Gabilex

Nº 42
Segundo trimestre
2025

REVISTA DEL GABINETE JURÍDICO DE CASTILLA-LA MANCHA

REVISTA DEL GABINETE JURÍDICO DE CASTILLA-LA MANCHA

Número 42. Junio 2025

Revista incluida en Latindex, Dialnet, MIAR, Tirant lo Blanch

Solicitada inclusión en SHERPA/ROMEO, DULCINEA y REDALYC

Disponible en SMARTECA, VLEX y LEFEBVRE-EL DERECHO

Editado por Vicepresidencia

D.L. TO 862-2014

ISSN 2386-8104

revistagabinetejuridico@jccm.es

DIRECCIÓN

Dª Mª Belén López Donaire

Directora de los Servicios Jurídicos de la Administración de la Junta de Comunidades de Castilla-La Mancha.

Letrada del Gabinete Jurídico de la Junta de Comunidades de Castilla-La Mancha.

CONSEJO DE REDACCIÓN

Dª. Antonia Gómez Díaz-Romo

Letrada Coordinadora del Gabinete Jurídico de la Junta de Comunidades Castilla-La Mancha

D. Roberto Mayor Gómez

Letrado-Director de los Servicios Jurídicos de las Cortes de Castilla-La Mancha.

D. Leopoldo J. Gómez Zamora

Director adjunto de la Asesoría Jurídica de la Universidad Rey Juan Carlos.

Letrado del Gabinete Jurídico de la Junta de Comunidades de Castilla-La Mancha.

COMITÉ CIENTÍFICO

D. Salvador Jiménez Ibáñez

Ex Letrado Jefe del Gabinete Jurídico de la Junta de Comunidades de Castilla-La Mancha.

Ex Consejero del Consejo Consultivo de Castilla-La Mancha.

D. José Antonio Moreno Molina

Catedrático de Derecho Administrativo de la Universidad de Castilla-La Mancha.

D. Isaac Martín Delgado

Profesor Dr. Derecho Administrativo de la Universidad de Castilla-La Mancha.

Director del Centro de Estudios Europeos *"Luis Ortega Álvarez".*

CONSEJO EVALUADOR EXTERNO

D. José Ramón Chaves García

Magistrado de lo contencioso-administrativo en Tribunal Superior de Justicia de Asturias.

Dª Concepción Campos Acuña

Directivo Público Profesional.
Secretaria de Gobierno Local.

D. Jordi Gimeno Beviá

Facultad de Derecho de la UNED. Prof. Derecho Procesal

D. Jorge Fondevila Antolín

Jefe Asesoría Jurídica. Consejería de Presidencia y Justicia. Gobierno de Cantabria.
Cuerpo de Letrados.

D. David Larios Risco

Letrado de la Junta de Comunidades de Castilla-La Mancha.

D. José Joaquín Jiménez Vacas

Funcionario de carrera del Cuerpo Técnico Superior de Administración General de la Comunidad de Madrid

D. Javier Mendoza Jiménez

Doctor en Economía y profesor ayudante doctor de la Universidad de La Laguna.

SUMARIO

REVISTA DEL GABINETE JURÍDICO DE CASTILLA-LA MANCHA

SECCIÓN NACIONAL

ARTÍCULOS DOCTRINALES

-

ANÁLISIS DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL (AIA)

Dª Esther Molina Castañer

Letrada de la Administración de Justicia del Juzgado Mixto número 1 de LLiria, prestando servicios en la actualidad en comisión de servicios en los Juzgados Penales 5 y 13 de Valencia en funciones de refuerzo.

Resumen: En este artículo se revisa la regulación europea de la IA a través del Reglamento aprobado el 21 de mayo de 2024.Se hace referencia a los trabajos previos a su aprobación, la entrada en vigor del mismo y los aspectos relevantes que se regulan, como las actividades que comprende el Reglamento según el riesgo que implica para la salud, la seguridad y los derechos fundamentales; la exclusión de la IA generativa al no considerarla de alto riesgo, la exclusión de la identificación biometría como regla general, las autoridades encargadas del control de la aplicación o las sanciones que conlleva el incumplimiento de las mismas.

Abstract: This article reviews the European regulation of AI through the Regulation approved on May 21, 2024. Reference is made to the work prior to its approval, its

entry into force and the relevant aspects that are regulated, such as activities covered by the Regulation according to the risk they imply for health, safety and fundamental rights; the exclusion of generative AI as it is not considered high risk, the exclusion of biometric identification as a general rule, the authorities in charge of controlling the application or the sanctions that non-compliance entails.

Palabras clave: Identificación biométrica, autenticación biométrica, categorización biométrica, IA generativa, ChatGPT, proveedor, ciberseguridad.

Keywords: Biometric identification, biometric authentication, biometric categorization, generative AI, ChatGPT, provider, cybersecurity.

Sumario:

1.- Revisión de los trabajos previos a la aprobación del AIA.

1-1.- Fase inicial.

Desde abril de 2021 la intención de la UE ha sido la de unificar en un texto una regulación armonizada que pretenda fijar las líneas a seguir en relación con la IA. Como indica MORENO CATENA "es claro que la Inteligencia Artificial debe regularse".[1]

Existen otros grandes hitos que sirvieron de germen a la necesidad de regulación como la Convención de Budapest de 23 de noviembre de 2001[2] que pretende proteger a la sociedad frente a la ciberdelincuencia o el Libro Blanco sobre la Inteligencia Artificial de 19 de febrero de 2020, que analiza las implicaciones éticas y humanas de la IA. Especialmente relevante es la Carta de los Derechos Fundamentales de la Unión Europea (la «Carta»), en particular la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA en la Unión,

[1] MORENO CATENA, VICTOR, "Los datos en el sistema de justicia y la propuesta del Reglamento UE sobre Inteligencia Artificial en Uso de la información y de los datos personales en los procesos: los cambios en la Era Digital" *Edit.Thomson and Reuters-Aranzadi*, 2021.

[2] El Convenio fue ratificado por España el 3 de junio de 2010 y publicado en el BOE el día 17 de septiembre de 2009, si bien no entró en vigor hasta el día 1 de octubre de 2009.

así como brindar apoyo a la innovación. El uso de la IA debe dar confianza y ser fiable.

El 21 de abril de 2021 la Comisión publicó una propuesta para regular la inteligencia artificial en la Unión Europea. Tres meses después, el 20 de julio la Presidencia eslovena del Consejo de la Unión Europea organizó una conferencia virtual sobre la regulación de la inteligencia artificial, la ética y los derechos fundamentales. El 6 de agosto de 2021 se publicó un estudio[3] que analizaba el uso de técnicas biométricas desde una perspectiva ética y jurídica y que fue encargado por el Departamento de Política de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo y se abrió el periodo de consulta pública sobre la Ley de AI por parte de la Comisión Europea recibiendo la Comisión[4] 304

[3] Este estudio, encargado por el Departamento Temático del Parlamento Europeo para Derechos de Ciudadanía y Asuntos Constitucionales a petición de la JURI y PETI Comités, analiza el uso de técnicas biométricas desde un punto de vista ético y legal perspectiva. Las técnicas biométricas plantean una serie de cuestiones éticas específicas, como un individuo no puede cambiar fácilmente las características biométricas y como estas técnicas tienden a inmiscuirse en el cuerpo humano y, en última instancia, en el yo humano. Más los problemas se asocian más generalmente con la vigilancia a gran escala, algorítmica, toma de decisiones o elaboración de perfiles. El estudio analiza diferentes tipos de biometría técnicas y extrae conclusiones para la legislación de la UE.

[4] Comisión Europea coordina los esfuerzos de normalización para el AIA, es responsable del proyecto de solicitud de normalización, la propuesta, los anexos y las evaluaciones de

propuestas. Después de verano diversas instituciones y organismos de la UE sin poder legislativo emitieron dictámenes en los que aportaban su experiencia y conocimientos al AIA, tales el Banco Central Europeo (BCE)[5], el Comité de las Regiones (CDR)[6], el Comité Económico y Social Europeo (CESE)[7] y el Consejo Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos (SEPD) ofreciendo análisis sobre las implicaciones normativas y sociales del AIA. Posteriormente, el 29 de noviembre de 2021 la Presidencia rotatoria del Consejo de la UE compartió un primer texto de compromiso sobre el proyecto de la Ley de IA con cambios en los ámbitos de la puntuación social, los sistemas de reconocimiento biométrico y las aplicaciones de alto riesgo.

