

Índice General

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

CAPÍTULO IV

Los sistemas biométricos en el Reglamento de Inteligencia Artificial

MARTÍN MARÍA RAZQUIN LIZARRAGA.....	127
1. Premisas fundamentales: concepto, finalidad y uso de datos biométricos	128
1.1. <i>Concepto de datos biométricos</i>	128
1.2. <i>Finalidad y tipos de uso de datos biométricos</i>	129
2. El enfoque de riesgo como base para la clasificación de los sistemas de IA que utilizan datos biométricos	132
3. Usos inaceptables de datos biométricos. Las prácticas prohibidas	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
4. Sistemas de IA de alto riesgo por el uso de datos biométricos	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
5. Sistemas de IA de riesgo limitado	153
6. Sistemas de IA de bajo o nulo riesgo	154
7. El estado de la ciencia sobre las técnicas biométricas	155
8. El necesario equilibrio entre protección (RGPD) e innovación (RIA). la posición de la AEPD y del CEPD	158
9. Conclusiones	163
10. Bibliografía	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
1. Introducción	168
2. La regulación inicial del Reglamento eIDAS y su limitado ámbito de aplicación en el sector público	169
3. La cartera de identidad digital europea como piedra angular del ecosistema eIDAS2	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
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	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
5. Reflexión final	183
Bibliografía	185
CAPÍTULO VI	
El derecho al uso de los propios datos biométricos	
JOSÉ FRANCISCO ALENZA GARCÍA	187
1. La evolución de la acreditación de la identidad personal	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
2. Diversidad de tecnologías biométricas y diversidad de usos biométricos; en particular, las disruptivas referencias biométricas renovables	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
3. La identificación biométrica como sistema legalmente permitido y de riesgo bajo o inexistente	203

	<i>Página</i>
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
4. Fundamentos del derecho al uso de los propios datos biométricos	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
5. Conclusiones. Mis datos son míos: el derecho a usar mis datos biométricos para acreditar mi identidad.....	227
6. Bibliografía	231

CAPÍTULO VII

Transparencia, sistemas biométricos y Administraciones públicas

ARITZ ROMEO RUIZ.....	233
1. ¿Transparencia? ¿Qué transparencia?	234
2. La transparencia algorítmica	236
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
3. Transparencia y protección de datos biométricos.....	254
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
4. Transparencia administrativa: cuando es la Administración la que usa un SIA biométrico	260
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
5. A modo de reflexión final	279
6. Bibliografía	281

CAPÍTULO VIII

La protección jurídica de las personas vulnerables ante la biometría

MIREN SARASÍBAR IRIARTE	287
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).....	288
2. Los beneficios del uso de la biometría en las personas vulnerables	292
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
3. Los riesgos y sesgos en relación con la biometría y la consecuente afección a los derechos.....	296

	<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
4. La repercusión de la biometría en el Reglamento General de Protección de Datos	305
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
5. Los sistemas biométricos en el reciente Reglamento europeo de inteligencia artificial	311
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
6. Reflexión final	319
7. Bibliografía	320

CAPÍTULO IX

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

RUBÉN MARTÍNEZ GUTIÉRREZ	323
1. Introducción. La administración de datos en la era de la inteligencia artificial	323
2. La centralidad e importancia del dato en la UE	324
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
3. La interoperabilidad como conexión entre los datos y los sistemas de IA	328

	<i>Página</i>
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
4. Requisitos para la automatización en el intercambio de datos	331
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
5. Bibliografía	342

CAPÍTULO X

Contratación pública de sistemas biométricos y de inteligencia artificial

FCO. JAVIER VÁZQUEZ MATILLA.....	345
1. Introducción	345
2. La compra pública de soluciones que incorporen biometría	351
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
3. Inteligencia artificial y contratación pública	363
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
4. Conclusiones.....	369
5. Bibliografía	370
CAPÍTULO XI	
La ciberseguridad en las Administraciones públicas: regulación y gestión	
DOLORS CANALS AMETLLER.....	373
1. Introducción: las distintas acepciones del término «ciberseguridad».....	373
2. La regulación de la seguridad digital: entre lo normativo y lo no normativo	378
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
3. La gestión de los riesgos digitales	395
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
Bibliografía citada.....	402

CAPÍTULO XII

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

MARCO CALABRÒ.....	405
1. Prólogo.....	405
2. Evolución reciente del debate sobre la inteligencia artificial en el derecho administrativo italiano.....	407
3. Biometría y Administración pública en Italia: una relación aún por explorar.....	411
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
4. Seguridad urbana y uso de modelos de control biométrico..	418
5. Conclusiones.....	424
Bibliografía.....	426

CAPÍTULO XIII

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

MAITENA POELEMANS.....	433
1. Introducción.....	433
2. El uso de tecnología algorítmica legitima un marco legal para encuadrar la videovigilancia (VVA).....	436
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
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.....	441

	<i>Página</i>
4. La conformidad constitucional de la ley	443
5. Las principales aplicaciones de las cámaras de VVA.....	445
6. Las cuestiones pendientes.....	447
6.1. <i>¿Un verdadero experimento temporal?</i>	447
6.2. <i>¿Una verdadera exclusión de la biometría?</i>	448
7. La importancia de los controles	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
8. Conclusión: la necesidad de encontrar un equilibrio entre eficacia y democracia.....	451
9. Bibliografía	452
 CONCLUSIONES DEL CONGRESO INTERNACIONAL «BIOMETRÍA, DERECHO ADMINISTRATIVO Y DATOS», CELEBRADO EN PAMPLONA LOS DÍAS 7 Y 8 DE NOVIEMBRE DE 2024.....	 453