Cartografía jurídica de la identidad sintética: imagen, voz, dobles de datos e inteligencia artificial

Legal Cartography of Synthetic Identity: Image, Voice, Data Doubles and Artificial Intelligence

Fátima Solera Navarro
Doctora en Educación y Comunicación Social por la Universidad de Málaga.
ORCID: https://orcid.org/0000-0003-0143-7629

Fecha de recepción: 19.06.2026
Fecha de aceptación: 27.07.2026
Fecha de publicación en línea: octubre 2026

Resumen:
Este artículo propone pensar la identidad sintética como una de las formas más problemáticas que adopta la Inteligencia Artificial generativa cuando permite producir voces, imágenes, gestos, interpretaciones o declaraciones atribuibles a personas reales que no las han creado, consentido ni controlado. Para abordar este fenómeno, el texto parte del concepto de doble de datos formulado por Haggerty y Ericson, y lo pone en diálogo con la integridad contextual de Nissenbaum y la taxonomía de la privacidad de Solove. Desde este marco, se sostiene que la Inteligencia Artificial generativa intensifica el extractivismo de datos personales al transformar esos datos en presencias artificiales capaces de hablar, aparecer o actuar en nombre de alguien. A partir de ahí, se ofrece una cartografía jurídica que ordena la respuesta del Reglamento General de Protección de Datos, la Ley Orgánica 1/1982 sobre honor, intimidad y propia imagen, la Ley de Propiedad Intelectual, la Ley de Marcas y el Reglamento de Inteligencia Artificial según la operación técnica realizada, el material utilizado, el contexto de circulación y el daño producido. Se concluye que la identidad sintética no exige necesariamente una regulación autónoma, sino un mejor ensamblaje normativo y una comprensión de la privacidad como bien común.

Palabras clave:
Identidad sintética; doble de datos; inteligencia artificial generativa; datos biométricos; derecho a la propia imagen; integridad contextual.

Abstract:
This article proposes understanding synthetic identity as one of the most problematic forms taken by generative AI when it enables the production of voices, images, gestures, performances or statements attributable to real persons who have neither created, consented to nor controlled them. To address this phenomenon, the article takes as its starting point the concept of the data double formulated by Haggerty and Ericson, and brings it into dialogue with Nissenbaum's contextual integrity and Solove's taxonomy of privacy. From this framework, it argues that generative AI intensifies personal data extractivism by transforming such data into artificial presences capable of speaking, appearing or acting in someone's name. On that basis, the article offers a legal cartography that organizes the responses provided by the General Data Protection Regulation, Spain's Organic Law 1/1982 on honour, privacy and image rights, the Spanish Intellectual Property Act, the Spanish Trademark Act and the Artificial Intelligence Act, according to the technical operation involved, the material used, the context of circulation and the harm produced. It concludes that synthetic identity does not necessarily require autonomous regulation, but rather a better normative assemblage and an understanding of privacy as a common good.

Keywords:
Synthetic identity; data double; generative artificial intelligence; biometric data; right to one's image; contextual integrity.

Sumario:

1. Introducción. La marca como síntoma de una protección fragmentaria. **2.** De la identidad disponible a la identidad sintética. **3.** Genealogía teórica: control, ensamblaje, contexto y daño. **3.1.** Sociedades de control, modulación y contraseña. **3.2.** Del doble de datos al doble sintético. **3.3.** Integridad contextual y ruptura del flujo. **3.4.** Taxonomía de la privacidad como método de descomposición del daño. **4.** Cartografía jurídica de la identidad sintética. **4.1.** RGPD: la identidad sintética como cadena de tratamiento. **4.2.** Honor, intimidad y propia imagen: la identidad sintética como intromisión. **4.3.** Propiedad intelectual: obras, prestaciones y el límite de la imitación. **4.4.** Marca: signo distintivo y defensa lateral. **4.5.** Reglamento de IA: sistema, modelo y resultado sintético. **5.** Aplicación por escenarios. **5.1.** Scraping de imágenes, vídeos y audios identificables. **5.2.** Entrenamiento de modelos con canciones, entrevistas, videoclips o fotografías. **5.3.** Clonación de voz para publicidad, fraude o atención automatizada. **5.4.** Música sintética que parece interpretada por un artista en concreto. **5.5.** Imagen sexualizada generada mediante IA. **5.6.** Vídeo político falso con rostro y voz. **5.7.** Autenticación facial o vocal en banca, plataformas o accesos. **5.8.** Reconocimiento de emociones y categorización biométrica desde rostro o voz. **5.9.** Matriz de síntesis. **6.** ¿Más normas o mejor ensamblaje normativo?

Summary:

1. *Introduction. Trademark as a symptom of fragmented protection.* ***2.*** *From available identity to synthetic identity.* ***3.*** *Theoretical genealogy: control, assemblage, context and harm.* ***3.1.*** *Societies of control, modulation and password.* ***3.2.*** *From the data double to the synthetic double.* ***3.3.*** *Contextual integrity and the rupture of informational flow.* ***3.4.*** *The taxonomy of privacy as a method for decomposing harm.* ***4.*** *Legal cartography of synthetic identity.* ***4.1.*** *GDPR: synthetic identity as a chain of processing.* ***4.2.*** *Honour, privacy and the right to one's image: synthetic identity as intrusion.* ***4.3.*** *Intellectual property: works, performances and the limits of imitation.* ***4.4.*** *Trademark law: distinctive signs and lateral defence.* ***4.5.*** *The AI Act: system, model and synthetic output.* ***5.*** *Application by scenarios.* ***5.1.*** *Scraping of identifiable images, videos and audio.* ***5.2.*** *Model training with songs, interviews, music videos or photographs.* ***5.3.*** *Voice cloning for advertising, fraud or automated assistance.* ***5.4.*** *Synthetic music that appears to be performed by a specific artist.* ***5.5.*** *AI-generated sexualized image.* ***5.6.*** *False political video with face and voice.* ***5.7.*** *Facial or voice authentication in banking, platforms or access systems.* ***5.8.*** *Emotion recognition and biometric categorisation from face or voice.* ***5.9.*** *Synthesis matrix.* ***6.*** *More rules or better normative assemblage?*

1. Introducción. La marca como síntoma de una protección fragmentaria

A finales de abril de 2026 se conoció que TAS Rights Management, la empresa de la cantante Taylor Swift, había presentado ante la Oficina de Patentes y Marcas de Estados Unidos varias solicitudes para registrar dos clips de audio y una imagen concreta de la artista, en una estrategia orientada a reforzar su protección frente a vídeos y audios *deepfake* generados mediante Inteligencia Artificial (IA)[1]. La precisión resulta relevante, porque no se trataba de registrar "la voz" o "la imagen" en abstracto, como si la totalidad de una presencia pudiera convertirse sin más en objeto marcario, sino de proteger signos determinados que, por su capacidad distintiva, pudieran operar en el tráfico económico.

El recurso a la marca dice bastante del momento jurídico en que nos encontramos. Ante la dificultad de encajar la clonación de voz, la imitación de una apariencia o la producción de imágenes falsas dentro de una sola categoría jurídica, una artista con una identidad comercial extraordinariamente valiosa decidió acudir a una herramienta pensada para proteger signos distintivos en el mercado. La estrategia puede resultar comprensible, más en el contexto estadounidense, pero también revela una profunda desigualdad en las posibilidades de defensa frente a este tipo de daños: solo quienes han convertido su voz, su imagen o su nombre en activos económicamente reconocibles, y cuentan además con recursos suficientes para anticipar conflictos, registrar signos y litigar, pueden utilizar esta vía con cierta eficacia. Los *deepfakes*, sin embargo, no afectan únicamente a celebridades, artistas o figuras públicas. También alcanzan a menores, trabajadoras, docentes, activistas, periodistas o personas anónimas cuya imagen puede ser extraída de redes sociales, recompuesta artificialmente y puesta a circular sin que exista una marca, una estructura empresarial o una capacidad real de respuesta detrás.

Esta es la cuestión fundamental que articula el presente artículo: cómo debe responder el Derecho cuando una voz, un rostro, una imagen o una forma reconocible de estar en el mundo pueden separarse de la persona que los encarna y recombinarse artificialmente en un doble capaz de hablar, cantar, aparecer, recomendar, consentir o exponerse en su nombre.

[1] Brad Brooks, "Taylor Swift Files to Trademark Her Voice, Likeness to Ward off AI Deepfakes", *Reuters*, 27 de abril de 2026.

La respuesta no puede descansar en una sola vía de protección, ni quedar reservada a quienes pueden convertir su identidad en signo registrable. A falta de una categoría jurídica única que permita nombrar esta constelación de fenómenos, propongo utilizar la expresión "identidad sintética" para referirme a toda representación artificial, generada o manipulada mediante sistemas de IA, que permite reconocer, evocar o atribuir a una persona real una voz, una imagen, un rostro, un gesto, una interpretación, una conducta o una declaración que dicha persona no ha producido, consentido o controlado en ese contexto.

La definición es deliberadamente amplia, porque no pretende describir únicamente el *deepfake* audiovisual más evidente, sino también las zonas más ambiguas de sustitución: canciones que parecen interpretadas por un artista concreto, anuncios que explotan una apariencia reconocible, avatares comerciales, réplicas conversacionales, imágenes sexualizadas, apoyos políticos falsos o contenidos que no copian una obra preexistente, pero sí capturan una forma socialmente reconocible de presencia. La hipótesis que sostiene estas páginas es que la IA generativa convierte el doble de datos, descrito por Haggerty y Ericson[2], en doble sintético: si el doble de datos permitía reunir flujos informacionales para clasificar, predecir o intervenir sobre una persona, el doble sintético introduce una mutación adicional al producir una representación artificial capaz de hablar, cantar, aparecer o actuar en su nombre.

