

ESTUDIOS

CLAVES DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL: ANÁLISIS Y COMENTARIOS

ANTONIO JOSÉ SÁNCHEZ SÁEZ
DIRECTOR

INCLUYE LIBRO
ELECTRÓNICO

III ARANZADI

© Antonio José Sánchez Sáez (Dir.) y otros, 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/publicaciones>

Primera edición: 2025

Depósito Legal: M-11683-2025

ISBN versión impresa con complemento electrónico: 978-84-1085-123-8

ISBN versión electrónica: 978-84-1085-124-5

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, 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

CAPÍTULO 1

ALINEAMIENTO Y ACTUACIÓN ÉTICA DE LA INTELIGENCIA ARTIFICIAL

FERNANDO H. LLANO ALONSO	17
1. Introducción	18
2. La IA fuerte y el alineamiento de sus objetivos con los valores humanos	22
3. La ética de la IA y la ampliación de los principios de la bioética	25
4. ¿Hacia una superinteligencia artificial en la era de la singularidad tecnológica?.....	31
5. Conclusión	35
6. Bibliografía	36

CAPÍTULO 2

TRANSPARENCIA Y PUBLICIDAD EN EL USO DE ALGORITMOS Y DE INTELIGENCIA ARTIFICIAL EN EL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL: ESPECIAL REFERENCIA A LAS OBLIGACIONES DE TRANSPARENCIA REFERIDAS A LOS PODERES PÚBLICOS

ANDRÉS BOIX PALOP.....	39
1. El Reglamento europeo de Inteligencia artificial y su aplicación a los poderes públicos.....	41

2.	La transparencia algorítmica y su plasmación en el Reglamento Europeo de Inteligencia Artificial	44
3.	Algunas consideraciones sobre las obligaciones de transparencia en el uso de la IA y su aplicación por parte del RIA específicamente a los usos de IA llevados a cabo por los poderes públicos	49
	3.1. <i>Regulación de la IA en la administración pública y evaluación de su uso y del impacto en derechos fundamentales.</i>	52
	3.2. <i>Obligaciones de transparencia y de registro sobre el proceso de toma de decisiones algorítmicas o por IA</i>	54
	3.3. <i>El modelo de supervisión humana y su especial importancia para la transparencia y control de los algoritmos e IA empleados por las Administraciones Públicas</i>	56
	3.4. <i>Algunas ideas básicas sobre la implantación de sistemas de IA en la Administración pública</i>	57
4.	Algunas conclusiones finales.	60
5.	Bibliografía citada	61

CAPÍTULO 3

GARANTÍAS JURÍDICAS DEL CUMPLIMIENTO DE LOS REQUISITOS OBLIGATORIOS PARA LOS SISTEMAS DE ALTO RIESGO Y LOS MODELOS DE INTELIGENCIA ARTIFICIAL DE USO GENERAL

	JUAN ANTONIO CARRILLO DONAIRE	65
1.	El equilibrio entre seguridad y riesgos tolerados en el modelo regulatorio europeo de la inteligencia artificial	66
	1.1. <i>Aspectos comunes a la determinación del riesgo tolerable y al control de la seguridad de los productos. Los modelos regulatorios basados en la gestión de riesgos (risk-based regulation)</i>	66
	1.2. <i>El «nuevo enfoque» de armonización en materia de comercialización y seguridad de productos en la UE: normativa marco del Reglamento de Inteligencia Artificial.</i>	72

2. Requisitos esenciales obligatorios, normas técnicas y especificaciones comunes. El efecto de presunción de conformidad con los requisitos obligatorios del Reglamento de Inteligencia Artificial.	79
2.1. <i>Normas técnicas armonizadas y documentos europeos de normalización de los organismos de normalización</i>	84
2.2. <i>Especificaciones comunes de la Comisión</i>	87
2.3. <i>Otras soluciones técnicas equivalentes</i>	89
3. El control del cumplimiento de los requisitos esenciales . .	90
3.1. <i>Distinción entre sistemas integrado y no integrados.</i>	91
3.2. <i>Procedimientos de evaluación de conformidad, certificados de conformidad, marcado CE y registro de los sistemas de IA de alto riesgo</i>	93
4. Organismos notificados, autoridades notificantes y procedimiento de notificación	97

CAPÍTULO 4

AUTOMATIZACIÓN, DISCRECIONALIDAD Y SUPERVISIÓN HUMANA A LA VISTA DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL AGUSTÍ CERRILLO I MARTÍNEZ.	105
1. La automatización de la Administración pública	106
2. Los límites del uso de la inteligencia artificial en la actuación administrativa automatizada.	109
3. ¿Es posible la automatización del ejercicio de potestades discrecionales?	112
4. La supervisión humana como garantía del uso de la inteligencia artificial en la Administración pública	122
4.1. <i>La supervisión humana</i>	122
4.2. <i>La supervisión humana en el RIA</i>	126
4.3. <i>La supervisión humana en la legislación de régimen jurídico del sector público</i>	132

	<i>Página</i>
4.4. <i>Elementos de la supervisión humana para el ejercicio de potestades discrecionales</i>	134
5. Reflexiones finales	136
6. Referencias bibliográficas	138

CAPÍTULO 5

EL IMPACTO DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL EN LA ADMINISTRACIÓN AUTÓNOMICA

ANTONIO LUIS FAYA BARRIOS	147
1. Introducción	149
2. La transición digital y la IA en el ámbito de la Administración andaluza con anterioridad al RIA.	150
2.1. <i>Administraciones públicas en España y transición digital</i> ...	150
2.2. <i>En particular, la Administración de la Junta de Andalucía y la transición digital</i>	154
2.2.1. La Agencia Digital de Andalucía	155
2.2.2. Estrategia Andaluza de Inteligencia Artificial 2030	156
2.2.3. Guía para el diseño de ayudas. Con un enfoque orientado a la automatización.	156
3. El impacto del RIA en las Administraciones Públicas y en particular en la autonómica	156
3.1. <i>La pluralidad de posiciones jurídicas de la administración que el RIA trae consigo</i>	157
3.2. <i>El RIA condiciona los ámbitos en los que las administraciones pueden utilizar sistemas de inteligencia artificial</i>	159
3.2.1. Los condicionantes absolutos: supuestos de uso de inteligencia artificial prohibidos a las administraciones públicas	159
3.2.2. Los condicionantes relativos: los sistemas de inteligencia artificial de alto riesgo	161

	<i>Página</i>
3.2.3. Régimen jurídico de aplicación en Andalucía tras la aprobación del RIA.	164
4. A modo de conclusión. El camino por recorrer y las competencias de la Comunidad Autónoma de Andalucía	170
5. Bibliografía	173

CAPÍTULO 6

LA PREVENCIÓN DE LOS RIESGOS DEL USO DE IA PARA LA CIUDADANÍA: EL INFORME DE EVALUACIÓN DE IMPACTO RELATIVO A LOS DERECHOS FUNDAMENTALES

EVA M. ^a MENÉNDEZ SEBASTIÁN	175
1. Planteamiento	177
2. Contexto	178
3. De la burocracia a la IA: el eterno equilibrio entre eficacia y garantías	179
3.1. <i>¿IA lógica o IA conexionista?</i>	180
3.2. <i>Potestades regladas y potestades discrecionales.</i>	181
3.3. <i>¿Mejores servicios o más control?</i>	184
3.4. <i>Eficacia versus garantías.</i>	185
4. Los riesgos y las oportunidades del uso de IA en el sector público	187
5. El enfoque adoptado por el Reglamento europeo de IA.	193
6. El informe de evaluación de impacto relativo a los derechos fundamentales	197
6.1. <i>Ámbito objetivo: ¿a qué sistemas de IA se les exige este control?</i>	199
6.2. <i>Ámbito subjetivo: la particularidad del sector público.</i>	202
6.3. <i>Contenido de la evaluación</i>	204
7. Conclusiones	207
8. Bibliografía	208

CAPÍTULO 7

EL REGLAMENTO EUROPEO DE IA DESDE LA PERSPECTIVA DEL DERECHO ADMINISTRATIVO: ¿UNA NORMA DECEPCIONANTE?

