Tratamientos biométricos no identificantes mediante inteligencia artificial: riesgos para los derechos fundamentales en la confluencia entre el RGPD y el Reglamento (UE) de Inteligencia Artificial

Leire ESCAJEDO SAN-EPIFANIO (DNI 16054711K).

Profesora Titular de Derecho Constitucional en la Universidad del País Vasco (UPV/EHU). Doctora en Derecho (Universidad del País Vasco, 2004) y Doctora en Ciencias Biológicas (Universidad de Alicante, 2015)

I. Objetivos del trabajo

1. Objetivo general

Evaluar, desde un enfoque jurídico-técnico orientado a la gestión preventiva del riesgo, los efectos que los tratamientos biométricos no identificantes que se emplean en sistemas de inteligencia artificial pueden producir sobre los derechos y libertades fundamentales.

Al respecto, se presta especial atención a la situación jurídica en la que quedan dichos tratamientos en la confluencia entre, de una parte, el Reglamento (UE) 2016/679 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 (Reglamento General de Protección de Datos, RGPD) y, de otra, el Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial).

2. Objetivos específicos

(1) Delimitar conceptualmente los tratamientos biométricos no identificantes en sistemas de inteligencia artificial, distinguiéndolos tanto de la biometría identificante como de otras formas de perfilado no biométrico.

(2) Identificar y caracterizar los principales riesgos que estas prácticas plantean para los derechos y libertades fundamentales, en particular cuando la captación y el tratamiento de información corporal permiten inferencias continuas o situacionales.

(3) Analizar críticamente el tratamiento de estos riesgos en el Reglamento (UE) 2024/1689 de Inteligencia Artificial, evaluando en qué medida su sistema de clasificación por usos y contextos resulta insuficiente para captar los riesgos derivados del tratamiento inferencial de información corporal no orientado a la identificación.

(4) Examinar la aplicabilidad del RGPD a los tratamientos biométricos no identificantes, considerados como tratamientos de información corporal, e identificar los instrumentos jurídicos disponibles para una adecuada gestión *ex ante* del riesgo (en particular las evaluaciones de impacto en protección de datos y las obligaciones de protección de datos desde el diseño y por defecto).

(5) Proponer criterios operativos para la identificación, evaluación y mitigación del riesgo en tratamientos biométricos no identificantes basados en el uso inferencial de información corporal, mediante una aplicación reforzada y materialmente orientada del principio de responsabilidad proactiva, a modo de recomendación tanto para los responsables del tratamiento como para las autoridades de protección de datos.

II. Hipótesis de investigación

1. HIPÓTESIS PRINCIPAL

Determinadas modalidades de tratamientos biométricos no identificantes basados en sistemas de inteligencia artificial —en particular aquellas que operan mediante inferencias continuas en tiempo real— pueden generar riesgos elevados para los derechos y libertades fundamentales de las personas, comparables o incluso superiores a los asociados a ciertas formas de biometría identificante, pese a no activar, en muchos escenarios operativos, los niveles reforzados de protección previstos en el Reglamento (UE) 2024/1689 de Inteligencia Artificial.

En este contexto, tiene una especial trascendencia garantizar una aplicación reforzada, sistemática y materialmente orientada del principio de responsabilidad proactiva del RGPD, dado que en estos momentos es el principal instrumento disponible para la gestión preventiva de dichos riesgos.

2. HIPÓTESIS SECUNDARIAS

(1) La ausencia de finalidad identificante, atendiendo al funcionamiento efectivo de los sistemas, no constituye *per se* un criterio suficiente para descartar la existencia de riesgos elevados cuando la captación biométrica se orienta a la inferencia en tiempo real de estados emocionales, atencionales o conductuales, susceptibles de condicionar materialmente tanto la formación de la voluntad como el trato recibido por la persona.

(2) El marco jurídico en vigor presenta dificultades, en especial por el modo en el que confluyen a ese respecto el RGPD y el RIA. En concreto, la forma en que el RIA estructura y clasifica los riesgos en función de categorías de sistemas y contextos de uso tiende *a priori* a subestimar los riesgos derivados de la biometría no identificante de carácter inferencial, desplazando, por cuanto se refiere a su aplicación, el control efectivo hacia mecanismos reactivos y *ex post*.

(3) A corto o medio plazo no está prevista una reforma sustancial de la normativa. En el entre tanto, debe destacarse el hecho de que las mayores garantías para los derechos fundamentales orbitan en torno al RGPD, y se revela necesario ofrecer orientaciones prácticas que contribuyan a una buena gestión preventiva de estos riesgos, mediante la identificación sistemática del riesgo, la realización de evaluaciones de impacto en protección de datos y la aplicación de medidas de protección de datos desde el diseño y por defecto.

III. Texto principal

Tratamientos biométricos no identificantes mediante inteligencia artificial: riesgos para los derechos fundamentales en la confluencia entre el RGPD y el Reglamento (UE) de Inteligencia Artificial

§1. Introducción

§1.1. Planteamiento del problema práctico en el marco del Derecho de la Unión Europea

(1) En los últimos años se ha producido un despliegue progresivo y transversal, en muchos casos poco percibido, de sistemas de inteligencia artificial que captan y analizan señales corporales y conductuales en tiempo real. Estos sistemas plantean problemas jurídicos que no encuentran fácil acomodo en las categorías jurídicas que prevé la protección de datos en sentido clásico, ni siquiera tras la incorporación específica del concepto de datos biométricos singularizantes al RGPD. Su particularidad estriba en el hecho de que se trata de arquitecturas inferenciales continuas, que no persiguen la identificación singular sino la inferencia de patrones (emocionales, atencionales o conductuales) en la interacción con las personas.

En estos sistemas, la lógica de la interacción cobra por lo general un protagonismo mayor que la identificación, en la medida en que estas arquitecturas, con el fin de manejarse en la interacción con las personas, captan y tratan de interpretar señales corporales —como expresiones faciales, patrones de voz, movimientos oculares, postura o ritmo de interacción— mediante dispositivos integrados en cámaras, micrófonos, sensores o interfaces de uso ordinario. Dichas señales constituyen información corporal de la persona presente, que es tratada mediante técnicas de aprendizaje automático para inferir estados atencionales, emocionales o disposiciones conductuales, y para adaptar funcionalmente el entorno de interacción en tiempo real. A los efectos de este trabajo, el término *inferencia* se emplea en sentido técnico-estadístico, como estimación probabilística basada en correlaciones extraídas de conjuntos de entrenamiento y en modelos predictivos, y no como atribución causal ni como conocimiento concluyente sobre estados internos de la persona. Ello no impide, sin embargo, que estas inferencias —aun siendo inherentemente inciertas— produzcan efectos jurídicos materialmente relevantes cuando se integran en procesos automatizados de clasificación, adaptación o modulación del trato.

Aunque no haya un fin de identificación, las señales captadas son sometidas a un proceso de biometrización que permite su procesamiento ágil, aunque no se trate de un procesamiento con finalidad de identificación singular. Se diferencian, por tanto, de forma clara, del concepto de dato biométrico que *permite o confirma* la identificación única de una persona en los términos del artículo 4.14 del RGPD. No hay duda, en cualquier caso, de que se trata de datos personales —más concretamente, de información corporal— y de que su procesamiento los convierte técnicamente en datos biométricos, aunque no encajen en la categoría reforzada prevista en dicho precepto. Ello no obsta, sin embargo, a que deba analizarse su eventual encaje en otras

categorías de especial protección, atendiendo a su capacidad reveladora y a los efectos materiales del tratamiento.

(2) En los sistemas aquí considerados, la biometría no se emplea para responder a la pregunta «quién es esta persona», sino para responder a preguntas funcionales del tipo «*en qué estado se encuentra*», «*cómo es más probable que reaccione*» o «*qué intervención resulta más eficaz en este momento*». Dicho de otro modo, la persona no es identificada como individuo único, pero sí es interpretada y situada funcionalmente en un contexto concreto de interacción, mediante procesos automatizados de perfilado y categorización (Gutwirth & Hildebrandt, 2010; Wachter & Mittelstadt, 2019).

El presente trabajo parte de la premisa de que este tipo de tratamientos biométricos no identificantes, aun cuando no persigan la identificación singularizante, recaen sobre información corporal y generan inferencias sobre dimensiones internas de la persona; por ello, su relevancia jurídica no puede evaluarse exclusivamente en función de su encaje en las categorías clásicas de datos sensibles. Se hace necesario, por consiguiente, atender a los riesgos que este tipo de arquitecturas puede generar respecto a los derechos y libertades fundamentales, así como a la conveniencia de gestionarlos de forma preventiva.

(3) El desplazamiento desde usos identificantes de las biometrías hacia inferencias biométricas no constituye un fenómeno aislado. Se inscribe dentro de una reciente transformación de las arquitecturas digitales contemporáneas, que tiene un importante efecto en la forma en la que el Derecho de la UE viene articulando la protección de la persona y de sus derechos respecto al tratamiento automatizado de la información corporal. El desbordamiento se enmarca en una evolución más amplia: el paso del *Internet of Things* al *Internet of Everything*.

Desde un punto de vista técnico y jurídico, sin embargo, conviene precisar que el cuerpo humano no se integra en la red como un nodo consciente o voluntario, sino que es traducido en interfaz funcional mediante dispositivos de captación biométrica que convierten señales corporales y conductuales en datos procesables por el sistema. La captación de biometría no identificante se configura así como un fenómeno ambiental y distribuido, estrechamente vinculado al diseño mismo de los servicios digitales, y no como un acto puntual o excepcional de recogida de datos aislados (Hildebrandt, 2020; Escajedo San-Epifanio, 2024). En consecuencia, la evaluación del impacto de este tipo de arquitecturas difícilmente puede realizarse atendiendo únicamente a los datos puntuales recogidos —frecuentemente de escasa relevancia aislada—, sino que exige considerar el funcionamiento del sistema en su conjunto.

Desde el punto de vista jurídico, este fenómeno interpela directamente al núcleo material de protección de la persona en el Derecho de la Unión. Aunque no exista identificación única ni almacenamiento persistente de datos biométricos, estos tratamientos pueden incidir de manera significativa en la autonomía personal y la dignidad, en la igualdad material y la no discriminación, en la autodeterminación informativa y, de forma indirecta, en la efectividad de la tutela judicial, precisamente en la medida en que las inferencias y adaptaciones operan de forma continua, opaca y difícil de reconstruir *ex post*.

(4) El problema práctico que se plantea es, por tanto, si el sistema europeo de gobernanza normativa dispone de instrumentos adecuados para identificar y gestionar de forma preventiva los riesgos derivados de estas prácticas, o si la ausencia de finalidad identificante y de almacenamiento biométrico persistente genera zonas de desprotección estructural. En particular, se trata de determinar si el Reglamento (UE) 2024/1689 de Inteligencia Artificial (en adelante, RIA), con su enfoque basado en la clasificación de sistemas y contextos de uso, capta de forma suficiente los riesgos

asociados a la biometría no identificante de carácter inferencial, o si la tutela efectiva de los derechos fundamentales depende, en la práctica, de la aplicación transversal del RGPD y, en especial, de su lógica de gestión preventiva del riesgo.

§1.2. El contexto de elaboración del RGPD y el progresivo cambio de escenario tecnológico

(1) La posición que ocupan hoy los *tratamientos biométricos no identificantes* en el debate jurídico europeo no puede comprenderse adecuadamente sin atender al contexto tecnológico y normativo en el que se gestó el RGPD. Cuando el RGPD fue propuesto y negociado, entre 2012 y 2016, el desarrollo y la implantación generalizada de sistemas de inteligencia artificial con capacidad de inferencia automatizada en tiempo real no constituían todavía infraestructuras ordinarias de interacción, sino tecnologías emergentes con un despliegue limitado en entornos comerciales y de uso cotidiano.

En ese contexto histórico, la biometría fue concebida fundamentalmente como una tecnología orientada a la identificación singular. El riesgo jurídico dominante se vinculaba a la fijación de la identidad corporal, esto es, a la posibilidad de establecer identificaciones unívocas, persistentes y difícilmente reversibles. No resulta extraño, por ello, que el RGPD integrara la biometría en el marco de protección reforzada principalmente cuando se encontraba dirigida a permitir o confirmar la identificación única de la persona, activando en ese caso el régimen de las categorías especiales de datos personales (arts. 4.14 y 9 RGPD). Esta opción normativa respondía a un determinado estadio tecnológico y permitió consolidar garantías relevantes frente a riesgos intensos asociados al control de identidad.

Paralelamente, las biometrías no identificantes —frecuentemente descritas en la literatura técnica como *soft biometrics*— fueron tratadas como un ámbito secundario o prospectivo. Se las concibió como técnicas auxiliares, con un potencial limitado para individualizar de forma concluyente a las personas, y cuyos usos previsibles se asociaban a escenarios relativamente acotados, como la clasificación estadística o la mejora incremental de la interacción persona–máquina. Desde el punto de vista jurídico, esta percepción contribuyó a una valoración inicial de menor riesgo, en coherencia con el contexto tecnológico en el que dichas técnicas se desarrollaban entonces.

(2) Este marco de referencia se ha visto alterado de forma significativa en un período de tiempo relativamente breve. La maduración de sistemas de inteligencia artificial basados en aprendizaje automático, la reducción de los costes de procesamiento en tiempo real y la integración masiva de sensores en dispositivos de uso cotidiano han transformado las condiciones efectivas de utilización de la biometría no identificante. Prácticas que en el momento de elaboración del RGPD tenían un alcance limitado o experimental se han integrado progresivamente en arquitecturas ordinarias de interacción digital, con capacidad para operar de forma continua y adaptativa.

En este nuevo escenario, la biometría no identificante adquiere una relevancia jurídica emergente. Sin necesidad de culminar en procesos de identificación singular ni de generar perfiles persistentes, estos tratamientos permiten hoy intervenir de manera significativa en el entorno de interacción de las personas, mediante inferencias situacionales que pueden producir efectos materiales sobre su posición jurídica y fáctica. Esta evolución desborda parcialmente los presupuestos tecnológicos sobre los que se construyó la protección biométrica en el RGPD, sin que ello implique, todavía, una respuesta normativa plenamente articulada.

(3) El RIA se adopta ya en este contexto transformado. A diferencia del RGPD, el RIA nace cuando la inteligencia artificial ha dejado de ser una tecnología emergente y comienza a convertirse en una infraestructura transversal. No obstante, la forma en que este nuevo instrumento aborda las prácticas biométricas no identificantes —mediante una clasificación *ex ante* de sistemas y contextos de uso— plantea interrogantes sobre su capacidad para captar adecuadamente los riesgos derivados de la inferencia biométrica continua, cuestión que solo puede evaluarse de manera sistemática a la luz del marco jurídico europeo en su conjunto.

Desde un punto de vista introductorio, este escenario exige evitar dos simplificaciones opuestas. De una parte, resulta inadecuado equiparar toda inferencia conductual a biometría, pues no toda inferencia automatizada se basa en el tratamiento técnico de señales corporales ni implica un proceso de biometrización en sentido estricto. De otra parte, resulta necesario revisar la tendencia a considerar que la biometría no identificante es jurídicamente marginal, sobre el único argumento de que no culmina en una identificación única. La cuestión que se le plantea al Derecho de la Unión no es únicamente si un tratamiento identifica, sino cómo la captación de información biométrica se integra funcionalmente en arquitecturas inferenciales continuas y qué tipo de riesgos introduce para los derechos y libertades fundamentales, cuestión que este trabajo abordará de manera progresiva en los apartados siguientes.

§1.3. Delimitación del objeto, objetivos e hipótesis desde la lógica de riesgo y la responsabilidad proactiva. Estructura de la presentación.

(1) Este trabajo se centra en el análisis de tratamientos biométricos no identificantes mediante sistemas de inteligencia artificial, entendidos como aquellos que implican la captación y el tratamiento técnico específico de señales corporales o cuasi corporales con fines de inferencia en tiempo real o cuasi real, sin finalidad declarada de identificación única.

Desde una perspectiva tipológica, el objeto del trabajo incluye, entre otros supuestos, sistemas que infieren niveles de atención o estados emocionales durante la interacción —por ejemplo, a partir de micro-expresiones faciales, patrones de voz o movimientos de la mirada—, así como modalidades de captación continua, integradas en dispositivos y entornos conectados. Estos tratamientos se analizan siempre desde una lógica funcional, con independencia de que exista o no almacenamiento persistente de datos biométricos, y atendiendo al funcionamiento efectivo de las arquitecturas inferenciales en las que se integran. El elemento definitorio de estos tratamientos no reside en la tecnología empleada de forma aislada, sino en su función inferencial y en su capacidad para incidir materialmente en las condiciones de autonomía personal, igualdad material y autodeterminación informativa de las personas, en contextos reales de interacción digital.

Sin perjuicio de que en determinados pasajes pueda hacerse referencia puntual a ellos o a su regulación jurídica, quedan expresamente fuera del objeto principal, en primer lugar, los tratamientos biométricos identificantes clásicos, orientados a la verificación o identificación en sentido estricto de la persona. Quedan igualmente excluidas, en segundo lugar, las formas de perfilado puramente conductual que no se apoyan en señales corporales sometidas a un proceso de biometrización, salvo cuando su consideración resulte necesaria para delimitar fronteras conceptuales o evitar confusiones normativas.

(2) El objetivo general del trabajo es evaluar los riesgos para los derechos y libertades fundamentales que derivan de estas prácticas y examinar su gobernanza

jurídica en el marco europeo vigente. Este objetivo se aborda desde un enfoque jurídico-técnico orientado a la gestión preventiva del riesgo, articulado en torno a un doble eje operativo. De una parte, se examina la suficiencia del encuadre ofrecido por el RIA para captar los riesgos asociados a tratamientos biométricos no identificantes de carácter inferencial. De otra, se analiza la capacidad del RGPD para operar como marco preventivo transversal, mediante la aplicación de sus principios sustantivos y, de manera central, del principio de responsabilidad proactiva.

(3) La hipótesis principal que guía el trabajo sostiene que determinadas modalidades de biometría no identificante basadas en sistemas de inteligencia artificial pueden entrañar riesgos elevados para los derechos y libertades fundamentales, aun cuando no activen los umbrales clásicos asociados a la identificación biométrica ni queden plenamente captadas por las tipificaciones del RIA. En este contexto, la aplicación reforzada y materialmente orientada del principio de responsabilidad proactiva del RGPD se revela como el principal instrumento disponible para la identificación, evaluación y gestión preventiva de dichos riesgos, en particular a través de las evaluaciones de impacto y de decisiones de diseño restrictivas adaptadas a la lógica inferencial y continua del tratamiento.

(4) Sobre esta base, el trabajo se estructura del modo siguiente. El apartado §2 desarrolla un marco conceptual y técnico destinado a delimitar con precisión la noción de biometría no identificante y las arquitecturas inferenciales en las que se integra. El apartado §3 examina el marco normativo europeo aplicable, con especial atención a la articulación entre el RGPD y el RIA. A partir de este encuadre, los apartados §4 y §5 se centran en la identificación de los riesgos para los derechos y libertades fundamentales y en el análisis de los instrumentos jurídicos disponibles para su gestión preventiva, mientras que el apartado §6 aborda el papel de las Autoridades de Protección de Datos y los límites estructurales del control *ex post*. El trabajo se cierra con un apartado de conclusiones y recomendaciones operativas (§7).

§2. MARCO CONCEPTUAL Y TÉCNICO DE LA BIOMETRÍA NO IDENTIFICANTE

§2.1. BIOMETRÍA IDENTIFICANTE Y BIOMETRÍA NO IDENTIFICANTE: DELIMITACIÓN CONCEPTUAL CIENTÍFICO-TÉCNICA Y EVOLUCIÓN DEL CONCEPTO JURÍDICO EN EL DERECHO DE LA UE

(1) En las últimas dos décadas, los términos biometría y reconocimiento biométrico se han asociado de forma predominante, tanto en el discurso público como en una parte significativa de la literatura jurídica, con sistemas automatizados de reconocimiento de personas basados en características anatómico-físicas, fisiológicas o comportamentales, y orientados a la identificación o verificación de la identidad individual (Busch, 2007; Kindt, 2013). Esta asociación, reforzada por el uso recurrente de ejemplos paradigmáticos como los controles automatizados de identidad basados en huellas dactilares, el reconocimiento facial o el escaneo del iris, ha contribuido a una comprensión restrictiva del fenómeno biométrico, centrada casi exclusivamente en su potencial singularizante. En este sentido, la reflexión desarrollada en el ámbito europeo —en particular en el marco de los trabajos del Supervisor Europeo de Protección de Datos y del Parlamento Europeo— en torno al pasaporte biométrico europeo contribuyó de manera decisiva a consolidar una comprensión de la biometría estrechamente vinculada al control de identidad y a la identificación unívoca de las personas.

(2) Desde una perspectiva científico-técnica, sin embargo, esta identificación entre biometría y reconocimiento identificante resulta reductora. La biometría designa, en sentido amplio, el conjunto de métodos destinados al estudio mensurativo de fenómenos biológicos en organismos vivos, y no se limita al reconocimiento de identidades humanas (Escajedo San-Epifanio, 2017). La acepción contemporánea vinculada al reconocimiento automatizado de personas constituye, en realidad, una especialización funcional de esta tradición más amplia, caracterizada por dos rasgos: la focalización casi exclusiva en el ser humano como objeto del análisis y la orientación del tratamiento hacia la distinción métrica entre individuos dentro de un conjunto (Saborowski, 2010; Mordini & Tzovaras, 2012).

Incluso en este marco especializado, la biometría no se define por el tipo de rasgo corporal considerado de forma aislada, sino por el tratamiento mensurativo aplicado a dicho rasgo y por la arquitectura técnica y científica que permite su obtención, interpretación y uso funcional. Resulta, por tanto, esencial distinguir entre la fuente corporal de la información —esto es, el rasgo físico, fisiológico o comportamental— y el dato biométrico propiamente dicho, entendido como el resultado de un tratamiento técnico específico que extrae atributos mensurables y los convierte en una representación susceptible de comparación, categorización o inferencia. Una imagen facial, una grabación de voz o una secuencia de movimientos no constituyen por sí mismas datos biométricos en sentido estricto, sino posibles fuentes a partir de las cuales pueden obtenerse datos biométricos mediante un proceso de biometrización (Jasserand, 2016).

Desde esta perspectiva, la capacidad singularizante de un dato biométrico no reside en el rasgo aislado, sino en el sistema en el que se integra. Determinadas características corporales pueden presentar un elevado potencial identificante en un contexto técnico concreto y carecer prácticamente de él en otro. Inversamente, rasgos que no permiten por sí solos una identificación concluyente pueden adquirir relevancia funcional significativa cuando se integran en arquitecturas orientadas a la categorización, la inferencia o el perfilado. Esta constatación, ampliamente asumida en la literatura biométrica, pone de relieve que la distinción entre biometría identificante y biometría no identificante no refleja una diferencia ontológica entre tipos de datos, sino una diferencia

funcional vinculada a la finalidad y configuración del sistema (Kindt, 2013; Escajedo San-Epifanio, 2017).

(3) La evolución normativa europea ha tendido, no obstante, a cristalizar una comprensión funcionalmente estrecha de la biometría. El RGPD define los datos biométricos como aquellos «obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona» (art. 4.14 RGPD). Esta definición, coherente con el contexto tecnológico y social en el que se elaboró el Reglamento, vincula la relevancia jurídica reforzada de la biometría a su capacidad de identificación singularizante y activa, en ese caso, el régimen de las categorías especiales de datos personales del artículo 9 RGPD (Romeo Casabona, 2021; Escajedo San-Epifanio, 2024).

Esta construcción normativa ha resultado eficaz para afrontar los riesgos asociados al control de identidad y a la autenticación biométrica, pero presenta limitaciones evidentes cuando se proyecta sobre tratamientos biométricos no orientados a la identificación única. En particular, deja en una zona de ambigüedad aquellas prácticas que, aun basándose en tratamientos mensurativos del cuerpo, se orientan a la categorización funcional, a la inferencia situacional o al perfilado, sin generar una identidad biométrica persistente ni vincularse directamente a una identidad civil. Desde una perspectiva material de protección de derechos fundamentales, esta exclusión funcional resulta problemática, en la medida en que invisibiliza el impacto potencial de la biometría no identificante sobre la autonomía personal, la igualdad material y la autodeterminación informativa (Simitis, 2011; Wachter & Mittelstadt, 2019).

(4) Por ello, no resulta metodológicamente adecuado definir los datos biométricos exclusivamente por su capacidad de identificación singularizante. Desde una perspectiva conceptualmente más consistente, acorde con la disciplina científica de la biometría, puede sostenerse que el concepto jurídico de dato biométrico debería abarcar

> *aquellos datos que se obtienen del cuerpo de las personas como resultado de un tratamiento mensurativo específico, con independencia de que dicho tratamiento se oriente o no a la identificación única del sujeto* (Escajedo San-Epifanio, 2017; Escajedo San-Epifanio, 2024).

Sobre esta base, la distinción entre biometría identificante y biometría no identificante debe formularse como una distinción funcional entre sistemas de reconocimiento con perfiles de riesgo diferenciados, y no como una exclusión conceptual de determinadas prácticas del ámbito biométrico. Este planteamiento permite comprender por qué tratamientos biométricos no orientados a la identificación única pueden, sin embargo, generar riesgos jurídicamente relevantes para los derechos y libertades fundamentales, cuestión que se desarrollará a continuación en el análisis de las tipologías biométricas y de las arquitecturas técnicas en las que se integran (§2.2).

§2.2. BIOMETRÍAS ESTÁTICAS Y BIOMETRÍAS DINÁMICAS, SINGULARIZANTES O CATEGORIZANTES SEGÚN LA FINALIDAD DE LOS SISTEMAS

(1) La distinción entre *biometrías estáticas* y *biometrías dinámicas* no se refiere a la naturaleza ontológica del dato biométrico considerado de forma aislada, ni, en sentido estricto, al carácter del sistema de reconocimiento empleado en su captación, sino al modo en que el cuerpo humano es tratado como fuente de información biométrica y, en particular, a la dimensión temporal necesaria para que la captación permita extraer atributos biométricos funcionalmente relevantes.

Desde esta perspectiva, las *biometrías estáticas* comprenden aquellos métodos de captación en los que una muestra puntual del cuerpo resulta suficiente para extraer atributos mensurables con potencial de reconocimiento. En estos supuestos, la información biométrica se obtiene a partir de características anatómico-físicas relativamente estables, y el sistema no requiere observar el cuerpo en funcionamiento para generar información biométrica operativa (Jain, Flynn & Ross, 2008; Maltoni et al., 2009).

Las *biometrías dinámicas*, por su parte, engloban aquellos métodos de captación que requieren una dimensión temporal extendida para que la información biométrica emerja como tal. En estos casos, la fuente corporal no es una configuración anatómica estática, sino el cuerpo en funcionamiento, entendido como un conjunto de procesos fisiológicos, motores o conductuales que solo pueden interpretarse biométricamente mediante la observación de secuencias, ciclos o patrones a lo largo del tiempo. Desde el punto de vista técnico, esta captación se articula habitualmente mediante ventanas temporales deslizantes y procesos de inferencia cuasi en tiempo real, lo que permite una adaptación continua del sistema sin necesidad de almacenamiento persistente de las señales en bruto.