En ese desplazamiento, los marcos jurídicos existentes no desaparecen ni quedan automáticamente obsoletos, pero muestran sus costuras. Cada uno protege un objeto distinto y ninguno agota por sí solo la complejidad del daño. De ahí la necesidad de una cartografía jurídica de la identidad sintética, capaz de ordenar las capas normativas que se activan según la operación técnica realizada, el tipo de dato o material utilizado, el contexto de circulación, el daño producido y el objeto jurídico protegido. Para ello, el artículo se apoya en el marco teórico del doble de datos y del extractivismo de datos personales, así como en la taxonomía de la privacidad de Solove, que permite descomponer los daños en términos de recopilación, procesamiento, difusión e invasión, y proyecta después esa descomposición sobre el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 1/1982, la Ley de Propiedad Intelectual, la Ley de Marcas y el Reglamento de Inteligencia Artificial.

2. De la identidad disponible a la identidad sintética

Una parte importante de los debates actuales sobre IA generativa sigue atrapada en una formulación demasiado estrecha del problema. Se habla de contenidos falsos, de imágenes engañosas, de canciones imitativas, de *deepfakes* pornográficos, de anuncios apócrifos o de clonación de voz, como si cada una de estas expresiones pudiera aislarse en una categoría técnica o jurídica independiente. Sin embargo, todas ellas participan de una misma transformación: la separación creciente entre la persona encarnada y sus signos sensibles de reconocimiento.

La voz, el rostro, la imagen, la gestualidad o el estilo performativo han sido históricamente formas de comparecencia ante los demás. Reconocemos a alguien por su modo de hablar, por su timbre, por su manera de moverse, por ciertas inflexiones, por una expresión facial, por un gesto aprendido o por la acumulación de apariciones públicas que hacen que una presencia resulte identificable incluso cuando no hay nombre. La IA generativa altera ese régimen ordinario de reconocimiento al hacer técnicamente replicables elementos que hasta hace poco conservaban una fuerte vinculación con el cuerpo que los producía. La voz grabada deja de ser únicamente huella de una emisión pasada; puede transformarse en insumo para producir nuevas emisiones. La imagen deja de ser únicamente fijación de una apariencia; puede alimentar modelos capaces de producir otras apariencias suficientemente próximas. El estilo deja de ser únicamente una forma de autoría o de presencia; puede convertirse en patrón explotable.

La cuestión jurídica nace precisamente en ese desajuste entre exposición y disponibilidad. Que una voz haya sido emitida en una entrevista, una canción, una llamada de atención al cliente o un vídeo publicado en redes no implica que pueda quedar jurídicamente abierta a cualquier reutilización posterior. Que una fotografía haya circulado en un contexto informativo, promocional o comunitario no convierte esa imagen en material libre para entrenar modelos, producir avatares, generar pornografía sintética o construir bases de reconocimiento facial. La confusión entre publicidad y disponibilidad acompaña buena parte de la economía digital. La teoría de la integridad contextual de Nissenbaum permite formularlo con precisión: que una información sea accesible no significa que cualquier flujo posterior resulte social, ética o jurídicamente apropiado. Con la IA generativa, esa confusión adquiere otra intensidad, porque los materiales ya no se limitan a circular, indexarse o monetizarse, sino que pueden reensamblarse en una presencia nueva.

[2] Kevin D. Haggerty y Richard V. Ericson, "The Surveillant Assemblage", *British Journal of Sociology* 51, n.º 4 (2000): 605-622.

Por eso la identidad sintética no puede comprenderse únicamente como falsedad. Hay imágenes falsas sin personas reconocibles en ellas, audios sintéticos sin atribución individual y contenidos generados artificialmente que no producen un daño personal directo. La identidad sintética aparece cuando el resultado generado se anuda a una persona concreta o razonablemente identificable, cuando una voz, una cara, una figura o una forma de expresión permiten atribuir socialmente esa presencia a un individuo concreto. En ese punto, el daño no depende solo de que el contenido sea verdadero o falso: puede haber daño por apropiación de una identidad, por distorsión de la reputación, por sexualización, por explotación comercial, por interferencia política, por descontextualización o por erosión de la capacidad de una persona para modular su propia presentación ante los demás.

Esta perspectiva permite abandonar la pregunta, algo tramposa, sobre la propiedad aislada de una voz, una imagen, un timbre o un estilo, para atender al recorrido técnico y jurídico mediante el cual esos rasgos son extraídos de su contexto, recombinados por sistemas de IA y devueltos al espacio público como una forma de presencia atribuible a alguien. La respuesta aquí no puede ser unitaria, porque la misma voz puede funcionar como dato personal, como dato biométrico, como atributo de la personalidad, como interpretación artística fijada, como fonograma, como marca sonora o como *output* sintético sujeto a transparencia. A su vez, la misma imagen puede ser fotografía protegida, dato identificativo, propia imagen, material de entrenamiento, signo visual distintivo, plantilla biométrica o *deepfake*.

Ese carácter múltiple de la voz y la imagen exige abandonar dos tentaciones igualmente pobres. La primera consistiría en sostener que la IA generativa se mueve en un vacío jurídico, como si ninguna norma existente pudiera intervenir frente a la producción de dobles sintéticos. La segunda consistiría en suponer que basta con aplicar mecánicamente las normas ya disponibles, sin atender a los desplazamientos técnicos y contextuales que estas tecnologías producen. La dificultad aparece entre ambos extremos. Hay normas, pero no todas miran el mismo objeto. Hay remedios, pero no todos responden al mismo daño. Hay categorías, pero muchas de ellas fueron pensadas para un mundo donde la imitación de la presencia no tenía la escala, la velocidad ni la granularidad que hoy permite la IA generativa.

3. Genealogía teórica: control, ensamblaje, contexto y daño

3.1. Sociedades de control, modulación y contraseña

La identidad sintética debe pensarse en continuidad con el desplazamiento que Deleuze identifica al pasar de las sociedades disciplinarias a las sociedades de control. Si la disciplina operaba mediante instituciones cerradas y cuerpos localizados, el control se despliega a través de modulaciones continuas, accesos, claves, perfiles y contraseñas[3]. En este escenario, la identidad deja de funcionar únicamente como dato civil o atributo estable de la personalidad y se convierte en condición técnica de circulación. Entramos, salimos, desbloqueamos, verificamos, autorizamos y confirmamos mediante señales que prueban que somos quienes decimos ser, o al menos que el sistema puede tratarnos como tales.

La voz y el rostro ocupan aquí un lugar especialmente ambiguo. Parecen rasgos íntimos, personales, ligados a la presencia viva del cuerpo. Sin embargo, se han convertido en credenciales. Sirven para abrir dispositivos, verificar operaciones, acceder a edificios, desbloquear cuentas, confirmar identidades en servicios bancarios, cruzar fronteras o filtrar sospechas en sistemas de videovigilancia. La biometría transformó el cuerpo en contraseña, y la IA generativa introduce una perturbación grave dentro de esta lógica, porque hace replicables algunos de los signos sobre los que se había depositado la confianza. Si mi voz autoriza una operación, si mi rostro confirma mi presencia, si mi imagen respalda una recomendación o si mi cuerpo aparece como prueba de un acontecimiento, la posibilidad de sintetizar esos signos produce una crisis de autenticación corporal.

Esta crisis no se limita al fraude. En un sentido más amplio, la identidad sintética afecta a la forma en que el control contemporáneo distribuye confianza, acceso y credibilidad. Un sistema puede exigir más datos para compensar el riesgo de suplantación; una plataforma puede imponer más verificaciones; una institución puede reforzar procedimientos biométricos; una persona puede verse obligada a demostrar que no dijo, no hizo o no consintió aquello que una imagen o una voz parecen probar. Así, la simulación generativa no queda fuera de las sociedades de control, sino que las intensifica. Allí donde el control necesitaba signos verificables de identidad, la IA generativa introduce signos plau-

[3] Gilles Deleuze, "Post-scriptum sobre las sociedades de control", en *Conversaciones*, trad. José Luis Pardo (Valencia: Pre-Textos, 1995), 277-286.

sibles de identidad. Esa plausibilidad puede bastar para producir daño.

3.2. Del doble de datos al doble sintético

El concepto de doble de datos permite comprender que la identidad sintética no aparece de la nada, ni puede entenderse solo como una consecuencia espectacular de la IA generativa. Antes de que una voz clonada o una imagen sintética pudieran circular como si procedieran de una persona real, dicha persona ya había sido dividida en flujos discretos de información, separada de su cuerpo y reagrupada en perfiles, patrones, categorías y representaciones operativas. El ensamblaje de la vigilancia descrito por Haggerty y Ericson funciona precisamente así, pues no necesita capturar a la persona como totalidad, sino descomponerla en datos que después pueden recombinarse para intervenir sobre ella[4].

La identidad sintética añade una torsión a esta trayectoria. El doble de datos es, ante todo, una representación analítica: permite clasificar, puntuar, predecir o decidir sobre alguien. No se extraen únicamente datos para conocer, clasificar o predecir, sino rasgos sensibles de presencia para producir sustitutos. En esa transición, la voz y la imagen adquieren un valor jurídico y político particular. Tampoco son únicamente información sobre una persona, expresiones protegibles, signos comerciales o elementos técnicos para autenticar; son superficies de atribución. Una voz sintética puede hacer creer que alguien dijo algo; una imagen sintética puede hacer creer que alguien estuvo, hizo, consintió o deseó algo; una canción generada puede hacer creer que una artista interpretó algo; un anuncio falso puede hacer creer que una persona recomienda algo. Esa capacidad de atribución explica por qué la cartografía jurídica debe atender a la cadena completa: origen de los materiales, forma de procesamiento, contexto de generación, modo de difusión y daño producido.

A partir de esta genealogía puede formularse con mayor precisión el desplazamiento conceptual que propongo en este texto. El doble sintético es una actualización generativa del doble de datos: una representación artificial de una persona, producida a partir de datos personales, biométricos, expresivos o contextuales, que permite simular su presencia y atribuirle actos comunicativos, visuales, sonoros o performativos. La diferencia se formula así de manera sencilla, aunque sus consecuencias no lo sean: el doble de datos decide sobre mí; el doble sintético actúa como yo.