1.2. Fase de negociaciones sobre la Ley de Inteligencia Artificial y primeras propuestas y proyectos.

El 1 de diciembre de 2021 las comisiones de Mercado Interior y Libertades Civiles del Parlamento Europeo dirigen conjuntamente las negociaciones sobre la Ley de la AI. El 25 de enero de 2022 las principales comisiones del Parlamento Europeo, la de Mercado Interior y la de Libertades Civiles, mantuvieron un primer intercambio de puntos de vista conjunto sobre la propuesta de Ley de AI. Solo unos días después, el 2 de febrero de la

impacto ofrecen información sobre el marco regulador y sus posibles repercusiones en diversos sectores de la UE.

[5] DO C 115 de 11.3.2022, p. 5.

[6] DO C 97 de 28.2.2022, p. 60.

[7] DO C 517 de 22.12.2021, p. 56.

Comisión Europea presentó una nueva estrategia de normalización en la que expone su enfoque de las normas en el mercado único y a escala mundial. Las normas son la base del mercado único de la UE y de la competitividad mundial. Un día después la Presidencia francesa del Consejo difundió un texto de compromiso de los artículos 16 a 29 de la propuesta de Ley sobre la IA, relativos a las obligaciones de los usuarios y proveedores de sistemas de alto riesgo. Posteriormente, la Presidencia francesa difundió otro texto transaccional de los artículos 40-52, que se refieren a las normas armonizadas, las evaluaciones de conformidad y las obligaciones de transparencia para determinados sistemas de IA. Un mes después la Comisión de Asuntos Jurídicos (JURI) del Parlamento Europeo publicó sus enmiendas a la Ley de IA. La Comisión de Industria, Investigación y Energía (ITRE) del Parlamento Europeo publicó su proyecto de opinión sobe la Ley de IA un día después. Un mes después la Comisión de Asuntos Jurídicos (JURI) del Parlamento Europeo publicaron sus enmiendas a la Ley de IA. La Comisión de Industria, Investigación y Energía (ITRE) del Parlamento Europeo publicó su proyecto de opinión sobre la Ley de IA un día después. El 20 de abril de 2022 Brando Benifei y Dragoș Tudorache, publicaron su proyecto de informe. Solo un mes después, el 13 de mayo de 2022 la Presidencia francesa del Consejo publicó el texto sobre el artículo 4 bis[8]. Hasta el 1 de junio de 2022 cada grupo político del

[8] El artículo 4 bis propone regular los sistemas de IA de propósito general, que son sistemas de IA capaces de realizar una amplia gama de tareas, como tratar de comprender imágenes y voz, generar audio y vídeos, detectar patrones, responder preguntas y traducir textos.

Parlamento Europeo podía presentar enmiendas a la Ley de AI, presentándose miles de ellas. El 15 de junio de 2022 la Presidencia francesa del Consejo de la UE difundió su texto de compromiso final antes de que la República Checa asumiera la Presidencia.

Dos días después la Presidencia checa del Consejo de la UE compartió un documento de con otros gobiernos de la UE, en el que se enumeran las principales prioridades de la Ley de AI para ellos. Después de verano, la Comisión de Asuntos Jurídicos (JURI) del Parlamento Europeo aprobó su dictamen sobre la Ley de AI como última comisión del Parlamento. El día 28 de septiembre la Comisión Europea propuso una armonización específica de las normas nacionales de responsabilidad por IA, con el objetivo de complementar la Ley de IA facilitando las reclamaciones de responsabilidad civil por daños y perjuicios. La última actuación de ese año se llevó a cabo el día 6 de diciembre cuando el Consejo de la UE adoptó su posición común ("orientación general") sobre la Ley de AI

1.3. Fase de votación y acuerdos.

En el año 2023 se realizaron dos actuaciones muy relevantes, la primera el 14 de junio, fecha en la que el Parlamento Europeo adopta suposición negociadora sobre el Acta AI, con 499 votos a favor, 28 en contra y 93 abstenciones y el 9 de diciembre, cuando el Parlamento y el Consejo alcanzan un acuerdo provisional sobre la Ley de AI. Fue ya en el año 2024, en concreto el día 13 de febrero cuando los Comités de Mercado Interior y Libertades Civiles votaron 71-8 (7 abstenciones) para aprobar el resultado de las

negociaciones con los Estados miembros sobre la Ley de AI[9]. Ocho días después se crea la Comisión la Oficina Europea de Inteligencia Artificial, dependiente de la Dirección General de Redes de Comunicación, Contenidos y Tecnología, para apoyar la aplicación de la Ley de Inteligencia Artificial, especialmente para la IA de propósito general. El día 21 de mayo de 2024 el Consejo Europeo adopta formalmente la Ley de AI de la UE.

1.4. Publicación, despliegue y entrada en vigor.

Entre los meses de junio y julio de 2024 la Ley de IA se publicará en el Diario Oficial de la Unión Europea, sirviendo dicha publicación como notificación formal de la nueva ley.

La Ley de IA "entrará en vigor" 20 días después de su publicación en el Diario Oficial. A partir de esta fecha, se sucederán los siguientes hitos según el art. 113:

- ***6 meses después*** - Se aplicarán el Capítulo I y II (prohibiciones sobre IA de riesgo inaceptable).
- ***12 meses después*** - Se aplicarán el Capítulo III, sección 4 (autoridades de notificación), Capítulo V (modelos de IA de propósito general), Capítulo VII (gobernanza), Capítulo XII

[9] Los 27 Estados miembros de la UE han respaldado unánimemente la Ley de AI, afirmando el acuerdo político alcanzado en diciembre.

(confidencialidad y sanciones) y el artículo 78 (confidencialidad), a excepción del artículo 101 (multas para los proveedores de IGPC).

- ***24 meses después*** - Se aplicará el resto de la Ley de IA, excepto;
- ***36 meses después*** - Se aplicarán el apartado 1 del artículo 6 y las obligaciones correspondientes del presente Reglamento. Los Códigos de buenas prácticas deben estar listos 9 meses después de su entrada en vigor, según el artículo 56.

2.- Estructura del Reglamento.

El Reglamento consta de doce títulos, 113 artículos, así como 13 anexos.

Título I: Disposiciones generales (art.1) En el título I se define el objeto del Reglamento y el ámbito de aplicación de las nuevas normas que abarcan la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA. Además, se establecen las definiciones utilizadas en todo el instrumento.

Título II: Prácticas prohibidas (art.5) En el título II se establece una lista de IA prohibidas. El Reglamento sigue un enfoque basado en los riesgos que distingue entre los usos de la IA que generan i) un riesgo inaceptable, ii) un riesgo alto, y iii) un riesgo bajo o mínimo. La lista de prácticas prohibidas que figura en el título II abarca

todos los sistemas de IA cuyo uso se considera inaceptable por ser contrario a los valores de la Unión, por ejemplo, porque violan derechos fundamentales.

Título III: Sistemas de alto riesgo (art.6) El título III contiene normas específicas para aquellos sistemas de IA que acarrean un alto riesgo para la salud y la seguridad o los derechos fundamentales de las personas físicas. En el capítulo 1 del título III se establecen las normas de clasificación y se definen las dos categorías principales de sistemas de IA de alto riesgo:

·los sistemas de IA diseñados para utilizarse como componentes de seguridad de productos sujetos a una evaluación de la conformidad ex ante realizada por terceros; y otros sistemas de IA independientes con implicaciones relacionadas principalmente con los derechos fundamentales, los cuales se indican explícitamente en el anexo III.

