

ESTUDIOS

# BIOMETRÍA, DERECHO ADMINISTRATIVO Y DATOS

MARTÍN MARÍA RAZQUIN LIZARRAGA  
JOSÉ FRANCISCO ALENZA GARCÍA  
DIRECTORES



ARANZADI

© Martín María Razquin Lizarrag y José Francisco Alenza García (Dirs.), 2025  
© 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>

**Primera edición:** junio 2025

**Depósito Legal:** M-13662-2025

**ISBN versión impresa:** 978-84-1085-159-7

**ISBN versión electrónica:** 978-84-1085-160-3

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](http://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, u 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.

## Índice General

*Página*

### PRESENTACIÓN

MARTÍN MARÍA RAZQUIN LIZARRAGA Y JOSÉ FRANCISCO ALENZA GARCÍA .....	21
---	----

### CAPÍTULO I

#### **El futuro de la inteligencia artificial desde la ética y los derechos fundamentales**

TOMÁS DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO.....	25
1. La pregunta por la ética y los derechos fundamentales en la regulación de la IA y su futuro.....	25
2. Las grandes aportaciones que se esperan de la IA para la sociedad y las personas como elemento inesquivable en su regulación.....	29
3. Tras tomar conciencia de los beneficios de la IA, tomarla también de sus riesgos para conjurarlos .....	32
4. El inevitable papel de la ética y los derechos fundamentales y libertades públicas en la regulación de la IA.....	37
5. Los rasgos característicos del Reglamento de IA.....	42
6. Las peculiaridades de la regulación de los ámbitos tecnológicos y de la IA en el Reglamento 2024/1689 y su correspondencia con las permanentes y seculares cuestiones de la jurisprudencia .....	46

## CAPÍTULO II

**El marco general de la innovación y la inteligencia artificial en un mundo cambiante**

JOSÉ LUIS PIÑAR MAÑAS.....	55
1. El Derecho ante la aceleración de la Historia y la sociedad digital .....	57
2. Derecho y técnica: un diálogo necesario, pero no siempre fácil .....	60
3. Derecho, ética y la importancia de los principios.....	64
4. ¿Qué regulación de la inteligencia artificial en un mundo cambiante?.....	66
5. La regulación por principios. Efectos en el control de la aplicación práctica del uso de sistemas de inteligencia artificial .....	68
6. Nuevos marcos regulatorios y la aplicación de las normas. En particular la autorregulación y el papel de <i>soft law</i> .....	73
7. ¿Nuevos derechos en un mundo cambiante y digital? Centralidad de la persona. Los derechos especialmente vulnerables ante la inteligencia artificial .....	79
8. Conclusiones.....	84
Bibliografía.....	85

## CAPÍTULO III

**La IA y su implantación. Reflexiones al hilo de un enfoque práctico**

PABLO GARCÍA MEXÍA, PHD. ....	91
1. El potencial disruptivo de la Inteligencia artificial.....	91
2. La regulación como respuesta frente a los riesgos de la IA...	93
2.1. Riesgos de la IA .....	93
2.2. Principales modelos regulatorios de la IA .....	96
2.3. El modelo regulatorio europeo de la IA .....	98
2.4. Algunas valoraciones (críticas) sobre el RIA. Europa y el falso dilema «regulación-innovación» .....	105

	<i>Página</i>
<b>3. Más allá de la regulación: Un sistema de gobernanza interna de la IA.....</b>	112
3.1. <i>Los contenidos de la gobernanza interna de la IA.....</i>	118
<b>4. Algunas reflexiones finales .....</b>	119
<b>Bibliografía.....</b>	124

## CAPÍTULO IV

### **Los sistemas biométricos en el Reglamento de Inteligencia Artificial**

MARTÍN MARÍA RAZQUIN LIZARRAGA.....	127
<b>1. Premisas fundamentales: concepto, finalidad y uso de datos biométricos.....</b>	128
1.1. <i>Concepto de datos biométricos.....</i>	128
1.2. <i>Finalidad y tipos de uso de datos biométricos .....</i>	129
<b>2. El enfoque de riesgo como base para la clasificación de los sistemas de IA que utilizan datos biométricos .....</b>	132
<b>3. Usos inaceptables de datos biométricos. Las prácticas prohibidas .....</b>	133
3.1. <i>Reconocimiento facial .....</i>	134
3.2. <i>Inferencia de emociones .....</i>	134
3.3. <i>Categorización biométrica .....</i>	135
3.4. <i>Sistemas de identificación biométrica remota en tiempo real en espacios de acceso público .....</i>	137
3.4.1. <i>La práctica prohibida.....</i>	137
3.4.2. <i>La excepción a la prohibición .....</i>	141
3.4.3. <i>La adopción de normas más restrictivas por los Estados.....</i>	146
<b>4. Sistemas de IA de alto riesgo por el uso de datos biométricos .....</b>	147
4.1. <i>Clasificación de sistema de alto riesgo.....</i>	147
4.2. <i>Los sistemas de IA de alto riesgo que utilizan datos biométricos .....</i>	148
4.2.1. <i>Sistemas de IA de biometría .....</i>	148

	<i>Página</i>
4.2.2. Sistemas de IA que pueden utilizar biometría....	150
4.3. <i>Requisitos y obligaciones. Evaluación de impacto</i> .....	152
<b>5. Sistemas de IA de riesgo limitado</b> .....	153
<b>6. Sistemas de IA de bajo o nulo riesgo</b> .....	154
<b>7. El estado de la ciencia sobre las técnicas biométricas</b> .....	155
<b>8. El necesario equilibrio entre protección (RGPD) e innovación (RIA). la posición de la AEPD y del CEPD</b> .....	158
<b>9. Conclusiones</b> .....	163
<b>10. Bibliografía</b> .....	165

## CAPÍTULO V

### **La regulación europea sobre la cartera de identidad en el Reglamento eIDAS2 ¿Hacia un cambio de paradigma en la regulación del entorno digital?**