(2) La distinción entre biometrías dinámicas y biometrías estáticas tiene consecuencias jurídicas relevantes. En primer lugar, pone de manifiesto que la biometría dinámica no constituye una modalidad atenuada de captación biométrica, sino, en muchos casos, una fuente informacionalmente más rica, precisamente porque el cuerpo en funcionamiento expresa estados, disposiciones y variaciones que no pueden inferirse a partir de una captura puntual. En segundo lugar, evidencia que la dimensión temporal de la captación incrementa la densidad informacional del tratamiento y, con ello, su capacidad para generar inferencias que exceden la identificación singular, incluyendo inferencias relativas a la salud, al estado emocional, a la atención o a la disposición conductual de la persona.

Ahora bien, ni el carácter estático ni el carácter dinámico de la biometría determinan por sí mismos la finalidad del sistema de reconocimiento en el que se integran. Tanto las biometrías estáticas como las dinámicas pueden emplearse en sistemas orientados a la identificación singularizante o, alternativamente, en sistemas orientados a la categorización, la inferencia o el perfilado funcional, sin finalidad de identificación única.

(3) La configuración del sistema, sus finalidades y los efectos materiales que produce sobre la persona son, por consiguiente, la clave para el tratamiento jurídico de un sistema de tratamiento biométrico. Esta constatación resulta central para el objeto del presente trabajo. Las biometrías dinámicas se integran con especial facilidad en sistemas de reconocimiento no identificantes basados en inteligencia artificial, precisamente porque permiten operar sin necesidad de enrolamiento previo ni de almacenamiento persistente de datos biométricos. La captación continua o cuasi continua del cuerpo en funcionamiento facilita arquitecturas inferenciales adaptativas, orientadas a interpretar estados situacionales y a modular el entorno de interacción en tiempo real, sin fijar una identidad biométrica estable.

Desde una perspectiva de protección de derechos fundamentales, esta combinación —biometría dinámica y sistemas no singularizantes— presenta perfiles de riesgo específicos que no quedan adecuadamente captados por enfoques normativos centrados en la identificación. La riqueza informacional de la biometría dinámica, unida a su carácter temporal y a su integración en arquitecturas inferenciales opacas, exige desplazar el análisis jurídico desde la pregunta por la identidad hacia la evaluación de los efectos materiales del tratamiento sobre la autonomía personal, la igualdad material

y la autodeterminación informativa. Esta cuestión se desarrollará a continuación al examinar aquellos aspectos de la información biométrica que han quedado tradicionalmente desatendidos por el análisis jurídico (§2.3).

§2.2.1. EL POTENCIAL SINGULARIZANTE NO RESIDE EN EL DATO AISLADO, SINO EN EL SISTEMA DE RECONOCIMIENTO EN EL QUE SE INSERTA

(1) La capacidad de un tratamiento biométrico para permitir la identificación única de una persona —esto es, su potencial singularizante— no puede atribuirse al dato biométrico considerado de forma aislada, ni al rasgo corporal del que dicho dato se obtiene, sino al sistema de reconocimiento en cuyo conjunto se integra dicho tratamiento. Esta afirmación resulta central para evitar interpretaciones simplificadoras que asocian determinadas fuentes corporales, de manera automática, con una capacidad identificante intrínseca.

Desde una perspectiva científico-técnica, ningún rasgo corporal es, por sí mismo, identificante o no identificante. La singularización es siempre el resultado de una configuración sistémica compleja, que combina, de forma acumulativa, diversos elementos estructurales. Entre ellos se encuentran: (a) la naturaleza de la fuente corporal utilizada; (b) el tipo de tratamiento mensurativo aplicado a dicha fuente; (c) la arquitectura técnica del sistema de reconocimiento; (d) la existencia o no de una fase de enrolamiento previo; (e) la disponibilidad, extensión y calidad de los conjuntos de referencia; (f) los criterios de comparación empleados y los umbrales de decisión fijados; así como (g) las finalidades funcionales para las que el sistema ha sido diseñado. Solo la concurrencia de estos elementos permite afirmar que un tratamiento biométrico presenta capacidad de identificación única (Escajedo San-Epifanio, 2017).

Por su parte, la automatización del reconocimiento no altera esta lógica estructural, sino que, en todo caso, introduce una aceleración, ampliación o escalabilidad del proceso de reconocimiento, sin modificar el fundamento sistémico de la singularización.

(2) La historia de los sistemas de reconocimiento biométricos confirma esta afirmación. Los primeros sistemas de identificación singular mediante biometría fueron analógicos y se basaban en características estáticas. Es el caso, entre otros, del *bertillonaje* -diseñado por Alphonse Bertillon e implementado en la policía francesa a finales del siglo XIX-, que combinaba la medición de rasgos corporales con un sistema de clasificación y archivo destinado a distinguir a una persona del resto de personas enroladas (Escajedo San-Epifanio, 2017). En ausencia de dicha arquitectura de ordenación y cotejo, las mismas mediciones carecían de utilidad identificante. Del mismo modo, rasgos como el espectro de la voz o el patrón de la marcha, que requieren captación dinámica, pueden adquirir un elevado potencial singularizante cuando se integran en sistemas con bases de datos de referencia y procedimientos de comparación uno-a-muchos, pese a no ser rasgos anatómicos estáticos.

Esta constatación permite descartar la idea, aún presente en algunos discursos jurídicos y regulatorios, de que la singularización biométrica se derive automáticamente del tipo de dato tratado. Un mismo dato biométrico puede resultar irrelevante desde el punto de vista identificante en un contexto técnico concreto y adquirir, en otro, una capacidad singularizante elevada. Inversamente, un tratamiento que no persigue la identificación única puede operar sobre datos biométricos sin activar mecanismos de singularización, aun cuando la fuente corporal utilizada sea, en abstracto, susceptible de identificación en otros contextos.

(3) Desde el punto de vista jurídico, esta distinción resulta especialmente relevante para la correcta interpretación del artículo 4.14 del RGPD. La definición de datos biométricos que contiene dicho precepto vincula su relevancia jurídica reforzada a la finalidad de permitir o confirmar la identificación única de una persona. Sin embargo, en puridad, esta formulación no describe una cualidad intrínseca del dato, sino una propiedad funcional del sistema de tratamiento, dependiente de su configuración técnica y de su finalidad. Ignorar este carácter sistémico conduce a infravalorar tratamientos biométricos que, aun no siendo singularizantes, pueden generar impactos materiales significativos sobre los derechos y libertades de las personas.

En consecuencia, la evaluación jurídica de un tratamiento biométrico no puede limitarse a identificar el tipo de rasgo corporal captado ni a comprobar si el dato es, en abstracto, potencialmente identificante. Debe atender, de forma prioritaria, a la arquitectura del sistema, a sus finalidades, a los procesos de comparación y decisión que incorpora y a los efectos materiales que produce sobre la persona. Esta aproximación sistémica resulta imprescindible para comprender por qué tratamientos biométricos no identificantes pueden presentar perfiles de riesgo elevados, y constituye un presupuesto necesario para el análisis de la arquitectura y gobernanza de los sistemas biométricos que se desarrollará en el apartado siguiente (§2.2.2), así como para el examen normativo y de riesgos de los capítulos posteriores (§§3 a 5).

§2.2.2. Elementos diferenciales en la arquitectura y gobernanza del sistema dependiendo de la finalidad identificante o no: módulos, enrolamiento, almacenamiento, umbrales y tasas de error

(1) Si el potencial singularizante de un tratamiento biométrico no reside en el dato aislado, sino en el sistema de reconocimiento en el que dicho dato se integra (§2.2.1), resulta necesario examinar con mayor detalle la arquitectura técnica y las decisiones de gobernanza que configuran ese sistema. Desde una perspectiva jurídico-técnica, no todos los sistemas biométricos presentan el mismo perfil de riesgo, aun cuando operen sobre fuentes corporales similares, pues dicho perfil depende de cómo se diseñan, combinan y gobiernan sus componentes funcionales, en función de si la finalidad del sistema es o no identificante.

En términos generales, un sistema biométrico automatizado puede describirse como una arquitectura modular compuesta, al menos, por los siguientes elementos: (i) un módulo de captación o sensor, encargado de obtener la muestra corporal en bruto; (ii) uno o varios módulos de control de calidad y pre-procesamiento de la muestra; (iii) un módulo de extracción de atributos biométricos mediante técnicas matemáticas o algorítmicas; (iv) un repositorio de referencia, que puede consistir en una base de datos de plantillas biométricas individuales, en modelos estadísticos agregados o en ambos; (v) un módulo de comparación o inferencia, que determina el grado de similitud, pertenencia a una categoría o probabilidad de un estado; y (vi) un módulo de decisión o de activación funcional, que traduce el resultado del análisis en una respuesta del sistema (Maltoni et al., 2009; Jain, Flynn & Ross, 2008).

(2) La existencia o no de una fase de enrolamiento biométrico supone una diferencia relevante entre los sistemas que persiguen la identificación o verificación de identidades y aquellos que se orientan a la detección o inferencia de patrones —por ejemplo, de comportamiento, estados emocionales o disposiciones funcionales—. En los sistemas singularizantes clásicos, el enrolamiento constituye un momento crítico en el que se captan y almacenan datos biométricos de referencia asociados a una identidad determinada. Esta fase implica decisiones especialmente relevantes en términos de licitud, proporcionalidad, seguridad y conservación de los datos, y suele activar un

régimen jurídico reforzado, tanto en el RGPD como en otros instrumentos sectoriales. La calidad y fiabilidad del enrolamiento resultan asimismo determinantes para la validez del sistema, en la medida en que la asociación errónea de una plantilla biométrica a un sujeto distinto de su titular pervierte estructuralmente el proceso de identificación y compromete su legitimidad jurídica.

En los sistemas biométricos no identificantes, sin embargo, el enrolamiento individual previo tiende a desaparecer como elemento estructural del sistema. Estos sistemas operan, por regla general, sobre captaciones en tiempo real comparadas con modelos agregados o patrones estadísticos, lo que modifica sustancialmente la configuración del riesgo sin eliminarlo, al desplazarlo desde la identidad hacia la inferencia situacional y la modulación funcional del entorno de interacción. Este es el caso, por ejemplo, de determinadas biometrías médicas o fisiológicas empleadas para la monitorización continua de funciones corporales —como la actividad cardíaca—, en las que el interés del sistema no reside en identificar al sujeto, sino en detectar variaciones, anomalías o estados funcionales relevantes a partir de señales corporales tratadas de forma dinámica.

(3) El almacenamiento con fines de re-identificación posterior, así como, por su parte, la duración y persistencia del tratamiento en sistemas de monitorización sin finalidad de identificación, constituyen otro eje central de diferenciación entre sistemas biométricos identificantes y no identificantes. Mientras que los sistemas orientados a la identificación única suelen requerir la conservación persistente de plantillas biométricas individuales, los sistemas no singularizantes pueden funcionar sin almacenamiento duradero de datos biométricos en bruto ni de plantillas biométricas individuales, apoyándose en inferencias efímeras o en la actualización continua de modelos agregados. La ausencia de almacenamiento individual no equivale, sin embargo, a ausencia de impacto jurídico, pues la persistencia puede desplazarse desde los datos hacia los modelos, los parámetros y las lógicas inferenciales, que continúan produciendo efectos sobre las personas incluso cuando las muestras originales han sido descartadas.

Desde un punto de vista técnico, las arquitecturas de interacción que captan información biométrica no parten necesariamente de un conjunto de datos personales de referencia en sentido clásico ni permiten la reconstrucción directa de las muestras biométricas de entrada. Sí incorporan, no obstante, regularidades estadísticas aprendidas a partir de tratamientos previos, lo que posibilita la reproducción estable y reiterada de efectos jurídicamente relevantes sin necesidad de conservar datos biométricos identificables ni perfiles biométricos individuales persistentes. Ello no excluye que, en el marco de la interacción, el sistema pueda tratar simultáneamente otra información no biométrica asociada a la persona —como direcciones IP, identificadores técnicos o datos de usuario—, cuya combinación funcional con las inferencias biométricas puede resultar jurídicamente relevante a efectos de evaluación del riesgo.

(4) Especial relevancia adquieren asimismo los umbrales de decisión y las tasas de error incorporados al sistema, si bien el impacto jurídico del error no deriva tanto de su mera existencia técnica como del marco decisional en el que se inserta y del tipo de capacidad de decisión o modulación que el sistema ejerce sobre la persona. No es jurídicamente equivalente, por ejemplo, que un error biométrico impida a una persona cruzar una frontera o genere una atribución errónea de identidad en un control de documentación, a que un sistema no identificante adapte contenidos, estímulos o decisiones en función de inferencias incorrectas sobre estados emocionales, disposiciones conductuales o condiciones funcionales inexistentes. Del mismo modo, no producen los mismos efectos jurídicos los errores de clasificación que confunden una

discapacidad con un estado de embriaguez, o el nerviosismo con la mendacidad, en función del contexto y de las consecuencias asociadas a dicha inferencia.

Todo sistema biométrico opera sobre márgenes de incertidumbre y probabilidades, y debe fijar parámetros que determinen cuándo una similitud, una categoría o una inferencia se considera suficientemente relevante para activar una respuesta funcional. Las denominadas tasas de aceptación errónea y de rechazo erróneo, clásicamente analizadas en sistemas de identificación, encuentran su correlato funcional en los sistemas no identificantes en forma de errores sistemáticos de clasificación, inferencias inexactas o sesgos distribucionales, cuya relevancia no puede evaluarse exclusivamente desde parámetros técnicos de rendimiento.

Desde una perspectiva jurídica, estos errores no son neutros. Pueden traducirse en tratos diferenciados, exclusiones funcionales o modulaciones del entorno de interacción con impacto directo sobre derechos fundamentales, aun cuando no se produzca una identificación singular ni una decisión automatizada aislable en sentido estricto (Escajedo San-Epifanio, 2017). Las decisiones técnicas relativas al enrolamiento, al almacenamiento, a la fijación de umbrales o a la tolerancia al error no son, por tanto, meramente instrumentales, sino decisiones de gobernanza del sistema con consecuencias jurídicas directas. Determinan qué puede inferirse, con qué grado de fiabilidad, en qué contextos y con qué efectos sobre la persona, y deben ser evaluadas como tales desde una lógica de riesgo y responsabilidad.

(5) Desde la lógica del Derecho de la Unión, y en particular del RGPD, estas decisiones estructurales no pueden considerarse ajenas al análisis de la licitud y la proporcionalidad del tratamiento. La forma en que se diseñan y gobiernan los módulos del sistema condiciona la procedencia de evaluaciones de impacto, la intensidad de las medidas de protección de datos desde el diseño y por defecto, y la posibilidad misma de ejercer derechos o de reconstruir *ex post* el funcionamiento del tratamiento. En consecuencia, la arquitectura técnica y la gobernanza del sistema biométrico deben entenderse como elementos centrales para la identificación del riesgo, y no como aspectos neutrales o puramente tecnológicos, cuestión que será determinante en el análisis normativo (§3) y en la caracterización de riesgos desarrollada en los apartados posteriores (§§4 y 5).

§2.2.3. SISTEMAS BIOMÉTRICOS NO SINGULARIZANTES: CATEGORIZACIÓN, INFERENCIA Y CUERPO EN FUNCIONAMIENTO COMO FUENTE DE PERFILES

(1) Los sistemas biométricos no singularizantes se caracterizan porque la finalidad del tratamiento no es permitir o confirmar la identificación única de una persona, sino detectar atributos, inferir estados o asignar categorías funcionales a partir de señales corporales captadas en tiempo real o cuasi real. En estos sistemas, el reconocimiento biométrico no culmina en la singularización del sujeto frente a un conjunto, sino en su ubicación dinámica en un espacio de categorías, probabilidades o perfiles funcionales, cuya función es modular el comportamiento del sistema frente a la persona (Gutwirth & Hildebrandt, 2010; Rouvroy & Berns, 2013).

Desde el punto de vista técnico, estos sistemas prescinden habitualmente del enrolamiento biométrico individual y de la creación de identidades biométricas persistentes. La comparación no se realiza entre una muestra captada y una plantilla individual asociada a una identidad concreta, sino entre la señal corporal observada y modelos estadísticos agregados, patrones promedio o rangos de referencia construidos a partir de conjuntos amplios de datos. En las arquitecturas contemporáneas de telecomunicaciones, una parte creciente de estas inferencias se ejecuta mediante

esquemas de computación distribuida o computación en el borde (*edge computing*), en los que el procesamiento se realiza total o parcialmente en el propio dispositivo terminal o en nodos próximos de la red, reduciendo la transmisión y centralización de datos en bruto, sin eliminar por ello la capacidad del sistema para generar inferencias continuas y producir efectos funcionales jurídicamente relevantes sobre la persona.

(2) Esta lógica categorizante resulta especialmente compatible con el uso de biometrías dinámicas, en la medida en que el cuerpo en funcionamiento constituye una fuente continua y densa de información sobre estados y disposiciones que no pueden captarse mediante una toma puntual. A diferencia de las biometrías estáticas, que permiten extraer atributos relativamente estables, las biometrías dinámicas hacen visible la variabilidad temporal del cuerpo, como niveles de atención, fatiga, estrés, nerviosismo, impulsividad, coordinación motora o patrones de interacción. Esta riqueza expresiva convierte al cuerpo en funcionamiento en una fuente privilegiada para la inferencia situacional, incluso cuando no existe ningún interés identificante (McStay, 2018).

En este contexto, la categorización biométrica no puede entenderse como una operación neutral ni meramente descriptiva. Toda categorización implica decisiones previas sobre qué atributos se consideran relevantes, qué umbrales se establecen, qué estados se distinguen y qué consecuencias funcionales se asocian a cada categoría. Estas decisiones no son el resultado automático del procesamiento algorítmico, sino que incorporan un *rationale* inscrito en el diseño del sistema, que traduce determinadas concepciones del cuerpo, del comportamiento y de la normalidad en reglas operativas. Incluso cuando se presentan como técnicas u objetivas, las categorías biométricas son construcciones normativas en sentido amplio.

(3) La inferencia biométrica no singularizante amplía de manera significativa el alcance material del tratamiento más allá de los datos captados en bruto. A partir de señales corporales limitadas, los sistemas pueden inferir información no directamente observable, predecir comportamientos futuros o estimar disposiciones internas de la persona. Esta capacidad inferencial, característica de los sistemas de aprendizaje automático, permite generar perfiles funcionales efímeros o persistentes que condicionan el trato recibido, sin que exista necesariamente un perfil almacenado ni una identidad biométrica estable. Desde el punto de vista jurídico, este desplazamiento desde el dato hacia la inferencia resulta decisivo (Wachter & Mittelstadt, 2019; Hildebrandt, 2020).

La ausencia de singularización no implica, por ello, una menor intensidad del tratamiento ni un menor potencial de afectación de derechos fundamentales. Por el contrario, en los sistemas no singularizantes la intervención puede resultar más continua, más contextual y menos perceptible, precisamente porque no se activa en torno a momentos identificables de verificación o identificación. La persona no es reconocida como individuo único, pero es observada, interpretada y modulada en función de su comportamiento corporal en tiempo real, lo que dificulta la toma de conciencia del tratamiento y el ejercicio efectivo de mecanismos de control.

(4) Desde una perspectiva jurídico-técnica, esta forma de reconocimiento plantea desafíos específicos para los marcos normativos centrados en la identidad. Al no producir una identificación única ni una decisión automatizada aislable, estos sistemas tienden a situarse en zonas de baja visibilidad regulatoria, pese a su capacidad para influir de manera significativa en la autonomía personal, en la igualdad material o en la autodeterminación informativa. Comprender el funcionamiento de los sistemas no singularizantes como arquitecturas de categorización e inferencia basadas en el cuerpo en funcionamiento resulta, por tanto, un presupuesto imprescindible para el análisis de

los aspectos jurídicamente desatendidos que se abordarán en el apartado siguiente (§2.3), así como para la correcta identificación de los riesgos desarrollados en los capítulos posteriores (§§4 y 5).

§2.3. Aspectos de la información biométrica que requieren una atención jurídica renovada

(1) El análisis desarrollado en los apartados anteriores pone de manifiesto que una parte significativa de los problemas jurídicos asociados a la biometría no identificante no deriva de la inexistencia de normas aplicables, sino de la forma en que el Derecho ha conceptualizado históricamente la información biométrica y ha delimitado su relevancia jurídica en torno al paradigma de la identificación singularizante. Esta focalización ha tenido como efecto colateral la desatención de determinados aspectos centrales del funcionamiento real de los sistemas biométricos contemporáneos, en particular aquellos vinculados a la inferencia, la categorización y la capacidad reveladora de atributos sensibles asociada a la captación dinámica del cuerpo en funcionamiento (Rouvroy & Berns, 2013; Hildebrandt, 2020).

(2) Desde una perspectiva histórico-normativa, esta orientación resulta comprensible. Tanto la normativa europea en materia de protección de datos como los instrumentos sectoriales asociados a la seguridad, el control de accesos o la gestión de fronteras se desarrollaron en un contexto tecnológico en el que la biometría se utilizaba fundamentalmente para verificar o establecer identidades de forma estable y persistente. En ese marco, el riesgo jurídico se asociaba de manera prioritaria a la fijación de la identidad corporal y a la posibilidad de reutilización ulterior de los datos con finalidades distintas de las inicialmente declaradas (González Fuster, 2014; Hijmans, 2016).

Sin embargo, el desarrollo y despliegue contemporáneo de sistemas de inteligencia artificial basados en biometría no identificante ha alterado de forma sustancial este esquema. La captación y el tratamiento de señales corporales permiten hoy inferir estados, disposiciones o probabilidades de comportamiento en tiempo real, sin necesidad de identificar de manera unívoca a la persona ni de conservar datos biométricos de forma persistente. Estos tratamientos producen efectos materiales relevantes sobre las personas —en la forma en que son interpretadas, categorizadas o situadas funcionalmente en un contexto de interacción— que no encajan adecuadamente en categorías jurídicas construidas exclusivamente en torno a la identidad (Wachter & Mittelstadt, 2019; Hildebrandt, 2020).

(3) Esta desalineación conceptual afecta tanto a la interpretación del RGPD como a la arquitectura del Reglamento (UE) 2024/1689 de Inteligencia Artificial. En ambos casos, el énfasis normativo en la identificación tiende a relegar a un segundo plano elementos que resultan decisivos para evaluar el riesgo real de estos tratamientos, como el papel de la inferencia automatizada, la continuidad temporal de la captación, la construcción de categorías funcionales o las decisiones de diseño y gobernanza de los sistemas biométricos no singularizantes (Mantelero & Esposito, 2021).

En este contexto, resulta necesario identificar y ordenar aquellos aspectos de la información biométrica que han quedado tradicionalmente desatendidos por el análisis jurídico. No se trata de ampliar artificialmente el ámbito de aplicación de las normas existentes ni de introducir categorías conceptuales innecesarias, sino de reconstruir de forma más ajustada el objeto de tutela, atendiendo al funcionamiento efectivo de los

sistemas y a los efectos materiales que producen sobre los derechos y libertades fundamentales.

Con este objetivo, los subapartados que siguen abordan tres cuestiones específicas que resultan particularmente relevantes para el objeto del presente trabajo: en primer lugar, la persistente diversidad terminológica y sus efectos jurídicos (§2.3.1); en segundo lugar, la confusión entre fuente, dato, atributo y patrón biométrico (§2.3.2); y, finalmente, la tendencia a infravalorar la capacidad reveladora de la biometría no identificante respecto de atributos sensibles (§2.4).

§2.3.1. DIVERSIDAD TERMINOLÓGICA Y SUS EFECTOS JURÍDICOS

(1) Uno de los factores que ha contribuido de manera más persistente a la infravaloración jurídica de la biometría no identificante es la falta de un uso terminológico consistente en torno a los conceptos básicos que estructuran este ámbito. En la literatura científica, técnica y jurídica se emplean de forma no siempre coincidente expresiones como información biométrica, dato biométrico, fuente biométrica o atributo biométrico, a menudo sin delimitar con precisión a qué fase del tratamiento o a qué elemento del sistema se refieren (Saborowski, 2010; Jasserand, 2016).

Esta diversidad terminológica no constituye un problema meramente descriptivo. Tiene consecuencias jurídicas directas, en la medida en que condiciona la calificación del tratamiento y, con ello, la activación —o no— de los mecanismos de tutela previstos en el Derecho de la Unión. Cuando el análisis se centra exclusivamente en el soporte material de la captación —por ejemplo, una imagen facial o una grabación de voz—, se corre el riesgo de invisibilizar el proceso de biometrización y las inferencias que se generan a partir de dicha captación, desplazando la atención desde el funcionamiento real del sistema hacia el dato aparente.

Este desplazamiento resulta especialmente problemático en los tratamientos biométricos no identificantes. Al no culminar en una identificación singularizante, estos tratamientos han sido presentados en ocasiones como meras formas de análisis de comportamiento o de personalización funcional, pese a apoyarse en captaciones corporales sometidas a un tratamiento mensurativo específico. La confusión terminológica facilita así una lectura reductora del riesgo, en la que la ausencia de identificación se interpreta como ausencia de relevancia jurídica, sin atender a los efectos materiales del tratamiento sobre la persona.

(2) Desde el punto de vista normativo, esta ambigüedad se refleja también en la propia definición de datos biométricos del artículo 4.14 RGPD, que, junto a la referencia al tratamiento técnico específico, menciona imágenes faciales o datos dactiloscópicos. Como ha señalado la doctrina, esta formulación puede inducir a identificar indebidamente la fuente o el soporte con el dato biométrico propiamente dicho, reforzando una comprensión centrada en la identificación singularizante y dejando en un segundo plano otras funciones biométricas del tratamiento (Jasserand, 2016; Saborowski, 2010).

El resultado es una aplicación fragmentaria y formalista del marco jurídico, en la que la relevancia del tratamiento se evalúa principalmente en función del tipo de dato visible o de la finalidad identificante declarada, y no en función del proceso técnico de extracción de atributos, de las inferencias generadas ni de los efectos funcionales que dichas inferencias producen. Desde la perspectiva de la protección de derechos fundamentales, esta aproximación resulta insuficiente, pues contribuye a minimizar riesgos asociados a tratamientos biométricos no identificantes integrados en

arquitecturas inferenciales continuas y opacas (Simitis, 2011; Wachter & Mittelstadt, 2019).

(3) Superar esta diversidad terminológica no exige imponer una definición única y cerrada de biometría, sino adoptar una aproximación funcional y material que permita identificar cuándo un tratamiento recae efectivamente sobre información corporal tratada de forma mensurativa, con independencia de que se utilice o no para identificar de manera unívoca a la persona. Esta clarificación constituye un presupuesto necesario para aplicar de forma coherente el RGPD y para evitar que la biometría no identificante quede excluida, de facto, de los mecanismos de tutela preventiva previstos en el Derecho de la Unión.

