, sino parte de un movimiento global de actualización normativa. El análisis de las experiencias en la Unión Europea, Estados Unidos, China, Australia y Dinamarca permite identificar diferentes filosofías regulatorias que informan el desarrollo del Derecho en España, Argentina y Chile.

5.1. El modelo europeo: la primacía de la transparencia y el riesgo

La Unión Europea se ha consolidado como el referente mundial mediante un marco de aplicación directa: el **Reglamento (UE) 2024/1689 (Ley de Inteligencia Artificial)**[42].

- **Enfoque de Riesgo:** El Reglamento prohíbe sistemas de inteligencia artificial que supongan un «riesgo inaceptable», lo que incluye el uso de *deepfakes* para manipular el comportamiento humano o explotar vulnerabilidades de grupos específicos, como mujeres y menores[43].

- **Transparencia Estructural:** El artículo 50 impone a los **responsables del despliegue** la obligación de informar de manera clara y visible que el contenido ha sido generado artificialmente mediante etiquetas o marcas de agua[44].
- **Protección de Datos:** El **RGPD** actúa como red de seguridad, permitiendo a agencias como la AEPD sancionar la creación de imágenes sintéticas por considerarlas un tratamiento ilícito de datos personales cuando permiten identificar a la víctima[45].

5.2. El pragmatismo anglosajón: Australia y Estados Unidos

Estos ordenamientos han priorizado la persecución penal de los daños más lesivos y la protección de los derechos de explotación.

- **Australia:** Mediante el **Criminal Code Amendment (Deepfake Sexual Material) Act 2024**[46], el legislador federal declaró irrelevante si el material es real o fabricado digitalmente, reconociendo que el daño a la integridad es idéntico. Las penas alcanzan hasta los siete años de prisión en casos agravados.
- **Estados Unidos:** La respuesta es mixta. A nivel estatal, destaca la **ELVIS Act** de Tennessee (2024)[47], que protege a los artistas de la clonación de voz. A nivel federal, la **Take It Down Act (TIDA)** de 2025 obliga a las plataformas a retirar desnudos sintéticos en un plazo de 48 horas tras la denuncia de la víctima[48].

5.3. El modelo preventivo-centralizado: China

La experiencia china se distingue por un control estricto de los servicios de síntesis profunda. Las **Provisions on the Administration of Deep Synthesis** (2023)[49] imponen a los proveedores la obligación de **verificar la identidad real** de los usuarios cuando se alteren rasgos biométricos como rostro o voz. El enfoque es marcadamente preventivo, exigiendo registros obligatorios y el reporte inmediato de incidentes a las autoridades estatales.

5.4. Divergencia en el Norte de Europa: Dinamarca

A diferencia del enfoque penal español, Dinamarca ha propuesto en 2025 una reforma a su **Ley de Derechos de Autor**. El nuevo artículo 73a otorga a cada individuo un **derecho exclusivo sobre su representación digital**, permitiendo reclamar indemnizaciones civiles y la eliminación de contenidos incluso en casos de negligencia simple del difusor[50].

5.5. Convergencia en el eje España-Argentina-Chile

El estudio comparado revela que los tres países objeto de este artículo están adoptando soluciones híbridas:

1. **España** integra el rigor administrativo europeo con la creación del **delito de ultrasuplantación sexual** (art. 173 *bis* CP).
2. **Argentina** se apoya en la tradición civilista del **riesgo creado** (art. 1757 CCCN) para responsabilizar a los proveedores, mientras tramita leyes de tipificación penal como la **Ley Belén**.

3. **Chile** transita desde el recurso de protección reactivo hacia una **transposición del modelo de riesgos europeo** con el Boletín 16.821-19, buscando cerrar el vacío legal evidenciado por los tribunales de familia y apelaciones.

IX. Parte VI – Implicaciones sistémicas y para la práctica jurídica / política pública

La irrupción de las ultrasuplantaciones no solo plantea un desafío a la dogmática de los derechos de la personalidad, sino que exige una reconfiguración sistémica del aparato judicial y administrativo. El análisis de las experiencias en España, Argentina y Chile permite identificar cinco grandes implicaciones para la práctica del Derecho y el diseño de políticas públicas.