ORIOU MIR.	215
1. Introducción	216
2. La decepción inicial cuando se examina el RIA desde la perspectiva del Derecho administrativo	218
2.1. <i>El enfoque basado en la regulación de la seguridad de los productos y la protección de datos.</i>	218
2.2. <i>El limitado número de sistemas sujetos a sus previsiones más publicitadas</i>	222
2.3. <i>La demorada entrada en vigor del RIA, que en el caso de las autoridades públicas podrá extenderse hasta 2030</i>	226
3. La gran importancia del RIA para la toma automatizada de decisiones administrativas (adm-ADM) por parte de las autoridades públicas europeas.	226
3.1. <i>Prohibición de sistemas de IA propios de regímenes autoritarios</i>	227
3.2. <i>La importancia de los sistemas de IA de alto riesgo empleados por las autoridades públicas</i>	228
3.3. <i>La imposición de condiciones detalladas para el desarrollo de sistemas de alto riesgo por parte de las autoridades públicas y sus contratistas</i>	229
3.4. <i>La imposición de condiciones detalladas para el uso de sistemas de alto riesgo por parte de las autoridades públicas</i>	231
3.5. <i>Otras cuestiones relevantes</i>	236
4. Final.	237
5. Bibliografía	238

CAPÍTULO 8

**RÉGIMEN JURÍDICO DE LOS PROVEEDORES Y
RESPONSABLES DEL DESPLIEGUE DE SISTEMAS DE IA:
SUS OBLIGACIONES Y DERECHOS**

RICARDO RIVERO ORTEGA.	241
1. La necesaria definición del estatuto de los operadores económicos y los innovadores	241
2. Los destinatarios del Reglamento europeo de IA	244
3. Las obligaciones: preventivas e informativas	248
4. El problema de la definición de los deberes en normas técnicas que varían a lo largo del tiempo	254
5. Los derechos y las garantías	255
6. ¿Quién supervisa el cumplimiento de las obligaciones y protege los derechos?	258
7. Un estatuto que variará en tiempo real y debe ser versátil .	260
8. Referencias bibliográficas	261

CAPÍTULO 9

**LOS DATOS BIOMÉTRICOS EN EL REGLAMENTO
EUROPEO DE INTELIGENCIA ARTIFICIAL**

ANTONIO JOSÉ SÁNCHEZ SÁEZ.	265
1. Planteamiento del problema: eficacia versus derechos fundamentales	266
2. La verificación biométrica	270
3. La categorización biométrica	276
3.1. <i>Concepto y distinción de figuras afines</i>	276
3.2. <i>La finalidad del cumplimiento del derecho como legitimadora de la categorización biométrica y de la identificación biométrica</i>	278
4. La identificación biométrica remota en tiempo real	282

	<i>Página</i>
4.1. <i>En espacios públicos: SIA de alto riesgo y sus implicaciones .</i>	282
4.2. <i>La autoridad nacional de vigilancia del mercado en esta materia</i>	289
4.3. <i>La identificación biométrica en tiempo real en espacios privados</i>	291
4.4. <i>La identificación biométrica en espacios públicos en diferido .</i>	295
4.5. <i>El uso de SIA de identificación biométrica al margen de la finalidad de garantía del cumplimiento del Derecho</i>	298
4.6. <i>¿Cómo se lleva a cabo la evaluación de conformidad de los sistemas de IA que empleen biometría?</i>	300
4.7. <i>Uso de los sistemas de identificación biométrica con fines de seguridad nacional</i>	302
5. Bibliografía	303

CAPÍTULO 10

LA INTELIGENCIA ARTIFICIAL COMO INSTRUMENTO PARA LA ADMINISTRACIÓN PÚBLICA: UNA REFERENCIA AL SILENCIO ADMINISTRATIVO

MIREN SARASÍBAR IRIARTE	307
1. La consideración de la inteligencia artificial como un instrumento	308
2. La intervención de la inteligencia artificial en las actuaciones administrativas	310
2.1. <i>Actuaciones automatizadas y actuaciones autónomas.</i>	310
2.2. <i>Las limitaciones del Reglamento europeo de inteligencia artificial respecto del uso de la inteligencia artificial por la Administración</i>	314
3. La persona como fundamento principal del uso de la Inteligencia Artificial por la Administración pública	318
3.1. <i>El interés general como finalidad de la actuación administrativa</i>	318
3.2. <i>La necesaria protección de las garantías del particular</i>	319

	<i>Página</i>
4. La buena administración digital	321
4.1. <i>La «bondad» de la administración hasta en lo digital</i>	321
4.2. <i>El necesario cumplimiento de la obligación de motivación</i> ...	323
5. El reto del uso de la Inteligencia Artificial ante la figura del silencio administrativo	327
6. Bibliografía	334

CAPÍTULO 11

LA INTELIGENCIA ARTIFICIAL Y LA PRIVACIDAD: DESAFÍOS Y OPORTUNIDADES EN LA ERA DE LA ECONOMÍA DEL DATO

MIGUEL A. ADAME MARTÍNEZ	339
1. Introducción	341
2. Marco legal y regulatorio	343
2.1. <i>Evolución del marco normativo</i>	343
2.2. <i>El Reglamento General de Protección de Datos (RGPD)</i>	346
2.3. <i>El Reglamento 2023/2854. Ley Europea de Datos (Data Act)</i>	348
2.4. <i>El Reglamento 2024/1698 (IA Act)</i>	349
2.5. <i>La Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial</i>	352
3. Desafíos específicos de la IA para la privacidad: el concepto de privacidad y su posible vulneración por la IA	353
3.1. <i>El concepto de privacidad. Las formas de privacidad. Elementos comunes y diferenciadores</i>	353
3.2. <i>Las posibles formas de infracción</i>	360
3.3. <i>Derecho al olvido y IA</i>	364
3.4. <i>La llamada privacy fallacy</i>	365
4. Estrategias técnicas para la protección de la privacidad en sistemas de IA	370
4.1. <i>Anonimización y seudonimización</i>	371

	<u>Página</u>
4.2. <i>Privacidad diferencial</i>	375
4.3. <i>Aprendizaje federado y Criptografía homomórfica</i>	376
5. El papel del consentimiento en la era de la IA	376
5.1. <i>Aspectos clave del consentimiento y su revocación en las distintas advocaciones de la privacy</i>	377
5.2. <i>Evolución del concepto de consentimiento en la protección de datos</i>	378
5.3. <i>Limitaciones del consentimiento en la protección de datos en el contexto de la IA</i>	378
5.4. <i>El papel del consentimiento en la Estrategia Europea de Datos</i>	379
5.5. <i>El consentimiento en la Ley Europea de Datos (Data Act)</i>	380
5.6. <i>Diferencias de exigencia de consentimiento en distintas normas sectoriales</i>	382
6. Espacios europeos de datos y su relación con la privacidad	384
7. La insuficiencia de la teoría contractualista para proteger la privacidad	385
8. Retos éticos y sociales	406

Capítulo 3

Garantías jurídicas del cumplimiento de los requisitos obligatorios para los sistemas de alto riesgo y los modelos de Inteligencia Artificial de uso general

JUAN ANTONIO CARRILLO DONAIRE
Universidad de Sevilla

SUMARIO: 1. EL EQUILIBRIO ENTRE SEGURIDAD Y RIESGOS TOLERADOS EN EL MODELO REGULADORIO EUROPEO DE LA INTELIGENCIA ARTIFICIAL. 1.1. *Aspectos comunes a la determinación del riesgo tolerable y al control de la seguridad de los productos. Los modelos regulatorios basados en la gestión de riesgos (risk-based regulation).* 1.2. *El «nuevo enfoque» de armonización en materia de comercialización y seguridad de productos en la UE: normativa marco del Reglamento de Inteligencia Artificial.* 2. REQUISITOS ESENCIALES OBLIGATORIOS, NORMAS TÉCNICAS Y ESPECIFICACIONES COMUNES. EL EFECTO DE PRESUNCIÓN DE CONFORMIDAD CON LOS REQUISITOS OBLIGATORIOS DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL. 2.1. *Normas técnicas armonizadas y documentos europeos de normalización de los organismos de normalización.* 2.2. *Especificaciones comunes de la Comisión.* 2.3. *Otras soluciones técnicas equivalentes.* 3. EL CONTROL DEL CUMPLIMIENTO DE LOS REQUISITOS ESENCIALES. 3.1. *Distinción entre sistemas integrado y no integrados.* 3.2. *Procedimientos de evaluación de conformidad, certificados de conformidad, marcado CE y registro de los sistemas de IA de alto riesgo.* 4. ORGANISMOS NOTIFICADOS, AUTORIDADES NOTIFICANTES Y PROCEDIMIENTO DE NOTIFICACIÓN.

1. EL EQUILIBRIO ENTRE SEGURIDAD Y RIESGOS TOLERADOS EN EL MODELO REGULATORIO EUROPEO DE LA INTELIGENCIA ARTIFICIAL

1.1. ASPECTOS COMUNES A LA DETERMINACIÓN DEL RIESGO TOLERABLE Y AL CONTROL DE LA SEGURIDAD DE LOS PRODUCTOS. LOS MODELOS REGULATORIOS BASADOS EN LA GESTIÓN DE RIESGOS (RISK-BASED REGULATION)

La reacción jurídica frente el riesgo tecnológico ha alumbrado en las últimas décadas una nueva concepción de la intervención pública en la Unión Europea que rebasa las tradicionales formas y procedimientos administrativos de intervención en los productos que generan riesgos para los consumidores. El reto jurídico de este modelo regulatorio basado en el riesgo es definir el riesgo asumible o tolerable y sus límites y prohibiciones, de un lado; y, de otro, establecer cómo se gestiona y controlan los riesgos permitidos.

La insuficiencia de las tradicionales medidas administrativas de carácter correctivo e imperativo frente a los riesgos del progreso tecnológico, ha hecho emerger soluciones jurídicas que rompen el esquema clásico en un triple plano: desde una perspectiva funcional u objetiva, también en su enfoque instrumental o procedimental y, en tercer lugar, en el plano subjetivo de los actores del sistema de control.