1. Clasificación (art.6)

2. Requisitos (art.8) Gestión de riesgos (art.9) Datos y su gobernanza (art.10) Documentación técnica (art.11) Registros de operación (art.12) Transparencia (art.13) Supervisión (art.14) Precisión, robustez y ciberseguridad (art.15)

3. Obligaciones de proveedores, usuarios y otros (art.16)

4. Autoridades notificantes y entidades notificadas (art.30)

5. Normas y conformidad (art. 40)

Título IV: Obligaciones de transparencia (art.52) El título IV se centra en determinados sistemas de IA para tener en cuenta los riesgos específicos de manipulación que conllevan. Se aplicarán obligaciones de transparencia a los sistemas que i) interactúen con seres humanos, ii) se utilicen para detectar emociones o determinar la asociación a categorías (sociales) concretas a partir de datos biométricos, o iii) generen o manipulen contenido (ultrafalsificaciones).

Título V: Medidas para fomentar la innovación (art.53) El título V contribuye al objetivo de crear un marco jurídico que favorezca la innovación, resista el paso del tiempo y sea resiliente a las perturbaciones.

Título VI: Gobernanza (art.56) En el título VI se establecen los sistemas de gobernanza nacionales y a escala de la Unión. En la Unión, la propuesta establece un Comité Europeo de Inteligencia Artificial («el Comité»), integrado por representantes de los Estados miembros y la Comisión.

- Consejo Europeo de IA

- Directrices de la Comisión

- Autoridades nacionales

Título VII: Base de datos europea de sistemas de alto riesgo (art.60) El título VII tiene por objeto facilitar la labor de seguimiento de la Comisión y las autoridades

nacionales mediante el establecimiento de una base de datos para toda la UE donde figuren los sistemas de IA de alto riesgo independientes con implicaciones principalmente para los derechos fundamentales.

Título VIII: Monitorización post-comercialización (art.61-68) En el título VIII se definen las obligaciones de seguimiento y presentación de información que deben cumplir los proveedores de sistemas de IA en relación con el seguimiento posterior a la comercialización y la comunicación e investigación de incidentes y defectos de funcionamientos relacionados con la IA. Las autoridades de vigilancia del mercado controlarían también el mercado e investigarían el cumplimiento de las obligaciones y los requisitos aplicables a todos los sistemas de IA de alto riesgo que ya se han introducido en el mercado

Título IX: Códigos de conducta (art.69) El título IX crea un marco para la elaboración de códigos de conducta, cuyo objetivo es fomentar que los proveedores de sistemas de IA que no son de alto riesgo cumplan de manera voluntaria los requisitos que son obligatorios para los sistemas de IA de alto riesgo

Título X: Confidencialidad (art.70) El título X hace hincapié en la obligación de todas las partes de respetar la confidencialidad de la información y los datos, y establece normas para el intercambio de la información que se obtenga durante la aplicación del Reglamento.

Título XI: Delegación de poderes y procedimientos del comité (art.73) En el título XI se establecen las normas

para el ejercicio de las competencias de delegación y de ejecución. Se remite a los anexos I a VII.

Título XII: Disposiciones finales (art.75-113) En el título XII se recoge la obligación de la Comisión de evaluar regularmente la necesidad de actualizar el anexo III y preparar informes periódicos sobre la evaluación y el examen del Reglamento. Asimismo, establece las disposiciones finales, entre ellas un período transitorio.

3.-Ámbito de aplicación.

Es interesante recordar el objeto del presente Reglamento definido en el art. 1: "El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales, en particular la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de inteligencia artificial («sistemas de IA») en la Unión, así como brindar apoyo a la innovación"

La nueva normativa establece obligaciones para proveedores y usuarios en función del nivel de riesgo de la IA. Aunque muchos sistemas de IA plantean un riesgo mínimo, es necesario evaluarlos todos. El art. 6 de Reglamento establece la clasificación de los riesgos y regula los considerados de alto riesgo.

Riesgo inaceptable

Los sistemas de IA de riesgo inaceptable son los que se consideran una amenaza para las personas y serán prohibidos. Incluyen:

- manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos: por ejemplo, juguetes activados por voz que fomentan comportamientos peligrosos en los niños
- puntuación social: clasificación de personas en función de su comportamiento, estatus socioeconómico o características personales
- sistemas de identificación biométrica en tiempo real y a distancia, como el reconocimiento facial.

Aunque existen algunas excepciones a esta calificación. Por ejemplo, los sistemas de identificación biométrica a distancia "a posteriori", en los que la identificación se produce tras un retraso significativo, se permitirán para perseguir delitos graves y sólo cuando haya previa aprobación judicial, no estando autorizada la identificación biométrica remota en tiempo real.

La definición de «datos biométricos» se encuentra en el artículo 4, punto 14, del Reglamento (UE) 2016/679[10] como los datos personales obtenidos a partir de un

[10] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

También se definen en el artículo 3, punto 18, del Reglamento (UE) 2018/1725, y en el artículo 3, punto 13, de la Directiva (UE) 2016/680[11]con la misma definición.

Es especialmente reseñable a nivel nacional el caso de Mercadona donde instaló, en junio de 2020, como parte de un proyecto piloto, un sistema de identificación mediante reconocimiento facial en cuarenta de sus establecimientos, es decir un sistema biométrico de identificación en tiempo real. El objetivo era reconocer si la persona identificada era alguna de las personas que tenía vigente una sentencia o una orden de alejamiento de Mercadona o sus trabajadores[12].Dicha actuación fue

[11] DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[12]https://facua.org/noticias/mercadona-paga-una-multa-de-25-millones-por-el-sistema-de-reconocimiento-facial-denunciado-por-facua/.

condenada y se confirmó por la AAP Barcelona en auto 72/2021, 15 de Febrero de 2021[13].

El Informe 36/2020, la AEPD diferencia entre identificación biométrica y autenticación o verificación biométrica.

"En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma."

La AEPD concluía que:

"Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica

[13] Roj: SAP B 2184/2021 - ECLI:ES:APB:2021:2184

(uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).”

El Reglamento europeo aclara en los Considerandos 14 a 17 que se excluye los sistemas de IA destinados a la verificación biométrica, que comprende la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, así como la identidad de una persona física con la finalidad exclusiva de que tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local[14]; en cambio sí que

[14]Por el contraposición a espacio cerrado se considera espacio de acceso público según el Considerando 19 «espacio de acceso público» se refiere a cualquier lugar físico al que pueda acceder un número indeterminado de personas físicas y con independencia de si es de propiedad privada o pública y de la actividad para la que pueda utilizarse el lugar, ya sean actividades comerciales (por ejemplo, tiendas, restaurantes, cafeterías), de prestación de servicios (por ejemplo, bancos, actividades profesionales, hostelería), deportivas (por ejemplo, piscinas, gimnasios, estadios), de transporte (por ejemplo, estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte), de entretenimiento (por ejemplo, cines, teatros, museos, salas de conciertos, salas de conferencias), de ocio o de otro tipo (por ejemplo, vías y plazas públicas, parques, bosques, parques infantiles). Asimismo, debe considerarse que un lugar es de acceso público si, con independencia de posibles restricciones de capacidad o de seguridad, el acceso está sujeto a determinadas condiciones previamente definidas que puede satisfacer un número indeterminado de personas, como la adquisición de una entrada o un título de transporte, el registro previo o tener una determinada edad. Por el contrario, un lugar no debe considerarse de acceso público si únicamente pueden acceder a él determinadas personas físicas definidas, ya sea en virtud

ampara y reconoce la identificación biométrica, a fin de determinar la identidad de una persona comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos de referencia, independientemente de que la persona haya dado o no su consentimiento.