MARÍA CRISTINA TIMÓN LÓPEZ Y JULIÁN VALERO TORRIJOS .....	167
<b>1. Introducción</b> .....	168
<b>2. La regulación inicial del Reglamento eIDAS y su limitado ámbito de aplicación en el sector público</b> .....	169
<b>3. La cartera de identidad digital europea como piedra angular del ecosistema eIDAS2</b> .....	170
3.1. <i>Mandato y modalidades de provisión</i> .....	172
3.2. <i>Funcionalidades y requisitos de la cartera digital. Especial referencia a la protección de datos de carácter personal</i> .....	173
3.3. <i>La obligatoria aceptación de la cartera de identidad digital europea: delimitación y alcance</i> .....	176
3.4. <i>La vinculación de la cartera digital con los datos de identificación (PID)</i> .....	178
<b>4. El creciente papel de la intervención pública en la era digital y su proyección sobre la regulación de la identidad digital: un cambio de paradigma</b> .....	180
4.1. <i>¿Liderazgo del sector público o protagonismo del mercado?</i> ...	180

	<i>Página</i>
4.2. <i>Hacia un intento de recuperar la soberanía digital por parte de la Unión Europea</i> .....	181
<b>5. Reflexión final</b> .....	183
<b>Bibliografía</b> .....	185

## CAPÍTULO VI

### **El derecho al uso de los propios datos biométricos**

JOSÉ FRANCISCO ALENZA GARCÍA .....	187
<b>1. La evolución de la acreditación de la identidad personal</b> .....	188
1.1. <i>La progresiva asunción por el Estado de la función pública de acreditación de la identidad</i> .....	188
1.2. <i>Los medios de acreditación de la identidad: posesión, conocimiento e inherencia</i> .....	189
1.3. <i>La biometría como único sistema que garantiza la certeza de la identidad</i> .....	192
<b>2. Diversidad de tecnologías biométricas y diversidad de usos biométricos; en particular, las disruptivas referencias biométricas renovables</b> .....	193
2.1. <i>Los conceptos jurídicos de biometría y de identificación biométrica</i> .....	193
2.2. <i>Tecnologías biométricas y variedad de usos biométricos</i> .....	196
2.2.1. <i>Diversidad de tecnologías biométricas</i> .....	196
2.2.2. <i>La paradoja biométrica: comodidad y fiabilidad vs miedos infundados</i> .....	197
2.3. <i>La necesaria diferenciación entre las Referencias Biométricas y las Referencias Biométricas Renovables</i> .....	199
2.4. <i>Los sistemas de identificación biométrica basados en RBR como sistemas robustos, seguros y confiables: fin de la dicotomía seguridad vs. privacidad</i> .....	202
<b>3. La identificación biométrica como sistema legalmente permitido y de riesgo bajo o inexistente</b> .....	203

	<u>Página</u>
3.1. <i>La identificación biométrica como sistema permitido (de riesgo bajo o inexistente) por la legislación europea de inteligencia artificial</i> .....	203
3.2. <i>La legislación de protección de datos personales no prohíbe el uso de datos biométricos</i> .....	206
3.2.1. Los datos biométricos como categoría especial de datos personales.....	206
3.2.2. El consentimiento como base legitimadora de la licitud del tratamiento de los datos biométricos	208
3.2.3. El rechazo de la AEPD al consentimiento como base legitimadora del uso de los datos biométricos para la acreditación de la identidad ¿Puede la AEPD eliminar el derecho de uso de los propios datos biométricos? .....	210
<b>4. Fundamentos del derecho al uso de los propios datos biométricos</b> .....	213
4.1. <i>Autonomía de la voluntad, derecho a la intimidad y poder de disposición sobre los datos biométricos</i> .....	213
4.2. <i>El derecho a la identidad incluye el derecho a decidir el sistema de identificación</i> .....	215
4.2.1. La acreditación de la identidad como deber, como carga y como derecho: el derecho a elegir el medio de acreditación de la identidad.....	216
4.2.2. El derecho a la identidad digital .....	217
4.3. <i>La identificación biométrica como el método más seguro para la protección de otros derechos del ciudadano</i> .....	218
4.3.1. Prevención del fraude y seguridad ciudadana...	218
4.3.2. Utilización fraudulenta de datos personales, igualdad y derecho de sufragio .....	220
4.4. <i>Los sistemas de identidad biométrica como herramienta para el cumplimiento de determinados principios constitucionales y garantía de los derechos digitales</i> .....	223
4.4.1. Brecha digital y protección de colectivos vulnerables .....	223

	<i>Página</i>
4.4.2. La libertad de empresa para proporcionar servicios de identificación biométrica .....	224
<b>5. Conclusiones. Mis datos son míos: el derecho a usar mis datos biométricos para acreditar mi identidad.....</b>	<b>227</b>
<b>6. Bibliografía .....</b>	<b>231</b>

## CAPÍTULO VII

### **Transparencia, sistemas biométricos y Administraciones públicas**

ARITZ ROMEO RUIZ.....	233
<b>1. ¿Transparencia? ¿Qué transparencia? .....</b>	<b>234</b>
<b>2. La transparencia algorítmica .....</b>	<b>236</b>
2.1. <i>La transparencia: una técnica y una deber frente a la opacidad algorítmica.....</i>	<i>236</i>
2.1.1. ¿Qué debemos entender por transparencia algorítmica?.....	237
2.1.2. La explicabilidad: la otra cara de la moneda.....	239
2.2. <i>Las obligaciones de transparencia algorítmica en el Reglamento Europeo de Inteligencia Artificial.....</i>	<i>240</i>
2.3. <i>Sistemas de biometría en función del riesgo.....</i>	<i>244</i>
2.3.1. Sistemas biométricos de riesgo inasumible.....	245
2.3.2. Sistemas biométricos de alto riesgo.....	246
2.3.3. Sistemas biométricos de riesgo bajo.....	247
2.4. <i>Obligaciones de transparencia algorítmica aplicadas a los sistemas biométricos .....</i>	<i>247</i>
2.4.1. Los deberes de transparencia del artículo 13 RIA.....	247
2.4.2. Los deberes de transparencia de los responsables del despliegue de sistemas de IA de alto riesgo.....	249
2.4.3. Los deberes de transparencia de los responsables del despliegue de sistemas de IA de alto riesgo.....	250

