

ESTUDIOS

EL RECONOCIMIENTO BIOMÉTRICO EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

VIGILANCIA CORPORAL DE LA IDENTIDAD,
EL COMPORTAMIENTO Y LAS EMOCIONES

LEIRE ESCAJEDO SAN-EPIFANIO
IGOR FILIBI

**Si quieres adquirir esta
obra haz click aquí**



III ARANZADI

© Leire Escajedo San-Epifanio e Igor Filibi, 2026
© ARANZADI LA LEY, S.A.U.

ARANZADI LA LEY, S.A.U.

C/ Collado Mediano, 9

28231 Las Rozas (Madrid)

www.aranzadilaley.es

Atención al cliente: <https://areacliente.aranzadilaley.es/publicaciones>

Primera edición: septiembre 2026

Depósito Legal: M-15976-2026

ISBN versión impresa: 978-84-1085-982-1

ISBN versión electrónica: 978-84-1085-983-8

Este trabajo se ha desarrollado en el marco del proyecto AI-BIOSURV, *AI-based Biovigilance in the Post-COVID Era: Corporeality, Identity, and Fundamental Rights* (TED 2021-129975B-C21, MICINN), cuyos investigadores principales son Leire Escajedo San-Epifanio y Francisco Balaguer Callejón. En el desarrollo de la investigación se realizaron dos estancias de investigación: Igor Filibi llevó a cabo una estancia en la Facultad de Derecho de la Universidad de Granada (España); Leire Escajedo San-Epifanio realizó una estancia de investigación de varios meses en el Max Planck Institute for the Study of Crime, Security and Law (Friburgo de Brisgovia, Alemania).

El trabajo se integra igualmente en las actividades del Grupo de Investigación EU-Frames, *Establishing Innovative Regulatory Frameworks in the EU* (GIU24/007), cuyos investigadores principales son L. Escajedo San-Epifanio e I. Filibi.

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.

Printed in Spain

© ARANZADI LA LEY, S.A.U. Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, ARANZADI LA LEY, S.A.U., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

ARANZADI LA LEY no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, o cualesquiera otras herramientas de participación. Igualmente, ARANZADI LA LEY se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

ARANZADI LA LEY queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

ARANZADI LA LEY se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de ARANZADI LA LEY, S.A.U., es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

Si quieres adquirir esta
obra haz click aquí



Índice general

	<u>Página</u>
ABREVIATURAS Y ACRÓNIMOS DE USO FRECUENTE	21
PRESENTACIÓN	
IGOR FILIBI y LEIRE ESCAJEDO SAN-EPIFANIO	32

PARTE I

EL ESTATUTO JURÍDICO DEL RECONOCIMIENTO BIOMÉTRICO EN LA UE EN SU CONJUNTO: MARCO POLÍTICO, NORMATIVO Y CONCEPTUAL PARA SU ANÁLISIS

CAPÍTULO I

CAPTAR EL «YO» CORPÓREO: RECONOCIMIENTO BIOMÉ- TRICO, IDENTIDAD E INFERENCIA AUTOMATIZADA

LEIRE ESCAJEDO SAN-EPIFANIO	35
I. La transformación digital del «yo» corpóreo: reconocimiento y gubernamentalidad	35
II. Identidad e identificación: fundamentos conceptuales y artefactos para la identificación	38
III. Biometrías automatizadas: la datificación del cuerpo y su captación tecnológica	40
IV. Del reconocimiento a la inferencia: la IA y la vigilancia emocional	42



V. El reconocimiento biométrico mediante IA en el marco europeo: economía de la atención, riesgo y derechos fundamentales	44
--	-----------

CAPÍTULO II

DE COMPETIR EN IA A REGULAR LA CONFIANZA: LA VISIÓN EUROPEA PARA EL LIDERAZGO GLOBAL

IGOR FILIBI	49
I. La construcción de marcos reguladores de la IA en el contexto del capitalismo digital	49
II. La doble carrera de la inteligencia artificial: desarrollo tecnológico y disputa por su regulación	52
III. La estrategia de la Unión Europea en la geopolítica de la IA ..	55
<i>III.1. La ambición de convertirse en líder global de la IA confiable ..</i>	55
<i>III.2. Crisis existencial y capacidad de reflexión estratégica</i>	58
III.2.1. El Consejo Europeo y los gobiernos de los Estados miembros	60
III.2.2. El Parlamento Europeo	61
<i>III.3. La implementación de la estrategia de la UE: UE, OCDE, Consejo de Europa y más allá del Occidente ampliado</i>	62
III.3.1. El acuerdo interno y la definición de la estrategia de IA de la UE	64
III.3.2. Despliegue de la estrategia europea	67
III.3.3. Avances en la OCDE y en el Consejo de Europa ..	69
III.3.4. The EU Artificial Intelligence Regulation spearheading a global strategy	72
IV. Más allá de Europa: hacia una regulación global de la IA ...	76
V. Conclusiones	81
(Anexo) Cronología. Hacia una regulación europea y mundial de la Inteligencia Artificial	84



CAPÍTULO III

RECONOCIMIENTO BIOMÉTRICO EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL: EL MAPA NORMATIVO

LEIRE ESCAJEDO SAN-EPIFANIO	93
I. El enfoque del RIA ante el reconocimiento biométrico: contexto, antecedentes y problemas de delimitación	94
II. Antecedentes relevantes: la distancia entre el Libro Blanco y las Resoluciones del Parlamento europeo sobre algunas modalidades de reconocimiento biométrico	96
III. Esquema regulatorio de las tecnologías de reconocimiento biométrico en el RIA	98
IV. El dato personal en el RGPD: concepto y evolución en la era digital	101
IV.1. <i>Una noción expansiva y tecnológicamente neutra</i>	101
IV.2. <i>De la identificación a la inferencia: el dato personal en la sociedad digital</i>	102
IV.3. <i>El principio de responsabilidad proactiva y la protección desde el diseño</i>	103
IV.4. <i>La protección de datos en el contexto digital europeo</i>	104
V. La tensión estructural entre el RGPD y el Reglamento Europeo de Inteligencia Artificial	104
V.1. <i>Dos lógicas regulatorias: enfoque de derechos frente a enfoque de gestión de riesgos</i>	105
V.2. <i>La doble capa de cumplimiento</i>	105
V.3. <i>Las autoridades competentes: un reparto aún inestable</i>	106
V.4. <i>Tres focos de fricción en la práctica</i>	107
V.5. <i>Hacia una articulación constitucional del ecosistema normativo ..</i>	108
VI. Nudos problemáticos en la aplicación conjunta del RGPD y el Reglamento Europeo de Inteligencia Artificial	109
VI.1. <i>Biometría emocional, categorización y sesgos estructurales ..</i>	109
VI.2. <i>La verificación biométrica «uno a uno» y su tratamiento dispar ..</i>	110



	<u>Página</u>
VI.3. <i>Grandes sistemas informáticos y régimen transitorio</i>	111
VI.4. <i>Exclusiones por seguridad nacional y defensa</i>	112
VI.5. <i>Fragmentación institucional y coordinación insuficiente</i>	112
VI.6. <i>Hacia una síntesis de gobernanza coherente</i>	113
 CAPÍTULO IV	
DEL DATO BIOMÉTRICO A LOS SISTEMAS DE RECONOCIMIENTO: CONCEPTOS CLAVE PARA INTERPRETAR EL RIA	
LEIRE ESCAJEDO SAN-EPIFANIO	115
I. ¿Es necesaria una noción de «datos biométricos» más amplia que la del artículo 4.14 RGPD? Las inconsistencias del RIA ..	117
I.1. <i>Antes del RIA: contraste entre la definición del RGPD y las nociones científico-técnicas de datos biométricos</i>	117
I.2. <i>La necesidad de una noción funcional que abarque los datos biométricos con y sin potencial identificante</i>	119
II. Sistemas de identificación biométrica y «aplicaciones biométricas no singularizantes»: requisitos funcionales y los límites conceptuales	120
II.1. <i>Taxonomía de la Biometría (de lo poblacional a lo singular) y primeros sistemas históricos de identificación de humanos en sentido estricto</i>	120
II.2. <i>Clasificación y naturaleza de los datos biométricos en los estudios mensurativos</i>	121
II.2.1. <i>Datos biométricos estáticos: captaciones instantáneas de la anatomía o fisiología corporal</i>	122
II.2.2. <i>Datos biométricos dinámicos: captaciones del cuerpo en lapsos de tiempo</i>	122
II.3. <i>Del dato con potencial singularizante a la construcción de un sistema de identificación: La primera experiencia biométrica en sentido moderno - el sistema antropométrico diseñado por Alphonse Bertillon (el Bertillonage o signalement anthropométrique)</i>	124