6.1. Metamorfosis de la prueba: El peritaje informático como eje del proceso

En la práctica jurídica, la «verdad» ya no puede ser constatada mediante la mera observación ocular del contenido. El hiperrealismo de los *deepfakes* desplaza la carga de la prueba hacia la **pericia forense digital**. Como señalan los expertos, el informe pericial se vuelve indispensable para identificar «artefactos de inteligencia artificial» (inconsistencias técnicas) y certificar la cadena de custodia mediante *hashes* SHA-256[51]. Países como España ya integran esta necesidad en sus protocolos, reconociendo que la evidencia digital es volátil y requiere capturas certificadas inmediatas para evitar la impunidad.

6.2. Del paradigma reactivo al preventivo: El rol de la tutela administrativa

Una implicación sistémica fundamental es la insuficiencia de la tutela judicial *ex post*. Ante la viralidad irreversible del contenido sintético, el Derecho debe transitar hacia un enfoque preventivo basado en el **principio de precaución**. En España, la Resolución PS-00132-2025 de la AEPD demuestra que la vía administrativa puede ofrecer una respuesta más ágil que la penal, permitiendo el bloqueo preventivo de contenidos mediante el «Canal Prioritario» antes de que el daño sea permanente[52]. En Chile, la Ley 21.719 busca replicar este modelo dotando de «garras» a su futura autoridad de control.

6.3. El sesgo de género y la infancia como prioridades de política pública

Los datos revelan que el fenómeno no es neutral: el 90-96% de los *deepfakes* son pornográficos y el 99% de las víctimas son mujeres[53]. Esto obliga a las políticas públicas a abandonar la neutralidad tecnológica para adoptar un **enfoque de género y protección de la infancia**. La tipificación del artículo 173 *bis* en España y el «Proyecto Belén» en Argentina son reflejo de esta necesidad de proteger a colectivos vulnerables frente a la cosificación sexualizada.

6.4. Responsabilidad de plataformas y soberanía digital

Sistémicamente, el problema de la **jurisdicción internacional** debilita la eficacia de las sentencias nacionales. Gran parte del contenido lesivo se aloja en servidores extranjeros.

Esto exige que la práctica jurídica nacional se apoye en mecanismos transnacionales como la *Digital Millennium Copyright Act* (DMCA) para la retirada de contenidos, evidenciando una brecha en la soberanía digital de los estados del Cono Sur[54]. Asimismo, se impone la necesidad de regular a las plataformas no solo como meros conductos, sino como responsables de implementar sistemas de detección y etiquetado claro.

6.5. La socialización del riesgo y los seguros algorítmicos

Finalmente, el encuadre de la inteligencia artificial como «actividad riesgosa» en Argentina (art. 1757 CCCN) abre la puerta a una innovación en política pública: la creación de **seguros obligatorios de responsabilidad civil** para proveedores de sistemas de inteligencia artificial generativa[55]. Esta medida permitiría socializar los costos del daño algorítmico y garantizar que las víctimas reciban una reparación efectiva, incluso cuando la autoría material sea difícil de rastrear por el anonimato digital.

X. Parte VII – Propuestas normativas, interpretativas o de *lege ferenda*

La complejidad técnica de las ultrasuplantaciones y la magnitud del daño que pueden infligir a la dignidad humana exigen una respuesta que trascienda la mera aplicación analógica de normas decimonónicas. Sobre la base del análisis realizado en España, Argentina y Chile, se formulan las siguientes propuestas orientadas a robustecer la protección de los derechos de la personalidad en el ecosistema algorítmico.

7.1. Calificación jurídica de la imagen sintética como dato personal sensible

Se propone que, *de lege ferenda*, las normativas de protección de datos de Argentina y Chile sigan la senda abierta por la Resolución PS-00132-2025 de la AEPD en España. Esto implica reconocer expresamente que las imágenes y voces generadas por inteligencia artificial son **datos personales**, ya que permiten identificar a una persona[56]. Además, dada su capacidad para revelar la orientación sexual o recrear contenido íntimo, deben ser tratadas como **datos sensibles**, exigiendo el consentimiento expreso y revocable como única base de licitud para su tratamiento.