	<i>Página</i>
2.4.4. Los deberes de transparencia de determinados sistemas de IA (art. 50 RIA) .....	251
<b>3. Transparencia y protección de datos biométricos.....</b>	<b>254</b>
3.1. <i>La transparencia como principio del tratamiento de datos personales</i> .....	254
3.2. <i>Obligaciones de transparencia que se derivan del tratamiento de datos personales</i> .....	257
<b>4. Transparencia administrativa: cuando es la Administración la que usa un SIA biométrico .....</b>	<b>260</b>
4.1. <i>El uso de sistemas de IA por parte de la Administración pública conlleva el cumplimiento de las obligaciones de transparencia</i> .....	260
4.2. <i>La aplicación de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno a la actividad administrativa basada en sistemas de Inteligencia Artificial.....</i>	270
4.2.1. Obligaciones de publicidad activa.....	270
4.2.2. Derecho de acceso a la información .....	272
<b>5. A modo de reflexión final .....</b>	<b>279</b>
<b>6. Bibliografía .....</b>	<b>281</b>

## CAPÍTULO VIII

### **La protección jurídica de las personas vulnerables ante la biometría**

MIREN SARASÍBAR IRIARTE .....	287
<b>1. El sujeto como centro de atención de la inteligencia artificial: en especial, los colectivos vulnerables (desarrollo tecnológico versus protección de la persona y sus derechos).....</b>	<b>288</b>
<b>2. Los beneficios del uso de la biometría en las personas vulnerables .....</b>	<b>292</b>
2.1. <i>Avances tecnológicos para mejorar la calidad de vida de las personas con discapacidad</i> .....	292
2.2. <i>Utilidades de la biometría para los menores de edad</i> .....	294
<b>3. Los riesgos y sesgos en relación con la biometría y la consecuente afección a los derechos.....</b>	<b>296</b>

	<i>Página</i>
3.1. <i>La especial vulnerabilidad de las personas con discapacidad ante la biometría</i> .....	296
3.2. <i>La fragilidad de la juventud ante la biometría</i> .....	301
<b>4. La repercusión de la biometría en el Reglamento General de Protección de Datos</b> .....	<b>305</b>
4.1. <i>La autenticación o verificación y la identificación biométrica.</i>	305
4.2. <i>La identificación biométrica remota en tiempo real y en diferido</i> .....	309
<b>5. Los sistemas biométricos en el reciente Reglamento europeo de inteligencia artificial</b> .....	<b>311</b>
5.1. <i>El riesgo como eje vertebrador</i> .....	311
A) Prácticas prohibidas .....	312
B) Sistemas de alto riesgo .....	313
C) Sistemas de riesgo limitado .....	316
D) Sistemas de bajo o nulo riesgo .....	317
5.2. <i>La necesaria regulación de las garantías del sujeto</i> .....	317
<b>6. Reflexión final</b> .....	<b>319</b>
<b>7. Bibliografía</b> .....	<b>320</b>

## CAPÍTULO IX

### **Presupuestos estructurales de la IA en el sector público: datos e interoperabilidad**

RUBÉN MARTÍNEZ GUTIÉRREZ .....	323
<b>1. Introducción. La administración de datos en la era de la inteligencia artificial</b> .....	<b>323</b>
<b>2. La centralidad e importancia del dato en la UE</b> .....	<b>324</b>
2.1. <i>La Estrategia Europea de Datos</i> .....	324
2.2. <i>Los Espacios de Datos</i> .....	326
2.3. <i>La configuración de los Espacios de Datos</i> .....	326
<b>3. La interoperabilidad como conexión entre los datos y los sistemas de IA</b> .....	<b>328</b>

	<u>Página</u>
3.1. <i>Concepto y alcance de la interoperabilidad para los Espacios de Datos</i> .....	328
3.2. <i>Las dimensiones de la interoperabilidad</i> .....	329
<b>4. Requisitos para la automatización en el intercambio de datos</b> .....	<b>331</b>
4.1. <i>Requisitos del Reglamento de Datos</i> .....	331
4.2. <i>Requisitos del Reglamento sobre la Europa interoperable. Creación de espacios controlados de pruebas</i> .....	333
4.3. <i>Requisitos del Reglamento UE de Inteligencia Artificial</i> .....	338
4.3.1. <i>Requisitos y obligaciones generales en sistemas de alto riesgo</i> .....	338
4.3.2. <i>La evaluación de impacto</i> .....	340
<b>5. Bibliografía</b> .....	<b>342</b>

## CAPÍTULO X

### **Contratación pública de sistemas biométricos y de inteligencia artificial**

FCO. JAVIER VÁZQUEZ MATILLA.....	345
<b>1. Introducción</b> .....	<b>345</b>
<b>2. La compra pública de soluciones que incorporen biometría</b>	<b>351</b>
2.1. <i>Concepto y usos de la biometría</i> .....	351
2.2. <i>Consultas preliminares</i> .....	355
2.3. <i>El diseño del contenido obligacional del contrato</i> .....	356
2.4. <i>Fórmulas de contratación</i> .....	359
2.5. <i>Criterios de solvencia</i> .....	359
2.6. <i>Criterios de adjudicación</i> .....	361
<b>3. Inteligencia artificial y contratación pública</b> .....	<b>363</b>
3.1. <i>Perspectiva Dual de la Inteligencia Artificial en la Contratación Pública</i> .....	363
3.2. <i>La utilidad para la contratación pública de la IA</i> .....	364