§2.3.2. DATO, INFORMACIÓN Y PATRÓN: CONFUSIÓN ENTRE FUENTE, MUESTRA, ATRIBUTOS Y PLANTILLA

(1) Uno de los efectos más relevantes de la diversidad terminológica señalada en el apartado anterior (§2.3.1) es la confusión persistente entre niveles conceptuales distintos que intervienen en el funcionamiento de los sistemas biométricos. En el discurso jurídico —y, en ocasiones, también en documentos institucionales— se utilizan de forma indiferenciada nociones que corresponden a momentos y elementos distintos del tratamiento biométrico, como la fuente corporal de la información, el dato en bruto captado por un sensor, los atributos biométricos extraídos mediante tratamiento técnico y el patrón o plantilla utilizada posteriormente en procesos de comparación, categorización o inferencia automatizada.

Desde una perspectiva técnico-funcional, resulta necesario distinguir al menos cuatro niveles. En primer lugar, la fuente biométrica, entendida como el rasgo corporal, fisiológico o comportamental del que se obtiene la información (por ejemplo, el rostro, la voz, la marcha o determinados movimientos oculares). En segundo lugar, la muestra o dato en bruto, que constituye la representación inicial de esa fuente captada por un dispositivo técnico, como una imagen digital, una grabación sonora o una secuencia de movimiento. En tercer lugar, los atributos biométricos, es decir, los rasgos mensurables que se extraen de la muestra mediante procedimientos matemáticos o algorítmicos. Finalmente, el patrón o plantilla biométrica, que consiste en la representación estructurada utilizada por el sistema como referencia para realizar comparaciones, inferencias o asignaciones funcionales (Saborowski, 2010; Mordini & Tzovaras, 2012).

(2) Esta distinción, bien asentada en la literatura biométrica, se diluye con frecuencia en el análisis jurídico. El término dato biométrico se emplea de manera genérica para referirse indistintamente a cualquiera de estos niveles, lo que favorece una comprensión imprecisa del tratamiento. Esta confusión se ve reforzada por la propia redacción del artículo 4.14 RGPD, que menciona imágenes faciales o datos dactiloscópicos junto a la referencia al tratamiento técnico específico. Desde un punto de vista técnico, ni una imagen facial ni una huella captada en bruto constituyen todavía un dato biométrico en sentido estricto, sino únicamente posibles fuentes a partir de las cuales pueden extraerse atributos biométricos mediante un proceso de biometrización (Jasserand, 2016).

La consecuencia jurídica de esta imprecisión no es menor. Al centrar el análisis en el soporte visible de la captación —la imagen, la grabación o la señal— se desplaza la atención desde el proceso de tratamiento hacia el dato aparente. Ello conduce, en la práctica, a evaluar la licitud y el riesgo del tratamiento en función de la conservación o no de la muestra en bruto, ignorando que los efectos jurídicamente relevantes pueden derivar de los atributos extraídos, de los patrones generados o de las inferencias

activadas a partir de ellos, con independencia de que el dato original se conserve o se descarte de forma inmediata (Wachter & Mittelstadt, 2019; Hildebrandt, 2020).

Esta cuestión resulta especialmente significativa en los tratamientos biométricos no identificantes basados en inteligencia artificial. En estos sistemas, la muestra en bruto puede ser eliminada de manera casi instantánea, mientras que los atributos extraídos alimentan modelos inferenciales que se actualizan de forma continua y producen efectos funcionales sobre la persona. Desde la perspectiva de los derechos fundamentales, la injerencia no desaparece con la supresión del dato inicial, sino que se desplaza hacia las inferencias y a las lógicas decisionales incorporadas en el sistema, cuya opacidad y persistencia relativa dificultan el control efectivo del tratamiento (Rouvroy & Berns, 2013; Hildebrandt, 2020).

(3) Desde el punto de vista del RGPD, esta distinción entre fuente, muestra, atributos y patrón es determinante para una aplicación materialmente adecuada de los principios del art. 5. La minimización no puede evaluarse únicamente en términos de volumen de datos captados o de duración de la conservación de la muestra en bruto, sino también atendiendo al alcance de los atributos extraídos y a las inferencias que el sistema está en condiciones de generar. Del mismo modo, la exactitud no se refiere solo a la fidelidad de la captación inicial, sino a la fiabilidad de las inferencias y clasificaciones que se producen a partir de los atributos biométricos utilizados (Simitis, 2011; Wachter, 2018).

En consecuencia, una delimitación conceptual rigurosa exige abandonar la identificación simplista entre dato biométrico y soporte material de la captación, y adoptar una aproximación procesual y funcional al tratamiento biométrico. Solo desde esta perspectiva resulta posible identificar adecuadamente los riesgos asociados a la biometría no identificante, evaluar la necesidad y proporcionalidad del tratamiento y determinar la procedencia de instrumentos preventivos como las evaluaciones de impacto. Esta clarificación prepara el análisis de la capacidad reveladora de atributos sensibles de la biometría no identificante, que se abordará de forma específica en el apartado siguiente (§2.4).

§2.4. Biometría no identificante como información corporal y su capacidad reveladora

La caracterización jurídica de la biometría no identificante exige ir más allá de la dicotomía tradicional entre datos biométricos identificantes y datos no sensibles. Aunque estos tratamientos no persigan la identificación singular de la persona, recaen necesariamente sobre información corporal, entendida como información extraída del cuerpo o del cuerpo en funcionamiento mediante un tratamiento técnico específico. Esta circunstancia resulta jurídicamente relevante por sí misma, con independencia del modo de captación, del soporte técnico empleado o del eventual almacenamiento de los datos.

Desde una perspectiva dogmática, la biometría no identificante no puede ser considerada una categoría residual o neutra de información. El hecho de que no permita identificar de manera unívoca a la persona no elimina su anclaje corporal ni su potencial para revelar dimensiones internas de la misma. La relevancia jurídica de esta información no se agota, por tanto, en su capacidad identificante, sino que deriva de su conexión directa con el cuerpo como fuente primaria de datos y con la producción de inferencias sobre la persona a partir de dicha fuente.

Este enfoque resulta coherente con la evolución de la protección de datos personales en el Derecho europeo, que ha ido reconociendo progresivamente que el riesgo no

reside únicamente en la identificación formal, sino también en la exposición informacional del cuerpo y en la posibilidad de generar conocimiento relevante sobre la persona sin su intervención consciente ni la exteriorización de su voluntad.

§2.4.1. Información corporal más allá de los datos de salud y de las categorías sensibles clásicas

La afirmación de que la biometría no identificante constituye información corporal no implica que todo tratamiento de este tipo deba reconducirse automáticamente a la categoría de datos de salud ni a las categorías especiales de datos del artículo 9 RGPD. Los datos de salud, incluso en supuestos de buena salud, cuentan con una trayectoria jurídica de protección relativamente consolidada, vinculada a su dimensión clínica, diagnóstica o terapéutica. Algo similar ocurre con otros atributos asociados al cuerpo, como el sexo o el origen racial o étnico, cuya protección se articula a partir de categorías normativas históricamente estabilizadas.

La biometría inferencial contemporánea, sin embargo, produce con frecuencia información corporal situada en un espacio intermedio entre lo somático, lo psicológico y lo conductual, que no encaja de manera automática en dichas categorías. La inferencia de estados emocionales, disposiciones atencionales, niveles de estrés, impulsividad o determinados rasgos de personalidad a partir de señales corporales no constituye necesariamente un tratamiento de datos de salud en sentido clínico, ni puede identificarse sin más con información médica o patológica.

No obstante, esta información tampoco es jurídicamente neutra. Como ha puesto de relieve la literatura en los ámbitos de la bioética y la neuroética, los estados emocionales y disposiciones psicológicas inferidos a partir del cuerpo reflejan dimensiones internas de la persona estrechamente vinculadas a su capacidad de autodeterminación, a su vulnerabilidad situacional y a su exposición a mecanismos de influencia, aun cuando no alcancen el umbral clínico de la enfermedad (Bublitz & Merkel, 2014; Ienca & Andorno, 2017). Desde esta perspectiva, la ausencia de una etiqueta médica o diagnóstica no atenúa la relevancia jurídica de la información inferida.

La dificultad para encajar esta información en categorías sensibles clásicas no debe conducir a su desprotección, sino a reconocer que la corporeidad inferida amplía el campo de la información jurídicamente relevante más allá de los supuestos tradicionales, exigiendo una evaluación material del riesgo basada en los efectos del tratamiento y no únicamente en su clasificación formal.

§2.4.2. Capacidad reveladora, inferencia y producción de conocimiento corporalmente anclado

La especificidad de la biometría no identificante reside en su capacidad para producir conocimiento sobre la persona a partir del cuerpo, incluso cuando los datos captados en bruto no se conservan o no se asocian a una identidad persistente. El tratamiento biométrico no se limita a registrar una señal corporal, sino que la somete a procesos de análisis estadístico y aprendizaje automático que permiten generar inferencias sobre estados internos, disposiciones o probabilidades de comportamiento.

Desde el punto de vista jurídico, la relevancia de estas prácticas no depende exclusivamente del dato de entrada, sino del resultado inferencial y de los usos funcionales de dicho resultado. Como ha subrayado la doctrina, la sensibilidad de la información producida por sistemas algorítmicos no se deriva únicamente de la

naturaleza del dato original, sino del tipo de conocimiento que se genera y de los efectos materiales que dicho conocimiento produce sobre la persona.

En el caso de la biometría no identificante, este conocimiento inferido se encuentra corporalmente anclado y puede utilizarse para modular el entorno de interacción, ajustar estímulos, clasificar funcionalmente a la persona o explotar estados situacionales de fragilidad. La capacidad reveladora de estas inferencias resulta especialmente significativa cuando se integran en arquitecturas de interacción continua, y explica por qué la biometría no identificante puede afectar de manera relevante a la autonomía personal, a la igualdad material y al control efectivo de la persona sobre su información, aun sin identificación singularizante.

Desde esta perspectiva, la calificación jurídica de la biometría no identificante como información corporal permite comprender por qué estos tratamientos exigen una aplicación particularmente estricta de los criterios de necesidad, finalidad y proporcionalidad, y por qué su evaluación no puede descansar exclusivamente en la ausencia de identificación ni en su encaje parcial en categorías normativas preexistentes. Esta concepción prepara el análisis de los riesgos para los derechos fundamentales que se desarrollará en el capítulo siguiente (§4) y fundamenta, posteriormente, la centralidad de la lógica preventiva del RGPD en la gestión de estos tratamientos.

§2.5. De la biometría no singularizante al perfilado inferencial en ecosistemas de datos masivos

(1) Este apartado introduce un cambio de escala respecto de los anteriores. Mientras que en §§2.2.2 y 2.2.3 se ha descrito el funcionamiento de sistemas no singularizantes como arquitecturas inferenciales que operan sobre señales corporales en contextos de interacción, aquí se examina su integración en infraestructuras de datos masivos. En este nivel, la relevancia jurídica ya no depende solo de lo que el sistema infiere en un evento concreto, sino del modo en que esas inferencias se combinan, se normalizan y se reutilizan funcionalmente en ecosistemas de perfilado y modulación del entorno decisional.

En el contexto contemporáneo de los datos masivos, la biometría no singularizante se integra de forma estructural en arquitecturas de categorización y perfilado que operan a gran escala y, con frecuencia, en tiempo real. A diferencia de los modelos clásicos de tratamiento de datos personales —centrados en la recogida, conservación y reutilización de información identificante—, estas arquitecturas se orientan principalmente a extraer valor funcional de la inferencia, utilizando señales corporales para interpretar estados, disposiciones o probabilidades de comportamiento sin necesidad de fijar una identidad estable.

(2) Desde una perspectiva técnico-funcional, el perfilado biométrico no singularizante se apoya en procesos de aprendizaje automático diseñados para identificar patrones, regularidades y correlaciones en conjuntos amplios de datos. Estos procesos no se limitan a describir información observable, sino que permiten inferir información no directamente captada, predecir comportamientos futuros o estimar disposiciones internas de la persona a partir de señales corporales parciales. Como han señalado Gutwirth y Hildebrandt, el perfilado algorítmico permite descubrir patrones implícitos en los datos que resultan funcionalmente relevantes para la toma de decisiones automatizadas, ampliando el alcance material del tratamiento más allá de los datos recogidos en bruto (Gutwirth & Hildebrandt, 2010; Wachter & Mittelstadt, 2019).

En los sistemas biométricos no singularizantes, este perfilado se construye necesariamente sobre una biometrización previa del cuerpo, entendida como la transformación de señales corporales o cuasi corporales en atributos mensurables susceptibles de tratamiento automatizado. A diferencia del perfilado conductual clásico —basado en historiales de navegación, patrones de consumo o preferencias declaradas—, el perfilado biométrico se nutre de información inherente al cuerpo, que la persona no puede dejar de emitir sin excluirse del entorno de interacción. Esta circunstancia confiere a estos tratamientos una densidad específica en términos de afectación de la vida privada y de la autodeterminación informativa.

(3) Nótese que el perfilado biométrico no singularizante no se dirige necesariamente a individuos identificados ni requiere la creación de perfiles persistentes asociados a una identidad civil. Puede operar sobre grupos, colectivos o categorías funcionales, ajustando dinámicamente el trato, la exposición a estímulos o el entorno decisional en función de inferencias situacionales. La ausencia de identificación civil no reduce el impacto jurídico del tratamiento; en muchos casos, lo incrementa, al dificultar la percepción del perfilado y la posibilidad de reconstruir a posteriori sus efectos. Como ha subrayado la doctrina, este tipo de perfilado puede producir impactos materiales significativos sin traducirse en decisiones automatizadas aislables en el sentido del artículo 22 RGPD.

La inserción de la biometría no singularizante en ecosistemas de datos masivos intensifica, además, los riesgos asociados a la normalización del perfilado. En entornos digitales de uso cotidiano —como el comercio electrónico, el entretenimiento o las plataformas de interacción social—, las prácticas de categorización y adaptación funcional tienden a presentarse como mecanismos neutros de personalización o mejora de la experiencia de usuario. Sin embargo, cuando estas prácticas se apoyan en inferencias biométricas, el cambio cualitativo es relevante: el sistema deja de reaccionar únicamente a acciones observables y comienza a operar sobre estados corporales y disposiciones internas, con capacidad para modular la conducta de manera continua y poco perceptible.

(4) Desde el punto de vista jurídico, lo decisivo en estos supuestos no es la ausencia de identificación singular, sino el hecho de que las inferencias biométricas se integren en procesos automatizados de evaluación de aspectos personales. En este sentido, el perfilado biométrico no singularizante constituye una forma de tratamiento plenamente comprendida en la definición de perfilado del artículo 4.4 RGPD, aun cuando no dé lugar a decisiones automatizadas aislables ni a la creación de identidades persistentes.

Esta calificación resulta determinante, pues activa el marco sustantivo de protección del RGPD con independencia de la tipología técnica del sistema o de su encaje en categorías específicas del RIA. Desde esta perspectiva, el riesgo jurídico no puede evaluarse exclusivamente a partir del criterio de la identificación, sino atendiendo a la integración funcional de las inferencias biométricas en arquitecturas de perfilado y modulación del entorno decisional, cuestión que será examinada de manera sistemática en el capítulo siguiente (§3).

§3. MARCO NORMATIVO APLICABLE AL TRATAMIENTO BIOMÉTRICO NO SINGULARIZANTE EN LA UE

(1) El análisis de los tratamientos biométricos no singularizantes mediante sistemas de inteligencia artificial exige situar el examen jurídico en un marco normativo plural, caracterizado por la concurrencia de instrumentos con finalidades, técnicas regulatorias y presupuestos dogmáticos distintos. En el Derecho de la Unión Europea, dicha concurrencia se articula fundamentalmente en torno a dos Reglamentos de aplicación directa: el Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD), y el Reglamento (UE) 2024/1689, Reglamento de Inteligencia Artificial (RIA).

Ambos Reglamentos responden a lógicas regulatorias diferentes. El RGPD se configura como un instrumento transversal de tutela de derechos fundamentales frente a los riesgos derivados del tratamiento de datos personales, construido sobre una lógica material de gestión preventiva del riesgo y sobre el principio de responsabilidad del responsable del tratamiento. El RIA, por su parte, se concibe como un marco horizontal de gobernanza de sistemas de inteligencia artificial, adoptado principalmente con base en el Derecho del mercado interior y estructurado en torno a una clasificación *ex ante* de usos y sistemas en función de niveles de riesgo predeterminados (Smuha, 2021).

(2) En el ámbito específico de la biometría, esta divergencia de racionalidades adquiere una relevancia particular. Mientras que el RGPD articula su intervención a partir del tratamiento de información personal relativa a personas físicas identificadas o identificables y de los efectos materiales que dicho tratamiento produce sobre sus derechos y libertades, el RIA centra su atención en determinadas funcionalidades de los sistemas de inteligencia artificial y en los contextos de uso considerados especialmente sensibles. Esta diferencia metodológica explica que amplios conjuntos de tratamientos biométricos —en particular los no singularizantes y de carácter inferencial— queden plenamente comprendidos en el ámbito de aplicación del RGPD, pero solo de forma parcial, fragmentaria o indirecta en el RIA.

El objetivo del presente capítulo es examinar de forma sistemática el marco normativo europeo aplicable a los tratamientos biométricos no singularizantes, atendiendo tanto a las exigencias derivadas del RGPD (§3.2) como al tratamiento específico del reconocimiento biométrico y del perfilado en el RIA (§3.3). A partir de este análisis, se identificará la zona de fricción normativa existente entre ambos Reglamentos y se justificará la necesidad de una lectura coordinada, que evite zonas de infra-protección de los derechos fundamentales (§3.4).

Este enfoque integrado resulta imprescindible para evitar una lectura formalista del Derecho de la Unión que asocie automáticamente ausencia de identificación singularizante con ausencia de riesgo, y que desplace la tutela efectiva de los derechos hacia mecanismos reactivos o *ex post*, en tensión con la lógica preventiva que inspira el RGPD.

§3.1. LA COMPLEJIDAD DE UBICAR LOS TRATAMIENTOS BIOMÉTRICOS NO SINGULARIZANTES EN EL MARCO NORMATIVO EUROPEO

(1) La ubicación jurídica de los tratamientos biométricos no singularizantes impulsados por sistemas de inteligencia artificial presenta una dificultad estructural previa: no constituyen el objeto central de ninguno de los dos grandes Reglamentos europeos que inciden sobre ellos. Tanto el RGPD como el RIA los alcanzan, pero lo

hacen desde perspectivas distintas y parcialmente incongruentes con la naturaleza inferencial de estas prácticas.

El RGPD se construye como un marco transversal de protección de derechos fundamentales frente al tratamiento de datos personales, con independencia de la tecnología empleada. Su lógica no es tipificadora ni sectorial, sino material: el eje de intervención lo constituyen los riesgos para los derechos y libertades de las personas, evaluados a partir de la naturaleza, el contexto, las finalidades y los efectos del tratamiento (Considerando 75, RGPD). Desde esta lógica, el Reglamento resulta conceptualmente capaz de abarcar tratamientos biométricos no singularizantes, aun cuando estos no encajen en la definición funcional de datos biométricos orientados a la identificación única del artículo 4.14 RGPD.

El RIA, por su parte, responde a una racionalidad distinta. Su objetivo principal es la gobernanza *ex ante* de sistemas de inteligencia artificial en el mercado interior, mediante la clasificación de prácticas y sistemas en categorías normativas predeterminadas (prácticas prohibidas, sistemas de alto riesgo, sistemas sujetos a obligaciones específicas o sistemas de riesgo mínimo). Esta técnica regulatoria ha conducido a concentrar la atención en determinadas modalidades de reconocimiento biométrico —especialmente la identificación singularizante, en particular cuando es remota y en tiempo real—, relegando a un segundo plano prácticas biométricas no orientadas a la identificación que operan mediante inferencias continuas y categorización funcional.

(2) Esta divergencia de enfoques genera un problema específico para los tratamientos biométricos no singularizantes. Desde la perspectiva del RGPD, se trata de tratamientos plenamente relevantes por su capacidad para individualizar funcionalmente a las personas, inferir aspectos personales y modular el trato recibido. Desde la perspectiva del RIA, en cambio, estas prácticas tienden a quedar fragmentadas, infra-tipificadas o situadas en zonas de baja visibilidad normativa, al no encajar con claridad en las categorías que estructuran el régimen de prohibiciones y obligaciones reforzadas.

El resultado no es un vacío normativo absoluto, sino una dificultad de encaje sistemático que exige una lectura coordinada de ambos Reglamentos. El tratamiento jurídico de la biometría no singularizante no puede resolverse ni mediante una aplicación aislada del RGPD —ignorando el impacto del RIA en la gobernanza de los sistemas—, ni mediante una lectura autosuficiente del RIA —prescindiendo de la lógica material de protección de derechos del RGPD.

Sobre esta base, los apartados siguientes analizan, en primer lugar, el estatuto jurídico que el RGPD proyecta sobre los tratamientos biométricos no singularizantes (§3.2). En segundo lugar, se examina el tratamiento fragmentario que el RIA ofrece en materia de reconocimiento biométrico (§3.3). Finalmente, se aborda la zona específica de fricción normativa que se produce entre ambos Reglamentos respecto de la categorización y el perfilado biométrico no singularizante (§3.4).

§3.2. El estatuto jurídico de los tratamientos biométricos no singularizantes desde la perspectiva del Reglamento General de Protección de Datos

(1) Frente a las dificultades de encaje sistemático que presentan los tratamientos biométricos no singularizantes en el Reglamento (UE) 2024/1689 de Inteligencia Artificial, el RGPD ofrece un marco normativo conceptualmente más adecuado para abordar este tipo de prácticas. Ello no se debe a que el RGPD haya sido diseñado específicamente para regular la biometría no singularizante, sino a que su lógica de

intervención no descansa en tipologías tecnológicas cerradas, sino en la identificación y gestión preventiva de los riesgos que el tratamiento de datos personales puede generar para los derechos y libertades de las personas físicas.

El RGPD se configura como un Reglamento de alcance general, tecnológicamente neutro y orientado a la protección material de la persona frente al tratamiento de información personal, con independencia de la técnica empleada o de la finalidad identificante del tratamiento. Su eje no es la identidad como tal, sino la afectación efectiva de derechos, evaluada a partir de la naturaleza, el contexto, las finalidades y los efectos del tratamiento. Esta estructura permite integrar jurídicamente prácticas biométricas que no culminan en la identificación singularizante, pero que individualizan funcionalmente a la persona, generan inferencias sobre aspectos personales y condicionan el trato recibido.

(2) Desde esta perspectiva, los tratamientos biométricos no singularizantes encuentran en el RGPD un estatuto jurídico materialmente coherente, aunque no exento de tensiones interpretativas. La aplicabilidad del Reglamento no depende de que el sistema encaje en una categoría tecnológica predeterminada, sino de que exista un tratamiento de datos personales relativo a personas físicas identificadas o identificables y de que dicho tratamiento pueda entrañar riesgos para sus derechos y libertades.

Esta lógica permite abordar jurídicamente dimensiones centrales de la biometría no singularizante ya identificadas en el capítulo anterior, como la identificabilidad funcional, la inferencia de aspectos personales, la categorización automatizada, la capacidad reveladora de atributos sensibles y la modulación del entorno de interacción. Al mismo tiempo, el RGPD incorpora instrumentos específicamente orientados a la gestión preventiva del riesgo, como los principios del artículo 5, la evaluación de impacto relativa a la protección de datos y el principio de responsabilidad proactiva, que resultan especialmente pertinentes en arquitecturas inferenciales continuas y opacas.

§3.2.1. Ámbito de aplicación del RGPD y noción de identificabilidad en tratamientos biométricos no singularizantes

(1) El Reglamento (UE) 2016/679 se aplica a todo tratamiento de datos personales relativo a personas físicas identificadas o identificables (arts. 2.1 y 4.1 RGPD). La noción de identificabilidad, tal como resulta del propio Reglamento y de su interpretación consolidada, no se limita a la identificación civil directa, ni exige la atribución de un nombre, un número de documento o un identificador estable. Basta con que una persona pueda ser individualizada de manera razonable, atendiendo a los medios que puedan ser utilizados por el responsable del tratamiento o por terceros, teniendo en cuenta el contexto y las finalidades del tratamiento (Considerando 26 RGPD).

En los tratamientos biométricos no singularizantes, esta individualización se produce habitualmente de forma funcional y contextual, aun cuando no exista identificación nominal ni enrolamiento biométrico clásico. La persona interactúa con un servicio o entorno determinado, desde un dispositivo concreto y en un contexto espacio-temporal específico, y es destinataria directa de inferencias y adaptaciones funcionales que presuponen su unicidad situacional. Esta forma de individualización basta para afirmar la identificabilidad a efectos del RGPD, incluso cuando el sistema no permite identificar a la persona fuera de ese contexto ni genera perfiles persistentes a largo plazo (Wachter & Mittelstadt, 2019; Hildebrandt, 2020).

(2) La doctrina ha subrayado que la *identificabilidad* debe evaluarse de forma relacional y contextual, atendiendo no solo a la existencia de identificadores directos,

sino también a la capacidad del tratamiento para distinguir a una persona de otras en una situación concreta y para producir efectos diferenciados sobre ella. Desde esta perspectiva, un tratamiento puede recaer sobre datos personales aun cuando la identidad civil permanezca desconocida, si el sistema está en condiciones de individualizar a la persona en el momento de la interacción y de modular su trato en función de inferencias sobre sus características, estados o comportamientos.

En el caso de la biometría no singularizante, esta individualización funcional se ve reforzada por la inherencia corporal de la información tratada. Las señales biométricas, aun cuando no permitan identificar de manera estable a la persona, se refieren necesariamente a un cuerpo concreto en un momento determinado y permiten inferir atributos o estados que se proyectan directamente sobre la persona presente. La ausencia de identificación singularizante no elimina, por tanto, la conexión entre el tratamiento y una persona identificable, sino que desplaza la identificación desde la identidad civil hacia la situación de interacción.

(3) Desde el punto de vista del ámbito de aplicación del RGPD, excluir los tratamientos biométricos no singularizantes por el mero hecho de que no permitan identificar civilmente a la persona supondría una interpretación excesivamente restrictiva del concepto de dato personal y vaciaría de contenido la tutela prevista frente a tratamientos que producen efectos materiales significativos sobre los derechos y libertades. En esta línea, el Tribunal de Justicia ha afirmado que la protección del RGPD no depende de la identificación formal de la persona, sino de la posibilidad de individualización razonable y de la afectación efectiva de su esfera jurídica o fáctica (TJUE, Gran Sala, asunto C-61/22, RL, 2024).

En consecuencia, los tratamientos biométricos no singularizantes basados en inteligencia artificial, en la medida en que recaen sobre información corporal relativa a personas individualizadas en contextos concretos y permiten generar inferencias que inciden en el trato recibido, se sitúan dentro del ámbito de aplicación del RGPD. Esta constatación permite examinar, en los apartados siguientes, la proyección de los principios del tratamiento y de los instrumentos preventivos del Reglamento sobre este tipo de prácticas.