En cuanto a la «categorización biométrica» a que hace referencia el Reglamento, se define como la inclusión de personas físicas en categorías específicas en función de sus datos biométricos. No se incluyen los sistemas de categorización biométrica que sean una característica meramente accesoria intrínsecamente vinculada a otro

---

del Derecho de la Unión o del Derecho nacional directamente relacionado con la seguridad pública o en virtud de una clara manifestación de voluntad de la persona que ejerza la autoridad pertinente en dicho lugar. La sentencia de la Audiencia Provincial de Barcelona SAP B 8002/2020 - ECLI:ES:APB:2020:8002 que reproduce la línea ya asentada por la SAP de Madrid, Sección 15ª, de fecha 03/05/2020 que ampara la captación de imágenes por los agentes policiales actuantes en el seno de una investigación policial, pese a tratarse de un espacio cerrado de titularidad privada pero público en cuanto a su uso, aunque de acceso restringido y sin que en el mismo, por su naturaleza se desarrollen actos que afecten al núcleo duro del derecho fundamental a la intimidad personal concernido, sin que dicha autorización judicial esté prevista en la transcrita norma ad hoc, al no presumirse que en dicho espacio se sugiera que en el mismo se puedan realizarse actos de desarrollo de vida privada en el sentido de la protección personal que se le dispensa a la inviolabilidad domiciliaria o en menor espectro que la jurisprudencia del TS o TC ha otorgado a la autorización judicial para la injerencia en el derecho fundamental a la intimidad personal por parte de las Fuerzas y Cuerpos de Seguridad.

servicio comercial, lo que significa que la característica no puede utilizarse, por razones técnicas objetivas, sin el servicio principal y que la integración de dicha característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas del presente Reglamento. La categorización biométrica puede contribuir a la discriminación y vulnerar derechos fundamentales, por ello como establece el Considerando 30 deben prohibirse los sistemas de categorización biométrica basados en datos biométricos de las personas físicas, como la cara o las impresiones dactilares de una persona física, para deducir o inferir las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona física. Dicha prohibición no debe aplicarse al etiquetado, al filtrado ni a la categorización lícitos de conjuntos de datos biométricos adquiridos de conformidad con el Derecho nacional o de la Unión en función de datos biométricos, como la clasificación de imágenes en función del color del pelo o del color de ojos, que pueden utilizarse, por ejemplo, en el ámbito de la aplicación de la ley[15].

Alto riesgo

[15] El artículo 9, apartado 1, del Reglamento (UE) 2016/679 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725 prohíben el tratamiento de datos biométricos con fines distintos de la aplicación de la ley, con las excepciones limitadas previstas en dichos artículos.

Los sistemas de IA que afecten negativamente a la seguridad o a los derechos fundamentales[16] se considerarán de alto riesgo y se dividirán en dos categorías.

1. Los sistemas de IA que se utilicen en productos sujetos a la legislación de la UE sobre la seguridad de los productos[17]. Esto incluye juguetes, aviación, automóviles, dispositivos médicos y ascensores.
2. Los sistemas de IA pertenecientes a ocho ámbitos específicos que deberán registrarse en una base de datos de la UE:

[16] Los derechos fundamentales que pueden estar en riesgo según el Considerando 48 del Reglamento Europeo de IA son el derecho a la dignidad humana, el respeto de la vida privada y familiar, la protección de datos de carácter personal, la libertad de expresión y de información, la libertad de reunión y de asociación, la no discriminación, el derecho a la educación, la protección de los consumidores, los derechos de los trabajadores, los derechos de las personas discapacitadas, la igualdad entre hombres y mujeres, los derechos de propiedad intelectual, el derecho a la tutela judicial efectiva y a un juez imparcial, los derechos de la defensa y la presunción de inocencia, y el derecho a una buena administración.

[17] La «"Guía azul" sobre la aplicación de la normativa europea relativa a los productos, de 2022» establece que la norma general es que la legislación de armonización de la Unión puede ser aplicable a un producto, ya que la comercialización o la puesta en servicio solamente puede producirse cuando el producto cumple toda la legislación de armonización de la Unión aplicable.

- identificación biométrica y categorización de personas físicas
- gestión y explotación de infraestructuras críticas
- educación y formación profesional
- empleo, gestión de trabajadores y acceso al autoempleo
- acceso y disfrute de servicios privados esenciales y servicios y prestaciones públicas
- aplicación de la ley
- gestión de la migración, el asilo y el control de fronteras
- asistencia en la interpretación jurídica y aplicación de la ley[18].

Todos los sistemas de IA de alto riesgo serán evaluados antes de su comercialización y a lo largo de su ciclo de vida. Los ciudadanos y las ciudadanas tendrán derecho a presentar reclamaciones sobre los sistemas de IA a autoridades nacionales específicas.

Establece el considerando 22 del Reglamento que para evitar la elusión del mismo y garantizar la protección efectiva de las personas físicas ubicadas en la Unión, el

[18] También deben considerarse de alto riesgo los sistemas de IA destinados a ser utilizados por los organismos de resolución alternativa de litigios con esos fines, cuando los resultados de los procedimientos de resolución alternativa de litigios surtan efectos jurídicos para las partes. La utilización de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe substituirlas: la toma de decisiones finales debe seguir siendo una actividad humana.

presente Reglamento también debe aplicarse a los proveedores y responsables del despliegue de sistemas de IA establecidos en un tercer país, en la medida en que se pretenda que la información de salida generada por dichos sistemas se utilice en la Unión.

Requisitos de transparencia

La IA generativa[19], como ChatGPT[20], no se considera de alto riesgo, pero tendrá que cumplir requisitos de transparencia[21] y con la legislación de la UE en materia de derechos de autor:

[19] El debate parlamentario sobre la IA generativa fue uno de los motivos en la demora de la aprobación del Reglamento Europeo de IA.
https://www.elperiodico.com/es/internacional/20240313/europa-parlamento-europeo-aprueba-ley-inteligencia-artificial-regulacion-ia-chatgpt-bruselas-union-europea-99388849

[20] ChatGPT (acrónimo del inglés *Chat Generative Pre-Trained Transformer*) es una aplicación de chatbot de inteligencia artificial desarrollado en 2022 por OpenAI que se especializa en el diálogo. El *chatbot* es un modelo de lenguaje ajustado con técnicas de aprendizaje tanto supervisadas como de refuerzo.Está compuesto por los modelosGPT-4 y GPT-3.5 de OpenAI.

[21] Son muchas las garantías que se exigen en esta actividad por las implicaciones que conlleva. Para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo, con sujeción a las garantías adecuadas para los derechos y libertades fundamentales de las personas físicas y tras la aplicación de todas las condiciones aplicables

- revelar que el contenido ha sido generado por IA
- diseñar el modelo para evitar que genere contenidos ilegales
- publicar resúmenes de los datos protegidos por derechos de autor utilizados para el entrenamiento

Los modelos de IA de uso general que cuenten con un alto impacto y que pudieran plantear un riesgo sistémico, como el modelo de IA más avanzado GPT-4, tendrán que someterse a evaluaciones exhaustivas e informar a la Comisión de cualquier incidente grave.

El contenido que haya sido generado o modificado con la ayuda de la IA, como imágenes, audio o vídeos (por ejemplo, las «ultrafalsificaciones»), tendrá que etiquetarse claramente como tal.

Riesgo mínimo o nulo

Esta categoría abarca la mayoría de las aplicaciones de IA utilizados actualmente en la Unión Europea como pueden ser los algoritmos de recomendación, videojuegos habilitados para IA o filtros de spam. Se respalda el uso libre de la inteligencia artificial de riesgo

establecidas en el presente Reglamento, además de las condiciones establecidas en los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680— ser capaces de tratar también categorías especiales de datos personales, como cuestión de interés público esencial en el sentido del artículo 9, apartado 2, letra g), del Reglamento (UE) 2016/679 y del artículo 10, apartado 2, letra g), del Reglamento (UE) 2018/1725

mínimo**.** En este contexto, se reconoce que estos sistemas no presentan riesgos significativos para la salud, seguridad o derechos fundamentales de las personas físicas.

La inclusión de las categorías de riesgo limitado y mínimo refleja la normativa mantiene una evaluación equilibrada y proporcionada del impacto de la IA como principio general, permitiendo la innovación y el desarrollo tecnológico sin imponer restricciones innecesarias.

4.- Ciberseguridad.