El plano funcional muestra una evolución de la acción correctiva puntual a una acción integral que pone el acento en la dimensión preventiva. En el plano instrumental se advierte el afloramiento de técnicas jurídicas nuevas que fuerzan la reconstrucción de categorías jurídicas clásicas en ámbitos como el sistema de fuentes, la técnica autorizatoria, el procedimiento administrativo de control o el régimen de responsabilidad. El plano subjetivo está marcado por la retirada de la Administración y la correlativa privatización de la gestión del riesgo, lo que ha supuesto el mayor protagonismo de la sociedad y del mercado, que —antes que en la propia Administración— es donde habita hoy el conocimiento experto. Más allá de una inicial colaboración de carácter meramente instrumental, el Derecho ha acabado por reconocer efectos jurídico-administrativos a las referencias técnicas generadas y a los controles ejercidos por estos sujetos especializados.

Las relaciones entre técnica y Derecho se han alterado profundamente en el contexto de la llamada «sociedad del riesgo»¹ en la que los peligros y

1. BECK, U., *Risk Society: Towards a New Modernity*, Sage Publications, London 1992; GIDDENS, A., BAUMAN, Z. LUHMANN, N., BECK, U., *Las consecuencias perversas de la modernidad: modernidad, contingencia y riesgo*, Anthropos, Barcelona 1996; ADAM, B., BECK, U., VAN LOON, J., *Positioning Risk*, Sage Publications, London, 1999;

amenazas potenciales no tienen ya su origen en una naturaleza indómita, sino en la actividad humana que persigue dominarla y ponerla a su servicio mediante el conocimiento científico y su aplicación técnica y tecnológica.

Una de las finalidades principales del desarrollo científico es paliar los peligros naturales, las amenazas y los riesgos conocidos. Pero, paradójicamente, a medida que avanza el conocimiento científico, la industrialización y la tecnología generan nuevos riesgos que muchas veces son imprevisibles y, en gran parte, desconocidos. Estos riesgos inherentes al desarrollo se manifiestan en todas y cada una de las actividades económicas y sociales. En los últimos tiempos, el extraordinario desarrollo de la inteligencia artificial se ha convertido en el mejor ejemplo de ello. Como expresamente reconoce el Reglamento (UE) 2024/1689 del Parlamento y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial), *dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concretos, la IA puede generar riesgos y menoscabar los intereses públicos y los derechos fundamentales que protege el Derecho de la Unión. Dicho menoscabo puede ser tangible o intangible e incluye los perjuicios físicos, psíquicos, sociales o económicos* (Cdo. 5.^o).

El concepto de riesgo empieza a tomar cuerpo allí donde se desvanece la confianza en la seguridad, y deja de ser relevante cuando ocurre el daño. El concepto habita, por tanto, en una zona intermedia entre la seguridad y la consumación de un daño, en la que reina la incertidumbre, adoptando la forma de un cálculo de probabilidades que expresa las posibles consecuencias indeseables ligadas a una determinada tecnología cuya aparición o efectos no se pueden determinar *a priori*. Desde un punto de vista cualitativo, los riesgos del progreso se caracterizan porque uno de los dos factores del riesgo, el daño posible o potencial, es esencialmente indeterminado y en gran medida imprevisible, de pronóstico incierto y conjetural. Desde un punto de vista cuantitativo, también es característico de este tipo de riesgos que el otro factor determinante de los mismos, la probabilidad de que el daño acontezca, se multiplica exponencialmente en una espiral creciente que es directamente proporcional al aumento del desarrollo tecnológico. Por ello, los riesgos del progreso constituyen un poderoso factor de desestabilización que cuestiona constantemente el papel y la legitimidad de las instancias políticas y administrativas con responsabilidades de control de la salud y la seguridad en materia de consumo o sobre la protección ambiental. Desde esta perspectiva, el desarrollo y expansión de la inteligencia arti-

ESTEVE PARDO, J., *El desconcierto de Leviatán. Política y derecho ante las incertidumbres de la ciencia*, Marcial Pons, Madrid 2009.

ficial supone una amenaza que es preciso regular jurídicamente desde un modelo basado en la gestión del riesgo. Modelo bien conocido en la Unión Europea en el marco de la legislación de seguridad de los productos, como más adelante veremos.

En la conjura de este desafío, el Derecho desempeña una función capital que requiere delimitar con claridad las relaciones entre técnica y Derecho y el papel de cada una de estas esferas en el tratamiento de los riesgos del progreso. Este es el objetivo de los modelos regulatorios basados en la gestión de riesgos, que es el que adopta el Reglamento de Inteligencia Artificial, que en su Cdo. 26.º declara que *con el fin de establecer un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, es preciso aplicar un enfoque basado en los riesgos claramente definido, que adapte el tipo y contenido de las normas a la intensidad y el alcance de los riesgos que puedan generar los sistemas de IA de que se trate. Por consiguiente, es necesario prohibir determinadas prácticas de IA que no son aceptables, definir los requisitos que deben cumplir los sistemas de IA de alto riesgo y las obligaciones aplicables a los operadores pertinentes, así como imponer obligaciones de transparencia a determinados sistemas de IA*².

El Derecho tiene una función racionalizadora de las relaciones entre técnica y riesgo y un innegable protagonismo directivo para arbitrar los criterios y procedimientos de toma de decisiones en un entorno de riesgo e incerteza. Pero, para orientar las soluciones jurídicas, el Derecho ha de tomar postura ante algunas cuestiones previas: el conocimiento, el análisis y la valoración de los riesgos del progreso. En el tratamiento jurídico del riesgo pueden diferenciarse estas tres fases que comprometen con desigual alcance al mundo del Derecho: la percepción o reconocimiento del riesgo, su valoración y su gestión y control.

- a) En primer lugar, la cuestión de la *percepción o reconocimiento del riesgo* es clave, puesto que lo que determina la acción frente al riesgo es su perceptibilidad y la información disponible sobre el mismo.

2. HACKER, F., «A legal framework for AI training data-from first principles to the Artificial Intelligence Act», *Law, Information and Technology*, n.º 13, 2021 <https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1977219>; LAXU, J., WACHTER, S., MITTELSTADT, B., «Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk», *Regulation and Governance*, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4230294; STUURMAN, K., LACHAUD, E., «Regulating AI. A Label To Complete the Proposed Act on Artificial Intelligence», 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3963890; NOVELLI, C., CASOLARI, F., ROTOLO, A., TADEO, M., FLORIDI, L., «How to evaluate the risks of Artificial Intelligence: a proportionality-based, risk model for the AI Act», 2023 https://www.researchgate.net/publication/372335638_AI_Risk_Assessment_A_Scenario-Based_Proportional_Methodology_for_the_AI_Act

El conocimiento y la definición de los concretos riesgos a los que nos enfrentamos constituyen un problema especialmente agudo y difícil. La razón es que los riesgos que genera nuestra forma de vida tan tecnificada son, tanto en un plano espacial como temporal, tendencialmente abiertos e indefinidos. Espacialmente abiertos porque el riesgo tiende a mundializarse. La expansión global de la inteligencia artificial y de los modelos de IA de uso general y de carácter generativo son ejemplos relevantes de esta fuerza expansiva y globalizadora del riesgo. En una dimensión temporal, el riesgo tecnológico es altamente veleidoso e imperceptible, mostrándose muchas veces al conocimiento de un modo simplemente indiciario; cuando no permanece ignoto, amenazadoramente oculto hasta eclosionar en forma de amenaza real o de daño cierto. Catástrofes ecológicas como la destrucción de la capa de ozono, el cambio climático o los daños en los sistemas inmunológicos provocados por sustancias manipuladas no se han presentado como síntomas hasta años después que empezaran a producirse de modo desapercibido. Todavía son imprevisibles o desconocidos muchos efectos del manejo del big data, el funcionamiento de los algoritmos de caja negra, u otras amenazas que acaso serán síntomas en el futuro, o tras combinarse con otros factores con los que puedan formar masa crítica³.

Aunque la percepción del riesgo atañe principalmente a las ciencias naturales y experimentales, es el orden jurídico quién ha de señalar cuáles son las referencias técnicas que determinan la inocuidad o peligrosidad de los productos y actividades riesgosas; qué tipo de conocimiento —o desconocimiento sobre las causas— se halla implicado en cada caso; y, a la postre, qué opiniones o hechos pueden considerarse como prueba suficiente en un contexto controvertido y probabilista. Asimismo, el Derecho ha de resolver cuestiones instrumentales a ésta como el procedimiento y las garantías que han de observarse para apreciar correctamente las evidencias del riesgo. Y también compete al Derecho la regulación del deber de información, de singular importancia en este ámbito en el que la escasez de información contrasta con la imperiosa necesidad de conocer para proteger, que ha de entrañar obligaciones específicas para los productores en la generación y puesta a disposición de la información.