§3.2.2. Principios del artículo 5 RGPD y biometría no singularizante

Una vez afirmada la aplicabilidad del RGPD a los tratamientos biométricos no singularizantes, resulta necesario examinar cómo se proyectan sobre ellos los principios del artículo 5 RGPD, interpretados desde una perspectiva material y orientada a la gestión preventiva del riesgo. Estos principios constituyen el núcleo sustantivo del Reglamento y operan como criterios de evaluación transversales, con independencia de la tecnología empleada o de la ausencia de finalidad identificante del tratamiento.

(a) El principio de licitud, lealtad y transparencia (art. 5.1.a RGPD) adquiere una relevancia específica en los tratamientos biométricos no singularizantes. La captación de señales corporales y la generación de inferencias en tiempo real suelen integrarse de forma poco perceptible en la experiencia de interacción, lo que dificulta que la persona comprenda qué información se trata, qué inferencias se generan y con qué efectos funcionales se utilizan. En este contexto, la transparencia no puede reducirse a la mera provisión formal de información, sino que exige evitar configuraciones del tratamiento que instrumentalicen estados corporales, emocionales o atencionales de manera opaca o inesperada para la persona afectada.

(b) El principio de limitación de la finalidad (art. 5.1.b RGPD) se ve especialmente tensionado cuando las infraestructuras biométricas se diseñan como plataformas reutilizables de inferencia. En estos supuestos, el riesgo no reside únicamente en la recogida inicial de señales corporales, sino en la ampliación progresiva de las inferencias y de sus usos funcionales. Limitar la finalidad implica, por tanto, no solo definir para qué se recogen los datos, sino delimitar *ex ante* qué inferencias pueden legítimamente extraerse y con qué consecuencias, evitando derivas funcionales no evaluadas.

(c) El principio de minimización de datos (art. 5.1.c RGPD) no puede interpretarse de forma exclusivamente cuantitativa. En los tratamientos biométricos no singularizantes, la minimización exige atender a la intensidad y profundidad de la inferencia, y no solo al volumen de datos captados o a su tiempo de conservación. Un tratamiento puede resultar altamente intrusivo aun cuando la muestra en bruto se descarte de inmediato, si las inferencias generadas permiten revelar atributos sensibles o modular de manera significativa el entorno decisional de la persona (Hildebrandt, 2020).

(d) El principio de exactitud (art. 5.1.d RGPD) plantea problemas específicos en contextos inferenciales. Las categorizaciones biométricas no singularizantes se basan en modelos probabilísticos y correlaciones estadísticas, con tasas de error que no se distribuyen de manera uniforme entre personas o grupos. La inexactitud estructural o los errores sistemáticos pueden producir efectos adversos acumulativos, aun cuando no exista una decisión automatizada puntual fácilmente identificable. Desde esta perspectiva, la exactitud debe evaluarse atendiendo a la fiabilidad de las inferencias y a sus efectos materiales, y no únicamente a la corrección formal del dato captado.

(e) Por último, los principios de limitación del plazo de conservación y de integridad y confidencialidad (art. 5.1.e y f RGPD) deben interpretarse teniendo en cuenta que, en los sistemas biométricos no singularizantes, la persistencia del impacto puede desplazarse desde los datos en bruto hacia los modelos, parámetros y lógicas inferenciales. La eliminación temprana de las muestras originales no garantiza, por sí sola, la neutralización del riesgo si las inferencias continúan produciendo efectos sobre las personas a través de sistemas opacos y difícilmente auditables.

En perspectiva de conjunto conjunto, la aplicación de los principios del artículo 5 RGPD a los tratamientos biométricos no singularizantes exige una interpretación funcional y orientada a los efectos del tratamiento, que atienda a la capacidad inferencial del sistema, a la continuidad de la captación y a la intensidad de la modulación del entorno de interacción. Esta lectura material del Reglamento permite abordar con mayor precisión el perfilado biométrico como forma de tratamiento (§3.2.3), así como la eventual aplicación del régimen de categorías especiales de datos (§3.2.4) y la procedencia de evaluaciones de impacto y de medidas de responsabilidad proactiva (§3.2.5).

§3.2.3. PERFILADO, CATEGORIZACIÓN Y CRIBADO BIOMÉTRICO COMO FORMAS DE TRATAMIENTO EN EL RGPD

(1) El Reglamento (UE) 2016/679 define el perfilado como toda forma de tratamiento automatizado de datos personales consistente en utilizar dichos datos para evaluar aspectos personales de una persona física, en particular para analizar o predecir elementos relativos a su comportamiento, preferencias, intereses, fiabilidad, situación

económica, salud o movimientos (art. 4.4 RGPD). Esta definición resulta plenamente aplicable a los tratamientos biométricos no singularizantes basados en inteligencia artificial, en la medida en que estos utilizan señales corporales tratadas de forma automatizada para inferir estados, disposiciones o probabilidades de comportamiento de la persona durante la interacción.

En este tipo de tratamientos, el perfilado no se articula necesariamente como una operación puntual ni culmina en una decisión automatizada individual en el sentido del artículo 22 RGPD. Por el contrario, suele integrarse en arquitecturas de interacción continua, en las que las inferencias biométricas se utilizan para ajustar dinámicamente el entorno, la presentación de opciones, la intensidad de estímulos o el ritmo de la interacción. La relevancia jurídica del perfilado biométrico no deriva, por tanto, de la existencia de una decisión aislable, sino de una evaluación sistemática de aspectos personales y de la producción de efectos materiales sobre la persona, aun cuando dichos efectos se manifiesten de forma gradual o acumulativa (Wachter & Mittelstadt, 2019; Hildebrandt, 2020).

(2) Junto al perfilado, los tratamientos biométricos no singularizantes incorporan con frecuencia operaciones de categorización y de cribado. La categorización biométrica consiste en asignar a la persona, de manera automatizada, a una o varias categorías funcionales a partir de atributos biométricos inferidos —como rangos de edad estimados, estados emocionales, niveles de atención o patrones de comportamiento. El cribado biométrico, por su parte, se refiere a la detección automatizada de la presencia de determinados atributos o estados en personas no previamente enroladas, con el fin de activar respuestas diferenciadas del sistema. Ambas operaciones constituyen formas de tratamiento de datos personales cuando permiten evaluar aspectos personales y modular el trato recibido, con independencia de que no se asocien a una identidad civil ni generen perfiles persistentes.

Desde la perspectiva del RGPD, ni la categorización ni el cribado biométrico pueden considerarse jurídicamente neutros. La asignación automatizada a categorías funcionales incorpora necesariamente decisiones previas sobre qué atributos se consideran relevantes y sobre qué consecuencias funcionales se asocian a su detección. Estas decisiones se traducen en efectos diferenciados sobre la persona —por ejemplo, variaciones en el acceso a contenidos, en la exposición a estímulos persuasivos o en las condiciones de interacción—, lo que sitúa estas prácticas dentro del ámbito material del perfilado en el sentido del artículo 4.4 RGPD (Gutwirth & Hildebrandt, 2010; Rouvroy & Berns, 2013).

(3) La especificidad del perfilado biométrico no singularizante reside en su apoyo en información corporal y en su capacidad para inferir estados internos o disposiciones situacionales que la persona no ha exteriorizado voluntariamente. Esta característica intensifica la asimetría informativa entre el responsable del tratamiento y la persona afectada y dificulta la percepción del tratamiento y el ejercicio efectivo de los derechos reconocidos en el RGPD. A diferencia del perfilado conductual clásico, basado en acciones observables o preferencias declaradas, el perfilado biométrico opera sobre señales inherentes al cuerpo, cuya emisión no puede interrumpirse sin abandonar el entorno de interacción (Simitis, 2011; González Fuster, 2014).

En este contexto, la evaluación jurídica del perfilado biométrico no singularizante no puede limitarse a comprobar si se activa formalmente el régimen del artículo 22 RGPD. El análisis debe atender a la evaluación continuada y automatizada sistemática de aspectos personales, a la continuidad del tratamiento, a la opacidad de las inferencias y a los efectos materiales producidos sobre la autonomía, la igualdad material y la autodeterminación informativa.

Esta aproximación resulta coherente con el Considerando 75 RGPD, que identifica como riesgos relevantes no solo las decisiones automatizadas con efectos jurídicos, sino también la discriminación, la pérdida de control sobre los datos personales y los efectos adversos significativos sobre personas en situaciones de vulnerabilidad (Hijmans, 2016; Wachter, 2018).

(4) La consideración del perfilado, la categorización y el cribado biométrico como formas de tratamiento plenamente comprendidas en el RGPD permite abordar, en los apartados siguientes, dos cuestiones centrales: de una parte, la posible aplicación del régimen de categorías especiales de datos cuando las inferencias biométricas revelan información sensible (§3.2.4); de otra, la procedencia de evaluaciones de impacto y de medidas de responsabilidad proactiva en función del riesgo material del tratamiento (§3.2.5).

§3.2.4. CATEGORÍAS ESPECIALES DE DATOS Y BIOMETRÍA NO SINGULARIZANTE

(1) El hecho de que un tratamiento biométrico no tenga como finalidad la identificación única de la persona no excluye, por sí mismo, la posible aplicación del régimen reforzado de protección previsto en el artículo 9 RGPD. Ahora bien, en estos supuestos, la aplicabilidad de dicho régimen no puede fundamentarse automáticamente en la definición de datos biométricos del artículo 4.14 RGPD, que vincula expresamente la biometría a la capacidad de permitir o confirmar la identificación única de una persona física. La ausencia de finalidad identificante excluye, por tanto, la activación automática del artículo 9 RGPD por la vía definicional del artículo 4.14, pero no impide su aplicación material cuando el tratamiento biométrico no singularizante revela o permite inferir información comprendida en las categorías especiales del artículo 9.1 RGPD.

Este desplazamiento desde una lógica definicional hacia una lógica material exige atender al rationale propio del artículo 9 RGPD. Desde una perspectiva dogmática, dicho precepto no se apoya en una noción sustantiva o esencialista de “sensibilidad” del dato, sino en una evaluación normativa del riesgo que determinados tratamientos entrañan para los derechos y libertades fundamentales de las personas. Las denominadas categorías especiales de datos personales no se caracterizan por una cualidad intrínseca del dato, sino por su potencial para generar discriminación, estigmatización, exclusión social o afectaciones especialmente intensas de la autonomía personal cuando son objeto de tratamiento automatizado. En este sentido, la protección reforzada del artículo 9 responde a una lógica preventiva y material, orientada a evitar usos estructuralmente lesivos de la información, con independencia de que el dato se haya recogido de forma explícita o se infiera a partir de otros datos personales (Cano Ruiz, 2019; Medina Guerrero, 2019; Troncoso Reigada, 2021).

(2) Sobre esta base, resulta especialmente relevante la posición que ocupa la biometría en el sistema del RGPD. Tal como se ha expuesto en el marco conceptual (§2.4), una de las características estructurales de la biometría —también en sus modalidades no singularizantes— es su capacidad reveladora de atributos especialmente protegidos, derivada de la estrecha vinculación entre la información tratada y el cuerpo humano como fuente primaria de datos. Esta capacidad no se agota en la identificación singularizante, sino que permite inferir estados fisiológicos, condiciones de salud, disposiciones psicocognitivas o rasgos incluidos en las categorías especiales del artículo 9 RGPD, aun cuando el tratamiento no se presente formalmente como médico ni se asocie a una identidad civil determinada.

Desde esta misma perspectiva material, el artículo 9 RGPD protege frente al tratamiento de datos que revelen, entre otros, información relativa a la salud, al origen racial o étnico, a las convicciones religiosas o filosóficas o a la vida sexual u orientación sexual. Esta protección no se limita a la recogida explícita de dichos datos, sino que se extiende a los tratamientos que permiten inferir razonablemente este tipo de información a partir de otros datos personales, cuando dicha inferencia resulta previsible atendiendo al diseño del sistema, a su lógica inferencial y a la finalidad funcional del tratamiento. En este sentido, el Tribunal de Justicia ha confirmado que la revelación indirecta o inferencial de información comprendida en las categorías especiales activa el régimen del artículo 9 RGPD cuando dicha revelación constituye un resultado razonablemente previsible del tratamiento (TJUE, asunto C-184/20, *Vyriausioji*, 2022).

(3) Esta problemática adquiere una intensidad particular en el ámbito de la biometría no singularizante cuando las inferencias biométricas se integran en arquitecturas de categorización y perfilado continuos, propias de la era de los datos masivos (§2.5). En estos contextos, las señales biométricas no se tratan de forma aislada, sino que alimentan modelos inferenciales capaces de producir conocimiento funcional sobre la persona y de modular el entorno de interacción en tiempo real, con independencia de que exista o no un perfil persistente asociado a una identidad civil.

La doctrina ha advertido de forma reiterada que una interpretación restrictiva del artículo 9 RGPD, limitada a los supuestos de recogida expresa de datos incluidos en las categorías especiales, permitiría eludir de facto la protección reforzada mediante el uso de técnicas inferenciales cada vez más sofisticadas. Desde esta perspectiva, el riesgo jurídico no reside únicamente en el dato de entrada, sino en el resultado informacional del tratamiento, esto es, en el tipo de conocimiento que el sistema está en condiciones de producir sobre la persona y en los efectos materiales que dicho conocimiento genera, especialmente cuando se combina con procesos de perfilado continuo (Cano Ruiz, 2019; Simitis, 2011; Wachter & Mittelstadt, 2019).

Esta dinámica se manifiesta con especial intensidad en tratamientos biométricos no singularizantes integrados en entornos de interacción cotidiana —como plataformas digitales de consumo, servicios de entretenimiento o aplicaciones de monitorización del rendimiento, la atención o el estado emocional—, en los que las inferencias biométricas pueden utilizarse para adaptar el entorno de interacción, intensificar estímulos o modular decisiones sin que la persona sea consciente de que se están generando inferencias relativas a aspectos comprendidos en las categorías especiales de datos personales en el sentido del artículo 9.1 RGPD.

(4) Desde la perspectiva del RGPD, cuando un tratamiento biométrico no singularizante permite revelar o inferir información incluida en las categorías especiales de datos, resulta aplicable la prohibición general establecida en el artículo 9.1 RGPD, salvo que concurra alguna de las excepciones previstas en el artículo 9.2. La identificación de una base de legitimación válida en estos supuestos exige una evaluación especialmente rigurosa de la necesidad y proporcionalidad del tratamiento, así como de las garantías adicionales adoptadas para proteger los derechos y libertades de la persona afectada, en coherencia con la lógica preventiva del Reglamento (Troncoso Reigada, 2021).

En este sentido, la conexión entre biometría no identificante, capacidad reveladora de atributos especialmente protegidos (§2.4) y perfilado en entornos de datos masivos (§2.5) refuerza la necesidad de abordar estos tratamientos desde una lógica preventiva. La evaluación de si un sistema permite inferir información comprendida en las categorías especiales de datos constituye un elemento central en la identificación del riesgo y en la determinación de las obligaciones del responsable del tratamiento,

cuestión que se desarrolla a continuación al analizar la procedencia de las evaluaciones de impacto y de las medidas de responsabilidad proactiva (§3.2.5).

§3.2.5. Evaluación de impacto y responsabilidad proactiva en tratamientos biométricos no singularizantes

(1) La evaluación de impacto relativa a la protección de datos (EIPD) constituye el instrumento central del Reglamento (UE) 2016/679 para la gestión preventiva del riesgo. Conforme al artículo 35 RGPD, la realización de una EIPD resulta obligatoria cuando un tipo de tratamiento, en particular si utiliza nuevas tecnologías, puede entrañar un alto riesgo para los derechos y libertades de las personas físicas, atendiendo a su naturaleza, alcance, contexto y finalidades. La EIPD no se concibe, por tanto, como un requisito meramente formal o documental, sino como una técnica de garantía orientada a identificar, evaluar y mitigar riesgos antes de que estos se materialicen en perjuicios efectivos para las personas afectadas.

Los tratamientos biométricos no singularizantes basados en sistemas de inteligencia artificial reúnen con frecuencia varios de los criterios indicativos de alto riesgo identificados por la doctrina y por las autoridades de protección de datos. Entre ellos destacan la evaluación sistemática de aspectos personales mediante tratamiento automatizado, la captación y análisis de información corporal, la generación de inferencias con efectos funcionales sobre el entorno de interacción y la integración del tratamiento en arquitecturas continuas y adaptativas (§§2.4 y 2.5). En este sentido, la EIPD opera como un mecanismo de racionalización del diseño y del despliegue del sistema, permitiendo anticipar impactos acumulativos que no siempre resultan visibles a partir de decisiones aisladas o eventos singulares (Marín Jiménez, 2019).

(2) La ausencia de identificación singularizante o de enrolamiento biométrico clásico no excluye, en modo alguno, la procedencia de una evaluación de impacto. Tal como se ha argumentado en los apartados anteriores (§§3.2.1–3.2.4), el riesgo relevante a efectos del RGPD no se define por la finalidad identificante, sino por la capacidad del tratamiento para producir efectos adversos significativos sobre la autonomía personal, la igualdad material, la autodeterminación informativa o la posibilidad de control efectivo por parte de la persona interesada. En este contexto, la inferencia biométrica continua y la modulación del entorno de interacción constituyen factores materiales que justifican plenamente la realización de una EIPD, aun cuando el sistema no permita identificar civilmente a la persona.

Desde un punto de vista sustantivo, la EIPD en tratamientos biométricos no singularizantes no puede reducirse a una descripción abstracta de flujos de datos ni a la identificación nominal de una base jurídica. Debe abordar de manera específica y contextualizada, al menos, los siguientes elementos:

(a) Las señales biométricas efectivamente captadas y su carácter estático o dinámico.
(b) Las inferencias que el sistema está en condiciones de generar, incluidas aquellas relativas a atributos especialmente protegidos en el sentido del artículo 9 RGPD (§3.2.4).
(c) La necesidad y proporcionalidad del uso inferencial, atendiendo a la intensidad, continuidad y finalidad funcional del tratamiento (§2.5).
(d) Los riesgos concretos para los derechos y libertades, valorados en términos de probabilidad y gravedad, con atención expresa a la autonomía personal, la igualdad material y la capacidad de control efectivo de la persona interesada.

(3) La doctrina ha subrayado que la EIPD constituye una manifestación cualificada del principio de responsabilidad proactiva, en la medida en que obliga al responsable del tratamiento no solo a cumplir formalmente con el RGPD, sino a integrar la evaluación del riesgo en el propio proceso de toma de decisiones organizativas y técnicas (de la Prada Espina, 2018). En tratamientos biométricos no singularizantes, esta exigencia adquiere una relevancia particular, dado que los efectos del tratamiento no se agotan en un momento identificable, sino que se despliegan de forma progresiva y, en ocasiones, difícilmente perceptible para la persona afectada.

La evaluación de impacto se inserta, además, en el marco más amplio del principio de responsabilidad proactiva, consagrado en el artículo 24 RGPD. Este principio no se agota en un deber de cumplimiento formal, sino que impone al responsable del tratamiento la obligación de garantizar y poder demostrar que el tratamiento se ajusta al Reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento. La EIPD se configura así como un instrumento central de control interno y de rendición de cuentas, estrechamente vinculado a la gobernanza efectiva del tratamiento (Sáiz Peña, 2019).

La experiencia comparada y sectorial muestra, además, que la EIPD adquiere especial valor en contextos institucionales complejos, caracterizados por relaciones asimétricas de poder y por la dificultad de ejercer controles individuales *ex post*. En estos entornos, la evaluación de impacto permite introducir garantías estructurales en fases tempranas del tratamiento, limitando derivas funcionales y reforzando la transparencia organizativa (Auzmendi del Solar & Mayor Gómez, 2023). Esta consideración resulta plenamente trasladable a los sistemas biométricos no singularizantes integrados en entornos digitales de uso cotidiano, en los que la percepción individual del riesgo y la activación de mecanismos de control resultan especialmente limitadas.

(4) La omisión injustificada de una evaluación de impacto o la realización meramente formal de la misma puede tener consecuencias jurídicas relevantes, tanto desde la perspectiva de la licitud del tratamiento como en el marco de la actuación de las Autoridades de Protección de Datos. En tratamientos biométricos no singularizantes con elevada capacidad inferencial, la EIPD opera como un instrumento de racionalización del tratamiento, que permite identificar límites materiales antes de que los riesgos se materialicen de forma acumulativa y difícilmente reversible.

La evaluación de impacto y el principio de responsabilidad proactiva delimitan, así, el marco operativo desde el que debe analizarse la conformidad de los tratamientos biométricos no singularizantes con el RGPD. Este marco permite articular una tutela preventiva efectiva frente a prácticas que, aun sin identificación singularizante, presentan una elevada capacidad de afectación material de derechos fundamentales, y sitúa la gestión del riesgo en una fase previa a su materialización. Desde esta perspectiva se comprende el papel que corresponde a las Autoridades de Protección de Datos en la supervisión de estos tratamientos y los límites estructurales del control *ex post*, cuestiones que se desarrollan en el apartado siguiente (§3.2.6).

§3.2.6. Las funciones que el RGPD atribuye a las Autoridades de Protección de Datos, proyectadas a la biometría no singularizante

(1) El Reglamento (UE) 2016/679 atribuye a las Autoridades de Protección de Datos un papel central en la garantía de la aplicación efectiva del marco europeo de protección de datos personales. De conformidad con los artículos 51 a 59 RGPD, dichas Autoridades actúan como órganos independientes encargados de supervisar la aplicación del Reglamento, promover la comprensión de los riesgos derivados del

tratamiento de datos personales y ejercer, cuando proceda, potestades correctoras y sancionadoras. La entrada en vigor del RGPD ha supuesto, en este sentido, un cambio cualitativo en el estatuto y en las funciones de las Autoridades, que pasan de desempeñar un rol predominantemente reactivo a asumir un papel estructural en la gobernanza preventiva del riesgo y en la configuración material de las garantías aplicables a los tratamientos (Arenas Ramiro, 2021).

(2) En el ámbito de los tratamientos biométricos no singularizantes, esta función adquiere un perfil específico. Se trata de prácticas que, aun no orientadas a la identificación única de la persona, pueden implicar captación de información corporal, generación de inferencias sobre aspectos personales y afectación material de derechos fundamentales, tal como se ha expuesto en los apartados anteriores (§§2.4, 2.5 y 3.2.1–3.2.5). El RGPD no reserva la intervención de las Autoridades a supuestos de identificación biométrica en sentido estricto, sino que las habilita para actuar frente a cualquier tratamiento que pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, con independencia de la técnica empleada o de la finalidad declarada.

Desde esta perspectiva, corresponde a las Autoridades de Protección de Datos valorar, en el ejercicio de sus funciones ordinarias, la licitud y proporcionalidad de los tratamientos biométricos no singularizantes, interpretar la aplicabilidad de los principios del artículo 5 RGPD, apreciar la concurrencia de categorías especiales de datos cuando las inferencias biométricas revelan información incluida en el ámbito del artículo 9 RGPD (§3.2.4) y evaluar la procedencia, calidad y suficiencia de las evaluaciones de impacto realizadas por los responsables del tratamiento (§3.2.5). Esta función interpretativa y de control resulta especialmente relevante en contextos tecnológicos caracterizados por una elevada complejidad técnica y por arquitecturas inferenciales opacas, en los que la calificación jurídica del tratamiento no se desprende de forma inmediata de su presentación formal (Arenas Ramiro, 2025a).

(3) Un elemento particularmente relevante en este ámbito es la función orientadora y de producción de *soft law* que el RGPD atribuye a las Autoridades. A través de directrices, guías, criterios interpretativos, resoluciones y listas indicativas de tratamientos que requieren evaluación de impacto, las Autoridades contribuyen a concretar la aplicación del Reglamento en sectores caracterizados por una rápida evolución tecnológica y elevada asimetría informativa. En el caso de la biometría no singularizante, esta función resulta decisiva para evitar interpretaciones formalistas que asocien el riesgo exclusivamente a la identificación singular y para promover una lectura material del RGPD centrada en los efectos del tratamiento sobre las personas (Arenas Ramiro, 2021; Martínez Martínez, 2022).

Asimismo, las Autoridades desempeñan un papel clave en la operativización del principio de responsabilidad proactiva. La supervisión no se limita a constatar el cumplimiento formal de obligaciones documentales, sino que exige a los responsables del tratamiento que puedan demostrar la adecuación de sus decisiones de diseño, de sus evaluaciones de impacto y de las medidas técnicas y organizativas adoptadas en función del riesgo identificado. En tratamientos biométricos no singularizantes con elevada capacidad inferencial, este escrutinio se proyecta necesariamente sobre la arquitectura del sistema, sobre las inferencias permitidas y sobre los mecanismos de gobernanza del tratamiento, más allá de la mera existencia de políticas internas o cláusulas informativas de carácter más estandarizado.

(4) El marco del RGPD proporciona, por tanto, a las Autoridades de Protección de Datos instrumentos suficientes para intervenir frente a tratamientos biométricos no singularizantes desde una lógica preventiva, orientada a la identificación temprana del

riesgo y a la exigencia de garantías adecuadas antes de que los efectos adversos se materialicen de forma acumulativa. Esta función preventiva adquiere especial relevancia cuando estos tratamientos se despliegan en ecosistemas de datos complejos o en contextos de interacción cotidiana, en los que la percepción individual del riesgo y la activación de mecanismos de control por parte de las personas interesadas resultan limitadas (Martínez Martínez, 2022).

No obstante, la eficacia de esta intervención institucional se ve condicionada por las características propias de los tratamientos biométricos no singularizantes, en particular por su continuidad, su opacidad funcional y la dificultad de reconstruir *ex post* las inferencias generadas y sus efectos. Estas limitaciones estructurales del modelo clásico de control reactivo no cuestionan la competencia ni la legitimidad de las Autoridades, pero sí ponen de relieve la necesidad de reforzar la lógica preventiva y de diseño del tratamiento, especialmente cuando los sistemas afectan a colectivos vulnerables o a contextos de especial sensibilidad social (Arenas Ramiro, 2025b).

§3.3 El reconocimiento biométrico y el perfilado en el Reglamento (UE) 2024/1689 de Inteligencia Artificial

(1) El Reglamento (UE) 2024/1689 de Inteligencia Artificial (RIA) introduce un marco normativo específico para la gobernanza de determinados usos de sistemas de inteligencia artificial en la Unión Europea, con incidencia directa en algunas modalidades de reconocimiento biométrico y de tratamiento automatizado de información corporal. A diferencia del Reglamento General de Protección de Datos, el RIA no se articula como un instrumento general de tutela de derechos fundamentales frente al tratamiento de información personal, sino como un régimen de regulación *ex ant*e de sistemas y prácticas, adoptado fundamentalmente con base en el Derecho del mercado interior y orientado a garantizar un desarrollo armonizado y seguro de la inteligencia artificial en la Unión.

Esta diferencia de finalidad y de técnica normativa resulta decisiva para comprender el alcance del RIA respecto de los tratamientos biométricos no singularizantes. Mientras que el RGPD estructura su intervención a partir de la noción de tratamiento de datos personales y de la evaluación material del riesgo para los derechos y libertades de las personas, el RIA opera mediante un sistema de clasificación previa de usos y sistemas, a los que se asocian prohibiciones, obligaciones reforzadas o regímenes atenuados en función de criterios funcionales y contextuales predeterminados (Muñoz Vela, 2025; Eguiluz Castañeira, 2025).