	<u>Página</u>
II.4 <i>Características de los sistemas automatizados de reconocimiento biométrico con potencial singularizante</i>	128
II.5 <i>biometrías inferenciales y reconocimiento de emociones: datos biométricos no orientados a la identificación única</i>	129
III. Evolución de la noción de datos biométricos en el proceso de elaboración del RIA	132
IV. La arquitectura subyacente a todos los sistemas biométricos	133
IV.1 <i>Arquitectura básica de los sistemas de reconocimiento biométrico</i>	133
IV.2 <i>Fuentes de datos biométricos, datos en crudo y patrones biométricos</i>	134
IV.3 <i>Utilidades biométricas que identifican, utilidades que no identifican</i>	135
V. Importantes limitaciones de los sistemas de reconocimiento biométrico: científico-técnicas, de arquitectura y ético-sociales . .	137
VI. Reflexión sobre la transición del concepto técnico a las categorías jurídicas de reconocimiento biométrico en el RIA	140

PARTE II

ANÁLISIS DETALLADO DE LOS REGÍMENES QUE SE APLICAN A LAS DIFERENTES UTILIDADES BIOMÉTRICAS EN EL RGPD Y EL RIA

CAPÍTULO V

UTILIDADES BIOMÉTRICAS EN LA ZONA GRIS ENTRE EL RIA Y EL RGPD: VERIFICACIÓN, AUTENTICACIÓN, CRIBADO E IDENTIFICACIÓN NO REMOTA

LEIRE ESCAJEDO SAN-EPIFANIO	145
I. Aplicaciones biométricas en el límite del RIA y del RGPD . .	145
II. el cribado biométrico: categorización, búsqueda y detección sin enrolamiento singularizante	147



	<u>Página</u>
III. La verificación biométrica uno a uno: exclusión parcial del RIA y persistencia de las garantías del RGPD	147
III.1. <i>Los sistemas de identificación civil: su concepto histórico</i>	147
III.2. <i>De los documentos tradicionales de identidad a los que implican verificación biométrica</i>	149
III.3. <i>La verificación biométrica en la tramitación del RIA</i>	153
III.4. <i>Criterios para delimitar la zona gris: finalidad, modalidad de cotejo y contexto de uso</i>	156
IV. La identificación no remota, el punto ciego del RIA	157
V. Recapitulación: la falsa «baja intensidad» de las biometrías más extendidas	159

CAPÍTULO VI

IDENTIFICACIÓN BIOMÉTRICA REMOTA EN TIEMPO REAL EN ESPACIOS DE ACCESO PÚBLICO: LA PROHIBICIÓN CONDICIONADA DEL ART. 5.1.H) RIA

LEIRE ESCAJEDO SAN-EPIFANIO	161
I. Planteamiento: la práctica biométrica más visible en la tramitación del Reglamento Europeo de IA	162
II. La prohibición del artículo 5.1.h) RIA: símbolo político y alcance jurídico efectivo	163
II.1. <i>De la línea roja parlamentaria a la prohibición condicionada</i>	163
II.2. <i>Estructura normativa de la aparente prohibición del uso de la vigilancia biométrica en tiempo real y espacios públicos. Autorizaciones y excepciones</i>	164
II.3. <i>Protección de datos y jurisprudencia europea como límites materiales a la vigilancia biométrica en tiempo real</i>	165
II.4. <i>Un equilibrio inestable entre seguridad y derechos fundamentales</i>	166
III. El debate comparado sobre la identificación biométrica remota en espacios de acceso público	167
III.1. <i>Estados Unidos: fragmentación normativa, litigio estratégico y expansión migratoria de la biometría</i>	167



	<u>Página</u>
III.2. <i>China: vigilancia biométrica y gobernanza inteligente</i>	169
III.3. <i>América Latina: del entusiasmo tecnológico a la corrección judicial</i>	169
III.4. <i>Tendencias comunes: entre libertad, seguridad, discriminación y control independiente</i>	170
IV. Conceptos clave de la prohibición del art. 5.1.h) RIA	171
IV.1. <i>Identificación biométrica remota: tiempo real y diferido</i>	171
IV.2. <i>Espacios de acceso público y fines de garantía del cumplimiento del Derecho</i>	172
IV.3. <i>Excepciones, estricta necesidad y autorización previa</i>	173
IV.4. <i>Los apartados 2 a 8 del art. 5 RIA: procedimiento, notificación y alcance práctico</i>	174
V. La prohibición visible y las concesiones menos visibles	176

CAPÍTULO VII

MÁS ALLÁ DE LA IDENTIFICACIÓN BIOMÉTRICA REMOTA: OTRAS PRÁCTICAS «PROHIBIDAS O RESTRINGIDAS» EN EL ART. 5 RIA

LEIRE ESCAJEDO SAN-EPIFANIO	179
I. Más allá de la vigilancia en tiempo real: otros usos Prohibidos o restringidos del reconocimiento biométrico	179
I.1. <i>La propuesta inicial de la Comisión</i>	181
I.2. <i>Toma de postura del Parlamento</i>	181
I.3. <i>La posición del Consejo y el texto finalmente aprobado</i>	183
II. Puntuación social, predicción de riesgo criminal y bases faciales: biometría, sospecha y clasificación	184
III. Reconocimiento biométrico «de emociones», intenciones y señales conductuales en los lugares de trabajo y en los centros educativos: prohibición parcial	187
IV. Categorización biométrica de atributos sensibles: alcance y límites de la prohibición	190



V. Recapitulación: prohibiciones biométricas, inferencia y clasificación de la persona	191
---	-----

CAPÍTULO VIII

BIOMETRÍAS PERMITIDAS DE ALTO RIESGO: ANEXO III, OBLIGACIONES Y GARANTÍAS EN EL RIA	193
--	-----

I. Del uso prohibido al «uso permitido de alto riesgo» en el RIA: planteamiento	193
II. Qué implica la calificación de alto riesgo en el RIA	195
II.1. <i>La clasificación de alto riesgo: artículo 6 y Anexo III</i>	195
II.2. <i>Requisitos aplicables a los sistemas biométricos de alto riesgo</i> ..	196
II.3. <i>Obligaciones de proveedores, responsables del despliegue y autoridades</i>	198
III. Sistemas biométricos expresamente incluidos en el Anexo III ..	199
III.1. <i>Identificación biométrica remota «no prohibida»</i>	199
III.2. <i>Categorización biométrica basada en atributos sensibles o protegidos</i>	200
III.3. <i>Reconocimiento de emociones en supuestos no cubiertos por la prohibición laboral/educativa</i>	201
IV. Biometrías de alto riesgo por el contexto de uso	202
IV.1. <i>Educación y formación profesional</i>	202
IV.2. <i>Empleo, gestión laboral y acceso al trabajo</i>	202
IV.3. <i>Servicios esenciales públicos y privados, garantía del cumplimiento del Derecho y en la Administración de Justicia</i>	203
IV.4. <i>Migración, asilo y control fronterizo</i>	203
V. El alcance incierto de las garantías previstas para las biometrías de alto riesgo	204
VI. Recapitulación: alto riesgo no equivale a legitimidad material	205



CAPÍTULO IX

INFRAESTRUCTURAS BIOMÉTRICAS EUROPEAS DE INFORMACIÓN: INTEROPERABILIDAD, FRONTERAS, COOPERACIÓN POLICIAL Y ALCANCE PARCIAL DEL RIA

LEIRE ESCAJEDO SAN-EPIFANIO	207
I. La biometría en las «grandes infraestructuras europeas de información»: planteamiento	208
II. De los sistemas de información a las infraestructuras biométricas europeas	210
III. Los Reglamentos de Interoperabilidad: de la fragmentación informacional al cotejo biométrico compartido	213
III.1. <i>El Portal Europeo de Búsqueda</i>	215
III.2. <i>El Servicio Compartido de Correspondencia Biométrica</i>	216
III.3. <i>El Repositorio Común de Datos de Identidad</i>	217
III.4. <i>El Detector de Identidades Múltiples</i>	218
III.5. <i>Interoperabilidad, finalidad y proporcionalidad</i>	219
IV. Sistemas comprendidos en la arquitectura interoperable: funciones biométricas y relevancia constitucional	220
IV.1. <i>El Sistema de Información de Schengen: cooperación policial, fronteras y biometría de alerta</i>	221
IV.2. <i>Eurodac: de la gestión del asilo a la comparación biométrica ampliada</i>	222
IV.3. <i>El Sistema de Información de Visados: verificación biométrica y política común de visados</i>	223
IV.4. <i>El Sistema de Entradas y Salidas: digitalización del cruce fronterizo</i>	225
IV.5. <i>ETIAS: autorización previa de viaje y conexión con la arquitectura interoperable</i>	226
IV.6. <i>ECRIS-TCN: antecedentes penales, nacionales de terceros países y datos biométricos</i>	227
IV.7. <i>Interpol, Europol y Prüm: conexiones externas y expansión del cotejo automatizado</i>	228