3. Son muy reveladores los ejemplos que expone O'NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, 2016.

- b) En segundo lugar, la *valoración del riesgo* alude al problema ponderativo de su asunción o rechazo. Pese a necesitar del antecedente del experto, esta actividad concierne de forma directa al orden jurídico. El Derecho tiene que decidir qué riesgos se asumen y cuales se rechazan mediante la definición de las nociones jurídicas de «seguridad» y «peligro», que decantan los niveles de riesgo tolerable e intolerable o prohibido. Dicho de otro modo, la valoración del riesgo requiere la discriminación entre riesgos jurídicamente relevantes y riesgos residuales, que lleva a establecer qué riesgos conocidos o reconocibles son asumibles y cuáles no en función de los bienes jurídicos en juego o de los afectados potenciales. En definitiva, esta operación consiste en calificar como riesgo la probabilidad de que ocurra un daño que se considera antijurídico y en diseñar, mediante un sistema de presunciones, mecanismos capaces de definirlo y minimizarlo, a partir de los cuales puedan establecerse consecuencias jurídicas.
- c) En tercer y último lugar, la *gestión, control y mitigación del riesgo* alude a la toma de decisiones frente al mismo, que es donde se aprecia con toda su agudeza la tensión entre el elemento científico-técnico y el elemento jurídico. En ella se trata de decidir la crucial cuestión de cuáles son las medidas de protección y de reacción que deben adoptarse ante el riesgo antijurídico, junto las consiguientes garantías procedimentales. Asimismo, la gestión del riesgo ha de abordar las consecuencias de su consumación y, por tanto, fijar cuándo hay responsabilidad en casos de daño y quién la asume.

A la vista de estas finalidades, el contexto de incertidumbre que caracteriza la gestión de los riesgos del progreso aboca a un planteamiento jurídico esencialmente precautorio y discrecional, en el que la constatación de la existencia de un riesgo, con independencia de su mayor o menor certidumbre, inclina a adoptar acciones imbricadas a una idea de prevención formulada en sentido negativo: lo que no habría de hacerse o hay que impedir para evitar la consumación de lo que hoy es simple incertidumbre.

Para realizar estas tareas de reconocimiento, valoración y gestión de los riesgos, los Estados se encuentran desbordados para gestionar las situaciones de riesgo con el grado de rapidez y competencia que éstas demandan. Antes que la Administración, hoy son las grandes empresas y las organizaciones profesionales quienes disponen del mayor y mejor conocimiento científico-técnico. La protección jurídica frente al riesgo aconseja aprovechar estas mejores posibilidades cognitivas del sector privado e inclina a trasladar a éste aspectos esenciales de la determinación del riesgo tolerado, de su valoración y de la toma de decisiones en un entorno de incertidumbre.

El mayor interés jurídico de esta interpenetración de los respectivos mundos de la técnica y el Derecho se justifica sobre todo por el trascendente cambio cualitativo que se ha producido en el establecimiento, verificación y control de los requisitos técnicos exigibles a los productos e instalaciones con riesgos⁴. A partir sobre todo del llamado «nuevo enfoque» de armonización técnica de la Unión Europea, que más adelante analizaremos detenidamente, la colaboración de sujetos privados provenientes del mundo del conocimiento experto ha motivado una intensa penetración de la colaboración privada; de tal forma que, en la inmensa mayoría de los casos, son sujetos puramente privados altamente especializados los que ejercitan las funciones de inspección, certificación y autorización de productos y actividades productivas que impliquen un riesgo potencial para la salud, seguridad de las personas o el medioambiente. Junto a ello, la intervención de sujetos privados también se hace presente en el aparentemente más impenetrable ámbito de la función normativa, del establecimiento de la regla de Derecho. El mundo de la técnica ha necesitado siempre patrones de comportamiento que se han desarrollado con una marcada autonomía respecto al mundo de las normas jurídicas, a través de un «para-ordenamiento» de la técnica cuya expresión más acabada es el sistema de normalización industrial. El derecho encuentra aquí una fuente plena de conocimiento técnico de la que se sirve para arbitrar soluciones jurídicas en un doble plano: el del conocimiento y valoración jurídica de los riesgos y el de la fijación de los límites del riesgo tolerable. Las normas jurídicas tienden así a centrarse en las cuestiones formales y procedimentales y a definir los requisitos mínimos o esenciales que obligatoriamente han de cumplir los productos riesgosos, pero la regulación de los aspectos materiales y sustantivos para conseguir esos objetivos es confiada a «normas técnicas» que surgen de un singular fenómeno de autorregulación privada. Estas «normas técnicas» son de aplicación voluntaria, porque su destino natural es el ámbito convencional y contractual privado; sin embargo, el Derecho público se sirve constantemente de ellas por vía de remisión, confiriendo a dichas normas —inicialmente privadas y voluntarias— fuerza y efectos jurídicos vinculantes, de modo que su cumplimiento presume el cumplimiento de los requisitos de seguridad legalmente exigibles.

El recurso al sector privado por la incapacidad e insuficiencia de la Administración en estos modelos regulatorios basados en el riesgo es un fenómeno común a escala nacional, europea e internacional. El fenómeno

4. He dedicado a esta cuestión algunos trabajos: *El Derecho de la seguridad y calidad industrial*, Marcial Pons, Madrid-Barcelona, 2000; «Seguridad y calidad productiva: de la intervención policial a la gestión de riesgos», *Revista de Administración Pública*, n.º 178, 2009; y «Derecho, técnica y riesgo: el principio de precaución en el ámbito medioambiental», *Revista de Fomento Social*, n.º 71, 2016.

descrito determina una modulación de las relaciones Estado-sociedad en el ámbito de la técnica que da entrada a fórmulas de colaboración privada de una intensidad hasta ahora desconocidas, que se articulan mediante la atribución a las decisiones de sujetos privados de efectos jurídico-públicos que son propios y consustanciales al ejercicio de poder público. Otro efecto de esta modalidad de la colaboración público-privada es una cierta desmaterialización del Derecho aplicable, que abandona la determinación sustantiva del umbral de seguridad y del riesgo tolerable, y la disminución de la capacidad decisora de la Administración en el control de su cumplimiento. Con ello, la voluntad normativa y la fuerza directiva del Derecho se ve reemplazada por la supuesta legalidad y legitimidad del saber experto y del mercado.

La atribución de potestades a sujetos privados para el ejercicio de funciones públicas encierra un cierto peligro, pues los sujetos privados que reciben esas potestades en función de su mejor posicionamiento para afrontar el riesgo son muchas veces los mismos que se lucran generando ese riesgo, y también los que están más expuestos a los intereses del mercado. El recurso a estas fórmulas de colaboración encierra una paradoja difícilmente reductible, pues probablemente no haya situación más peligrosa para la libertad y la seguridad jurídica que un sujeto privado dotado de prerrogativas públicas. Por ello, es preciso diseñar garantías jurídicas de objetividad que compensen la pérdida de dominio público con un mayor protagonismo de los aspectos formales y procedimentales que aseguren la participación de todas las partes interesadas, la imparcialidad y la transparencia en la determinación y valoración del riesgo y en la toma de decisiones para prevenirlo o corregirlo. De lo contrario correríamos el riesgo de caer en una tecnocracia que hurtaría a las decisiones que corresponden a los poderes públicos su fuente de legalidad y de legitimidad.

1.2. EL «NUEVO ENFOQUE» DE ARMONIZACIÓN EN MATERIA DE COMERCIALIZACIÓN Y SEGURIDAD DE PRODUCTOS EN LA UE: NORMATIVA MARCO DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

La Unión Europea se ha dotado de mecanismos diversos para armonizar las disposiciones nacionales de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior (artículo 114 del Tratado de Funcionamiento de la Unión Europea) y garantizar la libre circulación de mercancías.

El establecimiento por los Estados miembros de requisitos técnicos fundamentados en razones de orden público, de seguridad, de protección de

la salud o de los intereses de los consumidores es una fuente potencial de trabas a la libre circulación de mercancías que justifica su unificación en todo el mercado de la Unión mediante medidas normativas de armonización de legislaciones que impongan requisitos técnicos comunes a la producción y distribución de productos.

Con la regulación armonizada de cada producto se consigue, además, unificar los niveles de calidad y de seguridad que respondan a los intereses de la Unión y garanticen la protección de los consumidores europeos.

Con esta finalidad regulatoria supranacional y de prevención de riesgos, la Unión Europea ha articulado diversos mecanismos legislativos. En el origen se empleó una técnica de armonización «total» (que se sigue utilizando para algunos productos, como los vehículos a motor), en la que la legislación de armonización establecía exhaustivamente los requisitos técnicos y de seguridad que tenían que satisfacer los productos y sistemas para comercializarse en todo el mercado de la Unión. Desde mediados de los años ochenta, y a partir de la Resolución del Consejo 85/C 136/01, de 7 de mayo de 1985, relativa a una nueva aproximación o «nuevo enfoque» en materia de armonización técnica de productos, se establece una nueva base del modelo armonizador⁵.