El doble de datos pertenece a la historia de la vigilancia, la clasificación y la predicción. Se alimenta de registros, transacciones, formularios, búsquedas, historiales, desplazamientos, consumos, contactos, hábitos y metadatos. Opera en bases de datos, sistemas de *scoring*, perfiles publicitarios, modelos predictivos, arquitecturas policiales o plataformas comerciales. Su daño típico aparece cuando una persona es tratada de acuerdo con una representación que no controla: se le niega un acceso, se le asigna un riesgo, se le segmenta, se le vigila, se le clasifica o se decide sobre ella en función de datos que la sustituyen.

El doble sintético conserva esa base extractiva, pero introduce una forma distinta de sustitución. Ya no basta con producir una representación operativa de la persona; ahora se produce una presencia artificial que puede ocupar socialmente su lugar. El rostro vuelve como imagen generada, la voz vuelve como audio sintético, el cuerpo vuelve como vídeo manipulado, el estilo vuelve como patrón imitativo. Esta reaparición no repara la separación previa entre cuerpo y datos, sino que la profundiza, porque el cuerpo regresa bajo una forma disponible para terceros. Allí donde el doble de datos permitía operar sobre la persona a distancia, sin necesidad de su presencia física, el doble sintético permite hacerla comparecer artificialmente en contextos que no eligió.

La identidad sintética debe leerse, por tanto, como una forma específica de extractivismo de datos personales[5]. No se extraen únicamente datos para conocer, clasificar o predecir, sino rasgos sensibles de presencia para producir sustitutos. En esa transición, la voz y la imagen adquieren un valor jurídico y político particular. Tampoco son únicamente información sobre una persona, expresiones protegibles, signos comerciales o elementos técnicos para autenticar; son superficies de atribución. Una voz sintética puede hacer creer que alguien dijo algo; una imagen sintética puede hacer creer que alguien estuvo, hizo, consintió o deseó algo; una canción generada puede hacer creer que una artista interpretó algo; un anuncio falso puede hacer creer que una persona recomienda algo. Esa capacidad de atribución explica por qué la cartografía jurídica debe atender a la cadena completa: origen de los materiales, forma de procesamiento, contexto de generación, modo de difusión y daño producido.

[4] Kevin D. Haggerty y Richard V. Ericson, "The Surveillant Assemblage", *British Journal of Sociology* 51, n.º 4 (2000): 605-622.

[5] Fátima Solera Navarro, Privacidad, res/xistencia y procomún frente al extractivismo de datos personales: O cómo hacer democracia a través de tácticas de litigación colectiva y ofuscación expresiva (tesis doctoral, Universidad de Málaga, 2025), cap. 2.3.5.

El doble sintético tiene además una dimensión narrativa. No sustituye ontológicamente a la persona, pero puede disputar su relato público e interrumpir la continuidad entre cuerpo, palabra y responsabilidad. Puede producir pruebas aparentes de actos no realizados o declaraciones no pronunciadas; puede obligar a la persona afectada a ocupar una posición reactiva, desmintiendo aquello que nunca ocurrió, reclamando la retirada de contenidos que ya han circulado o reconstruyendo la confianza dañada por una apariencia. La identidad sintética no destruye la identidad real; la parasita, la rodea, la replica parcialmente y la hace disponible para usos ajenos.

3.3. Integridad contextual y ruptura del flujo

Como comentaba en líneas anteriores, la integridad contextual de Nissenbaum introduce aquí un matiz decisivo, porque impide confundir publicidad con disponibilidad. La privacidad no se vulnera únicamente cuando se revela información secreta, ni se protege solo restringiendo de forma absoluta la circulación de datos. Su propuesta desplaza la atención hacia la adecuación de los flujos de información a los contextos en los que esos datos circulan: qué tipo de información se transmite, quién la emite, quién la recibe, quién es el sujeto afectado y bajo qué principio se produce esa transmisión[6].

Este enfoque resulta especialmente interesante para la identidad sintética. Una entrevista pública puede circular legítimamente como entrevista, pero no por ello queda disponible para entrenar una voz artificial que promocione un producto. Una fotografía promocional puede haber sido difundida en un contexto comercial determinado, pero no por ello autoriza su uso para producir una imagen sexualizada o una base de reconocimiento facial. Una canción publicada puede estar destinada a ser escuchada, citada, interpretada o criticada, pero no necesariamente a alimentar un modelo que genere nuevas canciones atribuidas a la voz de quien la interpretó. La lesión aparece cuando se altera el contexto de circulación de los materiales, sus destinatarios, sus finalidades y las expectativas normativas que los sostenían.

La identidad sintética puede entenderse entonces como una tecnología de ruptura contextual. Toma materiales producidos en un entorno y los hace operar en otro, muchas veces sin conocimiento, consentimiento ni capacidad real de respuesta por parte de la persona afectada. Esa ruptura es especialmente visible en los casos de *deepfakes* sexuales o políticos, pero también aparece en escenarios menos espectaculares, como la clonación de voces en servicios de atención automatizada, la generación de avatares comerciales, el uso de rostros en *datasets* o la reutilización de grabaciones para mejorar sistemas de autenticación. El argumento de que una imagen o una voz "ya estaban en Internet" resulta insuficiente porque ignora precisamente aquello que Nissenbaum permite ver: la circulación legítima de información depende del contexto y de sus normas, no de una supuesta renuncia general derivada de la exposición.

3.4. Taxonomía de la privacidad como método de descomposición del daño

La taxonomía de Solove ayuda a no reducir este conflicto a una sola palabra. Hablar de privacidad en abstracto resulta insuficiente cuando la identidad sintética puede implicar recopilación, procesamiento, difusión e invasión al mismo tiempo[7].

La taxonomía se construye desde una preocupación eminentemente situada: identificar qué clase de perturbaciones producen determinadas prácticas informacionales en la vida de las personas afectadas. De ahí que Solove organice los problemas de privacidad no tanto por tecnologías o sectores, sino por la forma en que la recopilación, el procesamiento, la difusión o la invasión de información alteran la posición de los individuos[8]. En términos esquemáticos, la propuesta puede ordenarse del siguiente modo:

[6] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009).

[7] Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008).

[8] Fátima Solera Navarro, Privacidad, res/xistencia y procomún frente al extractivismo de datos personales: O cómo hacer democracia a través de tácticas de litigación colectiva y ofuscación expresiva (tesis doctoral, Universidad de Málaga, 2025), cap. 2.2.3.

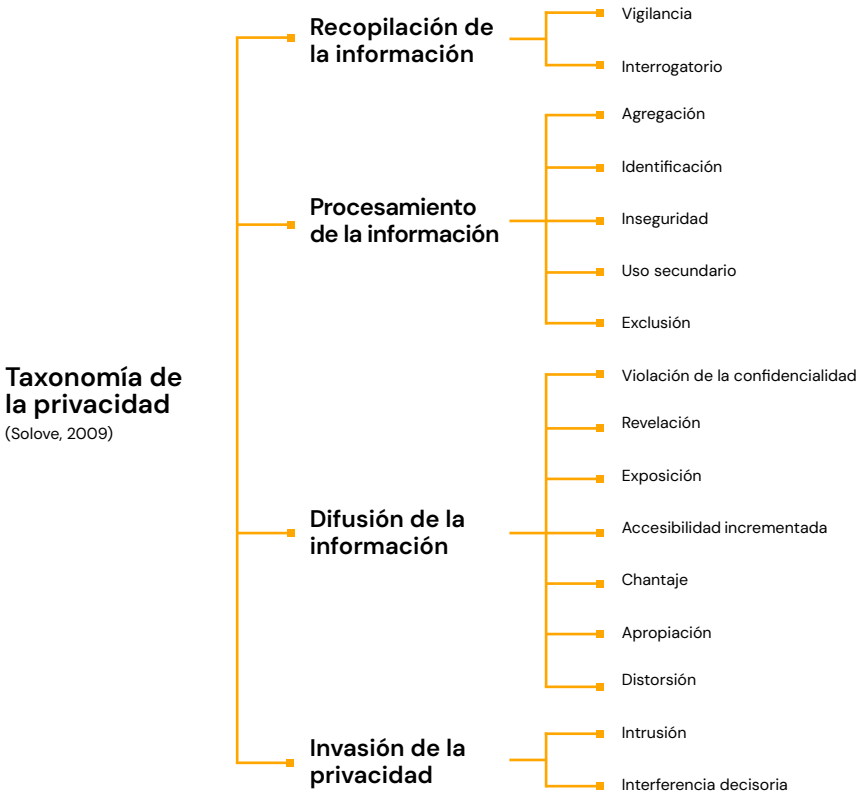


Figura 1: Esquema de la taxonomía de la privacidad de Solove (2009). Fuente: Elaboración propia.

El primer grupo de problemas es la recopilación de información, donde Solove sitúa la vigilancia y el interrogatorio. En la identidad sintética, esta fase aparece en la captura de fotografías, vídeos, audios, entrevistas, actuaciones, publicaciones o grabaciones que permiten alimentar bases de datos o modelos generativos. El daño no procede todavía del *deepfake* final, sino de la extracción inicial de materiales que hacen posible su producción. El segundo grupo es el procesamiento de la información, que incluye agregación, identificación, inseguridad, uso secundario y exclusión. Aquí se sitúan el entrenamiento de modelos, la generación de patrones faciales o vocales, la vinculación de materiales dispersos y la dificultad de que la persona afectada sepa qué se ha hecho con esos datos o pueda participar en su manejo.