V.	El artículo 111 RIA y el Anexo X: un régimen singular para infraestructuras biométricas estratégicas	229
V.1.	<i>El Anexo X como cartografía de las infraestructuras europeas de identidad, frontera y seguridad</i>	230
V.2.	<i>Cumplimiento diferido y continuidad institucional</i>	231
V.3.	<i>La aplicación del artículo 5 RIA a los sistemas del Anexo X ..</i>	232

PARTE III

REFLEXIONES JURÍDICO-CONSTITUCIONALES SOBRE EL PANORAMA ACTUAL: POR UNA RESPONSABILIDAD PROACTIVA

CAPÍTULO X

MÁS ALLÁ DEL REGLAMENTO EUROPEO DE IA: PRIMACÍA DEL DERECHO DE LA UNIÓN, VIGILANCIA BIOMÉTRICA Y DERECHOS FUNDAMENTALES EN LA ERA ALGORÍTMICA

	LEIRE ESCAJEDO SAN-EPIFANIO	237
I.	La insuficiencia estructural del RIA como instrumento de tutela de derechos fundamentales	238
I.1.	<i>Una lógica tipificadora frente a una lógica material de derechos</i>	239
I.2.	<i>Fragmentación conceptual y riesgos mal captados por las categorías del RIA</i>	240
I.3.	<i>Del control orientado al mercado a la centralidad de la persona</i>	242
I.4.	<i>Jurisprudencia europea y exigencias materiales de protección ..</i>	243
I.5.	<i>Necesidad de un anclaje en el derecho fundamental a la protección de datos</i>	244
II.	La primacía funcional del RGPD: responsabilidad proactiva, gobernanza de la inferencia y papel de las autoridades de protección de datos	245



	<u>Página</u>
II.1. <i>Responsabilidad proactiva y gobernanza algorítmica de la biometría</i>	246
II.2. <i>Evaluación de impacto y control ex ante</i>	246
II.3. <i>Autoridades de protección de datos y control independiente</i> ..	247
II.4. <i>Articulación RGPD-RIA: complementariedad y límites</i>	248
III. De la aprobación normativa a la eficacia material: aplicación, supervisión y riesgo de desactivación del modelo europeo ..	249
III.1. <i>Aplicación coherente y previsibilidad interpretativa</i>	250
III.2. <i>Implementación institucional y coordinación entre autoridades</i>	251
III.3. <i>Estándares, códigos y riesgo de formalización del cumplimiento</i> ..	252
III.4. <i>Grandes sistemas biométricos como prueba de coherencia del modelo europeo</i>	253
III.5. <i>El riesgo de una protección formalmente intensa y materialmente débil</i>	254
IV. Derechos fundamentales y capitalismo de vigilancia: continuidad histórica y mutación estructural	254
IV.1. <i>Continuidad histórica: del control documental a la vigilancia corporal automatizada</i>	255
IV.2. <i>Mutación estructural: inferencia, predicción y modulación de la conducta</i>	256
IV.3. <i>Dignidad, autonomía e identidad frente a la objetivación tecnológica</i>	257
IV.4. <i>Igualdad, sesgos y cuerpos no normativos</i>	258
V. La protección de las personas frente a la vigilancia biométrica estática y dinámica: una tarea constitucional pendiente	259
BIBLIOGRAFÍA Y REFERENCIAS DOCUMENTALES	263
I. Referencias bibliográficas	263
II. Documentos institucionales, normativos y jurisprudenciales	276



Capítulo IV

Del dato biométrico a los sistemas de reconocimiento: conceptos clave para interpretar el RIA

LEIRE ESCAJEDO SAN-EPIFANIO

SUMARIO: I. ¿ES NECESARIA UNA NOCIÓN DE «DATOS BIOMÉTRICOS» MÁS AMPLIA QUE LA DEL ARTÍCULO 4.14 RGPD? LAS INCONSISTENCIAS DEL RIA. I.1. *Antes del RIA: contraste entre la definición del RGPD y las nociones científico-técnicas de datos biométricos.* I.2 *La necesidad de una noción funcional que abarque los datos biométricos con y sin potencial identificante.* II. SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA Y «APLICACIONES BIOMÉTRICAS NO SINGULARIZANTES»: REQUISITOS FUNCIONALES Y LOS LÍMITES CONCEPTUALES. II.1. *Taxonomía de la Biometría (de lo poblacional a lo singular) y primeros sistemas históricos de identificación de humanos en sentido estricto.* II.2. *Clasificación y naturaleza de los datos biométricos en los estudios mensurativos.* II.2.1. *Datos biométricos estáticos: captaciones instantáneas de la anatomía o fisiología corporal.* II.2.2. *Datos biométricos dinámicos: captaciones del cuerpo en lapsos de tiempo.* II.3. *Del dato con potencial singularizante a la construcción de un sistema de identificación: La primera experiencia biométrica en sentido moderno — el sistema antropométrico diseñado por Alphonse Bertillon (el Bertillonage o signalement anthropométrique).* II.4 *Características de los sistemas automatizados de reconocimiento biométrico con potencial singularizante.* II.5. *biometrías inferenciales y reconocimiento de emociones: datos biométricos no orientados a la identificación única.* III. EVOLUCIÓN DE LA NOCIÓN DE DATOS BIOMÉTRICOS EN EL PROCESO DE ELABORACIÓN DEL RIA. IV. LA ARQUITECTURA SUBYACENTE A TODOS LOS SISTEMAS BIOMÉTRICOS. IV.1. *Arquitectura básica de los siste-*



mas de reconocimiento biométrico. IV.2. Fuentes de datos biométricos, datos en crudo y patrones biométricos. IV.3. Utilidades biométricas que identifican, utilidades que no identifican. V. IMPORTANTES LIMITACIONES DE LOS SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO: CIENTÍFICO-TÉCNICAS, DE ARQUITECTURA Y ÉTICO-SOCIALES. VI. REFLEXIÓN SOBRE LA TRANSICIÓN DEL CONCEPTO TÉCNICO A LAS CATEGORÍAS JURÍDICAS DE RECONOCIMIENTO BIOMÉTRICO EN EL RIA.

Si el Capítulo III ofrecía el mapa normativo general del reconocimiento biométrico en el RIA, el presente capítulo se detiene en los conceptos técnicos y jurídicos que permiten interpretar ese mapa: qué debe entenderse por dato biométrico, qué diferencia existe entre fuente, dato en crudo y patrón, cuándo un sistema singulariza a una persona y cuándo, por el contrario, extrae del cuerpo información no identificante. Sin esta precisión conceptual, las categorías del Reglamento —identificación, verificación, categorización, reconocimiento de emociones o sistemas de alto riesgo— pueden resultar equívocas.

El Reglamento (UE) 2024/1689, de Inteligencia Artificial, establece en su artículo 3 un extenso listado de definiciones. Algunas de ellas, como las de *identificación biométrica remota* (tanto en tiempo real como diferida), *categorización* o *perfilado*, serán objeto de un análisis detallado como parte de la tipificación de escenarios fácticos dentro del RIA. Sin embargo, existen otros conceptos de relevancia transversal a lo largo de los artículos relacionados con el reconocimiento biométrico que merecen una consideración temprana y minuciosa. Destaca, en particular, la noción de «datos biométricos» tal como se utiliza en el RIA, que diverge de la definición recogida en el artículo 4.14 del Reglamento (UE) 2016/679, General de Protección de Datos —en adelante, RGPD—. Igualmente relevante es el concepto de «verificación biométrica», una categoría que el RIA busca distinguir persistentemente de la identificación biométrica, especialmente en su forma remota (Comisión Europea, 2021).

Dentro del marco regulatorio y técnico, la *verificación biométrica* denota específicamente un proceso uno-a-uno destinado a confirmar la identidad de un individuo mediante la comparación de una muestra biométrica presentada con una plantilla almacenada, para verificar que el sujeto es quien dice ser (Jain, Ross y Nandakumar, 2011). En contras-



te, la *autenticación biométrica* abarca un espectro más amplio de procedimientos de validación de identidad que pueden combinar la verificación con métodos adicionales para establecer o corroborar la identidad (Jain *et al.*, 2011). La tipología del RIA enfatiza la verificación como el principal mecanismo procedimental para garantizar la coincidencia precisa de los datos biométricos, aunque las matizaciones conceptuales entre verificación y autenticación siguen siendo críticas para la interpretación y aplicación jurídica (Comisión Europea, 2021). Las fronteras entre verificación, autenticación e identificación no siempre resultan plenamente nítidas en la práctica.