En este nuevo enfoque, las instancias europeas se limitan a armonizar exclusivamente las exigencias o requisitos esenciales que obligatoriamente deben satisfacer los productos para beneficiarse de su distribución y libre circulación en el mercado de la Unión, que normalmente se predicen como objetivos y finalidades que deben atender los productos y servicios. Para acreditar el cumplimiento de dichos requisitos obligatorios, la legislación

5. Sobre el «nuevo enfoque» de armonización técnica de legislaciones europeas existe una abundante bibliografía a nivel europeo, dentro de la que destacan algunos trabajos clásicos, como los de PELKMANS, J., «The New Approach to Technical Harmonization and Standardization», *Journal of Common Market Studies*, 1987, vol. 25, issue 3; o GAMBELLI, F., *Aspects juridiques de la normalisation et de la réglementation technique européenne*, Eyrolles/Fédération des industries mécaniques 1994. Asimismo destacan los trabajos más recientes de SCHEPEL, H., *The Constitution of Private Governance. Products Standards in the Regulation of Integrating Markets*, Hart Publishing, Oxford, 2005; o CANTERO, M., y MICKLITZ, M.W., (eds.), *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes*, Edward Elgar Publishing, 2020. Es de gran utilidad por su extensión y alcance el trabajo de SCHEPEL, H., y FALKE, J., *Legal aspects of standardisation in the Member States of the EC and EFTA*, EU publications, 2000, Vol. 1: *Comparative report*, European Communities, <https://op.europa.eu/en/publication-detail/-/publication/9acd4259-13c6-436f-8c12-2740ccf7bb71>; y Vol. 2: *Country reports*, European Communities, <https://op.europa.eu/en/publication-detail/-/publication/3f721f1e-51c1-4cc1-beca-bd48023676b4>

de armonización no establece directamente los parámetros técnicos que han de observarse, remitiéndose para ello a las normas técnicas (EN) que elaboran los organismos de normalización europeos que serán las que establezcan esos parámetros. Dichos organismos no son instituciones de la UE, son sujetos de Derecho privado en los que están representados los operadores del mercado, las asociaciones empresariales y profesionales, las Asociaciones de consumidores los organismos de normalización de los Estados miembros y de terceros países del Espacio Económico Europeo y la propia Comisión Europea. Para el desarrollo de las especificaciones técnicas que garantizarían a producción conforme a dichos requisitos, la Comisión otorga mandatos de normalización a los organismos europeos de normalización para adoptar las normas europeas armonizadas (normas técnicas EN). Dichos organismos son el Comité Europeo de Normalización (CEN), cuyas funciones normalizadoras se extienden a todos los ámbitos de la seguridad y la calidad industrial, excluyendo la electrotecnia y las telecomunicaciones; el Comité Europeo de Normalización Electrotécnica (CENELEC) especializado en la normalización electrotécnica, y el Instituto Europeo de Normas de Telecomunicaciones, redes y servicios de comunicaciones electrónicas (ETSI).

Las normas técnicas que aprueban estos organismos (EN) no tienen carácter obligatorio, conservando su condición de normas voluntarias que nacen del consenso de los sectores afectados a partir del estado de la técnica. No obstante, las Administraciones han de reconocer a los productos fabricados de acuerdo con las mismas una presunción de conformidad con las exigencias esenciales que establece el Reglamento o la Directiva de armonización del «nuevo enfoque», lo que se acredita mediante un sistema de verificación basado también en la certificación experta e independiente que emite un prestador de servicios de certificación que realiza un control externo al fabricante. Estos organismos de certificación (organismos «notificados» en la terminología del «nuevo enfoque») son en su gran mayoría operadores privados, cuya solvencia técnica e independencia ha sido previamente acreditada para un determinado sector por otra entidad privada e independiente acreditación, que ha sido autorizada por un Estado miembro a tal efecto.

La técnica armonizadora del «nuevo enfoque» se basa en tres elementos básicos: a) en primer término, la existencia de unos requisitos esenciales obligatorios que debe respetar un producto y que se fijan directamente por el acto legislativo de armonización (Directiva o Reglamento); b) en segundo término, la regulación de las especificaciones técnicas que facilitan la justificación de la conformidad del producto con dichos requisitos esenciales se deriva a las entidades de normalización europeas, que elaboran las normas

técnicas armonizadas pertinentes, aunque pueden determinarse (como hace el Reglamento de Inteligencia Artificial) parámetros o referencias técnicas alternativos; c) en tercer término, se regulan controles y sistemas de certificación de la conformidad que permiten acreditar que el producto cumple con dichos requisitos obligatorios.

De este modo, frente al anterior modelo armonizador, o del «antiguo enfoque», la norma jurídica no tiene que establecer las especificaciones técnicas —que además de complejas son esencialmente cambiantes—, en su texto normativo, remitiendo su fijación y su control a un sistema autorregulado y autoreferenciado dotado de autonomía técnica y funcional, como es el mundo de la normalización y la certificación de conformidad a cargo de organismos externos y especializados de naturaleza privada.

La posibilidad de regular, mediante la adopción de una Directiva o un Reglamento de armonización, los requisitos comúnmente exigibles a un gran número de productos sin que esa Directiva o Reglamento deba someterse a frecuentes adaptaciones y modificaciones es el objetivo principal de esta técnica armonizadora del «nuevo enfoque», que por otro lado requiere que los ámbitos armonizados se caractericen por la existencia de una amplia gama de productos cuya homogeneidad permita la definición de exigencias esenciales comunes, como sucede con los sistemas de inteligencia artificial.

La armonización técnica basada en este «nuevo enfoque» armonizador se ha aplicado con éxito, entre otros productos, de las máquinas, aparatos metrológicos, aparatos eléctricos y electromecánicos, juguetes, ascensores, equipos de protección individual o productos sanitarios⁶; y, ahora se extiende su aplicación a los sistemas de inteligencia artificial. Para este último campo, la Comisión Europea adoptó una nueva estrategia de armonización y estandarización técnica denominada *Strategy on Standardisation. Setting global standards in support of a resilient, green and digital EU single market*, COM (2022) 31 final, de 2 de febrero de 2022, que tiene por objetivo abordar los desafíos a los que se enfrenta el sistema europeo de normalización en el contexto de las tecnologías digitales y de la inteligencia artificial, entre otros campos, con la pretensión de garantizar que las normas técnicas se adopten en consonancia con los intereses y valores estratégicos de la UE⁷.

6. El Anexo I del reglamento de inteligencia artificial contiene la lista completa y actualizada de los actos legislativos de armonización vigentes en los distintos sectores.
7. Con especial atención a estos ámbitos: DE GREGORIO, G., y DUNN, P., «The European risk-based approaches: Connecting constitutional dots in the digital age», *Common Market Law Review*, 59-2, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4071437. Centrados en la armonización técnica pretendida por el Reglamento de Inteligencia Artificial destacan los trabajos de McFADDEN, M., JONES, K., TAYLOR, E., OSBORN, G., (Oxford Information Labs) *Harmonising Artificial Intelligence*, Oxford

Además de la legislación sectorial de «nuevo enfoque» aplicable a un determinado producto o una categoría de productos, la armonización de legislaciones basada en el «nuevo enfoque» ha conllevado la adopción un conjunto de medidas legislativas transversales. Esta legislación general, que define la arquitectura del modelo, es la que regula el funcionamiento de los organismos de normalización, el procedimiento de aprobación de normas, la acreditación del cumplimiento de los requisitos esenciales de los productos y sistemas mediante la evaluación de conformidad y certificación «por tercera parte», u otras vías alternativas, el Mercado CE de conformidad y la verificación de los requisitos de solvencia, capacidad e independencia de los organismos de normalización nacionales y de los organismos de certificación mediante a acreditación de los mismos por otra entidad tercera igualmente independiente (autoridad de acreditación o «notificante»). Entre esas medidas generales de carácter transversal que definen el funcionamiento de la armonización sectorial basada en el «nuevo enfoque» relacionamos seguidamente las más importantes, que son las que enmarcan la aplicación del Reglamento de Inteligencia Artificial.

En primer lugar, la norma general de referencia es la Directiva 2001/95/CE del Parlamento Europeo y del Consejo, de 3 de diciembre de 2001, relativa a la seguridad general de los productos y al principio de reconocimiento mutuo consagrado en el Derecho de la UE para impedir obstáculos y promover la libre circulación de mercancías (establecido actualmente en el Reglamento UE 2019/515 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019)⁸. Esta Directiva impone la obligación de seguridad gene-

Commission on AI & Good Governance, 2021, <https://oxcaigg.oii.ox.ac.uk/wp-content/uploads/sites/11/2021/12/Harmonising-AI-ÖXIL.pdf>; ALVAREZ GARCÍA; V., y TAHIRI MORENO, J., «La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque», *Revista General de Derecho Administrativo*, n.º 63, 2023; y NATIVI, S., y DE NIGRIS, S., *AI Watch: AI Standardisation Landscape. State of play and link to the EC proposal for an AI regulatory framework* (2021) <https://op.europa.eu/en/publication-detail/-/publication/36c46b8e-e518-11eb-a1a5-01aa75ed71a1/language-en>. De este último hay una versión de 2023 bajo el título *JRC Technical Report, AI Watch: Artificial Intelligence Standardisation Landscape Update*, 2023 <https://publications.jrc.ec.europa.eu/repository/handle/JRC131155>

8. En virtud del principio de reconocimiento mutuo, las autoridades nacionales han de abstenerse de imponer requisitos adicionales a las mercancías legalmente producidas y/o comercializadas en otro Estado miembro. El principio fue esbozado por primera vez por el Tribunal de Justicia de la Unión Europea en el asunto C-120/78, *Rewe-Zentral AG contra Bundesmonopolverwaltung für Branntwein*, Rec. 1979, p. I-42, apartado 8, y desarrollado en jurisprudencia posterior, entre la que destaca las Sentencias recaídas en los asuntos C-525/14, *Comm'n vs. República Checa*, y C-481/12, *UAB Juvelta vs. Lieuvos prabavimo rūmai*.

ral⁹ y establece las medidas correctivas que han de adoptarse cuando se produce un problema de seguridad en un producto. A este último efecto, la Directiva introduce un sistema de alerta rápida de la UE para productos peligrosos que gestiona la Comisión¹⁰, del que están excluidos los alimentos, productos farmacéuticos y dispositivos médicos, que cuentan con sus propias disposiciones para casos de alerta.