	<i>Página</i>
3.3. <i>La adquisición de tecnologías de IA por el sector público .....</i>	366
<b>4. Conclusiones.....</b>	<b>369</b>
<b>5. Bibliografía .....</b>	<b>370</b>

## CAPÍTULO XI

### **La ciberseguridad en las Administraciones públicas: regulación y gestión**

DOLORS CANALS AMETLLER.....	373
<b>1. Introducción: las distintas acepciones del término «ciberseguridad».....</b>	<b>373</b>
<b>2. La regulación de la seguridad digital: entre lo normativo y lo no normativo .....</b>	<b>378</b>
2.1. <i>Complementariedad entre derecho, soft law, técnica y ética....</i>	378
2.2. <i>Las estrategias europeas .....</i>	382
2.3. <i>El marco normativo y no normativo europeo de la ciberseguridad y la ciberresiliencia.....</i>	385
2.3.1. <i>El marco no normativo: declaraciones y programas estratégicos.....</i>	385
2.3.2. <i>El marco normativo común europeo.....</i>	386
2.4. <i>El marco estatal: estrategias nacionales y derecho sustantivo</i>	389
2.5. <i>La regulación no normativa: guías, directrices, recomendaciones y normas técnicas .....</i>	391
2.6. <i>Regulación de la biometría y riesgos de ciberseguridad .....</i>	392
<b>3. La gestión de los riesgos digitales .....</b>	<b>395</b>
3.1. <i>La gestión de la «seguridad híbrida» ante riesgos de todo tipo</i>	395
3.2. <i>La ciberseguridad de la Administración pública digital .....</i>	396
3.3. <i>El enfoque de la normalización y certificación: los sistemas europeos y la certificación de los Esquemas Nacionales de Seguridad .....</i>	398
3.4. <i>La arquitectura institucional de la ciberseguridad.....</i>	400
<b>Bibliografía citada.....</b>	<b>402</b>

## CAPÍTULO XII

**La regulación de la inteligencia artificial y los sistemas biométricos en Italia**

MARCO CALABRÒ.....	405
<b>1. Prólogo.....</b>	<b>405</b>
<b>2. Evolución reciente del debate sobre la inteligencia artificial en el derecho administrativo italiano .....</b>	<b>407</b>
<b>3. Biometría y Administración pública en Italia: una relación aún por explorar .....</b>	<b>411</b>
3.1. <i>El plan de la regulación .....</i>	411
3.2. <i>Perspectiva ético-jurídica de la biometría.....</i>	411
3.3. <i>Técnicas biométricas y vigilancia de los funcionarios públicos .</i>	412
3.4. <i>El papel central otorgado a la Agencia de Protección de Datos.</i>	414
<b>4. Seguridad urbana y uso de modelos de control biométrico..</b>	<b>418</b>
<b>5. Conclusiones.....</b>	<b>424</b>
<b>Bibliografía.....</b>	<b>426</b>

## CAPÍTULO XIII

**La videovigilancia aumentada: cuando los Juegos Olímpicos y Paralímpicos 2024 permitieron a Francia experimentar**

MAITENA POELEMANS .....	433
<b>1. Introducción.....</b>	<b>433</b>
<b>2. El uso de tecnología algorítmica legitima un marco legal para encuadrar la videovigilancia (VVA) .....</b>	<b>436</b>
2.1. <i>El marco legal de la videovigilancia .....</i>	436
2.2. <i>El uso controvertido de la VVA en la ausencia de marco jurídico específico.....</i>	438
2.3. <i>La necesidad de una ley según el artículo 34 de la Constitución y de una norma según el RGPD.....</i>	439
<b>3. El contenido de la Ley 2023-380 de 2023 sobre los Juegos Olímpicos y Paralímpicos (JoP) del 19 de mayo de 2023 y del Decreto de aplicación.....</b>	<b>441</b>

	<u>Página</u>
<b>4. La conformidad constitucional de la ley .....</b>	443
<b>5. Las principales aplicaciones de las cámaras de VVA.....</b>	445
<b>6. Las cuestiones pendientes.....</b>	447
6.1. <i>¿Un verdadero experimento temporal? .....</i>	447
6.2. <i>¿Una verdadera exclusión de la biometría? .....</i>	448
<b>7. La importancia de los controles .....</b>	449
7.1. <i>El control de la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI).....</i>	449
7.2. <i>El control por la Comisión Nacional Informática y Libertades (CNIL).....</i>	450
<b>8. Conclusión: la necesidad de encontrar un equilibrio entre eficacia y democracia .....</b>	451
<b>9. Bibliografía .....</b>	452
 CONCLUSIONES DEL CONGRESO INTERNACIONAL «BIOMETRÍA, DERECHO ADMINISTRATIVO Y DATOS», CELEBRADO EN PAMPLONA LOS DÍAS 7 Y 8 DE NOVIEMBRE DE 2024.....	 453



# Transparencia, sistemas biométricos y Administraciones públicas<sup>1</sup>

ARITZ ROMEO RUIZ

*Profesor Permanente Laboral de Derecho Administrativo.  
Universidad Pública de Navarra*