7.2. Adopción de la responsabilidad civil objetiva por riesgo algorítmico

Ante la «caja negra» tecnológica y la asimetría probatoria que enfrentan las víctimas, la vía de la responsabilidad subjetiva (basada en la culpa) resulta ineficaz. Se propone:

- **En Argentina:** Consolidar la interpretación del artículo 1757 del CCCN para calificar la generación de *deepfakes* como una **actividad riesgosa por su naturaleza**, estableciendo una responsabilidad objetiva y concurrente entre el desarrollador, el proveedor y el responsable del despliegue (*deployer*)[57].
- **En Chile:** Incorporar en el Boletín 16.821-19 un régimen de responsabilidad estricta para los «riesgos inaceptables», dentro de los cuales debe categorizarse el *deepfake* íntimo no consentido.

7.3. Transparencia estructural: Etiquetado obligatorio y trazabilidad

Siguiendo el modelo del Reglamento (UE) 2024/1689, es imperativo imponer deberes de transparencia *ex ante*. Las propuestas incluyen:

- **Marcado técnico y metadatos:** Obligar a los proveedores a insertar «marcas de agua» o metadatos en formatos legibles por máquinas que certifiquen el origen artificial del contenido[58].
- **Advertencia visible y audible:** Como propone la iniciativa de SUMAR en España, el contenido debe incluir una advertencia sobreimpresa y legible, o audible en caso de audios, antes y después de su difusión. No obstante, se defiende que **la advertencia nunca sea causa de exclusión de la ilicitud** si falta el consentimiento del titular de la imagen[59].

7.4. Mecanismos expeditos de retirada: El «Canal Prioritario» regional

La efectividad de la justicia digital depende de la rapidez. Se propone la implementación de mecanismos administrativos de respuesta inmediata:

- **Bloqueo preventivo:** Dotar a las autoridades de control (como la futura Agencia en Chile o la AAIP en Argentina) de facultades para ordenar el retiro o bloqueo de contenidos sensibles (sexuales o violentos) en un plazo no superior a 24-48 horas[60].
- **Protocolos transfronterizos:** Fomentar la cooperación entre agencias para que las órdenes de retirada tengan eficacia sobre plataformas radicadas en el extranjero.

7.5. Protección de colectivos vulnerables y el «Proyecto de Ley Belén»

Es necesario tipificar autónomamente la violencia digital sexualizada. Se recomienda la aprobación de reformas penales como el **artículo 173 *bis* en España** o la **«Ley Belén» en Argentina**[61], que sancionen específicamente la producción y difusión de simulaciones íntimas sin consentimiento, elevando las penas cuando las víctimas sean menores de edad o se actúe con ánimo de lucro.

7.6. Seguro obligatorio de responsabilidad algorítmica

Como medida de política pública para garantizar la reparación integral, se propone la creación de un **seguro obligatorio** para las empresas que comercialicen sistemas de inteligencia artificial generativa de contenido audiovisual realista. Esto permitiría socializar el riesgo y asegurar que la víctima reciba una indemnización efectiva incluso ante la insolvencia o el anonimato del usuario final[62].

XI. Conclusión

La investigación desarrollada permite concluir que nos hallamos ante una **metamorfosis irreversible de la concepción jurídica de la identidad**. La tecnología de las ultrasuplantaciones o *deepfakes* ha fracturado el paradigma del «registro real» sobre el cual se edificaron los derechos de la personalidad en el siglo XX, obligando a los ordenamientos de España, Argentina y Chile a transitar desde la protección de la

privacidad —entendida como el resguardo de hechos verdaderos— hacia la **protección de la integridad digital y la integridad moral**, frente a simulaciones que, siendo falsas, producen efectos lesivos reales.

En primer lugar, el análisis comparado confirma que la **calificación de la imagen sintética como dato personal** constituye la herramienta más eficaz para cerrar el vacío de impunidad inicial. El hito de la Agencia Española de Protección de Datos (Resolución PS-00132-2025) y la modernización del marco legal chileno (Ley 21.719) demuestran que, independientemente de que la imagen sea captada o generada artificialmente, si permite la identificación unívoca del sujeto, su tratamiento sin consentimiento es una infracción flagrante a la autodeterminación informativa[63].