El tercer grupo es la difusión. En él aparecen la violación de confidencialidad, la revelación, la exposición, la accesibilidad incrementada, el chantaje, la apropiación y la distorsión. Esta es la zona más visible de la identidad sintética, porque aquí se sitúan la canción que parece interpretada por un artista concreto, el anuncio falso, la imagen sexualizada o el vídeo político manipulado. La apropiación resulta especialmente relevante cuando se usa la identidad o personalidad de alguien para fines ajenos, afectando a la capacidad de esa persona de ejercer cierta autoría sobre su propia narrativa; la distorsión aparece cuando se manipula la forma en que los demás perciben y juzgan a una persona mediante información falsa o engañosa.

El cuarto grupo es la invasión, que Solove distingue de los anteriores porque no siempre necesita involucrar información personal en sentido estricto. Este se divide en intrusión e interferencia decisoria: la primera perturba la vida cotidiana mediante una presencia o actividad no deseada; la segunda afecta a decisiones especialmente vinculadas al cuerpo, la sexualidad, la crianza o la vida personal. Esta última parte permite entender por qué ciertos dobles sintéticos dañan más allá de la revelación o falsedad de una información: una imagen sexualizada fabricada, una voz que consiente algo no consentido o un avatar que actúa en nombre de alguien invaden la posibilidad de decidir cómo y cuándo aparecer ante los demás. Desde esta lectura, la cartografía jurídica debe ordenar primero los daños y solo después las normas.

4. Cartografía jurídica de la identidad sintética

Solo desde esta arquitectura teórica puede entenderse por qué la respuesta jurídica no puede ser unívoca. Si la identidad sintética es ruptura contextual, recombinación de flujos, apropiación de personalidad, distorsión reputacional y producción de presencia artificial, ninguna rama del Derecho

agota por sí sola el problema. La cartografía jurídica no sustituye esa complejidad por una respuesta simple; intenta ordenar qué protege cada régimen, en qué fase interviene y qué zonas permanecen mal ensambladas.

4.1. RGPD: la identidad sintética como cadena de tratamiento

Desde la perspectiva del RGPD, la identidad sintética debe analizarse ante todo como una cadena de tratamiento. La captación, extracción, almacenamiento, estructuración, conservación, entrenamiento, generación, difusión o puesta a disposición de imágenes, audios, vídeos, patrones faciales, huellas vocales o metadatos relativos a una persona identificada o identificable encaja en la amplitud del concepto de tratamiento del artículo 4.2, mientras que la noción de dato personal del artículo 4.1 permite incluir cualquier información sobre una persona identificada o identificable[9]. Esto desplaza el análisis desde el resultado más llamativo —por ejemplo, el vídeo falso o la voz clonada— hacia el proceso que permitió producirlo, porque antes del *resultado* hubo una selección de fuentes, una extracción de rasgos, un almacenamiento de datos, una inferencia o un entrenamiento.

Esa cadena debe someterse a los principios del artículo 5: licitud, lealtad y transparencia; limitación de la finalidad; minimización; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva[10]. La identidad sintética tensiona todos ellos. La limitación de finalidad se ve comprometida cuando materiales publicados en un contexto determinado se reutilizan para entrenar modelos o producir nuevos contenidos atribuidos a la persona. La minimización queda en entredicho cuando se capturan grandes cantidades de imágenes, audios o vídeos porque la lógica técnica del modelo se alimenta de acumulación. La transparencia se vuelve especialmente difícil cuando los materiales proceden de *scraping*, bases de datos intermedias, plataformas de terceros o archivos distribuidos. La exactitud adquiere, además, un sentido peculiar, porque el problema puede estar en la producción de una apariencia falsa, pero verosímil, sobre una persona encarnada.

Esta tensión se vuelve especialmente visible en los modelos de uso general. Cuando un conjunto de imágenes, voces o vídeos se incorpora a un entrenamiento genérico, la finalidad puede formularse de manera amplia (mejorar un modelo, ampliar sus capacidades generativas, optimizar resultados), pero esa amplitud no debería vaciar de contenido el principio de limitación de la finalidad. La dificultad aparece cuando un modelo entrenado de forma general se especializa después, mediante ajustes, instrucciones, *fine-tuning* o integración con otros sistemas, para producir dobles sintéticos de personas concretas. En ese desplazamiento, la finalidad inicial y la finalidad ulterior dejan de coincidir de manera evidente: una cosa es entrenar un sistema con capacidades generales de generación audiovisual y otra utilizarlo, o adaptarlo, para reproducir una voz, una imagen o una forma reconocible de presencia. La compatibilidad del tratamiento ulterior debería analizarse atendiendo al contexto de recogida de los materiales, a las expectativas razonables de la persona afectada, a la naturaleza de los datos, a las consecuencias previsibles y a las garantías técnicas y organizativas disponibles[11].

La licitud del artículo 6 se vuelve especialmente delicada en estos supuestos. El consentimiento tendrá que ser libre, específico, informado e inequívoco, algo difícil cuando los conjuntos de datos proceden de materiales dispersos o cuando los usos futuros no están claramente determinados. La ejecución contractual rara vez cubrirá tratamientos masivos orientados a producir dobles sintéticos. El interés legítimo exigirá una ponderación estricta cuando el resultado pueda producir apropiación de identidad, daño reputacional, sexualización o suplantación. La misión de interés público y el cumplimiento de una obligación legal requerirán una base normativa clara, finalidades determinadas y garantías adecuadas.

La cuestión biométrica exige una distinción que conviene mantener con precisión. Una fotografía identificable, un vídeo o una grabación de voz pueden ser datos personales sin ser necesariamente datos biométricos en el sentido del RGPD. La definición del artículo 4.14 exige datos personales obtenidos a partir de un tratamiento técnico específico relativo a características físicas, fisiológicas o conductuales que permitan o confirmen la identificación única de una persona, como imágenes faciales o datos dactiloscópicos[12]. El considerando 51 aclara que el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales, salvo cuando se traten

[9] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, art. 4.1 y 4.2.

[10] Reglamento (UE) 2016/679, art. 5.

[11] Reglamento (UE) 2016/679, art. 5.1.b y art. 6.4.

[12] Reglamento (UE) 2016/679, art. 4.14.

con medios técnicos específicos que permitan la identificación o autenticación unívocas[13]. Esta distinción resulta fundamental para no convertir cualquier imagen o audio en biometría, aunque tampoco puede utilizarse para invisibilizar tratamientos técnicos de voz o rostro que, en la práctica, producen plantillas, *embeddings*, huellas vocales o patrones identificativos.

Cuando la voz o el rostro se tratan técnicamente para identificar de manera unívoca a una persona, entra en juego el artículo 9.1, que establece la prohibición general de tratar categorías especiales, incluidos los datos biométricos dirigidos a identificar de manera unívoca a una persona física, salvo que concurra alguna excepción del artículo 9.2[14]. La guía de la Agencia Española de Protección de Datos, la AEPD, sobre tratamientos de control de presencia mediante sistemas biométricos insiste, en esa línea, en la necesidad de analizar la biometría desde la idoneidad, necesidad y proporcionalidad del tratamiento, con evaluación de impacto cuando proceda y con especial cuidado ante el uso de estos sistemas en contextos laborales o de acceso[15]. Aunque dicha guía esté pensada para control de presencia, sus criterios resultan útiles para la identidad sintética cuando la voz o el rostro dejan de ser meros materiales audiovisuales y pasan a funcionar como patrones técnicos de identificación.

Esta cautela resulta todavía más necesaria cuando se invoca la excepción relativa a los datos manifiestamente hechos públicos por el interesado. El artículo 9.2.e RGPD no debería interpretarse aquí como una autorización general para transformar fotografías, vídeos o grabaciones accesibles en línea en plantillas biométricas, huellas vocales o materiales de entrenamiento destinados a identificar, autenticar o simular a una persona[16]. Que una imagen haya sido publicada en una red social, que una voz aparezca en una entrevista o que una actuación circule en una plataforma no significa, por sí solo, que la persona haya hecho manifiestamente públicos los datos biométricos que pueden derivarse de un tratamiento técnico posterior. La publicidad del soporte no equivale a la publicidad de todas las inferencias, patrones o usos que pueden extraerse de él. Esta lectura resulta coherente con la aproximación restrictiva del Comité Europeo de Protección de Datos en materia de reconocimiento facial y con la necesidad, también presente en el Convenio 108+, de acompañar el tratamiento de categorías especiales —incluidos los datos biométricos— de una base jurídica adecuada y garantías proporcionadas al riesgo[17].

El RGPD ofrece derechos de reacción que pueden resultar relevantes —acceso, supresión, oposición y, cuando proceda, garantías frente a decisiones automatizadas—, pero llegan tarde si la persona desconoce el tratamiento, si los datos han circulado entre proveedores, si el modelo ya ha sido entrenado o si el resultado se difunde de forma viral. De ahí la importancia de las obligaciones preventivas: protección de datos desde el diseño y por defecto, seguridad, registro de actividades, evaluación de impacto y consulta previa cuando el riesgo residual siga siendo alto. La identidad sintética debería tratarse como un fenómeno de alto riesgo cuando implique biometría, escala masiva, datos sensibles, perfilado, personas vulnerables, irreversibilidad práctica o generación de contenidos capaces de producir daño reputacional, sexual, económico o político.

El derecho de supresión plantea aquí una dificultad específica. Su ejercicio parece relativamente claro cuando la persona solicita la retirada de una fotografía, un audio o un vídeo identificable de una base de datos concreta; se vuelve mucho más incierto cuando esos materiales han sido replicados en conjuntos de datos de terceros, incorporados a procesos de entrenamiento o absorbidos por modelos ya distribuidos. En estos casos, la supresión del dato originario no garantiza necesariamente la desaparición de la capacidad del sistema para reproducir rasgos, patrones o similitudes vinculadas a la persona. De ahí que empiecen a adquirir relevancia técnica y jurídica nociones como el desentrenamiento, la eliminación selectiva de datos de entrenamiento, la documentación de procedencia o la imposición de medidas de bloqueo y no reutilización. Aunque el RGPD no formula expresamente un derecho al desentrenamiento del modelo, la efectividad del artículo 17 difícilmente puede evaluarse sin atender a estas posibilidades técnicas, a sus costes, a su proporcionalidad y al

[13] Reglamento (UE) 2016/679, considerando 51.