La Directiva 2001/95/CE ha sido recientemente sustituida por el Reglamento (UE) 2023/988, de 10 de mayo de 2023, sobre seguridad general de los productos, pero éste no entrará en vigor hasta el 13 de diciembre de 2024. El nuevo Reglamento profundiza en el marco de garantías en materia de salud y la seguridad de los consumidores, especialmente en los más vulnerables, delimita su ámbito de aplicación frente a productos excluidos (esencialmente medicamentos y alimentación y productos fitosanitarios) y establece obligaciones para los operadores económicos tradicionales y también para los prestadores de mercados en línea¹¹, además de aclarar las normas de vigilancia del mercado y las competencias de las autoridades nacionales.

En segundo lugar, sobre el modelo de acreditación de entidades de certificación destaca el Reglamento (CE) n.º 765/2008 del Parlamento Europeo

9. Un producto se considerará seguro si cumple los requisitos nacionales específicos o las normas de la UE. En ausencia tanto de requisitos como de normas, la evaluación de la seguridad deberá basarse en: las directrices de la Comisión, las mejores prácticas del sector correspondiente; el estado actual de los conocimientos y de la técnica, la seguridad que puedan esperar razonablemente los consumidores.
10. La Decisión de Ejecución (UE) 2019/417 establece directrices para la gestión del Sistema de Intercambio Rápido de Información de la UE (RAPEX).
11. Las obligaciones más relevantes para los productores que establece el nuevo Reglamento son: (i) garantizar a lo largo del ciclo de vida de los productos que han sido diseñados y fabricados conforme a los requisitos generales de seguridad del Reglamento, (ii) analizar los riesgos internos y elaborar documentación técnica con una descripción general de los productos y las características esenciales que sean necesarias para evaluar su seguridad, con carácter previo a su comercialización (iii) informar a los operadores de la cadena de suministro de cualquier problema de seguridad que hayan detectado en los productos fabricados, (iv) adoptar medidas correctivas cuando se produce un fallo de seguridad, llegando incluso a su retirada o recuperación del mercado; (v) investigar las reclamaciones presentadas y la información recibida sobre accidentes que afecten a la seguridad de los productos que hayan comercializado, llevando un registro interno sobre las incidencias de producto y las medidas correctivas adoptadas. Junto a ello, el Reglamento permite que los fabricantes designen a un representante autorizado, el cual tendrá encomendadas, como mínimo, las siguientes actuaciones: (i) facilitar toda aquella información y documentación requerida, (ii) advertir al fabricante sobre la existencia de un producto peligroso, (iii) informar a las autoridades nacionales competentes de cualquier medida adoptada para eliminar los riesgos en los productos a través del portal *Safety Business Gateway*, y (iv) cooperar en cualquier actividad destinada a eliminar los riesgos que presenten los productos.

y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos. Esta norma establece reglas comunes para los organismos nacionales de acreditación. También regula la actividad de la Asociación de cooperación europea para la Acreditación, que gestiona las evaluaciones por pares para garantizar la calidad de los servicios que prestan los organismos nacionales de acreditación. Asimismo, establece los principios generales para el «Mercado CE de conformidad», como marca distintiva de que el producto que lo ostenta cumple todas las normas que garantizan el cumplimiento de los requisitos de seguridad aplicables.

Con posterioridad a este Reglamento, el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos eliminó los artículos del Reglamento (CE) n.º 765/2008 que anteriormente trataban los aspectos de vigilancia del mercado, sustituyéndolos por una nueva regulación de las autoridades nacionales de vigilancia.

En tercer lugar, sobre el sistema de evaluación de conformidad es capital la Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos, por la que se deroga la Decisión 93/465/CEE del Consejo, relativa a la evaluación de conformidad. Siguiendo los principios del «nuevo enfoque», la legislación específica sobre los productos armonizados en este marco común pretende evitar que la legislación de armonización incorpore en su articulado un nivel de detalle técnico excesivo sobre los productos y se limita a establecer los requisitos esenciales de salud y seguridad. La pretensión de esta Decisión es que estos requisitos esenciales se redacten por la legislación sectorial aplicable a cada producto de manera suficientemente precisa para establecer obligaciones jurídicamente vinculantes, formulándose de modo que sea posible una evaluación de la conformidad respecto de dichos requisitos.

En cuarto lugar y último lugar, en lo relativo a la normalización europea, destaca el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012. Esta es la norma de cabecera en lo relativo a la elaboración de normas técnicas europeas armonizadas y especificaciones técnicas comunes. En este campo es igualmente relevante tener en cuenta el Reglamento (UE) 2022/2480 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 por el que se modifica el citado Reglamento (UE) n.º 1025/2012 en lo que se refiere a las decisiones de las organizaciones europeas de normalización relativas a las normas europeas y a los documentos europeos de normalización.

2. REQUISITOS ESENCIALES OBLIGATORIOS, NORMAS TÉCNICAS Y ESPECIFICACIONES COMUNES. EL EFECTO DE PRESUNCIÓN DE CONFORMIDAD CON LOS REQUISITOS OBLIGATORIOS DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

De acuerdo con la técnica armonizadora del «nuevo enfoque», la regulación de los requisitos esenciales que obligatoriamente deben respetar los productos los sistemas de inteligencia artificial de alto riesgo¹² y los modelos de IA de uso general¹³ se fijan como objetivos y finalidades concretas por la legislación armonizadora, en este caso un Reglamento, que establece dichos requisitos en la Sección 2ª del Capítulo III para los sistemas de IA de alto riesgo¹⁴ y en las Secciones 2ª y 3ª del Capítulo V para los modelos de IA de uso general¹⁵, que son más exigentes cuando éstos pueden represen-

12. Contemplados en el Capítulo III del Reglamento (fundamentalmente en los artículos 8 a 15) y en su Anexo III (al que se remite el artículo 6.2).
13. Los conceptos de sistemas y modelos de IA «de uso general» se introdujeron en el texto transaccional propuesto por el Consejo como consecuencia de la aparición y emergencia en el mercado de *Chat GPT* y tecnologías similares. Se trata de sistemas que, con independencia de la manera en la que se introduzcan en el mercado o se pongan en servicio, incluido el software de código abierto, han sido concebidos para desempeñar funciones de aplicación general, como el reconocimiento de imágenes y de voz, la generación de audio y vídeo, la detección de patrones, la respuesta a preguntas y la traducción, que se caracterizan por una gran capacidad generativa. Respondiendo a estas características, un «sistema de inteligencia artificial de uso general» está siempre basado en un modelo de uso general, y puede integrarse en otros sistemas de IA que lo incorporen o formar parte de los mismos (apartado 66 del artículo 3 del Reglamento). Mientras que los «modelos de IA de uso general» se definen como aquellos que son entrenados «con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado» (apartado 63 del del artículo 3 de Reglamento).
14. Consistentes en disponer de un sistema de gestión de riesgos y de un sistema de gestión de la calidad adecuado, de un modelo adecuado de tratamiento y gobernanza de los datos de los que se nutren, de la documentación técnica acreditativa de que sus características técnicas se ajustan a los requisitos obligatorios, permitiendo la conservación y trazabilidad de su funcionamiento. Asimismo, han de garantizar un determinado nivel de transparencia en su funcionamiento que además permita identificar a los responsables de su despliegue en el mercado, garantizar la posibilidad de supervisión humana, así como respetar determinados parámetros de precisión, solidez y ciberseguridad.
15. Según el artículo 53 del Reglamento de Inteligencia Artificial, los proveedores de modelos de IA de uso general han de elaborar y mantener actualizada la documentación e información relativa al proceso de entrenamiento y realización de pruebas y

tar riesgos sistémicos de los definidos en el apartado 65 del artículo 3 del Reglamento¹⁶. En segundo término, las especificaciones técnicas que garantizan su cumplimiento se establecen al margen del Reglamento en normas técnicas elaboradas por las entidades de normalización europeas siguiendo mandatos de la Comisión, si bien pueden ser fijadas excepcionalmente por la propia Comisión (especificaciones comunes) o incluso mediante parámetros técnicos alternativos a los anteriores (sean normas técnicas internacionales o nacionales, u otros parámetros técnicos como guías o códigos).