I. ¿ES NECESARIA UNA NOCIÓN DE «DATOS BIOMÉTRICOS» MÁS AMPLIA QUE LA DEL ARTÍCULO 4.14 RGPD? LAS INCONSISTENCIAS DEL RIA

I.1. ANTES DEL RIA: CONTRASTE ENTRE LA DEFINICIÓN DEL RGPD Y LAS NOCIONES CIENTÍFICO-TÉCNICAS DE DATOS BIOMÉTRICOS

Se advertía en la introducción que, hasta la aprobación del RIA, la noción jurídica más relevante de «datos biométricos» era la recogida en el número 14, artículo 4, del RGPD. El último inciso del art. 4.14 RGPD será excluido de nuestra reflexión, porque resulta un tanto desafortunado. En él, los legisladores presentan como ejemplos de datos biométricos las imágenes faciales y los datos dactiloscópicos (Romeo Casabona, 2021, 709-710). No obstante, por sí mismos, ni la foto de un rostro ni la información dactiloscópica —incluyendo una impresión de huellas— son en puridad datos biométricos. Son, cierto es, posibles fuentes de datos biométricos, pero será un tratamiento mensurativo lo que determinará si se obtienen o no de ellas datos biométricos singularizantes (Kindt, 2018; Romeo Casabona, 2021, pp. 709-710).

Excluido, por tanto, ese inciso ejemplificativo, cabe recordar que, conforme al RGPD, son datos biométricos los «datos personales 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). Procede ahora comparar esta noción, a partir de la cual el RGPD establece una categoría de datos especialmente protegidos, con una definición científico-técnica de datos biométricos coherente con la disciplina de la Biometría.



Antes incluso de la aprobación del RGPD, diferentes expertos venían advirtiéndolo ya sobre la distancia entre, de una parte, las nociones de datos biométricos recogidas en diferentes documentos jurídicos fueran vinculantes o no, y, de otra parte, el concepto de datos biométricos en perspectiva científica (Jasserand, 2016). Como señalaron Kindt y Jasserand (Jasserand, 2016; Kindt, 2018), existía una notable desalineación entre las posibilidades tecnológicas y la definición legal, problema que se vio agudizado con la aprobación del RGPD. En ese sentido, Kindt (2013, p. 11) propone definir los datos biométricos como «todos los datos personales que (a) se relacionan directa o indirectamente con características biológicas o de comportamiento únicas o distintivas de los seres humanos y (b) se utilizan o son aptos para ser utilizados por medios automatizados (c) para fines de identificación, verificación de identidad o verificación de una reclamación de personas físicas vivas», si bien por «personales» se refiere a procedentes de personas y no, por tanto, a datos que encajen necesariamente en la definición de datos personales del RGPD.

Por nuestra parte, venimos defendiendo la siguiente definición para la noción científico-técnica de datos biométricos postulando, además, que es deseable que progresivamente vaya siendo tenida en cuenta al diseñar los marcos reguladores de las técnicas de reconocimiento biométrico (Escajedo San-Epifanio, 2024): son datos biométricos aquellos que se obtienen del cuerpo de las personas como expresión de algún tipo de estudio mensurativo y, en su vasto conjunto, resulta relevante la distinción de dos grandes grupos, según se trate de datos que han sido obtenidos de biometrías estáticas o de biometrías dinámicas (Escajedo San-Epifanio, 2017, pp. 100-101).

Las biometrías estáticas agrupan aquellos métodos que captan información métrica puntual a partir de las características anatómico-físicas de un cuerpo humano. Las biometrías dinámicas, por su parte, comprenden los métodos que se aplican para captar de un cuerpo humano información secuencial o cíclica de las habilidades motoras, así como de las señas y parámetros corporales en sentido amplio, ya sea en sus dimensiones externa o interna, voluntaria o involuntaria.

Nótese, porque la distinción tendrá relevancia, que las biometrías estáticas y las dinámicas se diferencian por dos aspectos clave: en primer lugar, por el tipo de fuentes de las que obtienen información (características anatómico-físicas frente, de algún modo, al cuerpo en funcionamiento); y en segundo lugar, por el hecho de que la captación de las biometrías estáticas puede realizarse en un instante, mientras que la captación de las biometrías dinámicas requiere un mayor o menor lapso de tiempo. Dicho de otro



modo, las biometrías que captan el patrón de una huella dactilar o un iris, así como la geometría de un rostro, actúan sobre un dato en crudo puntual. Se extrae, por ejemplo, una impresión dactilar de los dermatoglifos de un dedo y esa impresión es suficiente como para dar comienzo al proceso de biometrización de los atributos que singularizan esa huella respecto a otras. Las tecnologías basadas en biometrías dinámicas, en cambio, como es el caso de las que analizan el espectro de la voz de una persona, el patrón de su marcha al caminar o la velocidad de sus latidos, son tecnologías que necesitan poder captar información de la fuente durante un lapso más o menos largo de tiempo.

I.2 LA NECESIDAD DE UNA NOCIÓN FUNCIONAL QUE ABARQUE LOS DATOS BIOMÉTRICOS CON Y SIN POTENCIAL IDENTIFICANTE

Según la Exposición de Motivos de la propuesta de RIA, este reglamento viene a completar —sin desplazar— el marco de garantías que ya recogen, entre otros, textos jurídicos como el RGPD. Respecto a este último, dice también la Exposición de Motivos, el RIA viene a ser una *lex specialis*, pero con un carácter fundamentalmente complementario. A pesar de esa afirmación, sin embargo, en el caso concreto del uso que se da en el RIA a la noción de datos biométricos, con una definición propia, la diferencia respecto al RGPD es muy relevante (Czarnocki, 2021: 1-4). Se describirá tal diferencia en este apartado, dejando para el apartado III tanto el modo en que Comisión, Parlamento y Consejo propusieron respectivamente atender a esta circunstancia, como la opción que se incorporó finalmente al RIA.

Aunque repite el criticado inciso final del art. 4.14 RGPD, al que nos hemos referido ya, la noción de datos biométricos que emplea el RIA se distingue de aquella en que se ha eliminado la exigencia de que se trate de datos que permitan o confirmen «la identificación única de una persona». En consecuencia, en el conjunto de datos que pueden emplearse en los sistemas de reconocimiento biométrico habrá datos sujetos al ámbito de aplicación del RGPD en tanto puedan considerarse personales, siendo algunos de ellos, además, pertenecientes a la categoría de especial protección (art. 9 RGPD). Por cuanto respecta al RIA, por su parte, algunas dimensiones del tratamiento de datos biométricos quedarán sujetas a su aplicación —con independencia de que se trate o no de datos singularizantes e, incluso, sin necesidad de que se trate de datos personales— y, al mismo tiempo, los sistemas de IA de verificación que emplean datos biométricos de categoría



especial (arts. 4.14 y 9 del RGPD) quedarán excluidos del RIA. En términos de garantías, ha de decirse, esta sistemática —con el añadido de la complicada redacción de algunos artículos del RIA— resulta bastante preocupante.

En este contexto se hace necesario realizar una serie de anotaciones sobre las características que deben reunir los sistemas de reconocimiento biométrico que pretenden ofrecer una funcionalidad de identificación (o singularización de identidad), frente a las características de aquellos sistemas que captan otro tipo de informaciones biométricas no singularizantes.

II. SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA Y «APLICACIONES BIOMÉTRICAS NO SINGULARIZANTES»: REQUISITOS FUNCIONALES Y LOS LÍMITES CONCEPTUALES

En este contexto, resulta imprescindible precisar qué características deben concurrir para que un sistema de reconocimiento biométrico pueda ofrecer propiamente una funcionalidad de identificación —o singularización de identidad— y distinguirlo de aquellos sistemas que captan información biométrica sin finalidad identificante. La diferencia no es meramente terminológica. De ella dependen el alcance funcional del sistema, sus implicaciones jurídicas y la intensidad de los riesgos para los derechos fundamentales.

Los sistemas orientados a identificar o verificar a una persona física operan sobre una lógica de singularización: comparan datos captados en fresco con datos previamente registrados o almacenados, con el fin de confirmar o determinar una identidad. En cambio, otras aplicaciones biométricas no buscan establecer quién es una persona, sino captar atributos, estados, rasgos o patrones que permitan clasificarla, evaluarla o inferir determinadas informaciones sobre ella. Esta distinción resulta decisiva para una interpretación adecuada del Reglamento (UE) 2024/1689, de Inteligencia Artificial, y para comprender los límites del paradigma identificante que ha dominado hasta ahora la regulación europea de la biometría.

II.1. TAXONOMÍA DE LA BIOMETRÍA (DE LO POBLACIONAL A LO SINGULAR) Y PRIMEROS SISTEMAS HISTÓRICOS DE IDENTIFICACIÓN DE HUMANOS EN SENTIDO ESTRICTO

La medición aplicada a seres vivos y su posterior procesamiento matemático han dado lugar a un amplio espectro de categorías biométricas, cuya sistematización resulta compleja. En este marco, destacan dos clasifi-



caciones particularmente útiles para la exposición de los resultados. Por un lado, la tipología tripartita propuesta por Irwin en 1959, basada en el tipo de muestra poblacional utilizada; por otro, la diferenciación entre datos biométricos estructurales y dinámicos, formulada también como distinción entre datos físicos y comportamentales por diversos autores.