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

[15] Agencia Española de Protección de Datos, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos* (Madrid: AEPD, 2023).

[16] Reglamento (UE) 2016/679, art. 9.2.e.

[17] Edward S. Dove y Jiahong Chen, "What Does It Mean for a Data Subject to Make Their Personal Data 'Manifestly Public'? An Analysis of GDPR Article 9(2)(e)", *International Data Privacy Law* 11, n.º 2 (2021): 107-124, DOI 10.1093/idpl/ipab005; Ludmila Georgieva y Christopher Kuner, "Article 9 Processing of Special Categories of Personal Data", en *The EU General Data Protection Regulation (GDPR): A Commentary*, ed. Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler y Luca Tosoni, 365-384 (Oxford: Oxford University Press, 2020), DOI 10.1093/oso/9780198826491.003.0038; European Data Protection Board, Guidelines 05/2022 en *Use of Facial Recognition Technology in the Area of Law Enforcement*, version 2.0, adopted on 26 April 2023, párr. 76; Council of Europe, *Guidelines on Facial Recognition*, T-PD(2020)03rev4, 28 January 2021.

riesgo residual que permanece cuando la identidad sintética puede seguir generándose a partir de modelos ya entrenados[18].

El límite del RGPD aparece con claridad cuando el daño excede la cadena de tratamiento. La norma no protege la voz como voz, ni la imagen como propia imagen, ni una canción como obra, ni un signo como marca. Protege a la persona frente al tratamiento de datos personales. Esa delimitación resulta útil, porque evita cargar al RGPD con funciones que pertenecen a otros regímenes, pero también muestra la necesidad de una cartografía. Una voz clonada en un anuncio falso puede implicar tratamiento ilícito de datos personales, aunque el núcleo del daño se sitúe en la apropiación de una identidad para fines comerciales. Una imagen sexualizada puede implicar tratamiento de datos personales, aunque el daño más intenso afecte a la intimidad, la dignidad y la imagen. Un vídeo político manipulado puede implicar tratamiento de datos, aunque su fuerza lesiva proceda de la distorsión pública de la posición de una persona. La capa de protección de datos es imprescindible, pero no es total.

4.2. Honor, intimidad y propia imagen: la identidad sintética como intromisión

La LO 1/1982 resulta central cuando el daño no se formula únicamente como tratamiento de datos, sino como intromisión en la esfera personal. Esta norma protege civilmente los derechos al honor, a la intimidad personal y familiar y a la propia imagen, que declara irrenunciables, inalienables e imprescriptibles, sin perjuicio de las autorizaciones o consentimientos concretos previstos en la propia ley[19]. En el terreno de la identidad sintética, sus artículos 7.5, 7.6 y 7.7 adquieren una relevancia evidente: captación, reproducción o publicación de la imagen por cualquier procedimiento en determinados contextos; utilización del nombre, la voz o la imagen para fines publicitarios, comerciales o de naturaleza análoga; e imputación de hechos o manifestación de juicios de valor que lesionen la dignidad, menoscabando la fama o atentando contra la propia estimación[20].

Esta capa permite abordar los supuestos en los que el daño aparece como apropiación o distorsión de la presencia personal. Un anuncio con una voz clonada coloca a alguien en el mercado recomendando un producto que jamás autorizó; una imagen sexualizada generada mediante IA afecta a la intimidad, a la imagen y a la dignidad aunque no reproduzca una fotografía concreta; un vídeo político manipulado puede atribuir a una persona una posición pública que no sostuvo. En estos casos, la identidad sintética opera como intromisión porque altera la relación de la persona con su modo de aparecer ante los demás.

Los artículos 7.6 y 7.7 permiten traducir jurídicamente dos daños frecuentes. El primero ofrece un punto de apoyo especialmente valioso para los usos comerciales, porque menciona expresamente la voz junto al nombre y la imagen; una voz sintética que promociona un producto o legitima una campaña vincula a la persona con un mensaje que no emitió y con una finalidad que no escogió. El segundo permite abordar la distorsión reputacional cuando se atribuyen hechos, declaraciones o posiciones que dañan la fama o la consideración social, como ocurre en vídeos políticos falsos, audios apócrifos o declaraciones inventadas.

La intimidad adquiere un lugar propio en los *deepfakes* sexuales o en las imágenes sintéticas que sitúan a la persona en escenas íntimas, corporales o sexualizadas. La lesión no depende de que el acontecimiento haya ocurrido, porque precisamente su falsedad forma parte del daño. La imagen creada no revela un secreto previo, pero produce una exposición íntima artificial. Esta idea resulta importante porque ciertas concepciones estrechas de la privacidad tienden a asociar la lesión con la difusión de información verdadera que debía permanecer reservada. La identidad sintética muestra que también puede haber invasión cuando se fabrica una apariencia íntima falsa, capaz de humillar, estigmatizar o erosionar la agencia sexual y reputacional de la persona afectada.

El consentimiento debe interpretarse de forma particularmente estricta. La autorización de un uso de imagen o voz en un contexto concreto no puede extenderse mecánicamente a cualquier uso posterior, menos aún cuando la tecnología permite generar nuevos actos comunicativos, visuales o sonoros que la persona nunca produjo. La lógica de la integridad contextual ayuda a interpretar los límites de dichas autorizaciones: consentir una entrevista, una sesión fotográfica, una interpretación musical o una campaña determinada no equivale a consentir la producción indefinida de dobles sintéticos. El consentimiento otorgado para fijar una presencia no debe entenderse como consentimiento para fabricar otras presencias.

[18] Reglamento (UE) 2016/679, art. 17.

[19] 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, arts. 1 y 2.

[20] Ley Orgánica 1/1982, art. 7.5, 7.6 y 7.7.

El artículo 9 de la LO 1/1982 completa el régimen al prever medidas de tutela judicial, incluyendo la adopción de medidas necesarias para poner fin a la intromisión, restablecer al perjudicado en el pleno disfrute de sus derechos, prevenir intromisiones inminentes o ulteriores e indemnizar los daños y perjuicios causados[21]. En la identidad sintética, estas medidas tienen un valor práctico evidente: retirada de contenidos, cese de usos comerciales, prohibición de nuevas difusiones, indemnización por daño moral, publicación de la sentencia o adopción de medidas técnicas para limitar la propagación. No obstante, la eficacia de estos remedios dependerá de la rapidez de actuación, de la identificación de responsables y de la posibilidad material de retirar contenidos que pueden haber sido replicados en múltiples plataformas.

4.3. Propiedad intelectual: obras, prestaciones y el límite de la imitación

La propiedad intelectual ocupa una posición necesaria y, al mismo tiempo, insuficiente. Es necesaria porque gran parte de los materiales que alimentan o vehiculan la identidad sintética son obras, prestaciones, fonogramas, grabaciones audiovisuales o fotografías protegidas. La LPI protege creaciones originales expresadas por cualquier medio o soporte, incluidas composiciones musicales, obras audiovisuales y obras fotográficas; reconoce derechos de explotación como reproducción, distribución, comunicación pública y transformación; y contempla derechos de artistas intérpretes o ejecutantes, productores de fonogramas y realizadores de meras fotografías[22].

Esta capa permite actuar con mayor claridad cuando la IA reproduce una grabación concreta, utiliza una fotografía protegida, transforma una obra musical, comunica públicamente una pieza protegida o explota una interpretación fijada. En el ámbito musical, por ejemplo, la generación de una canción que incorpore fragmentos de una grabación preexistente, reproduzca sustancialmente una composición o utilice una interpretación fijada podrá activar derechos de autor, derechos de artistas intérpretes o ejecutantes y derechos de productores de fonogramas. En el ámbito visual, la utilización de una fotografía protegida para producir un *resultado* derivado puede convocar reproducción o transformación, según la operación realizada y el grado de incorporación del material originario.

El entrenamiento de modelos introduce una dificultad añadida. Aunque la discusión doctrinal y jurisprudencial sobre si el entrenamiento implica reproducción relevante, uso transformativo, minería de textos y datos o infracción de derechos sigue abierta en muchos ordenamientos, en el marco europeo resulta imprescindible atender a la Directiva (UE) 2019/790 y a su transposición española. El Real Decreto-ley 24/2021 introdujo en España límites vinculados a minería de textos y datos, distinguiendo usos para investigación científica y otros usos permitidos siempre que el titular de derechos no haya reservado expresamente sus derechos de manera adecuada[23]. El Reglamento de IA añade a este punto una obligación propia para proveedores de modelos de IA de uso general: establecer directrices para cumplir el Derecho de la Unión en materia de derechos de autor y derechos afines, incluida la detección y cumplimiento de reservas de derechos, y publicar un resumen suficientemente detallado del contenido utilizado para el entrenamiento[24].

Aun así, la propiedad intelectual no ofrece una respuesta cómoda cuando el daño procede de la imitación de una identidad sin copia sustancial de una obra concreta. Una canción nueva "con la voz de" una artista puede no reproducir una composición anterior ni incorporar una grabación específica, pero aun así apropiarse de una identidad vocal reconocible. Un anuncio puede explotar una apariencia sin copiar una fotografía determinada. Un avatar puede evocar un estilo performativo sin reproducir literalmente una obra. En esos supuestos, la LPI puede quedarse corta porque protege obras y prestaciones, no la voz, el rostro, el estilo o la identidad pública en abstracto.

Este límite explica buena parte de la búsqueda de estrategias complementarias, incluidas marcas, derechos de imagen, publicidad, competencia desleal o acciones de responsabilidad civil. En la identidad sintética, la infracción del *copyright* puede ser la puerta de entrada cuando existen obras o grabaciones utilizadas sin autorización, pero el daño más propio de la simulación generativa no siempre consiste en copiar una obra. A menudo consiste en producir algo nuevo que parece proceder de alguien. Esa diferencia resulta decisiva. El derecho de autor protege la creación; la identidad sintética afecta a la atribución social de presencia, palabra, imagen o interpretación.