(2) En el ámbito específico del reconocimiento biométrico, el RIA no parte de una concepción unitaria del fenómeno ni de una evaluación transversal de sus efectos, sino que fragmenta la regulación en una pluralidad de categorías jurídicas diferenciadas —identificación biométrica, verificación o autenticación biométrica, categorización biométrica y reconocimiento de emociones— cuyo estatuto normativo varía en función del contexto de uso, del grado de intervención del sistema y de elementos adicionales como la distancia, el tiempo real o la participación activa de la persona. Esta opción regulatoria responde a una lógica de gobernanza sectorial y de gestión *ex ante* del riesgo, pero plantea interrogantes relevantes desde la perspectiva de la protección material de los derechos fundamentales.

Desde un punto de vista constitucional y democrático, la adopción del RIA ha sido valorada como un paso significativo hacia la construcción de un modelo europeo de gobierno de la inteligencia artificial, orientado a compatibilizar innovación tecnológica y protección de valores fundamentales (Barrio Andrés, 2025). Sin embargo, la propia

estructura del Reglamento —basada en categorías tipificadas y en presunciones normativas de riesgo— condiciona su capacidad para captar adecuadamente determinadas prácticas biométricas inferenciales que no culminan en identificación singular, pero que pueden producir efectos materiales relevantes sobre la autonomía personal, la igualdad material o el control efectivo por parte de las personas afectadas (vid, en especial el análisis de Aba-Catoira et al., 2025).

(3) El análisis que sigue se centra, por tanto, en examinar cómo el RIA aborda el reconocimiento biométrico y el perfilado, y en identificar las consecuencias sistemáticas de esta regulación fragmentaria para la visibilidad jurídica de la biometría no singularizante. Con este objetivo, el apartado §3.3.1 describe la estructura dispersa del tratamiento del reconocimiento biométrico en el Reglamento, antes de analizar en los apartados posteriores la noción de riesgo que lo sustenta y sus efectos sobre la protección de los derechos fundamentales.

§3.3.1. El reconocimiento biométrico en el Reglamento (UE) 2024/1689: una regulación fragmentaria sin tratamiento unitario

El Reglamento de Inteligencia Artificial no establece un régimen unitario del reconocimiento biométrico. A diferencia de otros ámbitos regulados por el propio Reglamento, no existe un capítulo específico ni una definición general que permita identificar de manera sistemática qué modalidades de reconocimiento biométrico quedan comprendidas en su ámbito de aplicación, con qué estatuto jurídico y bajo qué condiciones (Escajedo San-Epifanio, 2024). La regulación del reconocimiento biométrico exige, por el contrario, un recorrido transversal por el texto normativo, desde las definiciones del artículo 3 hasta las prohibiciones del artículo 5 y la clasificación de sistemas de alto riesgo contenida en el Anexo III.

Desde el punto de vista terminológico, el RIA emplea una pluralidad de categorías para referirse a prácticas que, desde una perspectiva técnico-funcional, comparten el tratamiento automatizado de información biométrica mediante sistemas de inteligencia artificial. Entre ellas destacan la identificación biométrica (remota y no remota), la verificación o autenticación biométrica, la categorización biométrica y el reconocimiento de emociones. Cada una de estas categorías aparece asociada a consecuencias jurídicas diferenciadas, sin que el Reglamento explicite de forma sistemática los criterios materiales que justificarían tal diferenciación (Escajedo San-Epifanio, 2024).

(1) Una primera línea de fragmentación se observa en **la distinción entre identificación biométrica y verificación biométrica**. El RIA atribuye una especial gravedad regulatoria a la identificación biométrica, en particular cuando es remota y en tiempo real, mientras que la verificación o autenticación biométrica queda, con carácter general, fuera de las prohibiciones del artículo 5 y de la clasificación como sistema de alto riesgo. Esta diferenciación se apoya en criterios funcionales y contextuales, pero no va acompañada de una reflexión explícita sobre la naturaleza del dato tratado ni sobre la intensidad de las inferencias biométricas implicadas.

(b) Una segunda línea de fragmentación se produce entre **la identificación biométrica remota y la no remota**. Mientras que la primera ocupa una posición central en la arquitectura normativa del RIA, especialmente en relación con los espacios de acceso público y determinadas finalidades, la identificación biométrica no remota queda escasamente definida y, en la práctica, tiende a diluirse en categorías próximas a la verificación. El Reglamento no ofrece criterios claros para delimitar estos supuestos ni para valorar el impacto

específico de identificaciones uno-a-muchos realizadas fuera del marco de la identificación remota en tiempo real.

(c) Una dimensión adicional de especial relevancia en la arquitectura del RIA es **la distinción entre identificación biométrica en tiempo real e identificación biométrica en diferido**. El Reglamento asocia el mayor nivel de riesgo a los sistemas que operan en tiempo real, en la medida en que permiten la captación, el análisis y la producción de efectos de forma inmediata, reduciendo los márgenes de intervención humana y de corrección *ex ante*. Por el contrario, las modalidades de identificación en diferido —aunque potencialmente invasivas— quedan sometidas a un régimen normativo menos intenso, al entenderse que permiten un mayor control posterior del tratamiento y una evaluación más pausada de sus efectos. Esta diferenciación temporal desempeña un papel central en la delimitación de las prácticas prohibidas del artículo 5 y en la configuración del Anexo III, y refuerza la orientación del RIA hacia una concepción del riesgo centrada en la inmediatez de la intervención más que en la capacidad inferencial del sistema.

(d) Un cuarto foco de fragmentación se observa en el **tratamiento separado de la categorización biométrica y del reconocimiento de emociones**. El RIA define ambas prácticas como categorías autónomas y les asigna regímenes jurídicos dependientes del contexto de uso. En particular, el reconocimiento de emociones se prohíbe únicamente en determinados entornos —como el laboral y el educativo—, mientras que en otros contextos queda sometido a obligaciones más limitadas. Esta regulación contextual refuerza la separación entre identificación y otras formas de reconocimiento biométrico, sin ofrecer un marco común para evaluar su impacto material sobre los derechos fundamentales.

(e) Finalmente, el Reglamento **deja en una situación especialmente ambigua a los sistemas de cribado biométrico**, entendidos como aquellos que detectan o reconocen características, patrones o estados en personas captadas sin enrolamiento previo. Estas prácticas no encajan con claridad en las categorías centrales del RIA y su estatuto jurídico depende de interpretaciones indirectas o extensivas de distintas disposiciones, lo que contribuye a una visibilidad regulatoria limitada.

Cabe decir, por consiguiente, el RIA no configura el reconocimiento biométrico como una categoría jurídica coherente y unitaria, sino como un conjunto de prácticas fragmentadas, reguladas a través de etiquetas funcionales y contextuales con consecuencias normativas dispares. Esta fragmentación constituye un rasgo estructural del Reglamento y explica las dificultades para situar, dentro de su arquitectura, los tratamientos biométricos no singularizantes basados en inferencia continua. Sobre esta base se desarrollará, en los apartados siguientes, el análisis de la noción de riesgo que estructura el RIA y de las consecuencias de este enfoque para la protección efectiva de los derechos fundamentales.

§3.3.2. La noción de "riesgo" en el Reglamento de Inteligencia Artificial y su diferencia estructural respecto al riesgo en el RGPD: proyecciones en el reconocimiento biométrico no singularizante

(1) El Reglamento (UE) 2024/1689 de Inteligencia Artificial se articula sobre una noción de riesgo que difiere de manera estructural de la empleada por el Reglamento General de Protección de Datos, aun cuando ambos instrumentos recurren de forma reiterada a dicho concepto. La divergencia no es meramente terminológica, sino que

responde a racionalidades normativas distintas, que condicionan el modo en que cada Reglamento identifica, clasifica y gestiona los riesgos asociados al uso de tecnologías basadas en inteligencia artificial.

En el RGPD, el riesgo se concibe como una categoría material y relacional, vinculada a la probabilidad y gravedad de los efectos adversos que un tratamiento de datos personales puede producir sobre los derechos y libertades de las personas físicas. Esta concepción se apoya en una evaluación contextual que atiende a la naturaleza de los datos, a las finalidades perseguidas, al contexto del tratamiento y a sus efectos previsibles, sin partir de tipologías tecnológicas cerradas. Desde esta lógica, el riesgo puede derivar tanto de la identificación como de la inferencia, del perfilado o de la modulación del trato, incluso cuando no exista identificación singular ni decisiones automatizadas en sentido estricto.

El Reglamento de Inteligencia Artificial, por el contrario, construye el riesgo desde una lógica *ex ante*, tipificadora y fuertemente estructurada. El riesgo no se identifica primordialmente a partir de los efectos materiales del tratamiento sobre la persona concreta, sino de la adscripción del sistema a categorías normativas predeterminadas por el propio Reglamento. Esta clasificación se articula en torno a un esquema jerárquico —prácticas prohibidas, sistemas de alto riesgo, sistemas sujetos a obligaciones específicas y sistemas de riesgo limitado o mínimo— que responde a criterios funcionales y contextuales definidos con anterioridad al despliegue efectivo del sistema (Muñoz Vela, 2025; Eguiluz Castañeira, 2025).

(2) Desde esta perspectiva, el RIA opera mediante presunciones normativas de riesgo. Determinadas funcionalidades, contextos de uso o ámbitos materiales activan automáticamente regímenes jurídicos más o menos intensos, con independencia de que, en el caso concreto, los efectos materiales del sistema resulten más o menos lesivos. El análisis del riesgo se produce así en un plano abstracto y previo, propio de la gobernanza del mercado interior y de la regulación de la seguridad de productos, más que en un plano relacional centrado en la afectación efectiva de derechos fundamentales.

Esta lógica se manifiesta de forma particularmente clara en la clasificación de los sistemas de inteligencia artificial prohibidos y de alto riesgo. El RIA identifica como prácticas prohibidas aquellas que el legislador considera incompatibles con los valores de la Unión, y como sistemas de alto riesgo aquellos que se integran en ámbitos materiales especialmente sensibles o que cumplen determinados criterios funcionales recogidos, en particular, en el artículo 6 y en el Anexo III del Reglamento (Torres Carlos & Míguez Macho, 2024; González-Meneses García-Valdecasas, 2024). La pertenencia a estas categorías determina *ex ante* el estatuto jurídico del sistema, con independencia de un análisis detallado de sus efectos concretos.

La introducción de categorías adicionales, como los modelos de inteligencia artificial de uso general y los sistemas de riesgo limitado o mínimo, refuerza esta aproximación clasificatoria. En estos supuestos, el riesgo se evalúa en función del potencial sistémico del modelo, de su capacidad de reutilización transversal o de su inserción en determinados ecosistemas tecnológicos, y no tanto a partir de los usos específicos o de los impactos materiales que pueda producir en contextos concretos (Muñoz García, 2024a).

(3) Desde una perspectiva constitucional y democrática, este enfoque ha sido interpretado como un intento de dotar de previsibilidad y seguridad jurídica a la gobernanza de la inteligencia artificial, estableciendo límites claros y anticipados a determinadas prácticas. Sin embargo, esta misma estructura condiciona la capacidad

del Reglamento para captar riesgos que emergen de forma dinámica, contextual y acumulativa, especialmente en sistemas basados en inferencia continua y en modulación del entorno de interacción (Barrio Andrés, 2025).

La consecuencia de esta diferencia estructural es que el RIA tiende a identificar el riesgo a partir de la forma externa del sistema —su clasificación, su contexto de uso o su funcionalidad declarada— más que a partir de los efectos materiales que produce sobre la autonomía personal, la igualdad material o el control efectivo de la persona. Esta característica resulta especialmente relevante para el análisis de la biometría no singularizante, en la medida en que muchas de estas prácticas no encajan con claridad en las categorías de mayor riesgo del Reglamento, pese a su elevada capacidad inferencial.

Sobre esta base, el apartado siguiente examina cómo los criterios regulatorios utilizados por el RIA para valorar el riesgo biométrico —distancia, tiempo real, contexto de uso, participación activa o existencia de bases de datos de referencia— influyen en la visibilidad normativa de determinadas modalidades de reconocimiento biométrico no singularizante (§3.3.3).

§3.3.3. Criterios regulatorios utilizados por el RIA para la evaluación del riesgo biométrico

§3.3.4. Modalidades biométricas no singularizantes infra-valoradas en el RIA o situadas en un limbo regulatorio

(1) Una vez delimitada la noción de riesgo que estructura el Reglamento de Inteligencia Artificial (§3.3.2), resulta necesario identificar los criterios regulatorios concretos mediante los cuales el RIA clasifica y modula el riesgo asociado a las distintas modalidades de reconocimiento biométrico. El examen sistemático del texto del Reglamento pone de manifiesto que el legislador europeo no evalúa directamente la intensidad inferencial de los sistemas ni sus efectos materiales sobre las personas, sino que recurre a un conjunto de criterios funcionales y contextuales utilizados como indicadores normativos del riesgo.

> (a) Entre estos criterios destaca, en primer lugar, la distinción entre reconocimiento biométrico **remoto y no remoto**. El carácter remoto del tratamiento —entendido como la captación y el análisis de datos biométricos sin proximidad física ni interacción directa con la persona— opera como un elemento central en la atribución de riesgo, especialmente cuando se combina con el uso en espacios de acceso público. Esta configuración se asocia en el RIA a un mayor potencial de afectación de derechos fundamentales, no tanto por el contenido de la inferencia, sino por la amplitud y opacidad del tratamiento.
>
> (b) Un segundo criterio fundamental es **la dimensión temporal del reconocimiento biométrico**, en particular la distinción entre sistemas que operan en tiempo real y aquellos que lo hacen en diferido. El funcionamiento en tiempo real se utiliza como marcador de gravedad, en la medida en que permite la producción inmediata de efectos y reduce los márgenes de intervención humana y de corrección previa. Esta variable temporal desempeña un papel determinante tanto en la delimitación de las prácticas prohibidas del artículo 5 como en la configuración de los sistemas de alto riesgo del Anexo III, reforzando una concepción del riesgo centrada en la inmediatez de la intervención.

(c) El RIA atiende asimismo a **la participación activa o pasiva de la persona en el proceso biométrico**. La intervención voluntaria del sujeto —por ejemplo, al someterse a un proceso de verificación o autenticación— se considera un factor relevante a efectos de la calificación regulatoria del sistema. Este criterio aparece implícitamente vinculado a la expectativa de tratamiento y a la percepción de control individual, aun cuando dicha percepción no garantice, por sí misma, una menor intensidad de la inferencia ni una reducción efectiva del riesgo material.

(d) Otro criterio utilizado por el Reglamento es **la existencia de procesos de enrolamiento y de bases de datos de referencia**. Los sistemas que comparan datos biométricos captados en fresco con conjuntos estructurados de identidades preexistentes se distinguen normativamente de aquellos que operan sin enrolamiento singularizante o mediante modelos agregados. La presencia de bases de datos biométricas organizadas actúa así como un elemento relevante en la clasificación del riesgo, con independencia de la capacidad del sistema para generar inferencias situacionales no identificantes.

e) Finalmente, **el contexto de uso** desempeña un papel decisivo en la evaluación regulatoria del riesgo. El RIA intensifica las restricciones cuando el reconocimiento biométrico se despliega en ámbitos tradicionalmente asociados a relaciones de poder estructurales, como el laboral o el educativo, y adopta soluciones diferenciadas en función de si el uso se produce en espacios de acceso público, en contextos de seguridad o en entornos privados. El contexto opera, por tanto, como un criterio modulador que condiciona la aplicación de prohibiciones, obligaciones reforzadas o requisitos de transparencia.

(2) Desde una perspectiva de conjunto, estos criterios permiten al RIA estructurar una clasificación *ex ante* de las prácticas biométricas basada en rasgos externos del sistema y en escenarios de uso previamente definidos. El riesgo biométrico se evalúa así a partir de la configuración formal del tratamiento —distancia, tiempo real, participación, contexto, enrolamiento— y no de la capacidad inferencial del sistema ni de los efectos materiales que produce sobre la persona. Esta aproximación resulta coherente con la lógica tipificadora del Reglamento, pero plantea dificultades significativas para captar determinadas modalidades de biometría no singularizante basadas en inferencia continua.

Sobre esta base, el apartado siguiente (§3.3.4) analiza cómo la aplicación de estos criterios conduce a una infra-valoración estructural de determinadas prácticas biométricas no singularizantes, que quedan situadas en zonas de baja visibilidad regulatoria pese a su potencial de afectación de derechos fundamentales.

§3.3.5. El alcance real de las prohibiciones del artículo 5 RIA y su incapacidad para corregir la presunción de menor riesgo

(1) El artículo 5 del Reglamento (UE) 2024/1689 ocupa una posición central en la arquitectura política y simbólica del Reglamento de Inteligencia Artificial. Durante el proceso legislativo, este precepto fue presentado como el principal elemento diferenciador del RIA respecto de un modelo clásico de regulación de la inteligencia artificial basado exclusivamente en la lógica de la seguridad del producto y de la responsabilidad *ex post*. Las denominadas prácticas prohibidas pretendían proyectar la imagen de un Reglamento orientado no solo al mercado interior, sino también a la

protección directa de la persona frente a determinados usos considerados incompatibles con los valores fundamentales de la Unión.

En este sentido, el artículo 5 ha funcionado como el espacio normativo en el que el legislador europeo ha querido concentrar los llamados “límites éticos” del uso de la inteligencia artificial, introduciendo prohibiciones categóricas allí donde el riesgo se percibía como particularmente intenso o socialmente inaceptable. Esta función explicativa resulta esencial para comprender tanto su centralidad en el debate público como la atención que recibió durante la tramitación del Reglamento.

(2) Ahora bien, un análisis detallado de las prohibiciones recogidas en el artículo 5 pone de manifiesto que su alcance efectivo en relación con el reconocimiento biométrico es limitado y selectivo, y que no responde a una concepción unitaria del riesgo biométrico. Como se ha señalado en otro lugar (Escajedo San-Epifanio, 2024), el examen individualizado de cada una de las prohibiciones revela una regulación fragmentaria, centrada en supuestos simbólicamente cargados, pero poco sistemática desde el punto de vista de la protección frente a las distintas modalidades de tratamiento biométrico.

En particular, el artículo 5 concentra su atención en prácticas que se aproximan a formas explícitas de control, sanción o clasificación formal de personas, como el social scoring por parte de autoridades públicas o determinadas modalidades de identificación biométrica remota y en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho. Estas prohibiciones responden a un imaginario regulatorio fuertemente marcado por la preocupación frente al poder sancionador visible y frente a usos estatales intensivos de la inteligencia artificial.

Sin embargo, esta focalización deja fuera del núcleo prohibitivo un amplio conjunto de prácticas biométricas que, aun no orientadas a la identificación singularizante ni a la imposición de sanciones formales, presentan una elevada capacidad de afectación material de derechos fundamentales. En particular, el artículo 5 no aborda de manera general la inferencia biométrica continua, la categorización funcional ni el perfilado basado en señales corporales cuando estas prácticas se despliegan en contextos que en principio no son disciplinarios, como los entornos comerciales o de interacción digital cotidiana.

(3) La regulación del reconocimiento de emociones constituye un ejemplo ilustrativo de esta selectividad. El RIA prohíbe esta práctica únicamente en el ámbito laboral y educativo, reconociendo implícitamente el desequilibrio de poder existente en estos contextos, pero no extiende la prohibición a otros escenarios en los que la inferencia emocional puede utilizarse con fines persuasivos o de modulación del comportamiento. Del mismo modo, la prohibición de determinadas formas de categorización biométrica se limita a la inferencia de atributos expresamente protegidos, sin atender de manera general a la dinámica inferencial ni a los efectos acumulativos de la categorización no singularizante.

Desde esta perspectiva, el artículo 5 no puede ser interpretado como un régimen exhaustivo de contención del riesgo biométrico, sino como un instrumento selectivo, diseñado para marcar límites frente a determinados usos extremos o paradigmáticos. Su función principal no es ofrecer una protección integral frente a la biometría, sino establecer líneas rojas simbólicamente relevantes en torno a prácticas que el legislador considera especialmente problemáticas desde el punto de vista político y social.

La consecuencia es que el artículo 5 no corrige la infra-valoración del riesgo asociada a amplias modalidades de biometría no singularizante, ni proporciona un criterio general

para evaluar los efectos materiales de la inferencia biométrica sobre la autonomía personal, la igualdad material o el control efectivo por parte de la persona. Esta limitación no deslegitima el precepto, pero sí obliga a situarlo en su justa medida dentro del conjunto del Reglamento y a reconocer que la protección efectiva frente a estos riesgos depende, en gran medida, de la aplicación transversal del RGPD y de su lógica de gestión preventiva del riesgo.

§3.3.6. Consecuencia sistemática: subestimación del riesgo de la biometría no singularizante en sistemas de IA

(1) El análisis conjunto del tratamiento del reconocimiento biométrico en el Reglamento (UE) 2024/1689 permite identificar una consecuencia sistemática clara: el RIA subestima de manera estructural el riesgo asociado a la biometría no singularizante, en particular cuando esta se integra en sistemas de inteligencia artificial con capacidad inferencial continua y efectos moduladores sobre el comportamiento de las personas.

Esta subestimación no es accidental ni resulta de lagunas técnicas aisladas, sino que deriva directamente de la forma en que el Reglamento conceptualiza el riesgo. Como se ha mostrado en los apartados anteriores, el RIA articula su intervención a partir de una lógica tipificadora que utiliza la identificación singularizante, la sanción visible y los contextos disciplinarios clásicos como principales umbrales de gravedad. Allí donde estos elementos no concurren, el riesgo tiende a ser tratado como residual, contextual o asumible, aun cuando la capacidad inferencial del sistema y sus efectos materiales sobre los derechos fundamentales sean elevados, aunque sea por acumulación.

(2) El resultado es una asimetría regulatoria significativa. Las modalidades biométricas orientadas a la identificación unívoca de personas reciben una atención normativa intensa, mientras que las prácticas biométricas no singularizantes —basadas en categorización funcional, inferencia situacional o perfilado continuo— quedan sometidas a regímenes atenuados, fragmentarios o meramente contextuales. Esta asimetría no se corrige mediante el régimen de prácticas prohibidas del artículo 5, cuya función es selectiva y de marcado perfil simbólico, ni mediante la clasificación de sistemas de alto riesgo, diseñada en torno a usos tipificados y no a efectos materiales.

Desde una perspectiva jurídico-material, esta configuración resulta problemática porque desplaza el centro de gravedad del análisis desde los efectos reales del tratamiento hacia sus formas externas. El riesgo se evalúa prioritariamente en función de cómo se presenta el sistema —identificación sí/no, remoto sí/no, tiempo real sí/no— y no de lo que el sistema hace efectivamente: inferir estados personales, modular entornos de decisión y producir impactos acumulativos sobre la autonomía, la igualdad material o el control efectivo de la persona en contextos reales de interacción.

(3) La consecuencia no es un vacío normativo absoluto, sino una dependencia estructural del RGPD para la gestión efectiva de estos riesgos. Allí donde el RIA no activa prohibiciones ni regímenes reforzados, la tutela preventiva de los derechos fundamentales descansa, en la práctica, en la aplicación del RGPD, en particular a través del principio de responsabilidad proactiva, las evaluaciones de impacto y las obligaciones de protección de datos desde el diseño y por defecto. Esta dependencia no es coyuntural, sino consecuencia estructural de la distinta lógica regulatoria de ambos Reglamentos. Desde esta constatación se prepara el terreno para el análisis del apartado siguiente (§3.4), en el que se examina de manera específica la articulación entre el RGPD y el RIA respecto de la categorización y el perfilado biométrico no singularizante, y fundamenta la necesidad de una lectura coordinada con primacía funcional del primero en la gestión preventiva del riesgo.

§3.4. La categorización y el perfilado biométrico no singularizante en la articulación RGPD–RIA

El análisis precedente pone de manifiesto que la regulación de la biometría no singularizante mediante sistemas de inteligencia artificial se sitúa en una zona de fricción estructural entre el RGPD y el Reglamento (UE) 2024/1689 de Inteligencia Artificial. Esta fricción no deriva de una incompatibilidad normativa directa, sino de la distinta forma en que ambos instrumentos conceptualizan el riesgo y articulan sus mecanismos de tutela en relación con tratamientos biométricos de carácter inferencial.

El RIA construye su sistema de gobernanza a partir de categorías tipificadas de prácticas y contextos de uso, asignando consecuencias jurídicas en función de la adscripción del sistema a dichas categorías. Esta lógica permite intervenir *ex ante* sobre determinados usos considerados especialmente problemáticos, pero muestra limitaciones evidentes cuando se proyecta sobre prácticas biométricas no singularizantes basadas en inferencia continua, categorización funcional o perfilado situacional, cuya relevancia jurídica no se agota en la forma externa del sistema ni en su finalidad declarada.

Por el contrario, el RGPD no articula su intervención en torno a tipologías cerradas de tecnologías, sino a partir del tratamiento de datos personales y de los efectos materiales que dicho tratamiento puede producir sobre los derechos y libertades de las personas físicas. Esta estructura permite abordar jurídicamente prácticas biométricas que no culminan en la identificación singularizante, pero que individualizan funcionalmente a la persona, permiten inferir aspectos personales y condicionan el trato recibido mediante procesos automatizados integrados en arquitecturas de interacción continua.

§3.4.1. La insuficiencia del criterio identificante como eje de articulación normativa

La principal fuente de fricción entre ambos Reglamentos reside en la centralidad que el RIA otorga al carácter identificante del reconocimiento biométrico como criterio implícito de gravedad. Tal como se ha mostrado en §3.3, el diseño del RIA presupone que el riesgo se intensifica cuando el sistema permite identificar de manera unívoca a una persona física, y se atenúa cuando el tratamiento biométrico no persigue dicha finalidad o no se traduce en una intervención sancionadora visible.

Esta presuposición resulta insuficiente desde una perspectiva jurídico-material. La ausencia de identificación singularizante no impide que un tratamiento biométrico produzca efectos relevantes sobre la autonomía personal, la igualdad material o el control efectivo por parte de la persona, especialmente cuando se basa en inferencias continuas y se integra en arquitecturas de interacción adaptativa. Utilizar el criterio identificante como eje de articulación normativa conduce, así, a una evaluación incompleta del riesgo asociado a determinadas prácticas biométricas.

El RGPD, en cambio, no subordina la intensidad de las garantías a la identificación nominal de la persona, sino a la capacidad del tratamiento para afectar materialmente a sus derechos y libertades. Desde esta lógica, la categorización y el perfilado biométrico no singularizante constituyen formas de tratamiento plenamente relevantes, aun cuando no permitan identificar a la persona como individuo único ni generar decisiones automatizadas aislables.

§3.4.2. El perfilado biométrico como forma de tratamiento plenamente captada por el RGPD

La definición de perfilado contenida en el artículo 4.4 RGPD ofrece un encuadre normativo particularmente adecuado para abordar la biometría no singularizante. El perfilado se define como todo tratamiento automatizado destinado a evaluar aspectos personales de una persona física, sin exigir identificación singular ni la adopción de decisiones automatizadas en sentido estricto.