El peso del control del cumplimiento de los requisitos obligatorios recae, en tercer lugar, en los organismos de evaluación de la conformidad acreditados por las correspondientes entidades nacionales de acreditación. No obstante, como desarrollaremos en el siguiente epígrafe, no siempre es exigible una evaluación o certificación «por tercera parte», pues el sistema admite la «autocertificación» del propio fabricante. Esta última, que no es en principio la fórmula de evaluación de la conformidad más recomendable, tiene que ser necesariamente habilitada en este campo, donde, con la excepción de los sistemas de inteligencia artificial integrados en productos que ya cuentan con una norma de armonización del «nuevo enfoque» y algunos

los resultados de su evaluación, que contendrá, como mínimo, la información establecida en el anexo XI del Reglamento con el fin de facilitarla, previa solicitud, a la Oficina de IA y a las autoridades nacionales competentes. También han de elaborar y mantener actualizada información y documentación ajustada al Anexo XII del Reglamento que han de poner a disposición de los proveedores de sistemas de IA que tengan la intención de integrar el modelo de IA de uso general en sus sistemas de IA, de modo que permita entender bien las capacidades y limitaciones del modelo de IA de uso general y cumplir sus obligaciones como proveedores de sistemas de IA. Asimismo, adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor y derechos afines, en particular para detectar y cumplir la reserva de derechos expresada por los titulares de derechos con arreglo al artículo 4, apartado 3, de la Directiva (UE) 2019/790. Finalmente, el artículo 54 del Reglamento establece las obligaciones de los proveedores establecidos en terceros países en relación con la designación y las tareas que les corresponden a sus representados autorizados establecidos en la Unión Europea.

16. Según el artículo 55 del Reglamento de Inteligencia Artificial, además de las obligaciones establecidas para los proveedores de modelos de IA de uso general, cuando este puede conllevar un «riesgo sistémico» han de: a) evaluar los modelos de conformidad con protocolos y herramientas normalizados que reflejen el estado de la técnica, lo que incluye la realización y documentación de pruebas de simulación con vistas a detectar y mitigar riesgos sistémicos; b) evaluar y mitigarán los posibles riesgos sistémicos a escala de la Unión que puedan derivarse de su utilización, así como el origen de dichos riesgos; c) vigilar, documentar y comunicar a la Oficina de IA y, en su caso, a las autoridades nacionales competentes, la información pertinente sobre incidentes graves y las posibles medidas correctoras para resolverlos; y, d) velar por un nivel adecuado de protección de la ciberseguridad para el modelo de IA de uso general con riesgo sistémico y la infraestructura física del modelo.

sistemas de alto riesgo, está llamada a ser, al menos al principio, la vía ordinaria o común para la acreditación del cumplimiento de los objetivos esenciales del Reglamento dada la falta de referenciales técnicos sólidos y maduros en este campo.

En el caso de los sistemas de inteligencia artificial, tanto la normalización técnica como la certificación por tercera parte están a día de hoy muy inmaduras y en gran parte por desarrollar (lo que explica en buena medida la dilatada previsión de entrada en vigor del Reglamento, en los términos del artículo 113), por lo que el Reglamento establece posibilidades y parámetros técnicos alternativos a las normas técnicas de las entidades de normalización europeas, aún inexistentes o en un estadio muy prematuro de elaboración¹⁷, al igual que sucede con las normas técnicas internacionales que les corresponde adoptar a los organismos de normalización de ámbito internacional, por lo que tampoco es posible acudir a los mecanismos de transposición de las mismas que son habituales en otros campos del «nuevo enfoque»¹⁸. La inmadurez del sistema es, en consecuencia, equivalente en lo que se refiere a los sistemas de certificación «por tercera parte» que apli-

17. El trabajo de MCFADDEN, M., JONES, K., TAYLOR, E., OSBORN, G., (2021) contiene un apéndice en sus pp. 29 a 42 que analiza el avance de los estándares técnicos para los sistemas de inteligencia artificial en las distintas organizaciones de normalización europeas e internacionales. Asimismo, la ETSI publicó en 2019 un *Bildt report on EU standardisation* que aborda las estrategias de normalización conjuntas de este organismo con otros organismos de normalización, europeos (el CEN y el CENELEC), disponible en <https://www.etsi.org/images/files/ETSI-Report-of-the-Task-Force.pdf> Para el desarrollo de su trabajo normalizador en la materia inteligencia artificial, el ETSI creó en 2018 el *Industry Specification Group on Securing Artificial Intelligence* (ETSI ISG SAI). Y CEN/CENELEC instauraron conjuntamente en 2019 el *Joint Technical Committee 21 on Artificial Intelligence* (JTC 21). La Comisión Europea hace un seguimiento de la labor normalizadora *AI Watch*, que se refleja en su informe *Artificial Intelligence Standardisation Landscape*, de 2023 <https://publications.jrc.ec.europa.eu/repository/handle/JRC131155>
18. Los organismos de normalización europeos tienen suscritos acuerdos de colaboración con las organizaciones internacionales de normalización homólogas: la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI) y la Unión Internacional de Telecomunicaciones (UIT). A través de estos acuerdos, las normas técnicas de carácter internacional pueden adoptarse por los organismos europeos, evitando la duplicación de esfuerzos normalizadores y reduciendo el tiempo en la elaboración de normas. Por ejemplo, en virtud del Acuerdo de Viena suscrito entre el CEN y la ISO en 1991, CEN e ISO se comprometieron a planificar conjuntamente nuevos proyectos de normas. Asimismo, el Acuerdo prevé que cuando una norma ISO es adoptada puede convertirse en norma europea (EN) cuando aquella norma ha sido adoptada teniendo en cuenta los objetivos perseguidos por la normativa europea, convirtiéndose en una norma ISO-EN. Recientemente, en el seno de la ISO, y en coordinación con la CEI, se ha creado un Comité técnico para desarrollar trabajos de normalización en esta materia se constituyó un Subcomité (SC 42) sobre IA adscrito al *Joint Technical Committee 1* (ISO/IEC JTC 1).

can dichos referenciales, lo que obliga a recurrir a parámetros técnicos alternativos, de un lado; y, de otro, a darle mayor cabida a la «autocertificación» por parte del productor o fabricante, al menos hasta que el sistema de normalización y de certificación se desarrolle.

En todo caso, los productos y sistemas que se ajusten a las normas técnicas que desarrollan los requisitos obligatorios del Reglamento y acrediten su cumplimiento mediante un sistema de certificación fehaciente podrán disponer del Mercado CE de conformidad que garantiza frente a terceros que dicho producto cumple los requisitos esenciales de seguridad de carácter obligatorio y habilita su comercialización.

Ha de subrayarse que la obligación de cumplir los requisitos esenciales u obligatorios que establece el Reglamento solo afecta a los sistemas de inteligencia artificial de alto riesgo, que son aquellos que pueden provocar daños significativos para la salud, para la seguridad o para los valores y derechos fundamentales en la Unión, a los que se equiparan parcialmente los modelos de IA de uso general. Como se ha analizado en otro lugar de esta obra, la intensidad del riesgo se mide en atención tanto a la finalidad prevista para la que se crea el sistema como a las modalidades de uso que éste tenga. Como ya hemos señalado, el Reglamento de inteligencia artificial equipara a estos sistemas de alto riesgo los modelos de IA de uso general de la Sección 2ª del Capítulo V y los modelos de IA de uso general que pueden ocasionar riesgos sistémicos que contempla la Sección 3ª del Capítulo V, que también se someten a requisitos esenciales obligatorios específicos (artículos 53 a 55 del Reglamento).

Los sistemas de inteligencia artificial de alto riesgo son los que se enumeran en el Anexo III (sistemas de identificación biométrica, de protección de infraestructuras críticas, de selección y promoción de personal, de utilización en fronteras, o los usados por las Fuerzas y Cuerpos de Seguridad del Estado o la Administración de Justicia, entre otros), con la excepción contemplada en el artículo 6.3 y 6 del Reglamento¹⁹. Se trata de un listado sujeto a revisión. El artículo 7.1 del Reglamento prevé que este listado pueda

19. Bien, en primer lugar, porque un determinado sistema que en principio contempla el Anexo III no se considere de alto riesgo por no comportar un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones cuando se da alguno de las circunstancias del apartado 3.º del artículo 6 (que el sistema esté destinado a una tarea de procedimiento limitada, a mejorar el resultado de una actividad humana ya realizada, que se destine a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o que el sistema de IA esté destinado

ser ampliado por la Comisión cuando se trate de sistemas de IA destinados a ser utilizados en cualquiera de los ámbitos que figuran en el Anexo III y planteen un riesgo de perjudicar la salud y la seguridad o de tener repercusiones negativas en los derechos fundamentales equivalente a, o mayor que, el riesgo de perjuicio o de repercusiones negativas que plantean los sistemas de IA de alto riesgo que ya se mencionan en el Anexo III. También se prevé que la Comisión pueda acordar lo contrario, eliminando sistemas de IA de dicho listado cuando ya no plantean riesgos significativos (artículo 7.3).

Los sistemas de alto riesgo son admisibles en el mercado europeo, pero su distribución y comercialización está condicionada a acreditar el cumplimiento de los requisitos esenciales obligatorios con carácter previo a dicha comercialización, lo que se consigue demostrando que los sistemas de inteligencia artificial en cuestión han sido desarrollados siguiendo las exigencias técnicas establecidas en normas armonizadas (fijadas por los organismos europeos de normalización), en especificaciones comunes (elaboradas por la Comisión) o a través de otras soluciones técnicas equivalentes (generadas muy a menudo por los propios operadores mediante fórmulas de autorregulación).