Conviene mantener separadas las preguntas sobre entrenamiento y resultado. El entrenamiento puede utilizar obras protegidas, fotografías, fonogramas o vídeos sin que el resultado final repro-

[21] Ley Orgánica 1/1982, art. 9.

[22] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, arts. 10, 17, 18, 20, 21, 106-108, 115-116 y 128.

[23] Real Decreto-ley 24/2021, de 2 de noviembre, arts. 66 y 67.

[24] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, art. 53.1.c y 53.1.d.

duzca de manera reconocible ninguno de esos materiales; a la inversa, un resultado puede lesionar la propia imagen o la reputación aunque no exista una infracción clara durante el entrenamiento. La licitud de una fase no sanea automáticamente la otra. Entre ambas intervienen decisiones técnicas, instrucciones de usuario, mecanismos de filtrado, políticas de despliegue y contextos de difusión que deben analizarse por separado.

4.4. Marca: signo distintivo y defensa lateral

La propiedad industrial ocupa en esta cartografía una posición lateral pero reveladora. La Ley de Marcas permite proteger palabras, nombres de personas, imágenes o sonidos cuando cumplen una función distintiva y sirven para identificar productos o servicios en el mercado. Desde ahí se entiende el carácter sintomático del caso Taylor Swift: la marca no protege toda la personalidad, pero puede ofrecer una herramienta frente a usos comerciales de la identidad sintética cuando existe riesgo de confusión, asociación o aprovechamiento del carácter distintivo o del renombre[25].

La propia Ley de Marcas contiene límites relevantes para signos vinculados a personas, al impedir el registro sin autorización del nombre civil, la imagen u otros signos que identifiquen a alguien distinto del solicitante. Esa conexión entre signo distintivo e identidad personal puede servir para impedir apropiaciones marcarias de rasgos ajenos, aunque su alcance sigue siendo limitado: la marca no protege una voz por pertenecer a alguien, ni un rostro como dimensión personal, ni un estilo artístico como tal. Funciona cuando la identidad se ha convertido en signo distintivo; la identidad sintética excede con mucho ese supuesto[26].

4.5. Reglamento de IA: sistema, modelo y resultado sintético

El Reglamento de IA añade una capa distinta, porque no protege directamente una obra, una marca o una imagen personal, sino que introduce obligaciones sobre sistemas, modelos y determinados resultados. En materia de identidad sintética, su relevancia aparece en las prácticas prohibidas del artículo 5, las definiciones del artículo 3, las obligaciones de transparencia del artículo 50, las obligaciones de los proveedores de modelos de IA de uso general del artículo 53 y la clasificación de ciertos sistemas biométricos o de reconocimiento de emociones como sistemas de alto riesgo conforme al anexo III. Esta capa se suma al RGPD cuando hay tratamiento de datos personales; no lo sustituye[27].

De hecho, la definición de ultrasuplantación del artículo 3.60 es uno de los puntos más cercanos al concepto de identidad sintética. El Reglamento entiende por ultrasuplantación un contenido de imagen, audio o vídeo generado o manipulado por IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y puede inducir a una persona a pensar erróneamente que son auténticos o verídicos[28]. Esta definición no exige necesariamente la lesión de derechos de la personalidad ni la existencia de datos biométricos, pero capta una parte del fenómeno: la producción de apariencias audiovisuales capaces de ser confundidas con lo real. El doble sintético se sitúa dentro de esa familia, aunque no se agota en ella, porque puede operar también como voz comercial, avatar, simulación conversacional o imitación performativa.

Con todo, el artículo 50 resulta especialmente importante para los contenidos sintéticos. En su apartado 2, impone a los proveedores de sistemas de IA que generen contenido sintético de audio, imagen, vídeo o texto la obligación de velar porque los resultados estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados artificialmente[29]. En su apartado 4, obliga a los responsables del despliegue de sistemas que generen o manipulen imágenes o contenidos de audio o vídeo constitutivos de ultrasuplantación a hacer público que esos contenidos han sido generados o manipulados de manera artificial, con excepciones y modulaciones para usos autorizados por ley y para obras o programas creativos, satíricos, artísticos, de ficción o análogos[30].

Esta obligación tiene valor, pero no debe sobredimensionarse. La transparencia informa sobre la naturaleza artificial del contenido, pero no convierte en lícito un tratamiento de datos personales

[25] Ley 17/2001, de 7 de diciembre, de Marcas, arts. 4 y 34.

[26] Ley 17/2001, art. 9.

[27] Reglamento (UE) 2024/1689, arts. 3, 5, 50, 53 y anexo III.

[28] Reglamento (UE) 2024/1689, art. 3.60.

[29] Reglamento (UE) 2024/1689, art. 50.2.

[30] Reglamento (UE) 2024/1689, art. 50.4.

carente de base jurídica, ni sustituye el consentimiento para usar la imagen o voz de una persona, ni repara un daño reputacional, sexual o comercial. Un *deepfake* sexual etiquetado sigue pudiendo lesionar la intimidad y la imagen. Un anuncio falso marcado como sintético puede seguir apropiándose de una voz o de una apariencia con fines comerciales. Un vídeo político manipulado que declare su artificialidad puede seguir explotando la reconocibilidad de una persona. La transparencia reduce el riesgo de engaño, pero no agota el análisis jurídico.

El artículo 53 desplaza la mirada hacia los modelos de IA de uso general. Los proveedores deben elaborar y mantener documentación técnica, poner cierta información a disposición de proveedores posteriores, establecer directrices para cumplir el Derecho de la Unión en materia de derechos de autor y derechos afines —incluida la detección y cumplimiento de reservas de derechos— y publicar un resumen suficientemente detallado del contenido utilizado para el entrenamiento. Para la identidad sintética, esta obligación tiene una importancia práctica clara, porque muchos dobles sintéticos se producen a partir de modelos entrenados con grandes volúmenes de contenido audiovisual, textual y sonoro. La trazabilidad del entrenamiento, aunque sea parcial, puede ayudar a conocer qué tipos de materiales alimentan los modelos y a discutir la relación entre obras, datos personales, voces, imágenes y resultados[31].

El Reglamento de IA también es relevante cuando la identidad sintética se cruza con biometría, categorización o reconocimiento de emociones. El artículo 5.1.e prohíbe crear o ampliar bases de reconocimiento facial mediante extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión. El artículo 5.1.f prohíbe, salvo excepciones médicas o de seguridad, inferir emociones en lugares de trabajo y centros educativos, y el artículo 5.1.g prohíbe determinadas categorizaciones biométricas destinadas a deducir o inferir categorías sensibles. El anexo III clasifica además como de alto riesgo ciertos sistemas de identificación biométrica remota, categorización biométrica y reconocimiento de emociones[32].

Conviene distinguir, sin embargo, el plano del Reglamento de IA y el del RGPD. El artículo 5.1.g del Reglamento de IA se dirige a determinadas prácticas de categorización biométrica que clasifican individualmente a las personas para deducir o inferir categorías sensibles; el artículo 9 RGPD, en cambio, regula el tratamiento de categorías especiales de datos personales, incluidos los datos biométricos cuando se tratan con la finalidad de identificar de manera unívoca a una persona física. Ambos preceptos pueden concurrir, pero no cumplen la misma función. El primero opera como límite a ciertas prácticas de clasificación algorítmica; el segundo impone una prohibición general de tratamiento salvo excepción aplicable. En la identidad sintética, esta diferencia resulta importante porque un mismo rostro o una misma voz pueden servir para generar una presencia artificial, para identificar a una persona o para inferir categorías especialmente protegidas[33].

Estas previsiones muestran que el Reglamento de IA no se limita a exigir etiquetas en los *deepfakes*. Interviene también en prácticas biométricas especialmente intrusivas, en la inferencia emocional y en la clasificación sensible. Para la identidad sintética esto resulta relevante porque rostro y voz pueden utilizarse para generar un doble artificial, pero también para identificar, autenticar, categorizar o inferir estados y atributos de la persona.

Esta capa debe leerse con cautela. Aporta herramientas imprescindibles para ordenar sistemas, modelos y resultados —transparencia, marcado, documentación y prohibición de determinadas prácticas—, pero no crea un derecho general a la voz ni a la imagen, no sustituye las acciones civiles por intromisión ilegítima, no regula de manera exhaustiva el entrenamiento con datos personales ni resuelve todos los conflictos de propiedad intelectual. Su función dentro de la cartografía es ordenar la infraestructura de producción y circulación de la identidad sintética, no absorber todas las lesiones que esta puede producir.

5. Aplicación por escenarios

La cartografía adquiere sentido cuando se aplica a escenarios concretos. El apartado anterior distinguía capas normativas; este apartado muestra cómo esas capas se superponen en casos recurrentes. La finalidad no es ofrecer respuestas cerradas para todos los supuestos, sino proponer una matriz de lectura: qué operación técnica se realiza, qué flujo contextual se rompe, qué daño describe mejor la taxonomía de Solove, qué tipo de doble se produce y qué normas pueden intervenir.

[31] Reglamento (UE) 2024/1689, art. 53.1.

[32] Reglamento (UE) 2024/1689, arts. 5.1.e, 5.1.f, 5.1.g y anexo III.

[33] Reglamento (UE) 2024/1689, art. 5.1.g; Reglamento (UE) 2016/679, art. 9.

5.1. Scraping de imágenes, vídeos y audios identificables

El *scraping* de imágenes, vídeos o audios identificables constituye la fase de recopilación más evidente. Puede realizarse sobre redes sociales, plataformas de vídeo, bancos de imágenes, entrevistas, podcasts, retransmisiones, webs institucionales o archivos informativos. En términos de Solove, nos situamos ante vigilancia, recopilación y, muchas veces, agregación anticipada. Desde Nissenbaum, el problema aparece como ruptura de flujo: materiales producidos para una audiencia o finalidad concreta pasan a integrarse en *datasets* orientados a entrenamiento, identificación, clasificación o generación.