El control humano de la IA es esencial, no se puede dejar todo al algoritmo y en todo caso el Reglamento IA regula la posibilidad de los sistemas de IA de alto riesgo incluyan mecanismos orienten e informen a las personas físicas a las que se haya asignado la supervisión humana para que tomen decisiones con conocimiento de causa acerca de si intervenir, cuándo hacerlo y de qué manera, a fin de evitar consecuencias negativas o riesgos, o de detener el sistema si no funciona según lo previsto[22].

[22] Según el Considerando 75 la solidez técnica es un requisito clave para los sistemas de IA de alto riesgo, que deben ser resilientes en relación con los comportamientos perjudiciales o indeseables por otros motivos que puedan derivarse de limitaciones en los sistemas o del entorno en el que estos funcionan (p. ej., errores, fallos, incoherencias o situaciones inesperadas). Por consiguiente, deben adoptarse medidas técnicas y organizativas para garantizar la solidez de los sistemas de IA de alto riesgo, por ejemplo, mediante el diseño y desarrollo de soluciones técnicas adecuadas para prevenir o minimizar ese comportamiento perjudicial o indeseable. Estas

La ciberseguridad[23] es fundamental para garantizar que los sistemas de IA resistan a las actuaciones de terceros maliciosos que, aprovechando las vulnerabilidades del sistema, traten de alterar su uso, comportamiento o funcionamiento o de poner en peligro sus propiedades de seguridad. Pueden ser objetivo de los ataques las vulnerabilidades de los activos digitales del sistema de IA o la infraestructura de TIC, por ello deben crearse y practicarse controles de seguridad. Los riesgos para la ciberresiliencia de un sistema de IA por lo que respecta a los intentos de terceros no autorizados de alterar su uso, comportamiento o funcionamiento, incluidas las vulnerabilidades específicas de la IA, como el

soluciones técnicas pueden incluir, por ejemplo, mecanismos que permitan al sistema interrumpir de forma segura su funcionamiento (planes de prevención contra fallos) en presencia de determinadas anomalías o cuando el funcionamiento tenga lugar fuera de determinados límites predeterminados.

[23]La protección en materia de ciberseguridad relacionada con los riesgos sistémicos asociados al uso malintencionado o a los ataques debe tener debidamente en cuenta las fugas accidentales de modelos, las divulgaciones no autorizadas, la elusión de las medidas de seguridad y la defensa contra los ciberataques, el acceso no autorizado o el robo de modelos. Esta protección podría facilitarse asegurando los pesos, los algoritmos, los servidores y los conjuntos de datos del modelo, por ejemplo, mediante medidas de seguridad operativa para la seguridad de la información, medidas específicas en materia de ciberseguridad, soluciones técnicas adecuadas y establecidas y controles de acceso cibernéticos y físicos, en función de las circunstancias pertinentes y los riesgos existentes.

envenenamiento de datos o los ataques adversarios, así como, los riesgos para los derechos fundamentales.

Por la experiencia de ENISA[24] en materia de política de ciberseguridad y las tareas que se le encomiendan en virtud del Reglamento (UE) 2019/1020, la Comisión debe cooperar con ENISA en las cuestiones relacionadas con la ciberseguridad de los sistemas de IA[25].

5.- Elemento subjetivo.

Son diversas las personas que se mencionan en el Reglamento europeo de IA.

El Considerando 84 del Reglamento incluye en la categoría de proveedor[26] de sistema de alto riesgo a riesgo a cualquier distribuidor, importador, responsable del despliegue u otro tercero que debe asumir todas las obligaciones pertinentes. Se incluye la responsabilidad de esos sujetos cuando se modifica la finalidad prevista de un sistema de IA partiendo de un sistema de IA de

[24] https://www.enisa.europa.eu/about-enisa/about/es. Es la Agencia europea de ciberseguridad.

[25] El procedimiento de evaluación de la conformidad fundamentado en un control interno que se establece en un anexo VI del presente Reglamento.

[26] El art. 3 del Reglamento en su apartado tercero define al «proveedor» como una persona física o jurídica o autoridad, órgano u organismo de otra índole públicos que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca comercial, previo pago o gratuitamente.

uso general, que ya se haya introducido en el mercado o puesto en servicio y que no esté clasificado como sistema de alto riesgo y posteriormente pase a ser un sistema de IA de alto riesgo de conformidad con el Reglamento.

A su vez, el fabricante del producto debe cumplir las obligaciones que el presente Reglamento impone al proveedor y, en particular, debe garantizar que el sistema de IA integrado en el producto final cumpla los requisitos del presente Reglamento según el Considerando 87.

A los terceros[27] que ponen a disposición del público herramientas, servicios, procesos o componentes de IA que no sean modelos de IA de uso general no se les debe imponer la obligación de cumplir los requisitos relativos a las responsabilidades a lo largo de la cadena de valor de la IA, en particular por lo que respecta al proveedor que haya utilizado o integrado dichas herramientas, servicios, procesos o componentes de IA, cuando el acceso a dichas herramientas, servicios, procesos o componentes de IA esté sujeto a una licencia libre y de código abierto como establece el Considerando 89.

[27] Según el Reglamento se debe animar a los desarrolladores de herramientas, servicios, procesos o componentes de IA libres y de código abierto que no sean modelos de IA de uso general a que apliquen prácticas de documentación ampliamente adoptadas, como tarjetas de modelo y hojas de datos, como una forma de acelerar el intercambio de información a lo largo de la cadena de valor de la inteligencia artificial, permitiendo la promoción en la Unión de sistemas de IA fiables. Se intenta potenciar la creación de un sistema seguro.

Los responsables del despliegue deben adoptar las medidas técnicas y organizativas adecuadas para garantizar que se utilizan los sistemas de IA de alto riesgo conforme a las instrucciones de uso, así como que las personas que ponen en práctica las instrucciones de uso y la supervisión humana establecidas en el presente Reglamento tengan las competencias necesarias, en particular un nivel adecuado de alfabetización, formación y autoridad en materia de IA para desempeñar adecuadamente dichas tareas.

Los empleadores tienen la obligación de informar y consultar a los trabajadores o a sus representantes sobre la decisión de poner en servicio o utilizar sistemas de IA[28], Los responsables del despliegue de un sistema de IA de alto riesgo desempeñan un papel fundamental a la hora de garantizar la protección de los derechos fundamentales, como complemento de las obligaciones del proveedor al desarrollar el sistema de IA. Dentro de la información que se debe facilitar[29] debe incluirse la

[28]Existe un derecho a la información que es accesorio y necesario para el objetivo de protección de los derechos fundamentales de los trabajadores.

[29] Es preciso notificar a las personas físicas cuando estén expuestas a sistemas que, mediante el tratamiento de sus datos biométricos, puedan determinar o inferir sus emociones o intenciones o incluirlas en categorías específicas. Estas categorías específicas pueden referirse a aspectos como el sexo, la edad, el color del pelo, el color de ojos, los tatuajes, los rasgos personales, el origen étnico o las preferencias e intereses personales. Esta información y estas notificaciones deben facilitarse en formatos accesibles a las personas con discapacidad.

finalidad prevista y el tipo de decisiones que se toman por medio del sistema de IA.

Los responsables del despliegue de sistemas de IA de alto riesgo que sean organismos de Derecho público o los operadores privados que presten servicios públicos y los operadores que desplieguen determinados sistemas de IA de alto riesgo enumerados en un anexo III del Reglamento, como las entidades bancarias o de seguros, deben llevar a cabo una evaluación de impacto relativa a los derechos fundamentales antes de su puesta en funcionamiento.

La evaluación de impacto[30] debe aplicarse al primer uso del sistema de IA de alto riesgo y debe actualizarse cuando el responsable del despliegue considere que alguno de los factores pertinentes ha cambiado.