El Reglamento de inteligencia artificial, consciente del escaso desarrollo de la normalización en este campo, habilita que la certificación del cumplimiento de los requisitos obligatorios establecidos para los sistemas de inteligencia artificial de alto riesgo (sección 2ª del Capítulo III) o, en su caso, para los modelos de inteligencia artificial de uso general (secciones 2 y 3 del Capítulo V), pueda hacerse a través de tres tipos de parámetros técnicos de contraste. En primer lugar, las normas armonizadas y los documentos europeos de normalización adoptadas por los organismos de normalización europeos siguiendo mandatos que a tal efecto les curse la Comisión (artículo 40.2), que es lo habitual en la legislación sectorial del «nuevo enfoque». En segundo lugar, de no existir éstas o considerarlo necesario la Comisión, las especificaciones comunes que puede adoptar la Comisión en los casos previstos en el artículo 41. Y, en tercer lugar, en defecto de las anteriores, otras soluciones técnicas equivalentes a aquellas (artículo 41.5).

a realizar una tarea preparatoria para una evaluación que sea pertinente a efectos de los casos de uso enumerados en el Anexo III), siempre que no se trate de un sistema de elaboración de perfiles, en cuyo caso se considerará siempre de alto riesgo. O bien, en segundo lugar, porque la Comisión adopte un acto delegado con arreglo al artículo 97 al objeto de modificar el apartado 3.º del artículo 6 añadiendo nuevas condiciones, o modificando estas, cuando existan pruebas concretas y fiables de la existencia de sistemas de IA que entren en el ámbito de aplicación del Anexo III, pero que no planteen un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales.

2.1. NORMAS TÉCNICAS ARMONIZADAS Y DOCUMENTOS EUROPEOS DE NORMALIZACIÓN DE LOS ORGANISMOS DE NORMALIZACIÓN

La regla general en los modelos armonización técnica del «nuevo enfoque» es que los requisitos esenciales obligatorios establecidos en la norma armonizadora se desarrollen, a efectos de poder certificar su cumplimiento y producir el efecto de presunción de conformidad a aquellos, mediante normas técnicas armonizadas europeas (EN) o documentos europeos de normalización armonizados (HD)²⁰. Estas normas y documentos se aprueban por los organismos de normalización europeos siguiendo mandatos expresos de la Comisión, que a su vez acepta (o no) su resultado una vez que la norma o documento de normalización se elabora. De ser aceptados y publicarse su referencia en el Diario Oficial de la Unión Europea (mediante la indicación de su título y código numérico), la fabricación de un producto o sistema de acuerdo con las mismas siguiendo un procedimiento de «evaluación de la conformidad» produce el efecto de presunción de conformidad que acredita el cumplimiento de los requisitos esenciales y obligatorios que han de satisfacer los productos.

En principio, el cumplimiento de estas normas técnicas y documentos de normalización es voluntario para los productores, aunque su aplicación práctica es generalizada por el efecto de presunción de conformidad de cumplimiento de los requisitos obligatorios de la norma armonizada que produce la acreditación de su cumplimiento²¹.

20. La distinción formal entre una norma técnica armonizada europea (EN) y un documento de normalización o de armonización (HD) es que estos últimos no tienen la condición formal de «norma armonizada», y se definen como «cualquier especificación técnica distinta de la norma europea» (artículo 2.2 del Reglamento n.º 1025/2012). Pero la diferencia fundamental entre normas técnicas y documentos de normalización es que los segundos no son de obligatoria transposición como norma técnica nacional para las organizaciones de normalización de los Estados miembros, mientras que las normas EN sí lo son. Los organismos de normalización europeos no solo adoptan normas técnicas armonizadas y documentos de normalización. Al margen del mecanismo del «nuevo enfoque», también adoptan normas técnicas que no obedecen a mandatos de la Comisión (no son normas técnicas «armonizadas»), «especificaciones técnicas» distintas a las normas técnicas y a los documentos de normalización (que podrían llegar a ser normas EN pero que aún no cuentan con el consenso necesario para serlo, o bien el campo que cubren está desarrollándose en el aspecto técnico, teniendo en ese caso un carácter más experimental). Y también adoptan «guías» con orientaciones y recomendación y «acuerdos de trabajo» que tampoco tienen el status de norma.

21. El efecto de presunción de conformidad ha llevado al TJUE a caracterizar las normas técnicas armonizadas como Derecho de la Unión, apelando al mecanismo del mandato previo y la validación ulterior de las mismas por la Comisión (Sentencia «*James Elliott Construction Limited vs. Irish Asphalt Limited*» (C-613/14), de 27 de octubre de 2016).

El Reglamento de Inteligencia Artificial prevé que, de conformidad con el artículo 10 del Reglamento (UE) n.º 1025/2012, de 25 de octubre de 2012²², la Comisión formule peticiones de normalización que contemplen los requisitos establecidos en la Sección 2ª del Capítulo III del Reglamento de Inteligencia Artificial para los sistemas de IA de alto riesgo o, en su caso, las obligaciones establecidas en las Secciones 2ª y 3ª del Capítulo V para los modelos IA de uso general. La petición de normalización también incluirá la solicitud de documentos sobre los procesos de presentación de información y documentación a fin de mejorar el funcionamiento de los de los sistemas de IA de alto riesgo y los modelos de IA de uso general desde el punto de vista de su sostenibilidad, con especial atención a la reducción del consumo de energía, y de otros requisitos ligados a su ciclo de vida. Cuando prepare una petición de normalización, la Comisión consultará al Consejo de IA que crea el Reglamento (artículos 65 y 66) y a las partes interesadas pertinentes, incluido el Foro consultivo que el Reglamento crea para asesorar a aquél (artículo 67). Cuando dirija una petición de normalización, la Comisión especificará que las normas deben ser claras, coherentes y destinadas a garantizar que los sistemas de IA de alto riesgo o los modelos de IA de uso general introducidos en el mercado o puestos en servicio en la Unión cumplan los requisitos u obligaciones obligatorios establecidos en el Reglamento²³.

Efectuada la petición, la organización europea de normalización de que se trate indicará si acepta la petición de la Comisión. En caso afirmativo, las normas armonizadas y los documentos europeos de normalización se adoptarán siguiendo el procedimiento previsto en el artículo 22.3 del citado Reglamento (UE) n.º 1025/2012 a cuyo efecto el organismo de normalización puede solicitar y obtener financiación por parte de la Comisión en forma de subvención (artículos 15 a 19 del Reglamento).

Las organizaciones europeas de normalización informarán a la Comisión sobre las actividades emprendidas para la elaboración de las normas armonizadas o los documentos de normalización resultantes.

-
22. Este precepto prevé que la Comisión pueda pedir a una o varias organizaciones europeas de normalización que elaboren una norma europea o un documento europeo de normalización en un plazo determinado. Esas normas europeas y los documentos europeos de normalización deberán tomar en consideración el interés público y permitir que los productos y sistemas alcancen los objetivos expuestos en la petición de la Comisión, debiendo basarse en el mercado y ser fruto del consenso.
23. La Comisión adoptó el 27 de octubre de 2015, un documento de trabajo llamado «Vademécum de la normalización europea en apoyo de la legislación y las políticas de la Unión Europea» SWD(2015) 205 final, que describe los pormenores del procedimiento de petición de normas técnicas por la Comisión a los organismos de normalización europeos, disponible en <https://ec.europa.eu/docsroom/documents/13507/attachments/1/translations/es/renditions/pdf>

ESTUDIOS

Este libro colectivo trata de algunas de las cuestiones esenciales que ha suscitado el Reglamento (UE) 2024/1689, del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Coordinados por el Catedrático de Derecho Administrativo de la Universidad de Sevilla, Prof. Antonio José Sánchez Sáez, los autores son profesores de varias Universidades españolas, especialistas en la materia. El hilo conductor de la obra es el impacto que, en las Administraciones públicas, ha generado la aprobación del RIA. En el libro se tocan temas como la ética y metaética de la IA, la *privacy*, las novedades del RIA desde el punto de vista de las Administraciones públicas, las garantías jurídicas del cumplimiento de los requisitos obligatorios para los sistemas de alto riesgo, las formas de ayuda de la IA a la Administración pública en sus actuaciones —con especial referencia al silencio administrativo—, el régimen jurídico de los proveedores y los responsables del despliegue de sistemas, el informe de evaluación de impacto relativo a los derechos fundamentales, la supervisión humana de la IA, los algoritmos, el régimen jurídico de los datos biométricos y la aplicación de la IA en la administración autonómica. Los autores parten de una premisa: se hace necesario dotar a esta novedosa herramienta, cada vez más poderosa y de uso más común, de las garantías, procedimientos y límites que impone la protección de los derechos fundamentales, promoviendo un uso razonable de ella en la actuación de las Administraciones públicas.

El precio de esta obra incluye la publicación en formato DÚO sin coste adicional (papel + libro electrónico)

ACCEDE A LA VERSIÓN ELECTRÓNICA SIGUIENDO LAS INDICACIONES DEL INTERIOR DEL LIBRO

ISBN: 978-84-1085-123-8