SUMARIO: 1. ¿TRANSPARENCIA? ¿QUÉ TRANSPARENCIA? 2. LA TRANSPARENCIA ALGORÍTMICA. 2.1. *La transparencia: una técnica y una deber frente a la opacidad algorítmica.* 2.1.1. ¿Qué debemos entender por transparencia algorítmica? 2.1.2. La explicabilidad: la otra cara de la moneda. 2.2. *Las obligaciones de transparencia algorítmica en el Reglamento Europeo de Inteligencia Artificial.* 2.3. *Sistemas de biometría en función del riesgo.* 2.3.1. *Sistemas biométricos de riesgo inasumible.* 2.3.2. *Sistemas biométricos de alto riesgo.* 2.3.3. *Sistemas biométricos de riesgo bajo.* 2.4. *Obligaciones de transparencia algorítmica aplicadas a los sistemas biométricos.* 2.4.1. *Los deberes de transparencia del artículo 13 RIA.* 2.4.2. *Los deberes de transparencia de los responsables del despliegue de sistemas de IA de alto riesgo.* 2.4.3. *Los deberes de transparencia de los responsables del despliegue de sistemas de IA de alto riesgo.* 2.4.4. *Los deberes de transparencia de determinados sistemas de IA (art. 50 RIA).* 3. TRANSPARENCIA Y PROTECCIÓN DE DATOS BIOMÉTRICOS. 3.1. *La transparencia como principio del tratamiento de datos personales.* 3.2. *Obligaciones de transparencia que se derivan del tratamiento de datos personales.* 4. TRANSPARENCIA ADMINISTRATIVA: CUANDO ES LA ADMINISTRACIÓN LA QUE USA UN SIA BIOMÉTRICO. 4.1. *El uso de sistemas de IA por parte de la Administración pública conlleva el cumplimiento de las obligaciones de transparencia.* 4.2. *La aplicación de la Ley de Transparencia, Acceso a la*

1. Este trabajo se enmarca en el Proyecto «Biometría, Derecho Administrativo y Datos —BIO-DATA—» PID2021-125170NB-100, financiado por MCIN/AEI/10.13039/501100011033/y por FEDER Una manera de hacer Europa.

*Información Pública y Buen Gobierno a la actividad administrativa basada en sistemas de Inteligencia Artificial.* 4.2.1. Obligaciones de publicidad activa. 4.2.2. Derecho de acceso a la información. 5. A MODO DE REFLEXIÓN FINAL. 6. BIBLIOGRAFÍA.

## 1. ¿TRANSPARENCIA? ¿QUÉ TRANSPARENCIA?

El concepto de transparencia ha sido y es ampliamente invocado en el ámbito social, político y, más precisamente en al ámbito de las relaciones entre la ciudadanía y la administración pública.

La transparencia es un concepto polisémico, cuyas múltiples definiciones resultan complejas de delimitar. Además, se trata de una cualidad que evoca una idea positiva, pues supone arrojar luz y apertura<sup>2</sup> frente a la oscuridad en el ámbito de que se trate, especialmente (aunque no de manera exclusiva) en la actuación de los poderes públicos.

Por otro lado, podría decirse que es un concepto dotado de una gran transversalidad, pues es utilizado como herramienta en múltiples ámbitos y disciplinas, en cada uno de los cuales adquiere matices diferentes. El término, además, tiene mucho de simbólico. En puridad, según la RAE transparencia es la cualidad de lo transparente, es decir, de aquello que en los cuerpos «permite ver los objetos con nitidez a través de él». Por ello, su uso en ámbitos como el Derecho, la Economía o la Ciencia Política es, fundamentalmente un uso alegórico, una metáfora de lo que, en realidad, no deja de ser una cualidad de los cuerpos físicos<sup>3</sup>.

La transparencia, es, por tanto, un ideal. Una aspiración hacia la que se debe avanzar, un horizonte que ha de buscarse, aún a sabiendas de que nunca será plenamente alcanzado. Ni las políticas públicas, ni la actividad administrativa ni, menos aún los sistemas de inteligencia artificial pueden ser nunca enteramente transparentes. Por muchas medidas de transparencia que se adopten y por muy eficaces que sean, jamás serán éstas lo suficientemente efectivas para poder ver con absoluta nitidez todo lo que hay detrás de ellas.

Por esa razón, la transparencia debe ser entendida como un instrumento. O, si se prefiere, una técnica, que aplicándola nos acerca a la consecución de objetivos deseables.

En el caso de las administraciones públicas, la transparencia debe ser vista como una herramienta que contribuye a la realización del principio de

2. Schram (2002: 35).

3. Cotino Hueso (2022: 25 a 28).

integridad, que, a su vez, forma parte del derecho a una buena administración, recogido en el artículo 41 de la Carta de los Derechos Fundamentales de la Unión Europea<sup>4</sup>, y que, tal y como ha aseverado el Tribunal Supremo en su STS de 15 de octubre de 2020 (rec. 1652/2019) «es sabido que (...) está implícito en nuestra Constitución (arts. 9.3, 103 y 106)».

Como vemos, la vinculación del principio de transparencia con el derecho a una buena administración ha sido advertida por la jurisprudencia<sup>5</sup>. La STS de 30 de abril de 2012, que se refiere al derecho a una buena administración como un «derecho de última generación», que se relaciona con el principio de transparencia y con el derecho de acceso a los registros y los archivos. También la STSJ de Cataluña, de 1 de octubre de 2020, considera que el derecho a una buena administración «aparece conectado con el principio de transparencia de la actividad administrativa, eficiencia, claridad y una aplicación individualizada del Derecho al caso».

Todo lo anterior se refiere al principio de la transparencia aplicado a la actuación de las administraciones públicas. Sin embargo, llevado al uso de sistemas de IA, la transparencia se refiere a un fenómeno más amplio, que trasciende la actividad administrativa y que se sitúa en un plano más extenso, como es el desarrollo, puesta en servicio y uso final de un SIA, ya sea por parte de una administración pública o de un poder público, ya sea por parte de particulares.