Cuando el proveedor de un modelo de IA[31] de uso general integre un modelo propio en un sistema de IA

[30]Para evaluar el impacto, los responsables del despliegue de un sistema de IA de alto riesgo, en particular cuando el sistema de IA se utilice en el sector público, pueden contar con la participación de las partes interesadas pertinentes, como los representantes de grupos de personas que probablemente se vean afectados por el sistema de IA, expertos independientes u organizaciones de la sociedad civil, tanto en la realización de dichas evaluaciones de impacto y en el diseño de las medidas que deben adoptarse en caso de materialización de los riesgos.
[31]Los modelos de IA de uso general permiten la generación flexible de contenidos, por ejemplo, en formato de texto, audio, imágenes o vídeo, que pueden adaptarse fácilmente a una amplia gama de tareas diferenciadas por ello son según el

propio que se comercialice o ponga en servicio, se debe considerar que dicho modelo se ha introducido en el mercado y, por tanto, se deben seguir aplicando las obligaciones establecidas en el presente Reglamento en relación con los modelos, además de las establecidas en relación con los sistemas de IA. Su responsabilidad es particular a lo largo de la cadena de valor de la IA, ya que los modelos que suministran pueden constituir la base de diversos sistemas de etapas posteriores, que a menudo son suministrados por proveedores posteriores que necesitan entender bien los modelos y sus capacidades, tanto para permitir la integración de dichos modelos en sus productos como para cumplir sus obligaciones en virtud del presente Reglamento o de otras normas[32].

La Oficina de IA debe supervisar si el proveedor ha cumplido dichas obligaciones, fomentar y facilitar la

Considerando 99 de Reglamento los grandes modelos de IA generativa.

[32]Existe la obligación de presentar un resumen del contenido utilizado para el entrenamiento del modelo y la obligación de adoptar directrices para el cumplimiento del Derecho de la Unión en materia de derechos de autor. Según el estado de la técnica en el momento de la entrada en vigor del presente Reglamento, la cantidad acumulada de cálculos utilizados para el entrenamiento del modelo de IA de uso general, medida en operaciones de coma flotante (FLOPS), es una de las aproximaciones de las capacidades del modelo. Este umbral será deberá ir ajustando para reflejar los cambios tecnológicos e industriales, como las mejoras algorítmicas o el aumento de la eficiencia del hardware, y debe complementarse con parámetros de referencia e indicadores de la capacidad de los modelos.

elaboración, revisión y adaptación de códigos de buenas prácticas, teniendo en cuenta los enfoques internacionales. Los códigos de buenas prácticas deben centrarse en medidas específicas de evaluación y reducción de riesgos. Los proveedores deben poder basarse en códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones. Debe presumirse que se han cumplido las obligaciones correspondientes del presente Reglamento a menos que surjan riesgos sistémicos significativos no cubiertos por el Reglamento (UE) 2022/2065[33] y se detecten en dichos modelos. Dichos prestadores también están obligados a adoptar las medidas de reducción de riesgos adecuadas respetando los derechos fundamentales. Cuando un proveedor indica que un sistema de IA es conforme con los requisitos establecidos en el capítulo II, sección 2, y con otros actos aplicables de la legislación de armonización de la Unión enumerados en el anexo I se debe poner la marca CE en el producto. El distribuir debe comprobar la existencia de dicha marca.

La Comisión debe poder establecer, mediante actos de ejecución y previa consulta al foro consultivo, especificaciones comunes para determinados requisitos previstos en el presente Reglamento.

Sin perjuicio del uso de normas armonizadas y especificaciones comunes debe presumirse que los proveedores de un sistema de IA de alto riesgo han

[33]Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales).

entrenado y probado con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto que se utilice el sistema de IA cumplen la medida pertinente prevista en el requisito en materia de gobernanza de datos establecido en el presente Reglamento.

Para poder realizar las evaluaciones externas de la conformidad[34], las autoridades nacionales competentes deben notificar, a los organismos notificados, siempre que cumplan una serie de requisitos[35]. Las autoridades nacionales competentes deben enviar la notificación[36] de dichos organismos a la Comisión y a los demás Estados miembros a través del sistema de notificación electrónica desarrollado y gestionado por la Comisión con arreglo a

[34] Si el sistema de IA se considera un sistema de IA nuevo debe someterse a una nueva evaluación de la conformidad. Sin embargo, los cambios que se produzcan en el algoritmo y en el funcionamiento de los sistemas de IA que sigan «aprendiendo» después de su introducción en el mercado o su puesta en servicio no deben constituir una modificación sustancial, siempre que dichos cambios hayan sido predeterminados por el proveedor y se hayan evaluado en el momento de la evaluación de la conformidad.

[35] Los requisitos se refieren a independencia, sus competencias y la ausencia de conflictos de intereses, así como requisitos adecuados de ciberseguridad.

[36] El art. 3 del Reglamento en su apartado 19 define la «autoridad notificante» como la autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión.

lo dispuesto en el artículo R23 del anexo I de la Decisión n.º 768/2008/CE[37].

Se regulan también las autoridades de vigilancia de mercado[38]. Su función es muy relevante dado que por motivos de seguridad pública o con vistas a proteger la vida y la salud de personas físicas, el medio ambiente y activos fundamentales de la industria y de las infraestructuras pueden autorizar la introducción en el mercado o la puesta en servicio de sistemas de IA que no hayan sido sometidos a una evaluación de la conformidad.

Previo acuerdo entre las autoridades nacionales competentes y los participantes en el espacio controlado de pruebas para la IA, las pruebas en condiciones reales también podrán gestionarse y supervisarse en el marco del espacio controlado de pruebas para la IA.

[37]El Comité debe establecer dos subgrupos permanentes a fin de proporcionar una plataforma de cooperación e intercambio entre las autoridades de vigilancia del mercado y las autoridades notificantes sobre cuestiones relacionadas, respectivamente, con la vigilancia del mercado y los organismos notificados.

[38]Cada Estado miembro debe designar al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado como autoridades nacionales competentes que se encarguen de supervisar su aplicación y ejecución. Los Estados miembros pueden decidir designar cualquier tipo de entidad pública para que desempeñe las tareas de las autoridades nacionales competentes en el sentido del presente Reglamento, de conformidad con sus características y necesidades organizativas nacionales específicas.

Los Estados miembros deben utilizar los canales existentes y establecer, cuando proceda, nuevos canales de comunicación específicos con las pymes, las empresas emergentes, los responsables del despliegue, otros innovadores y, cuando proceda, las autoridades públicas locales, para apoyar a las pymes durante toda su trayectoria de desarrollo ofreciendo orientaciones y respondiendo a las preguntas sobre la aplicación del presente Reglamento.

Organismos europeos en el desarrollo del presente Reglamento son Agencia de los Derechos Fundamentales de la Unión Europea, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Comité Europeo de Normalización (CEN)[39], el Comité Europeo de Normalización Electrotécnica (Cenelec) y el Instituto Europeo de Normas de Telecomunicaciones (ETSI).

Se creará un foro consultivo para proporcionar conocimientos técnicos y asesorar al Comité y a la Comisión, así como para contribuir a las funciones de estos en virtud del presente Reglamento según el art. 67 del Reglamento.

6.- Responsabilidad y sanciones.

El Considerando 168 establece que se debe poder exigir el cumplimiento del presente Reglamento mediante la imposición de sanciones y otras medidas de ejecución respectando el principio de *non bis in idem.* Deben

[39]https://www.cnmc.es/ambitos-de-actuacion/postal/actividad-internacional/comite-europeo-de-normalizacion

establecerse los límites máximos para la imposición de las multas administrativas en el caso de ciertas infracciones concretas. A la hora de determinar la cuantía de las multas, los Estados miembros deben tener en cuenta todas las circunstancias pertinentes de la situación en cuestión, considerando especialmente la naturaleza, gravedad y duración de la infracción y de sus consecuencias, así como el tamaño del proveedor, en particular si este es una pyme o una empresa emergente.

Deben establecerse multas de una cuantía apropiada en caso de incumplimiento de las obligaciones del Reglamento con sujeción a los plazos de prescripción pertinentes de conformidad con el principio de proporcionalidad.

Todas las decisiones adoptadas por la Comisión en virtud del presente Reglamento están sujetas al control del Tribunal de Justicia de la Unión Europea, de conformidad con lo dispuesto en el TFUE.

Las personas físicas y jurídicas cuyos derechos y libertades se vean perjudicados por el uso de sistemas de IA tiene el derecho a presentar una reclamación ante la correspondiente autoridad de vigilancia del mercado o el pertinente recurso.