Según Irwin (1959), los estudios biométricos pueden dividirse en tres categorías, atendiendo al objeto de medición. La primera incluye aquellos estudios que implican la toma de medidas sobre amplias poblaciones o incluso poblaciones enteras. La segunda se refiere a estudios centrados en pequeños grupos de individuos. La tercera agrupa los estudios que recogen datos biométricos de individuos identificados. Estos últimos incluyen tanto información de perfil singularizante como biomarcadores, que abarcan desde medidas macroscópicas, como la altura o el peso, hasta otras que requieren instrumentación específica o análisis de laboratorio, como la hematimetría.

En la década de 1960, la biometría aún se centraba principalmente en la caracterización de poblaciones. Sin embargo, a partir de experiencias como las de Bertillon, se consolida una nueva orientación: la identificación individual (Aparicio Salom, 2013). Esta evolución sienta las bases para el desarrollo de infraestructuras informáticas que, con mayor precisión y velocidad, siguen basándose en la comparación entre los rasgos del individuo y aquellos previamente registrados y almacenados. En la actualidad, la asociación entre biometría y sistemas de reconocimiento resulta tan predominante que tiende a constituir la acepción principal del término «dato biométrico» (Kindt, 2013; Jasserand, 2016).

II.2. CLASIFICACIÓN Y NATURALEZA DE LOS DATOS BIOMÉTRICOS EN LOS ESTUDIOS MENSURATIVOS

Dentro del ámbito de los estudios mensurativos, los datos biométricos presentan distintos grados de potencial singularizante, que dependen tanto de las propiedades intrínsecas de la información captada como de las técnicas y métodos empleados para su obtención. Esta variabilidad permite clasificar los datos biométricos en categorías diferenciadas según el tipo de rasgo analizado y el modo en que se registra la información.

El potencial singularizante no se basa solo en el grado de unicidad del dato en sí mismo —entendido como las diferencias objetivas existentes en un rasgo humano susceptible de ser captado—, sino también en la dispo-



nibilidad y eficacia de los sistemas tecnológicos que permiten captar ese potencial con mayor o menor precisión. En este sentido, la capacidad técnica para detectar variaciones sutiles puede potenciar significativamente el valor singularizante de ciertos datos biométricos (Jain *et al.*, 2011; Maltoni *et al.*, 2009).

II.2.1. Datos biométricos estáticos: captaciones instantáneas de la anatomía o fisiología corporal

Los denominados datos biométricos anatómico-físicos son aquellos que se obtienen en un momento puntual, a partir de características anatómico-físicas del cuerpo humano. Es precisamente la conjunción de estos dos elementos —el carácter estático de la recogida y la referencia a la estructura corporal— lo que permite distinguir este conjunto de datos respecto del segundo grupo que se examinará a continuación.

Entre los ejemplos más representativos de esta categoría se encuentran las huellas dactilares, la geometría de la mano, los patrones del iris y del fondo venoso de la retina, así como la composición química del olor corporal. En todos estos casos, en un momento concreto se extrae una muestra biométrica —o dato en crudo— que sirve de base para realizar el análisis mensurativo y, a partir de él, obtener el patrón biométrico correspondiente. En consecuencia, se incluyen en esta categoría todos aquellos parámetros corporales que puedan registrarse de forma estática, esto es, sin necesidad de observar un proceso en el tiempo. A diferencia de ello, como se verá a continuación, los datos que requieren algún tipo de monitorización o registro prolongado de la actividad corporal del sujeto se ubican en otra categoría, que implica una aproximación sustancialmente distinta.

II.2.2. Datos biométricos dinámicos: captaciones del cuerpo en lapsos de tiempo

La biometría dinámica, también denominada comportamental, constituye el conjunto más complejo de datos en este ámbito. Inicialmente, el Grupo de Trabajo del Artículo 29 (GT29) aludió a *características físicas, fisiológicas y comportamentales* como *fuentes de datos biométricos*, sin ofrecer todavía una taxonomía cerrada entre biometrías estáticas y dinámicas. Posteriormente, en 2012, el propio Grupo amplió esta caracterización aludiendo a «*fuentes biométricas dinámicas*». No obstante, más allá de estas definiciones preliminares, no existe aún una categorización consensuada, y la



literatura especializada mantiene posturas divergentes en torno a la asignación de determinados datos biométricos a una u otra categoría.

En términos generales, se tiende a agrupar bajo la etiqueta de biometría dinámica aquellos datos que no derivan directamente de un rasgo físico estático. Sin embargo, se mantiene cierta controversia respecto a la clasificación de las señales corporales o de aquellos datos que, si bien provienen del cuerpo, exigen una medición continua o contextualizada. Esta heterogeneidad ha llevado a reunir en un mismo conjunto informaciones que presentan notables diferencias en cuanto a origen, naturaleza y modo de captura.

Algunas de las descripciones más detalladas de esta categoría han sido ofrecidas por la Agencia de Ciberseguridad de la Unión Europea (ENISA) y por autores como Yampolskiy y Govindaraju. Ambos enfoques identifican tres grandes subconjuntos: por un lado, los datos obtenidos del control motor voluntario, como el modo de firmar, escribir, hablar, gesticular o utilizar dispositivos como teclados o ratones; por otro, las señales fisiológicas, que incluyen variables como el ritmo cardíaco, la temperatura corporal, la actividad cerebral (EEG), la frecuencia respiratoria, el parpadeo, la sudoración o el temblor. Un caso paradigmático de esta segunda subcategoría es el proyecto FAST del Departamento de Seguridad Interior de los Estados Unidos, diseñado para identificar intenciones hostiles a partir de patrones fisiológicos y comportamentales. Finalmente, un tercer subconjunto estaría constituido por la información generada en la interacción con dispositivos o entornos automatizados, como pueden ser programas informáticos, videojuegos, plataformas de comercio electrónico o análisis lingüísticos de correos electrónicos y conversaciones.

A nuestro juicio, esta triple subdivisión puede reducirse con mayor claridad a dos fuentes principales de captación de datos: por una parte, las habilidades motoras; por otra, las señales y parámetros corporales. En ambos casos, la información relevante se genera a lo largo de un intervalo temporal, como resultado de la actividad fisiológica del cuerpo humano. En cuanto al tercer grupo, consideramos que los datos derivados de la interacción con dispositivos automatizados pueden reconducirse a alguno de los dos anteriores, en función de si la interacción revela habilidades motoras o expresiones fisiológicas que sean objeto de captación biométrica.

Conviene señalar, además, que tanto las habilidades motoras como las señales fisiológicas pueden ser registradas con o sin intervención activa del sujeto. Por ello, no resulta adecuada la distinción entre características «acti-



vas» y «pasivas» como criterio clasificatorio entre fuentes de datos estáticos y dinámicos. Tal dicotomía podría inducir a confusión, en la medida en que tanto en el ámbito de la biometría anatómico-física como en el de la dinámica, es posible captar información sin que el sujeto deba realizar una acción consciente o voluntaria.

II.3. DEL DATO CON POTENCIAL SINGULARIZANTE A LA CONSTRUCCIÓN DE UN SISTEMA DE IDENTIFICACIÓN: LA PRIMERA EXPERIENCIA BIOMÉTRICA EN SENTIDO MODERNO - EL SISTEMA ANTROPOMÉTRICO DISEÑADO POR ALPHONSE BERTILLON (EL BERTILLONAGE O SIGNALEMENT ANTHROPOMÉTRIQUE)

Aunque investigadores como Francis Galton centraron su atención en estudios poblacionales —más que en la identificación de individuos singulares—, los trabajos que abordaban rasgos mensurables de los seres humanos, ya fueran físicos o conductuales, advertían frecuentemente sobre el potencial de la biometría para el reconocimiento individual. Este es el caso, entre otros, de las investigaciones de antropólogos como Paul Broca, fundador de la Sociedad de Antropología de París. Antes incluso de que Galton acuñara el término «biometría», Broca empleaba mediciones y cálculos estadísticos para describir las características de grupos humanos.

En lo que respecta específicamente a la toma de medidas con fines identificativos, la figura clave es un discípulo de su escuela: Alphonse Bertillon. El sistema antropométrico de identificación de delincuentes diseñado por Bertillon constituye un hito fundamental en la aplicación histórica de la biometría con el propósito de evitar agravantes penales derivados de la reincidencia. En Francia, la abolición de la marca de fuego para condenados, el 31 de agosto de 1832, complicó la tarea de identificar reincidentes, ya que la única referencia para ello eran los archivos documentales, cuya consulta era poco práctica y vulnerable a engaños, dado que los delincuentes reincidentes solían falsear su identidad para eludir sanciones más severas (Auger, 2005).