Desde el RGPD, la cuestión inicial será determinar si esos materiales contienen datos personales. Una fotografía, un vídeo o una grabación de voz de una persona identificada o identificable entran en el artículo 4.1, y su descarga, extracción, almacenamiento u organización constituyen tratamiento conforme al artículo 4.2. La operación deberá contar con una base jurídica del artículo 6, respetar los principios del artículo 5 y cumplir las obligaciones de información de los artículos 13 o 14, salvo excepción aplicable. Si el *scraping* crea o amplía bases de reconocimiento facial mediante extracción no selectiva de imágenes de internet o CCTV, aparece además la prohibición del artículo 5.1.e del Reglamento de IA. La propiedad intelectual intervendrá si los materiales son obras, fonogramas, vídeos o fotografías protegidas; la LO 1/1982, si la captación o reproducción afecta a la propia imagen o a usos comerciales de voz o imagen.

5.2. Entrenamiento de modelos con canciones, entrevistas, videoclips o fotografías

El entrenamiento desplaza el análisis hacia el procesamiento. La información recopilada se convierte en material de aprendizaje, ajuste o generación. En términos de Solove, aparecen agregación, identificación, uso secundario, inseguridad y exclusión: materiales dispersos se integran en una infraestructura común, se vinculan a una persona o permiten producir resultados reconocibles, cambian de finalidad y quedan incorporados a sistemas sobre los que la persona afectada suele tener escasa información y menor capacidad de intervención.

El RGPD obliga a examinar base jurídica, finalidad y compatibilidad del uso ulterior. Si una entrevista se publicó con fines informativos, una canción se difundió para escucha pública o una fotografía se compartió en redes, la reutilización para entrenar modelos generativos no puede asumirse automáticamente como compatible. La propiedad intelectual tendrá un papel destacado si el entrenamiento incorpora obras, interpretaciones, fonogramas o fotografías protegidas, con atención a los límites de minería de textos y datos y a la reserva de derechos. El Reglamento de IA intervendrá especialmente ante modelos de IA de uso general, mediante obligaciones de documentación, política de respeto del copyright y resumen del contenido utilizado en entrenamiento.

5.3. Clonación de voz para publicidad, fraude o atención automatizada

La clonación de voz concentra algunos de los problemas más difíciles de la identidad sintética, porque la voz puede funcionar a la vez como dato personal, dato biométrico, atributo de personalidad, interpretación protegida, marca sonora o resultado sintético. Cuando se utiliza en un anuncio falso, la apropiación resulta evidente: el artículo 7.6 de la LO 1/1982 ofrece una vía directa si se emplea la voz, el nombre o la imagen para fines publicitarios, comerciales o análogos sin autorización. El RGPD puede intervenir por el tratamiento de grabaciones, huellas vocales o datos utilizados para generar la voz; la LPI será relevante si se copia una grabación o interpretación fijada; la marca puede reforzar la reacción si la voz o frase tiene valor distintivo registrado; y el Reglamento de IA exigirá marcado o transparencia cuando el audio constituya ultrasuplantación o contenido sintético sujeto al artículo 50.

Cuando la clonación se utiliza para fraude o atención automatizada, el análisis se desplaza hacia la seguridad, el vínculo de confianza y la extensión del consentimiento. Simular la voz de una persona de confianza explota una credencial social. Si una empresa reutiliza grabaciones para generar nuevas locuciones, habrá que examinar base jurídica, cesiones contractuales, derechos de intérprete, límites de finalidad y grado de reconocibilidad. En estos supuestos, la identidad sintética aparece también como conflicto laboral, contractual y de seguridad.

5.4. Música sintética que parece interpretada por un artista en concreto

Una canción sintética que parece interpretada por un artista en concreto, sin copia directa de una grabación, muestra con claridad las costuras del sistema. Si el resultado reproduce una obra musical, una letra o una grabación, la propiedad intelectual ofrece un marco relativamente reconocible. Si genera una composición nueva con una voz artificial identificable, el problema cambia: la persona

parece cantar algo que no cantó y el público puede atribuir la interpretación a quien no intervino. La identidad vocal se separa entonces de la voluntad artística.

Desde el RGPD habría que examinar si la voz generada deriva del tratamiento de datos personales o biométricos; desde la LO 1/1982, si la explotación comercial o la atribución de determinados mensajes afecta a la voz, imagen u honor; desde la LPI, si hubo uso de obras, fonogramas o interpretaciones protegidas durante el entrenamiento o en el resultado; desde la marca, si existen signos sonoros o denominativos registrados; y desde el Reglamento de IA, si el audio sintético exige marcado o transparencia. Puede haber imitación dañina sin copia sustancial de obra, explotación de una voz sin reproducción de fonograma y confusión pública sin infracción marcaria directa.

5.5. Imagen sexualizada generada mediante IA

La imagen sexualizada generada mediante IA constituye uno de los casos más graves de identidad sintética como invasión. En la taxonomía de Solove aparecen exposición, distorsión, apropiación e invasión; desde Nissenbaum, la ruptura contextual es radical, porque una imagen de rostro, una fotografía ordinaria o un vídeo público se reensamblan para producir una escena íntima o sexual que la persona no vivió ni consintió. La falsedad del contenido no reduce el daño: muchas veces lo intensifica, porque obliga a la persona afectada a enfrentarse a una imagen que sabe falsa, pero que circula como si revelara algo de su cuerpo o de su sexualidad.

El RGPD puede intervenir si la imagen identifica a la persona y si se han tratado datos personales para generarla o difundirla; el artículo 9 puede adquirir relevancia cuando el contenido revele o sugiera aspectos relativos a la vida sexual, salud, orientación sexual u otras categorías sensibles, con los matices que exige el análisis de datos sintéticos. La LO 1/1982 ofrece una vía central por intimidad, propia imagen y honor. La propiedad intelectual tendrá un papel secundario salvo que se haya usado una fotografía protegida u otra obra preexistente; la marca será normalmente irrelevante. El Reglamento de IA exigirá transparencia si el contenido constituye ultrasuplantación, pero esa etiqueta no evita la humillación, la sexualización ni la circulación lesiva.

5.6. Vídeo político falso con rostro y voz

El vídeo político falso con rostro y voz combina distorsión, accesibilidad incrementada e interferencia en la formación de la opinión pública. Puede afectar a una candidata, una periodista, una activista, una jueza, una investigadora o cualquier persona cuya voz pública pueda ser instrumentalizada. La identidad sintética opera aquí como atribución falsa de discurso: coloca a la persona afectada en la necesidad de desmentir una presencia audiovisual que parece probar aquello que nunca ocurrió.

Desde el RGPD, se tratarán datos personales si el rostro o la voz permiten identificar a la persona y se han utilizado materiales previos para producir el vídeo. Desde la LO 1/1982, el artículo 7.7 será relevante cuando se atribuyan hechos o declaraciones que lesionen la dignidad, fama o propia estimación, junto con el artículo 7.5 por uso de imagen. La propiedad intelectual dependerá de la incorporación de materiales protegidos. El Reglamento de IA exige transparencia en los *deepfakes* audiovisuales, pero la advertencia sobre la artificialidad no agota el daño cuando la pieza contamina la deliberación pública o erosiona la confianza en la prueba audiovisual.

5.7. Autenticación facial o vocal en banca, plataformas o accesos

La autenticación facial o vocal pertenece a otra familia de problemas. Aquí el doble sintético amenaza la función de la biometría como mecanismo de verificación. Si el rostro o la voz se utilizan para confirmar identidad, el tratamiento puede incluir datos biométricos en el sentido del artículo 4.14 RGPD, con posible activación del artículo 9 cuando esté dirigido a identificar de manera unívoca a una persona. La pregunta central será si el tratamiento es necesario, proporcionado, seguro y si existen alternativas menos intrusivas.

La AEPD ha insistido en la necesidad de superar el análisis de idoneidad, necesidad y proporcionalidad en tratamientos biométricos. Estos criterios son trasladables a otros usos de autenticación: la biometría promete comodidad y seguridad, pero crea riesgos por la inmutabilidad del rasgo, la dificultad de revocación, los falsos positivos, las exclusiones, los usos secundarios y las brechas de seguridad. La identidad sintética añade el riesgo de engañar al sistema mediante voz o rostro generados artificialmente, lo que puede llevar a reforzar aún más la vigilancia[34].

[34] Agencia Española de Protección de Datos, *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*.

5.8. Reconocimiento de emociones y categorización biométrica desde rostro o voz

El reconocimiento de emociones y la categorización biométrica desplazan la identidad sintética hacia la inferencia. La voz y la cara ya no sirven para representar a una persona, sino para deducir estados, características o categorías: cansancio, estrés, atención, credibilidad, satisfacción, tristeza, edad, género, origen u otros rasgos protegidos. La taxonomía de Solove permite ubicar el daño en agregación, identificación, uso secundario, exclusión y distorsión, porque la persona queda sometida a una lectura técnica de sí misma que puede ser errónea, reductora o discriminatoria.

Desde el RGPD, estos tratamientos pueden implicar perfilado del artículo 4.4, datos biométricos del artículo 4.14, categorías especiales del artículo 9, decisiones automatizadas del artículo 22 y evaluación de impacto del artículo 35. El Reglamento de IA endurece el análisis: el artículo 5.1.f prohíbe, salvo motivos médicos o de seguridad, los sistemas destinados a inferir emociones en lugares de trabajo y centros educativos, y el artículo 5.1.g prohíbe determinadas categorizaciones biométricas sensibles. En este punto, la identidad sintética y la biometría se encuentran: la persona puede ser simulada mediante voz o rostro, pero también clasificada e interpretada por sistemas que dicen leer esos mismos rasgos.