En este caso, la transparencia algorítmica es, además de una garantía para el adecuado uso y buen funcionamiento técnico del SIA, una técnica de protección de los ciudadanos frente a los riesgos que la IA presenta para los derechos y libertades fundamentales, tanto para evitar que los mismos resulten lesionados, como, para en el caso que lo sean, permitir el ejercicio de la defensa frente a tal vulneración. Esto es algo que se ve muy claramente explicado en el punto n.º 37 de la Recomendación sobre la ética de la IA de la UNESCO, de 2021<sup>6</sup> (n.º 37):

«La transparencia y la explicabilidad de los sistemas de IA suelen ser condiciones previas fundamentales para garantizar el respeto, la protección y la promoción de los derechos humanos, las libertades fundamentales y los principios éticos. La transparencia es necesaria para que los regímenes nacionales e internacionales pertinentes en materia de responsabilidad funcionen

- 
4. No podemos desdeñar el valor jurídico de la Carta, que forma parte del Derechos de Tratados, desde que el artículo 6 del TUE le atribuyera carácter jurídicamente vinculante.
  5. Garrido Mayol (2020: 115-141).
  6. UNESCO, *Recomendación sobre la ética de la inteligencia artificial*, Conferencia General, 4ª reunión, París, 41 c/73, de 22 de noviembre de 2021.

eficazmente. La falta de transparencia también podría mermar la posibilidad de impugnar eficazmente las decisiones basadas en resultados producidos por los sistemas de IA y, por lo tanto, podría vulnerar el derecho a un juicio imparcial y a un recurso efectivo, y limita los ámbitos en los que estos sistemas pueden utilizarse legalmente.»

Como puede apreciarse, cuando nos referimos la transparencia en el ámbito de la IA, estamos refiriéndonos a «otro» tipo de transparencia, que es diferente de la transparencia administrativa. Obviamente, cuando sea una administración pública quien ponga en uso un SIA, además podría estar vinculada por la transparencia administrativa.

Mientras la transparencia administrativa es un escudo protector frente a la mala administración de los poderes públicos y las administraciones, la transparencia algorítmica lo es en relación con el uso de sistemas de IA y su funcionamiento.

Además de ello, debe tenerse en cuenta que los SIA funcionan gracias al tratamiento de grandes cantidades de datos, que, en no pocas ocasiones, pueden ser datos personales. En el momento en que un SIA está tratando datos personales, resulta de aplicación su marco normativo de protección que en la UE está representado por el RGPD y, en España, además, por la LOPDPGDD, que, a los efectos de este trabajo, reproduce el contenido del Reglamento Europeo. Entre las obligaciones que se imponen a los responsables de tratamientos de datos personales, hay también importantes obligaciones de transparencia. Por lo tanto, cuando, como consecuencia del funcionamiento de un SIA se traten datos personales, nos encontraremos ante un tercer tipo de obligaciones de transparencia, que son las que establece el RGPD.

Por ello, al plantear la cuestión del régimen jurídico en cuanto a la transparencia, por el uso de sistemas biométricos, mediante sistemas de IA, por las administraciones públicas, la primera pregunta que hay que responder es a qué tipo de transparencia nos estamos refiriendo. Y es que hemos de diferenciar tres bloques de obligaciones de transparencia: la transparencia algorítmica, la transparencia respecto de los tratamientos de datos personales y la transparencia administrativa.

## **2. LA TRANSPARENCIA ALGORÍTMICA**

### **2.1. LA TRANSPARENCIA: UNA TÉCNICA Y UNA DEBER FRENTE A LA OPACIDAD ALGORÍTMICA**

La primera modalidad a la que voy a referirme es la que podemos denominar como «transparencia algorítmica», es decir, aquellas obligaciones que

se derivan del uso, comercialización o puesta en servicio de un sistema de inteligencia artificial.

Tal y como ha propuesto la profesora VELASCO RICO en varios de sus trabajos, la transparencia es una forma de hacer frente a la opacidad de los algoritmos. Esa opacidad trae causa en factores diversos, como el funcionamiento de los algoritmos de caja negra, el uso de datos de entrenamiento que sean total o parcialmente desconocidos, la voluntad de las empresas que desarrollan los SIA, con el fin de proteger su derecho a la propiedad industrial, o por la complejidad técnica de los sistemas que los hacen difícilmente comprensibles para una persona sin conocimientos técnicos muy específicos<sup>7</sup>.

Si la opacidad trae graves consecuencias cuando los SIA se utilizan por empresas y particulares del sector privado, dicha gravedad es aún mayor cuando el SIA lo utilizan las administraciones públicas, pues pueden afectar al control de la actividad administrativa, y a la obligación de motivar los actos administrativos.

La transparencia se alza así en un presupuesto necesario para procurar las garantías de los particulares cuando se ven sometidos a la actuación de un SIA, ya sea por parte de entidades del sector privado, pero, fundamentalmente, cuando se trata de actuaciones administrativas en las que haya intervenido una IA.

### **2.1.1. ¿Qué debemos entender por transparencia algorítmica?**

Más allá de los esfuerzos doctrinales de determinar qué debemos entender por transparencia algorítmica, considero que, en un ejercicio de pragmatismo, lo más adecuado puede ser recurrir a una definición ampliamente aceptada y que ha sido el punto de partida del Reglamento Europeo de Inteligencia Artificial en esta materia.

Me refiero al concepto manejado en las Directrices Éticas para una IA confiable, de 2019, del Grupo Independiente de expertos de alto nivel sobre IA (GIE en adelante) creado por la comisión. Dicho informe dedica su apartado n.º 4 al principio de transparencia, que es uno de los requisitos de fiabilidad de la IA.

Antes de eso, en cuanto a los requisitos para una IA fiable, el GIE afirma que, si bien a los desarrolladores les corresponde integrar los requisitos de

---

7. Velasco (2024: 55).

fiabilidad en el diseño de un SIA, y a los responsables del despliegue les compete asegurarse de que los sistemas y productos que utilizan y ofrecen cumplen esos requisitos, a los usuarios finales les corresponde estar informados sobre dichos requisitos y poder pedir que, en su caso, se cumplan. Por tanto, la transparencia, no sólo está entre los requisitos para la IA sea fiable, sino que es un requisito cuyo fundamento consiste, precisamente, en que los usuarios puedan comprobar, conocer, y, en su caso, reclamar el cumplimiento de los requisitos<sup>8</sup>. Es decir, la transparencia es, además de fundamento de fiabilidad de la IA, una herramienta necesaria para el ejercicio de derechos por parte de los usuarios finales.