Esta dificultad contribuyó a la creación de un cuerpo especializado dentro de la policía: la llamada policía técnica (Dias, 2000: 12). A finales del siglo XIX, los archivos judiciales franceses contenían datos de más de cinco millones de personas, pero el acceso a la información era ineficiente, dado que las fichas estaban organizadas alfabéticamente en formato papel. En caso de que un detenido no facilitase su nombre real o lo falseara, la posi-



bilidad de relacionarlo con una ficha dependía de circunstancias fortuitas, como el testimonio de testigos o indicios relacionados con su identidad. Fue el reconocimiento mediante características físicas el que permitió avances significativos en estas tareas.

Alphonse Bertillon, hijo del antropólogo y estadista Louis Adolphe Bertillon —miembro fundador de la Escuela de Antropología de París fundada por Broca (Spencer, 1997)—, ingresó en 1879 en la Prefectura de Policía de París con la misión de elaborar fichas «signaléticas» detalladas de individuos (Madureira, 2005; Bertillon, 1896). Su sistema, conocido como *signalement anthropométrique*, combinaba medidas antropométricas con descripciones detalladas, fotografías y anotaciones sobre marcas individuales como tatuajes y cicatrices, siguiendo técnicas desarrolladas por Broca y colaboradores en el Laboratorio de Antropología de la *École Pratique des Hautes Études* de París.

Bertillon estaba influenciado también por los trabajos de Lambert Quetelet, quien sostenía que *no existen dos esqueletos humanos con medidas idénticas*, y demostró que ciertos huesos no sufren cambios significativos tras los 20 años de edad. Así, su sistema no era simplemente un método métrico, sino que vinculaba las descripciones físicas con un sistema organizado de clasificación, que facilitaba la consulta manual de la base de datos (Stiegler, 1999; Hacking, 1990; Cole, 2001).

Entre sus obras más relevantes destacan *La photographie judiciaire* (1890) y *L'Anthropologie métrique* (1909). Este sistema fue ampliamente adoptado en Occidente antes de la introducción de la dactiloscopia y consistía en la toma de múltiples medidas corporales —como la envergadura, el tamaño del cráneo, la longitud del codo, pies u orejas— para identificar a los detenidos. En Reino Unido, Edward Henry introdujo el método en Scotland Yard, complementándolo con fichas detalladas que incluían, por ejemplo, la longitud de los dedos (Trucco, 2004).

En la narrativa histórica del reconocimiento mediante Biometría se ha venido insistiendo de forma recurrente en cómo *el caso de los dos Will West* (Will y William West) supuso la crisis definitiva del Bertillonage y su sustitución por la identificación mediante la impresión dactilar. En la actualidad se revisa críticamente esta forma de narrar los hechos, advirtiendo de que los datos sobre lo acontecido y sus consecuencias fueron publicados en las primeras décadas del siglo XX, en un momento en el que, de forma interesada, algunos sectores doctrinales querían impulsar definitivamente el uso de las huellas dactilares en la identificación.



Ciertamente, el *Bertillonage* planteaba dificultades relacionadas con la calidad de la toma de medidas y el hecho de que en algunos lugares se empleasen unidades métricas diferentes. Carecemos, sin embargo, de estudios que nos permitan conocer con detalle cuál era la tasa de error en la aplicación del *Bertillonage* y desconocemos, asimismo, qué porcentaje de los errores se debía al método y cuál a la falta de pericia de quien tomaba las medidas.

Muy distinto es lo sucedido en el *caso West*, en el que el capricho del azar atrajo una serie de circunstancias cuyo concurso, a todas luces, parecía extremadamente improbable. En el año 1903 llegó a la prisión de Leavenworth un nuevo recluso: *Will West*. Él insistía en que nunca antes había estado en dicha prisión, pero una persona de la secretaría de la administración decía conocerle sin el menor atisbo de duda. Analizados los ficheros, se obtuvo la ficha de un recluso anterior, que no solo tenía las mismas medidas craneales que Will, sino que —como muestran las fotografías de la época— guardaba con él un asombroso parecido (Shoninregun/Crossier, 2008)

Por si ello fuera poco, el nombre recogido en aquella ficha no era otro que West, *William West*. La probabilidad de que existieran dos delincuentes, encarcelados en un relativamente breve lapso de tiempo en la misma prisión estadounidense, y que además coincidieran no solo en medidas craneales sino también en el nombre se consideraba algo tan remoto, que es comprensible que en primer término se concluyera que se trataba de una única persona. Solo la comparación de las huellas dactilares de Will con las de la ficha de William fue la que determinó que se trataba de dos personas diferentes.

Coincidimos, con Simon A. Cole (Cole, 2002), en que no fue el caso de *los dos Will West* lo que desbancó al *Bertillonage*. A pesar de la identidad de medidas craneales, las fichas de ambos mostraban diferencias destacables en otras medidas corporales —como, por ejemplo, las medidas de los pies—. Al parecer, el mito se creó veinte años después del suceso, para impulsar el uso de las huellas dactilares y alentado por voces que afirmaban que el *Bertillonage* —de origen europeo— no era adecuado para distinguir a los delincuentes de raza afroamericana o asiática, estadísticamente más frecuentes en el territorio norteamericano. Es fácil apreciar que, comparativamente, la obtención, clasificación, almacenamiento y comparación de las huellas dactilares resultaba mucho más sencilla que el *Bertillonage*, y que además facilitaba la distinción entre hermanos o gemelos que guardaban importantes semejanzas físicas.



Fue esa constatación la que progresivamente fue haciendo que las medidas antropométricas dejaran de ser la única base de identificación policial y progresivamente se completasen con otros tipos de datos. Debe tenerse en cuenta, además, que si bien desde la década de 1880 existían referencias —aún sin método— sobre la posibilidad de una identificación cuantitativa de los individuos a través de sus huellas, de autores como Henry Faulds, William Herschel o Francis Galton (Faulds, 1880; Galton, 1888; Herschel, 1880; mayo *et al.*, 2008), hubo que esperar aún unos años para que se propusieran métodos de obtención, clasificación y gestión de este tipo de muestras. La madurez de estos sistemas (como los de Vučetič o, en España, Federico Oloriz Aguilera) coincidió temporalmente con *el caso West*, lo que sirvió de caldo de cultivo a la leyenda (Escajedo San-Epifanio, 2017). En los países anglosajones se había ido extendiendo el sistema que Scotland Yard adoptó en 1901, con una oficina de huellas dactilares dirigida por Edward Henry. Éste había desarrollado un sistema de clasificación de las huellas cuando era administrador en Bengala (India) y completó el sistema propuesto por Galton, dando lugar al que se conoce como sistema *Galton - Henry*. En Alemania se había adoptado el sistema de Roscher.

Con una base científica muy similar, aunque instrumentalizada de otro modo, llegaron los sistemas de reconocimiento automatizado. Desde hace ya más de dos décadas, los sistemas de reconocimiento biométrico contemporáneo son descritos en la literatura como «métodos automatizados de verificación o reconocimiento de la identidad de una persona viva con base en características fisiológicas o comportamentales» (Wayman *et al.*, 2008, pp. 1-2), descripción en la que destaca por su novedad el componente de automatización (Biometrics Institute, 2006; IBG, 2001; OCDE, 2004, pp. 10-11; Nanavati *et al.*, 2002; Sethi, 2006, pp. 117-134), aunque destaca también el objetivo de identificación que se atribuye a estas técnicas.

Ello explica que algunos autores, como Meuth (Meuth, 2005; 35-36), hablen de una *Biométrica* como ciencia emparentada —aunque diferente— respecto a la biometría, definiéndola como «la ciencia del establecimiento de la identidad de un individuo con base en sus atributos físicos, químicos o comportamentales» o «la ciencia de emplear información biológica con fines de identificación o verificación» (Magnet, 2011, 21).

Por otra parte, y aunque suele hacerse referencia abreviada al conjunto de estas tecnologías como *biometrics* o *biometric technologies*, en opinión de autores destacados como James Wayman o Anil K. Jain, bien pudiéramos referirnos a estos sistemas como una «autenticación antropométrica» automatizada, en el sentido de que: en primer lugar, en la actualidad que-



dan fuera de este conjunto aquellos métodos de identificación forense que no disponen aún de versiones tecnológicas (Meuth, 2005); y, en segundo lugar, en tanto estos sistemas se emplean en una única especie: la humana. La propuesta terminológica ISO de 2012 matiza, además, que la expresión verificación o reconocimiento es más correcta que autenticación, lo cual nos dejaría el concepto en «reconocimiento antropométrico automatizado».