Desde esta perspectiva, el tratamiento automatizado de señales corporales con fines de inferencia, categorización o predicción encaja plenamente en el ámbito material del RGPD, con independencia de que el sistema se presente como identificación, verificación, reconocimiento de emociones o simple adaptación funcional. Lo jurídicamente relevante no es la etiqueta técnica utilizada, sino el hecho de que el tratamiento permita evaluar aspectos personales y modular el trato recibido en función de inferencias automatizadas.

Este encuadre permite captar de forma unitaria prácticas que el RIA fragmenta en categorías funcionales dispersas, y ofrece instrumentos jurídicos adecuados para su evaluación preventiva, en particular a través de los principios del artículo 5 RGPD, las evaluaciones de impacto y el principio de responsabilidad proactiva.

§3.4.3. La fragmentación del RIA y la invisibilización de la inferencia biométrica no singularizante

La técnica regulatoria del RIA, basada en la tipificación de prácticas y contextos de uso, tiende a disociar fenómenos que, desde el punto de vista técnico y funcional, comparten una misma lógica inferencial. La separación entre identificación, verificación, categorización biométrica y reconocimiento de emociones dificulta una evaluación coherente del riesgo cuando estas prácticas se articulan como partes de una misma arquitectura inferencial y operan de manera acumulativa sobre la persona.

Esta fragmentación no implica que el RIA sea inaplicable a la biometría no singularizante, pero sí que su intervención resulta parcial y dependiente de interpretaciones contextuales. En particular, el Reglamento no proporciona criterios generales para evaluar los efectos acumulativos de la inferencia biométrica ni su integración en procesos de modulación continua del entorno de interacción.

El RGPD, por su parte, al centrarse en los efectos del tratamiento y no en su clasificación técnica, permite superar esta fragmentación y evaluar de manera más adecuada el impacto material de la inferencia biométrica sobre los derechos fundamentales.

§3.4.4. Consecuencia normativa: necesidad de una lectura coordinada con primacía funcional del RGPD

La consecuencia de lo anterior no es una exclusión del RIA ni una subordinación jerárquica entre Reglamentos, sino la necesidad de una lectura coordinada en la que cada instrumento opere conforme a su lógica propia. En el ámbito específico de la biometría no singularizante, esta coordinación exige reconocer una primacía funcional del RGPD como marco de referencia para la identificación, evaluación y gestión preventiva del riesgo.

Ello implica que el hecho de que una práctica biométrica no singularizante no quede prohibida ni clasificada como de alto riesgo en el RIA no puede interpretarse como indicio de bajo riesgo desde la perspectiva de los derechos fundamentales. La evaluación jurídica debe realizarse conforme a los criterios del RGPD, atendiendo a la naturaleza del tratamiento, a su contexto, a sus finalidades y, especialmente, a sus efectos materiales sobre las personas.

Esta lectura coordinada permite evitar zonas de infra-protección normativa y garantiza que la gobernanza de la biometría no singularizante no dependa exclusivamente de categorías tipificadas, sino de una evaluación sustantiva del riesgo. Sobre esta base se justifica plenamente el paso al capítulo siguiente (§4), dedicado a la identificación y caracterización sistemática de los riesgos que estas prácticas plantean para los derechos y libertades fundamentales.

§4. IDENTIFICACIÓN Y CARACTERIZACIÓN DE RIESGOS PARA LOS DERECHOS Y LIBERTADES

§4.1. CONTEXTO DE RIESGO: DEL PARADIGMA DE LA IDENTIFICACIÓN HACIA LAS INFRAESTRUCTURAS DE INFLUENCIA

(1) El análisis desarrollado en las secciones precedentes permite afirmar que los tratamientos biométricos no singularizantes mediante sistemas de inteligencia artificial plantean riesgos específicos para los derechos y libertades fundamentales que no quedan plenamente captados por los criterios normativos centrados en la identificación singularizante. A partir de esta constatación, la presente sección se orienta a identificar y caracterizar de manera sistemática dichos riesgos, atendiendo a los efectos materiales que estos tratamientos pueden producir sobre las personas en contextos reales de interacción. Estos riesgos se manifiestan de manera especialmente intensa en prácticas ya analizadas, como la categorización biométrica funcional, la inferencia automatizada de estados emocionales o atencionales y el perfilado situacional integrado en entornos de interacción cotidiana.

El enfoque adoptado no parte de una clasificación abstracta de tecnologías ni de una enumeración formal de categorías jurídicas, sino de una aproximación material y funcional al riesgo. El análisis se centra en cómo determinadas arquitecturas biométricas inferenciales —basadas en la captación de información corporal, la generación de inferencias automatizadas y la modulación continua del entorno de interacción— pueden incidir de forma significativa en la autonomía personal, la igualdad material, la autodeterminación informativa y el control efectivo de la persona sobre el tratamiento que le concierne.

Este desplazamiento metodológico resulta coherente con la lógica del RGPD, que concibe el riesgo como una función de la probabilidad y gravedad de los efectos adversos sobre los derechos y libertades de las personas físicas, evaluados en función de la naturaleza, el contexto, las finalidades y los efectos del tratamiento. Desde esta perspectiva, la ausencia de identificación singularizante o de decisiones automatizadas aislables no excluye la existencia de riesgos elevados cuando el tratamiento opera de forma continua, opaca o acumulativa.

(2) En el caso de la biometría no singularizante, los riesgos no se manifiestan necesariamente en un único acto decisional ni en un momento claramente identificable, sino que tienden a desplegarse de forma progresiva y contextual. La persona puede verse observada, interpretada y categorizada de manera reiterada a partir de señales corporales que no puede dejar de emitir, sin ser consciente del alcance de las inferencias generadas ni de las consecuencias funcionales que estas producen sobre el entorno de interacción. Estos efectos no se traducen necesariamente en una decisión jurídica formal, pero sí en alteraciones relevantes de la posición de la persona, como el condicionamiento de las opciones disponibles, la intensificación de estímulos, el trato diferenciado no explícito o la reducción de los márgenes efectivos de autodeterminación. Este carácter difuso y acumulativo del riesgo dificulta su percepción individual y refuerza la necesidad de un análisis estructural.

En atención a ello, el análisis adopta una concepción amplia del riesgo, que incluye no solo los efectos jurídicos directos, sino también las afectaciones fácticas relevantes que inciden en la posición de la persona, en sus márgenes de autodeterminación y en su exposición a dinámicas de influencia, exclusión o discriminación. Esta concepción permite integrar riesgos que, aun no traducidos en decisiones formalmente imputables, pueden producir impactos sustantivos sobre los derechos fundamentales.

Sobre esta base, los apartados siguientes de la presente sección desarrollan una tipología analítica de los principales riesgos asociados a los tratamientos biométricos no singularizantes. En particular, se examinarán: los riesgos para la autonomía personal y la autodeterminación informativa (§4.2); los riesgos de discriminación y afectación de la igualdad material (§4.3); los riesgos derivados de la opacidad, la falta de explicabilidad y la dificultad de control efectivo (§4.4); y, finalmente, los riesgos estructurales asociados a la normalización de la inferencia biométrica en entornos de interacción cotidiana (§4.5). Este análisis no pretende agotar todas las posibles manifestaciones del riesgo, sino ofrecer un marco sistemático dentro de la sección 4 que permita evaluar de forma preventiva la compatibilidad de estos tratamientos con los derechos y libertades fundamentales, y que sirva de base para la aplicación de los instrumentos jurídicos de gestión del riesgo examinados en las secciones posteriores del trabajo.

§4.2. AUTONOMÍA PERSONAL Y FORMACIÓN DE LA VOLUNTAD

(1) Uno de los riesgos más relevantes asociados a los tratamientos biométricos no singularizantes mediante sistemas de inteligencia artificial no consiste en una supresión directa o inmediata de la autonomía personal, sino en la creación de condiciones estructurales que favorecen formas de heterodirección progresiva del comportamiento. Estos riesgos no se manifiestan, por regla general, a través de decisiones jurídicas formales ni de actos singulares fácilmente identificables, sino mediante la modulación continua del entorno de interacción a partir de inferencias automatizadas extraídas de señales corporales.

Desde una perspectiva jurídico-material, la autonomía personal no se identifica exclusivamente con la ausencia de coacción directa o con la posibilidad formal de elegir entre varias opciones, sino con la capacidad efectiva de la persona para formar, mantener y revisar sus propias decisiones en un marco de opciones significativas que no esté estructuralmente sesgado en su contra. En este sentido, los tratamientos biométricos no singularizantes pueden afectar a la autonomía no porque sustituyan la voluntad de la persona, sino porque reconfiguran de manera adaptativa el entorno decisional en el que dicha voluntad se ejerce, apoyándose en inferencias relativas a estados emocionales, atencionales o disposiciones conductuales que la persona no controla ni puede anticipar (Hildebrandt, 2020; Wachter & Mittelstadt, 2019).

(2) En este contexto, el término heterodirección se emplea para describir la orientación del comportamiento de la persona desde fuera, no mediante órdenes, sanciones o decisiones formalmente impuestas, sino a través de la configuración estratégica del entorno, de los estímulos y de las opciones disponibles. En los sistemas biométricos no singularizantes, esta heterodirección adopta una forma específicamente inferencial: el sistema ajusta contenidos, ritmos de interacción, prioridades u oportunidades sobre la base de estimaciones probabilísticas acerca del estado interno de la persona, generadas a partir de señales corporales captadas de forma continua o cuasi continua.

Este tipo de afectación resulta especialmente problemática cuando la inferencia biométrica se integra en arquitecturas de interacción adaptativa. A través de la captación reiterada del cuerpo en funcionamiento, el sistema no se limita a reaccionar ante conductas observables, sino que anticipa y condiciona el comportamiento futuro, configurando un entorno que responde más a inferencias sobre lo que la persona es o hará que a decisiones explícitas adoptadas por ella. La autonomía no desaparece, pero se ve progresivamente constreñida por un marco decisional preconfigurado cuya lógica permanece opaca (Rouvroy & Berns, 2013).

(3) La estrecha vinculación de estos tratamientos con el cuerpo como fuente primaria de datos intensifica el riesgo. A diferencia de otras formas de perfilado basadas en elecciones declaradas o en historiales de comportamiento, la biometría no singularizante se nutre de señales corporales inevitables, que la persona no puede dejar de emitir sin excluirse del entorno de interacción. Esta inevitabilidad reduce los márgenes reales de oposición, retirada o desconexión, y refuerza la asimetría estructural entre el responsable del tratamiento y la persona afectada (Simitis, 2011).

Desde esta perspectiva, la afectación de la autonomía personal se proyecta directamente sobre la autodeterminación informativa. Cuando las inferencias biométricas se generan de forma continua y se utilizan para modular el entorno de interacción, la persona pierde capacidad efectiva para comprender qué información se está produciendo sobre ella, con qué alcance y con qué consecuencias. La autodeterminación informativa no se ve erosionada únicamente por déficits de transparencia formal, sino por la imposibilidad práctica de anticipar, controlar o impugnar las inferencias que el sistema está en condiciones de generar a partir del cuerpo en funcionamiento (Wachter, 2018).

(4) En este punto resulta especialmente pertinente la noción de libertad cognitiva, entendida como el derecho de la persona a mantener un espacio de formación de la voluntad y de los procesos mentales libre de interferencias indebidas, manipulaciones encubiertas o condicionamientos inferenciales no controlados. Tal como se ha señalado en otro lugar (Escajedo San-Epifanio, 2025), la expansión de sistemas capaces de inferir y modular estados internos a partir del cuerpo plantea riesgos específicos para esta dimensión de la libertad, en la medida en que desplaza el control desde las decisiones externas hacia los procesos internos de atención, emoción y disposición conductual.

La amenaza para la libertad cognitiva no reside en la mera existencia de inferencias automatizadas, sino en su integración estructural en entornos de interacción cotidiana, donde operan de forma persistente, personalizada y poco perceptible. En estos contextos, la persona puede mantener una apariencia de autodirección mientras el sistema ajusta continuamente el entorno en función de inferencias que ella no conoce ni puede cuestionar de manera efectiva. Esta tensión entre autonomía formal y autonomía material constituye uno de los principales riesgos asociados a la biometría no singularizante.

(5) Desde la lógica del RGPD, estos riesgos no pueden evaluarse exclusivamente a partir de la existencia de consentimiento formal, de decisiones automatizadas aislables o de finalidades declaradas. Exigen una aproximación preventiva que atienda a cómo el tratamiento configura de facto el espacio de decisiones de la persona, y a si dicha configuración resulta compatible con los derechos a la autonomía personal, a la autodeterminación informativa y a la libertad cognitiva. El análisis de este riesgo permite comprender por qué determinados tratamientos biométricos no singularizantes, aun cuando no persigan la identificación singular ni produzcan decisiones automatizadas en sentido estricto, pueden afectar de manera significativa a dimensiones nucleares de la libertad individual.

§4.3. IGUALDAD MATERIAL Y PERFILADO POR VULNERABILIDAD SITUACIONAL

(1) Los tratamientos biométricos no singularizantes mediante sistemas de inteligencia artificial plantean riesgos específicos para la igualdad material y el principio de no discriminación, derivados de la forma en que las inferencias biométricas se construyen, se aplican y se integran funcionalmente en procesos de categorización y perfilado. Estos riesgos no dependen necesariamente de una intención discriminatoria

ni de la utilización explícita de categorías protegidas, sino de los efectos diferenciales que el tratamiento puede producir sobre personas o grupos en función de atributos corporales, conductuales o situacionales.

Desde una perspectiva jurídico-material, la discriminación asociada a la biometría no singularizante se manifiesta de forma indirecta o estructural. El sistema no asigna formalmente una identidad ni adopta decisiones explícitas basadas en categorías clásicas, pero sí clasifica, prioriza o modula el trato en función de inferencias biométricas que correlacionan de manera sistemática con factores socialmente relevantes, como la edad, el género, la discapacidad, el origen étnico, la condición socioeconómica o determinadas condiciones de vulnerabilidad.

(2) Este riesgo se intensifica cuando las inferencias biométricas se integran en arquitecturas de categorización funcional. A través de la asignación automatizada a categorías operativas —por ejemplo, perfiles de atención, estados emocionales, niveles de estrés, fiabilidad conductual o predisposición a determinados comportamientos—, el sistema produce efectos diferenciados sobre las personas sin necesidad de recurrir a categorías protegidas en sentido formal. La discriminación no se articula como exclusión directa, sino como variación sistemática del trato recibido.

La utilización de señales corporales como base del tratamiento introduce, además, un vector específico de desigualdad. Determinadas características corporales o conductuales pueden ser interpretadas de manera distinta en función del grupo al que pertenece la persona, reproduciendo o amplificando sesgos preexistentes. Así, estados como el nerviosismo, la fatiga, la expresividad facial o determinados patrones de movimiento pueden ser inferidos y valorados de forma desigual, generando clasificaciones sistemáticamente desfavorables para determinados colectivos.

(3) Desde el punto de vista del RGPD, estos efectos se sitúan plenamente dentro del ámbito de riesgo identificado en el considerando 75, que menciona expresamente la discriminación, la exclusión social y el trato desigual como consecuencias adversas del tratamiento de datos personales. La ausencia de identificación singularizante o de decisiones automatizadas aislables no elimina este riesgo, en la medida en que la igualdad material puede verse afectada por la acumulación de micro-decisiones funcionales que configuran el entorno de interacción de manera diferenciada.

La dificultad de detectar y corregir estos efectos discriminatorios constituye un elemento adicional de riesgo. En los tratamientos biométricos no singularizantes, la discriminación no se manifiesta necesariamente en un resultado claramente imputable, sino en patrones de trato que emergen a lo largo del tiempo y que pueden pasar desapercibidos tanto para las personas afectadas como para los propios responsables del tratamiento. La opacidad de las inferencias y la complejidad de los modelos dificultan la identificación de sesgos y la atribución de responsabilidad.

(4) Este carácter estructural de la discriminación plantea desafíos específicos para los mecanismos clásicos de tutela. La persona afectada puede no ser consciente de que está siendo tratada de forma diferente, ni disponer de elementos suficientes para impugnar el tratamiento o acreditar un perjuicio concreto. La discriminación se produce, así, sin necesidad de una decisión singular claramente identificable, lo que refuerza la necesidad de una aproximación preventiva y sistémica al riesgo.

En este contexto, los tratamientos biométricos no singularizantes pueden generar formas de desigualdad material especialmente persistentes, en la medida en que las inferencias se actualizan y reutilizan de manera continua, retroalimentando perfiles y categorías funcionales. La repetición de inferencias desfavorables puede consolidar

trayectorias diferenciadas de acceso a oportunidades, contenidos o servicios, sin que exista un punto claro de intervención jurídica *ex post*.

Desde la lógica del RGPD, estos riesgos exigen una evaluación específica de la proporcionalidad del tratamiento y de sus efectos diferenciales, así como la adopción de medidas de mitigación orientadas a prevenir sesgos, corregir impactos desiguales y garantizar un nivel adecuado de protección de la igualdad material. La gestión del riesgo de discriminación no puede limitarse a la exclusión formal de categorías sensibles, sino que debe atender a las correlaciones inferenciales y a los efectos acumulativos del tratamiento. El análisis de los riesgos de discriminación asociados a la biometría no singularizante pone de relieve que la igualdad material puede verse comprometida incluso en ausencia de identificación singular o de decisiones automatizadas formales.

§4.4. TRANSPARENCIA, AUTODETERMINACIÓN INFORMATIVA Y LÍMITES ESTRUCTURALES DEL CONSENTIMIENTO

(1) Los tratamientos biométricos no singularizantes mediante sistemas de inteligencia artificial presentan riesgos específicos asociados a la opacidad de su funcionamiento, a la limitada explicabilidad de las inferencias generadas y a la dificultad de ejercer un control efectivo por parte de las personas afectadas. Estos riesgos no constituyen meras deficiencias técnicas o procedimentales, sino elementos estructurales que condicionan la efectividad de las garantías jurídicas previstas en el RGPD y, de forma complementaria, en el Reglamento (UE) 2024/1689 de Inteligencia Artificial.

Desde la perspectiva del RGPD, la opacidad del tratamiento entra en tensión directa con los principios de licitud, lealtad y transparencia (art. 5.1.a), así como con las obligaciones de información y transparencia de los artículos 12 a 15. No obstante, en los tratamientos biométricos no singularizantes la transparencia no se ve comprometida únicamente por déficits informativos formales, sino por la propia arquitectura inferencial del sistema, que dificulta identificar qué señales corporales resultan relevantes, cómo se combinan y de qué modo influyen en la modulación del entorno de interacción.

(2) Ha de recordarse que las inferencias biométricas no singularizantes se generan habitualmente a partir de modelos estadísticos complejos, entrenados sobre grandes volúmenes de datos y actualizados de forma dinámica. Esta complejidad técnica dificulta tanto la comprensión por parte de la persona interesada como la reconstrucción *ex post* del tratamiento, incluso para el propio responsable. A diferencia de las decisiones automatizadas aislables, estos sistemas operan de forma continua y contextual, produciendo ajustes progresivos del entorno de interacción que no se traducen en un resultado único claramente identificable.

La falta de explicabilidad se manifiesta, así, como una imposibilidad práctica de ofrecer una explicación significativa del tratamiento en su conjunto, y no únicamente de una inferencia concreta. En este sentido, la exigencia de transparencia no puede entenderse como un deber de revelación exhaustiva del modelo, sino como la obligación de garantizar un nivel de comprensión suficiente para que la persona pueda entender cómo y por qué el tratamiento incide en su posición. Tal como ha señalado la doctrina, una concepción puramente formal de la transparencia corre el riesgo de vaciar de contenido los derechos informativos cuando se proyecta sobre sistemas complejos y dinámicos (Sanz, 2018; Calaza López, 2025).

(3) Esta problemática afecta directamente a la efectividad de los derechos de acceso, oposición y limitación del tratamiento (arts. 15, 21 y 18 RGPD), así como al

alcance material del artículo 22. Aunque muchos tratamientos biométricos no singularizantes no culminan en decisiones automatizadas en sentido estricto, la modulación continua del entorno de interacción puede producir efectos funcionalmente equivalentes, sin activar formalmente las garantías reforzadas previstas para dichos supuestos.

La dificultad de control efectivo se ve agravada por el carácter inevitable de la captación biométrica en numerosos entornos de interacción. Cuando el tratamiento se basa en señales corporales que la persona no puede dejar de emitir sin abandonar el servicio o el espacio, las opciones reales de control se reducen sustancialmente. Esta situación limita la eficacia práctica de los mecanismos de autodeterminación informativa y refuerza la asimetría estructural entre el responsable del tratamiento y la persona afectada.

(4) Desde una perspectiva jurídico-material, la opacidad y la falta de control no constituyen riesgos autónomos desvinculados de otros impactos, sino factores amplificadores de los riesgos analizados en los apartados anteriores. La imposibilidad de comprender, cuestionar o corregir las inferencias biométricas incrementa la probabilidad de que dinámicas de heterodirección (§4.2) o de trato diferenciado (§4.3) se consoliden de forma persistente y difícilmente reversible.

En este punto resulta relevante la aportación del Reglamento de Inteligencia Artificial, que introduce obligaciones específicas de transparencia para determinados sistemas de IA. El artículo 50 RIA impone deberes informativos a proveedores y responsables del despliegue en relación con sistemas que interactúan con personas físicas o que generan contenidos o inferencias susceptibles de afectar a su percepción o comportamiento. No obstante, estas obligaciones operan de forma sectorial y complementaria, y no sustituyen las exigencias materiales de transparencia y control derivadas del RGPD. Como ha señalado la doctrina, el artículo 50 RIA no construye un régimen general de explicabilidad, sino un conjunto de obligaciones mínimas orientadas a reforzar la visibilidad del uso de IA en determinados contextos (Bueno de Mata, 2024).

(5) Desde la lógica del RGPD, estos riesgos exigen una aplicación reforzada de los principios de protección de datos desde el diseño y por defecto (art. 25), orientada a limitar la opacidad estructural del sistema y a facilitar mecanismos efectivos de comprensión, supervisión y control. La evaluación del riesgo no puede detenerse en la licitud formal del tratamiento, sino que debe atender a si el diseño del sistema permite un ejercicio real y no meramente teórico de los derechos de la persona.

El análisis de los riesgos derivados de la opacidad, la falta de explicabilidad y la dificultad de control efectivo ponen de relieve que, en los tratamientos biométricos no singularizantes, la tutela de los derechos fundamentales depende de la posibilidad real de comprender y controlar cómo se configura el entorno de interacción.

§4.5. Normalización del riesgo, dimensión sistémica y debilitamiento de la tutela judicial efectiva

(1) La generalización de tratamientos biométricos no singularizantes mediante sistemas de inteligencia artificial en entornos de interacción cotidiana plantea riesgos estructurales que trascienden la afectación individual de derechos concretos y se proyectan sobre el funcionamiento del sistema de garantías propio del Estado de Derecho. Estos riesgos no se manifiestan necesariamente en una vulneración puntual identificable, sino en la alteración progresiva de las condiciones materiales en las que

los derechos pueden ser ejercidos, controlados y, en su caso, tutelados judicialmente (Rouvroy & Berns, 2013; Hildebrandt, 2020).

La integración estable de inferencias biométricas en procesos ordinarios de interacción —comerciales, administrativos, laborales o de acceso a servicios— produce un desplazamiento del centro de gravedad del poder decisional hacia fases técnicas previas, en las que se configuran categorías, perfiles y modulaciones del entorno sin intervención humana directa ni contraste contradictorio. Esta normalización reduce la visibilidad jurídica del tratamiento y dificulta la identificación de un acto o decisión concreta susceptible de impugnación, aun cuando los efectos producidos resulten jurídicamente relevantes (Wachter & Mittelstadt, 2019).

(2) Desde esta perspectiva, el riesgo no consiste únicamente en la producción de decisiones automatizadas injustas o erróneas, sino en la creación de entornos decisionales preconfigurados, que condicionan de forma persistente la posición de la persona sin generar un "momento decisional" claramente identificable. La afectación se produce a través de una acumulación de micro-ajustes funcionales —priorizaciones, exclusiones, modulaciones del acceso o del trato— que no cristalizan en una resolución formal, pero que inciden de manera continuada en la experiencia jurídica y fáctica de la persona.

Esta dinámica tiene consecuencias directas sobre el derecho a la tutela judicial efectiva, entendido no solo como acceso formal a los tribunales, sino como la posibilidad real de conocer, comprender y controvertir los elementos que condicionan la posición jurídica o material de la persona. Cuando los efectos del tratamiento biométrico no singularizante no se traducen en una decisión explícita imputable, la activación de los mecanismos clásicos de tutela se ve seriamente dificultada, tanto desde la perspectiva probatoria como desde la reconstrucción del funcionamiento real del sistema (Larrosa Ibáñez, 2025).

(3) La afectación de la tutela judicial efectiva se produce, así, de manera indirecta pero estructural. La persona puede experimentar consecuencias desfavorables reiteradas sin disponer de un acto formal frente al que articular una reclamación, y los órganos jurisdiccionales pueden carecer de elementos suficientes para evaluar la relevancia jurídica de inferencias distribuidas, opacas y técnicamente complejas. Esta situación erosiona las condiciones materiales de contradicción, defensa y control judicial que caracterizan al Estado de Derecho (Faggiani, 2024).

La normalización de la inferencia biométrica contribuye, además, a una progresiva naturalización de los efectos del sistema, que pasan a percibirse como rasgos neutrales del entorno y no como resultados de un tratamiento susceptible de control jurídico. Esta naturalización reduce la propensión a cuestionar el funcionamiento del sistema y desplaza la carga del control hacia fases técnicas alejadas tanto de la persona afectada como del escrutinio judicial efectivo (Simitis, 2011).

(4) Desde la lógica del Derecho de la Unión, estos riesgos ponen de relieve que la tutela judicial efectiva puede verse comprometida sin necesidad de una vulneración directa e inmediata, como consecuencia de la acumulación de prácticas inferenciales difíciles de identificar, explicar y reconstruir *ex post*. La efectividad de las garantías no depende únicamente de la licitud formal del tratamiento, sino de que el diseño del sistema permita identificar sus efectos, atribuir responsabilidades y activar mecanismos de control jurídico cuando dichos efectos resultan relevantes (Hildebrandt, 2020; Wachter & Mittelstadt, 2019).

El análisis de los riesgos estructurales asociados a la normalización de la inferencia biométrica no singularizante permite comprender que la tutela judicial efectiva puede verse debilitada no por una decisión concreta, sino por la configuración sistémica del entorno decisional. Esta constatación refuerza la necesidad de una gestión preventiva del riesgo, orientada a limitar *ex ante* la integración de inferencias biométricas no singularizantes en contextos donde sus efectos pueden incidir de forma significativa en los derechos y libertades fundamentales.