Igualmente, las personas afectadas deben tener derecho a obtener una explicación clara y significativa de un responsable del despliegue cuando dicha decisión produzca efectos jurídicos o afecte significativamente de modo similar a dichas personas, de manera que

consideren que tiene un efecto negativo en su salud, su seguridad o sus derechos fundamentales.

7.- Regulación de la IA a nivel mundial.

En EEUU el presidente Joe Biden emitió una orden ejecutivo el día 30 de octubre de 2023, la Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence [40]para el desarrollo de una IA segura, la protección de la privacidad de los estadounidenses, la promoción de la equidad y los derechos civiles, la defensa de los consumidores y trabajadores, la promoción de la innovación y la competencia, promover el liderazgo estadounidense en materia de IA y garantizar el uso gubernamental responsable y eficaz de la IA. Se pretende provechar la IA para siempre y aprovechar sus innumerables beneficios y para ello se requiere mitigar sus riesgos sustanciales.

Se reseña la rápida velocidad a la que avanzan las capacidades de IA y que impulsa la necesidad de regulación en materia de IA en dicha nación para tomar la delantera por el bien su seguridad, economía y sociedad. Para fijar dicha regulación debe tenerse en cuenta las opiniones de otras agencias, la industria, los miembros de Academia, sociedad civil, sindicatos, aliados y socios internacionales y otras organizaciones relevantes.

[40]https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

Tanto en el desempeño como en la posterior a la implementación debe garantizarse el uso indebido de la IA, la eliminación de modificaciones peligrosas y un desarrollo ético, seguro y en el que se cumpla con las leyes y políticas federales aplicables. Al igual que en la UE por la Administración se pretende desarrollar mecanismos efectivos de etiquetado y procedencia del contenido, para que los estadounidenses puedan determinar cuándo el contenido se genera utilizando IA y cuándo no.

El desarrollo y uso responsable de la IA requiere un compromiso de apoyar a los trabajadores estadounidenses. La IA no debe implementarse de manera que socave los derechos, empeore la calidad del empleo, fomente una vigilancia indebida de los trabajadores, reduzca la competencia en el mercado, introduzca nuevos riesgos para la salud y la seguridad o cause perturbaciones perjudiciales en la fuerza laboral.

Los sistemas de Inteligencia Artificial implementados de manera irresponsable han reproducido e intensificado las desigualdades existentes, han causado nuevos tipos de discriminación dañina y han exacerbado los daños físicos y en línea por ello debe evitarse implementar de una manera inadecuada. Para ello ya se han emitido el Plan para una Declaración de Derechos de la IA, el Marco de Gestión de Riesgos de la IA y la Orden Ejecutiva 14091 del 16 de febrero de 2023 (Avanzando aún más en la equidad racial y el apoyo a las personas desatendidas).

También hay que destacar que EEUU ha alcanzado un acuerdo con las grandes empresas tecnológicas OpenAI,

Alphabet, Meta Platforms, Anthropic, Inflection, Amazon y Microsoft[41].

En el caso de la República Popular China[42] en el año 2017 el Consejo de Estado publicó el Plan de Desarrollo de la IA de Próxima Generación (Plan 2017), que propone una visión general de la futura política de IA y articula las consideraciones clave que los funcionarios chinos deberían adoptar al llevar a cabo tareas departamentales. Para implementar el Plan 2017, el gobierno chino estableció dos instituciones: el Comité Asesor Estratégico de IA (Comité y la Oficina de Planificación y Promoción de IA. Liderados por el Ministerio de Ciencia y Tecnología, estos organismos se convirtieron en las primeras instituciones responsables exclusivamente de supervisar la política de IA a nivel nacional. En 2019, el Comité creó un organismo especializado adicional para fortalecer la investigación sobre cuestiones legales, éticas y sociales relacionadas con las tecnologías de inteligencia artificial de próxima generación, así como profundizar la cooperación internacional.

Se han promulgado rápidamente regulaciones obligatorias y específicas de tecnología que han

[41]https://elpais.com/internacional/2023-07-21/estados-unidos-lanza-nuevas-reglas-para-la-inteligencia-artificial.html#
[42]https://www.twobirds.com/en/insights/2024/china/ai-governance-in-china-strategies-initiatives-and-key-considerations

cambiado drásticamente el panorama de la gobernanza de la IA en China. Los tres más importantes son:

Disposiciones sobre gestión de recomendaciones algorítmicas del Servicio de información de Internet de 2021 (Disposiciones sobre algoritmos de recomendación de 2021, vigentes a partir del 1 de marzo de 2022).

Disposiciones de gestión de síntesis profunda del servicio de información de Internet 2022 (Disposiciones de síntesis profunda de 2022, vigentes a partir del 1 de enero de 2023).

Las Medidas para la Gestión de Servicios de Inteligencia Artificial Generativa 2023 (Medidas de IA Generativa de 2023, en vigor desde el 15 de agosto de 2023).

Existe un creciente número de documentos regulatorios de IA desarrollados por los gobiernos provinciales. Ciudades piloto como Shenzhen y Shanghai han tomado la iniciativa en la emisión de regulaciones para promover el desarrollo de la IA y crear experimentos administrativos a nivel local para atraer inversiones en IA y la aprobación política del gobierno central. Existe un Plan de Trabajo Legislativo 2023 del Consejo de Estado que formularán una ley general de IA en los próximos años, a pesar de ello en la actualidad cuenta con una regulación muy fragmentada. Los objetivos principales son los contenidos e información generados y difundidos en línea, la protección y seguridad de los datos personales y el uso de algoritmos para tomar decisiones sobre individuos. Como consecuencia del XX Congreso Nacional del Partido Comunista de China, celebrado del 16 al 22 de octubre de 2022.

El Plan de Trabajo Legislativo 2023 [43]crea una norma compuesta por 73 artículos y estructurados en siete capítulos. En su art. 2 se establece que el ámbito de aplicación es la investigación y desarrollo, suministro y uso de la IA, así como a la regulación de la IA, dentro de las fronteras de la República Popular de China (RPC). Sin embargo, añade una previsión de extraterritorialidad al establecer que "Las actividades relacionadas con la investigación y el desarrollo, el suministro y el uso de la IA realizadas fuera del territorio de la RPC que afecten o puedan afectar a la seguridad nacional, los intereses públicos o los derechos e intereses legítimos de personas u organizaciones de la RPC, están sujetas a ésta.

Reino Unido es el país donde se encuentra la sede de Google DeepMind[44], ha dicho que no tiene la intención de regular la IA a corto plazo. Sin embargo, cualquier empresa de fuera de la UE, la segunda economía más grande del mundo tendrá que cumplir la Ley de IA si quiere hacer negocios en el bloque comercial.

Anu Bradford, catedrática de Derecho de la Universidad de Columbia, ha llamado a esto el "efecto Bruselas"[45]: al ser la primera en regular, la UE puede establecer la norma mundial *de facto*, configurando la forma en que el

[43]https://diariolaley.laleynext.es/dll/2023/09/01/china-aprueba-una-regulacion-de-la-inteligencia-artificial-y-de-la-inteligencia-artificial-generativa

[44] Google DeepMind es una compañía inglesa de investigación y desarrollo de inteligencia artificial inglesa adquirida en 2014 por Alphabet Inc, empresa matriz de Google.

[45] Anu Bradford, *The Brussels Effect: How the European Union Rules the World, 2020.*

mundo hace negocios y desarrolla la tecnología. La UE lo consiguió con su estricto régimen de protección de datos, el RGPD, que se ha copiado en todos los países. Se espera el mismo efecto respecto de la regulación la IA.

En África[46] el Instituto Africano de las Ciencias Matemáticas[47] lanzó una maestría en inteligencia artificial, patrocinada por Facebook y Google. En Lagos, el centro *Data Science Nigeria* se ha fijado el objetivo de formar un millón de nigerianos/as en ciencias de datos para el 2027 y de crear un ecosistema pujante para hacer del país un socio ideal a escala internacional. En 2020 se creó el Instituto Etíope de Inteligencia Artificial[48] que tiene como objetivo ser el principal centro africano de investigación y desarrollo de IA para 2030 y desempeñar un papel clave en la creación de soluciones innovadoras basadas en IA.