5.9. Matriz de síntesis

La siguiente matriz propone resumir la cartografía propuesta, entendida como herramienta de orientación y no como sustituto del análisis caso por caso:

Escenario	Daño / operación	Capa jurídica principal	Artículos y matices
Scraping de imágenes, vídeos o audios	Recopilación, vigilancia, ruptura de flujo	RGPD; LO 1/1982; LPI; Reglamento de IA	RGPD arts. 4.1, 4.2, 5, 6 y 13-14; LO 1/1982 arts. 7.5 y 7.6 si hay uso de imagen o voz; LPI si hay obras o fotografías; Reglamento de IA art. 5.1.e si se crean bases faciales mediante scraping indiscriminado.
Entrenamiento de modelos	Procesamiento, agregación, uso secundario	RGPD; LPI; Reglamento de IA	RGPD arts. 5, 6, 9, 14, 21 y 35; LPI y límites de minería de textos y datos; Reglamento de IA art. 53 para modelos de IA de uso general.
Clonación de voz comercial	Apropiación, distorsión, falsa atribución	LO 1/1982; RGPD; LPI; marcas; Reglamento de IA	LO 1/1982 arts. 7.6 y 7.7; RGPD si hay tratamiento de voz o huella vocal; LPI si se copia grabación o interpretación; Ley de Marcas arts. 4, 8, 9, 34 y 41; Reglamento de IA art. 50.
Canción con voz sintética	Apropiación de identidad vocal	LO 1/1982; LPI; RGPD; marcas; Reglamento de IA	La LPI será central si hay obra, fonograma o interpretación copiada; resulta más débil ante imitación pura. Pueden operar LO 1/1982 arts. 7.6 y 7.7, RGPD si la voz deriva de datos personales, marca si hay signo registrado y Reglamento de IA arts. 50 y 53.
Imagen sexualizada	Exposición, invasión, distorsión	LO 1/1982; RGPD; Reglamento de IA	LO 1/1982 arts. 7.1, 7.3, 7.5, 7.7 y 9; RGPD arts. 5, 6, 9 y 17 si identifica o revela datos sensibles; Reglamento de IA art. 50. LPI solo si se copia una fotografía u obra.
Vídeo político falso	Distorsión e interferencia pública	LO 1/1982; RGPD; Reglamento de IA	LO 1/1982 arts. 7.5 y 7.7; RGPD arts. 5, 6, 17, 21 y 22 según uso; Reglamento de IA art. 50; LPI según materiales incorporados.
Autenticación facial o vocal	Identificación, inseguridad, exclusión	RGPD; Reglamento de IA	RGPD arts. 4.14, 5, 6, 9, 22, 25, 32 y 35; Reglamento de IA anexo III según sistema y art. 50.3 si hay categorización o emociones.
Reconocimiento de emociones	Inferencia, clasificación, exclusión	RGPD; Reglamento de IA	RGPD arts. 4.4, 4.14, 5, 6, 9, 22 y 35; Reglamento de IA art. 5.1.f y anexo III. LO 1/1982 puede intervenir si hay daño a dignidad o imagen.

Tabla 1. Cartografía jurídica de la Identidad Sintética. Fuente: Elaboración propia.

6. ¿Más normas o mejor ensamblaje normativo?

La identidad sintética muestra que los retos jurídicos de la IA generativa no proceden únicamente de una carencia normativa, sino de una dificultad de articulación entre regímenes diseñados para proteger objetos distintos. El RGPD protege frente al tratamiento ilícito de datos personales; los derechos al honor, a la intimidad y a la propia imagen protegen la esfera personal frente a intromisiones ilegítimas; la propiedad intelectual protege obras y prestaciones; la marca protege signos distintivos; y el Reglamento de IA introduce obligaciones sobre sistemas, modelos y contenidos sintéticos. El doble sintético atraviesa todas esas categorías, porque puede nacer de datos personales, alimentarse de obras protegidas, adoptar la forma de una voz o imagen reconocible, circular como *deepfake* y producir apropiación, distorsión o daño reputacional.

La respuesta no debería formularse entonces en términos de más o menos regulación. El marco europeo y español ya ofrecen herramientas relevantes para muchos supuestos. Sería inexacto afirmar que la IA generativa opera en un vacío jurídico absoluto. Derecho hay; la dificultad aparece al calificar la operación concreta, probar la cadena técnica, coordinar remedios y evitar que cada régimen actúe como si el daño pudiera encerrarse en su propio objeto protegido. Tampoco basta con afirmar que todo se resuelve aplicando mejor lo existente. La voz como timbre personal no encaja cómodamente en el copyright si no hay copia de una grabación; la imagen sintética puede no reproducir una fotografía concreta y, aun así, apropiarse de una identidad reconocible; la transparencia del *deepfake* no equivale a consentimiento ni repara por sí misma el daño; y las reglas de entrenamiento de modelos siguen generando incertidumbre cuando confluyen obras protegidas, datos personales, interpretaciones, imágenes y voces. La prueba de origen de los *datasets*, similitud, atribución, entrenamiento, responsabilidad y daño seguirá siendo uno de los grandes puntos de tensión.

Por eso quizá no sea necesaria una codificación total de la identidad sintética como primer reflejo regulatorio. Sí parece necesaria una arquitectura de aplicación coordinada que articule protección de datos, derechos de la personalidad, propiedad intelectual, propiedad industrial, competencia desleal, responsabilidad civil y Reglamento de IA. Esa arquitectura debería reforzar la trazabilidad de los materiales de entrenamiento, aclarar la relación entre transparencia y consentimiento, facilitar mecanismos de retirada y reparación, mejorar la cooperación entre autoridades y ofrecer criterios probatorios capaces de responder a la opacidad técnica de los modelos.

Ahora bien, esa arquitectura no puede descansar únicamente sobre la capacidad individual de cada persona para reclamar, oponerse, registrar, litigar o desmentir. La identidad sintética permite ver con especial claridad que la privacidad no funciona solo como una prerrogativa individual, sino también como un bien público: cuando se normaliza la extracción de rostros, voces, gestos y estilos para producir presencias artificiales, no se debilita únicamente la posición de quien aparece en un contenido concreto, sino las condiciones compartidas que permiten confiar en la autenticidad de una voz, en la atribución de una imagen, en la posibilidad de presentarnos ante los demás sin quedar permanentemente disponibles para la recombinación técnica. En ese sentido, la defensa de la privacidad frente a la IA generativa requiere pensar también en un *procomún* de la privacidad, entendido no como una reserva romántica de lo íntimo, sino como el conjunto de normas, infraestructuras, prácticas y límites colectivos que hacen posible que la vida social no quede enteramente sometida al extractivismo de datos personales[35].

Desde esta perspectiva, aplicar mejor el Derecho existente no significa solo multiplicar acciones individuales, sino fortalecer las condiciones comunes de protección: minimizar la recolección de datos, exigir transparencia y rendición de cuentas sobre los modelos, impedir que la carga de la prueba recaiga siempre sobre la persona afectada, diseñar mecanismos eficaces de retirada, favorecer la acción colectiva y construir arquitecturas tecnológicas menos dependientes de la acumulación indiscriminada de información personal. La privacidad como *procomún* obliga a desplazar la pregunta desde "cómo se defiende cada individuo frente a su doble sintético" hacia otra más exigente: qué condiciones jurídicas, técnicas y sociales necesitamos para que la disponibilidad técnica de una voz, un rostro o una imagen pública no se convierta, sin más, en disponibilidad jurídica de la persona.

[35] Fátima Solera Navarro, Privacidad, res/xistencia y procomún frente al extractivismo de datos personales: O cómo hacer democracia a través de tácticas de litigación colectiva y ofuscación expresiva (tesis doctoral, Universidad de Málaga, 2025), conclusiones.

Bibliografía

Brooks, Brad. "Taylor Swift Files to Trademark Her Voice, Likeness to Ward off AI Deepfakes". *Reuters*, 27 de abril de 2026. https://www.reuters.com/legal/litigation/taylor-swift-files-trademark-her-voice-likeness-ward-off-ai-deepfakes-2026-04-27/

Clarke, Roger. "The Digital Persona and Its Application to Data Surveillance". *The Information Society* 10, n.º 2 (1994): 77-92. https://doi.org/10.1080/01972243.1994.9960160

Consejo de Europa. *Guidelines on Facial Recognition*. T-PD(2020)03rev4, 28 January 2021. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

Deleuze, Gilles. "Post-scriptum sobre las sociedades de control". En *Conversaciones*, traducido por José Luis Pardo, 277-286. Valencia: Pre-Textos, 1995.

Dove, Edward S., y Jiahong Chen. "What Does It Mean for a Data Subject to Make Their Personal Data 'Manifestly Public'? An Analysis of GDPR Article 9(2)(e)". *International Data Privacy Law* 11, n.º 2 (2021): 107-124. https://doi.org/10.1093/idpl/ipab005

European Data Protection Board. *Guidelines 3/2019 on Processing of Personal Data through Video Devices*. Bruselas: EDPB, 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

European Data Protection Board. *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*. Bruselas: EDPB, 2023. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en

Georgieva, Ludmila, y Christopher Kuner. "Article 9 Processing of Special Categories of Personal Data". En *The EU General Data Protection Regulation (GDPR): A Commentary*, editado por Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler y Luca Tosoni, 365-384. Oxford: Oxford University Press, 2020. https://doi.org/10.1093/oso/9780198826491.003.0038

Haggerty, Kevin D., y Richard V. Ericson. "The Surveillant Assemblage". *British Journal of Sociology* 51, n.º 4 (2000): 605-622. https://doi.org/10.1080/00071310020015280

Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press, 2001.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2009. https://doi.org/10.1515/9780804772891

Solera Navarro, Fátima. *Privacidad, res/xistencia y procomún frente al extractivismo de datos personales: O cómo hacer democracia a través de tácticas de litigación colectiva y ofuscación expresiva*. Tesis doctoral, Universidad de Málaga, 2025. https://riuma.uma.es/entities/publication/d9c150fc-a77f-459d-8242-32cbcd97b3e8

Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.