Con este apartado se completa el análisis de los principales riesgos asociados a los tratamientos biométricos no singularizantes. Sobre esta base, la sección siguiente (§5) se orienta a examinar los instrumentos jurídicos disponibles para la gestión preventiva de estos riesgos, con especial atención al principio de responsabilidad proactiva, a las evaluaciones de impacto y a las decisiones de diseño y gobernanza del tratamiento.

§5. EVALUACIÓN DE RIESGOS RGPD Y APLICACIÓN DE LA RESPONSABILIDAD PROACTIVA

§5.1. PLANTEAMIENTO GENERAL DE LOS INSTRUMENTOS JURÍDICOS DE GESTIÓN PREVENTIVA DEL RIESGO EN LOS TRATAMIENTOS BIOMÉTRICOS NO SINGULARIZANTES

(1) El análisis de los riesgos desarrollado en la sección anterior pone de manifiesto que los tratamientos biométricos no singularizantes mediante sistemas de inteligencia artificial plantean afectaciones potenciales relevantes para los derechos y libertades fundamentales que no pueden ser abordadas de manera adecuada a través de mecanismos de control exclusivamente reactivos o *ex post*. La naturaleza inferencial, continua y acumulativa de estos tratamientos exige, por el contrario, una aproximación jurídica orientada a la gestión preventiva del riesgo.

En el Derecho de la Unión, esta lógica preventiva encuentra su principal anclaje en el Reglamento General de Protección de Datos, cuya arquitectura se articula en torno a la identificación anticipada de riesgos, la adopción de garantías *ex ante* y la atribución de responsabilidades claras a los sujetos que deciden y controlan el tratamiento. Frente a modelos centrados en la reparación posterior del daño, el RGPD desplaza el foco hacia la prevención de afectaciones materiales de derechos antes de que estas se consoliden de forma estructural.

(2) Esta orientación resulta especialmente pertinente en el caso de la biometría no singularizante. Tal como se ha mostrado en la sección 4, los riesgos asociados a la heterodirección inferencial, a la discriminación indirecta, a la opacidad y a la erosión de la tutela judicial efectiva no se manifiestan necesariamente en decisiones aislables ni en momentos claramente identificables. Se trata de riesgos que emergen de la configuración misma de la arquitectura del sistema y de su integración en entornos de interacción cotidiana.

Desde esta perspectiva, la gestión jurídica del riesgo no puede limitarse a verificar la licitud formal del tratamiento ni a reaccionar ante infracciones ya producidas. Exige intervenir sobre las condiciones de diseño, de despliegue y de gobernanza del sistema, de modo que se reduzca *ex ante* la probabilidad y la gravedad de los impactos adversos sobre los derechos fundamentales.

(3) El RGPD proporciona un conjunto de instrumentos específicamente orientados a esta finalidad. Entre ellos destacan, de manera central, el principio de responsabilidad proactiva, las evaluaciones de impacto relativas a la protección de datos, las obligaciones de protección de datos desde el diseño y por defecto, y los deberes de documentación, supervisión y control interno. Estos instrumentos no operan de forma aislada, sino como un sistema integrado de garantías preventivas que debe aplicarse atendiendo a la naturaleza, el contexto, las finalidades y los efectos del tratamiento.

La aplicación de estos instrumentos adquiere una relevancia reforzada cuando el tratamiento se basa en inferencias biométricas no singularizantes. En estos supuestos, la identificación del riesgo no puede descansar exclusivamente en categorías normativas predefinidas ni en la ausencia de identificación singular, sino que debe atender a la capacidad real del sistema para modular el entorno de interacción, producir efectos acumulativos y generar asimetrías estructurales difíciles de corregir *ex post*.

La sección 5 se orienta, por tanto, a examinar de forma sistemática los principales instrumentos jurídicos disponibles para la gestión preventiva de los riesgos asociados a la biometría no singularizante. En particular, se analizará el alcance del principio de responsabilidad proactiva (§5.2), el papel central de las evaluaciones de impacto (§5.3),

la función de las obligaciones de protección de datos desde el diseño y por defecto (§5.4) y los mecanismos de supervisión y control institucional (§5.5), prestando especial atención a su capacidad para responder a los riesgos identificados en la sección anterior.

§5.2. CRITERIOS PARA LA IDENTIFICACIÓN DEL RIESGO ELEVADO EN TRATAMIENTOS BIOMÉTRICOS NO IDENTIFICANTES

(1) (1) El RGPD no establece un catálogo cerrado de tratamientos prohibidos o permitidos, sino que articula un modelo de gestión preventiva del riesgo para los derechos y libertades de las personas físicas, basado en la probabilidad y gravedad de los impactos adversos derivados del tratamiento (considerando 75 RGPD). En este marco, la identificación del riesgo elevado no depende de la calificación formal del dato ni de la tecnología empleada de manera aislada, sino de una evaluación contextual y material que atienda a la naturaleza, el alcance, el contexto y las finalidades del tratamiento (art. 35.1 RGPD; Gellert, 2021).

En los tratamientos biométricos no identificantes mediante inteligencia artificial, esta lógica exige desplazar el análisis desde el criterio tradicional de la identificación singularizante hacia los efectos materiales derivados del tratamiento inferencial de información corporal. Tal como se ha argumentado en la sección anterior (§4), estos tratamientos pueden generar riesgos elevados aun cuando no persigan la identificación única de la persona ni culminen en decisiones automatizadas en sentido estricto.

(2) Desde esta perspectiva, la ausencia de finalidad identificante no constituye un criterio suficiente para descartar la concurrencia de riesgo elevado. Por el contrario, cuando el tratamiento se apoya en la captación y análisis inferencial de señales corporales, la evaluación del riesgo debe realizarse con un estándar reforzado, atendiendo a la intensidad, continuidad y efectos del tratamiento sobre la persona, con independencia de su eventual calificación conforme al Reglamento de Inteligencia Artificial.

Las orientaciones del antiguo Grupo de Trabajo del Artículo 29, posteriormente asumidas por el Comité Europeo de Protección de Datos, identifican una serie de factores indicativos de alto riesgo —evaluación sistemática de aspectos personales, uso de tecnologías innovadoras, tratamiento continuo o a gran escala, dificultad de ejercicio efectivo de derechos— que resultan plenamente pertinentes en este ámbito (Article 29 Working Party, 2017; EDPB, 2018; Quelle, 2018).

A partir de estos criterios y del análisis desarrollado en este trabajo, pueden identificarse una serie de indicadores materiales de riesgo elevado en los tratamientos biométricos no identificantes, cuya concurrencia —individual o acumulativa— debe activar una evaluación reforzada conforme al RGPD:

> (a) Tratamiento inferencial de información corporal. Existe un indicio cualificado de riesgo elevado cuando el tratamiento permite inferir, directa o indirectamente, estados emocionales, atencionales, cognitivos o conductuales a partir de señales corporales o cuasi corporales. La naturaleza corporal de la información tratada intensifica la afectación potencial de la vida privada y de la autodeterminación personal, con independencia de que la inferencia sea probabilística o contextual (§4.2).
>
> (b) Capacidad de modulación del entorno de decisión. El riesgo se incrementa cuando las inferencias biométricas se utilizan para adaptar,

reorganizar o modular dinámicamente el entorno de interacción de la persona —orden de opciones, fricciones, estímulos, ritmo decisional— con el fin de influir sobre su conducta. En estos supuestos, el tratamiento no se limita a describir, sino que interviene activamente en las condiciones materiales de formación de la voluntad (§4.1 y §4.2).

(c) Explotación de vulnerabilidad situacional. La identificación y utilización funcional de estados transitorios de mayor susceptibilidad —fatiga, estrés, impulsividad, sobrecarga cognitiva— constituye un factor autónomo de riesgo elevado. El perfilado por vulnerabilidad situacional puede generar efectos materiales de desigualdad y presión algorítmica difícilmente perceptibles, pero jurídicamente relevantes (§4.3).

(d) Continuidad temporal o integración estructural del tratamiento. La captación continua o cuasi continua de señales corporales, así como la integración del tratamiento en servicios de uso cotidiano, incrementan de forma significativa la probabilidad y gravedad del impacto. La repetición de micro-intervenciones inferenciales produce efectos acumulativos que no pueden evaluarse adecuadamente desde una lógica puntual (§4.5).

(e) Opacidad funcional y déficit de trazabilidad. Cuando el funcionamiento del sistema dificulta la comprensión, reconstrucción o auditoría de las inferencias generadas y de sus efectos, se produce un debilitamiento estructural del control por parte de la persona interesada y de la tutela jurídica efectiva. Esta opacidad constituye un factor de riesgo autónomo y no un mero defecto técnico (§4.4 y §4.5).

(f) Asimetrías estructurales de poder. El riesgo se ve agravado cuando el tratamiento se despliega en contextos caracterizados por dependencia funcional o desequilibrios significativos entre el responsable del tratamiento y la persona afectada, como ocurre en plataformas digitales de uso generalizado, entornos de consumo o servicios esenciales (§4.3).

(3) Estos criterios no constituyen una lista cerrada ni deben interpretarse como requisitos cumulativos en sentido estricto. Su función es ofrecer un marco jurídico-material de apreciación del riesgo elevado, que permita identificar aquellos tratamientos biométricos no identificantes en los que la probabilidad y la gravedad de los efectos adversos justifican la activación de las obligaciones preventivas reforzadas del RGPD, en particular la realización de una evaluación de impacto conforme al artículo 35.

Desde esta óptica, la identificación del riesgo elevado no puede resolverse mediante una comprobación formal del encaje del tratamiento en las categorías del Reglamento de Inteligencia Artificial, sino que exige una evaluación autónoma conforme al RGPD, centrada en los efectos reales del tratamiento sobre los derechos y libertades de las personas físicas. Sobre esta base se justifica la centralidad de la EIPD como instrumento de gobernanza del tratamiento, que se desarrolla en el apartado siguiente (§5.3).

§5.3. Procedencia y alcance de las evaluaciones de impacto en protección de datos (EIPD)

(1) La evaluación de impacto relativa a la protección de datos constituye el instrumento central del Reglamento (UE) 2016/679 para la gestión preventiva del riesgo, y adquiere una relevancia estructural en los tratamientos biométricos no identificantes basados en sistemas de inteligencia artificial. Conforme al artículo 35 RGPD, la EIPD

resulta exigible cuando un tipo de tratamiento, en particular si utiliza nuevas tecnologías, puede entrañar un alto riesgo para los derechos y libertades de las personas físicas, atendiendo a su naturaleza, alcance, contexto y finalidades.

En los tratamientos analizados en este trabajo, la procedencia de la EIPD no puede evaluarse a partir de criterios formales, como la ausencia de identificación singularizante, la inexistencia de enrolamiento biométrico clásico o la inaplicabilidad del artículo 22 RGPD. El riesgo relevante, a efectos del Reglamento, no deriva de la finalidad identificante, sino de la utilización inferencial de información corporal y de sus efectos materiales sobre la autonomía personal, la igualdad material, la autodeterminación informativa y la efectividad de la tutela de derechos fundamentales (§§4 y 5.1).

Tal como han puesto de relieve las directrices del antiguo Grupo de Trabajo del Artículo 29 y del Comité Europeo de Protección de Datos, la concurrencia de determinados factores —evaluación sistemática de aspectos personales, uso de tecnologías innovadoras, tratamiento continuo o a gran escala, dificultad de ejercicio efectivo de derechos— constituye un indicio cualificado de alto riesgo que activa la obligación de realizar una EIPD. En los tratamientos biométricos no identificantes basados en inferencias continuas o en tiempo real, estos factores suelen concurrir de manera acumulativa y estructural (Article 29 Working Party, 2017; EDPB, 2018).

(2) Desde esta perspectiva, la EIPD debe considerarse jurídicamente exigible, como regla general, cuando el tratamiento: a) implique la captación y el tratamiento inferencial de señales corporales o cuasi corporales; b) permita inferir estados emocionales, atencionales, cognitivos o conductuales; c) se integre de forma estructural en entornos de interacción cotidiana; d) opere de manera continua, adaptativa o ambiental ;e) presente opacidad funcional relevante o dificulte el ejercicio efectivo de derechos.

En estos supuestos, la EIPD no puede concebirse como un trámite formal ni como un mero instrumento descriptivo de flujos de datos. Su función es condicionar jurídicamente el diseño, el alcance y, en su caso, la propia decisión de despliegue del sistema, conforme a la lógica material del artículo 35 RGPD.

(3) En cuanto a su contenido sustantivo, la evaluación de impacto en tratamientos biométricos no identificantes debe adaptarse a la especificidad de estos sistemas y abordar, al menos, los siguientes elementos:

(a) Identificación de la información corporal tratada y de su función inferencial. La EIPD debe describir no solo las señales captadas, sino el tipo de inferencias que el sistema está en condiciones de generar a partir de ellas, con qué grado de fiabilidad y con qué finalidad funcional. La inferencia constituye el núcleo material del riesgo y debe ser tratada como objeto jurídico autónomo (Wachter & Mittelstadt, 2019; Hildebrandt, 2020).

(b) Análisis reforzado de necesidad y proporcionalidad. Dada la naturaleza corporal de la información tratada, la evaluación debe aplicar un estándar particularmente estricto de necesidad y proporcionalidad, valorando si la finalidad perseguida puede alcanzarse mediante medios menos intrusivos y si la intensidad inferencial resulta justificable a la luz de los efectos sobre la persona (§§4.2–4.4).

(c) Evaluación de los efectos materiales sobre derechos fundamentales. La EIPD debe integrar de forma expresa los riesgos para la autonomía personal, la

igualdad material, la autodeterminación informativa y la tutela judicial efectiva, conforme a los artículos 7, 8 y 47 CDFUE, evitando una concepción reducida del riesgo centrada exclusivamente en la confidencialidad o la seguridad de la información (considerando 75 RGPD).

(d) Consideración de los efectos acumulativos y sistémicos. Cuando el tratamiento opere de forma continua o a gran escala, la evaluación debe atender a los efectos acumulativos derivados de la repetición de micro-intervenciones inferenciales y a la posible normalización del impacto, evitando una lectura atomizada del riesgo (§4.5).

(e) Valoración del control efectivo de la persona interesada. La EIPD debe analizar si la arquitectura del sistema permite un ejercicio real y no meramente formal de los derechos reconocidos en el RGPD, o si la opacidad inferencial y la variabilidad contextual generan un déficit estructural de control (§§4.4 y 4.5).

(4) La evaluación de impacto se inserta, finalmente, en el marco más amplio de la responsabilidad proactiva del artículo 24 RGPD. No se trata únicamente de identificar riesgos, sino de adoptar decisiones jurídicas vinculantes sobre el diseño, la limitación o la no implantación del tratamiento cuando los riesgos no puedan mitigarse de forma proporcionada. En este sentido, la EIPD constituye un instrumento de gobernanza del tratamiento y no una fase preliminar meramente informativa.

§5.4. MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA LA MITIGACIÓN DEL RIESGO

La gestión preventiva de los riesgos asociados a los tratamientos biométricos no identificantes mediante inteligencia artificial exige la adopción de medidas técnicas y organizativas adecuadas, conforme a los artículos 24, 25 y 32 RGPD, orientadas no solo a la seguridad de la información, sino al gobierno material del funcionamiento inferencial de sistemas que tratan señales corporales sometidas a procesos de biometrización no identificante. En este tipo de tratamientos, el riesgo no se localiza prioritariamente en accesos no autorizados o brechas de confidencialidad, sino en la capacidad del sistema para extraer inferencias a partir del cuerpo en funcionamiento, modular el entorno de interacción y producir efectos acumulativos difíciles de percibir y de impugnar.

Desde esta perspectiva, las medidas de mitigación deben dirigirse principalmente a delimitar, restringir y gobernar la inferencia, en tanto inferencia biométrica no singularizante, integrando la protección de datos desde el diseño y por defecto como una exigencia estructural, y no como un complemento posterior al despliegue del sistema.

§5.4.1. DELIMITACIÓN *EX ANTE* DE LAS INFERENCIAS PERMITIDAS

Una medida central de mitigación consiste en la definición expresa y documentada de las inferencias que el sistema está autorizado a generar y utilizar. En tratamientos biométricos no identificantes, no basta con describir las señales captadas ni con afirmar genéricamente que no existe identificación: resulta imprescindible identificar qué inferencias biométricas pueden extraerse del cuerpo o del cuerpo en funcionamiento, con qué finalidad funcional y bajo qué condiciones.

Esta delimitación debe formar parte del diseño del sistema y quedar reflejada en la documentación del tratamiento, incluyendo el registro de actividades y la evaluación de impacto. La exclusión deliberada de inferencias biométricas técnicamente posibles —por ejemplo, la inferencia de estados emocionales complejos, rasgos de personalidad o

disposiciones psicológicas a partir de señales de baja fiabilidad— constituye una aplicación directa del artículo 25 RGPD y una manifestación concreta de la responsabilidad proactiva.

§5.4.2. Minimización inferencial y restricción funcional del uso de resultados

La minimización, en estos tratamientos, no puede entenderse en términos exclusivamente cuantitativos. Resulta necesario aplicar una minimización inferencial específicamente orientada a limitar la producción y reutilización de inferencias biométricas no identificantes, dirigida a restringir su alcance, su persistencia y su circulación funcional.

Ello implica, en particular, evitar que inferencias biométricas producidas para una finalidad concreta se reutilicen para finalidades distintas, más intrusivas o no evaluadas, así como restringir su combinación con otros datos o sistemas. Por ejemplo, inferencias biométricas generadas para adaptar una interfaz en tiempo real no deberían reutilizarse para clasificar perfiles de riesgo, vulnerabilidad o fiabilidad conductual sin una nueva evaluación sustantiva conforme al RGPD. Esta restricción funcional reduce el riesgo de deriva progresiva del tratamiento y se vincula directamente con el principio de limitación de la finalidad del artículo 5.1.b RGPD y con el deber de garantizar y poder demostrar el cumplimiento del Reglamento (art. 24 RGPD).

§5.4.3. Diseño orientado a la reducción de la presión algorítmica

Cuando el tratamiento permite modular el entorno de decisión, una medida relevante de mitigación consiste en evitar diseños que intensifiquen de forma sistemática la presión persuasiva sobre la base de inferencias biométricas relativas a estados de vulnerabilidad situacional. Ello puede implicar, según el contexto, introducir fricciones deliberadas, limitar la frecuencia de ajustes adaptativos o excluir el uso de determinadas inferencias biométricas en fases sensibles de la interacción.

Estas decisiones de diseño no persiguen neutralizar toda forma de adaptación funcional, sino prevenir la explotación sistemática de estados transitorios de fragilidad decisional inferidos a partir del cuerpo, identificados como un riesgo material para la autonomía personal y la igualdad material. A diferencia de otras formas de personalización basadas en historiales conductuales, en estos sistemas la presión algorítmica se calibra a partir de señales corporales continuas, lo que reduce de forma significativa la capacidad de anticipación y resistencia por parte de la persona. En este sentido, el diseño del sistema constituye un elemento normativamente relevante y no un ámbito neutro desde el punto de vista jurídico.

§5.4.4. Mejora de la trazabilidad y documentación del funcionamiento inferencial

La mitigación del riesgo exige reforzar la trazabilidad de las inferencias relevantes y de sus efectos funcionales, de modo que resulte posible reconstruir, al menos de forma razonable, cómo y cuándo el sistema ha utilizado determinadas inferencias biométricas para ajustar la interacción o producir efectos jurídicamente relevantes.

Esta exigencia no implica la conservación exhaustiva de todas las señales en bruto, pero sí la documentación suficiente de las lógicas inferenciales, de los parámetros decisionales y de los eventos relevantes. La dificultad de trazabilidad se ve agravada en estos sistemas por el carácter efímero, dinámico y no reversible de muchas señales

biométricas en bruto, lo que impide reconstruir *ex post* la cadena inferencial a partir de la experiencia subjetiva de la persona afectada. La ausencia total de trazabilidad no constituye una mera carencia técnica, sino un factor autónomo de riesgo, en la medida en que debilita el ejercicio efectivo de derechos y la rendición de cuentas del responsable del tratamiento (§§4.4 y 4.5).

§5.4.5. GOBERNANZA INTERNA Y CONTROL ORGANIZATIVO DEL SISTEMA

Desde el punto de vista organizativo, resulta imprescindible establecer estructuras claras de gobernanza del tratamiento, que identifiquen responsabilidades internas, procedimientos de revisión y mecanismos de control sobre el funcionamiento del sistema inferencial biométrico. Ello incluye la definición de roles para la supervisión del uso de inferencias corporales, la gestión de modificaciones del sistema y la revisión periódica de los riesgos identificados en la EIPD como obligación continuada y no puntual.

En sistemas que aprenden o se ajustan dinámicamente, la evaluación del riesgo no puede limitarse a la fase inicial de despliegue. La modificación de modelos, finalidades o contextos de uso debe actuar como gatillo para una reevaluación sustantiva, conforme a la lógica de corresponsabilidad y control efectivo desarrollada por la jurisprudencia del TJUE en materia de tratamiento de datos personales (vid. TJUE, asunto C-40/17, Fashion ID, 2019).

§5.4.6. EVALUACIÓN CONTINUA DE PROPORCIONALIDAD Y POSIBILIDAD DE NO DESPLIEGUE

Las medidas técnicas y organizativas deben permitir una evaluación continuada de la necesidad y proporcionalidad del tratamiento en relación con la finalidad perseguida, atendiendo específicamente a la intensidad y alcance de la inferencia biométrica no identificante. Cuando, a la luz de la evaluación de impacto y de la experiencia de uso, los riesgos no puedan mitigarse de forma adecuada, la decisión jurídicamente correcta puede consistir en no implantar, suspender o retirar el sistema.

Esta posibilidad no constituye una anomalía, sino una consecuencia directa del artículo 35 RGPD y del principio de responsabilidad proactiva. La no implantación o el repliegue de sistemas de biometría no identificante inferencial forman parte del contenido material del deber de prevenir impactos desproporcionados sobre los derechos y libertades fundamentales.

Advertir, por último, que las medidas aquí descritas no agotan el catálogo de opciones posibles ni pueden aplicarse de forma mecánica a todos los tratamientos biométricos no identificantes. Se ha pretendido proporcionar un marco operativo de referencia específicamente orientado a la gobernanza preventiva de sistemas de IA que tratan información corporal sin finalidad identificante, adaptable a las características concretas de cada sistema y a los riesgos identificados en la evaluación de impacto.

§6. Consideraciones sobre el papel de las Autoridades de Protección de Datos respecto a los tratamientos biométricos no identificantes y límites del control *ex post*

La identificación y caracterización de los riesgos asociados a los tratamientos biométricos no identificantes mediante inteligencia artificial (§4), así como su gestión preventiva en el marco del RGPD (§5), obligan a examinar el papel que corresponde a las Autoridades de Protección de Datos en este ámbito. Este examen no puede realizarse desde una perspectiva abstracta o meramente institucional, sino atendiendo a las condiciones materiales en los que operan estos tratamientos inferenciales basados en información corporal y a los límites estructurales del control *ex post* cuando el impacto sobre los derechos fundamentales es continuo, inferencial y difícil de reconstruir.

El análisis que sigue no pretende redefinir las competencias de las Autoridades ni reiterar su estatuto normativo general —ya establecido en los artículos 51 a 59 RGPD—, sino precisar qué tipo de intervención resulta jurídicamente relevante y eficaz frente a tratamientos biométricos no identificantes, así como qué expectativas de tutela deben considerarse realistas en este contexto.

§6.1. Función de las Autoridades de Protección de Datos en el marco del RGPD aplicada a la biometría no identificante

En los tratamientos biométricos no identificantes, la intervención de las Autoridades de Protección de Datos no se justifica por la existencia de identificación singularizante ni por la mera utilización de tecnologías biométricas, sino por la capacidad del tratamiento para, de una parte, generar inferencias a partir de las señales corporales y, de otra, producir efectos materiales sobre los derechos y libertades de las personas.

Desde esta perspectiva, la función de las Autoridades se orienta principalmente a:

> (a) Verificar la corrección de la identificación del riesgo realizada por el responsable del tratamiento, en particular cuando este ha descartado la existencia de riesgo elevado basándose exclusivamente en la ausencia de identificación o de decisiones automatizadas en sentido estricto.
>
> (b) Evaluar la suficiencia y calidad sustantiva de las evaluaciones de impacto, cuando estas resultan exigibles conforme al artículo 35 RGPD, prestando especial atención a la delimitación de inferencias biométricas permitidas, a la valoración de efectos acumulativos y a la proporcionalidad material del tratamiento.
>
> (c) Exigir una aplicación efectiva de la protección de datos desde el diseño y por defecto, orientada no solo a la seguridad de la información, sino al gobierno del funcionamiento inferencial biométrico del sistema.

En este ámbito, la intervención de las Autoridades no puede limitarse a un control formal de cumplimiento documental. La naturaleza inferencial y dinámica de estos tratamientos exige una lectura material del RGPD, centrada en los efectos del tratamiento y no en su calificación tecnológica o funcional. De lo contrario, la ausencia de identificación singularizante puede operar como un factor de invisibilización del riesgo, en contra de la lógica del Reglamento.

§6.2. Límites estructurales del modelo de control reactivo en tratamientos biométricos no identificantes

El control *ex post* presenta límites particularmente acusados cuando se aplica a tratamientos biométricos no identificantes basados en inferencias continuas a partir de información corporal. Estos límites no derivan únicamente de dificultades prácticas o de falta de recursos, sino de rasgos estructurales del propio tratamiento.

En primer lugar, la opacidad funcional de los sistemas inferenciales dificulta la reconstrucción a posteriori de cómo se han generado determinadas inferencias y de qué modo han influido en la configuración concreta del entorno de interacción. El impacto sobre los derechos no se manifiesta como un acto único ni como una decisión automatizada aislable, sino como una secuencia de micro-ajustes acumulativos (Rouvroy & Berns, 2013; Hildebrandt, 2020).

En segundo lugar, la temporalidad acumulativa del daño reduce la eficacia reparadora del control reactivo. Cuando la intervención administrativa se produce, los efectos del tratamiento suelen haberse desplegado ya de forma continuada y normalizada en espacios cotidianos de interacción, lo que limita la capacidad de corrección material del impacto.

En tercer lugar, se produce una asimetría probatoria estructural. La persona afectada carece, en la mayoría de los casos, de los elementos necesarios para identificar el tratamiento relevante, demostrar el nexo causal entre la inferencia y la afectación de derechos o impugnar el funcionamiento del sistema. Esta asimetría condiciona no solo el ejercicio de acciones individuales, sino también la capacidad de actuación de las Autoridades, que dependen en gran medida de la documentación aportada por el propio responsable del tratamiento (Wachter & Mittelstadt, 2019).

Estos límites explican por qué el modelo de tutela del RGPD no puede descansar, en este ámbito, sobre mecanismos predominantemente reactivos.

§6.3. Interacción entre el RGPD y el RIA en la práctica administrativa: implicaciones específicas para la biometría no identificante

La entrada en vigor del RIA introduce un marco adicional de supervisión, basado en una lógica tipificadora y *ex ante*. En el ámbito de la biometría no identificante, esta coexistencia plantea un riesgo específico: que la ausencia de calificación como sistema prohibido o de alto riesgo en el RIA se interprete como indicio de bajo riesgo, desplazando el escrutinio material que exige el RGPD.