Según el documento de Directrices Éticas la transparencia se relaciona con conceptos fronterizos. Entre estos está la trazabilidad, que consiste en que los procesos y conjuntos de datos que dan lugar al SIA se documenten correctamente a fin de que pueda trazarse un seguimiento, y aumentar la transparencia, permitiendo identificar en qué punto del proceso se ha podido producir un error o sus causas.

Por otro lado, el GIE se refiere a la explicabilidad como la capacidad de explicación de los procesos técnicos que subyacen tras el diseño y puesta en funcionamiento de un SIA. Es decir, que los aspectos técnicos y las decisiones adoptadas por un sistema de inteligencia artificial han de ser comprensibles para los humanos y han de permitir su rastreo. Finalmente, la comunicación hace referencia a que los SIA deben identificarse como inteligencias artificiales, de manera que los seres humanos con los que interactúan deben poder ser plenamente conscientes de que se están relacionando con una inteligencia artificial. Esto exige, además, que se informe de la posibilidad de interactuar, si se desea, con un ser humano, en lugar de con un SIA cuando esto sea posible, así como dar información sobre las capacidades y limitaciones del SIA a los profesionales y usuarios finales.

Como podemos observar, cuando hablamos de la transparencia algorítmica nos encontramos ante un concepto complejo, que tras de sí esconde diversos significados. Si se prefiere, podríamos hablar de lo poliédrico de la transparencia de los algoritmos, pues detrás de la misma se esconden, a su vez, diversas subcategorías. Sin ánimo de exhaustividad (pues no se

8. Los siete requisitos para una IA fiable son, según el documento «Directrices Éticas para una IA confiable» del GIE: acción y supervisión humanas; solidez técnica y seguridad; gestión de la privacidad y de los datos; transparencia; diversidad, no discriminación y equidad; bienestar social y ambiental; y rendición de cuentas. COMISIÓN EUROPEA, Grupo de Expertos de Alto nivel sobre Inteligencia Artificial, «Directrices éticas para una IA fiable», Bruselas, 2019.

trata aquí de ahondar en cada uno de dichos subconceptos, aunque sí puede resultar ilustrativo presentarlos), nos hacemos eco a continuación de la propuesta del profesor SIMÓN CASTELLANO, que distingue las siguientes subcategorías<sup>9</sup>, que nos pueden aportar luz en la comprensión del concepto de transparencia algorítmica:

- La simulabilidad: significa que un SIA debe poder ser simulado o entendido completamente por un ser humano.
- La descomponibilidad: las diferentes partes de que se compone un SIA (datos de entrada, parámetros, operaciones de cálculo, datos de salida...), han de poderse descomponer, es decir, ser entendidas por un humano, independientemente del resto del SIA, y han de ser accesibles y comprensibles por separado.
- La legibilidad: un ser humano tiene que ser capaz de leer los predictores del algoritmo.
- La auditabilidad: es una de las medidas clásicas de seguridad de los sistemas informáticos. Su relación con la transparencia se produce en tanto en cuanto los informes de auditoría del código algorítmico pueden ser objeto de publicidad activa.
- La publicidad activa: que se refiere a aquellos elementos informativos sobre el SIA que los responsables (en sus distintas figuras y roles y, por tanto, en cumplimiento de obligaciones que difieren en virtud de su función con respecto a la implantación del SIA), deben facilitar directamente sin necesidad de ser requeridos para ello.

### **2.1.2. La explicabilidad: la otra cara de la moneda**

Por otro lado, como categoría diferente a la transparencia, pero en clara interacción con ella, está la explicabilidad, que se refiere a que el SIA y sus elementos deben ser comprensibles y deben poder ser explicados de manera que un ser humano medio pueda entenderlos con facilidad.

La explicabilidad es, por tanto, una cualidad que hace mención a cómo debe ser presentada o comunicada la información que es objeto del principio de transparencia. Sin embargo, la explicabilidad es compleja y difícil de conseguir dada la complejidad técnica de los SIA.

Y, aunque, en estricto, explicabilidad no es propiamente un sinónimo de transparencia, sí es, necesariamente, una cualidad necesaria de la trans-

9. Simón (2023: 127 y ss.).

parencia algorítmica, especialmente en ámbitos tan complejos y de tanta especialización técnica como el de la IA.

Para que haya una verdadera transparencia y esta opere como una garantía eficaz frente a los riesgos de la IA, es necesario que la información presentada en el seno del principio de transparencia sea fácilmente entendible desde el punto de vista de una persona media ideal.

SIMÓN CASTELLANO propone una disección del principio de explicabilidad que nos permite una mejor comprensión del concepto<sup>10</sup>. De esta manera plantea una división del término en varias subcategorías como son la inteligibilidad, la comprensibilidad y la interpretabilidad, que, aunque parecen hacer mención a cuestiones muy similares, presentan matices que las diferencian.

Así, la inteligibilidad supone que un ser humano pueda entender cómo funciona el SIA, sin necesidad de conocer su estructura interna. Aunque, ciertamente, como señala COTINO, interpretabilidad y explicabilidad no son exactamente lo mismo, pues la primera se refiere, según el NIST (*National Institute of Standards and Technology*), a poder comprender los resultados que arroja una SIA y a que el usuario pueda valorar su funcionamiento, mientras que la explicabilidad se refiere a hacer comprensibles los mecanismos internos que permiten que el SIA funcione. En cualquier caso, ambos conceptos contribuyen a la comprensión de los aspectos técnicos del algoritmo<sup>11</sup>.

Por otro lado, la comprensibilidad supone que el SIA muestre, de manera entendible para un ser humano, el conocimiento aprendido por el propio SIA.