Ruanda [49] tiene en su capital Kigali la Noorsken Kigali House, impulsada por una fundación sueca homónima, un centro de emprendimiento digital más grande del continente. A través de *start-up*, incuban o aceleran ideas innovadoras para concretarlas en negocios viables. En Ruanda se encuentra la sede de Smart África una colaboración intergubernamental entre más de 30 países

[46] https://idrc-crdi.ca/es/historias/inteligencia-artificial-la-africana
[47] https://idrc-crdi.ca/es/iniciativa/instituto-africano-de-ciencias-matematicas
[48] https://www.aii.et/
[49]https://elpais.com/planeta-futuro/2022-10-06/ruanda-aspira-a-convertirse-en-el-silicon-valley-africano.html

para mejorar la conectividad e impulsar transformaciones digitales.

En Sudáfrica[50] existen 5 centros de investigación y 1.000 investigadores dedicados a áreas como aprendizaje automático, procesamiento del lenguaje natural y visión artificial. Las aplicaciones de IA se extienden a sectores como finanzas, salud, agricultura, minería y manufactura, con ejemplos que van desde la detección de fraude hasta la automatización de procesos. A través de la IA se ve un fuerte potencial para el desarrollo económico y social en África.

8.-Conclusiones

Efectuar una regulación de los sistemas de IA es prever a ciegas como avanzará el estado de la tecnología y los posibles problemas que puedan existir en el futuro con la aplicación de los mismos. Por ello es comprensible que la regulación sea parca, abierta e indefinida en algunos aspectos. Este Reglamento supone el esqueleto sobre el que empezar a trabajar de forma armonizada en el futuro, establece unas premisas y unos mínimos a cumplir en aras al respecto de los derechos de los ciudadanos y tratando de evitar las formas de discriminación, vulneraciones indeseadas y proteger en la medida de los posible los datos de los usuarios.

Existe una falta de concreción de las autoridades nacionales que se encargarán de la notificación,

[50] FS_Inteligencia artificial en Sudáfrica 2024_REV.pdf

vigilancia de mercado, sus requisitos, su forma de actuar y las funciones concretas que desempeñarán.

La exclusión de la IA generativa como sistema de alto riesgo es una cuestión no pacífica pero posiblemente necesaria para la aprobación del Reglamento debido a su complejidad y la extensa regulación que conllevaría.

Considero que a la larga se irá revisando la inclusión de algunas actividades dentro del sistema de alto riesgo y se irán recalificando los niveles de riesgo de otras tantas. La práctica y el uso de los sistemas de IA serán los indicadores de esa necesidad de calificación. Está prevista la necesidad de revisión por parte de la Comisión y la comunicación al Parlamento y al Consejo en principio a los dos años de la entrada en vigor del Reglamento y posteriormente cada cuatro años debe efectuarse una revisión. Me parece más acertado el periodo de dos años que el de cuatro dado que los cambios y evolución de la tecnología pueden ser muy repentinos.

Es fundamental el reconocimiento del derecho de los ciudadanos al conocimiento de las situaciones en las que se están utilizando sistemas de IA. Son esenciales las tareas de supervisión humana y notificación al ciudadano de la información sobre la información del funcionamiento de los sistemas de IA que deben tender a alcanzar el máximo nivel de seguridad y transparencia.

Recuerda a la carrera espacial que se inició en 1955 la prisa que tienen los países por efectuar una regulación

sobre sistemas que utilizan IA[51], cuando de la lectura de sus propuestas se deduce que se tiende a unas mismas premisas y sistemas de mínimos donde se respeten los derechos de los ciudadanos. Por ello, tal vez sería más interesante el establecimiento de unos estándares uniformes a nivel mundial máxime cuando el uso de las nuevas tecnologías traspasa fronteras en el mundo globalizado actual en el que vivimos. La otra opción es esperar a que el efecto Bruselas sea efectivo también en materia de IA tras la regulación efectuada por la UE.

BIBLIOGRAFÍA:

BARONA VILAR, SILVIA., "La digitalización y la algoritmización, claves del nuevo paradigma de justicia eficiente y sostenible" en *Uso de la información y de los datos personales en los procesos: los cambios en la Era Digital*. *Edit. Thomson and Reuters-Aranzadi*, 2021.

CONDE FUENTES JESÚS., y SERRANO HOYO, GREGORIO., (Dir.), *La justicia digital en España y la Unión Europea: situación actual y perspectivas de futuro*. Edit. Atelier libros jurídicos. 2019.

FERNANDEZ HERNÁNDEZ, CARLOS., "Aproximación al fututo marco normativo europeo de la inteligencia artificial", núm. 23 (julio-septiembre de 2021) *Revista de Privacidad y Derecho Digital.*

MORENO CATENA, VICTOR., "Los datos en el sistema de justicia y la propuesta del Reglamento UE sobre

[51] https://www.technologyreview.es//s/16069/vuelta-al-mundo-por-las-regulaciones-de-la-ia-en-2024

Inteligencia Artificial en Uso de la información y de los datos personales en los procesos: los cambios en la Era Digital" *Edit.Thomson and Reuters-Aranzadi*, 2021.

O´NEIL CATHY., *Armas de destrucción matemática: como el Big data aumenta la desigualdad y la amenaza de la democracia*. Editorial Capitán Swing, 2018.

VELASCO NÚÑEZ, ELOY., *Marco normativo de la UE para la transformación digital.* Edit. La Ley. 2023.

VIGURI CODERO, JORGE AGUSTÍN., *La implementación del Reglamento General de Protección de Datos en España y el impacto de sus cláusulas abiertas*. Edit. Tirant lo Blanch, Valencia, 2023.

EDITORIAL

En el número 42 de la Revista Gabilex, se incluyen en la sección nacional cinco artículos doctrinales todos ellos de máximo interés.

En primer lugar, debe destacarse el excelente trabajo de Dª. Esther Molina Castañer con el artículo que lleva por título "Análisis del reglamento europeo de inteligencia artificial (AIA)."

El siguiente artículo que podrán disfrutar los lectores corresponde a Dª. María Belén Robleño Mariano, con el

artículo que lleva por título "El recurso de casación autonómico ante el orden jurisdiccional Contencioso-Administrativo". La autora pone de manifiesto que urge una regulación del recurso de casación autonómico que sea completa y garantice la uniformidad en la interpretación y aplicación del derecho autonómico, esto es, la función del propio recurso.

A continuación, Dª Almudena Monge González analiza con brillantez la incorporación de la perspectiva de género en los contratos públicos como herramienta esencial para lograr una compra pública responsable.

Dª Mª Teresa Ortega-Villaizán Santiago aborda bajo el título "El carácter preceptivo de las cláusulas sociales en la contratación pública" un interesante trabajo sobre la transversalidad de las cláusulas sociales, en particular las de carácter laboral y cómo pueden introducirse en las distintas fases de la contratación, desde la preparación del contrato hasta su ejecución.

A continuación, Dª. Miriam Carralero Valera en el "Dictamen jurídico-civil sobre nulidad de escritura de reconocimiento de deuda otorgada en virtud de poder de ruina" explica las actuaciones seguidas por el letrado en un procedimiento civil, en un caso de un poder otorgado por una hija a su padre que lo utiliza para autocontratar en perjuicio de ella.

Dentro de la sección Reseña de Jurisprudencia, Dª Paloma Cascales Bernabeu trata bajo el título "Violencia económica: una dimensión invisibilizada de la violencia de género. Análisis jurisprudencial", el fenómeno de la violencia económica desde una perspectiva jurídico-

práctica, con especial atención al artículo 227 del Código Penal y a la jurisprudencia más reciente del Tribunal Supremo.

Por último, la Revista se cierra con la Recensión de D. José Joaquín Jiménez Vacas sobre la obra «Tecnocracia y Buen Gobierno», un manual de gobierno, que hará las delicias de los autores.

El Consejo de Redacción