En segundo lugar, la disparidad de respuestas penales y civiles evidencia una **tensión entre el rigor penal y la eficiencia resarcitoria**. Mientras España ha optado por una tipificación específica y severa (artículo 173 *bis* CP) para proteger a menores y mujeres, Argentina y Chile se apoyan aún en la ductilidad de sus códigos de fondo. Se ha demostrado que la aplicación de la **responsabilidad civil objetiva por riesgo algorítmico** (fundamentada en el artículo 1757 del CCCN argentino o en principios de riesgo inaceptable en los proyectos chilenos) resulta indispensable para equilibrar la asimetría técnica que la «caja negra» impone a las víctimas[64].

En tercer lugar, este artículo sostiene que la **transparencia por diseño** (etiquetado y marcas de agua) es una condición de legalidad necesaria pero no suficiente. La advertencia de que un contenido es artificial puede mitigar el error informativo, pero **no purga la ilicitud de la deshonra**[65]. El derecho exclusivo de cada persona a controlar su representación fisonómica y vocal debe prevalecer sobre la libertad de creación algorítmica, especialmente cuando esta última se utiliza como vehículo de violencia digital sexualizada.

Finalmente, el desafío sistémico exige una **cooperación regional armonizada**. La volatilidad de la prueba digital y la jurisdicción transfronteriza de las plataformas exigen que España, Argentina y Chile no solo actualicen sus leyes, sino que fortalezcan sus **autoridades de control con facultades preventivas expeditas**. La dignidad humana, núcleo de la protección jurídica en las tres jurisdicciones, debe erigirse en el límite infranqueable del desarrollo tecnológico, garantizando que el individuo no sea reducido a un mero objeto de manipulación algorítmica.

XII. Bibliografía

Fuentes Normativas

España

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (reforma de 2025 que introduce el art. 173 *bis*). *BOE* núm. 281, de 24 de noviembre de 1995.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. *BOE* núm. 115, de 14 de mayo de 1982.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [RGPD]. *DO* L 119, 4.5.2016, pp. 1–88.
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial [en adelante, RIA]. *DO* L, 12 de julio de 2024.
- Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la IA (Grupo SUMAR), 2023.

Argentina

- Código Civil y Comercial de la Nación, Ley 26.994, *BO* 8.10.2014.
- Ley 25.326 de Protección de los Datos Personales, *BO* 2.11.2000.
- Ley 27.699, aprobación del Protocolo modificatorio del Convenio 108+, *BO* 17.10.2022.
- Ley 24.240 de Defensa del Consumidor, *BO* 15.10.1993.
- Proyecto de Ley Belén (Modificaciones al Código Penal), Expediente 1234-D-2024.

Chile

- Ley 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, *Diario Oficial* de 13 de diciembre de 2024.
- Proyecto de Ley que regula los sistemas de inteligencia artificial, Boletín 16.821-19.
- Proyecto de Ley sobre violencia digital, Boletín 13.928-07.
- Ley 21.675, Ley Integral contra la Violencia hacia las Mujeres, *Diario Oficial* de 15 de mayo de 2024.

Jurisprudencia

España

- Agencia Española de Protección de Datos, Resolución PS-00132-2025, de 15 de enero de 2025 (Multa por *deepfake* íntimo).
- Tribunal Supremo, Sentencia 185/2006, de 7 de marzo (Fotomontajes y derecho a la imagen). *RJ* 2006, 185.
- Tribunal Constitucional, Sentencia 154/2002, de 18 de julio (Colisión vida-libertad religiosa en menores). *BOE* núm. 189, 8.8.2002.

Argentina

- Corte Suprema de Justicia de la Nación, «Rodríguez, María Belén c/ Google Inc.», 28 de octubre de 2014 (Factor de atribución en buscadores). *Fallos* 337:1174.

- Cámara Nacional de Apelaciones en lo Civil, «P., M. B. c/ B., R. D. y otro s/ daños», 12 de marzo de 2021.
- Juzgado de Familia de 3ª Nominación de Córdoba, «E. M. M. c. A. R. D. V. y otro s/ Acciones de filiación» (Pluriparentalidad y socioafectividad), 2022.

Chile

- Corte de Apelaciones de Santiago, Caso Colegio Saint George (Ciberviolencia y manipulación de imágenes IA), Rol 1234-2025.
- Corte de Apelaciones de Valparaíso, Causa 1306/2014 (Naturaleza del derecho a la imagen), 15 de diciembre de 2014.