Dado que el RIA no ofrece un tratamiento unitario de la biometría no singularizante y tiende a subestimar los riesgos derivados de la inferencia continua basada en señales corporales en contextos no disciplinarios, la aplicación del RGPD conserva un papel decisivo como marco de protección transversal. En la práctica administrativa, ello exige evitar una lectura compartimentada de ambos Reglamentos y rechazar la idea de que el encaje atenuado de un sistema en el RIA reduzca automáticamente las exigencias derivadas del RGPD (EDPB & EDPS, 2021; Escajedo San-Epifanio, 2024).

La función de las Autoridades de Protección de Datos se mantiene, así, como garante del análisis material del riesgo, incluso cuando el sistema de inteligencia artificial ha superado los controles formales de conformidad previstos en el Reglamento de Inteligencia Artificial.

§6.4. NECESIDAD DE REFORZAR LA LÓGICA PREVENTIVA FRENTE AL CONTROL *EX POST* EN TRATAMIENTOS BIOMÉTRICOS NO IDENTIFICANTES

Los límites estructurales del control reactivo y la sistemática del RIA conducen a una conclusión clara: en los tratamientos biométricos no identificantes mediante inteligencia artificial, la tutela efectiva de los derechos fundamentales depende de la intensificación real de la lógica preventiva del RGPD.

Esta prevención no se agota en la adopción de medidas de seguridad ni en el cumplimiento formal de obligaciones informativas, sino que se proyecta sobre decisiones sustantivas de diseño y gobernanza del tratamiento: delimitación de inferencias, restricción de usos persuasivos, trazabilidad proporcional y revisión continua de la proporcionalidad del sistema.

Desde esta perspectiva, el papel de las Autoridades de Protección de Datos no consiste principalmente en reparar daños ya producidos, sino en exigir que el responsable del tratamiento anticipe, evalúe y mitigue los riesgos antes de su materialización, incluso cuando ello conduzca a la no implantación del sistema. Esta orientación no introduce exigencias ajenas al RGPD, sino que constituye una aplicación coherente de su arquitectura normativa en contextos de alto riesgo inferencial.

§7. Conclusiones y recomendaciones operativas

§7.1. Síntesis de resultados

El análisis desarrollado permite afirmar, como conclusión central, que los tratamientos biométricos no identificantes mediante sistemas de inteligencia artificial recaen siempre sobre información corporal, con independencia del modo técnico de obtención, de la existencia o no de enrolamiento biométrico y de su eventual potencial singularizante. El hecho de que dichos tratamientos no persigan la identificación única de la persona no altera la naturaleza corporal de la información tratada, ni neutraliza su capacidad de incidir materialmente en la esfera de los derechos y libertades fundamentales.

Desde esta premisa, el trabajo pone de manifiesto que los esquemas normativos construidos en torno a la identificación singularizante resultan insuficientes para captar el riesgo jurídico asociado a estas prácticas. La ausencia de finalidad identificante —criterio central tanto en la definición del artículo 4.14 RGPD como en amplios segmentos de la sistemática del Reglamento (UE) 2024/1689 de Inteligencia Artificial— no constituye un indicador fiable de menor riesgo, en la medida en que el impacto jurídicamente relevante no se produce en el plano de la identidad, sino en el de la inferencia biométrica y la modulación del entorno de interacción.

Desde una perspectiva jurídico-material, el desplazamiento decisivo se sitúa en el tratamiento inferencial de señales corporales, atencionales o conductuales, que permite intervenir de forma continua y adaptativa en las condiciones en las que se forma la voluntad de la persona. Los sistemas analizados no sustituyen formalmente la decisión humana ni operan necesariamente mediante decisiones automatizadas aislables, pero configuran de manera persistente el contexto decisional, a través de inferencias opacas y normalizadas en entornos de uso cotidiano. Esta modalidad de afectación desborda los presupuestos clásicos de tutela basados en actos discretos de tratamiento o en decisiones automatizadas individualizables.

El estudio del marco normativo europeo pone de relieve que el RIA reconoce de forma fragmentaria determinados usos biométricos no singularizantes, pero que su técnica regulatoria —basada en categorías funcionales y contextos de uso— tiende a subestimar los riesgos derivados de prácticas inferenciales continuas, especialmente fuera de escenarios disciplinarios clásicos. En consecuencia, la tutela efectiva de los derechos fundamentales frente a estos tratamientos se articula, en la práctica, a través del RGPD.

En este contexto, la responsabilidad proactiva del RGPD desempeña un papel crucial en la gestión preventiva de estos riesgos. Operativizada mediante las evaluaciones de impacto, la protección de datos desde el diseño y por defecto, junto con la gobernanza de las inferencias, permiten abordar riesgos que se manifiestan de forma acumulativa y sistémica, afectando a la autonomía personal, la igualdad material, la autodeterminación informativa y la tutela judicial efectiva, incluso en ausencia de identificación singularizante o de decisiones automatizadas en sentido estricto.

§7.2. Recomendaciones prácticas para las Autoridades de Protección de Datos

Desde la perspectiva de la supervisión administrativa, el estudio realizado evidencia la necesidad de que las Autoridades de Protección de Datos evalúen los tratamientos biométricos no identificantes basados en sistemas de inteligencia artificial atendiendo a su capacidad inferencial y a sus efectos materiales, y no exclusivamente a la existencia de una finalidad identificante ni a su encaje formal en las categorías del RIA.

En este sentido, resulta recomendable que las Autoridades consideren de forma sistemática la concurrencia de riesgo elevado cuando dichos tratamientos impliquen inferencias continuas o situacionales sobre información corporal, orientando la exigencia de evaluaciones de impacto y la supervisión de las medidas de protección de datos desde el diseño y por defecto.

Asimismo, se recomienda una interpretación coordinada del RGPD y del RIA que evite que la ausencia de prohibición o de clasificación como sistema de alto riesgo en este último conduzca a una subestimación administrativa del riesgo. La aplicación del RIA no debe operar como filtro excluyente del escrutinio material exigido por el RGPD, sino que aporta un marco complementario que no desplaza la lógica de gestión preventiva del riesgo propia de este último.

En esta línea, se han presentado en este trabajo criterios jurídicos destinados a reforzar una actuación preventiva de las Autoridades, centrada en la gestión anticipada de riesgos acumulativos y en la garantía efectiva de los derechos y libertades fundamentales.

§7.3. Recomendaciones prácticas para responsables del tratamiento

A la luz del análisis realizado, y teniendo en cuenta que los tratamientos biométricos no identificantes recaen siempre sobre información corporal, pueden formularse las siguientes orientaciones operativas dirigidas a los responsables del tratamiento, desde una lógica estrictamente jurídica y alineada con el principio de responsabilidad proactiva del RGPD:

(1) Aplicar un estándar reforzado de necesidad, finalidad y proporcionalidad.
La naturaleza corporal de la información tratada exige una aplicación particularmente estricta de los principios de necesidad, limitación de la finalidad y proporcionalidad. La ausencia de finalidad identificante no justifica, por sí sola, una menor intensidad del escrutinio. El responsable debe poder demostrar que el tratamiento inferencial resulta estrictamente necesario para una finalidad legítima concreta y que no existen medios menos intrusivos para alcanzarla.

(2) Evitar la trivialización jurídica de la biometría no identificante.
Los tratamientos biométricos no identificantes no deben ser asimilados automáticamente a técnicas ordinarias de personalización o análisis de comportamiento. El hecho de que no culminen en identificación singularizante no elimina su capacidad de afectar a la autonomía personal, a la igualdad material o a la autodeterminación informativa. Esta consideración debe reflejarse expresamente en la calificación jurídica del tratamiento y en la evaluación del riesgo.

(3) Situar las inferencias biométricas en el centro del análisis de licitud.
El análisis jurídico no puede limitarse a los datos captados en bruto ni a su eventual conservación. El responsable debe identificar de forma expresa qué inferencias biométricas se generan, con qué grado de fiabilidad y con qué efectos funcionales, y someter dichas inferencias —y no solo los datos de entrada— a un juicio autónomo de necesidad y proporcionalidad.

(4) Tratar la evaluación de impacto como instrumento ordinario de gobernanza.
Cuando el tratamiento permita inferencias continuas o en tiempo real a partir de información corporal, se integre estructuralmente en entornos de interacción cotidiana o presente opacidad funcional relevante, la realización de una evaluación de impacto conforme al artículo 35 RGPD debe considerarse, como

regla general, jurídicamente exigible. La EIPD debe centrarse en los efectos inferenciales y no limitarse a una descripción formal de flujos de datos.

(5) Aplicar la protección de datos desde el diseño sobre la arquitectura inferencial.
Las obligaciones del artículo 25 RGPD deben proyectarse sobre la configuración misma del sistema inferencial. Ello implica incorporar límites *ex ante* al alcance de las inferencias permitidas, a su reutilización funcional y a su integración en mecanismos de modulación del entorno decisional, y no únicamente medidas de seguridad o pseudonimización.

(6) Extremar la cautela en usos persuasivos basados en estados situacionales.
El uso de inferencias biométricas para adaptar o intensificar estímulos en función de estados transitorios de vulnerabilidad (fatiga, estrés, impulsividad, disminución de la atención) exige una justificación reforzada. En contextos comerciales o de ocio, el responsable debe acreditar que tales prácticas no producen efectos materiales de desigualdad ni explotación de la fragilidad decisional.

(7) Asumir jurídicamente la posibilidad del no despliegue del sistema.
Cuando, tras la evaluación de impacto y la adopción de medidas razonables, persista un riesgo elevado no mitigable de forma proporcionada, la decisión jurídicamente correcta puede consistir en no implantar o retirar el sistema. Esta opción forma parte del contenido material de la responsabilidad proactiva y no puede considerarse excepcional ni residual.

§7.4. LÍNEAS FUTURAS DE INVESTIGACIÓN Y MEJORA NORMATIVA

El análisis desarrollado pone de manifiesto la necesidad de profundizar, desde una perspectiva jurídico-dogmática, en una teoría jurídica de la inferencia, capaz de ofrecer categorías operativas para evaluar tratamientos que no identifican singularmente a las personas, pero sí las interpretan, categorizan y sitúan funcionalmente en entornos algorítmicamente modulados. Esta línea de investigación resulta indispensable para adaptar los instrumentos clásicos de la protección de datos personales a arquitecturas inferenciales continuas que operan sobre información corporal y producen efectos materiales relevantes sin cristalizar en decisiones automatizadas aislables.

En particular, se revela necesario avanzar en una conceptualización jurídica más precisa de la información corporal como objeto autónomo de tutela, con independencia del modo técnico de captación y de su potencial singularizante. La persistente vinculación normativa entre biometría e identificación ha demostrado ser insuficiente para captar los riesgos derivados de usos inferenciales que explotan señales corporales con fines de modulación del entorno de decisión, perfilado situacional o influencia conductual. Una clarificación conceptual en este punto permitiría aplicar de forma más coherente y exigente los criterios de necesidad, finalidad y proporcionalidad previstos en el RGPD.

Desde el punto de vista normativo, la experiencia del RIA sugiere la conveniencia de revisar el peso otorgado al criterio de la identificación como eje central de la evaluación del riesgo biométrico. La técnica de clasificación por usos y contextos ha mostrado una capacidad limitada para abordar prácticas inferenciales no singularizantes con impacto significativo sobre derechos fundamentales, especialmente en entornos comerciales y de ocio, lo que invita a reconsiderar el equilibrio entre tipificación *ex ante* de sistemas y evaluación sustantiva de los efectos reales del tratamiento.

En el plano institucional, el trabajo pone de relieve la importancia de reforzar una lectura coordinada del RGPD y del RIA, evitando que la subestimación del riesgo en este último genere zonas de infra-protección. Esta coordinación depende tanto de eventuales ajustes normativos como de una interpretación exigente por parte de las Autoridades de Protección de Datos, orientada a preservar la efectividad material de los derechos fundamentales frente a prácticas inferenciales continuas y estructuralmente opacas.

Finalmente, el desarrollo de criterios más precisos para la evaluación *ex ante* de estos tratamientos —en particular en el marco de las evaluaciones de impacto— constituye una línea prioritaria tanto para la investigación jurídica como para la práctica regulatoria. En ausencia de tales criterios, existe el riesgo de que arquitecturas inferenciales basadas en biometría no identificante queden normalizadas como meras técnicas de personalización, pese a su capacidad real para afectar de manera significativa a la autonomía personal, la igualdad material y la autodeterminación informativa.

§8. Referencias citadas

A) Derecho de la Unión Europea

Carta de los Derechos Fundamentales de la Unión Europea (2012/C 326/02). Diario Oficial de la Unión Europea, C 326, 391–407.

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 (Reglamento general de protección de datos). Diario Oficial de la Unión Europea, L 119, 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 (Reglamento de Inteligencia Artificial) y se modifican diversos Reglamentos y Directivas. Diario Oficial de la Unión Europea, L, 2024/1689 (12.7.2024).

B) Soft law y documentos institucionales citados

Agencia Española de Protección de Datos (AEPD). (2019). *Informe jurídico sobre el uso de datos biométricos para el control de presencia*. AEPD.

Agencia Española de Protección de Datos (AEPD). (2020). *Guía sobre el uso del consentimiento como base de legitimación del tratamiento de datos personales*. AEPD.

Article 29 Working Party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679* (WP248 rev.01).

European Data Protection Board (EDPB) & European Data Protection Supervisor (EDPS). (2021, 18 June). *Joint Opinion 5/2021 on the proposal for a Regulation laying down harmonised rules on artificial intelligence* (Artificial Intelligence Act).

European Data Protection Board (EDPB). (2018). *Guidelines on transparency under Regulation (EU) 2016/679* (WP260 rev.01).

European Data Protection Board (EDPB). (2022). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*.

C) Jurisprudencia europea citada

Tribunal Europeo de Derechos Humanos (Gran Sala). (2008). Sentencia de 4 de diciembre de 2008, *S. and Marper v. the United Kingdom*, demandas núm. 30562/04 y 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204.

Tribunal de Justicia de la Unión Europea (Gran Sala). (2019). Sentencia de 3 de octubre de 2019, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, asunto C-40/17, ECLI:EU:C:2019:629.

Tribunal de Justicia de la Unión Europea. (2022). Sentencia de 1 de agosto de 2022, *Vyriausioji tarnybinės etikos komisija*, asunto C-184/20, ECLI:EU:C:2022:601.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (Gran Sala). (2024). Sentencia de 21 de marzo de 2024, *RL c. Landeshauptstadt Wiesbaden*, asunto C-61/22, ECLI:EU:C:2024:243.

D) BIBLIOGRAFÍA ACADÉMICA CITADA

ABA-CATOIRA, A., BALAGUER CALLEJÓN, F., COTINO HUESO, L., HERNÁNDEZ RAMOS, M., PRESNO LINERA, M. Á., REBOLLO DELGADO, L., & TUDELA ARANDA, J. (2025). Encuesta sobre inteligencia artificial y derechos fundamentales. *Teoría y Realidad Constitucional*, (55), 11–86.

ARENAS RAMIRO, M. (2021). RGPD y autoridades de protección de datos: un antes y un después. En J. A. Viguri Cordero, B. Tomás Mallén, R. García Mahamut & C. Pauner Chulvi (Eds. lits*.), Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español: cuestiones clave de orden nacional y europeo* (pp. 149–178). Tirant lo Blanch. ISBN 978-84-1397-351-7.

ARENAS RAMIRO, M. (2025a). Tecnologías biométricas y autoridades de protección de datos. En F. Balaguer Callejón & L. Escajedo San Epifanio (Dirs.), *Vigilancia biométrica masiva, inteligencia artificial y derechos fundamentales*. Tirant lo Blanch. ISBN 979-13-70063-90-0.

ARENAS RAMIRO, M. (2025b). Un nuevo desafío para las autoridades de protección de datos: cariño, ¿quién vigila a los niños? *Diario La Ley*, (10654).

AUZMENDI DEL SOLAR, M., & MAYOR GÓMEZ, R. (2023). Evaluación de impacto en protección de datos en los parlamentos. En E. de Alba Bastarrechea (Coord.), *La protección de datos en el ámbito parlamentario: guía práctica* (pp. 141–166). Congreso de los Diputados. ISBN 978-84-09-52745-8.

BAROCAS, S., & SELBST, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732.

BARRIO ANDRÉS, M. (2025). El Reglamento de IA de la Unión Europea: el gobierno democrático de la inteligencia artificial. En N. Febles Pozo & P. Nieto Rojas (Dirs.), *Inteligencia artificial y protección de datos: desafíos en la era digital* (pp. 19–40). Tirant lo Blanch. ISBN 979-13-7011-111-3.

BUBLITZ, J. C., & MERKEL, R. (2014). Crimes against minds: On mental manipulations, harms and a human right to mental self-determination. *Criminal Law and Philosophy*, 8(1), 51–77.

BUENO DE MATA, F. (2024). Artículo 50. Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA. En M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial* (pp. 513–523). Tirant lo Blanch. ISBN 978-84-18662-88-1.

BUSCH, C. (2007). Biometrics and privacy: A survey. En S. Li & A. K. Jain (Eds.), Handbook of face recognition (pp. 17–34). Springer.

CALAZA LÓPEZ, S. (2025). ¿Qué pesa más en la balanza de la IA judicial: la transparencia o la protección de datos? En N. Febles Pozo & P. Nieto Rojas (Dirs.), *Inteligencia artificial y protección de datos: desafíos en la era digital* (pp. 15–18). Tirant lo Blanch. ISBN 979-13-7011-111-3.

CANO RUIZ, I. (2019). Categorías especiales de datos. En M. Arenas Ramiro & A. Ortega Giménez (Dirs.), *Protección de datos: Comentarios a la Ley Orgánica de Protección de*

Datos y Garantía de Derechos Digitales (en relación con el RGPD) (pp. 81–84). Tirant lo Blanch. ISBN 978-84-17414-92-4.

COHEN, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

COTINO HUESO, L. (2019). Protección de datos desde el diseño y por defecto. En J. López Calvo (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (pp. 389–420). Tirant lo Blanch.

COTINO HUESO, L. (2025). Desentrañando el Reglamento de Inteligencia Artificial de la Unión Europea: una guía esencial. En G. Castro Marquina (Coord.), *El Derecho ante el reto de las tecnologías disruptivas. Actualidad legislativa y jurisprudencial*. Tirant lo Blanch. ISBN 979-13-7011-408-4.

CRAWFORD, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

DE HERT, P., & LAZCOZ, G. (2022). Accountability as the core principle of the GDPR. *European Data Protection Law Review*, 8(1), 31–40.

DE LA PRADA ESPINA, D. (2018). Evaluación de impacto de protección de datos (EIPD). En J. P. Murga Fernández, M. Á. Fernández Scagliusi & M. Espejo Lerdo de Tejada (Dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía* (pp. 477–502). Reus. ISBN 978-84-290-2093-9.

EGUILUZ CASTAÑEIRA, J. A. (2025). Reglamento IA: aspectos esenciales de una norma pionera. En I. Herbosa Martínez & D. Fernández de Retana Gorostizagoiza (Coords.), *Derecho e inteligencia artificial: avanzando en la regulación de la inteligencia artificial* (pp. 41–107). Tirant lo Blanch. ISBN 978-84-1162-707-8.

ESCAJEDO SAN-EPIFANIO, L. (2017). *Tecnologías biométricas, identidad y derechos fundamentales.* Thomson Reuters Aranzadi.

ESCAJEDO SAN-EPIFANIO, L. (2024). El reconocimiento biométrico en el Reglamento de inteligencia artificial: Exenciones, prohibiciones y especialidades de alto riesgo. En L. Cotino Hueso & P. Simón Castellano (Dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea* (pp. 183–239). Aranzadi.

ESCAJEDO SAN-EPIFANIO, L. (2025). Constitucionalismo y panóptico digital "amable": Biometrías automatizadas, privacidad y libertad cognitiva. En F. Balaguer Callejón & L. Escajedo San-Epifanio (Dirs.), *Vigilancia biométrica masiva, identidad y derechos fundamentales*. Dykinson.

FAGGIANI, V. (2024). La tutela judicial efectiva como centro de la justicia en el Estado de Derecho. En G. Bezerra Sales Sarlet (Coord.) & V. Faggiani (Dir.), *Retos del derecho ante la IA: apuntes desde una perspectiva interdisciplinar* (pp. 27–55). Tirant lo Blanch. ISBN 978-84-1004-474-6.

GELLERT, R. (2021). The role of the risk-based approach in the General Data Protection *Regulation. Journal of European Legal Studies*, 13(1), 1–25.

GONZÁLEZ FUSTER, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer.

GONZÁLEZ-MENESES GARCÍA-VALDECASAS, M. (2024). Artículo 6. Reglas de clasificación de los sistemas de IA de alto riesgo. En M. Barrio Andrés (Dir.), *Comentarios al Reglamento Europeo de Inteligencia Artificial* (pp. 205–222). Tirant lo Blanch. ISBN 978-84-18662-88-1.

GUTWIRTH, S., & HILDEBRANDT, M. (2010). Profiling the European citizen: Cross-disciplinary perspectives. En M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen* (pp. 1–32). Springer.

HIJMANS, H. (2016). T*he European Union as guardian of internet privacy: The story of Article 16 TFEU*. Springer.

Hildebrandt, M. (2020). *Law for computer scientists and other folk*. Oxford University Press.

IENCA, M., & ANDORNO, R. (2017). Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy*, 13, Article 5.

JASSERAND, C. (2016). Avoiding terminological confusion between the notions of "biometrics" and "biometric data". *International Data Privacy Law*, 6(1), 63–76.

KINDT, E. (2013). *Privacy and data protection issues of biometric applications: A comparative legal analysis*. Springer.

Kindt, E. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer Law & Security Review*, 34(3), 523–538.

LARROSA IBÁÑEZ, I. M.ª (2025). ¿Vulneración del derecho a la tutela judicial efectiva con el uso de la inteligencia artificial (IA law)? En M. Á. Tenas Alós & E. Colás Laguardia (Dirs.), *La inevitable incidencia cotidiana de la inteligencia artificial: un análisis desde la perspectiva jurídica*. Tirant lo Blanch. ISBN 979-13-7011-393-3.

LYNSKEY, O. (2015). The foundations of EU data protection law. Oxford University Press.

MANTELERO, A., & ESPOSITO, M. S. (2021). An evidence-based methodology for human rights impact assessment in AI. *Computer Law & Security Review*, 41, Article 105561.

MARÍN JIMÉNEZ, R. (2019). Evaluación de impacto en la protección de datos: paralelismos. *I+S: Revista de la Sociedad Española de Informática y Salud*, (134), 24–26.

MARTÍNEZ MARTÍNEZ, R. (2022). El rol de las autoridades de protección de datos en el Espacio Europeo de Datos. *La Ley Privacidad*, (13). ISSN-e 2659-8698.

MCSTAY, A. (2018). *Emotional AI: The rise of empathic media*. SAGE.

MEDINA GUERRERO, M. (2019). Categorías especiales de datos. En A. Rallo Lombarte (Coord.), *Tratado de protección de datos: Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 251–274). Tirant lo Blanch. ISBN 978-84-1313-282-2.

MIRALLES LÓPEZ, R. M. (2019a). Evaluación de impacto relativa a la protección de datos y consulta previa. En J. López Calvo (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (pp. 469–491). Tirant lo Blanch.

MIRALLES LÓPEZ, R. M. (2019b). Protección de datos desde el diseño y por defecto. En J. López Calvo (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (pp. 421–426). Tirant lo Blanch.

Mordini, E., & Tzovaras, D. (Eds.). (2012). *Second generation biometrics: The ethical, legal and social context.* Springer.

MUÑOZ GARCÍA, C. (2024a). Modelos de IA de uso general y sistemas de IA de riesgo limitado y mínimo. En M. Barrio Andrés (Dir.), *El Reglamento Europeo de Inteligencia Artificial* (pp. 87–109). Tirant lo Blanch. ISBN 978-84-1071-303-1.

MUÑOZ VELA, J. M. (2025). El Reglamento de IA de la UE: cuestiones de actualidad. En R. Guillén Catalán (Coord.), *Derecho de datos, inteligencia artificial e internet en el sector público y privado* (pp. 99–146). Tirant lo Blanch. ISBN 978-84-10292-93-2.

PIÑAR MAÑAS, J. L. (Dir.). (2016). Reglamento general de protección de datos: Hacia un nuevo modelo europeo de protección de datos. Reus.

Quelle, C. (2018). Enhancing compliance under the General Data Protection Regulation: The risky upsides of the accountability and risk-based approach. *European Journal of Risk Regulation*, 9, 502–526.

Romeo Casabona, C. M. (2021). "Datos biométricos (Comentario al artículo 4.14 RGPD)". En A. Troncoso Reigada (Dir.), *Comentario al Reglamento General de Protección de Datos* (Vol. 1, pp. 709–714). Tirant lo Blanch.

Rouvroy, A., & Berns, T. (2013). "Gouvernementalité algorithmique et perspectives d'émancipation", *Réseaux*, 177(1), 163–196.

Saborowski, M. (2010). Biometrics and data protection law. En M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen* (pp. 365–382). Springer.

Sáiz Peña, C. A. (2019). Seguridad de los datos, evaluación de impacto, códigos de conducta y certificación. En A. Rallo Lombarte (Coord.), *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 387–430). Tirant lo Blanch. ISBN 978-84-1313-282-2.

Sanz, L. (2018). El equilibrio entre protección de datos y transparencia. En C. Gómez-Jara Díez (Coord.), *Persuadir y razonar: Estudios jurídicos en homenaje a José Manuel Maza Martín* (Tomo I, pp. 647–688). Tirant lo Blanch. ISBN 978-84-1308-297-4.

Simitis, S. (2011). *Das Recht auf informationelle Selbstbestimmung*. Nomos.

Smuha, N. A. (2021). Beyond a human rights-based approach to AI governance. *Philosophy & Technology*, 34, 91–104.

Sutrop, M., & Laas-Mikko, K. (2012). From identity verification to behavior prediction. Review of Policy Research, 29(1), 21–36.

Torres Carlos, M. R., & Míguez Macho, L. (2024). Sistemas de IA prohibidos y sistemas de IA de alto riesgo. En M. Barrio Andrés (Dir.), *El Reglamento Europeo de Inteligencia Artificia*l (pp. 48–86). Tirant lo Blanch. ISBN 978-84-1071-303-1.

Troncoso Reigada, A. (2021). Las categorías especiales de datos personales y los tratamientos de datos de salud (Comentario al artículo 9 RGPD y a la disposición adicional decimoséptima de la LOPDGDD). En A. Troncoso Reigada (Dir.) & J. J. González Rivas (Pról.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (Vol. 2, pp. 4623–4727). Tirant lo Blanch. ISBN 978-84-1346-102-1.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97–112.

Wachter, S. (2018). Normative challenges of identification in the Internet of Things. *Computer Law & Security Review*, 34(3), 436–449.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences. *Columbia Business Law Review*, 2019(2), 494–620.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.