II.4 CARACTERÍSTICAS DE LOS SISTEMAS AUTOMATIZADOS DE RECONOCIMIENTO BIOMÉTRICO CON POTENCIAL SINGULARIZANTE

Los sistemas de reconocimiento con potencial de identificación única solo pueden asentarse sobre conjuntos de datos biométricos que reúnen una serie de características, a las que la literatura se refiere como los *seven pillars* (Escajedo San-Epifanio, 2017, pp. 88-98), entre las que destacan la universalidad, el potencial singularizante, la inherencia o la permanencia. Un sistema de reconocimiento biométrico con potencial singularizante debe asentar su base en una característica o atributo que sea *universal*, en el sentido de que la fuente de información biométrica esté, en principio, disponible en todos los seres humanos (o con muy pocas excepciones).

A esa universalidad ha de añadirse, además, que la fuente de información debe permitir captar en ella la *presencia de elementos singularizantes*. Los dedos de las manos tienen una presencia prácticamente universal y la mayoría de las personas tienen en ellos dermatoglifos, o pliegues de la piel, que dejan huellas dactilares en su contacto con las superficies. Un sistema de reconocimiento biométrico que cuantifique el número de dedos en la mano derecha no resulta lo suficientemente singularizante, por la elevada coincidencia de la cantidad de cinco dedos en la mayoría de las manos humanas. El caso de los dermatoglifos, en cambio, es diferente. Se trata de una fuente de información en la que podemos captar una singularidad tan elevada que, estadísticamente, se considera improbable que existan dos dedos —incluso en la misma persona— con una huella idéntica. Eso hace que la biometría dactilar sea de un elevado potencial singularizante, potencial que además puede captarse. Esa circunstancia contrasta, por ejemplo, con el ADN, que, siendo muy singularizante en los humanos, en la actualidad no puede captarse y procesarse de forma automatizada.

Para servir de soporte a un sistema de identificación, por último, es también muy relevante que la información biométrica de referencia sea una información *inherente* al cuerpo de la persona —o al menos razona-



blemente difícil de modificar o suplantar a voluntad— y que *permanezca* a pesar del paso del tiempo (IPTs, 2005, p. 37; Mordini *et al.*, 2021; Zhang *et al.*, 2013). La permanencia no se exige en términos absolutos, sino más bien en el sentido de que tenga una estabilidad suficiente como para que pueda ser útil para *reidentificar* a la persona transcurrido un período razonable de tiempo.

El patrón de pabellón auricular, por ejemplo, permanece a pesar de que el tamaño de la oreja varíe con la edad. Puede ponerse también el ejemplo de la imagen del DNI, que no es biométrica pero sí fuente de datos. Esta imagen, por los requisitos con los que es tomada, se estima que razonablemente puede servir para reidentificar a alguien dentro de un período de diez años desde su emisión o, incluso, durante más tiempo cuando la persona ha alcanzado cierta edad; de ahí la emisión de un DNI permanente a partir de los 70 años.

La permanencia permite garantizar que el esfuerzo de desplegar un sistema de identificación biométrica en sentido estricto se verá compensado con la posibilidad de emplearlo de forma dilatada en el tiempo. Respecto a otros atributos biometrizables, la universalidad y facilidad de captación contrastan con la escasa permanencia de los datos obtenidos. Condiciones ambientales y/o temporales impactan de forma relevante en esos datos (Escajedo San-Epifanio, 2017, pp. 93-96). Por ejemplo, el peso de una persona o la longitud de su cabello (salvo que carezca de este) son fáciles de medir, pero en una misma persona están sometidos a una importante variabilidad a lo largo de su vida. No tendría sentido construir un sistema de identificación única sobre la base de datos de esas características. Los dermatoglifos, sin embargo, terminan de formarse hacia el tercer o cuarto mes del desarrollo fetal y se mantienen —salvo lesiones externas— a lo largo de toda la vida de la persona, pudiendo incluso ser captados en algunos estadios post-mortem. De hecho, la disciplina científica de la necropapiloscopia dispone de técnicas para la captación que pueden, incluso, aplicarse a dedos petrificados o momificados (Alegretti *et al.*, 2007).

II.5. BIOMETRÍAS INFERENCIALES Y RECONOCIMIENTO DE EMOCIONES: DATOS BIOMÉTRICOS NO ORIENTADOS A LA IDENTIFICACIÓN ÚNICA

Por cuanto se refiere a las categorizaciones no identificantes y, en especial, al reconocimiento de emociones, los sistemas que aplican este tipo de modalidades tienden a emplear biometrías débiles (*soft biometrics*), con bajo



rango de permanencia y reducido potencial identificante (Dantcheva *et al.*, 2016; Reid *et al.*, 2014).

El caso de las emociones es especialmente ilustrativo. Desde los trabajos fundacionales sobre *affective computing*, se ha explorado la posibilidad de que los sistemas computacionales detecten, clasifiquen o respondan a estados afectivos humanos a partir de señales corporales, faciales, vocales o fisiológicas (Picard, 1997, 2003; McStay, 2018). Ahora bien, este tipo de tratamiento no responde ya al paradigma clásico de la identificación. Su finalidad no es determinar quién es una persona, ni confirmar que es quien dice ser, sino producir una inferencia sobre su estado corporal, emocional, atencional o conductual.

La relevancia jurídica de estas prácticas no deriva, por tanto, de su capacidad de identificar, sino de su capacidad reveladora e inferencial. El riesgo no reside únicamente en saber quién es la persona, sino en producir conocimiento operativo sobre ella a partir de su cuerpo y utilizarlo para clasificarla, evaluarla o modular el entorno en el que actúa (Wachter y Mittelstadt, 2019).

Esta cuestión es especialmente delicada porque la correspondencia entre expresiones faciales y emociones discretas no puede asumirse como una relación universal, estable ni científicamente pacífica. La literatura psicológica reciente ha cuestionado la tesis de que las emociones puedan inferirse de forma fiable a partir de configuraciones faciales aisladas, especialmente fuera de contextos experimentales controlados (Barrett *et al.*, 2019; Crawford, 2021).

Desde esta perspectiva, la biometría inferencial plantea un doble problema: por un lado, puede no identificar singularmente a la persona; por otro, puede producir efectos jurídicamente relevantes mediante inferencias inciertas, sesgadas o descontextualizadas. Esa combinación muestra los límites del paradigma identificante que estructura buena parte del RGPD y del RIA (Kindt, 2013; Jasserand, 2016). Esta dimensión resulta especialmente significativa en los sistemas de inteligencia artificial que operan en tiempo real o cuasi real. A diferencia de la biometría estática orientada a la identificación, las biometrías inferenciales suelen basarse en el cuerpo en funcionamiento: microexpresiones faciales, tono de voz, ritmo de habla, cadencia de tecleo, movimientos oculares, postura corporal, frecuencia cardíaca o señales fisiológicas. La captación se despliega durante un lapso temporal y permite construir inferencias dinámicas, no siempre perceptibles para la persona afectada.



La ausencia de identificación singular no elimina el riesgo. En estos sistemas, la persona puede no ser identificada como individuo único, pero sí individualizada funcionalmente y situada en categorías dinámicas que condicionan el trato recibido. Desde la perspectiva del RGPD, estas prácticas pueden encajar en la definición de perfilado del artículo 4.4 cuando implican la evaluación automatizada de aspectos personales relativos a una persona física. Lo relevante no es que el sistema conozca el nombre del sujeto, sino que utilice información referida a él para evaluarlo, clasificarlo o influir en su entorno de interacción (Wachter y Mittelstadt, 2019).

Esta constatación obliga a relativizar el peso del criterio identificante. El artículo 4.14 RGPD vincula la categoría específica de «datos biométricos» a aquellos datos personales obtenidos a partir de un tratamiento técnico específico relativos a características físicas, fisiológicas o conductuales que *permitan o confirmen la identificación única de una persona física*. Sin embargo, los tratamientos biométricos no identificantes pueden generar riesgos elevados para los derechos fundamentales aun cuando no activen la protección reforzada propia de los datos biométricos identificantes.

El RIA sí ha reconocido parcialmente esta realidad al regular, de forma diferenciada, los sistemas de reconocimiento de emociones y los sistemas de categorización biométrica. No obstante, su técnica regulatoria sigue siendo fragmentaria. Determinadas modalidades quedan prohibidas en contextos específicos —como el reconocimiento de emociones en centros de trabajo y educativos, salvo motivos médicos o de seguridad—, mientras que otras se reconducen a categorías de alto riesgo o quedan sometidas a obligaciones más débiles. El resultado es una cobertura desigual de la biometría inferencial.