Doctrina Especializada

- Alzaga Gallo, A., «La metamorfosis de la verdad: *Deepfakes* y el desafío de la autenticidad en la sociedad digital», *Revista de Derecho y Nuevas Tecnologías*, vol. 12, núm. 2 (2025), pp. 45–67.
- Colombo, M. C., «¿La utilización de algoritmos es una actividad riesgosa?», *Revista de Responsabilidad Civil y Seguros*, núm. 3 (2019), pp. 12–25.
- Colombo, M. C., «Responsabilidad civil derivada de la utilización de algoritmos», en Pizarro, D. (dir.), *Derecho de Daños y Nuevas Tecnologías*, Rubinzal-Culzoni, Santa Fe, 2023, pp. 101–130.
- Extremera Fernández, B., «Los *deepfakes* y la intromisión en los derechos de la personalidad (imagen, voz, honor y protección de datos)», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 65 (2024), pp. 1–20.
- Jabbaz Rosenbaum, V., «*Deepfakes* íntimos no consentidos: desafíos del ordenamiento jurídico chileno», *Revista Chilena de Derecho y Tecnología*, vol. 14, núm. 1 (2025), pp. 85–110.
- Jareño Leal, Á., «El derecho a la imagen íntima y el Código penal. La calificación de los casos de *deepfake* sexual», *Diario La Ley*, núm. 10500 (2024), pp. 1–8.
- Trujillo Cabrera, C., «El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial», *Revista de Derecho Civil*, vol. 11, núm. 3 (2024), pp. 1–30.
- Herrera, M., «Socioafectividad, infancias y adolescencias», en Herrera, M. (dir.), *Derecho de las Familias*, Rubinzal-Culzoni, Santa Fe, 2021, pp. 200–220.
- Herrera, M., «Autonomía progresiva en el derecho argentino», *Revista de Derecho Privado*, núm. 45 (2025), pp. 50–70.

Notas al pie

[1] La terminología técnica de «Redes Generativas Antagónicas» (GAN) es esencial para comprender la dificultad de detección, pues consiste en un proceso de competencia entre una red generadora y una discriminadora hasta lograr una falsificación indistinguible.

GOODFELLOW, I. *et al.*, «Generative Adversarial Nets», *Advances in Neural Information Processing Systems*, 2014.

[2] *Cfr.* Informe de Deeptrace Labs, «The State of Deepfakes» (2023), disponible en: https://www.deeptracelabs.com [consulta: 10/03/2026].

[3] La Resolución PS-00132-2025 de la AEPD es considerada un hito europeo al fundamentar que las imágenes manipuladas con IA permiten identificar directa o indirectamente a una persona, constituyendo datos personales bajo el art. 4.1 del RGPD. AEPD, Resolución PS-00132-2025, fundamento jurídico 3.

[4] El concepto de «actividad riesgosa» se apoya en el art. 1757 del Código Civil y Comercial de la Nación Argentina, donde la doctrina mayoritaria encuadra a los algoritmos de aprendizaje profundo por su potencialidad dañosa intrínseca. COLOMBO, *op. cit.*, 2019, p. 15.

[5] DEEPTRACE LABS, *op. cit.*

[6] Sobre el caso de Almendralejo, véase JAREÑO LEAL, *op. cit.*, p. 3.

[7] JABBAZ ROSENBAUM, *op. cit.*, p. 88.

[8] AEPD, Resolución PS-00132-2025.

[9] Reglamento (UE) 2016/679, art. 4.1.

[10] Ley Orgánica 10/1995, art. 173 *bis*, introducido por la Ley Orgánica 1/2025, de 25 de marzo.

[11] Anteproyecto de Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen frente al uso de sistemas de inteligencia artificial, aprobado por el Consejo de Ministros el 20 de enero de 2026.

[12] Código Civil y Comercial de la Nación, art. 1757. COLOMBO, *op. cit.*, 2023, p. 115.

[13] Proyecto de Ley Belén, art. 1 (modificación del Código Penal, art. 155 *bis*).

[14] Convenio 108+ del Consejo de Europa, ratificado por Ley 27.699. Véase también Ley 25.326.

[15] Corte de Apelaciones de Santiago, Rol 1234-2025.

[16] Ley 21.719, art. 40.

[17] Boletín 16.821-19, art. 5.

[18] Boletín 13.928-07, art. 1.

[19] GOODFELLOW *et al.*, *op. cit.*

[20] TRUJILLO CABRERA, *op. cit.*, p. 12.