Finalmente, la interpretabilidad consiste en que los datos de salida, el resultado o la decisión que adopta el SIA y cómo se ha producido, sea comprensible para un humano, lo que permite la supervisión humana y la prevención del sesgo algorítmico.

## 2.2. LAS OBLIGACIONES DE TRANSPARENCIA ALGORÍTMICA EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL

El RIA desarrolla el principio de transparencia y determina, con un alto grado de concreción, el principio de transparencia.

La transparencia es en el RIA un principio de actuación, un derecho, pero también, y, sobre todo, tiene un carácter instrumental. Se trata de una técnica

10. Simón (2023: 132 y 133).

11. Cotino (2022: 57).

para lograr una IA más confiable, garantista y que respete los derechos y libertades de las personas usuarias finales, y, en general de las personas que puedan resultar afectadas por la puesta en marcha de diferentes sistemas de inteligencia artificial.

De hecho, el considerando 9º destaca que el objeto del RIA es reforzar la eficacia de los derechos y de las vías de recurso, para lo que establece requisitos y obligaciones específicas, con los que concreta el contenido de la documentación técnica y las medidas concretas de transparencia que han de adoptarse.

El concepto de transparencia que se recoge en el RIA está basado, tal y como se reconoce en el Considerando 27, en la definición dada por el Grupo de Expertos de Alto Nivel sobre IA creado por la Comisión. La transparencia es uno de los principios que todo sistema de IA debe cumplir para ser confiable, y, a pesar de que en la definición del Grupo de Expertos era considerado un principio «no vinculante», a partir de la entrada en vigor del RIA las obligaciones de transparencia algorítmica son deberes jurídicos que vinculan a los sujetos afectados por los mismos.

Según la definición del Grupo de Expertos, recogida en el precitado considerando 27 del RIA, para que un SIA sea transparente, debe desarrollarse de tal manera que permita conocer su trazabilidad y su explicabilidad.

Pero, además de eso, el SIA debe procurar la información necesaria para que las personas sean plenamente conscientes de que están interactuando con una IA.

Además de lo anterior, el SIA ha de permitir que el responsable del despliegue esté informado sobre los riesgos y limitaciones a los que puede enfrentarse el desarrollo del SIA.

Finalmente, en virtud del principio de transparencia, las personas afectadas han de contar con información suficiente en relación con los derechos que les asisten y el modo de ejercerlos.

Como es sabido, el RIA establece una regulación basada en el riesgo, y, por tanto, las obligaciones de transparencia van a diferir en función del nivel de riesgo que represente el SIA en cuestión para los derechos fundamentales.

De esta manera, las obligaciones de transparencia van a ser graduales<sup>12</sup>, por lo que las exigencias para los SIA de alto riesgo van a resultar más exi-

12. Carlón (2025: 209 y ss).

gentes que los SIA de riesgo limitado, tal y como dispone el considerando 72 del RIA. Para superar la preocupación que genera la posible opacidad de los sistemas de alto riesgo, unido a su complejidad técnica, se les exigen importantes deberes de transparencia que han de cumplirse antes de su introducción en el mercado. Estos deben servir, además, para facilitar a los responsables del despliegue el cumplimiento de sus obligaciones.

A este respecto, es necesario que los responsables del despliegue puedan entender cómo funciona el SIA, han de tener la información necesaria para poder evaluar su funcionalidad, y, además, ser capaces de comprender sus fortalezas y sus limitaciones.

Por esa razón, entre los deberes de transparencia está el que los SIA deben acompañar información sobre el sistema en forma de instrucciones de uso. Instrucciones que deben contener incluir las características, las capacidades y las limitaciones y funcionalidades del SIA.

Más precisamente, estas deben integrar la información sobre posibles circunstancias en las que el SIA puede generar riesgos para la salud, la seguridad o para los derechos fundamentales. Entre estas circunstancias de riesgo potencial se incluyen la actuación que pueda desarrollar el responsable del despliegue, que pueda afectar al comportamiento y al funcionamiento del sistema.

También deben estar previstas medidas para facilitar información sobre los cambios que el proveedor haya predeterminado y haya evaluado de cara a lograr la conformidad del SIA.

Además, deben reflejarse las medidas de supervisión humana que sean necesarias<sup>13</sup>.

Esas instrucciones de uso son un elemento más que forma parte de los sistemas de transparencia a los que deben someterse los SIA que estén calificados de alto riesgo, por lo que forman parte del principio de transparencia algorítmica.

Y el fin de la transparencia es, tal y como se establece en el considerando 72 de RIA, permitir que los responsables del despliegue puedan hacer un uso adecuado del SIA, y, de esa manera, puedan tomar decisiones basadas en un conocimiento suficiente del SIA que están implementando. Esto les

---

13. Las técnicas de supervisión humana parecen una solución menos drástica que la reserva de humanidad, tal y como se firma en Ponce (2022: 64).

## ESTUDIOS

Los trece capítulos del libro abordan diversos aspectos del régimen jurídico y ético de la inteligencia artificial y de la biometría, con especial atención a la identificación biométrica, teniendo en cuenta el RIA, el RGPD y otras normas sobre identificación digital y ciberseguridad. Los estudios adoptan una perspectiva práctica y parten de la premisa de que la biometría no debe poner en riesgo los derechos fundamentales de las personas y, al mismo tiempo, puede contribuir a su protección frente a las limitaciones de los métodos de identificación no biométricos. La legislación permite el uso de los sistemas de identificación biométrica, los cuales son los únicos que garantizan la identidad cierta (y no presunta) de las personas. Además, la implantación de tecnologías biométricas adecuadas que aseguren la privacidad por defecto y desde el diseño —como las basadas en Referencias Biométricas Renovables— favorecerá la implantación en nuestra sociedad una inteligencia artificial centrada en el ser humano, fiable y segura.

ISBN: 978-84-1085-159-7