Por ello, la distinción entre datos biométricos singularizantes y datos biométricos no singularizantes no debe interpretarse como una distinción entre tratamientos jurídicamente relevantes y tratamientos irrelevantes. Más bien permite identificar dos formas distintas de riesgo. En los sistemas de identificación, el riesgo principal se vincula a la singularización, la trazabilidad y la posible vigilancia de la identidad. En las aplicaciones inferenciales, el riesgo se desplaza hacia la clasificación, la evaluación probabilística, la influencia sobre la conducta y la pérdida de control sobre informaciones corporales que la persona no puede dejar de emitir sin abandonar el entorno de interacción. La inferencia biométrica de emociones revela así los límites del paradigma identificante. El cuerpo ya no es solo fuente de identidad; se convierte también en fuente de predicción, categorización y modulación conductual. Esta transformación exige una lectura



jurídico-material de la biometría, atenta no solo a la identificación única, sino también a la capacidad de los sistemas para extraer conocimiento del cuerpo y producir efectos relevantes sobre la autonomía, la igualdad y la autodeterminación informativa.

III. EVOLUCIÓN DE LA NOCIÓN DE DATOS BIOMÉTRICOS EN EL PROCESO DE ELABORACIÓN DEL RIA

Por si en algún momento se revisa la descoordinación actual entre las nociones de datos biométricos respectivamente previstas en el RIA y el RGPD, resulta de interés señalar cómo se fraguó la noción finalmente incorporada al RIA. Comisión, Parlamento y Consejo ofrecieron diferentes alternativas, que se analizarán, aunque, sorprendentemente, en algún momento de los trilogos terminó imponiéndose una noción que dice inspirarse en el RGPD, pero, como se ha avanzado ya, en realidad se aleja de éste.

El considerando 7.º de la Propuesta de la Comisión recogía que su noción de «datos biométricos» coincidía con la noción de «datos biométricos» definida en el artículo 4, punto 14 RGPD, en el artículo 3, punto 18, del Reglamento (UE) 2018/1725 y en el artículo 3, punto 13, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Se indicaba, en coherencia, que tal noción debía interpretarse en consonancia con la del RGPD. En sí misma, la noción no planteaba dudas. Resultaba problemático, no obstante, que ni esta ni otras nociones atendieran al hecho de que mediante la IA era posible el tratamiento de datos biométricos no identificantes.

El Parlamento, por su parte, sí atendió esta última necesidad. La noción de datos biométricos que adoptó en su postura coincidía literalmente con la de la Comisión, pero propuso añadir un nuevo concepto al listado de definiciones del art. 3. RIA: el concepto de *datos de base biométrica*. Esta segunda noción, diferenciada de la noción de *datos biométricos*, se propone como fórmula para completar a los efectos del RIA las limitaciones funcionales del art. 4.14 RGPD. Los «datos de base biométrica», conforme a la enmienda del Parlamento Europeo que propone su inclusión como número 33 bis del art. 3, son definidos como «*datos obtenidos a partir de un tratamiento técnico específico relativos a las señales físicas, fisiológicas o conductuales de una persona física*».



Este segundo concepto es, sin embargo, descartado en la última versión del RIA, estimándose preferible utilizar una única noción de datos biométricos para todo el texto. Con el objetivo de reducir la inseguridad jurídica, en cualquier caso, se procede a modificar la propuesta inicial de noción de datos personales realizada por la Comisión, respaldada en las tomas de postura del Consejo y el Parlamento. Así, y según el punto 34 del artículo 3 RIA, a los efectos de dicho texto serán datos biométricos *«los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos»*. Dicen los considerandos que esa noción debe interpretarse a la luz del concepto de datos biométricos del artículo 4.14 RGPD, pero las diferencias entre ambas nociones son obvias.

IV. LA ARQUITECTURA SUBYACENTE A TODOS LOS SISTEMAS BIOMÉTRICOS

IV.1. ARQUITECTURA BÁSICA DE LOS SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO

Sea identificante o no, para que un dato biométrico pueda servir de base a un sistema de reconocimiento biométrico, es necesario construir un sistema. En concreto, un sistema con capacidad de examinar el cuerpo de las personas y «reconocer» en él, sea de forma puntual sea de forma secuencial, algún atributo que pueda vincularse con la información que, como referencia, ha sido almacenada previamente —en una base de datos o en dispositivos de almacenamiento externo, como los chips que portan algunos documentos identificativos—. Hubo sistemas de reconocimiento biométrico no automatizados, como el mítico Bertillonage analizado supra, pero en la actualidad el término sistema de reconocimiento biométrico se aplica por lo común a estructuras que combinan hardware y *software*, cada vez con más tendencia a ser impulsadas por IA.

En su arquitectura básica, los sistemas automatizados de reconocimiento biométrico necesitan un mínimo de módulos que suele operar de forma secuencial (Escajedo San-Epifanio, 2017): interfaces que incorporan lectores o sensores, módulos de mejora de la captación y de extracción de atributos, espacios de almacenamiento y, por supuesto, módulos de cotejo de información captada en fresco respecto a la almacenada.

Por otra parte, y por cuanto se refiere a sus fases de funcionamiento, los sistemas de reconocimiento biométrico comprenden una serie de procesos



o fases que de forma genérica pueden agruparse en cuatro (Escajedo San-Epifanio, 2017): a) fase de enrolamiento, sea de una persona en singular, sea de una categoría como las de «emoción miedo», «franja de edad de mayores de 65» o categorías de sexo; b) fase de elaboración del patrón, que puede comprender a su vez varias subfases; c) captación del patrón en fresco, es decir, el momento en que se coloca a una persona ante el sistema para que reconozca en ese cuerpo una información captable y susceptible de ser cotejada; y d) cotejo del patrón captado en fresco con el patrón almacenado.

IV.2. FUENTES DE DATOS BIOMÉTRICOS, DATOS EN CRUDO Y PATRONES BIOMÉTRICOS

En términos absolutos no existe una biometría que pueda señalarse como *la óptima para el reconocimiento*. Aquello que se desea reconocer en un cuerpo puede ser muy diverso, como también han de tenerse en cuenta las posibilidades de los escenarios operativos en los que se aplicará el reconocimiento. Por poner un ejemplo, las huellas dactilares son muy singularizantes, pero en la entrada y salida de una excavación arqueológica o de una obra en construcción, o en la entrada y salida de un comedor escolar de infantil, es poco previsible que el promedio de personas tenga las manos lo suficientemente limpias como para poder captarlas bien. Si el grupo de sujetos enrolados no es muy elevado, daría mejor servicio un sistema de reconocimiento basado en la geometría de la mano, aunque en términos netos resulte menos singularizante.

Desde el punto de vista científico-técnico, se procede a una importante distinción entre tres conceptos. Como primer concepto, ha de decirse que son *fuentes de datos biométricos* aquellas características anatómico-físicas o dinámicas del cuerpo humano de las que se capta información para el funcionamiento de un sistema de reconocimiento biométrico, con independencia de que éste sea identificante o no. En segundo lugar, son *datos en crudo* los atributos biometrizable que están presentes en esa fuente y pueden captarse como tales. En tercer y último lugar, son patrones o plantillas biométricas (*biometric template* o *empreinte numérique*), las versiones transformadas o tecnificadas de la información captada. Estos patrones son susceptibles de almacenamiento digital y posterior comparación y, en puridad, coinciden con las nociones de datos biométricos que ofrecen el art. 3.34 RIA y el art. 4.14 RGPD, en el sentido de que son el resultado de un tratamiento técnico de características físicas, fisiológicas o conductuales de una persona física.



ESTUDIOS

El cuerpo humano se ha convertido para la inteligencia artificial en una fuente creciente de datos. El rostro, la voz, la marcha, los gestos, las expresiones emocionales o determinados parámetros fisiológicos pueden ser captados y tratados para identificar, verificar, clasificar, predecir o evaluar conductas. Esta obra aborda el problema jurídico que plantea esa transformación: quién puede captar, interpretar y clasificar el cuerpo humano, con qué finalidad, bajo qué condiciones y con qué límites.

La monografía analiza diferentes modalidades de reconocimiento biométrico y el estatuto jurídico que les aplica el Reglamento (UE) 2024/1689, de Inteligencia Artificial, en diálogo con el RGPD, la Carta de Derechos Fundamentales de la Unión Europea y la jurisprudencia europea. Ordena un régimen fragmentado y ofrece criterios para distinguir entre prácticas prohibidas, sistemas de alto riesgo, exclusiones y zonas de ambigüedad.

El análisis se proyecta sobre cuestiones centrales para la práctica jurídica, institucional y tecnológica: identificación biométrica remota, verificación uno-a-uno, reconocimiento de emociones, categorización biométrica, cribado y grandes sistemas europeos de información vinculados a fronteras, migración y cooperación policial.

Su aportación principal es situar la biometría no solo como técnica de identificación, sino como forma de inferencia y vigilancia sobre la identidad, la autonomía, la igualdad y la dignidad de la persona.

**Si quieres adquirir esta
obra haz click aquí**



ISBN: 978-94-1085-982-1