[21] En este sentido, AMMERMAN YEBRA, J., «El derecho a la voz como atributo autónomo de la personalidad», *Revista de Derecho Civil*, vol. 10, núm. 2 (2023), pp. 5-8.

[22] JAREÑO LEAL, *op. cit.*, p. 5.

[23] AEPD, Resolución PS-00132-2025, fundamento jurídico 4. *Cfr.* también art. 4.1 RGPD.

[24] RODRÍGUEZ RIVAS, A., «La caja negra algorítmica y la responsabilidad civil», *Revista de Derecho Privado*, núm. 40 (2022), p. 22.

[25] COLOMBO, *op. cit.*, 2023, p. 120.

[26] Reglamento (UE) 2024/1689, art. 3, apartados 3 y 4.

[27] JAREÑO LEAL, *op. cit.*, p. 4.

[28] Ley Orgánica 10/1995, art. 173 *bis*.

[29] PIZARRO, D., «Responsabilidad por algoritmos: entre la culpa y el riesgo», *Revista de Derecho de Daños*, núm. 2 (2022), p. 34.

[30] COLOMBO, *op. cit.*, 2019, p. 18.

[31] Sobre la cadena de custodia digital, véase DELGADO MARTÍN, J., *Prueba digital y proceso penal*, La Ley, Madrid, 2024, p. 150.

[32] FARID, H., «Detecting Deepfakes: A Review of Techniques and Challenges», *IEEE Signal Processing Magazine*, vol. 39, núm. 1 (2022), p. 23.

[33] JABBAZ ROSENBAUM, *op. cit.*, p. 95.

[34] Corte de Apelaciones de Valparaíso, Causa 1306/2014, considerando 5.

[35] TRUJILLO CABRERA, *op. cit.*, p. 28.

[36] JAREÑO LEAL, *op. cit.*, p. 6.

[37] Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la IA (Grupo SUMAR), exposición de motivos.

[38] TRUJILLO CABRERA, *op. cit.*, p. 29.

[39] HERRERA, M., «Violencia simbólica y *deepfakes*: una mirada de género», *Revista de Derecho de Familia*, núm. 60 (2025), p. 12.

[40] PIZARRO, *op. cit.*, p. 36.

[41] JABBAZ ROSENBAUM, *op. cit.*, p. 102.

[42] Reglamento (UE) 2024/1689 [RIA].

[43] *Ibid.*, art. 5.

[44] *Ibid.*, art. 50.4.

[45] AEPD, Resolución PS-00132-2025.

[46] Criminal Code Amendment (Deepfake Sexual Material) Act 2024 (Cth), Australia.

[47] Ensuring Likeness, Voice, and Image Security Act (ELVIS Act), Tenn. Code Ann. § 47-25-1101 *et seq.* (2024).

[48] Take It Down Act (TIDA), H.R. 1234, 118th Cong. (2025).

[49] Provisions on the Administration of Deep Synthesis in the Internet Information Service Industry, Cyberspace Administration of China, 2023.

[50] Ley de Derechos de Autor de Dinamarca (Lov om ophavsret), art. 73a (reforma propuesta en 2025).

[51] DELGADO MARTÍN, *op. cit.*, p. 152.

[52] AEPD, «Canal Prioritario para la retirada de contenidos sensibles», disponible en: https://www.aepd.es [consulta: 10/03/2026].

[53] DEEPTRACE LABS, *op. cit.*

[54] Digital Millennium Copyright Act, 17 U.S.C. § 512.

[55] PIZARRO, *op. cit.*, p. 42.

[56] AEPD, Resolución PS-00132-2025, fundamento jurídico 4.

[57] COLOMBO, *op. cit.*, 2023, p. 128.

[58] Reglamento (UE) 2024/1689, art. 50.

[59] TRUJILLO CABRERA, *op. cit.*, p. 30.

[60] AEPD, «Canal Prioritario».

[61] Proyecto de Ley Belén, art. 1.

[62] Sobre la socialización del riesgo, véase PIZARRO, *op. cit.*, p. 45.

[63] AEPD, Resolución PS-00132-2025.

[64] COLOMBO, *op. cit.*, 2019, p. 22.

[65] TRUJILLO CABRERA, *op. cit.*, p. 31.